

(b) (6)

From:

(b) (6), (b) (7)(C), (b) (7)(F), (b) (7)(E)

Sent:

Friday, December 9, 2016 1:32 PM

To:

(b) (6), (b) (7)(C), (b) (7)(F), (b) (7)(E)

Subject:

President Obama orders full review of Russian hacking during the 2016 election

<http://www.latimes.com/nation/la-na-hacking-election-20161209-story.html>

(b) (6), (b) (7)(C), (b) (7)(F), (b) (7)(E)

U.S. Department of Energy LNO

Cyber Threat Intelligence

Department of Homeland Security

National Cybersecurity & Communication Integration Center

(b) (7)(E), (b) (7)(F)

e-mail (b) (6), (b) (7)(C), (b) (7)(F), (b) (7)(E)

SIPR:

JWIC

(b) (6)

From: (b) (6), (b) (7)(C), (b) (7)(F), (b) (7)(E)
Sent: Friday, December 16, 2016 8:14 AM
To: (b) (6), (b) (7)(C), (b) (7)(F), (b) (7)(E)
Cc: NCCIC - USCERT
Subject: Russian-Speaking Hacker Selling Access to the US Election

Title: Russian-Speaking Hacker Selling Access to the US Election
Assistance Commission
Source: (b) (6) Recorded Future blog
Date Published: 15 December 2016

Excerpt:

"On December 1, 2016, Recorded Future threat intelligence technology identified chatter related to a suspected breach of the U.S. Election Assistance Commission (EAC).

Further research identified a Russian hacker (Recorded Future refers to this actor as Rasputin) soliciting a buyer for EAC database access credentials.

The EAC was established by the Help America Vote Act of 2002 (HAVA), and among many other responsibilities, the Commission is mandated to test and certify voting equipment, maintain the National Voter Registration form, and administer a national clearinghouse on elections. This includes developing shared practices, distributing information for voters, and providing other resources to improve elections. EAC also accredits testing laboratories and voting systems, as well as conducts a financial audit of HAVA programs.

...

It's unclear how long the EAC vulnerability has been active; however, it could have been potentially discovered and accessed by several parties independently. Based on Rasputin's historical criminal forum activity, Recorded Future believes it's unlikely that Rasputin is sponsored by a foreign government. Recorded Future's artificial intelligence technology is continuously scanning and analyzing the internet for updated threat indicators and tactics. Prior to this incident, no previous malicious activity related to EAC has been identified."

To read the complete article see:

<<https://www.recordedfuture.com/rasputin-eac-breach/>>

(b) (6), (b) (7)(C), (b) (7)(F), (b) (7)(E)

U.S. Department of Energy LNO
Cyber Threat Intelligence
Department of Homeland Security

National Cybersecurity & Communication Integration Center
(b) (7)(E), (b) (7)(F)

e-mail (b) (6), (b) (7)(C), (b) (7)(F), (b) (7)(E)

SIPR:

JWIC

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<http://oversight.house.gov>

October 20, 2017

The Honorable Robert Kolasky
Acting Deputy Under Secretary
National Protections and Programs Directorate
Department of Homeland Security
Washington, DC 20528

Dear Acting Deputy Under Secretary Kolasky:

Last month, the Department of Homeland Security reportedly notified election officials in 21 states that Russian government hackers had targeted those states during the 2016 election.¹ We are writing to request copies of these notifications and additional documents, as well as a briefing from top Department officials on these matters.

The Department's notifications to these states came nearly a year after the election and three months after the Department publicly disclosed that individuals connected with the Russian government sought to hack voter registration files and public election sites in 21 states.² They also came after numerous other reports that Russia engaged in a multifaceted campaign to disrupt the 2016 election, including widespread cyber-attacks on state-election infrastructure systems.³

The Department's recent convening of the Government Coordinating Council for the Election Infrastructure Subsector, with representatives from the Election Assistance Commission, the National Association of Secretaries of State and state and local election officials, will hopefully facilitate the sharing of information and expertise.⁴

¹ *DHS Tells States About Russian Hacking During 2016 Election*, Washington Post (Sept. 22, 2017) (online at www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.55b916d66ca3).

² *Russians Tried to Hack Election Systems in 21 States, U.S. Officials Say*, Chicago Tribune (June 21, 2017) (online at www.chicagotribune.com/news/nationworld/ct-homeland-security-chief-intelligence-panel-20170621-story.html).

³ See, e.g., Department of Homeland Security, *Joint Analysis Report: GRIZZLEY STEPPE—Russian Malicious Cyber Activity* (Dec. 29, 2016) (online at www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf); Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (Jan. 6, 2017) (online at www.dni.gov/files/documents/ICA_2017_01.pdf).

⁴ Department of Homeland Security, *DHS and Partners Convene First Election Infrastructure Coordinating Council* (Oct. 14, 2017) (online at www.dhs.gov/news/2017/10/14/dhs-and-partners-convene-first-election-infrastructure-coordinating-council).

We request that you produce, by October 31, 2017, copies of the notifications sent by the Department to these 21 states, as well as all accompanying materials relating to Russian government-backed attempts to hack state election systems.

We also request a briefing from appropriate Department officials within the same timeframe on the following issues:

- (1) the types of voting equipment that were attacked;
- (2) the timeline by which the Department provided information to these states and the reasons for not sharing additional information sooner;
- (3) services and trainings offered to states to detect and prevent cyber-attacks;
- (4) plans to work with states to detect and prevent future cyber-attacks; and
- (5) the operational plans and goals of the newly convened Election Infrastructure Coordinating Council.

If you have any questions, please contact Jennifer Daehn with the Democratic Committee staff at (202) 225-5051. Thank you for your consideration of this request.

Sincerely,



Elijah E. Cummings
Ranking Member
Committee on Oversight and
Government Reform



Robin Kelly
Ranking Member
Subcommittee on
Information Technology

cc: The Honorable Trey Gowdy, Chairman
Committee on Oversight and Government Reform

The Honorable Will Hurd, Chairman
Subcommittee on Information Technology

From: [Manfra, Jeanette](#)
To: (b) (6)
Subject: FW:
Date: Wednesday, December 13, 2017 12:18:22 PM

From: (b) (6)
Sent: Friday, September 29, 2017 5:22 PM
To: Krebs, Christopher (b) (6) Kolasky, Robert
(b) (6) Manfra, Jeanette (b) (6)
Cc: (b) (6)
(b) (6) Taylor, Cindy (b) (6) Hess, David
(b) (6) Ahr, Daniel (b) (6)
Subject: FW:

(b) (5)

From: (b) (6)]
Sent: Friday, September 29, 2017 5:08 PM
To: (b) (6) (b) (6)
Cc: (b) (6)

Subject:

(b) (6)

We would be interested to hear from DHS about their response to the below story raising questions about the notification. If you had any info or explanation, we'd appreciate it.

Thanks
(b) (6)

Holes punched in latest Russia hacking claims

State officials are punching holes in recent claims by the federal government that their election systems were targeted last year by hackers believed to be Russian

agents.

Department of Homeland Security officials notified officials in 21 states last week about the hacking attempts.

But California Secretary of State Alex Padilla issued a statement this week saying the “scanning activity” in question happened on the California Department of Technology statewide network, “not any Secretary of State website.”

“Based on this additional information, California voters can further rest assured that the California Secretary of State elections infrastructure and websites were not hacked or breached by Russian cyber actors,” he said. “Our notification from DHS last Friday was not only a year late, it also turned out to be bad information.”

According to the Associated Press, DHS also has reversed course and told Wisconsin officials the Russian government did not scan the state’s voter registration system, though later reiterated that it still believed it was one of 21 targeted states.

Homeland Security first told state elections officials last Friday that Wisconsin was one of the states targeted. But on Tuesday, Homeland Security said an agency that doesn’t deal with elections was the target of scans by Russian IP addresses.

The situation appeared to be similar in California.

In response, though, the DHS maintained that states were nevertheless targeted in some fashion.

“The Department stands by its assessment that Internet-connected networks in 21 states were the target of Russian government cyber actors seeking vulnerabilities and access to U.S. election infrastructure,” the statement said.

DHS said in most of the 21 states, “only preparatory activity like scanning was

observed.”

Some involved “direct scanning of targeted systems” and others involved “malicious actors” who “scanned for vulnerabilities in networks that may be connected to those systems or have similar characteristics in order to gain information about how to later penetrate their target.”

“This assessment was based on a variety of sources, including scanning detected from malicious IP addresses and intelligence information that cannot be publicly disclosed,” DHS said.

The DHS warning last week was quickly picked up by Democratic lawmakers, who complained about the year delay in notification and pointed to the warning as further evidence of Russian interference in last year’s election.

"We have to do better in the future," said Sen. Mark Warner, D-Va., the vice chairman of the Senate Intelligence Committee -- which is also investigating Russian meddling in last year's election.

In most cases, the states had not known until notified by DHS Friday. The government did not say initially who was behind the hacking attempts or provide details about what had been sought. But officials told the AP the hackers were believed to be Russian agents.

The disclosure to the states comes as a special counsel probes whether there was any coordination during the 2016 presidential campaign between Russia and associates of Donald Trump.

Fox News’ Jake Gibson and Bill Mears and The Associated Press contributed to this report.

From: [Manfra, Jeanette](#)
To: (b) (6)
Subject: FW: News from the WEC: Update on Wisconsin Elections Cyber Security
Date: Wednesday, December 13, 2017 12:11:38 PM
Attachments: [image004.png](#)
[image005.png](#)
[image003.emz.msg](#)
[NR Elections - Election Security UPDATE 9-29-17.pdf](#)
[~WRD000.jpg](#)
[image002.jpg](#)

From: (b) (6)
Sent: Friday, September 29, 2017 2:53 PM
To: Manfra, Jeanette (b) (6) Kolasky, Robert (b) (6)
Figueroa, Juan (b) (6) Mitchell,
Jeffrey R (b) (6) Horne, Sabra (b) (6)
Cc: Robinson, Ernest (b) (6) Taylor, Cindy (b) (6)
Subject: FW: News from the WEC: Update on Wisconsin Elections Cyber Security

Fyi – Wisconsin put out another release, attached.

