April 22, 2019

Via Email [*joshua.lawson@ncsbe.gov*]

Josh Lawson, Esq.
General Counsel
North Carolina State Board of Elections
430 N. Salisbury Street, Third Floor
Raleigh, North Carolina 27603

Re: State Board Request for assurance from VR Systems, Inc.

Dear Mr. Lawson:

We are in receipt of North Carolina State Board of Elections ("Board") 18 April 2019 correspondence seeking immediate assurance by VR Systems, Inc. ("VR Systems") regarding the security of its network and the electronic poll book product marketed as "EViD."

Specifically, the Board seeks to (1) confirm whether VR Systems or its agent is "Vendor 1" referenced in the *Indictment* at Paragraph 73 and/or in the *Report* at page 51 as the "voting technology company that developed software . . . to manage voter rolls"; (2) indicate whether VR Systems believes its responses to discovery remain accurate, given any new information it has received; and (3) provide representations to the Board regarding the present security of VR Systems' network and EViD product.

VR Systems represents to the Board in this correspondence that all responses to previous litigation discovery remain accurate, VR Systems was not breached during a phishing attempt, and VR Systems doesn't host voter registration data. Since VR Systems first alerted the Federal Bureau of Investigation ("FBI") in August 2016 of an attempted spearphishing attack, to VR Systems's knowledge, EViD has never been hacked.

Addressing current security, VR Systems issued the following statement 18 April 2019 (attached):

> Today's report [the *Report*] reiterates details that have been known for several years about the spear phishing attempts made during the 2016 election period. At VR Systems, our number one priority is and has always been ensuring the integrity of the elections process. We engage top cyber security experts to continuously monitor our systems and provide best-in-class technology, training and support to elections officials across the country.

1101 Haynes Street, Suite 205
P.O. Box 121
Raleigh, NC 27602-0121
T: 919-679-1776 F: 919-679-1783

> Immediately after the spear phishing attempt, VR Systems implemented a comprehensive program to ensure integrity in elections. This included engaging a leading global cyber security firm to consult, test and monitor VR's systems and servers, and a host of best practices and training with employees and customers. We are pleased that we were the first elections vendor to complete a Risk Vulnerability Assessment (RVA) by the Department of Homeland Security. While we are proud of these efforts, we know that no system is ever completely secure and we work tirelessly every day to protect our systems and our customers.

VR Systems has no independent knowledge and is unable to confirm or deny whether it is Vendor 1 of Paragraph 73 in the *Indictment*, or the "voting technology company that developed software . . . to manage voter rolls" referenced by the *Report* at Page 51. Neither the FBI, the Department of Homeland Security ("DHS"), nor the National Security Agency ("NSA") has ever contacted VR Systems as to these specific "hacking" incidents.

In fact, VR Systems contacted the FBI after the spearphishing attempts, and worked with DHS for a Risk and Vulnerability Assessment (RVA), and a DHS Cyber Hunt activity to ensure VR Systems is not breached and to proactively hunt for malicious activity. The results found no indications of a breach of any kind. VR Systems continues to participate in DHS Cyber Hygiene scans with weekly results on actions needed. Finally, at the time of the attack, VR Systems hired a third-party computer security vendor to conduct an analysis of all systems used to develop software and support customers, finding no breaches during phishing attempts or any intrusions found on those systems. This third-party vendor continues to provide real-time monitoring and attack mitigation for VR Systems.

Your letter states, "[t]he Special Counsel's Report and Indictment state that Russian cyber actors in 2016 targeted a vendor of software systems used to verify voter registration information—identified as "Vendor 1" in the *Indictmen*[1] and in redacted form [PP…..] in the *Report*. Specifically, today's *Report* indicates that Russian intelligence successfully "installed malware on the company network," which "permitted the GRU to access the infected computer," along with "at least one Florida county government." [*Footnote references removed*]

Your letter misrepresented the *Report*'s findings. As the *Indictment* and *Report* clearly state, these are two separate hacking attempts by GRU. You misstate that Russian intelligence installed malware on the company network (*which did not occur at VR Systems*) permitting GRU to access the infected computer, along with one Florida county government.

There is no causal link between the attempted hack into VR Systems, and the apparent access to one Florida county government from a separate spearphishing attack.

> In or around August 2016, KOVALEV and his co-conspirators hacked into the computers of a U.S. vendor ("Vendor 1") that supplied software used to verify voter registration information for the 2016 U.S. elections. KOVALEV and his co-conspirators used some of the same

> infrastructure to hack into Vendor 1 that they had used to hack into SBOE.
>
> In or around November 2016 and prior to the 2016 U.S. presidential election, KOVALEV and his co-conspirators used an email account designed to look like a Vendor 1 email address to send over 100 spearphishing emails to organizations and personnel involved in administering elections in numerous Florida counties. The spearphishing emails contained malware that the Conspirators embedded into Word documents bearing Vendor 1's logo.[1]

No information has been provided by the FBI, DHS, NSA, or the Office of Special Counsel to verify that VR Systems' computers were hacked, much less had malware installed on its company network. Further, the *Report* explicitly states the Office of Special Counsel did not independently verify FBI beliefs, nor undertake any investigative steps to do so.

> Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel involved in voting technology. In August 2016, GRU officers targeted employees of Vendor 1, a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election.
>
> The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer. **The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so**.[2] (*Emphasis added*)

[1] Indictment ¶¶73 and 76, *U.S. v. Viktor Borisovich Netyksho, et al* (1:18-cr-215, District of Columbia) (2018)

[2] Pages 50-51, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* by Special Counsel Robert S. Mueller III (18 April 2019) (the "*Report*")

Since 9 June 2017 (at least), Ben Martin, the Chief Operating Officer has offered and been available to discuss any security concerns the Board might have.[3] VR Systems and Mr. Martin continue to be available for consultation regarding any matter.

Similarly, you made comments to the media hours after the Board's communication was transmitted to counsel on 18 April 2019, insinuating this alleged "hacking" into VR Systems' EViD software was possibly responsible for 2016 voting issues in Durham County.

> But if the company is in fact the one referenced in the Mueller report, Lawson said, it will be the first acknowledgement that hackers were actually successful in compromising the firm's network.
> …
> In those court filings, elections officials asked VR Systems if it "ever experienced a breach of security regarding EViD." The company's answer: No.
>
> "If there was knowledge of any type of breach and the answer was a two letter answer – 'no' – we need to know why," Lawson said Thursday evening.
> …
> In a statement Thursday evening, Gannon said elections investigators believe "user error" by Durham County poll workers contributed to the voting issues in 2016. But he said that's not conclusive, "in part because the agency lacks the necessary technical expertise to forensically analyze the computers used in Durham County, and other government agencies declined the agency's requests to evaluate them."
>
> Lawson said he hopes the company's response will provide clarity.
>
> "That file has not been closed," Lawson said. "There are plausible explanations, but they do not fully explain why what happened."
>
> https://web.archive.org/web/20190419125743/https://www.wral.com/in-wake-of-mueller-report-nc-elections-officials-want-answers-from-electronic-pollbook-vendor/18334949/

As you and the Board are well aware, State Board of Elections spokesman Pat Gannon stating that "…VR Systems failed to immediately explain what happened. When Durham County hired a digital forensics firm to investigate, its report was inconclusive" is patently false. A third-party report found, "…the EViD application did not fail during the election. It appears that certain steps were not

[3] *VR Systems, Inc. v. North Carolina State Board of Elections & Ethics Enforcement*, 20 November 2017, Petitioner-Appellee's Benjamin Martin Affidavit, Page 4, ¶14

taken to verify all laptops were properly prepared for the November election." Durham County election board workers handled laptop preparation, not VR Systems.[4]

VR Systems previously offered to pay for additional forensic third-party investigation to help determine the cause of failure. However, the Board has rejected these offers, meanwhile sequestering all of the evidence, including computer hard drives, and refusing to permit any access to it or even a mirrored copy of the hard drives.

There is a certain irony in the Board's security concerns about VR Systems yet refusing to answer any questions about its own security issues in litigation.[5]

> 8. Have you ever experienced a breach of security regarding EViD, SEIMS, SOSA, or OVRD, including but not limited to unauthorized access to the codes, voter data, voting data, or personally identifiable information?
>
> **ANSWER:**
>
> The SBE objects to this interrogatory as seeking information that is neither relevant to the subject matter of this action nor reasonably calculated to lead to the discovery of admissible evidence. The SBE further objects to this interrogatory as it is undefined, ambiguous, overbroad, unduly burdensome, and vague.

Particularly, when Marc Burris, the Board's Chief Information Officer acknowledged the Board's website might have been compromised.

> Today I was alerted by the FBI that our NCSBE election website might have been compromised. Upon initial review we did identify those groups successfully inserted unauthorized index.html files into our public website. Our systems quickly identified the corrupt file and replaced it with the original file, which is why you probably are not seeing this in the news. Upon review of our logs this happened on 6/25/2017 and again today around 2:30pm.[6]

[4] Ibid, Page 4, ¶13

[5] *VR Systems, Inc. v. North Carolina State Board of Elections & Ethics Enforcement*, 2 April 2018, Respondent's Response to Petitioner's First Set of Interrogatories and First Request for Production of Documents.

[6] *VR Systems, Inc. v. North Carolina State Board of Elections & Ethics Enforcement*, 20 November 2017, Petitioner-Appellee's Benjamin Martin Affidavit, Exhibit 3

Should you need any further clarification or information prior to another Board release of VR Systems correspondence to the press, please don't hesitate to call me at 919.679.1776 at any time, or by email at mlweisel@caplawgrp.com.

Sincerely,

CAPITAL LAW GROUP

Michael L. Weisel

MLW/emp

Enclosures:
1. VR Systems, Inc. Statement 18 April 2019
2. Indictment, *U.S. v. Viktor Borisovich Netyksho, et al* (1:18-cr-215, District of Columbia) (2018)
3. Excerpt – pages 50-51, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* by Special Counsel Robert S. Mueller III (18 April 2019)
4. *VR Systems, Inc. v. North Carolina State Board of Elections & Ethics Enforcement*, 20 November 2017, Petitioner-Appellee's Benjamin Martin Affidavit

FOR IMMEDIATE RELEASE:
April 18, 2019

Statement from VR Systems
Regarding 4-18-19 Special Counsel Report

From Ben Martin, VR Systems, Chief Operating Officer

“Today’s report reiterates details that have been known for several years about the spear phishing attempts made during the 2016 election period.

