TLP: AMBER

WARNING: Information in this report is FOUO//TLP: AMBER. Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information. Recipients may only share this information within their own government organization, and only as necessary to act on that information, consistent with both the DHS policy relating to FOUO information and with the Traffic Light Protocol, http://www.us-cert.gov/tlp.

ACTIONS

A TTX is scheduled for the afternoon of November 1, to test federal communications and coordination processes and resolve any technical or coordination challenges ahead of Election Day.

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

[redacted]

INCIDENT SUMMARY

(b) (7)(E), (b) (5)	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

STATE VULNERABILITY SCANNING & ASSESSMENTS

(b) (5), (b) (7)(E)	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

MEETING

Daily Election Infrastructure Call (b) (6), EPMO)
Meeting designed to sync election outreach efforts across NPPD.
Monday | Wednesday | Friday, 0830-0900, Teleconference (FO, I&A, OLA, OGC, IGA, PLCY, S&T, NCATS, SECIR, IP, OCIA, OPA)

Daily Election Sync ((b) (6), NCCIC)
General sync call between NCCIC, FBI and CTIIC for information sharing purposes.
Daily, 1030-1100, Teleconference (FBI MM, CYWATCH, CTIIC, MS-ISAC)

UCG Seniors Call
Monday | Wednesday | Friday, 1200, Teleconference (DHS, FBI, CTIIC)

Election Related State Incidents

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

[redacted]	[redacted]
[redacted]	
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

(b) (5), (b) (7)(E) [redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

(b) (5), (b) (7)(E) [redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
-	CLASSIFIED						

(b) (5), (b) (7)(E) [redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
-			CLASSIFIED				
[redacted]	[redacted]	(b) (5), (b) (7)(E) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

(b) (5), (b) (7)(E) [redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

(b) (5), (b) (7)(E) [redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

(b) (5), (b) (7)(E)	
[redacted]	[redacted]
[redacted]	[redacted]

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Distributed as TLP: AMBER

Preliminary Digital Media Analysis Report (PDMAR) – INC10085551

2016-09-02

Incident Summary

Description: USG 112 requested that US-CERT provide digital media analysis of 1 hard drive image and 4 Virtual Box images.

This Preliminary Digital Media Analysis Report (PDMAR) is intended to establish the scope of examination and provide a rapid turnaround on immediately identifiable and actionable items. A detailed analysis with additional insight into the specific tactics, techniques, and procedures (TTPs) observed on the submitted media will be provided in the form of a Digital Media Analysis Report (DMAR) upon completion of the examination.

The Department of Homeland Security provides this analysis of submitter's data or media with the conditions set forth below under 'Notification'.

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. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this report, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the report.

The DHS does not endorse any commercial product or service, including the subject of the analysis in this report. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities, including the US-CERT name or logo, on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including US-CERT. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, US-CERT, or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

This document is distributed as TLP: AMBER. Recipients may share TLP: AMBER information only as widely as necessary to act on the information. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Executive Summary

On August 29, 2016 USG112 requested that US-CERT conduct digital media analysis of 1 hard drive image and 4 Virtual Box files of Citrix servers. The hard drive image is a desktop system that was previously infected with a keylogger. The keylogger was contained within 24 hours by Antivirus scans however; it is unknown if usernames and passwords were compromised during that timeframe. The daily users of the system have administrative privileges to make changes to the backend database which holds voter PII information. The Citrix client logs show user logins during off-duty hours. Preliminary analysis revealed the presence of 2 suspected malicious binaries. These files have been extracted for further analysis.

Analysis

(b) (5), (b) (7)(E) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

(b) (5), (b) (7)(E) [redacted]

(b) (5), (b) (7)(E) [redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

Initial triage of the file produced hits from several Antivirus vendors indicating that it was malicious.

Conclusion

The image submitted for analysis show signs of infection.

(b) (5), (b) (7)(E) [redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]
[redacted]

Further information on the malicious files will be provided in the form of a US-CERT Malware Initial Findings Report (MIFR) or Malware Analysis Report (MAR).

Further insight into the activity of the malicious files on the system will be provided in a final US-CERT Digital Media Analysis Report (DMAR).

