AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

COPY

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
JUN - 8 2018
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

United States of America

v.

PARK JIN HYOK, also known as ("aka") "Jin Hyok Park," aka "Pak Jin Hek,"

Defendant.

Case No. MJ 18-1479

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than September 2, 2014 and continuing through at least August 3, 2017, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1349	Conspiracy to Commit Wire Fraud

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Nathan P. Shields, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 06-08-18

ROZELLA A. OLIVER
Judge's signature

City and state: Los Angeles, California

Hon. Rozella A. Oliver, U.S. Magistrate Judge
Printed name and title

AUSAs: Stephanie S. Christensen, x3756; Anthony J. Lewis, x1786; & Anil J. Antony, x6579 REC: Detention

Contents

A F F I D A V I T

I, Nathan P. Shields, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2011. I am currently assigned to the Los Angeles Field Office, where I conduct investigations related to computer intrusions and national security. During my career as an FBI SA, I have participated in numerous computer crime investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology. Prior to becoming a Special Agent with the FBI, I was employed for eleven years as a Software Engineer where I worked on software projects at NASA's Johnson Space Center that supported the International Space Station and Space Shuttle mission simulators. I received a bachelor's degree in Aerospace Engineering with a minor in Computer Science from Embry-Riddle Aeronautical University. As a federal agent, I am authorized to investigate violations of the laws of the United States and have experience doing so. I am a law enforcement officer with authority to apply for and execute warrants issued under the authority of the United States.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against, and arrest warrant for, PARK JIN HYOK, also known as ("aka") "Jin Hyok Park," aka "Pak Jin Hek" ("PARK") for: (1) a violation of 18 U.S.C. § 371 (Conspiracy), for conspiring to commit the following offenses: 18 U.S.C. §§ 1030(a)(2)(c), 1030(a)(4), (a)(5)(A)-(C) (Unauthorized Access to Computer and Obtaining Information, with Intent to Defraud, and Causing Damage, and Extortion Related to Computer

Intrusion); and (2) a violation of 18 U.S.C. § 1349 (Conspiracy), for conspiring to commit the following offense: 18 U.S.C. § 1343 (Wire Fraud).

3. The information set forth in this affidavit is based upon:

- my personal observations;
- my training and experience;
- information from various law enforcement personnel and witnesses;
- computer scientists and other experts at the FBI;
- experts at Mandiant, a cybersecurity firm, which was retained by the United States Attorney's Office; and
- publicly available resources and reports produced by private cyber security companies, and other publicly available materials.

4. The evidence set forth herein was obtained from multiple sources, including from analyzing compromised victim systems, approximately 100 search warrants for approximately 1,000 email and social media accounts accessed internationally by the subjects of the investigation, dozens of orders issued pursuant to 18 U.S.C. §§ 2703(d) and 3123, and approximately 85 formal requests for evidence to foreign countries and additional requests for evidence and information to foreign investigating agencies. Many of those records were obtained from providers of email, social media, or other online or communication services ("providers" herein).

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant and does not purport to set forth all of my knowledge of the government's investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. Unless specifically indicated otherwise, all dates and times set forth below are on or about the dates and times indicated, and all amounts or sums are approximate.

III. SUMMARY

6. The facts set forth in this affidavit describe a wide-ranging, multi-year conspiracy to conduct computer intrusions and commit wire fraud by co-conspirators working on behalf of the government of the Democratic People's Republic of Korea, commonly known as "DPRK" or "North Korea," while located there and in China, among other places. The conspiracy targeted computers belonging to entertainment companies, financial institutions, defense contractors, and others for the purpose of causing damage, extracting information, and stealing money, among other reasons. One of the subjects was PARK, a North Korean computer programmer who was one of the co-conspirators (collectively, the "subjects" of the investigation). As described in greater detail below, PARK was employed by Chosun Expo Joint Venture, which is also known as "Korea Expo Joint Venture" or simply "Chosun Expo" (as it is referred to herein), a company that is a front for the North Korean government.

7. Among the successful intrusions by the subjects was the cyber-attack in November 2014 directed at Sony Pictures Entertainment ("SPE") and its comedic film "The Interview," which depicted a fictional Kim Jong-Un, the Chairman of the Workers' Party of Korea and the "supreme leader" of North Korea. The subjects targeted individuals and entities associated with the production of "The Interview" and employees of SPE, sending them malware that the subjects used to gain unauthorized access to SPE's network. Once inside SPE's network, the subjects stole movies and other confidential information, and then effectively rendered thousands of computers inoperable. The same group of subjects also targeted individuals associated with the release of "The Interview," among other victims.

8. These same subjects also targeted and then executed the fraudulent transfer of $81 million from Bangladesh Bank, the central bank of Bangladesh, in February 2016—the largest successful cyber-theft from a financial institution to date—and engaged in computer intrusions and cyber-heists at many more financial

services victims in the United States, and in other countries in Europe, Asia, Africa, North America, and South America in 2015, 2016, 2017, and 2018, with attempted losses well over $1 billion.

9. In addition to financial institutions and entertainment companies, the subjects have targeted—and continue to target—other victims and sectors, including U.S. defense contractors, university faculty, technology companies, virtual currency exchanges, and U.S. electric utilities.

10. The same subjects were also responsible for authoring the malware used in the global ransomware cyber-attack named "WannaCry 2.0," which quickly spread to computers around the world, including computers in the Central District of California, in approximately May 2017.

11. In sum, the scope and damage of the computer intrusions perpetrated and caused by the subjects of this investigation, including PARK, is virtually unparalleled.

12. While some of these computer intrusions or attempted intrusions occurred months or years apart, and affected a wide range of individuals and businesses, they share certain connections and signatures, showing that they were perpetrated by the same group of individuals (the subjects). For instance, many of the intrusions were carried out using the same computers or digital devices, using the very same accounts or overlapping sets of email or social media accounts, using the same aliases, and using the same cyber infrastructure, including the same IP addresses and proxy services.

13. Technical similarities also connect the malware used against SPE, Bangladesh Bank and other financial institutions, and defense contractors (among other actual and intended victims), and the WannaCry ransomware. Those technical similarities include common elements or functionality of the malware that was used, common encryption keys used to decrypt resources associated with the

malware, and domains programmed into the malware that were under the common control of a single computer or group of computers. These and other connections discussed below show that the subjects comprise members of the "Lazarus Group," the name that private security researchers (including Symantec, Novetta, and BAE) have given to the set of hackers who perpetrated the attacks on SPE, Bangladesh Bank, and other entities.

14. PARK, a member of the conspiracy behind these cyber-attacks and computer intrusions, was educated at a North Korean university, had proficiency in multiple programming languages, and had experience in developing software and in network security for different operating systems. He was a programmer employed by the government of North Korea, and worked for Chosun Expo, a North Korean government front company affiliated with one of the North Korean government's hacking organizations, sometimes known as "Lab 110," starting in at least 2002. Some programmers employed by Chosun Expo stationed abroad—including PARK—did some work for paying clients on non-malicious programming projects. In particular, PARK worked among a team of North Korean programmers employed by Chosun Expo in Dalian, China, who did programming and information technology projects for paying clients around the world, some of whom knew they were employing North Korean programmers. Although PARK worked in China for at least some time between 2011 and 2013, he appears to have returned to North Korea by 2014, before the cyber-attack on SPE.

15. PARK used multiple email accounts in the timeframe that he was in China (collectively, the "Chosun Expo Accounts"), and communications in some of those accounts made explicit reference to Chosun Expo and the work done on behalf of Chosun Expo. PARK used those Chosun Expo Accounts in his true name, and while it does not appear that PARK was necessarily the exclusive user of those accounts, PARK used his name to sign correspondence, in subscriber records, and to

create other social media accounts in his name using the Chosun Expo Accounts. Despite efforts to conceal his identity and the subjects' efforts to isolate the Chosun Expo Accounts from operational accounts that they used with aliases to carry on their hacking operations, there are numerous connections between these sets of accounts. Some of the operational accounts were used in the name "Kim Hyon Woo" (or variations of that name), an alias that the subjects used in connection with the targeting of and cyber-attacks on SPE, Bangladesh Bank, and other victims. Although the name "Kim Hyon Woo" was used repeatedly in various email and social media accounts, evidence discovered in the investigation shows that it was likely an alias or "cover" name used to add a layer of concealment to the subjects' activities.

16. While some of the work referenced in Chosun Expo Account messages involved non-malicious programming-for-hire, operational accounts connected to those Chosun Expo Accounts were used for researching hacking techniques, reconnaissance of victims, and ultimately sending spear-phishing messages to victims. For example, one of the Chosun Expo Accounts tied to PARK, ttykim1018@gmail.com, was connected in a number of ways to the similarly-named email account—tty198410@gmail.com—which was one used in the persona "Kim Hyon Woo." That email account, in turn, was used to subscribe or was accessed by the same computer as at least three other email or social media accounts that were each used to target multiple victims, including SPE and Bangladesh Bank.

17. These connections, among others, establish that PARK was a member of the conspiracy: he worked for Chosun Expo and used multiple Chosun Expo Accounts, which accounts in turn were tied to the accounts directly used for carrying out multiple computer intrusions. (*See* Chart 1 attached hereto and discussed below in paragraph 265.)