“At VR Systems, our number one priority is and has always been ensuring the integrity of the elections process. We engage top cyber security experts to continuously monitor our systems and provide best-in-class technology, training and support to elections officials across the country.

‘Immediately after the spear phishing attempt, VR Systems implemented a comprehensive program to ensure integrity in elections. This included engaging a leading global cyber security firm to consult, test and monitor VR’s systems and servers, and a host of best practices and training with employees and customers. We are pleased that we were the first elections vendor to complete a Risk Vulnerability Assessment (RVA) by the Department of Homeland Security. While we are proud of these efforts, we know that no system is ever completely secure and we work tirelessly every day to protect our systems and our customers.”

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	*	
	*	CRIMINAL NO.
v.	*	
	*	(18 U.S.C. §§ 2, 371, 1030, 1028A, 1956,
VIKTOR BORISOVICH NETYKSHO,	*	and 3551 et seq.)
BORIS ALEKSEYEVICH ANTONOV,	*	
DMITRIY SERGEYEVICH BADIN,	*	
IVAN SERGEYEVICH YERMAKOV,	*	
ALEKSEY VIKTOROVICH LUKASHEV,	*	
SERGEY ALEKSANDROVICH MORGACHEV,	*	
NIKOLAY YURYEVICH KOZACHEK,	*	
PAVEL VYACHESLAVOVICH YERSHOV,	*	
ARTEM ANDREYEVICH MALYSHEV,	*	
ALEKSANDR VLADIMIROVICH OSADCHUK,	*	
ALEKSEY ALEKSANDROVICH POTEMKIN, and	*	
ANATOLIY SERGEYEVICH KOVALEV,	*	
	*	
Defendants.	*	
	*	

****

INDICTMENT

The Grand Jury for the District of Columbia charges:

COUNT ONE
(Conspiracy to Commit an Offense Against the United States)

1. In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted large-scale cyber operations to interfere with the 2016 U.S. presidential election.

2. Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSANDR VLADIMIROVICH OSADCHUK, and ALEKSEY ALEKSANDROVICH POTEMKIN were GRU officers who knowingly and intentionally conspired with each other, and with persons known and unknown to the Grand Jury (collectively the "Conspirators"), to gain unauthorized access (to "hack") into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election.

3. Starting in at least March 2016, the Conspirators used a variety of means to hack the email accounts of volunteers and employees of the U.S. presidential campaign of Hillary Clinton (the "Clinton Campaign"), including the email account of the Clinton Campaign's chairman.

4. By in or around April 2016, the Conspirators also hacked into the computer networks of the Democratic Congressional Campaign Committee ("DCCC") and the Democratic National Committee ("DNC"). The Conspirators covertly monitored the computers of dozens of DCCC and DNC employees, implanted hundreds of files containing malicious computer code ("malware"), and stole emails and other documents from the DCCC and DNC.

5. By in or around April 2016, the Conspirators began to plan the release of materials stolen from the Clinton Campaign, DCCC, and DNC.

6. Beginning in or around June 2016, the Conspirators staged and released tens of thousands of the stolen emails and documents. They did so using fictitious online personas, including

"DCLeaks" and "Guccifer 2.0."

7. The Conspirators also used the Guccifer 2.0 persona to release additional stolen documents through a website maintained by an organization ("Organization 1"), that had previously posted documents stolen from U.S. persons, entities, and the U.S. government. The Conspirators continued their U.S. election-interference operations through in or around November 2016.

8. To hide their connections to Russia and the Russian government, the Conspirators used false identities and made false statements about their identities. To further avoid detection, the Conspirators used a network of computers located across the world, including in the United States, and paid for this infrastructure using cryptocurrency.

Defendants

9. Defendant VIKTOR BORISOVICH NETYKSHO (Нетыкшо Виктор Борисович) was the Russian military officer in command of Unit 26165, located at 20 Komsomolskiy Prospekt, Moscow, Russia. Unit 26165 had primary responsibility for hacking the DCCC and DNC, as well as the email accounts of individuals affiliated with the Clinton Campaign.

10. Defendant BORIS ALEKSEYEVICH ANTONOV (Антонов Борис Алексеевич) was a Major in the Russian military assigned to Unit 26165. ANTONOV oversaw a department within Unit 26165 dedicated to targeting military, political, governmental, and non-governmental organizations with spearphishing emails and other computer intrusion activity. ANTONOV held the title "Head of Department." In or around 2016, ANTONOV supervised other co-conspirators who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign.

11. Defendant DMITRIY SERGEYEVICH BADIN (Бадин Дмитрий Сергеевич) was a Russian military officer assigned to Unit 26165 who held the title "Assistant Head of Department." In or around 2016, BADIN, along with ANTONOV, supervised other co-conspirators who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign.

12. Defendant IVAN SERGEYEVICH YERMAKOV (Ермаков Иван Сергеевич) was a Russian military officer assigned to ANTONOV's department within Unit 26165. Since in or around 2010, YERMAKOV used various online personas, including "Kate S. Milton," "James McMorgans," and "Karen W. Millen," to conduct hacking operations on behalf of Unit 26165. In or around March 2016, YERMAKOV participated in hacking at least two email accounts from which campaign-related documents were released through DCLeaks. In or around May 2016, YERMAKOV also participated in hacking the DNC email server and stealing DNC emails that were later released through Organization 1.

13. Defendant ALEKSEY VIKTOROVICH LUKASHEV (Лукашев Алексей Викторович) was a Senior Lieutenant in the Russian military assigned to ANTONOV's department within Unit 26165. LUKASHEV used various online personas, including "Den Katenberg" and "Yuliana Martynova." In or around 2016, LUKASHEV sent spearphishing emails to members of the Clinton Campaign and affiliated individuals, including the chairman of the Clinton Campaign.

14. Defendant SERGEY ALEKSANDROVICH MORGACHEV (Моргачев Сергей Александрович) was a Lieutenant Colonel in the Russian military assigned to Unit 26165. MORGACHEV oversaw a department within Unit 26165 dedicated to developing and managing malware, including a hacking tool used by the GRU known as "X-Agent." During the hacking of the DCCC and DNC networks, MORGACHEV supervised the co-conspirators who developed and monitored the X-Agent malware implanted on those computers.

15. Defendant NIKOLAY YURYEVICH KOZACHEK (Козачек Николай Юрьевич) was a Lieutenant Captain in the Russian military assigned to MORGACHEV's department within Unit 26165. KOZACHEK used a variety of monikers, including "kazak" and "blablabla1234565." KOZACHEK developed, customized, and monitored X-Agent malware used to hack the DCCC

and DNC networks beginning in or around April 2016.

16. Defendant PAVEL VYACHESLAVOVICH YERSHOV (Ершов Павел Вячеславович) was a Russian military officer assigned to MORGACHEV's department within Unit 26165. In or around 2016, YERSHOV assisted KOZACHEK and other co-conspirators in testing and customizing X-Agent malware before actual deployment and use.

17. Defendant ARTEM ANDREYEVICH MALYSHEV (Малышев Артём Андреевич) was a Second Lieutenant in the Russian military assigned to MORGACHEV's department within Unit 26165. MALYSHEV used a variety of monikers, including "djangomagicdev" and "realblatr." In or around 2016, MALYSHEV monitored X-Agent malware implanted on the DCCC and DNC networks.

18. Defendant ALEKSANDR VLADIMIROVICH OSADCHUK (Осадчук Александр Владимирович) was a Colonel in the Russian military and the commanding officer of Unit 74455. Unit 74455 was located at 22 Kirova Street, Khimki, Moscow, a building referred to within the GRU as the "Tower." Unit 74455 assisted in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU.

19. Defendant ALEKSEY ALEKSANDROVICH POTEMKIN (Потемкин Алексей Александрович) was an officer in the Russian military assigned to Unit 74455. POTEMKIN was a supervisor in a department within Unit 74455 responsible for the administration of computer infrastructure used in cyber operations. Infrastructure and social media accounts administered by POTEMKIN's department were used, among other things, to assist in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas.

Object of the Conspiracy

20. The object of the conspiracy was to hack into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election.

Manner and Means of the Conspiracy

Spearphishing Operations

21. ANTONOV, BADIN, YERMAKOV, LUKASHEV, and their co-conspirators targeted victims using a technique known as spearphishing to steal victims' passwords or otherwise gain access to their computers. Beginning by at least March 2016, the Conspirators targeted over 300 individuals affiliated with the Clinton Campaign, DCCC, and DNC.

a. For example, on or about March 19, 2016, LUKASHEV and his co-conspirators created and sent a spearphishing email to the chairman of the Clinton Campaign. LUKASHEV used the account "john356gh" at an online service that abbreviated lengthy website addresses (referred to as a "URL-shortening service"). LUKASHEV used the account to mask a link contained in the spearphishing email, which directed the recipient to a GRU-created website. LUKASHEV altered the appearance of the sender email address in order to make it look like the email was a security notification from Google (a technique known as "spoofing"), instructing the user to change his password by clicking the embedded link. Those instructions were followed. On or about March 21, 2016, LUKASHEV, YERMAKOV, and their co-conspirators stole the contents of the chairman's email account, which consisted of over 50,000 emails.

b. Starting on or about March 19, 2016, LUKASHEV and his co-conspirators sent spearphishing emails to the personal accounts of other individuals affiliated with

the Clinton Campaign, including its campaign manager and a senior foreign policy advisor. On or about March 25, 2016, LUKASHEV used the same john356gh account to mask additional links included in spearphishing emails sent to numerous individuals affiliated with the Clinton Campaign, including Victims 1 and 2. LUKASHEV sent these emails from the Russia-based email account hi.mymail@yandex.com that he spoofed to appear to be from Google.

c. On or about March 28, 2016, YERMAKOV researched the names of Victims 1 and 2 and their association with Clinton on various social media sites. Through their spearphishing operations, LUKASHEV, YERMAKOV, and their co-conspirators successfully stole email credentials and thousands of emails from numerous individuals affiliated with the Clinton Campaign. Many of these stolen emails, including those from Victims 1 and 2, were later released by the Conspirators through DCLeaks.

d. On or about April 6, 2016, the Conspirators created an email account in the name (with a one-letter deviation from the actual spelling) of a known member of the Clinton Campaign. The Conspirators then used that account to send spearphishing emails to the work accounts of more than thirty different Clinton Campaign employees. In the spearphishing emails, LUKASHEV and his co-conspirators embedded a link purporting to direct the recipient to a document titled "hillary-clinton-favorable-rating.xlsx." In fact, this link directed the recipients' computers to a GRU-created website.