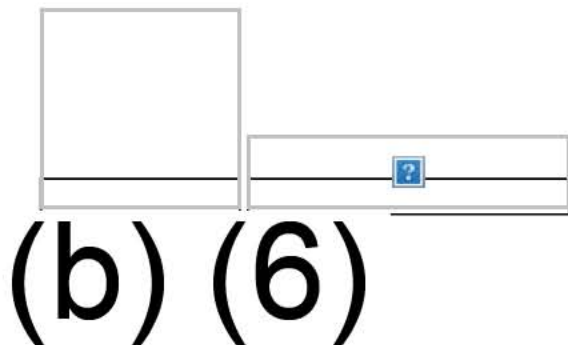
From: Marley, Patrick (b) (6)]
Sent: Friday, September 29, 2017 2:46 PM
To: (b) (6)
Cc: (b) (6)
Subject: Fw: News from the WEC: Update on Wisconsin Elections Cyber Security

(b) (6)

We're sending you these questions in light of the news release (attached and below) just released by the Wisconsin Elections Commission. A couple of my colleagues are CC'd on this email.

- The state says DHS now acknowledges it did not tell (until last week) any Wisconsin officials about specific attempts by the Russian government to hack Wisconsin's election system. Is it accurate that DHS does acknowledge this now? If so, why didn't DHS tell the state that?
- Can you now publicly release the eight IP addresses that you shared with the state of Wisconsin in October 2016 and why or why not? Didn't you later release these addresses as part of a larger group with the Grizzly Steppe report?

Patrick Marley | State Capitol reporter
.....



From: From the Wisconsin Elections Commission <elections@wi.gov>
Sent: Friday, September 29, 2017 12:03 PM
To: Marley, Patrick
Subject: News from the WEC: Update on Wisconsin Elections Cyber Security

cid:image004.png@01D3391A.EC06ADF0



FOR IMMEDIATE RELEASE:
September 29, 2017

FOR MORE INFORMATION, CONTACT:
Reid Magney, 608-267-7887

Update on Wisconsin Elections Cyber Security

MADISON, Wis. – Wisconsin Elections Commission Chair Mark Thomsen and Administrator Michael Haas issued the following statement.

In 2016, Russian government cyber actors unsuccessfully targeted Wisconsin's voter registration system. The U.S. Department of Homeland Security (DHS) helped Wisconsin's Division of Enterprise Technology (DET) successfully protect our systems from attack. However, DHS did not inform DET or the Wisconsin Elections Commission of the Russian government's involvement in those specific attempts until last Friday. Also, DHS incorrectly claimed that DET had been notified in October 2016 of the Russian government's involvement in this targeting.

Because DHS did not previously inform DET or WEC of its conclusions, we were surprised by the DHS notification last Friday, and the resulting confusion over the past week has been an unnecessary distraction from the fact that Wisconsin's systems are secure and have not been breached in any way. We have all learned many important lessons and DHS officials have

apologized and promised to improve their communications with state and local elections officials.

The past week has been dedicated to learning what actually happened and who knew what, and when. This has involved multiple meetings and phone calls with DHS, DET and other officials. We now understand that there were two separate events.

1. DHS has confirmed that Russian scanning activity on July 30 and 31, 2016 had actually occurred on an inactive IP address assigned to a Wisconsin Department of Workforce Development job center site. DET subsequently blocked access to Wisconsin systems from the suspicious IP address associated with the scanning activity.
2. In another event in August 2016, DET's firewalls blocked an advertisement embedded in a publicly available website from being displayed on a WEC computer. The ad could have led the user to a suspicious IP address, but DET's web content filtering system proactively blocked the ad, and the user had no opportunity to be directed to the suspect IP address. DET advised DHS of this suspect IP address, which DHS later determined is connected to Russian government cyber actors.

Since the initial notification Friday, WEC staff has had further discussions with high-level officials at DHS, we now understand that they consider Wisconsin to have been targeted based on a variety of sources, including intelligence information that cannot be publicly disclosed. We also understand that while Wisconsin's elections systems were not scanned directly, DHS believes the DWD scans were looking for vulnerabilities in order to gain information about how to target elections systems. This is based on activity DHS observed in other states where election agencies were not scanned directly.

Unfortunately, DHS did not initially provide the information supporting its conclusion that Russian government cyber actors targeted Wisconsin's voter registration system by attempting to scan another state agency. DHS communications led the Elections Commission to believe that it had not been targeted, which we announced at the Commission's meeting Tuesday. In further discussions, DHS officials have acknowledged that they did not inform DET officials that Wisconsin's elections systems had been targeted by Russian government cyber actors in 2016.

DET routinely blocks approximately 9 million scanning attempts each year. The basic fact remains that Wisconsin's cyber security defenses protected our elections systems from any intrusion, theft or damage. These scanning attempts were unremarkable, except for the fact that DHS later identified their source as being Russian government cyber actors.

We are confident that DHS and other federal agencies worked closely with DET and provided critical information which DET used to protect all of Wisconsin's systems. We will continue to work with DET and DHS to protect Wisconsin's elections into the future.

###

The Wisconsin Elections Commission is responsible for administration and enforcement of election laws in Wisconsin. The Commission is made up of six Commissioners – four appointed directly by the State Senate Majority Leader, Speaker of the Assembly and the Minority Leaders in the State Senate and Assembly. The remaining two Commissioners are by the Governor with confirmation by the State Senate from lists of former municipal and county clerks submitted by the legislative leadership in each party.

You are currently subscribed to newspaperdaily as **(b) (6)**

To unsubscribe click here: [http://lists.wi.gov/u?](http://lists.wi.gov/u?id=1861423.0467c77968063e68f6345ed4a3629eec&n=T&l=newspaperdaily&o=1291196)

[id=1861423.0467c77968063e68f6345ed4a3629eec&n=T&l=newspaperdaily&o=1291196](http://lists.wi.gov/u?id=1861423.0467c77968063e68f6345ed4a3629eec&n=T&l=newspaperdaily&o=1291196)

(It may be necessary to cut and paste the above URL if the line is broken)

or send a blank email to [leave-1291196-](mailto:leave-1291196-1861423.0467c77968063e68f6345ed4a3629eec@lists.wi.gov)

[1861423.0467c77968063e68f6345ed4a3629eec@lists.wi.gov](mailto:leave-1291196-1861423.0467c77968063e68f6345ed4a3629eec@lists.wi.gov)

Wisconsin Elections Commission

State of Wisconsin

212 E. Washington Ave., Third Floor ▪ Madison, WI 53703 ▪ elections@wi.gov ▪ (608) 266-8005 ▪ <http://elections.wi.gov>

FOR IMMEDIATE RELEASE:
September 29, 2017

FOR MORE INFORMATION, CONTACT:
Reid Magney, 608-267-7887

Update on Wisconsin Elections Cyber Security

MADISON, Wis. – Wisconsin Elections Commission Chair Mark Thomsen and Administrator Michael Haas issued the following statement.

In 2016, Russian government cyber actors unsuccessfully targeted Wisconsin's voter registration system. The U.S. Department of Homeland Security (DHS) helped Wisconsin's Division of Enterprise Technology (DET) successfully protect our systems from attack. However, DHS did not inform DET or the Wisconsin Elections Commission of the Russian government's involvement in those specific attempts until last Friday. Also, DHS incorrectly claimed that DET had been notified in October 2016 of the Russian government's involvement in this targeting.

Because DHS did not previously inform DET or WEC of its conclusions, we were surprised by the DHS notification last Friday, and the resulting confusion over the past week has been an unnecessary distraction from the fact that Wisconsin's systems are secure and have not been breached in any way. We have all learned many important lessons and DHS officials have apologized and promised to improve their communications with state and local elections officials.

The past week has been dedicated to learning what actually happened and who knew what, and when. This has involved multiple meetings and phone calls with DHS, DET and other officials. We now understand that there were two separate events.

1. DHS has confirmed that Russian scanning activity on July 30 and 31, 2016 had actually occurred on an inactive IP address assigned to a Wisconsin Department of Workforce Development job center site. DET subsequently blocked access to Wisconsin systems from the suspicious IP address associated with the scanning activity.
2. In another event in August 2016, DET's firewalls blocked an advertisement embedded in a publicly available website from being displayed on a WEC computer. The ad could have led the user to a suspicious IP address, but DET's web content filtering system proactively blocked the ad, and the user had no opportunity to be directed to the suspect IP address. DET advised DHS of this suspect IP address, which DHS later determined is connected to Russian government cyber actors.

Since the initial notification Friday, WEC staff has had further discussions with high-level officials at DHS, we now understand that they consider Wisconsin to have been targeted based

on a variety of sources, including intelligence information that cannot be publicly disclosed. We also understand that while Wisconsin's elections systems were not scanned directly, DHS believes the DWD scans were looking for vulnerabilities in order to gain information about how to target elections systems. This is based on activity DHS observed in other states where election agencies were not scanned directly.

Unfortunately, DHS did not initially provide the information supporting its conclusion that Russian government cyber actors targeted Wisconsin's voter registration system by attempting to scan another state agency. DHS communications led the Elections Commission to believe that it had not been targeted, which we announced at the Commission's meeting Tuesday. In further discussions, DHS officials have acknowledged that they did not inform DET officials that Wisconsin's elections systems had been targeted by Russian government cyber actors in 2016.