Mitigation Recommendations

US-CERT recommends the following:

- Monitoring for the abovementioned files, domains, and IP addresses as detection may be an indicator of additional malicious activity.
- Refraining from accessing, contacting, or probing the abovementioned domains and IP addresses as doing so could result in additional compromise or infection.
- Addressing the machines and accounts which may have been compromised.

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 thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate Access Control Lists (ACLs).

Please contact US-CERT at 1-888-282-0870 or soc@us-cert.gov if you have questions regarding this report.

FAQ

What is a PDMAR? A Preliminary Digital Media Analysis Report (PDMAR) is the US-CERT Digital Media Analysis (DMA) report intended to establish the scope for the DMA examination and provide a rapid turnaround on immediately identifiable and actionable items.

What is a DMAR? A Digital Media Analysis Report (DMAR) is the US-CERT DMA report that provides detailed examination findings with additional insight into the specific tactics, techniques, and procedures (TTPs) observed on the submitted media. The report is generated upon completion of the DMA examination.

I see that this document is labeled as TLP: AMBER. Can I distribute this to other people? Recipients should only share TLP: AMBER as widely as necessary to act on that information. Please contact US-CERT with specific distribution inquiries.

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, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov. Submit malware samples to virus-submit@us-cert.gov or via malware.us-cert.gov.

(Master Ticket # INC10082172)| US Business 55 Breach | Cyber Guardian Ticket: 320137 | Level 3 High (Orange)
Related tickets: INC10075440/10075502

| | - Correspondence with political organization

31 August:

1640: (b) (6) sent email identifying (b) (6) as a potential POC. (b) will get a POC for the NRSC this evening and someone from the Trump Campaign tomorrow.

1529: Received email from (b) (6) regarding correspondence from NC requesting to take advantage of (b) (6) offer.

1525: RWT learned DNC/DCCC MIFR was sent yesterday.

1503: Received email between (b) (6) and (b) (6) regarding connecting with Board of Elections groups. Want to know what we can share and what services we can offer.

1353: Received summary email from (b) (6) regarding the call between NCATS and the state of PA. (b) (5), (b) (7)(E)

1242: Through email (b) was introduced to (b) (6) and (b) (6) from FireEye iSIGHT intelligence, and would like to set up a classified meeting next week to cover threats to the election.

1123: Received email from (b) (6) to (b) (6) and (b) (6) informing them about the CISCP program and introducing him to the program manager if he or his clients would be interested.

1123: Email from (b) (6) regarding (b) (5), (b) (7)(E). (b) (5), (b) (7)(E)

1119: Received email from (b) (6) to (b) (6) informing him about the CISCP program and introducing him to the program manager if he or his clients would be interested.

1015: (b) (6) replied that he should have NRCC and NRSC contacts today and is searching for a Trump contact.

1001: (b) (6) email (b) (6) and (b) (6) informing them that we need contacts for NRCC, NRSC and Trump Campaign so any assistance he can provide would be greatly appreciated.

0953: (b) (6) replied to (b)'s email telling him we may need to take him up on his offer of the NRCC contact.

0952: (b) (6) forwarded an email from (b) (6) to (b) (6) with regards to missing (b)'s call last week and informing us he has a contact with the NRCC if we're interested.

0800: email from (b) (6) updating us on (b) (5), (b) (7), (b) (5), (b) (7)(E)

0659: Received email from (b) (5), (b) (6), (b) (7)(E) . Asked MS-ISAC if this has shown up anywhere else.

30 August:

1827: NCCIC NDO received an email from CyWatch with a general overview of what they know and don't know regarding the reported Ohio breach.

1555: Sent Mission Manager Election Updates to Executive distro.

1415: Received update from (b) (6) regarding the state outreach campaign, two states have shown interest; Nebraska and Pennsylvania

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

1259: TLP: AMBER MIFR from the DNC/DCCC analysis from (b) (6) was sent to Ozment and (b) (6)- will go out to the normal distribution soon.

1122: Received email from (b) (6) regarding (b) (5), (b) (7)(E) . Call will take place on August 31st.

1008: Email from (b) (6) to (b) (6)
Thanks for letting me know, and I will make sure that both you and (b) have the opportunity to connect when you return back. Thursday, September 8 or Friday, September 9 both work well for (b) . Please let me know what works best for your teams schedule and (b) will be happy to come down to your office.