22. The Conspirators spearphished individuals affiliated with the Clinton Campaign throughout the summer of 2016. For example, on or about July 27, 2016, the Conspirators

attempted after hours to spearphish for the first time email accounts at a domain hosted by a third-party provider and used by Clinton's personal office. At or around the same time, they also targeted seventy-six email addresses at the domain for the Clinton Campaign.

Hacking into the DCCC Network

23. Beginning in or around March 2016, the Conspirators, in addition to their spearphishing efforts, researched the DCCC and DNC computer networks to identify technical specifications and vulnerabilities.

a. For example, beginning on or about March 15, 2016, YERMAKOV ran a technical query for the DNC's internet protocol configurations to identify connected devices.

b. On or about the same day, YERMAKOV searched for open-source information about the DNC network, the Democratic Party, and Hillary Clinton.

c. On or about April 7, 2016, YERMAKOV ran a technical query for the DCCC's internet protocol configurations to identify connected devices.

24. By in or around April 2016, within days of YERMAKOV's searches regarding the DCCC, the Conspirators hacked into the DCCC computer network. Once they gained access, they installed and managed different types of malware to explore the DCCC network and steal data.

a. On or about April 12, 2016, the Conspirators used the stolen credentials of a DCCC Employee ("DCCC Employee 1") to access the DCCC network. DCCC Employee 1 had received a spearphishing email from the Conspirators on or about April 6, 2016, and entered her password after clicking on the link.

b. Between in or around April 2016 and June 2016, the Conspirators installed multiple versions of their X-Agent malware on at least ten DCCC computers, which allowed them to monitor individual employees' computer activity, steal passwords, and maintain access to the DCCC network.

c. X-Agent malware implanted on the DCCC network transmitted information from the victims' computers to a GRU-leased server located in Arizona. The Conspirators referred to this server as their "AMS" panel. KOZACHEK, MALYSHEV, and their co-conspirators logged into the AMS panel to use X-Agent's keylog and screenshot functions in the course of monitoring and surveilling activity on the DCCC computers. The keylog function allowed the Conspirators to capture keystrokes entered by DCCC employees. The screenshot function allowed the Conspirators to take pictures of the DCCC employees' computer screens.

d. For example, on or about April 14, 2016, the Conspirators repeatedly activated X-Agent's keylog and screenshot functions to surveil DCCC Employee 1's computer activity over the course of eight hours. During that time, the Conspirators captured DCCC Employee 1's communications with co-workers and the passwords she entered while working on fundraising and voter outreach projects. Similarly, on or about April 22, 2016, the Conspirators activated X-Agent's keylog and screenshot functions to capture the discussions of another DCCC Employee ("DCCC Employee 2") about the DCCC's finances, as well as her individual banking information and other personal topics.

25. On or about April 19, 2016, KOZACHEK, YERSHOV, and their co-conspirators remotely configured an overseas computer to relay communications between X-Agent malware and the AMS panel and then tested X-Agent's ability to connect to this computer. The Conspirators referred to this computer as a "middle server." The middle server acted as a proxy to obscure the connection between malware at the DCCC and the Conspirators' AMS panel. On or about April

20, 2016, the Conspirators directed X-Agent malware on the DCCC computers to connect to this middle server and receive directions from the Conspirators.

Hacking into the DNC Network

26. On or about April 18, 2016, the Conspirators hacked into the DNC's computers through their access to the DCCC network. The Conspirators then installed and managed different types of malware (as they did in the DCCC network) to explore the DNC network and steal documents.

a. On or about April 18, 2016, the Conspirators activated X-Agent's keylog and screenshot functions to steal credentials of a DCCC employee who was authorized to access the DNC network. The Conspirators hacked into the DNC network from the DCCC network using stolen credentials. By in or around June 2016, they gained access to approximately thirty-three DNC computers.

b. In or around April 2016, the Conspirators installed X-Agent malware on the DNC network, including the same versions installed on the DCCC network. MALYSHEV and his co-conspirators monitored the X-Agent malware from the AMS panel and captured data from the victim computers. The AMS panel collected thousands of keylog and screenshot results from the DCCC and DNC computers, such as a screenshot and keystroke capture of DCCC Employee 2 viewing the DCCC's online banking information.

Theft of DCCC and DNC Documents

27. The Conspirators searched for and identified computers within the DCCC and DNC networks that stored information related to the 2016 U.S. presidential election. For example, on or about April 15, 2016, the Conspirators searched one hacked DCCC computer for terms that included "hillary," "cruz," and "trump." The Conspirators also copied select DCCC folders, including "Benghazi Investigations." The Conspirators targeted computers containing information

such as opposition research and field operation plans for the 2016 elections.

28. To enable them to steal a large number of documents at once without detection, the Conspirators used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks. The Conspirators then used other GRU malware, known as "X-Tunnel," to move the stolen documents outside the DCCC and DNC networks through encrypted channels.

a. For example, on or about April 22, 2016, the Conspirators compressed gigabytes of data from DNC computers, including opposition research. The Conspirators later moved the compressed DNC data using X-Tunnel to a GRU-leased computer located in Illinois.

b. On or about April 28, 2016, the Conspirators connected to and tested the same computer located in Illinois. Later that day, the Conspirators used X-Tunnel to connect to that computer to steal additional documents from the DCCC network.

29. Between on or about May 25, 2016 and June 1, 2016, the Conspirators hacked the DNC Microsoft Exchange Server and stole thousands of emails from the work accounts of DNC employees. During that time, YERMAKOV researched PowerShell commands related to accessing and managing the Microsoft Exchange Server.

30. On or about May 30, 2016, MALYSHEV accessed the AMS panel in order to upgrade custom AMS software on the server. That day, the AMS panel received updates from approximately thirteen different X-Agent malware implants on DCCC and DNC computers.

31. During the hacking of the DCCC and DNC networks, the Conspirators covered their tracks by intentionally deleting logs and computer files. For example, on or about May 13, 2016, the Conspirators cleared the event logs from a DNC computer. On or about June 20, 2016, the

Conspirators deleted logs from the AMS panel that documented their activities on the panel, including the login history.

Efforts to Remain on the DCCC and DNC Networks

32. Despite the Conspirators' efforts to hide their activity, beginning in or around May 2016, both the DCCC and DNC became aware that they had been hacked and hired a security company ("Company 1") to identify the extent of the intrusions. By in or around June 2016, Company 1 took steps to exclude intruders from the networks. Despite these efforts, a Linux-based version of X-Agent, programmed to communicate with the GRU-registered domain linuxkrnl.net, remained on the DNC network until in or around October 2016.

33. In response to Company 1's efforts, the Conspirators took countermeasures to maintain access to the DCCC and DNC networks.

a. On or about May 31, 2016, YERMAKOV searched for open-source information about Company 1 and its reporting on X-Agent and X-Tunnel. On or about June 1, 2016, the Conspirators attempted to delete traces of their presence on the DCCC network using the computer program CCleaner.

b. On or about June 14, 2016, the Conspirators registered the domain actblues.com, which mimicked the domain of a political fundraising platform that included a DCCC donations page. Shortly thereafter, the Conspirators used stolen DCCC credentials to modify the DCCC website and redirect visitors to the actblues.com domain.

c. On or about June 20, 2016, after Company 1 had disabled X-Agent on the DCCC network, the Conspirators spent over seven hours unsuccessfully trying to connect to X-Agent. The Conspirators also tried to access the DCCC network using previously stolen credentials.

34. In or around September 2016, the Conspirators also successfully gained access to DNC computers hosted on a third-party cloud-computing service. These computers contained test applications related to the DNC's analytics. After conducting reconnaissance, the Conspirators gathered data by creating backups, or "snapshots," of the DNC's cloud-based systems using the cloud provider's own technology. The Conspirators then moved the snapshots to cloud-based accounts they had registered with the same service, thereby stealing the data from the DNC.

Stolen Documents Released through DCLeaks

35. More than a month before the release of any documents, the Conspirators constructed the online persona DCLeaks to release and publicize stolen election-related documents. On or about April 19, 2016, after attempting to register the domain electionleaks.com, the Conspirators registered the domain dcleaks.com through a service that anonymized the registrant. The funds used to pay for the dcleaks.com domain originated from an account at an online cryptocurrency service that the Conspirators also used to fund the lease of a virtual private server registered with the operational email account dirbinsaabol@mail.com. The dirbinsaabol email account was also used to register the john356gh URL-shortening account used by LUKASHEV to spearphish the Clinton Campaign chairman and other campaign-related individuals.

36. On or about June 8, 2016, the Conspirators launched the public website dcleaks.com, which they used to release stolen emails. Before it shut down in or around March 2017, the site received over one million page views. The Conspirators falsely claimed on the site that DCLeaks was started by a group of "American hacktivists," when in fact it was started by the Conspirators.

37. Starting in or around June 2016 and continuing through the 2016 U.S. presidential election, the Conspirators used DCLeaks to release emails stolen from individuals affiliated with the Clinton Campaign. The Conspirators also released documents they had stolen in other spearphishing operations, including those they had conducted in 2015 that collected emails from individuals

affiliated with the Republican Party.

38. On or about June 8, 2016, and at approximately the same time that the dcleaks.com website was launched, the Conspirators created a DCLeaks Facebook page using a preexisting social media account under the fictitious name "Alice Donovan." In addition to the DCLeaks Facebook page, the Conspirators used other social media accounts in the names of fictitious U.S. persons such as "Jason Scott" and "Richard Gingrey" to promote the DCLeaks website. The Conspirators accessed these accounts from computers managed by POTEMKIN and his co-conspirators.