DET routinely blocks approximately 9 million scanning attempts each year. The basic fact remains that Wisconsin's cyber security defenses protected our elections systems from any intrusion, theft or damage. These scanning attempts were unremarkable, except for the fact that DHS later identified their source as being Russian government cyber actors.

We are confident that DHS and other federal agencies worked closely with DET and provided critical information which DET used to protect all of Wisconsin's systems. We will continue to work with DET and DHS to protect Wisconsin's elections into the future.

###

The Wisconsin Elections Commission is responsible for administration and enforcement of election laws in Wisconsin. The Commission is made up of six Commissioners – four appointed directly by the State Senate Majority Leader, Speaker of the Assembly and the Minority Leaders in the State Senate and Assembly. The remaining two Commissioners are by the Governor with confirmation by the State Senate from lists of former municipal and county clerks submitted by the legislative leadership in each party.

From: (b) (6), (b) (7)(C), (b) (7)(F)
To:
Cc: [NCC](#)
Subject: DHS/DNI Statement from Oct
Date: Tuesday, December 20, 2016 12:46:15 PM

(b) (6), (b) (7)(C), (b) (7)(F)

As discussed, [here is the October statement](#).

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.

V/R,
(b) (6), (b) (7)(C), (b) (7)(F)

NCCIC Policy

Department of Homeland Security
(b) (6), (b) (7)(C), (b) (7)(F)

From: [NCC](#)
To: (b) (6), (b) (7)(C), (b) (7)(F)
Cc:
Subject: FW: Emailing - 17-00000357-1484226677.pdf
Date: Thursday, January 12, 2017 8:24:00 AM
Attachments: [17-00000357-1484226677.pdf](#)

(b) (6), (b) (7)(C), (b) (7)(F)

Sharing for your situational awareness.

Best Regards,
(b) (6), (b) (7)(C), (b) (7)(F)

NCC Watch Operations

National Coordinating Center for Communications COMM-ISAC

National Cybersecurity & Communications Integration Center

Department of Homeland Security

Work: COMM/STE: (b) (7)(E), (b) (7)(F)

Fax: (b) (7)(E), (b) (7)(F)

Email: (Un (b) (7)(E), (b) (7)(F)

Email: (Sec

Email: (JW

From: (b) (6), (b) (7)(C), (b) (7)(F)]

Sent: Thursday, January 12, 2017 8:15 AM

To: NCC(b) (6), (b) (7)(C), (b) (7)(F)

Subject: Emailing - 17-00000357-1484226677.pdf

NCC Please pass this along to all leadership as this is directly related to Grizzly Steppe.

(b) (6), (b) (7)(C), (b) (7)(F)

APT28: At the Center of the Storm: Russia Strategically Evolves Its Cyber Operations

Operational (OP)

Cyber Espionage (CE)

Hacktivism (HK)

Enterprise (EN)

Critical Infrastructure (CI)

Cyber Crime (CC)

Vulnerability and Exploitation (VE)

January 10, 2017 03:14:00 PM, 17 00000357, Version: 1

Executive Summary

- The Democratic National Committee's (DNC) June 2016 announcement attributing its network breach to the Russian Government triggered an international debate over Russia's sponsorship of information operations against the U.S. At issue is the question of proof: did the Russian Government direct the group responsible for the breaches and related data leaks? If so, is this simply a matter of accepted state espionage, or did it cross a line? Was the DNC breach part of a concerted effort by the Russian Government to interfere with the U.S. presidential election? Unfortunately, many failed to ask the most consequential question: how will Russia continue to employ a variety of methods, including hacks and leaks, to undermine the institutions, policies, and actors that the Russian Government perceives as constricting and condemning its forceful pursuit of its state aims?
- Our visibility into the network operations of APT28, a group we believe the Russian Government sponsors, has given us insight into some of the government's targets, as well as its objectives and the activities designed to further them.
- To this end, FireEye iSIGHT Intelligence will be releasing this report on APT28 on Wednesday, Jan. 11, 2017, to the public. It is available now to our subscribers.

Threat Detail

Introduction

The Democratic National Committee's (DNC) June 2016 announcement attributing its network breach to the Russian Government triggered an international debate over Russia's sponsorship of information operations against the U.S. At issue is the question of proof: did the Russian Government direct the group responsible for the breaches and related data leaks? If so, is this simply a matter of accepted state espionage, or did it cross a line? Was the DNC breach part of a concerted effort by the Russian Government to interfere with the U.S. presidential election?

Unfortunately, we have failed to ask the most consequential question: how will Russia continue to employ a variety of methods, including hacks and leaks, to undermine the institutions, policies, and actors that the Russian Government perceives as constricting and condemning its forceful pursuit of its state aims?

Our visibility into the network operations of APT28, a group we believe the Russian Government

sponsors, has given us insight into some of the government's targets, as well as its objectives and the activities designed to further them. We have tracked and profiled this group through multiple investigations, endpoint and network detections, and continuous monitoring. Our visibility into APT28's operations, which date to at least 2007, has allowed us to understand the group's malware, operational changes, and motivations. This intelligence has been critical to protecting and informing our clients, exposing this threat, and strengthening our confidence in attributing APT28 to the Russian Government.

Overview

On Dec. 29, 2016, the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) released a Joint Analysis Report confirming FireEye's long held public assessment that the Russian Government sponsors APT28. Since at least 2007, APT28 has engaged in extensive operations in support of Russian strategic interests. A sophisticated and prolific set of developers and operators, the group has historically collected intelligence on defense and geopolitical issues. APT28 espionage activity has primarily targeted entities in the U.S., Europe, and the countries of the former Soviet Union, including governments and militaries, defense attaches, media entities, and dissidents and figures opposed to the current Russian Government.

Over the past two years, Russia appears to have increasingly leveraged APT28 to conduct information operations commensurate with broader strategic military doctrine. After compromising a victim organization, APT28 will steal internal data that is then leaked to further political narratives aligned with Russian interests. To date, these have included the conflict in Syria, NATO-Ukraine relations, the European Union refugee and migrant crisis, the 2016 Olympics and Paralympics Russian athlete doping scandal, public accusations regarding Russian state-sponsored hacking, and the 2016 U.S. presidential election.

This report details our observations of APT28's targeting, our investigation into a related breach, shifts in the group's tool development and use, and the tactics APT28 employs to compromise its victims.

APT28 Targeting and Intrusion Activity

In October 2014, FireEye released *APT28: A Window into Russia's Cyber Espionage Operations?* and characterized APT28's activity as aligning with the Russian Government's strategic intelligence requirements. While tracking APT28, we noted the group's interest in foreign governments and militaries, particularly those of European and Eastern European nations, as well as regional security organizations, such as the North Atlantic Treaty Organization (NATO) and the Organization for Security and Cooperation in Europe (OSCE), among others. Table 1 highlights some recent examples of this activity.

Entity	Timeframe	APT28 Targeting and Intrusion Activity
OSCE	November 2016	The OSCE confirmed that it had suffered an intrusion, which a Western intelligence service attributed to APT28.
Germany's Christian Democratic Union (CDU)	April - May 2016	Researchers at Trend Micro observed APT28 establish a fake CDU email server and launch phishing emails against CDU members in an attempt to obtain their email credentials and access their accounts.
Pussy Riot	August 2015	APT28 targets Russian rockers and dissidents Pussy

		Riot via spear-phishing emails
NATO Afghan Ministry of Foreign Affairs Pakistani Military	July 2015	FireEye detected APT28 using two domains (nato-news.com and bbc-news.org) to host an Adobe Flash zero-day exploit to target NATO, the Afghan Ministry of Foreign Affairs, and the Pakistani military.
German Bundestag & Political Parties	June 2015	Germany's Federal Office for Security in Information Technology (BSI) announced that APT28 was likely responsible for the spear-phishing emails sent to members of several German political parties. The head of Germany's domestic intelligence agency, Bundesamt für Verfassungsschutz (BfV), also attributed the June 2015 compromise of the Bundestag's networks to APT28.
Kyrgyzstan Ministry of Foreign Affairs	October 2014 through September 2015	FireEye iSIGHT Intelligence identified changes made to domain name server (DNS) records that suggest that APT28 intercepted email traffic from the Kyrgyzstan Ministry of Foreign Affairs after maliciously modifying DNS records of the ministry's authoritative DNS servers.
Polish Government & Power Exchange Websites	June and September 2014	APT28 employed "Sedkit" in conjunction with strategic web compromises to deliver "Sofacy" malware on Polish Government websites, and the websites of Polish energy company Power Exchange.

Table 1: APT28 targeting of political entities and intrusion activity

Since 2014, APT28 network activity has likely supported information operations designed to influence the domestic politics of foreign nations. Some of these operations have involved the disruption and defacement of websites, false flag operations using false hacktivist personas, and the theft of data that was later leaked publicly online. Table 2 highlights incidents in which victims suffered a compromise that FireEye iSIGHT Intelligence, other authorities, or the victims themselves later attributed to the group we track as APT28. All of these operations have aimed to achieve a similar objective: securing a political outcome beneficial to Russia.