(b) sent email to (b) (6) asking her to check (b) (6) and (b) (6)'s calendars and set aside an hour on one of these two dates.

29 August:

1553: (b) (6) replied to (b) (6) earlier email from 1418, he supplied DHS' response to the NASS cal.
I do not have complete information but I am aware of 5 states that have reached out to us to learn more of our services. I do not know whether any have taken us up on them. I think that this is partly a function of our main outreach to States on this issue has been through the S1 call. We are following up this week with NASS on answers to some of their follow up questions (draft attached). That may trigger further inquiry.

1540: Email reply from (b) (6) to (b) (6) regarding the email at 1523:
I think that it's more important to have my smart guys lay out for (b) what we have, what we can do to support etc. I do not want to delay that just for my schedule…

1523: Email exchanged from (b) (6) to (b) (6):
It is completely your preference regarding the meeting. (b) will be in DC the following week (September 12) if you want to hold the meeting until then when you return.

Please let me know.

1513: (b) (6) replied to (b) (6)'s Election Update email requesting:
A/S (b) (6) really liked this update. He has asked for updates to be sent directly to him from now on. (I did re-format to a Word document to clean it up a bit…)

Please also cc: (b) (6) and (b) (6) .

Email was forwarded to; (b) (6) and (b)

1418: (b) (6) emailed:

Do we know if any other states have taken up the election assistance offer from NCCIC
I have a NPPD PAO reacting to a report from GovExec wanting to know how many states are taking up the offer. Last week told her that had states involved. Has there been an increase.

1244: Email from (b) (6) to (b) (6) regarding the email at 1240:
I understand completely – in fact I leave 06SEP afternoon for Idaho Falls…in any event, a couple of options – 1) we do it by phone 2) my team leads (who more important to this effort than I am) meet with (b) (6) when he can on 7-9SEP in DC – we are in Ballston area of NoVA.
Can we work with that?

1240: Email from (b) (6) to (b) (6) regarding setting up a meeting between NCCIC and (b) (6) [redacted].
The 6th is going to be problematic for (b) (6)'s schedule. Can we look at a time later in the week or during the following week? He will be in NJ on Friday, September 16, but every other day he is available in DC.

Please let me know what works best.

0907: (b) (6) sent email stating (b) (5), (b) (7)(E):
(b) (5), (b) (7)(E)

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

0825: (b) (6) replied to an email from (b) (6) on August 25 regarding an additional IP found during the MD technical analysis (73.128.172.222)
We ran a SILK query for activity from this IP between 7/29 – 7/30. No activity was identified

26 August:

1729: Received email from (b) (6) giving an update to USG 112, USG 113, USG 114
Media for 112 arrived this morning, it has gone through the intake process and analysis will begin Monday morning

Still awaiting media for 113, we have provided them our mailing address so they can send us some log data, unsure about status of system image(s)

We have finished the preliminary report for 114, will get with Brian Gross on Monday to make sure dissemination is handled properly

1510: (b) (6) called (b) (6) and (b) (6) letting them know we didn't forget about them and still want to talk when leadership decides what they want to offer and asked if they have anything else that may have come up.

1240: Received email from (b) (6) giving an update to USG 112 & USG 113
Media from 112 arrived this morning. It is going through our intake process and analysis will begin Monday.

No updates yet for 113.

0709: Received final three company profiles from OCIA (MicroVote General Corp, Unilect Corp and IVS LLC).

25 August:

0846: email from (b) (6) stating (b) (5), (b) (7)(E)

(b) and (b) are checking Einstein and passing to CTIS and (b) (6) will run a SILK query from 7/28-7/30 but won't have results until Monday, August 29, 2019.

0751: (b) (6) email (b) (6), (b) (6) and myself telling us to prep for a discussion with (b) (6) who is associated with the Trump Transition Team for the first week in September 2016.

0733: (b) (6) commenting on (b) (5)
(b) (5)

Need to find out what he wants done with that comment?

0701: Received 5 company profiles from OCIA (Clear Ballot, DFM Associates, Danaher Controls, Hart InterCivic, Avante Technology); 5 profiles remain.

24 August:

1844: (b) (6) replied to email from 1548, stating this was the first he was hearing of it.