39. On or about June 8, 2016, the Conspirators created the Twitter account @dcleaks_. The Conspirators operated the @dcleaks_ Twitter account from the same computer used for other efforts to interfere with the 2016 U.S. presidential election. For example, the Conspirators used the same computer to operate the Twitter account @BaltimoreIsWhr, through which they encouraged U.S. audiences to "[j]oin our flash mob" opposing Clinton and to post images with the hashtag #BlacksAgainstHillary.

Stolen Documents Released through Guccifer 2.0

40. On or about June 14, 2016, the DNC—through Company 1—publicly announced that it had been hacked by Russian government actors. In response, the Conspirators created the online persona Guccifer 2.0 and falsely claimed to be a lone Romanian hacker to undermine the allegations of Russian responsibility for the intrusion.

41. On or about June 15, 2016, the Conspirators logged into a Moscow-based server used and managed by Unit 74455 and, between 4:19 PM and 4:56 PM Moscow Standard Time, searched for certain words and phrases, including:

Search Term(s)
“some hundred sheets”
“some hundreds of sheets”
dcleaks
illuminati
широко известный перевод [widely known translation]
“worldwide known”
“think twice about”
“company’s competence”

42. Later that day, at 7:02 PM Moscow Standard Time, the online persona Guccifer 2.0 published its first post on a blog site created through WordPress. Titled “DNC’s servers hacked by a lone hacker,” the post used numerous English words and phrases that the Conspirators had searched for earlier that day (bolded below):

> **Worldwide known** cyber security company [Company 1] announced that the Democratic National Committee (DNC) servers had been hacked by “sophisticated” hacker groups.
>
> I’m very pleased the company appreciated my skills so highly))) [. . .]
>
> Here are just a few docs from many thousands I extracted when hacking into DNC’s network. [. . .]
>
> **Some hundred sheets**! This’s a serious case, isn’t it? [. . .]
>
> I guess [Company 1] customers should **think twice about company’s competence**.
>
> F[***] the **Illuminati** and their conspiracies!!!!!!!!! F[***] [Company 1]!!!!!!!!!

43. Between in or around June 2016 and October 2016, the Conspirators used Guccifer 2.0 to release documents through WordPress that they had stolen from the DCCC and DNC. The Conspirators, posing as Guccifer 2.0, also shared stolen documents with certain individuals.

a. On or about August 15, 2016, the Conspirators, posing as Guccifer 2.0, received a

request for stolen documents from a candidate for the U.S. Congress. The Conspirators responded using the Guccifer 2.0 persona and sent the candidate stolen documents related to the candidate's opponent.

b. On or about August 22, 2016, the Conspirators, posing as Guccifer 2.0, transferred approximately 2.5 gigabytes of data stolen from the DCCC to a then-registered state lobbyist and online source of political news. The stolen data included donor records and personal identifying information for more than 2,000 Democratic donors.

c. On or about August 22, 2016, the Conspirators, posing as Guccifer 2.0, sent a reporter stolen documents pertaining to the Black Lives Matter movement. The reporter responded by discussing when to release the documents and offering to write an article about their release.

44. The Conspirators, posing as Guccifer 2.0, also communicated with U.S. persons about the release of stolen documents. On or about August 15, 2016, the Conspirators, posing as Guccifer 2.0, wrote to a person who was in regular contact with senior members of the presidential campaign of Donald J. Trump, "thank u for writing back . . . do u find anyt[h]ing interesting in the docs i posted?" On or about August 17, 2016, the Conspirators added, "please tell me if i can help u anyhow . . . it would be a great pleasure to me." On or about September 9, 2016, the Conspirators, again posing as Guccifer 2.0, referred to a stolen DCCC document posted online and asked the person, "what do u think of the info on the turnout model for the democrats entire presidential campaign." The person responded, "[p]retty standard."

45. The Conspirators conducted operations as Guccifer 2.0 and DCLeaks using overlapping computer infrastructure and financing.

a. For example, between on or about March 14, 2016 and April 28, 2016, the

Conspirators used the same pool of bitcoin funds to purchase a virtual private network ("VPN") account and to lease a server in Malaysia. In or around June 2016, the Conspirators used the Malaysian server to host the dcleaks.com website. On or about July 6, 2016, the Conspirators used the VPN to log into the @Guccifer_2 Twitter account. The Conspirators opened that VPN account from the same server that was also used to register malicious domains for the hacking of the DCCC and DNC networks.

b. On or about June 27, 2016, the Conspirators, posing as Guccifer 2.0, contacted a U.S. reporter with an offer to provide stolen emails from "Hillary Clinton's staff." The Conspirators then sent the reporter the password to access a nonpublic, password-protected portion of dcleaks.com containing emails stolen from Victim 1 by LUKASHEV, YERMAKOV, and their co-conspirators in or around March 2016.

46. On or about January 12, 2017, the Conspirators published a statement on the Guccifer 2.0 WordPress blog, falsely claiming that the intrusions and release of stolen documents had "totally no relation to the Russian government."

Use of Organization 1

47. In order to expand their interference in the 2016 U.S. presidential election, the Conspirators transferred many of the documents they stole from the DNC and the chairman of the Clinton Campaign to Organization 1. The Conspirators, posing as Guccifer 2.0, discussed the release of the stolen documents and the timing of those releases with Organization 1 to heighten their impact on the 2016 U.S. presidential election.

a. On or about June 22, 2016, Organization 1 sent a private message to Guccifer 2.0 to "[s]end any new material [stolen from the DNC] here for us to review and it will

have a much higher impact than what you are doing." On or about July 6, 2016, Organization 1 added, "if you have anything hillary related we want it in the next tweo [*sic*] days prefable [*sic*] because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after." The Conspirators responded, "ok . . . i see." Organization 1 explained, "we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting."

b. After failed attempts to transfer the stolen documents starting in late June 2016, on or about July 14, 2016, the Conspirators, posing as Guccifer 2.0, sent Organization 1 an email with an attachment titled "wk dnc link1.txt.gpg." The Conspirators explained to Organization 1 that the encrypted file contained instructions on how to access an online archive of stolen DNC documents. On or about July 18, 2016, Organization 1 confirmed it had "the 1Gb or so archive" and would make a release of the stolen documents "this week."

48. On or about July 22, 2016, Organization 1 released over 20,000 emails and other documents stolen from the DNC network by the Conspirators. This release occurred approximately three days before the start of the Democratic National Convention. Organization 1 did not disclose Guccifer 2.0's role in providing them. The latest-in-time email released through Organization 1 was dated on or about May 25, 2016, approximately the same day the Conspirators hacked the DNC Microsoft Exchange Server.

49. On or about October 7, 2016, Organization 1 released the first set of emails from the chairman of the Clinton Campaign that had been stolen by LUKASHEV and his co-conspirators. Between on or about October 7, 2016 and November 7, 2016, Organization 1 released

approximately thirty-three tranches of documents that had been stolen from the chairman of the Clinton Campaign. In total, over 50,000 stolen documents were released.

Statutory Allegations

50. Paragraphs 1 through 49 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

51. From at least in or around March 2016 through November 2016, in the District of Columbia and elsewhere, Defendants NETYKSHO, ANTONOV, BADIN, YERMAKOV, LUKASHEV, MORGACHEV, KOZACHEK, YERSHOV, MALYSHEV, OSADCHUK, and POTEMKIN, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit offenses against the United States, namely:

a. To knowingly access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, where the value of the information obtained exceeded $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B); and

b. To knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, and where the offense did cause and, if completed, would have caused, loss aggregating $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

52. In furtherance of the Conspiracy and to effect its illegal objects, the Conspirators committed the overt acts set forth in paragraphs 1 through 19, 21 through 49, 55, and 57 through

64, which are re-alleged and incorporated by reference as if fully set forth herein.

53. In furtherance of the Conspiracy, and as set forth in paragraphs 1 through 19, 21 through 49, 55, and 57 through 64, the Conspirators knowingly falsely registered a domain name and knowingly used that domain name in the course of committing an offense, namely, the Conspirators registered domains, including dcleaks.com and actblues.com, with false names and addresses, and used those domains in the course of committing the felony offense charged in Count One.

All in violation of Title 18, United States Code, Sections 371 and 3559(g)(1).

COUNTS TWO THROUGH NINE
(Aggravated Identity Theft)

54. Paragraphs 1 through 19, 21 through 49, and 57 through 64 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

55. On or about the dates specified below, in the District of Columbia and elsewhere, Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSANDR VLADIMIROVICH OSADCHUK, and ALEKSEY ALEKSANDROVICH POTEMKIN did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), namely, computer fraud in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B), knowing that the means of identification belonged to another real person:

Count	Approximate Date	Victim	Means of Identification
2	March 21, 2016	Victim 3	Username and password for personal email account
3	March 25, 2016	Victim 1	Username and password for personal email account
4	April 12, 2016	Victim 4	Username and password for DCCC computer network
5	April 15, 2016	Victim 5	Username and password for DCCC computer network
6	April 18, 2016	Victim 6	Username and password for DCCC computer network
7	May 10, 2016	Victim 7	Username and password for DNC computer network
8	June 2, 2016	Victim 2	Username and password for personal email account
9	July 6, 2016	Victim 8	Username and password for personal email account

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT TEN
(Conspiracy to Launder Money)

56. Paragraphs 1 through 19, 21 through 49, and 55 are re-alleged and incorporated by reference as if fully set forth herein.

57. To facilitate the purchase of infrastructure used in their hacking activity—including hacking into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election and releasing the stolen documents—the Defendants conspired to launder the equivalent of more than $95,000 through a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin.

58. Although the Conspirators caused transactions to be conducted in a variety of currencies, including U.S. dollars, they principally used bitcoin when purchasing servers, registering domains, and otherwise making payments in furtherance of hacking activity. Many of these payments were

processed by companies located in the United States that provided payment processing services to hosting companies, domain registrars, and other vendors both international and domestic. The use of bitcoin allowed the Conspirators to avoid direct relationships with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds.

