

B139

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

Criminal No. 20-316

SCANNED

YURIY SERGEYEVICH ANDRIENKO,
SERGEY VLADIMIROVICH DETISTOV,
PAVEL VALERYEVICH FROLOV,
ANATOLIY SERGEYEVICH KOVALEV,
ARTEM VALERYEVICH OCHICHENKO, and
PETR NIKOLAYEVICH PLISKIN,

18 U.S.C. §§ 371, 1030(a)(2)(C),
1030(a)(5)(A), 3559(g)(1)
(Conspiracy)
18 U.S.C. § 1349
(Conspiracy to Commit Wire Fraud)
18 U.S.C. § 1343 (Wire Fraud)
18 U.S.C. § 1030(a)(5)(A) and
1030(c)(4)(B) (Damage to Computers)
18 U.S.C. § 1028A (Aggravated Identity
Theft)
18 U.S.C. § 2 (Aiding and Abetting)

Defendants.

FILED

OCT 15 2020

[UNDER SEAL]

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

INDICTMENT

COUNT ONE

(Conspiracy to Commit an Offense Against the United States)

The grand jury charges:

1. At all times relevant to the indictment, from at least in and around November 2015 through in and around October 2019, the Russian Federation (“Russia”) operated a military intelligence agency called the Main Intelligence Directorate of the General Staff of the Armed Forces (“GRU”). The GRU was headquartered in Moscow, Russia, and was comprised of multiple units, including Military Unit 74455, which was also known within the GRU as the “Main Center for Special Technologies” (also known as “GTsST”) and by cybersecurity researchers as Sandworm Team, Telebots, Voodoo Bear, and Iron Viking. Military Unit 74455 was primarily

located at 22 Kirova Street, Khimki, Moscow, Russia, a building referred to within the GRU as “the Tower.”

2. Defendants YURIY SERGEYEVICH ANDRIENKO (Юрий Сергеевич Андриенко), SERGEY VLADIMIROVICH DETISTOV (Сергей Владимирович Детистов), PAVEL VALERYEVICH FROLOV (Павел Валерьевич Фролов), ANATOLIY SERGEYEVICH KOVALEV (Анатолий Сергеевич Ковалев), ARTEM VALERYEVICH OCHICHENKO (Артем Валерьевич Очиченко), and PETR NIKOLAYEVICH PLISKIN (Петр Николаевич Плискин) were GRU officers working for Military Unit 74455 who knowingly and intentionally conspired with each other and with persons known and unknown to the grand jury (collectively, the “Conspirators”) to deploy destructive malware and take other disruptive actions, for the strategic benefit of Russia, through unauthorized access to victim computers. This included cyber-enabled malicious actions aimed at supporting broader Russian government efforts—regardless of the consequences to innocent parties and critical infrastructure worldwide—to undermine, retaliate against, or otherwise destabilize: (1) Ukraine; (2) the country of Georgia; (3) France’s elections; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent on foreign soil; and (5) the 2018 Winter Olympics after a Russian government-sponsored doping effort led to Russian athletes being unable to participate under the Russian flag.

THE VICTIMS

3. Among the victims targeted by Military Unit 74455 were thousands of U.S. and international corporations, organizations, and political campaigns and parties; foreign governments; entities and corporations associated with the 2018 Winter Olympic Games; and their respective employees. The victims included:

- a. Ukraine, through the Conspirators' deployment in and around December 2015 and December 2016 of destructive "BlackEnergy," "KillDisk," and "Industroyer" malware against companies supporting Ukraine's electric power grid and against Ukraine's Ministry of Finance and State Treasury Service;
- b. France, through spearphishing campaigns in and around April and May 2017 targeting local government entities, political parties, and campaigns, including now-French President Emmanuel Macron's "La République En Marche!" political party in connection with Macron's 2017 presidential campaign;
- c. Hundreds of worldwide victims of the "NotPetya" malware attacks in and around June 2017, including: (1) civilian critical infrastructure, such as the Heritage Valley Health System, located in Sewickley, Pennsylvania, and Beaver, Pennsylvania, in the Western District of Pennsylvania, which had approximately 80 affected medical facilities; (2) a FedEx Corporation subsidiary, TNT Express B.V., which was one of the world's largest express delivery companies; and (3) a large U.S. pharmaceutical manufacturer, which together had nearly \$1 billion in losses resulting from the attacks;
- d. International victims associated with the 2018 Winter Olympic Games, including: (1) Olympic partners and athletes, Republic of Korea (also known as South Korea) government agencies, and the International Olympic Committee ("IOC"), which the Conspirators targeted through

spearphishing campaigns from in and around December 2017 until in and around February 2018; (2) South Korean nationals and international visitors to South Korea, whom the Conspirators targeted with malicious mobile applications in and around December 2017 and January 2018; and (3) the 2018 Winter Olympic Games more generally, through the deployment of destructive “Olympic Destroyer” malware against computer systems used by the Olympic Games’ information technology vendor and the PyeongChang Organizing Committee for the 2018 Olympic & Paralympic Winter Games (“PyeongChang Organizing Committee”) in and around February 2018;

- e. International and government organizations investigating the poisoning of a former GRU officer and his daughter in the United Kingdom, through, among other conduct, a spearphishing campaign in and around April 2018 targeting the Organisation for the Prohibition of Chemical Weapons (“OPCW”) and the United Kingdom’s Defence Science and Technology Laboratory (“DSTL”); and
- f. The country of Georgia and Georgian non-government organizations and private companies, including through a spearphishing campaign in and around January 2018 targeting a Georgian media outlet and a cyber attack in and around October 2019 that defaced approximately 15,000 websites and disrupted service to some of these websites.

THE DEFENDANTS

4. Defendant YURIY SERGEYEVICH ANDRIENKO was a Russian military intelligence officer assigned to Military Unit 74455. ANDRIENKO, together with PAVEL VALERYEVICH FROLOV, SERGEY VLADIMIROVICH DETISTOV, and PETR NIKOLAYEVICH PLISKIN, developed components of the NotPetya malware. ANDRIENKO, together with PLISKIN, also developed components of the Olympic Destroyer malware.

5. Defendant SERGEY VLADIMIROVICH DETISTOV was a Russian military intelligence officer assigned to Military Unit 74455. During his tenure with the unit, DETISTOV held the position of captain. DETISTOV developed components of the NotPetya malware and prepared infrastructure for a spearphishing campaign targeting the 2018 Winter Olympics.

6. Defendant PAVEL VALERYEVICH FROLOV was a Russian military intelligence officer assigned to Military Unit 74455. FROLOV developed components of the NotPetya malware and the malware that the Conspirators used against Ukraine's Ministry of Finance and State Treasury Service.

7. Defendant ANATOLIY SERGEYEVICH KOVALEV was a Russian military intelligence officer assigned to Military Unit 74455. KOVALEV sent spearphishing emails targeting a wide variety of entities and individuals, including those associated with French local government entities, political parties, and campaigns; the 2018 Winter Olympics; the DSTL; and a Georgian media entity. KOVALEV also engaged in spearphishing campaigns for apparent personal profit, including campaigns targeting large Russian real estate companies, auto dealers, and cryptocurrency miners, as well as cryptocurrency exchanges located outside of Russia.

KOVALEV is a charged defendant in federal indictment number 18-CR-215 in the District of Columbia.

8. Defendant ARTEM VALERYEVICH OCHICHENKO served as a Russian military intelligence officer in Military Unit 74455. OCHICHENKO developed malicious email attachments and sent spearphishing emails containing those attachments to individuals working for the 2018 Winter Olympics' official timekeeping partners and their subsidiaries. OCHICHENKO was also involved in the Conspirators' targeting of the Georgian government and other Georgian entities in 2019.

9. Defendant PETR NIKOLAYEVICH PLISKIN served as a Russian military intelligence officer in Military Unit 74455 from the beginning of the conspiracy until in and around June 2018. During his tenure with the unit, PLISKIN served in a supervisory role as a Development Team Lead/IT manager. PLISKIN developed components of the NotPetya and Olympic Destroyer malware.

(Images of defendants ANDRIENKO, DETISTOV, FROLOV, KOVALEV, OCHICHENKO, and PLISKIN are attached as Exhibit A.)