IV. TERMINOLOGY

18. This Part discusses and explains some of the terms that are used throughout this affidavit. The explanations herein are based upon my training and experience, as well as information from other FBI agents and a computer scientist.

19. Backdoor: A "backdoor" is a type of malware that allows a hacker to maintain access to a compromised computer after a computer is first compromised. A backdoor can operate in a number of ways, but its basic function is to allow a hacker a way to re-gain access to a compromised computer in the event that the access is disrupted, such as if the hacker is detected, if other malware associated with the intrusion is deleted, or if the connection is interrupted.

20. Code: "Binary code," which is also known as "machine code," "compiled code," or "executable code," is a set of specially formatted instructions that direct a computer's processor to manipulate and store data. A computer "program," "software," or "executable file" are all various ways to refer to a complete body of binary code that has a defined set of functionality. Binary code appears as unintelligible, cryptic strings of numbers that cannot reasonably be comprehended—let alone written—by a human when editing or creating software. As such, programming "languages" provide an abstracted syntax that allows programmers to write simple, structured instructions, or "source code," in a manner that resembles the English language. Special software called a "compiler" can then translate, or "compile," this source code into binary code.

21. Contacts Lists: "Stored contacts" or a "contacts list" are essentially the "address book" or digital Rolodex for an online account. These lists are sometimes automatically populated or may be manually populated by the user, depending on the particular email, social media, or other communication provider.

22. DNS: The Domain Name Service, or "DNS," is a naming system for computers, services, or any other resources connected to the internet. An often-used

analogy to explain the DNS is that it serves as the phone book for the internet by "resolving" human-friendly computer hostnames to IP addresses. For example, the domain name "www.justice.gov" may resolve to the IP address 149.101.146.50.

23. DDNS: Dynamic DNS, or "DDNS," is a service offered in which the provider will allow users to control the IP address assignment of a domain, or more typically, a sub-domain such as http://subdomain.domain.com. The user can access this IP address assignment through the provider and make changes as needed. One of the key aspects of a DDNS service (compared to a traditional DNS service) is that changes to the IP assignments can be set to quickly propagate across the internet, while a traditional DNS service may take longer to populate or update various sources where a computer might seek to "look up" or resolve a domain. DDNS domains also, however, can be used for malicious purposes, as the subjects of this investigation have done on numerous occasions. Specifically, hackers can choose to command-and-control their malware by embedding DDNS domains in malware, instead of hard-coded IP addresses. This gives the hacker certain advantages, for example:

a. First, if the hacker loses access to the intermediary computer that he or she was using to command-and-control the malware and victim computer, the hacker can simply log into the DDNS account maintained by the provider and update the IP address of the malicious DDNS domain to a new IP address assigned to a computer that the hacker still controls. This eliminates the need for the hacker to update and re-compile the malware on the victim system to point it to a new IP address.

b. Second, the hacker can assign a non-malicious IP address to the DDNS domain when the hacker is not using the victim computer, and then assign a malicious IP address to the DDNS domain when the hacker is ready to hack into the victim computer. Alternatively, as discussed further in paragraph 49, the

hacker can assign a pre-computed IP address to the domain that is a "fake" command-and-control IP address, then program the malware so that it uses the "fake" command-and-control IP address to run an algorithm to compute the value of the "true" command-and-control IP address. This can make identifying the source of the malicious network traffic more difficult for the victim.

24. Hashes: A "hash" value—such as MD5, SHA1, or SHA256—can be calculated for any computer file by applying a one-way algorithm to the data contained in the file. If any of the content of the file is changed, even a change as minor as adding an extra "space" character, the algorithm will produce a different hash when it is applied to the file. Although there is an extremely small possibility of two separate files calculating the same hash (it has been proven by researchers to be possible), when two files have the same hash value they are assumed to be identical files, thus providing verification to a very high degree of confidence that the two files are identical. The differences between MD5, SHA1, and SHA256 are simply differences in the mathematical algorithms that are used to create the hash, and they result in different lengths of hash value, with MD5 resulting in a 128-bit value (*i.e.*, how long the hash value is), SHA1 in a 160-bit value, and SHA256 in a 256-bit value.

25. Hop point: The term "hop point" often refers to a computer used by an unwitting victim that has been compromised by hackers and is then used by the hackers as part of their infrastructure for further computer intrusions. A hacker's use of a hop point will often carry on even while the unwitting victim continues to use the computer for legitimate purposes, unaware that part of its storage and processing capacity is being used by intruders. A hop point can serve a similar purpose as a proxy service, in that a hacker can use it as a relay when carrying out an intrusion so that a victim will only "see" the hop point's IP address, concealing to a degree the hacker's true home IP address. But because a hop point is often an

entire functioning computer, rather than simply a relay, it can be used for other purposes as well. For example, a hacker may use a compromised computer to store malware intended to infect victim computers, to communicate with victim computers and send them commands, to store stolen data or tools used in an intrusion, or for other staging activities.

26. IP address: An Internet Protocol version 4 address, also known as an "IPv4 address," or more commonly an "IP address," is a set of four numbers or "octets," each ranging from 0 to 255 and separated by a period (".") that is used to route traffic on the internet. A single IP address can manage internet traffic for more than one computer or device, such as in a workspace or when a router in one's home routes traffic to one's desktop computer, as well as one's tablet or smartphone, while all using the same IP address to access the internet. Use of a common IP address typically indicates the use of shared or common computer infrastructure or use of the same physical space to connect to the internet.

27. Malware: "Malware" is malicious computer software intended to cause the victim computer to behave in a manner inconsistent with the intention of the owner or user of the victim computer, usually unbeknownst to that person.

28. North Korean IP Addresses: Throughout this affidavit, certain IP addresses are referred as "North Korean." Those references are to IP addresses from two blocks. The first is a block of IP addresses, 175.45.176.0–175.45.179.255, which are registered to a company in Pyongyang, North Korea. The second set is a block of IP addresses, 210.52.109.0–210.52.109.255, which—according to multiple publicly available sources—are registered to a company in China, but which have been leased or used by North Korea since before North Korea was allocated the first block of IP addresses around late-2009.

29. Phishing: A "phishing" email is typically one that is sent to one or more recipients and is designed to appear legitimate in order to get the recipient(s)

to take a certain action, such as clicking on a link or opening a file that would cause a victim's computer to be compromised by a hacker. For example, a hacker might send a phishing email to a large number of recipients, where that phishing email is designed to look like it is from a particular bank. In doing this, the sender hopes that some recipients do in fact have accounts at that bank and may be tricked into thinking it is a legitimate email. At times malware may be attached as a file to the message, or malware might be stored on a server and the phishing message may contain a "hyperlink," also known as a "link," that would cause the victim's computer to download a file from that server.

30. Proxy service: A "proxy service" offers the use of "proxy servers," which are computers connected to the internet that serve as relays, sometimes between a person using a personal computer and the website that the person was accessing. When using a proxy service, websites that a person is accessing generally do not "see" the location of the "true" or "home" originating IP address or country where the internet traffic originated, which would reveal the location of the person's computer. Instead, the website accessed via a proxy would only "see" the IP address of the proxy server that was serving as the relay. The subjects use a number of methods to hide (or "proxy") their internet traffic, including services that route web or other internet traffic, as well as virtual private network ("VPN") services that encrypt traffic between a "home" IP address and the VPN's server before connecting to the internet.

31. Ransomware: Ransomware is a type of malware that infects a computer and encrypts some or all of the data or files on the computer, and then demands that the user of the computer pay a ransom in order to decrypt and recover the files, or in order to prevent the malicious actors from distributing the data.

32. Recovery Emails: Email and social media providers frequently require subscribers to list a "secondary," "recovery," or "alternative" email account when signing up for an email or social media account. Recovery email accounts can be used by a provider to authenticate that the person trying to access the account is in fact the user entitled to do so. For example, if a user has forgotten his or her password, a one-time password might be sent to a recovery email account, which would allow a user to re-gain access to his or her account. Because the secondary email address can in some instances allow access to the primary account, the secondary or recovery account is often used by the same person who controls the primary account or, at a minimum, someone close to or trusted by the user of the primary account. In this affidavit, the terms "secondary" or "recovery" account are used synonymously with an email address that is used to "subscribe" another email or social media account as described in this paragraph.

33. Spear-phishing: A "spear-phishing" email is a phishing email that is not only designed to appear legitimate, but is also tailored and personalized for the intended recipient or recipients. Spear-phishing emails often include information that the hacker knows about the recipient based on reconnaissance or other sources of information about the intended victim.

34. URL: A Uniform Resource Locator, also known as a "URL," is a website address that is used to direct a computer to a particular web server or a website hosted on that web server. URLs can be lengthy strings of words and characters, and some companies, such as Google, offer "shortened URLs" that compress a full URL into a smaller string of characters that is easier to fit in social media messages like Twitter that limit the number of characters that can be used. If a shortened URL is entered into a web browser, the web browser will be re-directed to the complete URL. A shortened URL also, however, obscures the actual domain to which it will connect a computer whose user clicks on that link.

35. Worm: A "worm" is a type of malware that attempts to progressively infect computers, typically by exploiting a vulnerability in the victim computers or by "brute force" attacks upon victim computers. A "brute force" attack on a computer or network occurs when a hacker or the hacker's malware attempts to log-in to a potential victim computer using a predetermined list of possible username and password combinations, which lists often contain thousands of common combinations of usernames and passwords that include specific default settings used on certain applications and devices.