1548: Received email from (b) (6) (OGC) through (b) (6) with the draft elections contact protocol attached. (b) asked (b) (6) if he has any guidance that we should be aware of.

1428: (b) (6) replied to email from 1407 stating he has not been working the Campaign outreach side, he asked (b) if she's working it.

1407: Sent email to (b) (6) asking about the status of a protocol when dealing with reaching out to political organizations
Do you know where we are in this process? We need this and what the organization is willing to offer before we can finish reaching out to the remaining political organizations. One of the concerns raised by OGC was offering support to one party while waiting several days to provide support to another party. As of right now, the reach out has been unbalanced with the last contact occurring August 11th.

1315: Received two company profiles from OCIA (Unisyn Voting Solutions)

1141: (b) (6) (USSS) replied that USSS and FBI ar (b) (5), (b) (7)(E).

0743: Asked the NDO by email to reach out to the CYWATCH and ask (b) (5), (b) (7)(E).

0639: Received two company profiles from OCIA (Dominion and ES&S)

23 August:

1155: Received email from ANDO with an open source article referencing an unconfirmed attack on the computer systems of Presidential Candidate Donald Trump. (http://www.reuters.com/article/us-usa-cyber-republicans-idUSKCN10T2HY). Assigned ticket number 10085538 and asked FBI Liaison if they have anything on the situation.

1058: Received email from (b) (6) requesting the DNC/DCCC MIFR not be published at all, but DHS can use the indicators for network defense in the Einstein systems. FBI executive management will send a formal request in writing to (b) (6).

1019: Received email from Justin Brecese regarding (b) (5), (b) (7)(E)

[redacted]

1001: Received email from (b) (6) (MS-ISAC) giving additional details for the potential North Dakota voter issue, "they identified malicious activity from "a couple of the IPs and URLs" we provided in the 8/1 Cyber Alert". Updated daily reports.

22 August:

1306: (b) (6) provided an answer to the request from (b) (6), Ticket number INC000010085294. Will close out with CERT.

1135: Public Affairs request for assistance from (b) (6), (b) (6) of Government Executive regarding NCCIC and election cybersecurity. She is interested in how the NCCIC, specifically its personnel and EINSTEIN vulnerability scans, is helping to improve election cybersecurity.

1. Is DHS offering to have the NCCIC/CERT deploy EINSTEIN on voting systems?

2. If so, does that require dispatching a DHS expert to visit the town's system for EINSTEIN assistance -- or do you have some sort of agreement with local ISPs to do that?

3. Has any locality taken up DHS on its offer to provide NCCIC vulnerability scans (I.e. EINSTEIN)? If so, how many? Can you name any?

Ticket number INC000010085294.

19 August:

NSTR

18 August:

1500: US-CERT ((b) (6), (b) (6)) held a call with USG 114 to discuss the potential incident. CERT Digital Media Analysis team will be taking images of 2 servers for analysis as a precaution; there is no indication there was a compromise.

1300: Met with (b) (6) to help her get started on an incident response plan for the elections in the unlikely chance something goes wrong.

1253: Email from (b) (6) stating a conference call is scheduled for today at 3 pm ET with USG114. We'll be speaking with (b) (6) .

0737: SITREP [UPDATE-4] was distributed on the low side with the following updates.

- Tuesday, August 16, 2016 - (b) (5), (b) (7)(E)

- Monday, August 15, 2016 - NCCIC engaged the Republican Presidential Candidate Transition Team to offer technical assistance. NCCIC will continue discussions with the campaign at a later date.

- Friday, August 12, 2016 - A hacker known as Guccifer 2.0, posted on a blog site, personal information comprising of phone numbers, email addresses and passwords, for nearly 200 current and former Democratic members of the U.S. Congress and their staff, including current members of intelligence and armed services committees. The hacker claims the information was stolen from the DCCC. LE is aware and working the situation.

17 August:

1708: SITREP [UPDATE-4] Was sent to CRG on the high side with the following updates.

- Tuesday, August 16, 2016 - (b) (5), (b) (7)(E)

- Monday, August 15, 2016 - NCCIC engaged the Republican Presidential Candidate Transition Team to offer technical assistance. NCCIC will continue discussions with the campaign at a later date.