OBJECT OF THE CONSPIRACY

10. The object of the conspiracy was to deploy destructive malware and take other disruptive actions, for the strategic benefit of Russia, through unauthorized access ("hacking") of victim computers.

MANNER AND MEANS OF THE CONSPIRACY

11. In furtherance of the conspiracy, ANDRIENKO, DETISTOV, FROLOV, KOVALEV, OCHICHENKO, PLISKIN, and others known and unknown to the grand jury

procured, maintained, and utilized servers, email accounts, malicious mobile applications, and related hacking infrastructure to engage in spearphishing campaigns and other network intrusion methods against computers used by the victims. Also in furtherance of the conspiracy, ANDRIENKO, DETISTOV, FROLOV, and PLISKIN developed and deployed destructive malware against victim entities around the world, including in the Western District of Pennsylvania.

12. In order to avoid detection by law enforcement, security researchers, and victims, and to mask their GRU affiliation and location in Russia, the Conspirators used a variety of fictitious names and personas, as well as online infrastructure (including servers, domains, cryptocurrency, email accounts, social media accounts, and other online services) provided by companies in the United States and elsewhere. The Conspirators used this infrastructure for a wide range of conduct in furtherance of the conspiracy, including to: (1) communicate, research, and probe victim computer networks; (2) register malicious websites and domains with names mimicking legitimate ones; (3) send spearphishing emails; (4) store and distribute additional malware; (5) manage malware; (6) transfer stolen data; and (7) negatively influence the public perception of some of the victims. The Conspirators reused some of the same infrastructure to target multiple victim organizations and individuals.

13. To further mask their identities and conduct and to facilitate the purchase and leasing of infrastructure (such as servers and domain names) used in their hacking activity, the Conspirators paid for infrastructure using cryptocurrencies, such as bitcoin, and often leased infrastructure from resellers rather than leasing infrastructure directly from hosting companies.

The Conspirators also used numerous operational accounts in fictitious names to purchase and lease infrastructure.

14. The Conspirators registered domain names and created URLs for use in their hacking activities that were designed to mimic or “spoof” those of legitimate websites that victims were familiar with, including email login pages, online file sharing and storage websites, and password reset pages. Examples include `msrole.com/office_conf` (which mimicked a website belonging to Microsoft) and `jeo.ang.ga` (with respect to which the Conspirators created the subdomain `mafra.go.kr.jeo.ang.ga`, which mimicked a website belonging to the Korean Ministry of Agriculture, Food, and Rural Affairs, 농림축산식품부). The Conspirators used each of these domain names in connection with spearphishing campaigns targeting entities and individuals associated with the 2018 Winter Olympics.

15. The Conspirators typically initiated their hacking activities by researching the victim organizations, including their computer networks and employees. This research provided technical and biographical information that the Conspirators could exploit in subsequent intrusion activities (*e.g.*, spearphishing campaigns).

16. The Conspirators crafted their spearphishing emails to trick unwitting recipients into giving the Conspirators access to their computers or account credentials (*e.g.*, usernames and passwords). The Conspirators crafted these emails to resemble emails from trustworthy senders, such as email providers or colleagues, and encouraged the recipients to click on hyperlinks in the messages. Other spearphishing emails crafted by the Conspirators attached documents containing malware that, when opened and executed by the victims, infected victims’ computers.

17. The Conspirators used malware and hacking tools such as “BlackEnergy,” “Industroyer,” “KillDisk,” “NotPetya,” and “Olympic Destroyer” to hack into victim computers and networks, maintain command and control over such computers and networks, steal network credentials, obtain access to sensitive and private data, and render such computers and networks inoperable. To craft their malware, the Conspirators customized publicly available malware and hacking tools, and, in some instances, purposefully attempted to mimic the malware of other hacking groups—including the Lazarus Group, a state-sponsored hacking team in the Democratic People’s Republic of Korea (which is also known as North Korea)—as part of a “false flag” operation. The Conspirators also created certain malware components from scratch, including components enabling the Conspirators to conduct the destructive portions of their attacks.

18. After hacking into victim computers, the Conspirators performed a variety of functions designed to identify, collect, package, and view targeted data on victims’ computers, including stealing credentials that allowed the Conspirators to move laterally and exponentially throughout victims’ computer networks. The Conspirators also overwrote files and erased data from victim computers.

19. In addition, both during and after operational activity, the Conspirators made efforts to cover their tracks by deleting information from their operational accounts and deleting data on servers they controlled or had compromised.

COMPUTER INTRUSIONS AND OTHER OVERT ACTS

The 2015 and 2016 Attacks Targeting Ukraine’s Electric Power Grid

20. On or about December 23, 2015, the Conspirators hacked into the computer systems belonging to three Ukrainian energy distribution companies, interacted remotely with

control systems in dozens of power distribution substations used by these companies, and successfully disrupted the supply of electricity to more than 225,000 Ukrainian customers.

21. The preparations for this attack commenced in and around late spring 2015, when the Conspirators used spearphishing emails to obtain access into the three energy distribution companies' computer systems and then used destructive malware against the computer systems.

- a. The spearphishing campaign targeted the companies' information technology staff and system administrators using emails attaching malware-laced files.
- b. Once they had obtained access to the victims' computer systems, the Conspirators used a particular variant of malware called "BlackEnergy" to steal user credentials. The Conspirators used the stolen credentials to access the Supervisory Control and Data Acquisition ("SCADA") networks at the Ukrainian energy distribution companies. The Conspirators also used destructive malware called "KillDisk" at the conclusion of the attacks to delete computer event logs and other files and reboot the infected computers. Once rebooted, the infected computers were inoperable.

22. Almost a year later, on or about December 17, 2016, the Conspirators conducted a computer intrusion against a Ukrainian electric transmission company ("Electric Company 1"). Electric Company 1's computer network had been compromised by the Conspirators since in and around April 2016. In furtherance of the attack, the Conspirators used malware—which was later named "Industroyer" by cybersecurity researchers—that was specifically designed to attack power grids by gaining control of electrical substation switches and circuit breakers.

23. The malware included a disk wiper plugin that the Conspirators used to delete Electric Company 1's key system files with certain file extensions (including common file extensions such as .zip and .exe, as well as file extensions specific to the brand of industrial control system used by Electric Company 1), thus rendering Electric Company 1's computer operating systems inoperable. In addition, the Conspirators' deployment of the malware disrupted the supply of electricity to Kiev, Ukraine, for approximately one hour.

The December 2016 Attacks Against Ukraine's
Ministry of Finance and State Treasury Service

24. On or about December 6, 2016, while Ukraine was preparing end-of-year pension payments as well as the following year's budget, the Conspirators deployed destructive malware against Ukraine's Ministry of Finance and State Treasury Service. As a result of the attack, the State Treasury Service's regional subdivisions were disconnected from the State Treasury Service's automated payment system, preventing the execution of approximately 150,000 electronic transactions. In addition, the attack temporarily disabled the Ministry of Finance's information and telecommunication infrastructure.

25. The attack against the State Treasury Service began in and around October 2016 with a spearphishing campaign that targeted the Service's system administrators.

- a. The spearphishing campaign utilized emails containing a malware-laced Microsoft Excel file called "MoF critical IT needs_eng.xls."
- b. The State Treasury Service's computer network was compromised by in and around October 2016 after a system administrator for the Service opened the Microsoft Excel file and enabled macros for the file. Allowing the macros to run resulted in the execution of the malware-laced file

“explorer.exe” on the employee’s computer, which ultimately established unauthorized, covert encrypted communication between the computer and a third-party service used by the Conspirators.

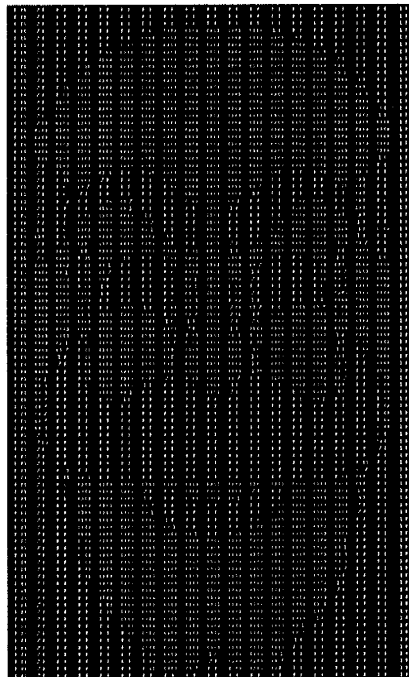
- c. The Conspirators thereafter used a dedicated network connection between the State Treasury Service and Ukraine’s Ministry of Finance to obtain unauthorized access to the Ministry of Finance’s computer network.