V. INFRASTRUCTURE

A. North Korean Computer Networks

36. Throughout this investigation, the subjects have used North Korean IP addresses to engage in malicious and non-malicious activity. Within the block of 1,024 IP addresses directly assigned to North Korea, two narrow ranges of IP addresses have been consistently linked to malicious activity and the individuals associated with that activity (*i.e.*, the subjects of this investigation). From early-2014 through the end of 2015, that malicious activity was originating from four specific North Korean IP addresses, referred to herein as North Korean IP Addresses #1, #2, #3, and #4. In late-March 2016, the previously identified activity was found to have shifted consistently by a specific numerical increase in the last octet of the IP address, with activities previously associated with North Korean IP Addresses #1, #2, #3, and #4 shifting to what will be referred to herein as North Korean IP Addresses #5, #6, #7, and #8 (where activities associated with #1 shifted to #5, #2 shifted to #6, #3 shifted to #7, and #4 shifted to #8).[1]

37. More specifically, and as will be discussed in this affidavit, activity that was previously originating from North Korean IP Address #1 and that was

[1] Between January 2016 and late-March 2016, some accounts and activities that were previously linked to North Korean IP address #2 were temporarily associated with a different North Korean IP address.

more recently originating from North Korean IP Address #5 has been linked to DDNS domains used in the malware called Contopee—which was used in intrusions at banks, and was also identified in a public report by cyber security firm Group IB as being used in a malicious cyber campaign against the Polish banking sector. Activity that was originating from North Korean IP Address #2 and that was more recently originating from North Korean IP Address #6 has been linked to malicious email and social media accounts using fake alias names that sent spear-phishing emails to potential victims, while also scanning and directly hacking into computer systems. Activity that was originating from North Korean IP Address #3 and that was more recently originating from North Korean IP Address #7 has been linked to both malicious activity as well as use by subjects to access their personal accounts (including the Chosun Expo Accounts) and work on non-malicious software development projects. Activity that was originating from North Korean IP Address #4 and that was more recently originating from North Korean IP Address #8 has been linked to some of these same subjects using North Korean IP Address #7 to access the Chosun Expo Accounts, including using their true names.

B. The "Brambul" Worm

38. The subjects of the investigation have repeatedly used as hop points particular computers that were compromised by a piece of malware known as the "Brambul" worm that crawls from computer to computer, trying to infect computers and then, if successful, relaying the credentials and victim host information (that are necessary to gain access to the compromised computers) to certain "collector" email accounts hard-coded into the malware. I know the following information about the Brambul worm based on email subscriber records, malware analysis reports, and the contents of the collector email accounts that were obtained from search warrants.

39. The worm has been in existence since at least 2009 and has been the subject of public reports by cyber security companies, some of which have referred to it as Trojan:W32.Brambul.A, Trojan/Brambul-A, or more commonly, and as it will be referred to in this affidavit, "Brambul." The worm spreads through self-replication by infecting new victim systems via brute force attacks on the victim's Server Message Block ("SMB") protocol. SMB is a method that Microsoft systems use to share files on a network.

40. When Brambul is successful in gaining access to a victim computer, the Brambul worm conducts a survey of the victim machine and collects certain information, including the victim's IP address, system name, operating system, username last logged in, and last password used. That information is then sent via Simple Mail Transfer Protocol ("SMTP") to one or more of the email addresses that are hard-coded in the Brambul worm. The Brambul worm sends that email from a spoofed email address. "Spoofed" in this context means that the email will appear to have come from a particular email address, but in reality, no actual connection or log-in is ever made to the spoofed email address that supposedly sent the message. It is the equivalent, in some ways, of using a fake return address on an envelope.

41. The email accounts programmed into different variants of the Brambul worm that have been used to receive those messages (*i.e.*, to collect those credentials) have varied, but have included xiake722@gmail.com, mrwangchung01@gmail.com, laohu1985@gmail.com, diver.jacker@gmail.com, and whiat1001@gmail.com. One of the more recently active Brambul collector email accounts, mrwangchung01@gmail.com, was accessed from North Korean IP Address #6 in 2017, and the Brambul collector email account diver.jacker@gmail.com was accessed from North Korean IP Address #7 on November 14, 2016 and December 16, 2016. The accounts xiake722@gmail.com and laohu1985@gmail.com were both created within three weeks of each other in 2009 from the same North Korean IP

address (neither North Korean IP Address #6 nor #7). Some variants of the Brambul worm, like the three found at SPE after the attack there, did not contain any email accounts programmed into them.

42. This use of collector emails thus allows the hacker to log-in to one of the collector email accounts that received those credentials and view the emails sent by the Brambul malware, each of which would contain the information necessary to log-in to a victim computer. These victim computers can then be used as hop points by the subjects.

C. Use of a Proxy Service

43. In addition to using the computers infected by Brambul as hop points to conceal their true IP addresses, the subjects have consistently used a set of specific anonymizing services (those specific services used repeatedly are referred to herein as the "Proxy Services").

44. As discussed above, anonymizing services can be used as a "relay" to conceal one's true IP address, and thus one's location, from the websites to which one is navigating. When such a service is used, the website being visited only "sees" the IP address of the proxy, not the user's true "home" IP address. In other words, "Jane" may pay a cable company for internet access, and Jane's home would be assigned an IP address to use when navigating the internet. If Jane were to connect directly from her home to her online email account in order to check her email, her online email provider would see the IP address assigned to her home. If, however, Jane were to use a proxy service to check her email account, her online email provider would only see the IP address of the proxy server connecting to the email account, not the IP address assigned to Jane's home. These proxy services can provide services to a large number of persons and thus have a significant volume of internet traffic relayed through their IP addresses, which would offer

Jane a level of anonymity (though the proxy would still be able to effectively route Jane's traffic to and from the websites she visits).

45. The subjects sometimes used Brambul-infected computers as hop points, sometimes used a proxy service, and other times used (or revealed) their true "home" IP addresses in North Korea without the protection of a proxy or relay. When the subjects have chosen to use an anonymizing service, they have consistently used several specific Proxy Services referenced herein. They have used the Proxy Services to do hacking-related research and to access email and social media accounts, as well as to scan victim computer systems, including SPE's.

46. This affidavit discusses below the IP addresses that the subjects have used to connect to both personal and operational email and social media accounts or to particular websites. In some instances, the subjects connected directly to those accounts from North Korean IP addresses, while on other occasions they connected to such accounts or websites from a North Korean IP address through a Proxy Service. Both methods of connection are referred to below as connections from North Korean IP addresses.

D. Dynamic DNS (DDNS)

47. Some of the malware used by the subjects in connection with their various computer intrusions would contain a domain or domains programmed directly in the malware. The malware would cause the victim's computer to try looking up that domain (or domains) and connecting with the IP address assigned to it. By using DDNS services (as explained above in paragraph 23), the subjects could ensure that when a victim computer "looked up" or tried to resolve a domain in the malware, the victim's computer would be directed to the IP address he or she assigned to that domain, even if a change was made moments before.

48. The domains that appeared in the various families of malware used by the subjects were hosted at multiple DDNS providers. As discussed above, DDNS

providers are companies that offer the ability to register for and use an account to manage a particular domain or sub-domain and control the IP address to which it is assigned (or to which it "resolves"). The subjects registered dozens of accounts at those DDNS providers from the same computer or digital device (*i.e.*, the same piece of computer hardware, such as a laptop, desktop, mobile device, or virtual machine[2] operating on that computer, herein a "device"). The subjects routinely accessed those DDNS accounts directly from North Korean IP addresses, through the Proxy Services, or by other IP addresses located around the world.

49. Some malware used by the subjects in their intrusions employed a variation on the DDNS technique described in paragraph 47. Analysis of that malware has revealed that it would cause a victim's computer to look up the IP address assigned to a specific domain. Instead of connecting to the IP address assigned to that domain, however, it would then cause the victim's computer to perform an additional function once it learned the assigned IP address; that function would generate a new IP address, and the victim computer would then navigate to that *new* IP address. Specifically, once the victim would receive the IP address assigned to the domain, the malware would then perform what is known as an "XOR" operation using a specific hard-coded XOR key; that operation would convert the IP address it received to a new IP address, and the malware would cause the victim computer to connect to that new IP address. Thus, even knowing the domain embedded in the malware would not allow a victim or investigator to learn the location of the computer under the subjects' control without a detailed analysis of how the malware operated and what the XOR key was. This served to conceal evidence of their activities and intrusions.

---

[2] A virtual machine is essentially a "virtual computer" within a computer, with its own operating system running that does not generally interact (at least in the same way) with files stored on the computer on which it is running. A single computer can host multiple virtual machines.

50. The subjects controlled the domains by logging into their accounts at DDNS providers. At times they used North Korean IP addresses to access those DDNS accounts, and North Korean IP addresses were used at times to access social media accounts that were also registered to the email accounts used to register those DDNS accounts.

VI. TARGETING TECHNIQUES USED

A. Reconnaissance

51. In multiple instances, the subjects' successful intrusions were preceded by a period of reconnaissance of their victims on the internet or social media. That online reconnaissance included research relating to the victim company or entity that the subjects were targeting, as well as relating to individual employees of the victim company. The subjects have also used the services of websites that specialize in locating email accounts associated with specific domains and companies, and the subjects have registered for business records search services that offer career postings, business searches, and marketing services. The subjects also have searched for specific software vulnerabilities, exploits, and hacking techniques.