- Friday, August 12, 2016 - A hacker known as Guccifer 2.0, posted on a blog site, personal information comprising of phone numbers, email addresses and passwords, for nearly 200 current and former Democratic members of the U.S. Congress and their staff, including current members of intelligence and armed services committees. The hacker claims the information was stolen from the DCCC. LE is aware and working the situation.

1517: Received email from (b) (6) regarding (b) (5), (b) (7)(E)

1430: Discussion between (b) (6) (b) (6) and (b) (6) regarding how best to engage Crowdstrike. Agreement has been reached to wait until (b) (5), (b) (7)(E) before trying to engage with Crowdstrike.

1119: (b) (6) emailed saying US-CERT is (b) (5), (b) (7)(E) .

0852: Received an email from (b) (6) asking for any details that can be shared regarding the NCCIC call with the state of Illinois. (b) shared (b) (5), (b) (7)(E)

(b) (5), (b) (7)(E) .

16 August:

1539: (b) (6) forwarded an email from MS-ISAC (b) (5), (b) (7)(E)

1121: (b) (6) provided the “READOUT OF SECRETARY JOHNSON’S CALL WITH STATE ELECTION OFFICIALS ON CYBERSECURITY” from the August 15th call between S1 and NASS. With respect to the NCCIC, S1 promoted Cyber Hygiene and recommended that all States request that service. He suggested that additional vulnerability assessments may be offered after the election. CSAs and PSAs were offered by DUS Schneck and Dr. Ozment as points of contact for engagement. The most “controversial” point of discussion was what it would mean to designate election infrastructure as critical infrastructure and whether to make that designation. There is a lot of misunderstanding at the States as to what that would mean. – (b) (6)

1116: (b) (6) provided an update to the DNC/DCCC malware DVD. The analysis is finished and they are working on getting the report published.

0852: (b) (6) provided a second POC ((b) (6)) at Crowdstrike to use for future coordination efforts.

0840: (b) (6) provided a POC (through (b) (6)) at Crowdstrike ((b) (6)) to use for future coordination efforts.

15 August:

1415: Teleconference with Congressman Rogers. (b) (6), Congressman Rogers, (b) (6), (b) (6) in attendance. Rogers will follow up in a few days with a technical POC for the Trump Campaign.

1300: (b) (6) informed (b) (6) he has not received a response from the Chief Operating Officer at Crowdstrike to obtain a company POC.

1000: Conference call with (b) (5), (b) (7)(E) with (b) (6) in attendance. (b) (5), (b) (7)(E)

0842: (b) (5), (b) (7)(E)

0741: (b) (6) sent the meeting notes from the August 12 EAC/NIST conference call to (b) (6). This conversation and the recommendations from EAC and NASS are going to result in significant changes to our near-term plan, to include potentially releasing NO products related to the cybersecurity of election infrastructure prior to the Election.

12 August:

1913: NDO provided email from (b) (6) to US-CERT to upload to the DCCC/DNC ticket INC10075440.

1855: Director (b) (6) sent an email saying we should be checking into the **FLASH: Threat Actor "Guccifer 2.0" Claims to Have Hacked the DCCC** with our incident efforts. He also requested it get passed to I&A as well.

1445: (b) (6) from I&A sent email saying there had been no activity for the week associated with the RNC/DNC/DCCC.

1139: (b) (6) sent email to (b) (6) and (b) (6) (GOP) providing (b) (6) 's, (b) (6) 's, (b) (6) 's, and (b) (6) ' email address since (b) (6) will be out of the office next week. (b) (5), (b) (7)

1051: (b) (6) sent an email to (b) (6) (OGC) regarding the Hatch Act. Requesting a read out of a transmission between the FBI and DOJ.

11 August:

1548: (b) (6) sent email to (b) (6) regarding setting up a time to receive daily updates associated with the DNC/DCCC/RNC activities.

1330: FBI conducted a classified brief regarding the time line of DNC events. Conference room 1002.

1200: Conference call with (b) (6) , to discuss (b) (5), (b) (7)(E) with (b) (6) in attendance. Technical details and specifics of intrusion were discussed; call ended with AZ agreeing to send images of impacted server and impacted user workstation to US-CERT for analysis.