26. On or about December 6, 2016, the Conspirators deployed an updated version of the KillDisk malware—which was very similar to the version of the KillDisk malware the Conspirators used in the December 2015 cyber attacks against Ukraine’s electric power grid—to: (1) delete the infected computers’ Windows event logs; (2) delete all of the files that matched a list of file extensions hardcoded into the malware; and (3) overwrite portions of the infected computers’ hard drives, thus rendering the computers inoperable.

- a. Once executed, the KillDisk malware used three different options to invoke different behaviors: (1) an option to set a specific date and time to execute the malware’s destructive mode; (2) an option to specify a desired delay, in minutes, before executing the destructive mode; and (3) an option to specify desired functionality, including the malware’s destructive mode. Once the KillDisk malware verified which options were selected, it prepared the infected computer system for file destruction.
- b. To do this, the KillDisk malware prepared several locations in the computer’s memory for overwriting files by allocating a set area in the computer’s memory. The KillDisk malware filled the first allocated

memory location with zeros and filled the second and third allocated memory locations with the repeated term “mrR0b07” and “fS0cie7y,” respectively, which reference the television show “Mr. Robot.” After the three allocated memory locations were filled with zeros, “mrR0b07,” and “fS0cie7y,” the KillDisk malware obtained a computer system privilege that allowed it to access all available files on the compromised computer system.

- c. FROLOV and other Conspirators designed the KillDisk malware such that the third option could create an art image of the “fsociety” mask from “Mr. Robot.” The KillDisk malware did not store an image of the “fsociety” mask within the malware. Instead, FROLOV designed the malware to draw the image in real time on the infected computer’s screen. The “fsociety” mask was computed from the following bitmap array embedded in the malware:



- d. Once the “fsociety” mask image was drawn in memory, the malware displayed the image on the victim’s computer screen on top of all other graphical windows:



- e. The third option could also enable KillDisk to destroy all files on the infected computer that ended with one of more than 100 different file extensions. To destroy each file on compromised computers, KillDisk: (1) overwrote the entire file with zeros, (2) deleted the file and then recreated it with the same name, and (3) populated the file with the repeating string “mrR0b07” or “fS0cie7y” as described above. To determine which string to populate, KillDisk generated a random number; if the number was odd, “mrR0b07” was written, and if the number was even, “fS0cie7y” was written. After all of the files were destroyed, KillDisk rebooted the compromised computer systems, which were inoperable because the malware had destroyed all of the key system files.

- f. The Conspirators designed KillDisk to attempt to clear the event logs on compromised computers in order to make it more difficult for forensic investigators to obtain digital evidence.

Interference in the 2017 French Elections

27. From on or about April 3, 2017, through on or about May 3, 2017 (during the days leading up to the May 7, 2017, presidential election in France), the Conspirators conducted seven spearphishing campaigns targeting more than 100 individuals who were members of now-President Macron's "La République En Marche!" ("En Marche!") political party, other French politicians and high-profile individuals, and several email addresses associated with local French governments. The topics of these campaigns included public security announcements regarding terrorist attacks, email account lockouts, software updates for voting machines, journalist scoops on political scandals, En Marche! press relationships, and En Marche! internal cybersecurity recommendations.

28. KOVALEV participated in some of these campaigns. For example, on or about April 21, 2017, KOVALEV developed and tested a technique for sending spearphishing emails themed around file sharing through Google Docs. KOVALEV then crafted a malware-laced document entitled "Qui_peut_parler_aux_journalists.docx" (which translates to "Who can talk to journalists") that purported to list nine En Marche! staff members who could talk to journalists about the previous day's terrorist attack on the Champs-Élysées in Paris. Later that day, the Conspirators used an email account that mimicked the name of then-candidate Macron's press secretary to send a Google Docs-themed spearphishing email to approximately 30 En Marche! staff members or advisors, which purported to share this document.

29. From on or about April 12, 2017, until on or about April 26, 2017, a GRU-controlled social media account communicated with various French individuals offering to provide them with internal documents from En Marche! that the user(s) of the account claimed to possess.

30. On or about May 3 and May 5, 2017, unidentified individuals began to leak documents purporting to be from the En Marche! campaign's email accounts.

The NotPetya Malware Attacks

31. On or about June 27, 2017—on the eve of Ukraine's Constitution Day, which commemorates the country's departure from the Soviet Union—the Conspirators executed a series of malware attacks to render inoperable the computer systems used by Ukrainian organizations, including banks, newspapers, and electricity companies. The malware used in the attacks was later named "NotPetya" by cybersecurity researchers. Because the NotPetya malware was designed to spread to connected networks belonging to other victims, the attacks also rendered inoperable computer systems belonging to victims in other countries, including in the United States.

32. In particular, the NotPetya malware compromised computer systems at two hospitals, 60 physician offices, and 18 community satellite facilities belonging to the Heritage Valley Health System ("Heritage Valley"), which, at all times during the conspiracy, was located in Sewickley, Pennsylvania, and Beaver, Pennsylvania, in the Western District of Pennsylvania. All of Heritage Valley's internet traffic was routed through servers located in the Western District of Pennsylvania, and all of the resulting damage and its effects, including those to mission-critical computer systems, impacted Heritage Valley's healthcare professionals and patients in the Western District of Pennsylvania.

33. The Conspirators designed NotPetya to masquerade as ransomware, a type of malware that encrypts and blocks access to a victim’s computer system and/or files until the victim pays a ransom. In particular, the Conspirators designed the NotPetya malware to emulate already-existing ransomware called “Petya.” However, the purported ransomware purpose of NotPetya was a ruse. Unlike Petya—which displayed a ransom note on infected computers demanding money and where, upon payment of the ransom, the computers could be decrypted—the NotPetya malware operated such that, even if victims paid the ransom (\$300 worth of bitcoin), the Conspirators would not be able to decrypt and recover the victims’ computer files.

34. The Conspirators disseminated the NotPetya malware using a popular Ukrainian accounting software called M.E.Doc that was used to facilitate the communication of tax information to the Ukrainian government. The software was periodically updated through an update server (the “Update Server”). The Conspirators commenced the NotPetya attacks on or about June 27, 2017, when they rerouted internet traffic from (1) computers attempting to update the M.E.Doc software via the Update Server to (2) a France-based server controlled by the Conspirators. This France-based server delivered the malware to the victim computers that connected to it.

35. Each organization that conducts business in Ukraine has a unique legal entity identifier called an EDRPOU number (Код ЄДРПОУ), which is similar to a tax identification number in the United States. The Update Server hosted a website (the “Certification Website”) that was used to check whether a company had a valid certificate for verifying electronic signatures. Entering a company’s EDRPOU number into the Certification Website would reveal

whether the company had a valid certificate as well as the name of the entity associated with a given EDRPOU number.

36. Beginning in and around April 2017, the Conspirators, including ANDRIENKO, PLISKIN, and FROLOV, familiarized themselves with the EDRPOU and M.E.Doc, including by querying the EDRPOU website and computer language sets specific to the Ukrainian alphabet.

37. The M.E.Doc software on customer networks periodically connected to the Update Server to check for new software updates. The Conspirators gained access to the software code for the M.E.Doc software prior to the NotPetya attacks, which allowed the Conspirators to surreptitiously add malicious functionality to the files containing the software updates (the “Update Files”). The Conspirators modified Update Files on or about April 14, 2017; May 15, 2017; and June 21, 2017. Computers receiving M.E.Doc software updates downloaded these Update Files, but the NotPetya malware file was not pushed to these computers by the Conspirators until on or about June 27, 2017.