52. Moreover, records produced pursuant to court orders have shown that subjects using North Korean IP Address #6 would visit the websites of some of their intended victims, such as Lockheed Martin, while simultaneously conducting online research about persons associated with Lockheed Martin, and sending messages to employees of Lockheed Martin.

53. While that online research reflected the subjects' operational activities, other online research by those subjects appeared to seek information more personal in nature, including information specific to North Korea, such as related to North Korean television or North Korean food supplies.

B. Spear-Phishing

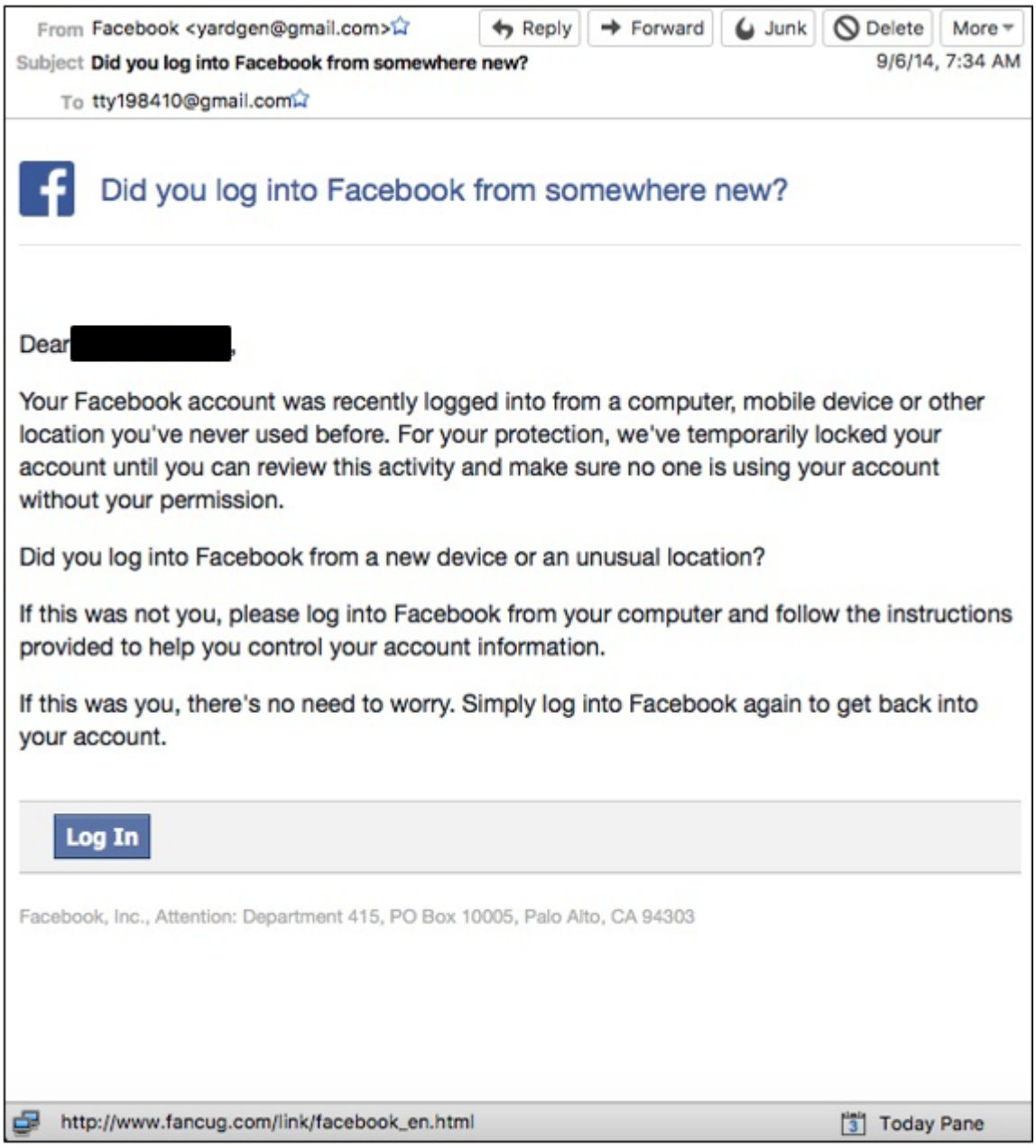
54. As mentioned above, I know based on my training and experience that hackers will search the internet or social media for specific entities or for persons affiliated with those entities as a form of reconnaissance prior to an attempted intrusion. The results of that reconnaissance are often then used by the hackers for "social engineering" when preparing spear-phishing messages to send by email or social media to persons affiliated with those entities. In general, the hackers intend their victims to open the spear-phishing messages while using their employers' computer systems, thus breaching the employers' network security. As noted above in paragraph 33, such spear-phishing emails that are the product of reconnaissance are often highly targeted, reflect the known affiliations or interests of the intended victims, and are crafted—with the use of appropriate formatting, imagery, and nomenclature—to mimic legitimate emails that the recipient might expect to receive. Some of the same accounts were used both to conduct online reconnaissance and to send spear-phishing emails. In some instances those accounts may have been used by more than one person, and thus references to a "user's" or "subject's" use of an account may be the work of multiple subjects using a single account.

55. The FBI has obtained spear-phishing emails from numerous sources. In some instances, they were obtained directly from victims. In others, they were obtained through records and information received pursuant to legal process from providers of internet, email, social media, and other services, including those located in the United States and those located in various foreign countries obtained through Mutual Legal Assistance requests and through law enforcement liaison with foreign authorities (herein referred to collectively as "provider records").

56. On multiple occasions when preparing to target victims, the subjects of this investigation have copied legitimate emails nearly in their entirety when

creating spear-phishing emails, but have replaced the hyperlinks in the legitimate email with hyperlinks that would re-direct potential victims to infrastructure under the subjects' control, presumably in order to deliver a payload of malware to the victims' computers.

57. For example, on occasion Facebook sent legitimate emails to some of the subjects' email accounts alerting them to the fact that a Facebook account associated with that email address was accessed by a new IP address. (In some instances, these emails from Facebook were prompted by log-ins to the subjects' Facebook accounts through a Proxy Service's IP addresses.) Those legitimate Facebook emails contained legitimate links that the user could click to follow-up on the new access to his or her Facebook account. In one instance, however, a subject made an exact copy of that email, shown below, but with slight modifications to turn it into a spear-phishing message. The spear-phishing message included essentially the same formatting as the legitimate Facebook email but with new links associated with the hyperlinked text "Log In" that pointed to http://www.fancug.com/link/facebook_en.html instead of a Facebook-operated website. (The subjects have used multiple domains and URLs in the links directing their intended victims to malware; this is just one example.) The hyperlink was presumably to malicious infrastructure under the subjects' control, but the hyperlink was no longer active when the FBI obtained the email. A subject also changed the name associated with the email account used to "Facebook," and re-sent the email as a test spear-phishing email to an email account associated with the alias "Kim Hyon Woo" (tty198410@gmail.com), which is discussed in detail below. This test spear-phishing email, sent from one account controlled by the subjects to another, seemed ultimately destined for one of the actors in the SPE movie "The Interview" as discussed below, to whose name the test spear-phishing email was addressed (but which is redacted here).



58. In other instances, the subjects created similar test spear-phishing emails purporting to be from Google. One such email claimed to welcome a recipient to Google's Drive remote file storage service, but instead of containing a hyperlink to Google's Drive service, included a link to "http://www.[DOMAIN REDACTED].com/x/o?u=2cfb0877-eaa9-4061-bf7e-a2ade6a30d32&c=374814". This hyperlink was likely an intermediary URL operated by an email tracking company that would direct a user to a malicious file, while also tracking when links

were clicked on so that it could report to the sender that the link was clicked. (As described below, this particular email tracking company is a legitimate company that provides mass mailing/email campaign services for emails sent through certain email services, and which allows a user to see when emails are opened by recipients and when a link inside an email sent through its service is clicked by a recipient.) Another test spear-phishing email a subject sent purporting to be from Google alerted the recipient that "Malicious activities are detected." In that email, the Google hyperlinks that offered information on mitigating possible malicious activities and to Google's terms of services were replaced with presumably malicious URLs unrelated to Google.

59. In other instances, as described in greater detail below in Part IX.A, the subjects created email accounts in the names of recruiters or high profile personnel at one company (such as a U.S. defense contractor), and then used the accounts to send recruitment messages to employees of competitor companies (such as other U.S. defense contractors).

VII. THE ATTACK ON SPE

60. As described below, the attack on SPE became overt in November 2014. It was preceded by a period in which the subjects targeted SPE, its employees, and actors and other personnel associated with the movie "The Interview." That targeting involved internet reconnaissance and spear-phishing messages directed at them beginning in September 2014. After the subjects successfully accessed SPE's network, they exfiltrated data from its network and posted some materials online, continuing to target SPE while also targeting a movie theater company scheduled to release "The Interview" and another production company in the U.K.

A. Initiation of Overt Contact and Email Communications

61. In November 2014, SPE learned that the cyber-attackers had gained unauthorized access to SPE's computer network, stole data, posted some of that data including financial data and the contents of movies online for public download, rendered inoperable thousands of SPE computer terminals, and emailed threatening communications to SPE's executives. The attack disabled significant parts of SPE's computer systems. The following is a summary of the attack. Where emails and messages from the subjects are quoted, the grammatical and spelling errors are in the original messages.