Victim	Timeframe	APT28 Network Activity	Associated Information Operations Activity
World Anti-Doping Agency (WADA)	September 2016	On Sept. 13, WADA confirmed that APT28 had compromised its networks and accessed athlete medical data.	On Sept. 12, 2016, the ""Fancy 'Bears' Hack Team"" persona claimed to have compromised WADA and released athletes' medical records as "proof of American athletes taking doping."
U.S. Democratic National	April – September	The DNC announced it had suffered a network compromise and that a subsequent investigation found evidence of two breaches, attributed to APT28 and APT29. FireEye	In June 2016, shortly after the DNC's announcement, the Guccifer 2.0 persona claimed responsibility for the DNC breach and leaked documents taken

Committee (DNC)	2016	=analyzed the malware found on DNC networks and determined that it was consistent with our previous observations of APT28 tools.	from the 'organization's network. Guccifer 2.0 continued to leak batches of DNC documents through September.
John Podesta	March – November 2016	Investigators found that John Podesta, Hillary Clinton's presidential campaign chairman, was one of thousands of individuals targeted in a mass phishing scheme using shortened URLs that security researchers attributed to APT28.	Throughout October and into early November, WikiLeaks published 34 batches of email correspondence stolen from John Podesta's personal email account. Correspondence of other individuals targeted in the same phishing campaign, including former Secretary of State Colin Powell and Clinton campaign staffer William Rinehart, were published on the "DC Leaks" website.
U.S. Democratic Congressional Campaign Committee (DCCC)	March - October 2016	In July, the DCCC announced that it was investigating an ongoing "cybersecurity incident" that the FBI believed was linked to the compromise of the DNC. House Speaker Nancy Pelosi later confirmed that the DCCC had suffered a network compromise. Investigators indicated that the actors may have gained access to DCCC systems as early as March.	In August, the Guccifer 2.0 persona contacted reporters covering U.S. House of Representative races to announce newly leaked documents from the DCCC pertaining to Democratic candidates. From August to October, Guccifer 2.0 posted several additional installments of what appear to be internal DCCC documents on "his" WordPress site.
TV5Monde	February - April 2015	In February, FireEye identified CORESHELL traffic beaconing from TV5Monde's network, confirming that APT28 had compromised TV5Monde's network.	In April 2015, alleged pro-ISIS hacktivist group CyberCaliphate defaced TV5Monde's websites and social media profiles and forced the company's 11 broadcast channels offline. FireEye identified overlaps between the domain registration details of CyberCaliphate's website and APT28 infrastructure.
			During the May 2014

Ukrainian Central Election Commission (CEC)	May 2014	Ukrainian officials revealed that the investigation into the compromise of the CEC's internal network identified malware traced to APT28.	Ukrainian presidential election, purported pro-Russian hackers CyberBerkut conducted a series of malicious activities against the CEC, including a system compromise, data destruction, a data leak, a distributed denial-of-service (DDoS) attack, and an attempted defacement of the CEC website with fake election results.
---	----------	---	--

Table 2 - APT28 network activity has likely supported information operations

From Olympic Slight to Data Leak: Investigating APT28 at the World Anti-Doping Agency

As news of the DNC breach spread, APT28 was preparing for another set of operations: countering the condemnation that Russia was facing after doping allegations and a threatened blanket ban of the Russian team from the upcoming Rio Games. Russia, like many nations, has long viewed success in the Olympic Games as a source of national prestige and soft power on the world stage. The doping allegations and prospective ban from the Games further ostracized Russia, and likely provided motivation to actively counter the allegations by attempting to discredit anti-doping agencies and policies. Our investigation of APT28's compromise of WADA's network, and our observations of the surrounding events, reveal how Russia sought to counteract a damaging narrative and delegitimize the institutions leveling criticism.

Allegations of Russian Athletes' Widespread Doping

- July 16
 - A WADA-commissioned report documents evidence of Russian athletes' widespread doping.
- July 18
 - WADA designates the Russian Anti-Doping Agency as non-compliant and recommends banning the Russian team from the upcoming Olympics.
- Aug. 4
 - The International Olympic Committee (IOC) bans 118 Russian athletes from competing in the Games.

APT28 Compromises WADA

- Early August
 - APT28 sends spear-phishing emails to WADA employees.
- Aug. 10

- APT28 uses a legitimate user account belonging to Yuliya Stepanova to log into WADA's Anti-Doping Administration and Management System (ADAMS) database. Stepanova was a member of WADA's Independent Pound Commission, which exposed widespread doping in Russia athletes.
- Aug. 25 – Sept. 12
 - APT28 gains access to an IOC account created specifically for the 2016 Olympic Games and views and downloads athlete data.

False Hacktivist Personas Claim to Target WADA, Leak Athlete Data

- Aug. 9
 - The actor @anpoland, purporting to represent "Anonymous Poland," claims to have defaced the WADA website.
- Aug. 11
 - On Aug. 11 (and Sept. 5), @anpoland threatens to conduct a DDoS attack against and leak data from WADA, but fails to follow through on the threats.
- Sept. 12
 - "Fancy Bears' Hack Team", a previously unknown group purporting to be affiliated with Anonymous, claims via Twitter to have compromised WADA, and directs readers to a website hosting stolen documents.
 - In tweets to international journalists and Twitter accounts that disseminate hacktivist and information security news, "Fancy Bears' Hack Team" claims to have "proof of American athletes doping."
- Sept. 13
 - WADA releases a statement confirming the breach and attributes the compromise and theft of athlete medical data to APT28.
- Sept. 15 – 30
 - "Fancy Bears' Hack Team" releases five additional batches of medical files for high-profile athletes from multiple nations, including the U.S., which had applied for and received Therapeutic Use Exemptions (TUEs) for medications otherwise banned from competition.
 - Claiming to support "fair play and clean sport," Fancy Bears' Hack Team calls TUEs "licenses for doping."

Based on this timeline of leak and threatened leak activity, as well as strikingly similar characteristics and distribution methods shared between @anpoland and "Fancy Bears' Hack Team," the same operators are highly likely behind the two personas. WADA officials, citing evidence provided by law enforcement, stated that the threat activity originated in Russia, possibly in retaliation for WADA's exposure of Russia's expansive, state-run doping. The statement prompted denials from the Russian Government, with Russian sports minister Vitaly Mutko asking, "How can you prove that the hackers are Russian? You blame Russia for everything, it is very in fashion now."

Conclusion

Since releasing our 2014 report, we continue to assess that APT28 is sponsored by the Russian Government. We further assess that APT28 is the group responsible for the network compromises of WADA, the DNC, and other entities related to the 2016 U.S. presidential election cycle. These breaches

involved the theft of internal data, mostly emails, that was later strategically leaked through multiple forums and propagated in a calculated manner almost certainly intended to advance particular Russian Government aims. In a report released on Jan. 7, 2017, the U.S. Directorate of National Intelligence described this activity as an "influence campaign."

This influence campaign, a combination of network compromises and subsequent data leaks, aligns closely with the Russian military's publicly stated intentions and capabilities. Influence operations, also frequently called "information operations," have a long history of inclusion in Russian strategic doctrine, and have been intentionally developed, deployed, and modernized with the advent of the internet. The recent activity in the U.S. is but one of many instances of Russian Government influence operations conducted in support of strategic political objectives, and it will not be the last. As the 2017 elections in Europe approach, most notably in Germany, France, and the Netherlands, we are already seeing the makings of similarly concerted efforts.

Appendix

In our 2014 report, we identified APT28 as a suspected Russian Government-sponsored espionage actor. We came to this conclusion in part based on forensic details left in the malware that APT28 had employed since at least 2007. We have provided an updated version of those conclusions, a layout of the tactics that they generally employ, and observations of apparent tactical shifts. For full details, please reference our 2014 report, *APT28: A Window into Russia's Cyber Espionage Operations?*

APT28 Malware and Tactics

APT28 employs a suite of malware with features indicative of the group's plans for continued operations, as well as the group's access to resources and skilled developers.

Key characteristics of APT28's toolset include:

- A flexible, modular framework that has allowed APT28 to consistently evolve its toolset since at least 2007.
- Use of a formal coding environment in which to develop tools, allowing the group to create and deploy custom modules in its backdoors.
- Incorporation of counter-analysis capabilities, including runtime checks to identify an analysis environment, obfuscated strings unpacked at runtime, and the inclusion of unused machine instructions to slow analysis.
- Code compiled during the normal working day in the Moscow time zone and within a Russian-language build environment. More than 97 percent of APT28's malware samples were compiled during the working week, with 88 percent of samples compiled between 8 am and 6 pm in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg. In addition, APT28's developers consistently built malware in Russian-language settings until 2013.

APT28's Malware Suite

Tool	Role	AKA
CHOPSTICK	backdoor	Xagent, webhp, SPLM, (v2 fysbis)
EVILTOSS	backdoor	Sedreco, AZZY, Xagent, ADVSTORESHELL,

		NETUI
GAMEFISH	backdoor	Sednit, Seduploader, JHUHUGIT, Sofacy
SOURFACE	downloader	Older version of CORESHELL, Sofacy
OLDBAIT	credential harvester	Sasfis
CORESHELL	downloader	Newer version of SOURFACE, Sofacy

APT28's Operational Changes Since 2014

APT28 continues to evolve its toolkit and refine its tactics in what is almost certainly an effort to protect its operational effectiveness in the face of heightened public exposure and scrutiny. In addition to the continued evolution of the group's first-stage tools, we have also noted APT28:

- Leveraging zero-day vulnerabilities in Adobe Flash Player, Java, and Windows, including CVE-2015-1701, CVE-2015-2424, CVE-2015-2590, CVE-2015-3043, CVE-2015-5119, and CVE-2015-7645.
- Using a profiling script to deploy zero-days and other tools more selectively, decreasing the chances researchers and others will gain access to the group's tools.
- Increasing reliance on public code depositories, such as Carberp, PowerShell Empire, P.A.S. webshell, Metasploit modules, and others in a likely effort to accelerate their development cycle and provide plausible deniability.
- Obtaining credentials through fabricated Google App authorization and Oauth access requests that allow the group to bypass two-factor authentication (2FA) and other security measures.
- Moving laterally through a network relying only on legitimate tools that already exist within victims' systems, at times forgoing their traditional toolset for the duration of the compromise.

These changes are not only indicative of APT28's skills, resourcefulness, and desire to maintain operational effectiveness, but also highlight the longevity of the group's mission and its intent to continue its activities for the foreseeable future.