- a. On or about April 14, 2017, the Conspirators published the first malicious Update File to the M.E.Doc Update Server. Before publishing the Update File, the Conspirators added computer code into the file to collect a list of all EDRPOUs associated with computers using the M.E.Doc software that had downloaded the Update File.
- b. The malicious Update File also caused victim computers to send a web request to the Update Server containing a cookie comprised of: (1) the EDRPOU list, and (2) the computer username that was logged into the computer that was running the M.E.Doc software. Once the Conspirators

redirected web traffic from the Update Server to the Conspirators' France-based server on June 27, 2017, the Conspirators received this information from incoming web requests.

- c. On or about June 21, 2017, the Conspirators published another malicious software update to the Update Server. This Update File closely resembled the April 2017 version and would ultimately deliver the NotPetya malware.
- d. In some instances, the Conspirators accessed the Update Server using the Certification Website to query EDRPOU numbers in order to identify organizations that had downloaded a malicious Update File.

38. On or about June 27, 2017, from approximately 12:14 p.m. to 3:31 p.m. Moscow Time, the June 21, 2017, Update File delivered the NotPetya malware to computers that attempted to receive the software update from the Update Server.

- a. The malware was delivered to these computers while the Conspirators temporarily rerouted network traffic bound for the Update Server to the France-based server controlled by the Conspirators. As a result, computers attempting to receive the software update instead connected to the Conspirators' server in France and downloaded the malware.
- b. Once victim computers downloaded the malicious Update File and the Conspirators rerouted the network traffic, victim computers could remotely receive and execute commands from the Conspirators. With these commands, the Conspirators could perform a variety of actions with respect

to the victims' computer systems, including obtaining system information and accessing, modifying, creating, and executing files.

- c. As designed by the Conspirators, once the malware was downloaded onto a computer, it attempted to escalate its privileges and determine whether particular antivirus processes were running on the computer. The malware then attempted to identify other computers on the same network to potentially compromise; if the malware had obtained a particular system privilege, it attempted to extract and execute a credential stealing program and/or escalate its privileges to achieve lateral movement to other computers on the network.
- d. Once the malware file was copied to victim computers, one of two methods was used to execute the malware. FROLOV and other Conspirators coded the malware such that, if both methods failed, the malware spread itself to other victim computers using either the exploit EternalBlue or EternalRomance, which allowed the Conspirators' malware to covertly connect to the computers without valid credentials. After victim computers were confirmed to be vulnerable to either the EternalRomance or EternalBlue exploit, the malware would copy itself to and execute on those computers.
- e. The Conspirators programmed the malware such that, after attempting lateral movement within the compromised computer's network, the malware searched for files ending with dozens of different file extensions