59. All bitcoin transactions are added to a public ledger called the Blockchain, but the Blockchain identifies the parties to each transaction only by alpha-numeric identifiers known as bitcoin addresses. To further avoid creating a centralized paper trail of all of their purchases, the Conspirators purchased infrastructure using hundreds of different email accounts, in some cases using a new account for each purchase. The Conspirators used fictitious names and addresses in order to obscure their identities and their links to Russia and the Russian government. For example, the dcleaks.com domain was registered and paid for using the fictitious name "Carrie Feehan" and an address in New York. In some cases, as part of the payment process, the Conspirators provided vendors with nonsensical addresses such as "usa Denver AZ," "gfhgh ghfhgfh fdgfdg WA," and "1 2 dwd District of Columbia."

60. The Conspirators used several dedicated email accounts to track basic bitcoin transaction information and to facilitate bitcoin payments to vendors. One of these dedicated accounts, registered with the username "gfadel47," received hundreds of bitcoin payment requests from approximately 100 different email accounts. For example, on or about February 1, 2016, the gfadel47 account received the instruction to "[p]lease send *exactly* **0.026043** bitcoin to" a certain thirty-four character bitcoin address. Shortly thereafter, a transaction matching those exact instructions was added to the Blockchain.

61. On occasion, the Conspirators facilitated bitcoin payments using the same computers that they used to conduct their hacking activity, including to create and send test spearphishing emails.

Additionally, one of these dedicated accounts was used by the Conspirators in or around 2015 to renew the registration of a domain (linuxkrnl.net) encoded in certain X-Agent malware installed on the DNC network.

62. The Conspirators funded the purchase of computer infrastructure for their hacking activity in part by "mining" bitcoin. Individuals and entities can mine bitcoin by allowing their computing power to be used to verify and record payments on the bitcoin public ledger, a service for which they are rewarded with freshly-minted bitcoin. The pool of bitcoin generated from the GRU's mining activity was used, for example, to pay a Romanian company to register the domain dcleaks.com through a payment processing company located in the United States.

63. In addition to mining bitcoin, the Conspirators acquired bitcoin through a variety of means designed to obscure the origin of the funds. This included purchasing bitcoin through peer-to-peer exchanges, moving funds through other digital currencies, and using pre-paid cards. They also enlisted the assistance of one or more third-party exchangers who facilitated layered transactions through digital currency exchange platforms providing heightened anonymity.

64. The Conspirators used the same funding structure—and in some cases, the very same pool of funds—to purchase key accounts, servers, and domains used in their election-related hacking activity.

a. The bitcoin mining operation that funded the registration payment for dcleaks.com also sent newly-minted bitcoin to a bitcoin address controlled by "Daniel Farell," the persona that was used to renew the domain linuxkrnl.net. The bitcoin mining operation also funded, through the same bitcoin address, the purchase of servers and domains used in the GRU's spearphishing operations, including accounts-qooqle.com and account-gooogle.com.

b. On or about March 14, 2016, using funds in a bitcoin address, the Conspirators purchased a VPN account, which they later used to log into the @Guccifer_2 Twitter account. The remaining funds from that bitcoin address were then used on or about April 28, 2016, to lease a Malaysian server that hosted the dcleaks.com website.

c. The Conspirators used a different set of fictitious names (including "Ward DeClaur" and "Mike Long") to send bitcoin to a U.S. company in order to lease a server used to administer X-Tunnel malware implanted on the DCCC and DNC networks, and to lease two servers used to hack the DNC's cloud network.

Statutory Allegations

65. From at least in or around 2015 through 2016, within the District of Columbia and elsewhere, Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSANDR VLADIMIROVICH OSADCHUK, and ALEKSEY ALEKSANDROVICH POTEMKIN, together with others, known and unknown to the Grand Jury, did knowingly and intentionally conspire to transport, transmit, and transfer monetary instruments and funds to a place in the United States from and through a place outside the United States and from a place in the United States to and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, namely, a violation of Title 18, United States Code, Section 1030, contrary to Title 18, United States Code, Section 1956(a)(2)(A).

All in violation of Title 18, United States Code, Section 1956(h).

COUNT ELEVEN
(Conspiracy to Commit an Offense Against the United States)

66. Paragraphs 1 through 8 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

Defendants

67. Paragraph 18 of this Indictment relating to ALEKSANDR VLADIMIROVICH OSADCHUK is re-alleged and incorporated by reference as if fully set forth herein.

68. Defendant ANATOLIY SERGEYEVICH KOVALEV (Ковалев Анатолий Сергеевич) was an officer in the Russian military assigned to Unit 74455 who worked in the GRU's 22 Kirova Street building (the Tower).

69. Defendants OSADCHUK and KOVALEV were GRU officers who knowingly and intentionally conspired with each other and with persons, known and unknown to the Grand Jury, to hack into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections.

Object of the Conspiracy

70. The object of the conspiracy was to hack into protected computers of persons and entities charged with the administration of the 2016 U.S. elections in order to access those computers and steal voter data and other information stored on those computers.

Manner and Means of the Conspiracy

71. In or around June 2016, KOVALEV and his co-conspirators researched domains used by U.S. state boards of elections, secretaries of state, and other election-related entities for website vulnerabilities. KOVALEV and his co-conspirators also searched for state political party email addresses, including filtered queries for email addresses listed on state Republican Party websites.

72. In or around July 2016, KOVALEV and his co-conspirators hacked the website of a state board of elections ("SBOE 1") and stole information related to approximately 500,000 voters, including names, addresses, partial social security numbers, dates of birth, and driver's license numbers.

73. In or around August 2016, KOVALEV and his co-conspirators hacked into the computers of a U.S. vendor ("Vendor 1") that supplied software used to verify voter registration information for the 2016 U.S. elections. KOVALEV and his co-conspirators used some of the same infrastructure to hack into Vendor 1 that they had used to hack into SBOE 1.

74. In or around August 2016, the Federal Bureau of Investigation issued an alert about the hacking of SBOE 1 and identified some of the infrastructure that was used to conduct the hacking. In response, KOVALEV deleted his search history. KOVALEV and his co-conspirators also deleted records from accounts used in their operations targeting state boards of elections and similar election-related entities.

75. In or around October 2016, KOVALEV and his co-conspirators further targeted state and county offices responsible for administering the 2016 U.S. elections. For example, on or about October 28, 2016, KOVALEV and his co-conspirators visited the websites of certain counties in Georgia, Iowa, and Florida to identify vulnerabilities.

76. In or around November 2016 and prior to the 2016 U.S. presidential election, KOVALEV and his co-conspirators used an email account designed to look like a Vendor 1 email address to send over 100 spearphishing emails to organizations and personnel involved in administering elections in numerous Florida counties. The spearphishing emails contained malware that the Conspirators embedded into Word documents bearing Vendor 1's logo.

Statutory Allegations

77. Between in or around June 2016 and November 2016, in the District of Columbia and

elsewhere, Defendants OSADCHUK and KOVALEV, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit offenses against the United States, namely:

a. To knowingly access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, where the value of the information obtained exceeded $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B); and

b. To knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, and where the offense did cause and, if completed, would have caused, loss aggregating $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

78. In furtherance of the Conspiracy and to effect its illegal objects, OSADCHUK, KOVALEV, and their co-conspirators committed the overt acts set forth in paragraphs 67 through 69 and 71 through 76, which are re-alleged and incorporated by reference as if fully set forth herein.

All in violation of Title 18, United States Code, Section 371.

FORFEITURE ALLEGATION

79. Pursuant to Federal Rule of Criminal Procedure 32.2, notice is hereby given to Defendants that the United States will seek forfeiture as part of any sentence in the event of Defendants' convictions under Counts One, Ten, and Eleven of this Indictment. Pursuant to Title 18, United

States Code, Sections 982(a)(2) and 1030(i), upon conviction of the offenses charged in Counts One and Eleven, Defendants NETYKSHO, ANTONOV, BADIN, YERMAKOV, LUKASHEV, MORGACHEV, KOZACHEK, YERSHOV, MALYSHEV, OSADCHUK, POTEMKIN, and KOVALEV shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds obtained directly or indirectly as a result of such violation, and any personal property that was used or intended to be used to commit or to facilitate the commission of such offense. Pursuant to Title 18, United States Code, Section 982(a)(1), upon conviction of the offense charged in Count Ten, Defendants NETYKSHO, ANTONOV, BADIN, YERMAKOV, LUKASHEV, MORGACHEV, KOZACHEK, YERSHOV, MALYSHEV, OSADCHUK, and POTEMKIN shall forfeit to the United States any property, real or personal, involved in such offense, and any property traceable to such property. Notice is further given that, upon conviction, the United States intends to seek a judgment against each Defendant for a sum of money representing the property described in this paragraph, as applicable to each Defendant (to be offset by the forfeiture of any specific property).

Substitute Assets

80. If any of the property described above as being subject to forfeiture, as a result of any act or omission of any Defendant --

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property that cannot be subdivided without difficulty;

it is the intent of the United States of America, pursuant to Title 18, United States Code, Section

982(b) and Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853, to seek forfeiture of any other property of said Defendant.

Pursuant to 18 U.S.C. §§ 982 and 1030(i); 28 U.S.C. § 2461(c).

Robert S. Mueller, III
Special Counsel
U.S. Department of Justice

A TRUE BILL:

_____
Foreperson

Date: July 13, 2018

them to PP [redacted] account that they controlled; from there, the copies were moved to GRU-controlled computers. The GRU stole approximately 300 gigabytes of data from the DNC cloud-based account.[185]

2. Intrusions Targeting the Administration of U.S. Elections

In addition to targeting individuals involved in the Clinton Campaign, GRU officers also targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities.[186] The GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations.[187] The GRU continued to target these victims through the elections in November 2016. While the investigation identified evidence that the GRU targeted these individuals and entities, the Office did not investigate further. The Office did not, for instance, obtain or examine servers or other relevant items belonging to these victims. The Office understands that the FBI, the U.S. Department of Homeland Security, and the states have separately investigated that activity.