APT28 Tactics

We have observed APT28 rely on four key tactics when attempting to compromise intended targets. These include sending spear-phishing emails that either deliver exploit documents that deploy malware onto users' systems, or contain a malicious URL designed to harvest recipients' email credentials and provide access to their accounts. APT28 has also compromised and placed malware on legitimate websites intending to infect site visitors, and has gained access to organizations by compromising their web-facing servers.

Figures 1 through 4 below describe ATP28 tactics:



Figure 1: Infection with malware via spear phish



Figure 2: Webmail access via spear phish

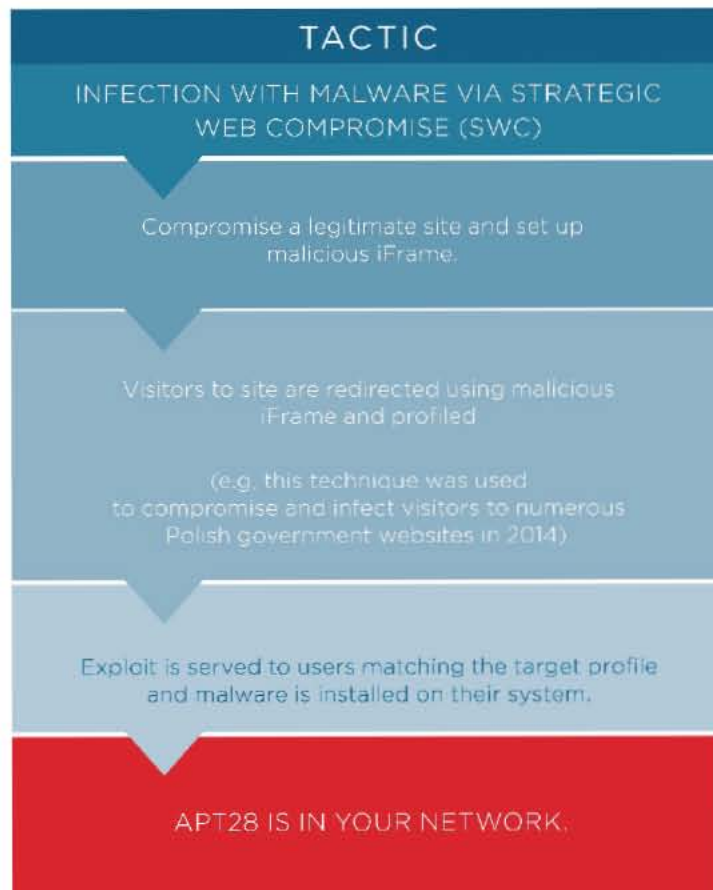


Figure 3: Infection with malware via strategic web compromise (SWC)

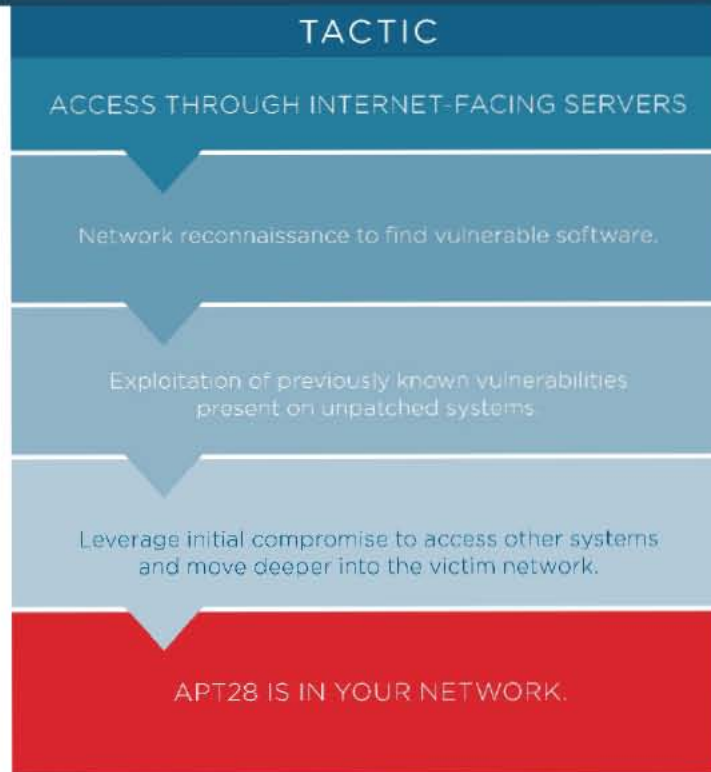


Figure 4: Access through internet-facing servers

First Version Publish Date

January 10, 2017 03:14:00 PM

Threat Intelligence Tags

Affected Industry

- Aerospace & Defense
- Financial Services
- Retail and Hospitality/Consumer Goods/Travel/Gaming/Food & Beverage
- Construction & Engineering
- Governments
- Civil Society → NGO/Nonprofit
- Civil Society
- Civil Society → International Governance (NATO/EU)
- Governments → Security/Military/Law Enforcement
- Governments → National Government
- Civil Society → Political Party/Political organization
- Civil Society → Religious Org
- Governments → US State and Local Governments and Agencies
- Education/Academia/Research Institutions
- Media/Entertainment/Publishing
- Governments → Regional Govt (Subnational govt outside of US)

Target Geography

- United States
- United Kingdom
- France

- Germany

Intended Effect

- Military Advantage
- Embarrassment/Exposure/Brand Damage
- Denial and Deception
- Political Advantage

Motivation

- Military/Security/Diplomatic

Source Geography

- Russian Federation

Targeted Information

- Customer Data
- Government Information
- Credentials

Actor

- Tsar Team

Version Information

Version:1.0, January 10, 2017 03:14:00 PM

APT28: At the Center of the Storm: Russia Strategically Evolves Its Cyber Operations



5950 Berkshire Lane, Suite 1600 Dallas, TX 75225

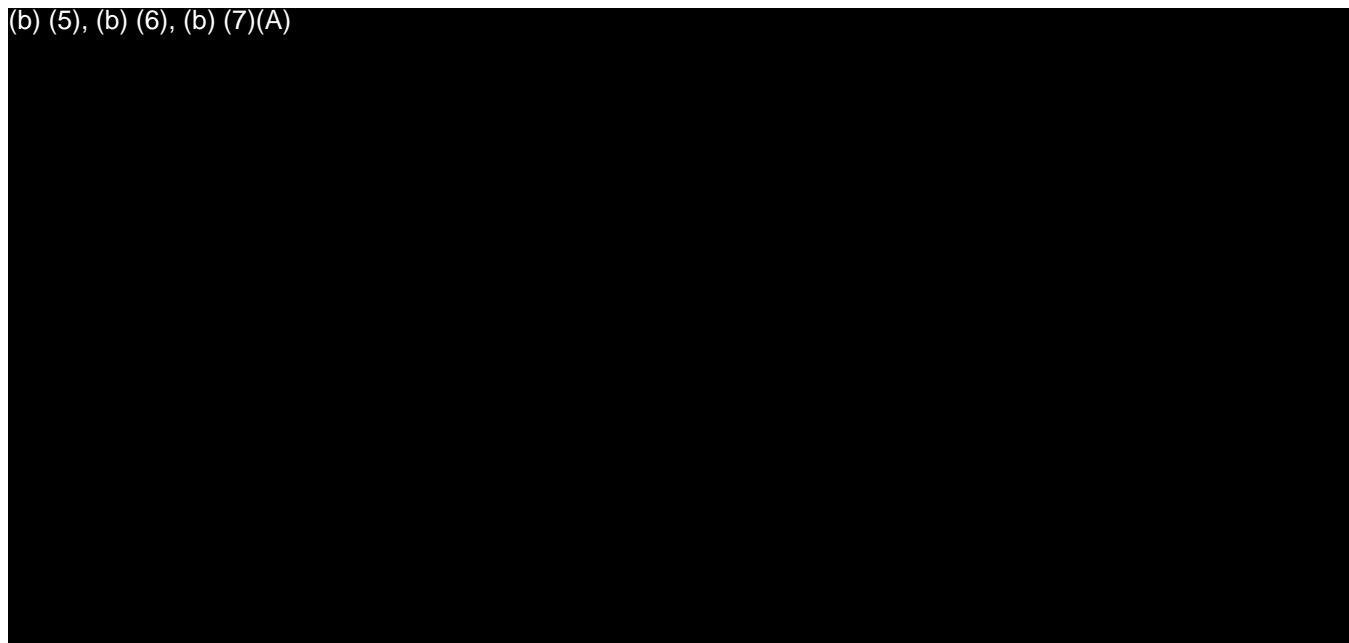
This message contains content and links to content which are the property of FireEye, Inc. and are protected by applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription [terms of service](#).

For more information on this or other FireEye products, please contact info@sightpartners.com.

For more information please visit: <https://mysight.sightpartners.com/report/fu/17-00000357>

© 2017, FireEye, Inc. All rights reserved.

(b) (5), (b) (6), (b) (7)(A)



https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.d6eb2ffc4ac6

Sabra

(b) (5), (b) (6), (b) (7)(E)



From: NCC

Sent: Thursday, December 29, 2016 8:31 PM

To: NCC(b) (7)(E), (b) (7)(F)

Subject: TLP: WHITE: NCCIC/US-CERT Joint Analysis Report (JAR)-16-20296: GRIZZLY STEPPE – Russian Malicious Cyber Activity **UPDATE**

NCCICC NCC Header



TLP:WHITE

TLP:WHITE

TLP:WHITE

Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

COMM-ISAC Government and Industry Reps,

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.