and began encrypting those files on the compromised computer. Once the files were encrypted, the malware created a text file inside every folder that contained encrypted files. The text file contained the NotPetya ransom note, which was later displayed on victim computers as in the example below:

```
Doops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $388 worth of Bitcoin to following address:

    1Mz7153HMuxXTuR2R1t7BmGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
    w0nsm1th123456@posteo.net. Your personal installation key:

    zRNagE-CDBMfc-pD58i4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

- f. DETISTOV and other Conspirators coded the malware such that, after the malware encrypted the files, it restarted the compromised computer using a shutdown command.
- g. DETISTOV and other Conspirators also programmed the malware such that, depending on the type of operating system, and after the malware identified files that were encrypted, it would try various ways to make it more difficult for forensic investigators to obtain digital evidence, including by deleting logs.

39. On or about June 27, 2017, at approximately 7:23 a.m. Eastern Daylight Time, the first computer in the Heritage Valley Health System's computer network became infected by the NotPetya malware. The infection occurred as the result of a connection between the Heritage Valley computer and the computer network of another entity that had itself been infected by the NotPetya malware. By stealing and using Heritage Valley user credentials to self-propagate, the malware then spread from the initial infected Heritage Valley computer to other computers on Heritage Valley's computer network.

40. For the next several hours, Heritage Valley's computer hard drives were encrypted; workstations were locked; patient lists, patient medical history information, physical examination files, and prior laboratory records were inaccessible (so pre-operative laboratory work needed to be redone); and Heritage Valley's servers were inaccessible. The attack also caused Heritage Valley to lose access to its mission-critical computer systems (such as those relating to cardiology, nuclear medicine, radiology, and surgery) for approximately one week and other administrative computer systems for almost one month. In addition to disrupting Heritage Valley's provision of critical healthcare to residents of the Western District of Pennsylvania, Heritage Valley spent more than \$2 million responding to, and recovering from, the attack.

41. Heritage Valley was one of many victims of the NotPetya malware attacks on June 27, 2017. For example, FedEx Corporation spent approximately \$400 million responding to, and recovering from, the attack on its subsidiary TNT Express B.V.'s computer systems, and a large U.S. pharmaceutical manufacturer spent in excess of \$500 million responding to, and recovering from, the attack on its computer systems.

42. On or about June 27, 2017, after the deployment of the NotPetya malware, ANDRIENKO, PLISKIN, and other Conspirators celebrated the attack.

The Attacks Against the 2018 Winter Olympics

Background

43. In 2014, a German documentary titled “Top Secret Doping: How Russia Makes its Winners” aired interviews of a husband and wife, who were a Russian anti-doping official and athlete, respectively, who both admitted to participation in the Russian state-sponsored doping program. Shortly thereafter, the World Anti-Doping Agency (“WADA”) launched an Independent Commission (“IC”) to investigate the validity of the allegations. In a November 2015 report, the WADA IC released its findings, namely, it “confirmed the existence of widespread cheating through the use of doping substances and methods to ensure, or enhance the likelihood of, victory for [Russian] athletes and teams.” The IC made “specific findings” regarding the involvement of the Russian Federal Security Service (“FSB”) in Russia’s efforts to evade anti-doping procedures and protections.

44. In May 2016, a prominent television newsmagazine and newspaper each published stories regarding allegations from the husband and wife whistleblowers, as well as a new Russian whistleblower who had previously managed Russia’s anti-doping laboratory. The whistleblowers all alleged a Russian state-sponsored doping effort at the 2014 Sochi Winter Olympics. In response, WADA named an “independent person” (“IP”) to investigate their allegations.

45. On July 18, 2016, the WADA-appointed IP published his first report, the “McLaren Report,” regarding Russia’s systematic state-sponsored subversion of the drug testing processes prior to, during and subsequent to the 2014 Sochi Winter Olympics. WADA’s Executive

Committee issued a statement accompanying this report, which recommended that the IOC and the International Paralympic Committee (“IPC”) “decline entries for Rio [Olympics] 2016, of all athletes submitted by the Russian Olympic Committee (“ROC”) and the Russian Paralympic Committee.”

46. On July 24, 2016, the IOC Executive Board announced a “preliminary decision” (later affirmed by the broader IOC) that, as a result of the WADA IP’s report, individual sporting federations could exclude Russian athletes from the 2016 Rio Summer Olympics. Ultimately, 111 Russian athletes were barred from participation in the Olympics. The IPC issued a blanket ban of Russian athletes for the 2016 Rio Summer Paralympics.

47. On December 2, 2017, after seventeen months of investigation and the issuance of an additional McLaren Report, the Schmid Commission—a separate Disciplinary Commission tasked with investigating the McLaren Reports’ findings—reported that it concurred with McLaren’s conclusions regarding “‘the existence of a systematic doping scheme in Russia,’ involving the ‘systematic manipulation of the anti-doping rules and system in Russia.’” The Schmid Commission further confirmed the involvement of a number of individuals within Russia’s Ministry of Sport and its subordinate entities.

48. On December 5, 2017, in response to the Schmid Commission Report, the IOC, among other sanctions, suspended the Russian Olympic Committee and its president and prohibited Russian athletes from participating in the 2018 Winter Olympics under the Russian flag (instead allowing demonstrably clean athletes to compete as “Olympic Athletes from Russia”). In response, the Conspirators designed a multi-faceted campaign to attack and disrupt the Olympics by conducting computer intrusions against Olympic partners and athletes, South Korean

government agencies, the IOC, South Korean nationals and international visitors to South Korea, and information technology providers supporting the Olympic Games.

The Spearphishing Campaign Targeting the 2018 Winter Olympics

49. The Conspirators' preparations for targeting the IOC, the Olympics, and Olympic partners (*i.e.*, companies that provided services to or otherwise sponsored the Olympics) through spearphishing campaigns commenced in and around early November 2017, approximately one month before the IOC suspended the Russian Olympic Committee and its president. Over approximately the next two months, the Conspirators conducted reconnaissance, tested spearphishing emails, and sent spearphishing emails relating to the IOC, including emails purporting to be from the IOC and spearphishing emails sent to members of the IOC.

- a. On or about November 28, 2017, KOVALEV crafted a spearphishing email purporting to be from the "IOC Commission Chairman." The email offered recipients a "list of delegates and their contacts," who would purportedly help "deal with any issues during the Olympics."
- b. Later that same day, the Conspirators sent a version of the spearphishing email that KOVALEV crafted (the only difference being that the spearphishing email purported to be from a Vice-President of the IOC) to 29 email addresses hosted at the IOC's domain pyeongchang2018.com. The Conspirators thereafter deleted the email. The email was sent by olympicgameinfo@gmail.com, included the subject line "List of Delegates," and attached a .zip file entitled "List of Delegates" that contained a malware-laced Microsoft Word file. Approximately two

minutes later, the Conspirators used olympicgameinfo@gmail.com to send an identical email to six email addresses hosted at a domain belonging to a Pyeongchang resort that hosted Olympic skiing events.

50. The Conspirators also conducted reconnaissance, tested spearphishing emails, and sent spearphishing emails relating to Olympic partners, including to employees of these partners.

- a. On or about December 4, 2017, the Conspirators conducted online reconnaissance of 2018 Olympic partners, which corresponded with a public list of such partners available at pyeongchang2018.com/en/partners.
- b. On or about December 6, 2017, and December 7, 2017, the Conspirators, using olympicgameinfo@gmail.com, sent approximately twenty-eight Olympics-themed spearphishing emails with the subject line "Further cooperation proposal." These emails (an example of which is shown below) listed the same individual on the signature line as the November 28, 2017, spearphishing email and targeted approximately 220 email addresses hosted at domains belonging to several Olympic partners, as well as the IOC:

From: IOC Info <olympicgameinfo@gmail.com> ☆Reply Reply All Forward Junk Delete More


Subject: Further cooperation proposal12/7/2017, 1:07 AM

To: [REDACTED] ☆ [REDACTED] ☆ [REDACTED] ☆ [REDACTED] ☆ [REDACTED] ☆ [REDACTED] ☆1 more

Dear partners,
The preparations for the XXIII Olympic Winter Games have successfully ended, and in this connection we would like to express our gratitude to you. We would be happy to foster our cooperation and present a list of our commercial offers.

Looking forward to further cooperation,

Ms. [REDACTED]
Vice-President of International Olympic Committee, Executive Members


INTERNATIONAL
OLYMPIC
COMMITTEE

1 attachment: CommercialOffers.zip 7.4 KBSave

- c. On or about December 7, 2017, the Conspirators sent approximately 78 Korean-language spearphishing emails from alert.safekorea@gmail.com to email addresses hosted at domains belonging to five Olympic partners. The emails, which purported to have been sent by the Korean “Ministry of Public Safety and Security” (국민안전처), contained the subject line “Breaking News - Earthquake” and included a message warning recipients about an earthquake. The attached .zip file contained a malware-laced Microsoft Word file that downloaded additional content from the conspirator-controlled domain templates-library.ml.
- d. On or about December 8, 2017, the Conspirators scanned Korean-based network infrastructure for vulnerabilities. The Conspirators thereafter used alert.safekorea@gmail.com to send six spearphishing emails to approximately 98 email addresses hosted at domains belonging to three Olympic partners, including the Korean Sport and Olympic Committee.