By at least the summer of 2016, GRU officers sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities. GRU officers, for example, targeted state and local databases of registered voters using a technique known as "SQL injection," by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents).[188] In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters,[189] and extracted data related to thousands of U.S. voters before the malicious activity was identified.[190]

GRU officers Investigative Technique scanned state and local websites for vulnerabilities. For example, over a two-day period in July 2016, GRU officers [redacted] Investigative Technique for vulnerabilities on websites of more than two dozen states. Investigative Technique [redacted]

[185] *Netyksho* Indictment ¶ 34; *see also* SM-2589105-HACK, serial 29 Investigative Technique [redacted].

[186] *Netyksho* Indictment ¶ 69.

[187] *Netyksho* Indictment ¶ 69; Investigative Technique [redacted]

[188] Investigative Technique [redacted]

[189] Investigative Technique [redacted]

[190] Investigative Technique [redacted]

Investigative Technique

Similar IT for vulnerabilities continued through the election.

Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of PP , a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election.[191] The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer.[192] The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so.

D. Trump Campaign and the Dissemination of Hacked Materials

The Trump Campaign showed interest in WikiLeaks's releases of hacked materials throughout the summer and fall of 2016. Harm to Ongoing Matter

1. HOM

a. Background

Harm to Ongoing Matter

[191] *Netyksho* Indictment ¶ 76; Investigative Technique

[192] Investigative Technique

APPENDIX A

No. COA P17-828 TENTH DISTRICT

****

NORTH CAROLINA COURT OF APPEALS

****

VR SYSTEMS, INC. Petitioner-Appellee, v. NORTH CAROLINA STATE BOARD OF ELECTIONS & ETHICS ENFORCEMENT, Respondent-Appellant.	)	From Wake County 17 CVS 13394

****

PETITIONER-APPELLEE'S BENJAMIN MARTIN AFFIDAVIT

****

Benjamin Martin, after being duly sworn, says as follows:

1. I am over 18 years of age, legally competent to give this declaration and have personal knowledge of the facts set forth in it, except such matters as are stated on information and belief, and as to those matters I believe them to be true.
2. I am the Chief Operating Officer of VR Systems, Inc. ("VR Systems"), a corporation authorized to do business in North Carolina.
3. VR Systems owns a proprietary electronic voter identification and polling place automation system known as the EViD electronic pollbook ("EViD"). EViD verifies a voter's eligibility

to vote using voter registration information from the North Carolina State Election Information Management System ("SEIMS") and records that the voter has checked in to vote.

4. I have reviewed the affidavit of Kimberly Westbrook Strach ("Strach Affidavit"), Executive Director for the North Carolina State Board of Elections and Ethics Enforcement ("State Board")[1], attached to Respondent-Appellant's Corrected Verified Petition for Writ of Supersedeas, and for Writ of Certiorari ("Writ") as Exhibit 5.
5. Contrary to assertions in the Strach Affidavit ¶35 that use of EViD e-pollbook version 17.4.21.326 in North Carolina "presents a substantial risk of disruption," EViD[2] e-pollbook was used during the 2017 election cycle in several North Carolina counties without any disruption, problem, or incident.
6. In the September 2017 municipal elections, Mecklenburg County utilized EViD with standard use (companion to paper poll book), with the exception they did not import voter history into SEIMS. Cleveland County used EViD in a voter look up function while processing Provisional Voters and Address and Name changes on the EViD, did not import voter history into SEIMS.
7. During October 2017 municipal elections, Mecklenburg County once again used EViD in standard use, with the same exception as September use. Nash County used EViD in a voter look up function only.
8. In the November 2017 municipal elections, Mecklenburg County fully utilized EViD (companion to paper poll book) including importing voter history into SEIMS, without

[1] As Respondent-Appellant notes, "Session Law 2017-06 consolidated the State Board of Elections and State Ethics Commission, among other things. Aspects of the legislation remain subject to litigation. For clarity, references to the "State Board" may include either the consolidated agency or the earlier State Board of Elections."

[2] All subsequent EViD references in ¶¶ 5 – 8, mean EViD e-pollbook version 17.4.21.326.

disruption, problem, or incident. Cleveland County looked up voters while processing Provisional Voters and Address and Name changes on EViD, with the history contained on EViD imported into SEIMS. Gaston, Nash, and Rowan Counties used EViD to look up voters.

9. The Strach Affidavit seems to contain factual errors or misstatements concerning Petitioner-Appellee, VR Systems.

10. The Strach Affidavit ¶ 10 states "In 2016, however, I became concerned that the EViD product was not appropriately receiving state voter data. Additional concerns surfaced after the March Primary, when a coding problem with EViD incorrectly reported that thousands of voters had made use of the so-called "reasonable impediment" exception to the photo identification requirement."

11. The state voter data VR Systems uses has not changed since certification and only uses data the State Board provides. The "coding problem" refers to errors caused directly as a result of the only third-party certified e-pollbook provider (VR Systems) not being notified of substantial coding changes by the State Board to the XML schema for the third-party export to SEIMS. The resolution process to the State Board created problem is documented at Petitioner-Appellee's Verified Petition for a Contested Case Hearing (Respondent-Appellant's Writ, Exhibit 1, Appendix 64 – 68).

12. The Strach Affidavit ¶ 18 states, "On Election Day 2016, the EViD software used in Durham County appeared to indicate that a number of voters had already cast ballots. My staff and I discussed the problem with VR Systems at or around 7:30 a.m. on Election Day, and a VR Systems employee indicated that the problem affecting five precincts may be more widespread than could immediately be determined. Since the extent of the EViD pollbook problems was

unknown … because EViD wrongly indicated the voters had already participated in that election."

13. Contrary to Strach's Affidavit ¶ 18, the EViD software did not indicate a number of voters had already cast ballots on Election Day, November 4, 2106. In one (1) Durham County precinct there was an issue with three (3) voters. Upon information and belief, Ms. Strach did not talk with anyone at VR Systems during the Durham incident. VR Systems only spoke with Veronica Degraffenreid at the State Board, and at no time was there an indication of a potential problem affecting more than five (5) Durham County precincts, or indications that a potential problem might become more widespread than could be immediately determined. A third-party forensic investigative firm, Protus3, hired by Durham County after the election, to identify possible flaws with EViD during the 2016 election determined "…the EViD application did not fail during the election. It appears that certain steps were not taken to verify all laptops were properly prepared for the November election." Durham County election board workers handled laptop preparation, not VR Systems. (Respondent-Appellant's Writ, Exhibit 1, Appendix 208 – 219)
14. The NSA foreign "hacking" attempt referenced by Strach Affidavit ¶¶ 27 – 29, did not indicate an attempted hacking of VR Systems or EViD e-pollbook version 17.4.21.326 software. (attached as Exhibit 1). There was an attempted email spear-phishing exercise. VR Systems initiated an immediate investigation and found no breach of VR Systems or EViD software. I provided information on the incident to Ms. Strach with an offer to discuss any questions she might have. (Exhibit 2)
15. No attempt was made by Ms. Strach to discuss the incident with any member of VR Systems. According to State Board documents, an investigation was conducted and all North Carolina county clients of VR Systems emails accounts were searched for evidence of spear-phishing.

According to the State Board no evidence of such attempts was found. (Respondent-Appellant's Writ, Exhibit 1, Appendix 195 – 197 – State Board Press Release)

16. Attempts to utilize VR Systems fake emails to hack North Carolina county board of elections had no impact or effect on the EViD e-pollbook software system. Similarly, a successful hack of the State Board's website on June 25 and 27, 2017 (Exhibit 3), had no impact or effect on the State Board's SEIMS software system, Strach Affidavit ¶ 31.

VERIFICATION

BENJAMIN MARTIN, first being duly sworn, deposes and says that he is Chief Operating Officer of VR Systems, Inc., that he has read the foregoing Affidavit and that the facts stated therein are true of his personal knowledge, except such matters as are stated on information and belief, and as to those matters he believes them to be true, and the Exhibits are correct and true copies.

Duly sworn and subscribed to this 20th day of November 2017 in Tallahassee, Florida.

VR SYSTEMS, INC.

By: Benjamin E Martin
Benjamin Martin, Chief Operating Officer

Seal-Stamp

KENDRA WARD
Commission # FF 958163
Expires February 8, 2020
Bonded Thru Troy Fain Insurance 800-385-7019

FLORIDA, Leon COUNTY.

I, a Notary Public of the County and State aforesaid, certify that Benjamin Martin personally appeared before me this day and being duly sworn, acknowledged that he is Chief Operating Officer of VR Systems, Inc., and that he, as Chief Operating Officer, being authorized to do so, executed the foregoing on behalf of the corporation.

Witness my hand and official stamp or seal, this 20th day of November, 2017.

Kendra L Ward
Notary Public

Kendra Ward
Printed Name of Notary Public

Use Blue Ink

My Commission expires: 2-8-2020

EXHIBIT 1

[redacted] DIRNSA [redacted]

National Security Agency

Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department which originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

(U//FOUO) CYBERSECURITY INFORMATION: (U//FOUO) The unclassified data in this report is protected from public disclosure by Federal Law. This report includes sensitive technical information related to computer network operations that could be used against U.S. Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, email addresses, or user names identified in this report is strictly prohibited. Information identified as UNCLASSIFIED//FOR OFFICIAL USE ONLY may be shared for cybersecurity purposes at the UNCLASSIFIED level once it is disassociated from NSA/CSS. Consult the originator prior to release of this information to any foreign government outside of the original recipients.

SUMMARY (U)

(TS//SI//OC/REL TO USA, FVEY/FISA) Russian General Staff Main Intelligence Directorate actors [redacted] executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that became available in April 2017. The actors likely used data obtained from that operation to create a new email account and launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations. The spear-phishing emails contained a Microsoft Word document trojanized with a Visual Basic script which, when opened, would spawn a PowerShell instance [redacted]

Declassify On: 20420505

and beacon out to malicious infrastructure. In October 2016, the actors also created a new email address that was potentially used to offer election-related products and services, presumably to U.S.-based targets. Lastly, the actors sent test emails to two non-existent accounts ostensibly associated with absentee balloting, presumably with the purpose of creating those accounts to mimic legitimate services.