Attached is an updated version of Joint Analysis Report (JAR) 16-20296 TLP: WHITE, titled "Grizzly Steppe Russian Malicious Cyber Activity" with corresponding documents containing technical indicators. Three documents total are attached. The PDF contains an updated NCCIC phone number, and the CSV and STIX files were updated with additional indicators

Very respectfully,
NCC Watch

National Coordinating Center for Communications – COMM-ISAC
National Cybersecurity & Communications Integration Center
Department of Homeland Security
COMM/STE (b) (7)(E), (b) (7)(F)
Fax (b) (7)(E), (b) (7)(F)
Unclassified (b) (7)(E), (b) (7)(F)
Secret: (b) (7)(E), (b) (7)(F)
JWICS (b) (7)(E), (b) (7)(F)
(b) (6), (b) (7)(C), (b) (7)(F)

Distro: Monday Morning NCC Director's Meeting

TLP:WHITE

TLP:WHITE

TLP:WHITE

From: (b) (6), (b) (7)(C), (b) (7)(F) on behalf of [NCCIC](#)
To: [NCCIC](#); (b) (6), (b) (7)(C), (b) (7)(F)

Cc: [NCCIC - USCERT](#)
Subject: NCCIC (DHS) News Leadership Briefing Report - December 30, 2016
Date: Friday, December 30, 2016 5:12:21 AM
Attachments: [20161230 NCCIC \(DHS\) News Leadership Briefing Report.docx](#)

NCCIC (DHS) News Leadership Briefing Report December 30, 2016 | 0500 EST

Multiple Sources (12/30): Obama Announces Sanctions Against Russia For Election Interference. Yesterday's announcement of US sanctions against Russia in response to that country's alleged interference in the US election led all three major network newscasts, and generated extensive coverage across much of the media spectrum.

NCCIC released a Joint Analysis Report (JAR-16-20296) on December 29, 2016.

NBC Nightly News described the sanctions as a "strong strike back against Russia for its hack of American political figures,"

New York Times to "the strongest American response ever taken to a state-sponsored cyberattack aimed at the United States."

Wired similarly reported that "the administration...finally shot back," with a "collection of retaliatory tactics" that "represents arguably the strongest-ever response to state-sponsored hacking attacks in the history of the internet." For example, it "goes significantly farther than the steps taken against North Korea in the wake of that country's 2014 hack of Sony."

Bloomberg Politics quotes Obama as saying in a statement, "All Americans should be alarmed by Russia's actions."

The Wall Street Journal further quotes Obama as saying, "These data theft and disclosure activities could only have been directed by the highest levels of the Russian government."

The Hill reports "the FBI and the Department of Homeland Security...released a joint report detailing how federal investigators linked the Russian government to hacks of Democratic Party organizations." The "13-page report provides technical details regarding tools and infrastructure used by Russian civilian and military intelligence services to 'compromise and exploit networks and endpoints associated with the US election, as well as a range of US Government, political, and private sector entities.'" The Hill noted that the "'Joint Analysis Report' or JAR, refers to the Russian hacking campaign as 'Grizzly Steppe.'" "US intelligence services don't often release the details of their analysis, but today they did,"

CBS Evening News reported. Investigators believe two Russian hacking units, in 2015 and again in the spring of 2016, sent malicious emails to thousands of recipients, including multiple US government victims. The emails gave the Russian operatives "access to the information of senior Democratic party officials, which was then leaked to the press and publicly disclosed."

Bloomberg News reports "Grizzly Steppe" started with a "simple trick." Russian hackers "sent e-mails with hidden malware to more than 1,000 people working for the American government and political groups." The hackers initially sent e-mails that "appeared to come from legitimate websites and other Internet domains tied to U.S. organizations and educational institutions, according to the report." That "spearphishing" campaign "provided a foothold into the Democratic National Committee...and key e-mail accounts for material that would later be leaked to damage Hillary Clinton in her losing campaign against Trump." DHS and FBI's report said the cyberattacks were part of a "decade-long campaign" by Russian intelligence services. The agencies added, "The U.S. government seeks to arm network defenders with the tools they need to identify, detect and disrupt Russian malicious cyber activity that is targeting our country's and our allies' networks."

PC Magazine explains that the joint analysis report included "technical details about the tools and infrastructure that Russian hackers used to compromise the computer systems of multiple American government and private entities." The report stated that "public attribution of these activities to RIS is supported by technical indicators from the US Intelligence Community, DHS, FBI, the private sector, and other entities."

Reuters adds that the report “largely corroborates earlier findings from private cyber firms, such as CrowdStrike, which probed the hacks at the DNC and elsewhere, and is a preview of a more detailed assessment from the U.S. intelligence community that President Barack Obama ordered completed before he leaves office next month, a source familiar with the matter said.”

Ars Technica adds that the joint analysis report “includes information that will allow security firms and companies to identify and block malware used by Russian intelligence services, along with a breakdown of the Russian malware operators’ standard methods and tactics.” DHS “has added these ‘indicators of compromise’ to their Automated Indicator Sharing service.”

The AP reports the JAR is the “most detailed report yet on Russia’s efforts to interfere in the U.S. presidential election by hacking American political sites and email accounts.” The 13-page analysis was the “first such report ever to attribute malicious cyber activity to a particular country or actors.” The report is also the “first time the U.S. has officially and specifically tied intrusions into the Democratic National Committee to hackers with the Russian civilian and military intelligence services, the FSB and GRU, expanding on an Oct. 7 accusation by the Obama administration.”

USA Today, meanwhile, reports “Thursday’s sanctions are essentially additions of ones the Obama administration placed on Russia after it annexed the Crimea region of Ukraine.”

The Hill said that “to levy the sanctions, Obama broadened a 2015 executive order giving the president the authority to punish foreign actors who carry out cyberattacks against the US.” That order “allows the Treasury Department to freeze the assets of individuals or entities who used digital means to damage US critical infrastructure or engage in economic espionage.” Yesterday’s “changes expanded the order to allow Treasury to sanction individuals and entities ‘responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.’”

The Los Angeles Times says the penalties “included sanctions of two of Russia’s intelligence agencies and three companies the US said provided support.” Moreover, “35 Russian officials in the US were ordered to leave within three days and access was cut off starting Friday to two Russian government-owned compounds, one in New York and one in Maryland.”

Philip Bump for the Washington Post writes that the nearly three dozen Russian citizens who were ordered to leave the US were declared “persona non grata,” which is a “powerful” phrase in international diplomacy. Bump says the phrase, which means “unwelcome person,” is a “declaration that someone is effectively banned from a country.”

The Baltimore Sun reports that “the 45-acre site on the [Maryland] Eastern Shore waterfront near Centreville was purchased by the Soviet Union in 1972, a State Department official said. Its ownership was not a secret – it has been widely covered by news organizations for decades – and Russian officials have previously said the site has been used as a retreat for diplomats and their families.”

The Washington Post notes that “at the time of its purchase, there was some resistance to the sale of the building to the Soviets, with the local newspaper reporting there were ‘fears of nuclear submarines surfacing in the Chester River to pick up American secrets and defectors.’”

The Daily Beast reported “the compound in Long Island being shuttered is a mansion called Killenworth, in the community of Glen Cove.” The Daily Beast added that “during the early 1980s, the city council of Glen Cove banned Soviet officials from using public beaches and tennis courts and argued with the federal government over the loss of property taxes, owing to the compound’s ownership by a foreign government.”

The Huffington Post quoted a “senior Obama administration official” as saying yesterday that “if a future president decided he wanted to allow in a large tranche of Russian intelligence agents, presumably a future president could do that. ... We don’t think it would make much sense to reopen Russian intelligence compounds. ... We don’t think it makes much sense to invite back in Russian intelligence agents.”

CNBC reports President Obama said an upcoming report to Congress will show that “Russia’s efforts to interfere in our election, as well as malicious cyber activity related to our election cycle in previous elections.” CNBC cites the DHS and FBI joint analysis report that “said that the 2016 election activity was part of an ongoing campaign targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations.” Obama “also called on the global technology community to help identify Russian cyber actors, and released technical information about Russian civilian and military intelligence cyber activity.”

Politico speculates that the US “may stealthily strike back at Russia” with a cover cyber response. Politico says the “cyber responses could range from erasing Russian government databases, to leaking embarrassing documents on Kremlin officials, to releasing copies of Moscow’s elite hacking tools.”

However, cybersecurity experts “cautioned that the Obama administration is not likely to pursue cloak-and-dagger steps against Russia now” for fear of escalation.

In an editorial, the New York Times defends the “correctness” of Obama’s action, even if it came “definitely too late” and “may also be too little,” and also concludes that the sanctions “clearly create a problem for Mr. Trump,” who “in less than a month...will have to decide if he stands with his democratic allies on Capitol Hill or his authoritarian friend in the Kremlin.”

USA Today similarly editorializes that “any effort by Trump to undo the sanctions could also drive a wedge between him and Republican leaders on Capitol Hill.”

The New York Times says the sanctions were “intended to box in” President-elect Trump, who “will now have to decide whether to lift” them against the opinion of key Republicans and “reject the findings of his intelligence agencies.”

Last night, Kellyanne Conway referred to that passage of the Times story on Fox News’ Hannity, saying, “I was really disappointed to read in David Sanger’s New York Times piece...the allegation or the supposition that perhaps one reason that the sanctions are taking place is to, quote, ‘box in’ President-elect Trump. ... I hope that this isn’t motivated by politics even a little bit.”

The NYTimes is not alone in this line of reporting. After sitting in on a background briefing at the White House, Andrea Mitchell said on MSNBC that the Administration is “taking steps, they think, if I could read into or infer from...those on the call, they are taking steps that will box in Donald Trump. ... So they are taking steps that are reversible, but are clearly not going to be easily reversed at first blush.”

Bloomberg Politics also reports Obama “is forcing his successor...into a difficult choice: reverse the sanctions the departing president just imposed on Russia for hacking the US election or put at risk his campaign vow to improve relations with Vladimir Putin.”