- e. On or about December 13, 2017, the Conspirators conducted technical research to identify vulnerabilities with respect to websites used by the Korean Sport and Olympic Committee, a Korean power company, and a Korean airport.

51. In support of their spearphishing campaigns, the Conspirators frequently used a service that allows individuals to send emails to numerous recipients simultaneously (the “Email Service”). The Conspirators used the Email Service in connection with Olympics-related (and other) spearphishing campaigns to send emails appearing to come from email addresses at

legitimate organizations' domains that the Conspirators did not control and had instead spoofed (e.g., the IOC's pyeongchang2018.com domain). With these spearphishing emails, the Conspirators targeted parts of the Republic of Korea's government, Olympic athletes, and additional official Olympic partners.

- a. On or about December 21, 2017, DETISTOV conducted online reconnaissance of the Korean Ministry of Agriculture, Food, and Rural Affairs (농림축산식품부 or "MAFRA") and its website (mafra.go.kr).
- b. On or about December 27, 2017, KOVALEV crafted a spearphishing email related to MAFRA that contained an image with an embedded link to the subdomain mafra.go.kr.jeojang.ga, which the Conspirators created to emulate MAFRA's website (*i.e.*, the same URL, but without jeojang.ga). The Conspirators had registered the jeojang.ga domain on or about December 22, 2017.
- c. On or about December 28, 2017, KOVALEV crafted and sent another spearphishing email that was spoofed using the Email Service so that it would appear to have been sent by info@nctc.go.kr, the official domain of South Korea's National Counterterrorism Center. This email included a malware-laced document that downloaded an image file; the file used an open-source steganography tool to establish an encrypted channel from the recipient's computer to the Conspirators' command-and-control server. This open-source tool, known as Invoke-PSImage, had been released publicly only eight days earlier.

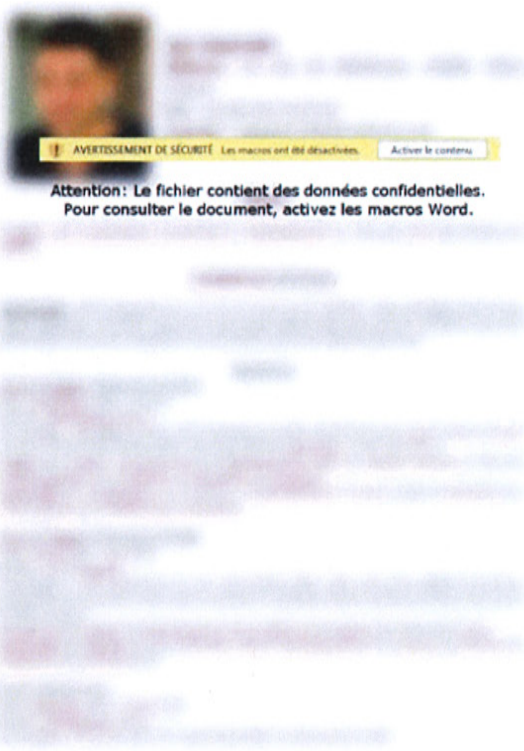
- d. On or about January 10 and 11, 2018, KOVALEV crafted spearphishing emails that were to be spoofed using the Email Service so that they would appear to be from planning.department@pyeongchang2018.com and planning.department@olympic.org; these emails contained the subject line “Accommodation conditions in hotel” and attached malware-laced files. The body of the emails included the following text: “Dear athletes! Please pay attention to the changed living conditions in the hotel complex. Yours faithfully, Accommodation Planning Department.”
- e. On or about January 12, 2018, KOVALEV used the Email Service to send emails purporting to be from service.department@olympic.org to target Olympic athletes. These emails included the accommodations-related language that KOVALEV had crafted over the prior two days.
- f. On or about January 31, 2018, the Conspirators created the operational email account nctc.go@gmail.com and used it to register an account with the Email Service.
- g. Later, on or about February 5, 2018, the Conspirators used the Email Service account registered with the nctc.go@gmail.com email address to send a spearphishing email, which was spoofed to appear to be from info.kr@nctc.go.kr, to an account belonging to a South Korean telecommunications company that was listed as an Olympic partner at pyeongchang2018.com/en/partners.

- h. On or about February 5 and 6, 2018, the Conspirators also used the same Email Service account to send spearphishing emails to 20 email addresses used by the South Korean National Counterterrorism Center.

52. The Conspirators also conducted reconnaissance, tested spearphishing emails, and sent spearphishing emails relating to the 2018 Winter Olympics' official timekeeping partners, including to employees of these partners.

- a. From on or about November 9, 2017, through on or about February 1, 2018, OCHICHENKO conducted reconnaissance relating to South Korea and the 2018 Winter Olympics, as well as more technical research relating to techniques and services that OCHICHENKO would later use to conduct a spearphishing campaign targeting the 2018 Winter Olympics' timekeeping partners, including the entity that provided official timekeeping services at the 2018 Winter Olympics (the "Olympic Timekeeping Service Company") and the entity providing timekeeping devices for the Olympics.
- b. On or about January 31, 2018, after months of preparatory activities, OCHICHENKO sent spearphishing emails to three email accounts used by the Olympic Timekeeping Service Company. The emails were written in French and purported to contain the résumé of an individual who was applying for a position as a "Field Operations Developer." The emails included an attachment that, when opened, displayed a blurred version of the résumé and a pop-up about needing to enable certain features to view the document. As designed, after the recipient clicked the option to enable

the features, the blurred image would be removed, and a malicious PowerShell script would run and call out to the malicious website msrole.com/office_conf, which was hosted on a domain that the Conspirators registered on or about November 15, 2017, to download the next stage of the malware:



Adresse: [REDACTED]
France
Tel: [REDACTED]
Courriel: [REDACTED]

Objectif

D'utiliser mes connaissances d'architecture et développement en .NET pour livrer des solutions de qualité.

Compétences techniques

Technologies: .NET Framework 1.0, 1.1, 2.0, 3.5, 4.0, 4.5, C#, VB.NET, T-SQL, Silverlight, RIA Services, Entity Framework, ASP.NET, Microsoft Visual Studio 2008 & 2010, Microsoft IIS, ASP.NET, SQL Server 2005 & 2008, SQL Server Integration Services (SSIS), SQL Server Reporting Services.

Expérience

Date: Septembre 2008 – Present
Position: Développeur sénior
Technologies: Silverlight v2 & v3, .NET Framework 3.5, WCF, WCF RIA Services, Linq To Sql, C#, Telerik Controls, Visual Studio 2005 & 2008, Expression Blend & Sketchflow, T-SQL, SQL Server
Engagé pour évaluer l'environnement de développement actuel de l'équipe évolution et faire des recommandations pour améliorer et standardiser les processus.
Responsable de l'architecture, la conception, le développement, la mise en place et l'évolution d'un outil de gestion des Métadonnées corporatives.

Date: Février 2007 – Juin 2008
Position: Chef d'équipe
Technologies: .NET Framework 2.0, C#, Visual Studio 2005, T-SQL, SQL Server 2005 & SQL Server Integration Services (SSIS), Smart Client Composite UI Application Block, Enterprise Library, Smart Client Software Factory
Membre clé de l'équipe de développement d'une plateforme de gestion des placements privés.
Responsable de la gestion de base de données. Mené le développement et la livraison du processus de chargement des données (ETL).

Date: Décembre 2006 – Janvier 2007
Position: Développeur sénior
Technologies: Microsoft .NET, C#, Visual Studio 2005, Commerce Server 2007

- c. On or about February 6 and 8, 2018, using infrastructure that was also used in the Olympic Destroyer malware attack, OCHICHENKO created email accounts with usernames reflecting the name of the Chief Executive Officer of the entity providing timekeeping devices for the Olympics.
- d. On or about February 8, 2018, OCHICHENKO used one of the newly created operational accounts to send a spearphishing email, which he had

crafted over the prior two days, to 13 email addresses hosted at the domain belonging to the Olympic Timekeeping Service Company. In this email, OCHICHENKO included a link to a file called “Bonuses.xls.”

- e. On or about February 9, 2018, at 2:23 p.m. Moscow Time, shortly after the deployment of the Olympic Destroyer malware, the Conspirators logged into a Moscow-based server used and managed by the Conspirators to locate news about one of the Olympics timekeeping partners.

Malicious Mobile Application Development Targeting the 2018 Winter Olympics

53. On or about December 11, 2017, the Conspirators created a malicious “Seoul Bus Tracker” mobile application and registered the application with a mobile application store approximately one hour later. The application became available to the public on or about December 18, 2017, but the application store promptly identified and suspended the application before any downloads occurred.

54. On or about December 25, 2017, the Conspirators created a mobile application called “HanMail” that mimicked the name of a legitimate Korean email service. The application became available to the public the next day, but the application store promptly identified and suspended the application before any downloads occurred.

55. On or about December 28, 2017, the Conspirators created a mobile application called “Hmail-App Naver Mail, Hanmail, Daum” that again mimicked the name of the legitimate Korean email service. The application became available to the public on or about January 6, 2018. 47 accounts installed this application before the mobile application store suspended the application.

The Olympic Destroyer Malware Attack

56. On or about February 9, 2018, employees of a company that provided information technology (“IT”) support to the Olympic Games (“IT Company 1”) reported laptops unexpectedly rebooting with messages from BitLocker, a full-volume encryption feature, asking for a recovery key. Multiple IT Company 1 servers experienced the same behavior. These events were caused by the Conspirators’ widespread deployment of malware, which cybersecurity researchers later named “Olympic Destroyer.” As a result, thousands of computers used by IT Company 1 and the PyeongChang Organizing Committee were compromised.

57. To accomplish this end result, the Conspirators first compromised IT Company 1’s computer network and traversed the network seeking user credentials and information related to IT services being provided to the 2018 Winter Olympics. Then, upon compromising the workstation for an IT Company 1 network architect, the Conspirators used this employee’s credentials to obtain access to the “Olympic environment” (*i.e.*, the IT Company 1 computers supporting the 2018 Winter Olympics). After successfully compromising a domain administration account, the Conspirators obtained the access they needed to deploy and execute the Olympic Destroyer malware.

58. The Conspirators designed the Olympic Destroyer malware to steal valid user credentials from victim computers and then spread and replicate itself across a victim’s computer network by exploiting those credentials. Before spreading to the next computer, the malware would overwrite itself to incorporate any additional usernames and passwords it was able to obtain from the previous computer to increase the success rate of its spreading capabilities. Then, among other destructive steps, the malware would delete files from hard drives, force shutdowns, and,

based in part on PLISKIN’s coding efforts in and around January 2018, impede rebooting and recovery by misconfiguring BitLocker. In short, as designed by the Conspirators, the malware’s primary objective was to render infected computer systems inoperable.