1135: (b) (6) from US-CERT sent email to US-CERT SWO with (b) (5), (b) (7)(E)

1118: (b) (6) provided the requested OCIA Company Profiles for the Democratic Congressional Campaign Committee (DCCC), National Association of Secretaries of State (NASS), National Association of State CIOs (NASCIO), and the US Elections Assistance Commission (EAC). Products are located in a binder at the Mission Manager desk in the bottom drawer of the cabinet and in a folder called "company profiles" within the NCCIC Mission Manager mailbox.

1014: AS (b) (6) sent email to (b) (6) saying that we needed to discuss NY Times articles (http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=1 and http://nyti.ms/2b9ZeiH) with FBI today because the S1 was asking about it. I have no insight into the summary of this conversation.

0930: Conference call completed with (b) (6) and (b) (6) (RNC Reps). NEED CALL SUMMARY.

10 August:

1532: (b) (6) from SLTT Cybersecurity Program sent an email to (b) (6) to loop in (b) (6) to contribute to the development of the 3 voting products.

1505: (b) (6) provided (b) (5), (b) (7)(E)

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

[redacted]

[redacted]

1442: (b) (6) sent an email saying that they hadn't pursued a contact at Crowdstrike, so (b) 's assistance on obtaining a POC would be appreciated.

0816: (b) (6) sent an invite to attend the Ops Coordination Meeting that day at 1430 in 1002 to discuss ongoing activity around the DNC/DCCC and our cybersecurity of Election Infrastructure work. General coordination meeting regarding the election issues and going over the proposed action campaign.

0704: (b) (6) provided the requested OCIA Company Profile for the National Association of State Election Directors (NASED) and the National Governors Association (NGA).

9 August:

1857: (b) (6) responded to (b) (6) 's email with the following; (b) (5), (b) (6)

1835: Email from D/AS (b) (6) to (b) (6) and (b) (6), the email text is as follows; " This afternoon we had an NPPD huddle to discuss election security issues. Alaska is of keen interest as they offer on-line voting options. U/S Spaulding would like to chat sometime before the end of the week with the Alaska Secretary State or senior official responsible for the state election infrastructure so that she can get a better understanding of how the state are addressing cyber and other risks to the election infrastructure. She asked me to reach out to you to see if you have a relationship with the Alaska leadership or a point of contact we can reach out to in order to set up the conversation?."

1827: Email from (b) (6) stating that we should ask OCIA to include the following "A risk assessment that can be used to clearly articulate the rational for our engagement strategy (e.g. who did we reach out to, who was first, why were they first, etc.). As part of this assessment, it should include the relevant variables that they used to make this determination (e.g. # of electoral votes, population size, accessibility to online methods of voting, etc.). This risk assessment should then be used as justification for the engagement strategy with each state (e.g. the type of response we see necessary [I don't imagine one size fits all here], level of importance, etc)."

1555: (b) (6) responded to the email from (b) (6) with the following DOJ contact information: (617) 892-2393 cell or (703) 633-5674 desk.

1545: FBI SSA (b) (6) sent an email to (b) (6) with the following text "I had a chance to reach out to (b) (6), about your request below. He had some excellent insight on the issues and had suggestions about engagement with the Election Assistance Commission (as well as other entities associated with the US Election Infrastructure). He is available for a call or meeting in the next couple days (he is not available late Thursday afternoon and all day Friday). Please let me know if you would like to confer with him and I will arrange the details." (b) (6)'s contact information is (b) (6).

1347: (b) (6) from the OCIA Integrated Analysis Cell sent an email to (b) (6) providing the requested OCIA Company Profile for the National Committee's (RNC & DNC).

1335: (b) (6) forwarded the DNC/DCCC SITREP-2 from NCCIC to staff on our Congressional committees of jurisdiction.

1335: (b) (6) received email saying that the RNC POC would be available after 2:00pm that day for a quick conference call.

1332: SITREP – UPDATE 3 Revision released.
0950:

8 August:

1930: SITREP – UPDATE 3 released.

1723: Email from (b) (6) approving release of SITREP – UPDATE 3, along with instructions to move to the high side and distribute to CRG members.