Campaign Against U.S. Company 1 and Voter Registration-Themed Phishing of U.S. Local Government Officials (S//SI//REL TO USA, FVEY/FISA)

Russian Cyber Threat Actors Target U.S. Company 1 (S//REL TO USA, FVEY/FISA)

(TS//SI//OC/REL TO USA, FVEY/FISA) Cyber threat actors [redacted] executed a spear-phishing campaign from the email address noreplyautomaticservice@gmail.com on 24 August 2016 targeting victims that included employees of U.S. Company 1, according to information that became available in April 2017.[1] This campaign appeared to be designed to obtain the end users' email credentials by enticing the victims to click on an embedded link within a spoofed Google Alert email, which would redirect the user to the malicious domain [redacted].[2] The following potential victims were identified:

- U.S. email address 1 associated with U.S. Company 1,
- U.S. email address 2 associated with U.S. Company 1,
- U.S. email address 3 associated with U.S. Company 1,
- U.S. email address 4 associated with U.S. Company 1,
- U.S. email address 5 associated with U.S. Company 1,
- U.S. email address 6 associated with U.S. Company 1, and
- U.S. email address 7 associated with U.S. Company 1.

(TS//SI//OC/REL TO USA, FVEY/FISA) Three of the malicious emails were rejected by the email server with the response message that the victim addresses did not exist. The three rejected email addresses were U.S. email address 1 to 3 associated with U.S. Company 1.

---

1. (TS//SI//OC/REL TO USA, FVEY/FISA) *The GRU* [redacted] *is also rendered as military unit* [redacted]
2. (TS//SI//OC/REL TO USA, FVEY/FISA) *For additional information on* [redacted] *and its cyber espionage mandate, specifically directed at U.S. and foreign elections, see* [redacted]

(TS//SI//OC/REL TO USA, FVEY) COMMENT: The [redacted] actors were probably trying to obtain information associated with election-related hardware and software applications. It is unknown whether the aforementioned spear-phishing deployment successfully compromised all the intended victims, and what potential data from the victim could have been exfiltrated. However, based upon subsequent targeting, it was likely that at least one account was compromised.

Cyber Threat Actors Create Spoofed Account and Voter Registration-Themed Targeting of Local Government Officials (TS//SI//OC/REL TO USA, FVEY/FISA)

(TS//SI//OC/REL TO USA, FVEY/FISA) The [redacted] cyber threat actors created a new operational email account vr.elections@gmail.com with the username "U.S. Company 1" on 27 October 2016. (COMMENT: It is likely that the cyber threat actors created this email address to appear as if they were an employee of U.S. Company 1.) The cyber threat actors had in the email account two trojanized Microsoft Word documents with the titles "New_EViD_User_Guides.docm" and "NEW_Staging_Checklist_AIO_Style_EViD.docm". Both of these documents had identical content and hash values, and contained the same malicious Visual Basic script. The body of the trojanized documents contained detailed instructions on how to configure EViD software on Microsoft Windows machines. According to EViD's FAQ website (UNCLASSIFIED), EViD software allows poll workers to quickly check a voter's registration status, name and address. (END OF COLLATERAL)

(TS//SI//OC/REL TO USA, FVEY/FISA) Subsequently, the cyber threat actors used the vr.elections@gmail.com account to contact U.S. email addresses 1 to 122 associated with named local government organizations. (COMMENT: It possible that the targeted email addresses were obtained from the previously compromised account(s) of U.S. Company 1.) The "NEW_Staging_Checklist_AIO_Style_EViD" document was last modified on 31 October 2016 and the "New_EViD_User_Guides" document was last modified on 1 November 2016. (COMMENT: This likely indicates that the spear-phishing campaign occurred either on 31 October or 1 November , although th e exact date of the spear-phishing campaign was not confirmed.)

(TS//SI//REL TO USA, FVEY) COMMENT: Given the content of the malicious email it was likely that the threat actor was targeting officials involved in the management of voter registration systems. It is unknown whether the aforementioned spear-phishing deployment successfully compromised the intended victims, and what potential data could have been accessed by the cyber actor.

Technical Analysis of the Trojanized Documents (U//FOUO)

(TS//SI//OC/REL TO USA, FVEY/FISA) Both trojanized Microsoft Word documents contained a malicious Visual Basic script that spawns PowerShell and uses it to execute a series of commands to retrieve and then

run an unknown payload from malicious infrastructure located at a U.S. IP address on port 8080, probably running Microsoft-IIS/7.5 Server. (COMMENT: The unknown payload very likely installs a second payload which can then be used to establish persistent access or survey the victim for items of interest to the threat actors.) The request used a user-agent string of "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko". Lastly, the malicious Microsoft Word documents hashed to the following values:

- MD5 Hash:5617e7ffa923de3a3dc9822c3b01a1fd,
- SHA-1 Hash:602aa899a6fadeb6f461112f3c51439a36ccba40, and
- SHA-256 Hash:f48c9929f2de895425bdae2d5b232a726d66b9b2827d1a9ffc75d1ea37a7cf6c.

Operational Accounts Spoofing Legitimate Elections-Related Services (S//REL TO USA, FVEY)

Spoofing Email Address Associated With U.S. Company 2 (U//FOUO)

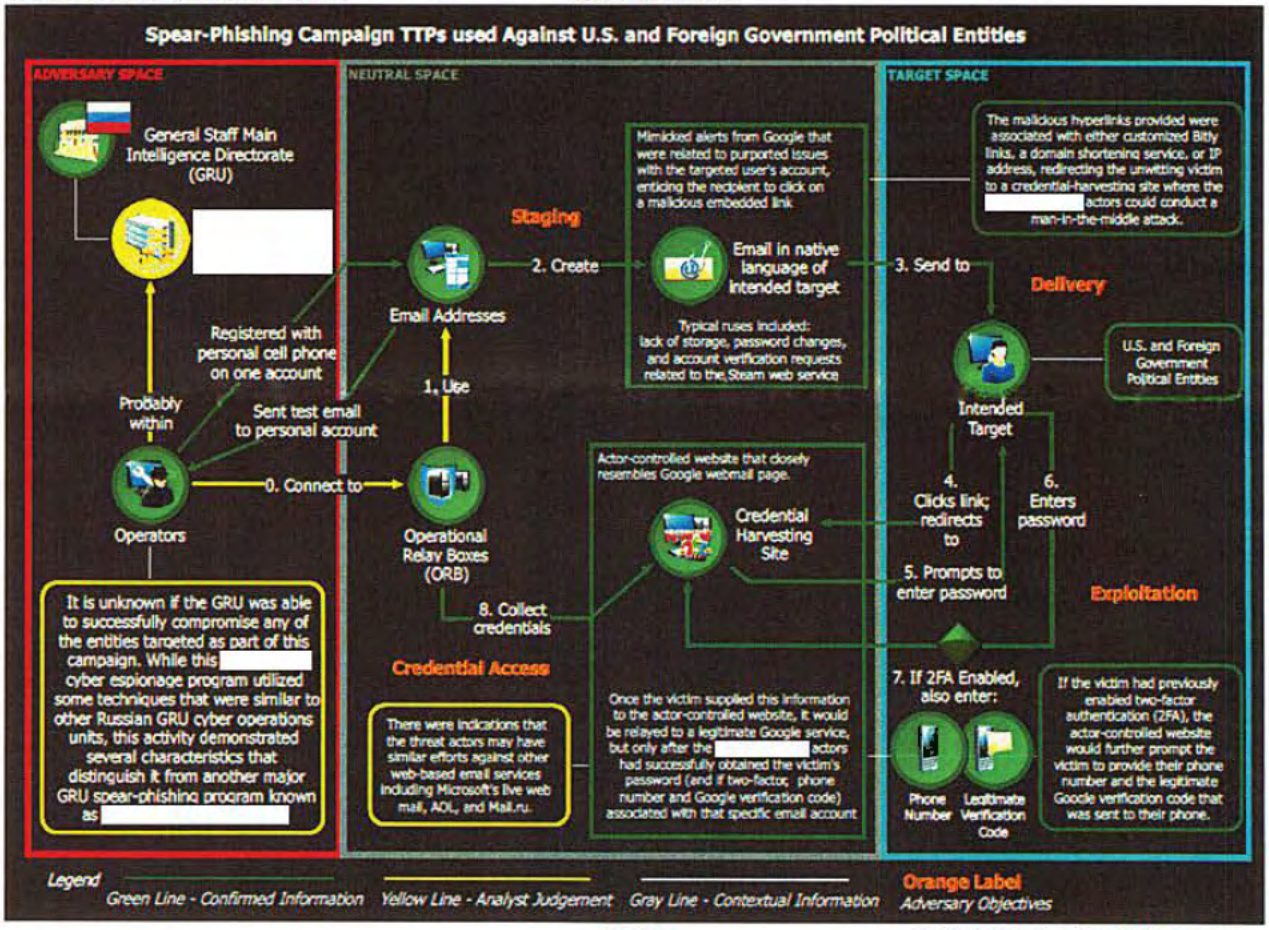
(TS//SI//OC/REL TO USA, FVEY/FISA) In parallel to the aforementioned campaign, the [redacted] cyber threat actors created another new operational email account elevationsystem@outlook.com on 19 October 2016. They then used this email address to send a test message to another known [redacted] operational email account. In that test email, which was written in English, the threat actors spoofed U.S. Company 2, and offered election-related products and services. All emails associated with this account were later deleted, and it was unknown if there was any targeting using this email account. (COMMENT: G iven that the email body was written in English and prepared less than 1 month before the 2016 U.S. Presidential election, it was likely intended for U.S.-based targets.)

Spoofing Absentee Ballot Email Addresses (U//FOUO)

(TS//SI//OC/REL TO USA, FVEY/FISA) Additionally, the [redacted] cyber threat actors sent what appeared to be a test email to two other accounts, requestabsentee@americansamoaelectionoffice.org and r-questabsentee@americansamoaelectionoffice.org. In both cases the actors received a response from the mail server on 18 October stating that the message failed to send, indicating that the two accounts did not exist.