62. On Friday, November 21, 2014, a subject using the name "Frank David" sent an email to high-ranking employees of SPE. The subject line of the email was "Notice to Sony Pictures Entertainment Inc.," and the body of the email stated the following:

> We've got great damage by Sony Pictures.
>
> The compensation for it, monetary compensations we want. Pay the damage, or Sony Pictures will be bombarded as a whole. You know us very well. We never wait long. You'd better behave wisely.
>
> From God'sApstls

63. I learned from records provided by Google that this "Frank David" email account was created on November 21, 2014, the same day the email was sent, from an IP address that is assigned to a Proxy Service. As discussed above, this particular Proxy Service is one that has frequently been used by members of the conspiracy to access their email and social media accounts, and in some instances to connect directly to SPE's network.

64. Three days later, on November 24, 2014, the FBI learned from SPE that when certain SPE employees logged into their computer workstations, a window appeared containing a purported ransom demand. The pop-up window read

"Hacked By #GOP" (later identified through references to the intrusion on social media as "Guardians of Peace") and contained a message that read:

> We've already warned you, and this is just a beginning. We continue till our request be met. We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release data shown below to the world. Determine what will you do till November the 24th, 11:00 PM (GMT).

a. The pop-up window then listed five links. I learned from other FBI agents and from SPE that each of those links contained essentially the same content—specifically, a very long directory file listing, *i.e.*, the list of files stored on a computer server.

b. I have also learned from other FBI agents who have been in contact with SPE that SPE has confirmed that the files reflected in the file directory listing posted on those links matched files stored on SPE's servers. Most of those SPE servers were in Los Angeles County, within the Central District of California.

65. The first SPE workstation that reported the defacement or pop-up window was in the United Kingdom, followed by an SPE call center in Latin America. Given that the intrusion appeared to be spreading worldwide throughout SPE's computers, SPE determined that it needed to disconnect between 7,500 and 8,000 workstations from the internet in order to contain the spread of the intrusion.

66. Also on November 24, 2014, approximately 21 Twitter accounts that were registered and used by SPE were compromised; namely, the SPE content was replaced with messages from the subjects. Some or all of the messages contained the text "Hacked by #GOP" and "You, the criminals . . . will surely go to hell. Nobody can help you." Those messages contained an image showing a "hellish" landscape with skeletons and an altered image of an SPE executive.

67. On November 26, 2014, a subject sent a follow-up email with a subject line of "We Will PUNISH You Completely" to at least four senior SPE employees, which stated:

> I am God'sApstls, the boss of GOP.
>
> We began to release data because Sony Pictures refused our demand.
>
> Sony Pictures will come to know what's the cost of your decision.
>
> We will make Sony Pictures deleted on the list of the Hollywood's Big Six majors.
>
> You are to collapse surely.
>
> Damn to gruel and reckless Sony Pictures!
>
> From the Apostles of God.

68. Approximately 50 minutes after that email, a subject sent a third email to approximately 28 Sony personnel. This email stated it had asked SPE "to pay the monetary compensation for the damage we got and there was no answer. So we hacked to paralyze the network of Sony Pictures warning of the releasing all of the data unless our demand met." The email stated they had already made some movies public, that "[a]ll of the data will soon be released," including "private data," and that they "ha[d] made a firm determination to collapse Sony Pictures." As with the previous email, this email ended, "Damn to gruel and reckless Sony Pictures!," and was signed, "The Apostles of God." I learned from another FBI agent that SPE employees verified that links provided in that email contained data taken from SPE, including SPE's confidential financial records.

69. This third email, like the first email sent on November 21, 2014, claimed to be from God'sApstls, and the sender claimed that God'sApstls was the "boss" of GOP, or Guardians of Peace, who claimed credit for the intrusion publicly in social media.

70. On December 5, 2014, a subject sent a fourth email to numerous SPE employees that stated:

> I am the head of G O P who made you worry.
>
> Removing Sony Pictures on earth is a very tiny work for our group which is a worldwide organization.
>
> And what we have done so far is only a small part of our further plan.
>
> It's your false if you think this crisis will be over after some time.
>
> All hope will leave you and Sony Pictures will collapse.
>
> This situation is only due to Sony Pictures.
>
> Sony Pictures is responsible for whatever the result is.
>
> Sony Pictues clings to what is good to nobody from the beginning.
>
> It's silly to expect in Sony Pictures to take off us.
>
> Sony Pictures makes only useless efforts.
>
> One beside you can be our member.
>
> Our supporters take their action at any place of the world.
>
> Many things beyond imagination will happen at many places of the world.
>
> Our agents find themselves act in necessary places.
>
> Please sign your name to object the false of the company at the email address below if you don't want to suffer damage.
>
> If you don't, not only you but your family will be in danger.
>
> [EMAIL ADDRESS OMITTED]
>
> Nobody can prevent us, but the only way is to follow our demand.
>
> If you want to prevent us, make your company behave wisely.

71. At approximately the same time that this email was sent, an additional set of data that appeared to contain SPE financial data was posted by the subjects to various sites on the internet.

B. Analysis of Malware and Infected Computers and Technical Details of the Intrusion

72. Based on conversations with and on information that I have obtained from FBI computer scientists and from other FBI agents who have received information from SPE, and from FBI and other government reports that I have read about some of the malware used in the attack, I have learned that the malware known as "Destover" that was used against SPE had multiple functionalities, including: (1) it contained a "dropper" mechanism to spread the malicious service from the network servers onto the host computers on the network; (2) it contained a "wiper" to overwrite or erase system executables or program files—rendering infected computers inoperable; and (3) it used a web-server to display the "Hacked By #GOP" pop-up window discussed above and to play a .wav file which had the sound of approximately six gunshots and a scream.

73. I have also learned from analysis of evidence obtained from SPE that one of the pieces of malware contained the names of approximately 10,000 individual SPE hostnames (*i.e.*, the names of specific computer workstations) "hard coded" into the malware. In other words, the subject or subjects who wrote the malware's code had learned and then written into the malware the names of individual SPE computers. Furthermore, among the malware were nine scripts designed to attack computers running Unix or Linux operating systems. Comparison of those scripts to known malware variants showed that four of them appeared to have been derived from other known strains of malware and five appeared to have been written to specifically target SPE's Unix or Linux machines.

74. Based on my training and experience and my knowledge of this investigation, I know that malware that has been customized in these ways was likely the product of a period of sustained covert reconnaissance by the subjects within SPE's network before they launched the attack that disabled SPE's computers.

75. I have also learned that analysis of SPE server logs revealed that a subject using North Korean IP Address #2 conducted a scan of an SPE website server on September 22, 2014, *i.e.*, two months before the attack became overt. Logs also revealed that the same IP address was used by a subject to browse an SPE website at various times between September 22, 2014 and October 30, 2014.

C. Theft of SPE's Data and Distribution by Email and a Social Media Account Created by the Subjects

76. As referenced above, separate from the disruption of SPE's computers and network, there is also evidence that the attackers obtained access to and stole SPE's confidential data.

a. First, as noted above in paragraphs 64–64.b, the subjects posted long directory file listings reflecting the contents of hundreds of SPE servers, showing that they had access to the data.

b. Second, as noted above in paragraph 68, the subjects both sent by email and posted online (using the links provided in email) confidential financial documents related to SPE, which they likely obtained from SPE's compromised computer systems.

c. Third, as explained below, the subjects distributed some of the stolen data through social media. For example, I learned the following from viewing the public Facebook page associated with the "Guardians of Peace" on November 26 and December 1, 2014:

i. The Facebook page claimed to be the "Official Site of The Guardians of Peace (#GOP)." The page contained a picture similar to the "hellish" landscape (containing skulls and an altered image of an SPE executive) that appeared on some of the compromised SPE Twitter accounts discussed above. The page had very little content aside from the images related to GOP and SPE and the links discussed below.

ii. The Facebook page also contained six links under the heading "2014 Movies Download Free HD." Included were movies that had not yet been released to the public.

iii. SPE verified that the copy of "Annie" that was downloaded from the above hyperlink was analyzed and, based on various security features contained within the downloaded film, SPE confirmed that the movie posted online was in fact a copyrighted, pre-release version of "Annie."

77. Additional emails purporting to be from the subjects were sent to SPE employees on December 11, 2014, and new sets of data stolen from SPE were disseminated by the subjects on December 17, 2014.