7 August:

1549: (b) (6) of the DNC acknowledged (b) (6)'s email, signifying that the DNC and their counsel – (b) (6) – are looking forward to hearing more about how DHS can support the DNC and he'll leave it to (b) (6) to follow up.

5 August:

1702: Mission Manager's Update 2 created and distributed. It summarized the fact that the US-CERT initiated a dialogue with the Clinton presidential campaign to offer US-CERT's technical assistance.

1146: (b) (6) replies to (b) (6)'s email

1130: Conducted conference call with Clinton Campaign reps (b) (6) and (b) (6) to offer technical assistance. (b) (6) in attendance. They are awaiting further comms from us once we have indicators to share. The acknowledged (b) (6)'s representation of them as well.

1041: Follow-up email from (b) to (b) (6) asking him to follow-up with FBI to verify if the empty directory was in fact supposed to contain files.

1035: (b) (6) responds to (b) (6) and informs him that he has a call scheduled with Hillary Clinton's Campaign COO and CIO at 1130.

1014: Email from (b) (6) sent to (b) (6) detailing the number of directories on the DVD (3, with 1 of them is empty), total number of files in those directories (22), and an estimated time to provide an initial analysis (2 – 3 days).

1008: (b) (6) asks (b) (6) via email that he please cc (b) (6) on further emails and is waiting on (b) to get back to him regarding information sharing.

0959: (b) responds to (b) (6) 's email clarifying the reason for the attempted outreach.

0909: Email from (b) (6) to (b) (6) regarding (b) 's attempted outreach on August 4 to DNC CTO and COO.

0855: LHM and Malware DVD were passed to (b) (6).

4 August:

2211: (b) (6) emails RNC/NCCIC group asking for the best time to connect.

1804: (b) (6) responds to the group.

1800: (b) responds to (b) 's email bringing in (b) (6).

1456: Response received from (b) identifying (b) (6) as a RNC POC.

Unknown: (b) (6) reached out to a third party ((b) (6), Fort Alice Solutions) to engage RNC.

Unknown: (b) (6) attempted to contact the alternate DNC/DCCC POCs (CTO, COO), negative contact made. POCs came through a third party (Cambridge Global) (b) (6).

3 August:

1711: Email sent by (b) (6) with his assessment of the DNC/DCCC coordination call. Additional information from this email recommended reaching out to the RNC/RCC and other political parties to offer similar assistance.

1430: Operations Coordination meeting to discuss roles and responsibilities for the development of products to support DNC/DCCC incidents, and the presidential campaign.

1100: (b) (5), (b) (6), (b) (7)(E)

1000: (b) (6) has requested that the vendors for the various voting machines be identified so they can be contacted for situational awareness on the risks associated with voting equipment.

0715: (b) (6) briefed on the current status of Mission Manager objectives. He also clarified that (b) (5), (b) (7) [redacted]. He also stated he wanted to actively engage the I&A team and he wants one product encompassing all aspects of the presidential election to include online voting and electronic voting machines.

2 August:

2327: (b) (5), (b) (7)(E) [redacted].

2000: (b) (5), (b) (7)(E) [redacted]

1346: Mission Manager updated SDB (SDB-1), however; it is still in draft format awaiting further changes.

1336: (b) (5), (b) (7)(E) [redacted] The Mission Manager has requested notification upon receipt of DVD.

1135: (b) (5), (b) (7)(E) [redacted]

1121: SITREP (Update – 2) sent. (b) (5), (b) (7)(E) [redacted]

1100: Mission Manager Assigned to DNC/DCCC Incident (b) (6) [redacted])

1 August:

Unknown: (b) (5), (b) (7)(E) [redacted].

31 July:

No new information for update

30 July:

On July 29, 2016, NCCIC submitted an SDB for August 1, 2016. NCCIC is also keeping senior leadership updated trough the SITREP process. US-CERT requested a coordination call with CyWatch and the FBI threat unit on August 1, 2016.

July 29, 2016:

No new information for update

July 28, 2016:

Open source reporting previously unreported cyber incident at the DCCC. Per NCCIC representatives at the MACC, the FBI Cyber program coordinator (PC) reported this was all part of the same intrusion set reported earlier. It is all part of the same case [DNC breach] the FBI opened that was discussed before the DNC began. (b) (5), (b) (7) (E) [redacted]