> (TS//SI//REL TO USA, FVEY) COMMENT: Given that the test email did not contain any malicious links or attachments, it appeared the threat actors' intent was to create the email accounts rather than compromise them, presumably with the purpose of mimicking a legitimate absentee ballot-related service provider.

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA [redacted] Spearphishing campaign



TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

EXHIBIT
2

From: **Ben Martin** <bmartin@vrsystems.com>
Date: Fri, Jun 9, 2017 at 8:37 AM
To: kim.strach@ncsbe.gov
Cc: Mindy Perkins <mperkins@vrsystems.com>

Ms Strach,

I know that you are conducting an investigation according to your press release. I wanted to share with you this set of FAQs that we sent to all of our customers in North Carolina yesterday. We developed it to help provide some clear answers to some of the questions and misrepresentation of the facts that have been in the public.

If you or your investigator wish to explore this further please contact me and I will make information and resources available to you.

Respectfully,
Ben Martin

--

VR elections
100% Employee Owned

Ben Martin, CERV
Chief Operating Officer

2840 Remington Green Circle
Tallahassee FL 32308
(w)850-668-2838/ (f)850-668-3193

From: **Strach, Kim** <kim.strach@ncsbe.gov>
Date: Fri, Jun 9, 2017 at 9:18 AM
To: Ben Martin <bmartin@vrsystems.com>
Cc: Mindy Perkins <mperkins@vrsystems.com>

Ben,

Thanks so much for the information. We'll be in touch if we have any questions.

Best regards,

Kim

Kimberly Westbrook Strach

Executive Director

North Carolina State Board of Elections and Ethics Enforcement

919-715-2334

From: Ben Martin [mailto:bmartin@vrsystems.com]
Sent: Friday, June 09, 2017 8:38 AM
To: Strach, Kim <kim.strach@ncsbe.gov>
Cc: Mindy Perkins <mperkins@vrsystems.com>
Subject: FAQs

Ms Strach,

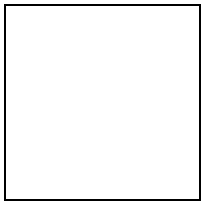
I know that you are conducting an investigation according to your press release. I wanted to share with you this set of FAQs that we sent to all of our customers in North Carolina yesterday. We developed it to help provide some clear answers to some of the questions and misrepresentation of the facts that have been in the public.

If you or your investigator wish to explore this further please contact me and I will make information and resources available to you.

Respectfully,

Ben Martin

--



100%
Employee Owned

Ben Martin, CERV
Chief Operating Officer

2840 Remington Green Circle
Tallahassee FL 32308
(w)850-668-2838/ (f)850-668-3193

Frequently Asked Questions
Recent Cybersecurity Reports
June 8, 2017

What do I need to know about the October spear-phishing emails?

Recent reports indicate that cyber actors impersonated VR Systems and other elections companies. Cyber actors sent an email from a fake account to election officials in an unknown number of districts just days before the 2016 general election. The fraudulent email asked recipients to open an attachment, which would then infect their computer, providing a gateway for more mischief.

Please note:

- We have heard of **no accounts of election officials** who opened the attachment. Most election officials have security systems in place that would have flagged the email before it even reached the intended recipient.

- Neither the EViD pollbook, nor any other VR Systems product, were targets of this attack.

What did the cyber actors hope to achieve? What weakness was the email trying to exploit?

The goal was to trick recipients into opening an attachment that contains malware. The malware would enter that recipient's network. We have no evidence that any customer (or any non-customer) opened the spear-phishing email or that any malware was downloaded.

How do I know if my office received the spear-phishing email?

Because the spear-phishing email did not originate from VR Systems, we do not know how many jurisdictions were potentially impacted. Many election offices report that they never received the email or it was caught by their spam filters before it could reach recipients.

It is our understanding that all jurisdictions, including VR Systems customers, have been notified by law enforcement agencies if they were a target of this spear-phishing attack.

What red flags were raised in the spear-phishing email?

1) It would be highly unusual for VR Systems to issue a communication suggesting a change of software inside a live election timeframe. VR Systems would never make any change to software during a live election unless under unusual circumstances and only after conferring with our customers and the State.

2) Grammatical mistakes and unusual spelling should alert a recipient to a concern.

3) The domain name was incorrect.

What steps should I take to protect my systems?

1) Consult with IT professionals to ensure that all systems are patched and regularly updated.

2) Train all office staff in cybersecurity safety.

3) Engage the services of security experts who can audit your systems and ensure the integrity of your data.

4) If you see something unusual, say something. VR Systems is available by phone any time and any hour, every day of the year and can respond immediately to a concern.

5) Secure all log-in credentials. No staff member from VR Systems will ask you for your log-in and password.

6) Participate in professional cyber-alliances to learn best practices.

For more information, please consult the Domestic Security Alliance Council (https://www.dsac.gov/topics/cyber-resources) which includes a number of links to government security agencies focused on cybercrime prevention.

What is needed to protect all systems?

Cybersecurity is a dynamic environment and it is important to remain vigilant and alert about the latest developments and tools. At VR Systems, we will do our best to communicate protocols and measures to assist our customers in remaining up to date with regard to security.

- Phishing email scams are common. We expect the security environment to become more complex in the coming years and strongly encourage election officials to stay on top of the latest security tools and protocols.

- A combination of technology and well-trained users are needed to prevent security issues.

VR Systems maintains a close relationship and is working in concert with security and law enforcement agencies to maintain robust and current security systems.

Was VR Systems' email hacked in August?

No. In August, a small number of phishing emails were sent to VR Systems. These emails were captured by our security protocols and the threat was neutralized. No VR Systems employee's email was compromised. This prevented the cyber actors from accessing a genuine VR Systems email account.

As such, the cyber actors, as part of their late October spear-phishing attack, resorted to creating a fake account to use in that spear-phishing campaign.

###

EXHIBIT
3

From: Burris, Marc [mailto:marc.burris@ncsbe.gov]
Sent: Tuesday, June 27, 2017 6:35 PM
To: SBOE_Grp - Directors.BOE
Cc: Strach, Kim; Lawson, Joshua; Degraffenreid, Veronica; Strange, Amy; Fleming, Joan; Gannon, Patrick
Subject: ISAC Threat - Election and Government Websites at Risk

Directors,

There has been a security alert issued for all election related websites. There are groups exploiting vulnerabilities in websites being hosted or created with DotNetNuke (DNN.) Please contact your county IT department or vendor hosting your election site to make them aware of the threat. While the groups are exploiting known vulnerabilities in DNN, they may also be poised to exploit other content management systems (CMS) like Drupal.

Today I was alerted by the FBI that our NCSBE election website might have been compromised. Upon initial review we did identify those groups successfully inserted unauthorized index.html files into our public website. Our systems quickly identified the corrupt file and replaced it with the original file, which is why you probably are not seeing this in the news. Upon review of our logs this happened on 6/25/2017 and again today around 2:30pm.

For security reasons, our state NCSBE website is currently isolated physically by itself in the cloud with no access to any other election system. That means that even if there was a full breach of our site, all that would have been compromised is our public facing website. While composing this email, I have just finished applying a new DNN patch to deal with this vulnerability, so we should not see this issue in the future.

The lesson here for us is that no matter how strong of a front door you have, you need to make sure you have other means to deal with intruders. For your piece of mind we have the same procedures wrapped around your county SEIMS servers so in the event intruders penetrate your county network, we have an automated means to detect and terminate unauthorized connections.

Feel free to contact me if you have any questions.

The following is the ISAC alert:

TLP: GREEN
MS-ISAC CYBER ALERT
TO: All MS-ISAC Members and IIC Partners
DATE ISSUED: June 26, 2017

SUBJECT: Mass Defacement Campaign Affecting SLTT Government Websites

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is aware of a mass website defacement campaign by the defacement group TeaM System Dz affecting state, local, tribal, and territorial (SLTT) government entities. As of June 26, 2017, 26 webpages belonging to eight SLTT governments have been affected by this mass defacement campaign. In addition to SLTT government websites, TeaM System Dz also compromised non-SLTT government websites running similar software during the same time period, suggesting the campaign is opportunistic in nature.

Based on information received from affected entities and additional MS-ISAC research, it is likely TeaM System Dz exploited file upload vulnerabilities in several third-party modules/plugins for the DotNetNuke content management system (CMS). The defacements added a new index.html defacement page or defaced the existing homepage of the website with anti-government/anti-U.S. messaging.

As of June 26, 2017, known affected third-party modules include:

- Mandeeps
  - Live Campaign
  - Live Content
  - Live Forms
  - Live Helpdesk
  - Live Utilities
- EasyDNN

TeaM System Dz is one of several known groups of cyber threat actors who sympathize with the terrorist organization ISIS. The MS-ISAC first observed this actor compromising SLTT government websites in early November 2014. Analysis of prior defacements indicates that the group engages in primarily opportunistic defacements and posts defacement messages that support ISIS. It is unlikely the group targets SLTT governments strategically due to their strong ties with ISIS and defacement messages that do not always relate to SLTT governments. The group often exploits CMS vulnerabilities, and previously used WordPress' multi-site mode to pivot to other connected sites. TeaM System Dz is not known for conducting cyber activity other than web defacements.

Recommendations

- Update DotNetNuke to the most current version 9.1.0.
- Ensure that web servers, CMSs, and related plugins and themes are up-to-date and patched regularly.
- Ensure that any unused plugins and themes, or software which does not meet a business need, are uninstalled from production web servers.
- Regularly assess the security of web servers using a web application vulnerability scanner and remediate any identified issues.
- Consider implementing a web application firewall and/or file integrity monitoring solution to identify and prevent attempted compromises.
- Ensure web server administrative functions require authentication, and secure accounts by replacing default passwords with a strong, complex password containing at least ten upper and lowercase letters, numbers, and special characters. Consider implementing two-factor

authentication, where available.

· Implement logging and monitor logs to ensure that only authorized users are accessing the web server and identify any unauthorized modifications or unusual traffic. Store logs for a minimum of 90 days.

Marc Burris, CGCIO
Chief Information Officer

NC State Board of Elections and Ethics

Ph: (919) 715 - 1673

MARC.BURRIS@NCSBE.GOV