59. The Conspirators’ preparations for the Olympic Destroyer malware attack had commenced approximately two months earlier, on or about December 4, 2017, which was the day before the IOC suspended the Russian Olympic Committee and its president. By on or about December 19, 2017—approximately 14 days after the IOC imposed sanctions against the Russian Olympic Committee—the Conspirators had begun compromising the computer network of the IT company (“IT Company 2”) that provided services to the PyeongChang Organizing Committee. By on or about December 21, 2017—approximately 16 days after the IOC imposed sanctions against the Russian Olympic Committee—the Conspirators had begun compromising IT Company 1’s computer network.

60. With unauthorized access to IT Company 1’s computer network, the Conspirators engaged in a variety of illicit activities to obtain credentials, escalate privileges, and move laterally throughout the network.

- a. The Conspirators began their reconnaissance and lateral movement across IT Company 1’s computer network by on or about December 21, 2017, using a particular IT Company 1 computer (“Computer 1”).
- b. On or about December 22, 2017, the Conspirators stole IT Company 1 credentials using an open-source, credential harvesting tool.
- c. On or about December 22, 2017, the Conspirators also sent a file containing four sets of credentials, including plaintext passwords, to Computer 1 to

assist in moving laterally across IT Company 1's computer network through privilege escalation. The file included credentials belonging to an IT Company 1 database developer, whose initials were K.S. The Conspirators later used these credentials from on or about January 4, 2018, until on or about February 1, 2018.

- d. On or about January 22, 2018, the Conspirators executed a malicious PowerShell script containing versions of a credential harvesting tool that operate only in memory and are not easily detectable by antivirus software. The Conspirators designed this script to gather user, IP address, and server data relating to all Remote Desktop Protocol ("RDP") sessions since June 1, 2017.
- e. The Conspirators accessed several systems using compromised accounts, mostly operating from Computer 1. In particular, on or about January 12, 2018, the Conspirators used stolen credentials to access a domain administration account (the "Domain Administration Account") for a particular IT Company 1 network domain ("Domain 1"). As a result of the Conspirators' efforts, they fully compromised Domain 1.
- f. On or about January 23, 2018, and January 24, 2018, the Conspirators used PowerShell scripts to dump credentials from more than 16,000 IT Company 1 computers and servers. This included the credentials of approximately 400 unique accounts associated with Domain 1.

61. The Conspirators also used Computer 1, the Domain Administration account, and other Domain 1 computers to obtain and view Olympics-related files and to access Olympics-related websites.

- a. On or about January 24, 2018—after extracting credentials from IT Company 1’s system—the Conspirators moved stolen credentials and other files to the Domain Administration Account’s computer storage. While on IT Company 1’s computer network, the Conspirators also accessed confidential files related to the IOC, the PyeongChang Olympics, and the Major Events sector of IT Company 1, including “PyeongChang 2018 - Network architecture.docx,” “PyeongChang2018 Disaster Recovery Master Plan.docx,” “PyeongChang2018-RnR_ServerManagement.docx,” “OCOG Domain Account Creation Form.xlsx,” and “Tokyo 2020 environments overview.xlsx.”
- b. On or about January 24, 2018; January 26, 2018; January 29, 2018; and January 30, 2018, the Conspirators used the Domain Administration Account to browse local and shared IT Company 1 network locations relating to the 2018 Winter Olympics.
- c. On or about January 31, 2018; February 2, 2018; and February 7, 2018, the Conspirators used Computer 1 to visit websites related to the Olympics, including pyeongchang2018.com (a domain belonging to the PyeongChang Organizing Committee—*i.e.*, the other entity with computers affected by the Olympic Destroyer malware), dms.pyeongchang2018.com (including a

self-service password reset webpage), extranet.pyeongchang2018.com (including password change, login, and security check webpages), and pwd.pyeongchang2018.com (including password management webpages).

- d. From on or about January 24, 2018, to February 9, 2018, the Conspirators repeatedly accessed and browsed files on a computer within Domain 1 that was used by a network architect for IT Company 1's Major Events team. During this time period, the Conspirators ran malicious scripts, explored the computer for credentials and credential files primarily relating to the PyeongChang Olympics, and pivoted to other computers. The files accessed by the Conspirators from on or about January 24, 2018, to on or about January 31, 2018, included "Winter Olympics.rdg," "Venues.rdg," and "Pyeongchang.rdg." The attackers also accessed files, such as "PyeongChang LAN Network Diagram.vsd," that would be useful for understanding how IT Company 1's computer network was configured and for moving laterally across the computer network.

62. The Conspirators used a particular IT Company 1 account (the "Deployer Account") to deploy the component of the Olympic Destroyer malware that wiped victim computers and servers and rendered them inoperable. The Conspirators also deployed the malware to the PyeongChang Organizing Committee's computer network.

- a. On or about February 9, 2018, at approximately 6:24 p.m. Korea Standard Time, the attackers uploaded the Olympic Destroyer malware to IT Company 1's computer network.

- b. Shortly thereafter, at approximately 7:42 p.m. Korea Standard Time—during the opening ceremony of the Olympics—the Conspirators used the Deployer Account to deploy and execute the wiper component of the Olympic Destroyer malware within Domain 1 using a technique that permits the deployment of software to multiple computers in the same network at the same time. The malware deployment was facilitated in part by PLISKIN’s and ANDRIENKO’s malware development efforts in and around January and February 2018.
- c. On or about February 9, 2018, from approximately 7:33 p.m. to 10:23 p.m. Korea Standard Time—after the Conspirators used a connection between IT Company 2’s computer network and the PyeongChang Organizing Committee’s computer network to compromise key computers within the Committee’s network—the Conspirators deployed the Olympic Destroyer malware to 30 computers used by the PyeongChang Organizing Committee. As with IT Company 1’s computers, the malware rebooted and wiped the PyeongChang Organizing Committee’s computers.
- d. On or about February 9, 2018, shortly after the deployment of the Olympic Destroyer malware, the Conspirators logged into a Moscow-based server used and managed by the Conspirators to locate news about the attacks and track the attacks’ impacts.

63. The Conspirators attempted to hide their activities and avoid being identified as the perpetrators of the Olympic Destroyer attack.

- a. For example, to obfuscate the true source of the malware, the Conspirators crafted the malware's computer code to emulate malware used by the Lazarus Group in North Korea. In the months prior to the attack, the Conspirators took steps to analyze Lazarus Group malware samples, system tools, and wipers in order to mimic the Group's malware.
- b. In the same approximate time period, ANDRIENKO worked on an algorithm the Conspirators used to obscure certain features of the Olympic Destroyer malware, in order to hinder any post-attack investigation and avoid the detection of the malware by antivirus software.
- c. In addition, on or about December 22, 2017, the Conspirators established a command-and-control implant on Computer 1 to create a single point of access between IT Company 1's internal network and a server hosted in France that the Conspirators controlled. This single tunnel allowed the Conspirators to better hide their activity on IT Company 1's network and to issue commands, install additional tools, and transfer data with respect to IT Company 1's computer system.

The Targeting of the DSTL and the OPCW

64. The OPCW is the body that implements the Chemical Weapons Convention of 1997 and includes 193 member nations, including the United States. The OPCW provided the United Kingdom with technical assistance (independent and separate from the U.K. authorities' investigation) with respect to the March 4, 2018, poisoning of former GRU officer Sergei Skripal, his daughter, and U.K. citizens in the United Kingdom (in Salisbury, England) with a nerve agent.

65. The DSTL is an executive agency of the United Kingdom’s Ministry of Defence and operates the Salisbury-based Porton Downs Science Campus. On or about April 3, 2018, the DSTL announced that it had identified the poison used against Skripal and others as a military-grade “Novichok” nerve agent.

66. On or about April 5, 2018, KOVALEV created an email account with a username that mimicked the name of a German national weekly newspaper. Shortly after creating the account, KOVALEV sent spearphishing emails regarding the “Incident in Salisbury,” purporting to be from a German journalist, to approximately 60 official DSTL email addresses. The next day, KOVALEV used the above-described Email Service to send emails, with malware attached, that appeared to be from a legitimate DSTL email address.

67. Also on or about April 6, 2018, the Conspirators conducted three related spearphishing campaigns that targeted the OPCW and U.K. agencies involved in the investigation of the poisoning.

- a. On or about April 6, 2018, the Conspirators used an operational account—which was created on or about April 5, 2018, and had a username mimicking the name of a U.K. journalist working for a U.K. media entity—to send approximately 20 spearphishing emails with the email subject line “Salisbury Spy Poisoning Investigation” to official OPCW email addresses. In the emails, the Conspirators purported to have information to share regarding the poisoning.
- b. After the Conspirators received an email from OPCW directing them to instead share their information with certain U.K. authorities at three

particular email addresses, the Conspirators used the same operational account to send spearphishing emails to those three email addresses.

- c. Also on or about April 6, 2018, the Conspirators created another operational account, with a username mimicking the name of another U.K. journalist at the same U.K. media entity, and shortly thereafter sent approximately 19 spearphishing emails with the subject line “Salisbury Spy Poisoning Investigation” to official OPCW email addresses. In the emails, the Conspirators again purported to have information to share regarding the poisoning.