NBC Nightly News likewise concluded that Trump “may have the power to reverse today’s sanctions,” but that would “prove difficult with Republicans and Democrats calling for tough steps against Russia,”

Roll Call similarly predicted “Trump’s opposition to...Obama’s retaliation against Russia...will immediately pit him against the hawkish wing of the Republican party,” and “soon could force him to veto additional penalties supported by his own party.”

Vice said the Obama moves “will undoubtedly force Trump to make tough decisions on a topic he has thus far shown little interest,”

And Salon that “although Trump could reverse the executive order...doing so...would increase suspicions among critics – including some within his own party – that he is too close to the Russian dictator and his regime.”

The Wall Street Journal also casts the sanctions as a challenge to Trump’s plans for a détente with Russia, and ponders whether the new Administration will seek to use Obama’s sanctions as leverage to obtain more from the Russians – such as more active collaboration in the fight against ISIL.

Jake Novak, in an op-ed posted on the CNBC website, said that “politically, this is winner for” Obama “on a lot of levels,” as it “solidifies” him “as a hero to Democrats and liberals who believe that Russia played a big role in helping...Trump,” and also “will endear him to quite a few Republicans and conservatives.” However, “this is where all the effectiveness ends,” because “diplomatically and economically, these new sanctions and expulsions won’t change a thing,” and “may serve to boost the myth of Russian king-making abilities worldwide.”

The New York Times also reports “veterans of the spy games offered mixed assessments of the administration’s actions.” Steven Hall, “a former senior C.I.A. official who ran Russia operations until his retirement in 2015,” called the sanctions “pretty weak” and “perhaps symbolic.”

Along those lines, The Hill reported, Conway said on CNN that the sanctions seem to be “largely symbolic.”

On CNN’s Situation Room Dr. Evelyn Farkas, the former Deputy Assistant Secretary of Defense for Russia/Ukraine/Eurasia, confirmed that she has seen the intelligence and said there is “no doubt” that Russia is behind the election interference. She added that with the intelligence community unanimous in their assessment, “I don’t understand why there are continued statements by the President-elect and others saying nobody knows.”

In an op-ed for Fox News, former Israeli military intelligence officer and co-founder of CyGov Brig. Gen. Eli Ben Muir argues that cyberwarfare is now the norm for conflicts between major countries. He opines that governments will have to use an “entirely different approach” if they want to “protect their vital interests.” He applauds Obama for ordering a review of cyber interference in elections going back to

2008, and it will hopefully “clarify what progress has been made since then and set out current capabilities.” Muir calls the assessment a “critical starting point,” but adds that governments must develop a “comprehensive plan which addresses the trends of tomorrow, rather than fire-fighting today’s immediate threats.” He urges governments to “invest [in] the right resources and apply the right technological solutions to provide long-term security, integrating them effectively into the everyday workings of government and key institutions.”

In an op-ed for CNBC, CEO and founder of cybersecurity firm empow Avi Chesla argues the cyberattacks by Russia on the US election are “devastating” because they likely signal the “new normal” between “prominent political players.” Chesla opines that to “better prepare for the possibility of cyber-assaults on our voting outcomes, we need to understand what sort of tactics were used in past attacks and what kind of new malicious strategies might we see in future.” Chesla adds that strategies must be developed to counter the tactics.

Sanctions Also A Response To “Harassment” Of US Diplomats In Moscow.

Bloomberg Politics quotes Obama as also saying in his Thursday statement, “Moreover, our diplomats have experienced an unacceptable level of harassment in Moscow by Russian security services and police over the last year. Such activities have consequences.”

In fact, Reuters reports, Obama’s moves were meant “to punish Russia for a campaign of intimidation of American diplomats in Moscow,” as well as its “interference in the US election.” A “senior US official” told reporters yesterday, “These actions were taken to respond to Russian harassment of American diplomats and actions by the diplomats that we have assessed to be not consistent with diplomatic practice.” Reuters adds “the State Department has long complained that Russian security agents and traffic police have harassed US diplomats in Moscow, and US Secretary of State John Kerry has raised the issue with Russian President Vladimir Putin and his foreign minister, Sergei Lavrov.”

Mother Jones reported “senior administration officials cited the assault of a US diplomat by a Russian police officer that was broadcast on Russian television in July.” The “officials also said the safety of US diplomats was compromised when some diplomats’ personal information was broadcast on Russian television.” Mother Jones cautioned, however, that “Russia has accused Washington of similar harassment toward its diplomats.”

The Huffington Post, meanwhile, quoted an “official” as describing “Russian government actions against US diplomats posted in Russia as part of the country’s ‘flagrant violation of diplomatic norms.’”

Slate quoted State Department spokesman Mark Toner as saying, “The harassment has involved arbitrary police stops, physical assault, and the broadcast on State TV of personal details about our personnel that put them at risk.”

Russia To Retaliate, Says Obama Trying To Hurt Trump.

ABC World News Tonight reported Russia is “blasting these measures as aggressive and unpredictable” and is “promising that countermeasures will be announced tomorrow.”

According to Fox News’ Special Report, Russia’s embassy in London tweeted that everybody, including the American people, “will be glad to see the last of this hapless” Administration.

The Washington Post reports Kremlin spokesman Dmitry Peskov said in response to the US moves, “I cannot say now what the response will be, although, as we know, there is no alternative here to the principle of reciprocity. ... The response will be formulated in a direction determined by the president of the Russia.”

McClatchy reports Peskov also “told reporters that the sanctions were designed to undermine Trump.” Said Peskov, “We think that such steps by a US administration that has three weeks left to work are aimed at two things: to further harm Russian-American ties, which are at a low point as it is, as well as, obviously, to deal a blow to the foreign policy plans of the incoming administration of the president-elect.”

Two hours after Peskov’s statement, Politico reports, “Russian authorities...announced the closure of the Anglo-American School of Moscow, hours after the Kremlin vowed to retaliate against recent US sanctions.” Politico adds that “the non-profit day school, which enrolls international students from pre-kindergarten through 12th grade, will be closed along with the US embassy vacation dacha in Serebryany Bor in the outskirts of Moscow.”

The Washington Post separately reports that Putin’s Internet adviser German Klimentko said Russia may disconnect itself from the global Internet to avoid retaliatory cyberattacks from the US. The Post says Klimentko’s comments “come as the United States is said to be mulling covert cyber-operations against Russia in retaliation for Moscow’s interference in the 2016 presidential election.”

Voice of America reported that a statement issued by Russian Foreign Ministry spokeswoman Maria

Zakharova complained that “we are already tired of the lies about ‘Russian hackers’ which continue to emanate from the very top of the US [government]. ... The Obama administration has launched this disinformation [campaign] half a year ago in an attempt to give a boost to its preferred candidate in the November presidential elections, and not having achieved the result it was seeking, it is looking for an excuse for its own failure, thus dealing a double blow to Russian-American relations.”

The New York Times reports that “much about Russia’s cyberwarfare program is shrouded in secrecy,” but “details of the government’s effort to recruit programmers in recent years...are shedding some light on the Kremlin’s plan to create elite teams of computer hackers.” The Times adds that “for more than three years, rather than rely on military officers working out of isolated bunkers, Russian government recruiters have scouted a wide range of programmers, placing prominent ads on social media sites, offering jobs to college students and professional coders, and even speaking openly about looking in Russia’s criminal underworld for potential talent.”

Trump Urges Country To “Move On,” But Will Discuss Investigation With Intel Officials.

The CBS Evening News reported, “As for...Trump, he released a statement today saying, ‘It’s time for our country to move on to bigger and better things.’ But he added that he will meet with leaders of the intelligence community next week to be updated on the facts of this situation.”

ABC World News Tonight said the statement echoed “what he said Wednesday.” Trump was shown saying, “I think we ought to get on with our lives. The whole, you know, age of computer has made it where nobody knows exactly what’s going on.”

Asked on Fox News’ The O’Reilly Factor about Trump’s stance on the sanctions, incoming White House chief of staff Reince Priebus said, “The President-elect put out a statement and he said, look, it’s time to move on to bigger and better things, but also, nevertheless, we’re going to be meeting and he is going to be meeting with intelligence officials next week to talk about this report and find out the details of exactly what happened, how the investigation took place. And maybe at that time or maybe later he’ll have a response. But right now we’re just not in a position to sit here and respond to all of these details before we have a full blown intelligence report on this particular matter.” Priebus added that “we just need to get to a point ourselves where we can talk to all of these intelligence agencies and find out once and for all what evidence is there, how bad is it?”

ABC World News Tonight said Trump has “repeatedly refused to accept the conclusion” of the intelligence community, and is “under scrutiny” for nominating Exxon CEO Rex Tillerson, who has “close ties to...Putin,” as his secretary of state.

The New York Times reports Trump was also “asked on Wednesday about statements by [Sen. Lindsey] Graham...that Mr. Putin should be personally sanctioned for the hacking.” Trump said “he was unaware of the comments by Mr. Graham, who was a Republican candidate for president before dropping out in December 2015.” Said Trump, “I don’t know what he’s doing. ...As you know, he ran against me.”

US News & World Report, meanwhile, indicated that “back in July, Trump invited Russia to launch cyber-attacks that would ‘be able to find the 30,000 emails that are missing,’ a reference to Democratic rival Hillary Clinton’s email server scandal.”

CNN’s Situation Room reported Sen. John McCain responded to Trump’s remarks “with a sarcastic jab.” He was shown saying, “I agree with the President-elect. We need to get on with our lives without having Russians and their outside influence, especially Vladimir Putin, who is a thug and murderer.”

Also on CNN’s Situation Room, Rep. Adam Smith said he thinks Trump’s reaction was “totally inappropriate” and praised McCain and Graham “for recognizing the seriousness of this, and pledging congressional action.”

In an editorial, the Wall Street Journal is critical of Trump’s call on Americans to “get on with our lives” on Wednesday night, but celebrates last night’s announcement that he would seek an update from US investigators. A failure to take Putin’s aggression seriously, warns the Journal, risks making Trump as ineffectual as Obama was.