D. The SPE Movie "The Interview"

78. Once the overt attack was underway, a group calling itself "GOP" or "Guardians of Peace" sent messages claiming responsibility for the attack. On December 8, 2014, a public message appeared on the website GitHub. It was titled "Gift of GOP for 4th day: Their Privacy." The body of the message stated:

> by GOP
>
> We are the GOP working all over the world.
>
> We know nothing about the threatening email received by Sony staffers, but you should wisely judge by yourself why such things are happening and who is responsible for it.
>
> Message to SONY

> We have already given our clear demand to the management team of SONY, however, they have refused to accept.
>
> It seems that you think everything will be well, if you find out the attacker, while no reacting to our demand.
>
> We are sending you our warning again.
>
> Do carry out our demand if you want to escape us.
>
> And, Stop immediately showing the movie of terrorism which can break the regional peace and cause the War!
>
> You, SONY & FBI, cannot find us.
>
> We are perfect as much.
>
> The destiny of SONY is totally up to the wise reaction & measure of SONY.
>
> Their Privacy

79. The post went on to list a password and 20 different links to data stolen from SPE.

80. SPE was scheduled to release the movie "The Interview" in U.S. theaters on December 25, 2014. The plot summary according to IMDB.com is as follows:

> Dave Skylark and his producer Aaron Rapport run the popular celebrity tabloid TV show "Skylark Tonight." When they discover that North Korean dictator Kim Jong-un is a fan of the show, they land an interview with him in an attempt to legitimize themselves as journalists. As Dave and Aaron prepare to travel to Pyongyang, their plans change when the CIA recruits them, perhaps the two least-qualified men imaginable, to assassinate Kim Jong-un.

81. Previously, according to an Associated Press Story issued on December 7, 2014, an unidentified spokesperson for North Korea's National Defense Commission denied responsibility for the SPE attack but stated that it "might be a righteous deed of the supporters and sympathizers" and that the film would "hurt[] the dignity of the supreme leadership of" North Korea.

82. On December 16, 2014, a subject used the website Pastebin to publicly post the following message:

> by GOP
>
> Notice
>
> We have already promised a Christmas gift to you.
>
> This is the beginning of the gift.
>
> Please send an email titled by "Merry Christmas" at the addresses below to tell us what you want in our Christmas gift.
>
> [EMAIL ADDRESSES OMITTED]
>
> Warning
>
> We will clearly show it to you at the very time and places "The Interview" be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to.
>
> Soon all the world will see what an awful movie Sony Pictures Entertainment has made.
>
> The world will be full of fear.
>
> Remember the 11th of September 2001.
>
> We recommend you to keep yourself distant from the places at that time.
>
> (If your house is nearby, you'd better leave.)
>
> Whatever comes in the coming days is called by the greed of Sony Pictures Entertainment.
>
> All the world will denounce the SONY.

83. The FBI learned that a copy of "The Interview" was maintained on a server that was compromised and then rendered inoperable. Unlike the other SPE movies that were "released" by the subjects, the "GOP" never released a pirated copy of "The Interview" on the internet. SPE officially released the movie on

December 24, 2014, through online distribution channels and a very limited number of theater chains that were willing to show the movie.

84. Prior to the cyber-attack on SPE, in the summer of 2014, public statements made through North Korea's official news agency called on the United States to ban the film (though not referring to it by name), calling it "reckless US provocative insanity," and threatening a "resolute and merciless response." In a statement to the United Nations Secretary General, North Korea's ambassador referred to the movie (again not by name) as insulting the supreme leadership and echoed the characterizations of the spokesperson for North Korea's National Defense Commission (*see* paragraph 81). Moreover, the North Korean government sent a letter to the United States National Security Council in October 2014 that stated:

> [T]he trailer of "The Interview" newly edited by the "Harlem Studio" of the United States has still impolite contents of deriding and plotting to make harm to our Supreme Leadership.
>
> We remind you once again that the production of such kind of movie defaming the supreme dignity that our Army and people sanctify is itself the evilest deed unavoidable of the punishment of the Heaven.
>
> . . .
>
> Once our just demand is not put into effect, the destiny of those chief criminals of the movie production is sure to be fatal and the wire-pullers will get due retaliation.

E. Social Media Accounts Were Used to Post Links to Malware on Other Social Media Accounts Related to "The Interview"

85. As set forth in this Part, in the few months preceding the overt attack on SPE, multiple social media accounts sent or posted links that would direct victim computers to a malicious file as a part of the scheme to attack the computer networks of SPE and others associated with "The Interview" movie. These included the Facebook accounts using aliases such as "Andoson David," "Watson Henny," and

"John Mogabe," some of which had been accessed from North Korean IP Address #2 in December 2014.

86. On December 8, 2014, I viewed the "official" Facebook pages of two of the actors in "The Interview," and noted the following.

a. On one actor's page on September 11, 2014, a Facebook account identified as "Andoson David" posted the comment: "Nude photos of many A-list celebrities. http://goo.gl/[REDACTED]."

b. This same comment and link by the same Facebook account was placed on another actor's page a day earlier, on September 10, 2014.

87. The links posted by "Andoson David" on the actors' Facebook pages were hyperlinks created using Google's "url shortener" service, available at http://goo.gl. This program instructs users to input a full or "long URL" and then the program generates a shortened version. As noted in paragraph 34, a shortened URL obscures the actual domain to which it will connect a computer whose user clicks on that link.

88. The FBI has analyzed those two shortened goo.gl links posted to the Facebook pages of actors in "The Interview" and confirmed that they actually contained links to malicious software (*i.e.*, malware). Specifically, the shortened URL http://goo.gl/[REDACTED] would navigate to an executable file located at the URL http://www.[REDACTED DOMAIN].com/Images/Pictures/Graphics/Nude%20Photo%20Gallery.exe, which was hosted on a web server in the United States (the "Compromised Web Server"[3]). The website hosted on the Compromised Web Server was the website of a legitimate company, but the specific resource (*i.e.*, the

[3] The subjects of this investigation have compromised numerous web servers in the United States and internationally. The affidavit refers to other such compromised computers in various places, but this particular web server is referred to as the "Compromised Web Server" throughout the affidavit.

executable file at that link) was not part of the website authorized and made available by the company that operates the website.

89. I learned the following from an FBI computer scientist who analyzed the malware file (whose MD5 hash value is 310f5b1bd7fb305023c955e55064e828, and which the security firm Symantec identifies by the name Backdoor.Destover):

a. When the executable file runs, it runs an actual screensaver called "[REDACTED NAME OF ACTOR[4]]-screensaver-II.exe" which contains approximately ten photos of a female model.

b. While this screensaver is playing, the original executable file runs or "drops" a malicious piece of code called netmonsvc.dll. This malware file, netmonsvc.dll, drops a configuration file called tmscompg.msi, server batch files, and the executable file tmsn.exe. The server batch files are used to erase the installation files once they are executed in order to avoid detection.

c. Once the malware is installed, it begins beaconing out to ten "command and control" IP addresses, likely to maintain a persistent presence on the infected computer and await commands from the attacker. The use of ten command and control IP addresses gives the subjects redundancy in the event one or more of the command and control nodes is taken offline or has the attacker's malware removed. Thus, if the attacker was able to access any of the ten command and control nodes, he or she could continue to issue commands to all machines infected with the malware.

90. As mentioned above, the domain resolved to the IP address of the Compromised Web Server. (Although a comparison of the logs of IP addresses that clicked on "http://goo.gl/[REDACTED]" with the known IP addresses used by SPE at the time of the attack (provided by SPE) did not reveal that anyone clicked on the

[4] This actor was not affiliated with "The Interview."

malicious link from within SPE's network prior to the attack, this appears to be one of the ways the attackers tried to gain access.)

91. Separately, persons claiming credit for the attack periodically sent emails to both SPE executives and to executives at other entertainment companies with a hyperlink from which one could download batches of stolen SPE data. I learned through the investigation that those batches included personally identifying information in one batch, security-related information such as passwords in another batch, and financial information in another batch. Those emails were sent from email accounts that were either "spoofed" (which as mentioned in paragraph 40 means that the email's header information showed a sending address, but that "sending" email account had not in fact sent the email) or from email addresses hosted in other countries.

92. One such email was sent to an executive at another entertainment company on December 5, 2014. I learned that the header information contained in that email showed that the IP address used to send the email was the IP address of the Compromised Web Server.

93. In other words, the Compromised Web Server was not only the place to which links posted by "Andoson David" on Facebook directed computers (where, if users clicked the link, they likely would have been infected with the malware hosted there), but it was also the same computer later used to send emails with links containing data that had been stolen from SPE.

94. This is thus an example of the subjects using a computer they compromised as a hop point—both as a computer where they kept malware used to infect victims, and a computer they used to send email messages with the fruits of their intrusion into SPE.

95. Multiple pieces of malware were found on the Compromised Web Server, one of which was a backdoor. The hash value of that backdoor had already

been identified as part of a family of backdoors. In at least one computer intrusion detected elsewhere in the United States, one variant of this backdoor (*i.e.*, a member of the same family of malware) had been transferred onto the victim computer via a separate piece of malware and had loaded, but not installed, the Brambul malware.

96. In one instance after the attack on SPE had subsided, on May 25, 2015, approximately three minutes after the Compromised Web Server had been accessed by North Korean IP Address #2, that same IP address was used to access the email account amazonriver1990@gmail.com. That user also conducted substantial online research regarding hacking-related topics between May 19, 2015 and September 10, 2015, including related to CVEs, software exploits, and methods of concealing one's IP address. ("CVE" refers to "Common Vulnerabilities and Exposures," which are known software vulnerabilities).

F. "Andoson David," "Watson Henny" and Related Accounts

97. Provider records showed that "Andoson David" was part of a cluster of accounts that engaged in sustained attempts to target SPE beyond the public postings described above.

1. "Andoson David"

98. I visited the Facebook page for "Andoson David" on December 8, 2014. The page contained little except for a photo of a baby, a list of favorite sports teams, and a single favorite movie: "The Interview." Aside from the small public footprint and the postings made with links to malware, "Andoson David" also actively searched for SPE, "The Interview," and related persons while sending malware to them by other means.