The Conspirators’ Activities Targeting the Country of Georgia

68. Similar to their targeting of Ukraine since 2015, the Conspirators engaged in a broad cyber campaign against government and private sector entities in the country of Georgia—including the Parliament of Georgia and a major media outlet—with disruptive and destructive attacks to undermine confidence in and otherwise destabilize Georgia.

69. For example, on or about January 25, 2018, KOVALEV created an email account with a username emulating the name of a Georgian media entity that focuses on news coverage. Shortly thereafter, KOVALEV used the account to send eight spearphishing emails with a malware-laced attachment to 68 email addresses hosted at the domain belonging to that same Georgian media entity.

70. On or about July 31, 2019, and August 1, 2019, OCHICHENKO conducted technical reconnaissance of the Parliament of Georgia’s official internet domain and attempted to gain unauthorized access to its network.

71. Months later, on or about October 28, 2019, the Conspirators engaged in a wider-ranging cyber attack against a large number of entities in the country of Georgia. This attack targeted websites belonging to Georgian government, non-government, and private sector entities and involved the defacement of approximately 15,000 websites and the disruption of service to some of these websites after the computer systems of a Georgian web hosting provider were compromised. In many cases, the Conspirators replaced website home pages with an image of a former Georgian president, who was known for his efforts to counter Russian influence in Georgia, along with the caption “I’ll be back.”

STATUTORY ALLEGATIONS

72. Beginning at least in and around November 2015 and continuing until at least in and around October 2019, the exact dates being unknown to the grand jury, in the Western District of Pennsylvania and elsewhere, defendants YURIY SERGEYEVICH ANDRIENKO, SERGEY VLADIMIROVICH DETISTOV, PAVEL VALERYEVICH FROLOV, ANATOLIY SERGEYEVICH KOVALEV, ARTEM VALERYEVICH OCHICHENKO, and PETR NIKOLAYEVICH PLISKIN, did knowingly and intentionally combine, conspire, confederate, and agree together, with each other and with others known and unknown to the grand jury, to commit offenses against the United States, namely:

- a. to access a computer without authorization and to obtain thereby information from a protected computer, in furtherance of a criminal and tortious act in violation of the laws of the United States, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, in violation of

Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii);
and

- b. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to cause damage without authorization to a protected computer, and where the offense did cause and would, if completed, have caused, loss aggregating more than \$5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, the modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals, a threat to public safety, and damage affecting at least 10 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).

73. In furtherance of the conspiracy, and as set forth in paragraphs 14, 51, and 52, 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 jeojang.ga and msrole.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).

COUNT TWO
(Wire Fraud Conspiracy)

The grand jury further charges:

74. The allegations contained in Paragraphs 1 through 9 and Paragraphs 11 through 71 of this indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

THE CONSPIRACY AND ITS OBJECTS

75. From at least in and around November 2015 and continuing through in and around October 2019, in the Western District of Pennsylvania and elsewhere, defendants YURIY SERGEYEVICH ANDRIENKO, SERGEY VLADIMIROVICH DETISTOV, PAVEL VALERYEVICH FROLOV, ANATOLIY SERGEYEVICH KOVALEV, ARTEM VALERYEVICH OCHICHENKO, and PETR NIKOLAYEVICH PLISKIN did knowingly and intentionally conspire, combine, and agree to commit an offense against the United States, that is, wire fraud, contrary to the provisions of Title 18, United States Code, Section 1343; to wit, the defendants, YURIY SERGEYEVICH ANDRIENKO, SERGEY VLADIMIROVICH DETISTOV, PAVEL VALERYEVICH FROLOV, ANATOLIY SERGEYEVICH KOVALEV, ARTEM VALERYEVICH OCHICHENKO, and PETR NIKOLAYEVICH PLISKIN, together with conspirators, having devised and intending to devise a scheme and artifice to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice.

76. Specifically, an object of the conspiracy was to deploy destructive malware and take other disruptive actions, for the strategic benefit of Russia, through hacking of victim

computers by means of false and fraudulent pretenses. These victims included those described in paragraph 3.

77. With respect to the NotPetya and Olympic Destroyer malware attacks, and other computer intrusions that were part of the conspiracy, the Conspirators used stolen authentication credentials to misrepresent their identities within the victims' networks to obtain unauthorized access to and move laterally within victim networks.

78. In addition, in order to gain unauthorized access to victims' computer networks, the Conspirators crafted and transmitted, in interstate and foreign commerce, spearphishing emails that targeted the victims. The Conspirators designed the spearphishing emails to appear legitimate in order to deceive recipient victims into opening the emails and clicking on malicious attachments or links that thereafter enabled the Conspirators to steal login credentials for the victims' computer networks. The malicious links included spoofed domains that resembled legitimate websites associated with the victim entities. For example, the Conspirators registered the domain msrole.com (which mimicked a legitimate Microsoft domain) on November 15, 2017, and the domain jeojang.ga (which mimicked a website belonging to MAFRA) on December 22, 2017, and thereafter utilized those spoofed domains in furtherance of the fraud scheme.

All in violation of Title 18, United States Code, Section 1349.

COUNTS THREE AND FOUR
(Wire Fraud)

The grand jury further charges:

79. The allegations contained in Paragraphs 1 through 9 and Paragraphs 11 through 71 of this indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

80. On or about the dates set forth below, in the Western District of Pennsylvania and elsewhere, the defendants, YURIY SERGEYEVICH ANDRIENKO, SERGEY VLADIMIROVICH DETISTOV, PAVEL VALERYEVICH FROLOV, ANATOLIY SERGEYEVICH KOVALEV, ARTEM VALERYEVICH OCHICHENKO, and PETR NIKOLAYEVICH PLISKIN, having devised and intending to devise a scheme and artifice to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice, and aided and abetted the same; to wit, the defendants did knowingly transmit the NotPetya malware by means of a wire to the computer systems of the victim identified below, on or about the dates and times set forth below, and stole the victim's user authentication credentials to move laterally to other parts of the victim's network, with each such transmission being a separate count of this indictment:

Count	Approximate Date and Time	Victim
3	June 27, 2017 at 7:23 a.m. Eastern Daylight Time	Heritage Valley Health System
4	June 27, 2017 at 7:24 a.m. Eastern Daylight Time	Heritage Valley Health System

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT FIVE

(Computer Fraud – Damage to Computers)

The grand jury further charges:

81. The allegations contained in Paragraphs 1 through 9 and Paragraphs 11 through 71 of this indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

82. On or about June 27, 2017, in the Western District of Pennsylvania and elsewhere, defendants YURIY SERGEYEVICH ANDRIENKO, SERGEY VLADIMIROVICH DETISTOV, PAVEL VALERYEVICH FROLOV, ANATOLIY SERGEYEVICH KOVALEV, ARTEM VALERYEVICH OCHICHENKO, and PETR NIKOLAYEVICH PLISKIN, did knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, caused damage without authorization to a protected computer; to wit, the defendants knowingly caused the transmission of the NotPetya malware, and aided and abetted the same, and as a result of such conduct, caused damage without authorization to computers used by the Heritage Valley Health System. The offense caused loss resulting from a related course of conduct affecting one or more protected computers aggregating at least \$5,000 in value, the modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals, a threat to public health or safety, and damage affecting 10 or more protected computers during a one-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B) and 2.

COUNTS SIX AND SEVEN
(Aggravated Identity Theft)

The grand jury further charges:

83. The allegations contained in Paragraphs 1 through 9 and Paragraphs 11 through 71 of this indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

84. On or about the dates set forth below, in the Western District of Pennsylvania and elsewhere, the defendants, YURIY SERGEYEVICH ANDRIENKO, SERGEY VLADIMIROVICH DETISTOV, PAVEL VALERYEVICH FROLOV, ANATOLIY SERGEYEVICH KOVALEV, ARTEM VALERYEVICH OCHICHENKO, and PETR NIKOLAYEVICH PLISKIN, did knowingly transfer, possess and use without lawful authority, a means of identification of another person, and aided and abetted the same, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), namely, conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, knowing that the means of identification belonged to another real person who worked on behalf of the targeted victim organization:

Count	Approximate Dates	Victim Organization	Means of Identification
6	January 4, 2018, to February 1, 2018	IT Company 1	Username and password for account used by K.S.
7	January 23, 2018, and January 24, 2018	IT Company 1	Usernames and passwords for multiple employee accounts

In violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4) and 2.

FORFEITURE ALLEGATIONS

85. The allegations contained in Counts One through Seven of this Indictment are incorporated herein by reference as though fully set forth herein for the purpose of alleging criminal forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(A).

86. The United States hereby gives notice to the defendants, YURIY SERGEYEVICH ANDRIENKO, SERGEY VLADIMIROVICH DETISTOV, PAVEL VALERYEVICH FROLOV, ANATOLIY SERGEYEVICH KOVALEV, ARTEM VALERYEVICH OCHICHENKO, and PETR NIKOLAYEVICH PLISKIN, charged in Count 1 that, upon their conviction of such offense, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(B), which require any person convicted of such offense to forfeit any property, real or personal, constituting or derived from proceeds obtained directly or indirectly as a result of such offense.

SUBSTITUTE ASSETS


87. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- 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 which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 982(b), to seek forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

A True Bill,

FOREPERSON


SCOTT W. BRADY
United States Attorney
PA ID No. 88352