Bloomberg Politics reports that “commenting before the Obama administration’s announcement, Trump transition spokesman Sean Spicer said Thursday if the government has any proof of foreign interference in the election, it should make that evidence known.” Said Spicer, “Right now we need to see further facts based on what we do know and what’s in the public domain.”

CNN noted that Spicer also said Thursday, “At some point, the question hasn’t even been asked of the (Democratic National Committee): Did you take basic measures to protect the data that was on there? ... Where’s the responsibility of them to protect their systems?”

Bolton: If Russia Interfered With Election, “Much Stronger Response” Needed.

Former Ambassador John Bolton said on Fox News' Hannity, "I think what...Obama announced today is incoherent and, if the reports about what Russia did are in fact correct, utterly inadequate. I think we need a much stronger response because we want to get into a position where Russia and everybody else who has been doing this kind of interference in the United States knows that we can cause a lot more pain to them than they can cause to us and we create structures of deterrence to make them stop it."

McCain And Graham Say Sanctions Not Tough Enough, Ryan Says They Illustrate Obama Failure.

Roll Call reported that Sens. John McCain and Lindsey Graham said in a statement yesterday, "The retaliatory measures announced by the Obama Administration today are long overdue. ... But ultimately, they are a small price for Russia to pay for its brazen attack on American democracy."

Reuters, meanwhile, reports House Speaker Ryan said "Russia 'has consistently sought to undermine' US interests and sanctions imposed by the Obama administration on Russia were overdue." Ryan went on to deride the sanctions as "an appropriate way to end eight years of failed policy with Russia," which "serves as a prime example of this administration's ineffective foreign policy that has left America weaker in the eyes of the world."

The Washington Post says "many" other Republicans, like Ryan, "lined their praise for the sanctions with criticism of the Obama-era foreign policy." Rep. Devin Nunes, chairman of the House Intelligence Committee, "said in a statement that he had urged action 'for years,'" adding that "this kind of indecision and delay helps to explain why now, at the end of Obama's eight-year presidency, America's influence has collapsed among both our allies and our enemies." The Post adds that "some back-bench Republicans refrained from criticizing Russia at all." Rep. Trent Franks, for example, "said on MSNBC that it was important to note that no one accused Russia of hacking the election itself,"

Rep. Ted Yoho told CNN's Situation Room "that he was 'not thoroughly convinced' that Russia had been behind the hack."

USA Today notes that Franks told MSNBC, "I'm all for doing what's necessary to protect the electorate but there's no suggestion that Russia hacked into our voting systems or anything like that. ... But the bottom line is if they succeeded, if Russia succeeded in giving the American people information that was accurate, then they merely did what the media should have done."

Brazile: Obama Actions "Insufficient."

The Hill reported that DNC interim chairwoman Donna Brazile on Thursday "called the Obama administration's retaliatory measures for hacking Democratic groups 'insufficient.'" Said Brazile, "Today's action alone by the White House is insufficient. Now it's time for...Trump and the Republican leadership in Congress to put our national security before politics and show the American people that they are serious about protecting our democracy."

US Lacked "Sufficient Evidence" To Indict Russian Officials.

The Washington Post reports "US officials...considered criminal indictments of Russian officials, but the FBI appears to have been unable so far to compile sufficient evidence to take that step."

Bloomberg Politics notes DOJ "has used indictments in the past to target foreign officials it believes participated in cyberattacks." For example, "in 2014, a grand jury indicted five Chinese military hackers the Obama administration alleges stole trade secrets and internal communications from an American business." Seven Iranians were also "indicted earlier this year for a series of cyberattacks against the US financial system and a US dam in New York state three years ago."

Politico: US Political System Will Remain Vulnerable Unless Major Changes Are Made.

In a 2,600-word analysis, Politico reports the US political system "will remain vulnerable to cyberattacks and infiltration from foreign and domestic enemies unless the government plugs major holes and commits millions of dollars in the coming years." Politico says there are "major political, financial and logistical obstacles stand in the way of ensuring that hackers are locked out of future elections, not to mention an incoming administration that is dismissive about the government's own allegations that Russia pulled off a widespread hacking campaign that fueled Americans' wariness of the political process and possibly helped President-elect Donald Trump win the White House." Congress has "shown little enthusiasm for offering financial aid to state and local election offices, for example, or for putting an agency like the Secret Service in charge of ensuring that campaigns or parties follow accepted cybersecurity practices."

Leaked Snowden Document May Shed Light On Russian Hacking Techniques.

The Huffington Post reports a classified document leaked by former NSA contractor Edward Snowden reveals that US intelligence officials have "tracked Russian hacking before and that the information they

gleaned may have helped this time around.” Russian hacking “also occurred in the case of Russian journalist and American citizen Anna Politkovskaya, who was gunned down in 2006 in her Moscow apartment after writing articles critical of the Kremlin and Russian President Vladimir Putin.” Her email was “hacked by Russian intelligence using malicious software not publicly available, according to an NSA document leaked by Snowden to The Intercept.” The Post says, “Not only does the document reveal that U.S. intelligence knew about the hacking of Politkovskaya’s email, it also shows that the NSA is adept at tracking cyberattacks by Russian intelligence.”

Mutiple Sources (12/29): FDA’S New Guidelines For Medical Devices Not Legally Enforceable. The FDA report “Postmarket Management of Cybersecurity in Medical Devices” was issued on December 28, 2016. The report cites ICS-CERT for resource and advisories concerning cybersecurity vulnerabilities or exploits on medical devices.

On its website, CNBC publishes an article by The Verge which says that recently, the FDA unveiled “its recommendations for how medical device manufacturers should maintain the security of internet-connected devices, even after they’ve entered hospitals, patient homes, or patient bodies.” Suzanne Schwartz, the FDA’s associate director for science and strategic partnerships, pointed out that “hospital networks experience constant attempts of intrusion and attack, which can pose a threat to patient safety. ... And as hackers become more sophisticated, these cybersecurity risks will evolve.” The piece says the new guidelines urge “manufacturers to monitor their medical devices and associated software for bugs, and patch any problems that occur,” yet they “are not legally enforceable – so they’re largely without teeth.”

The New York Post reports that the FDA, in its guidelines, did not “shy away from painting a horror scenario, one in which a researcher notifies a manufacturer that its implantable device ‘can be reprogrammed by an unauthorized user.’” Exploiting such a device “could result in permanent impairment, a life-threatening injury, or death,” according to the FDA.

Opinion: Cybersecurity Practices In Healthcare Industry Must Be Balanced. In an op-ed for Forbes, GreyCastle Security CEO Reg Harnish argues that “implementing industry-standard cybersecurity practices can inhibit clinicians’ work, also leading to life-and-death consequences.” He recommends cybersecurity professionals “should spend quality time with their healthcare clients, conducting in-depth interviews and visiting their workplaces, to develop cybersecurity measures that balance clinicians’ vital workflow operations with security and patient privacy.”

Reuters (12/29): Poroshenko Denounces Russian Cyber-War Against Ukraine. NCCIC has no comment.

Reuters reports Ukrainian President Petro Poroshenko said yesterday that “hackers have targeted Ukrainian state institutions about 6,500 times in the past two months, including incidents that showed Russian security services were waging a cyberwar against the country.” As a result, said Poroshenko, “acts of terrorism and sabotage on critical infrastructure facilities remain possible today.” He added that “the investigation of a number of incidents indicated the complicity directly or indirectly of Russian security services waging a cyberwar against our country.”

Team 3

NCCIC Duty Officer

National Cybersecurity and Communications

Integration Center (NCCIC)

U.S. Department of Homeland Security

STE: (b) (7)(E), (b) (7)(F)

NSTS: (b) (7)(E), (b) (7)(F)

Unclass ema (b) (7)(E), (b) (7)(F)

Unclass ema

SIPR/HSDN:

JWICS/C-LA

-

(b) (5), (b) (6), (b) (7)(A)

From: (b) (6)
Sent: Tuesday, June 13, 2017 7:26:02 AM
To: Taylor, Cindy; (b) (6)
Cc: (b) (6)
Subject: Hacking

(b) (5), (b) (6), (b) (7)(A)

SPEAKING OF THOSE CLOSE TIES -- "Russian Breach of 39 States Threatens Future U.S. Elections," by Bloomberg's Michael Riley and Jordan Robertson: "Russian hackers hit election systems in at least 39 states before Donald Trump's election as president, according to a person with direct knowledge of the matter, an attack on almost twice as many states as previously reported. The hacks were part of a wave of intrusions in the summer and fall of 2016, details of which were provided by the person and two others familiar with a U.S. investigation of the attacks. Hackers breached a campaign finance database in at least one unidentified state, they said, and tried to alter or delete data from a voter database in Illinois.

"The scope and sophistication of the attacks so concerned the White House that Obama administration officials for the first time used a dedicated communication channel -- the cyber equivalent of the nuclear 'red phone' -- to signal to the Kremlin that the attacks risked escalating into a broader conflict, according to two of the people. The U.S. also provided detailed documents it considered proof of an act of aggression, which they said met with a chilly Russian response." <https://bloom.bg/2rVU2p9><<http://go.politicoemail.com/?qs=601b6007b2d321c157baca169137c38a63e36c553ec66cdc707c13ef0cc63a2c6900991fdd5c117d7de93ebf75425635>>

(b) (6), (b) (5), (b) (7)(A)

(b) (6)
Deputy Assistant Secretary for Media Operations/Press Secretary Department of Homeland Security
(b) (6)

The subsequent 56 pages, (NPPD 001830 through NPPD 001885) are being withheld in their entirety pursuant to 5 U.S.C. § 552 (b)(5), (b)(6), (b)(7)(A), (b)(7)(C) and (b)(7)(E).

NPPD 001830 – NPPD 001885