99. Specifically, on multiple days between September 2 and October 26, 2014, "Andoson David" conducted online reconnaissance related to SPE and its

employees, "The Interview," and four specific actors and other personnel involved in "The Interview," among other online research.

100. "Andoson David" also conducted online research related to an exploit database on January 8, 2014, related to a U.S. defense contractor on December 3, 2013, and related to Korean Central Television (a North Korean television service) on June 6, 2013.

101. Concurrently with this research, "Andoson David" sent messages to personnel associated with "The Interview" either containing links to malware or simply attaching the malware itself to those messages:

a. For example, on September 2, 2014, "Andoson David" sent a message to the Facebook account of another person involved in the production of "The Interview" that said "Nude photos of many A-list celebrities." The link in that message was to http://www.[DOMAIN REDACTED].com/[RESOURCE REDACTED].htm, which would trigger a download of the same malware that was being stored and hosted on the Compromised Web Server.

b. On September 5, 2014, "Andoson David" sent a Facebook message to the Facebook account for "The Interview" that stated: "[REDACTED NAME OF ACTOR] nude photos were leaked online. As you can see from attached file, somebody made screen saver with the photos." Attached to that message was a compressed file named "[REDACTED NAME OF ACTOR]NudePhotoGallery.zip." The content of that .zip file, when opened, was a copy of the same malware stored and hosted on the Compromised Web Server.

c. That same day, "Andoson David" sent a similar Facebook message to the Facebook account with the name "[REDACTED NAME OF ACTOR] Unofficial" that stated: "Hi, [REDACTED LAST NAME OF ACTOR]... your nude photos were leaked online. As you can see from attached file, somebody made screen saver with the photos." (This "Unofficial" page was, as the name suggests,

not an actual Facebook account of the actor.) Attached to that message was a compressed .zip file with the same name, which also contained a copy of the same malware hosted on the Compromised Web Server.

102. The "Andoson David" Facebook page was subscribed using the email account tty198410@gmail.com, which is an email account, as described in detail in Parts XI.A and XII.B.1, with numerous connections to PARK.

2. "Watson Henny" and "John Mogabe"

103. After the "Andoson David" account was identified, agents and analysts at the FBI identified other social media accounts using similar text and posting the same link (http://goo.gl/[REDACTED]) that would direct computers to the executable malware. One such account was http://facebook.com/WatsonHenny, which, in September 2014, also posted the same goo.gl shortened link on the Facebook pages for the movie "The Interview" and one of the actors in it. The link was also posted with the same text that "Andoson David" used: "Nude photos of many A-list celebrities." The Facebook account listed "interests" that included two of the actors in "The Interview" as well as Sony Pictures.

104. This account was first created using the name "John Mogabe" on September 4, 2014 at 7:54 a.m. PST. Approximately an hour later, the user changed the name from "John Mogabe" to "WatsonHenny." (This account will be referred to herein as the "John Mogabe" Facebook account, given that another Facebook account was created using the name "WatsonHenny," which is discussed below.) The email addresses used to subscribe this Facebook account were watsonhenny@facebook.com, johnmogabe333@facebook.com, and mogbe123456@gmail.com. As its Facebook profile photographs, this Facebook account used both a publicly available photograph of an actual reporter for AOL and Forbes, as well as a photograph of an unidentified woman.

105. On multiple days between September 4 and 30, 2014, the user of the "John Mogabe" account conducted internet reconnaissance regarding many of the same persons and entities as "Andoson David" related to SPE, "The Interview," and some of the same actors involved in "The Interview."[5] Aside from internet research related to hacking and computer exploits on September 17, 2014, the vast majority of online reconnaissance by "John Mogabe" related to SPE, Mammoth Screen (discussed below), and other planned victims.

106. The "John Mogabe" Facebook account also sent a friend request to one of the actors in "The Interview," among others, and "liked" Sony Pictures and two of the actors in "The Interview." Months after the attack, on May 24, 2015, the account "liked" the Facebook page for "Sony Pictures (ID)."

107. The "John Mogabe" Facebook account was accessed by the same device as the "Andoson David" Facebook account on September 7, 9, 10, 11, 24, 25, and 29, 2014. The two accounts were often accessed within minutes of each other. Moreover, both accounts were used to conduct very similar searches, indicating either the same person was using both accounts or they were used by persons working closely in concert.

108. The email mogbe123456@gmail.com was used to subscribe the "John Mogabe" Facebook account. The subject using it conducted online reconnaissance on October 27, 2014 related to SPE personnel and executives, as well as defacements of SPE's website, nearly a month before the attack on SPE became overt. (The image that appeared on the Guardians of Peace Facebook page showed images of SPE executives against a "hell-scape" that showed the word "SONY.") The subject using mogbe123456@gmail.com also researched the email addresses of

[5] Other subjects conducted similar online reconnaissance. These and other subjects were at times in North Korea and at other times in countries in Asia and elsewhere.

a specific SPE executive on November 25, 2014, the day after the attack became overt.

109. Logs show that mogbe123456@gmail.com was accessed primarily from Proxy Service IP addresses, but also from North Korean IP Address #2 on December 3 and 12, 2014, and from two other North Korean IP addresses on August 28, September 3, 2014, and December 2, 2014. This shows the subjects actively had access to North Korean IP Address #2 while also having access to other North Korean IP addresses in nearly the same time period.

110. Separate from the Facebook account identified above that changed vanity names[6] from "John Mogabe" to "WatsonHenny," another Facebook account was created in the name "Watson Henny" using the email account watsonhenny@gmail.com (the "Watson Henny" Facebook account). This "Watson Henny" Facebook account was accessed by the same device as the Facebook account registered to agena316@gmail.com (a user of which, as discussed further in paragraphs 130.b and 159, searched for banks in Bangladesh).

a. Watsonhenny@gmail.com was also used to subscribe the Twitter account @watsonhenny, which followed various media outlets. Watsonhenny@gmail.com used tty198410@gmail.com as its secondary email address (tty198410@gmail.com has a number of connections to Chosun Expo Accounts, as described in detail in Parts XI.A and XII.B), and the two accounts were accessed by the same device on multiple occasions, including multiple times on November 13, 2014, just before the attack on SPE became overt.

b. On September 22, 2014, watsonhenny@gmail.com received an email from messages-noreply@spe.sony.com with a subject of "WatchDox

---

[6] A vanity name is a shortcut or moniker one can create for a Facebook account that allows other Facebook users to more easily find one's profile or navigate directly to it. It need not be the same as the name of the person whose name is used to subscribe an account.

Authentication Email" informing watsonhenny@gmail.com to click on an embedded verification link in order to become a "C2 user." According to the email, a C2 user could send and receive documents and open source information, indicating WatchDox is a file sharing service, which I confirmed from publicly available materials. This is evidence that watsonhenny@gmail.com was used to register for SPE services in the months prior to the attack, *i.e.*, that the malicious account signed up for a service offered by its intended victim, likely as a form of reconnaissance or an attempt to find a means to gain access to its network.

111. In addition to those Facebook accounts, the Twitter account @erica_333u also posted a link to the same malware hosted on the Compromised Web Server. Specifically, on September 10, 2014, the Twitter account @erica_333u posted the comment "Nude photos of many A-list celebrities. http://goo.gl/[REDACTED]" and added in the Tweet the Twitter account @TheInterview as well as the Twitter handles of two of the actors in "The Interview." This Twitter handle shares the "333" with the email address johnmogabe333@facebook.com described above, which was one of the accounts used to subscribe the "John Mogabe" Facebook account that posted the same links to the same malware.

3. <u>"Yardgen"</u>

112. Tty198410@gmail.com—the account used to subscribe the "Andoson David" Facebook page, watsonhenny@gmail.com, and Twitter account @hyon_u (discussed in Part XI.E)—was also accessed by the same device as another email account, yardgen@gmail.com, which was itself accessed by the same device used to access watsonhenny@gmail.com. In particular, both tty198410@gmail.com and yardgen@gmail.com were each accessed by the same device and the same IP address on September 6, 2014. In addition to these connections, a subject using yardgen@gmail.com (1) conducted internet reconnaissance on one of the actors in

"The Interview" (similar to the reconnaissance described above in paragraphs 99 and 105), (2) saved in its contacts email addresses related to two of the actors in "The Interview," and (3) sent the test spear-phishing email that was discussed and depicted above in paragraph 57.

113. The subject using yardgen@gmail.com conducted online research for the email address of one of the actors in "The Interview" on September 6, 2014. (Other research on September 6, 2014 related to certain address information discussed below in paragraphs 122–126.) A subject also conducted internet research using Korean characters on the same day.

114. The address book saved in yardgen@gmail.com contained seventeen email addresses that were variations of the names of three of the actors in "The Interview" at the domains gmail.com or hotmail.com.

115. Furthermore, the address book of yardgen@gmail.com contained approximately fifteen email accounts with the names or variants of actors affiliated with the movie "The Interview," indicating that the user of the account was likely targeting them.

116. Records related to the tty198410@gmail.com account showed further connection to yardgen@gmail.com on that same day, September 6, 2014. Specifically, at 1:31 a.m., tty198410@gmail.com received an email from Facebook addressed to "Andoson David" (the name of the Facebook account that tty198410@gmail.com had registered) alerting the user that the Facebook account had recently been accessed by a new computer or device from a location that had not been used before to access the "Andoson David" Facebook account. The email message contained a "button" at the bottom with a link to log in so that the user could control access to his or her account.

117. Then, as depicted in paragraph 57, at 7:34 a.m., yardgen@gmail.com sent an email to tty198410@gmail.com that appeared almost identical (*i.e.*, as if it

were an email from Facebook) with the following exceptions: it was sent from yardgen@gmail.com instead of from Facebook, but the name on the header had been changed to "Facebook" to make it appear as if it was sent by Facebook; it was addressed to one of the actors in "The Interview," not "Andoson David"; and the "link" in the "button" to log into the Facebook account had been changed to point to a URL that was not affiliated with Facebook. By the time the FBI obtained this message and tested the link, it was no longer active.

118. To summarize, the same person or persons likely used both tty198410@gmail.com and yardgen@gmail.com, and when tty198410@gmail.com received a security alert from Facebook, the user then likely copied and converted it into a test spear-phishing message designed to target one of the actors in "The Interview." The user then likely logged into yardgen@gmail.com from the same device (the accounts were accessed by the same device on September 6, 2014, the day the test spear-phishing message was sent) and used the yardgen@gmail.com to send the test spear-phishing message back to tty198410@gmail.com.

119. Further demonstrating the connection between yardgen@gmail.com and tty198410@gmail.com, three days before, on September 3, 2014, the email account jasmuttly@daum.net sent what appeared to be a test spear-phishing email to tty198410@gmail.com. The email contained a subject of "Invites you to the Hollywood Film Festival in 2014." Embedded in the email was a hyperlink that appeared to direct a person to the website associated with a film festival, but in fact the hyperlink would actually direct anyone that clicked on the link to the malware hosted on the Compromised Web Server.

120. The recovery email for yardgen@gmail.com was jasmuttly@hanmail.net, which shares the same "jasmuttly" "handle" as jasmuttly@daum.net (which sent the test spear-phishing email to

tty198410@gmail.com), just at a different South Korean email service (Hanmail, rather than Daum).

G. Malware Used in Successful Breach of SPE Network

121. Separate from the activities of the accounts described above involved in targeting SPE, a separate spear-phishing email appears to have been successful in gaining access to SPE's network in September 2014. I learned the following from other FBI agents and from SPE:

a. Forensic analysis found seven instances when SPE systems "beaconed" to a specific Chinese IP address between September 26 and October 6, 2014. The SPE user account used to connect with that IP address on six of the seven occurrences was that of a specific SPE employee.

b. A forensic team reviewed the hard drive of the SPE computer used by that employee in December 2014. The review found a spear-phishing email that was sent to that user from the email address bluehotrain@hotmail.com on September 25, 2014, about two months before the attack on SPE became overt. The user of bluehotrain@hotmail.com was listed as "Nathan Gonsalez." The copy of the email was recovered by carving it from a forensic image of the computer, and it contained a link that it asked the recipient to click on.

c. Where the text of the email read "Here is the link," there was a hyperlink to http://1drv.ms/1rvZpFi. The link was no longer active at the time it was found during the forensic review of the computer, but separately a file name of "[REDACTED NAME OF BUSINESS] Advertising Video Clips (Adobe Flash).exe" was found during the forensic review. I have learned, based on my training and experience, that hackers who engage in spear-phishing in order to distribute malware will give their malware files names that distract from the fact that the file is an executable file, *i.e.*, a file with an .exe ending that will install a new program on the computer. In this case, it appears that the words "(Adobe Flash)" were

designed to make the victim believe that he or she would be opening a media file that would play in Adobe's Flash player, when in fact the file was an executable file. Given that the spear-phishing email message referred to a "flash video," it is likely that the user of that computer station clicked the link, which led to the execution of that file by the SPE user's computer.

d. Forensic analysis revealed that this executable file was malware, and that when executed, it caused the infected computer to connect to five hard-coded IP addresses (*i.e.*, IP addresses programmed directly into the malware), one of which was the Chinese IP address referenced above in paragraph 121.a. The malware was programmed to receive commands that could be issued by the attacker that would allow the malware to collect host computer information, delete itself, list directories and processes, collect data in memory, write data to a file, and set sleep intervals. For the reasons set forth in the previous paragraph, this malware appears to be how the subjects gained access to SPE's network.

e. Based on internet searches, I know that there is a legitimate business that uses the name and address of the business (redacted above in paragraph 121.c.) that was listed in the spear-phishing email, and that the name of the executive used in the spear-phishing email is a real person who worked at that business at the time. (The name listed on the bluehotrain@hotmail.com email account at the time that the email was sent was "Nathan Gonsalez," which was not the same as the name used to sign the above-described email, indicating the sender likely was trying to obfuscate his/her true identity or had inadvertently forgotten to change the name on the account to one that corresponded to this spear-phishing email.) I know based on my training and experience that using the name of a real person as the sender of a spear-phishing email is a technique that can lend legitimacy to the email, because if the recipient looks up the sender on the internet, he or she will find confirmation that the "sender" is a real person.

122. Subscriber records for bluehotrain@hotmail.com also contained evidence connecting it to other accounts. Specifically, bluehotrain@hotmail.com was created on September 3, 2014 from a Proxy Service IP address, using the name "Jim Edward," and listing certain address information and a country of "US." But, according to the government records I have reviewed, the address information used to create that account was not valid.

123. That same piece of invalid address information, however, was used in connection with six Microsoft accounts between July and September 2014, one of which was marieperl@outlook.com, which is also discussed in paragraph 128. I know from my experience in cyber investigations that individuals will often intentionally, or sometimes unintentionally, use a particular feature on a recurring basis when they create accounts, and that the re-use of the invalid address information is likely an indication that the same individual or group of individuals created those six accounts at Microsoft.

124. Specifically, accounts using the same invalid address information were created on July 1, August 2, and September 2, 2014, and three accounts (including bluehotrain@hotmail.com) were created on September 3, 2014. All of the accounts, with the exception of two, were accessed using Proxy Service IP addresses, and many of them were accessed within minutes of each other from the same Proxy Service IP address on several days between September and November 2014. Moreover, the accounts were created or often accessed from either a Proxy Service IP address or from an IP address that has been used to create or access other accounts used by the subjects. One of those accounts also registered a Facebook page, the "Moniker 1 Facebook account," and the subject using it searched for employees of AMC Theatres and as well as other topics showing an intent to target SPE in December 2014. That Moniker 1 Facebook account was accessed from a North Korean IP address, and also was accessed by the same device as another

Facebook account, the "Moniker 2 Facebook account," which was also accessed from a North Korean IP address. A subject using the Moniker 1 Facebook account had conducted online reconnaissance of employees of a South Korean power company in March 2015.

125. Four of those email accounts that used the same invalid address information were also used to create Facebook profiles.

126. A spear-phishing email very similar to the one sent by bluehotrain@hotmail.com, referenced above, was sent by lazarex@outlook.com to an SPE employee on October 15, 2014. That email account, lazarex@outlook.com, was created using the same invalid address information, but was also accessed using the same Proxy Service IP address minutes apart from the accounts registered using the invalid address information. That email appeared as follows:

Subject: Getting Recruited By Sony Pictures Entertainment
From: Christina Karsten <lazarex@outlook.com>
Date: 10/15/2014 10:30 AM
To: "[redacted]" <[redacted]@spe.sony.com>

Dear Ms. [redacted],

I'm a sophomore at the University of Southern California and am very interested in graphic design of digital productions.
Mr. [redacted] suggested that I contact you.

Sony Pictures Entertainment has a reputation for excellence, and your commitment to innovative and creative design is near and dear to my heart.

I am a top student in my design program, am maintaining a 4.0 GPA, and have received a merit scholarship every semester since matriculating.
I am confident that I can be an asset to your company.

I would be appreciated if you could view my resume and portfolio.
Here is the link <http://1drv.ms/1qvRPGx>

I look forward to hearing from you.

Sincerely,
Christina Karsten

<http://[redacted]/img/common/img_logo14.png>

127. None of those accounts were accessed in the months after the first "Guardians Of Peace" email was sent on November 21, 2014. That is consistent with these accounts having been used by a person or persons trying to gain initial access to the SPE network through spear-phishing, and not needing to do so again once the network had been breached and other aspects of the attack were implemented.

128. Marieperl@outlook.com was used to register for services at a DDNS provider using the name "Annmarie Perlman" on September 9, 2014, from an IP address located in the United States. This is significant because this same IP address was one that was hard-coded into the malware described above in paragraph 121.d. In other words, once that malware infected a computer, it would cause that computer to connect with that U.S. IP address, which was the same IP address that was being used at the same time to register for DDNS services. This thus shows that the subjects would use a single IP address under their control for multiple purposes.

129. Because of the harmful nature of the attack on SPE in which vast amounts of data were overwritten and computers were rendered unrecoverable, a complete reconstruction of the subjects' activities during the period of the intrusion was not possible through a forensic analysis. Specifically, the harmful component of the attack overwrote the master file table, which is the legend that keeps track of where all of the files on the hard drive are physically stored on the hard drive, and the master boot record, which keeps track of how the hard drive is partitioned and which is needed for "booting" or starting up a computer's operating system. From connection logs, however, it was apparent when SPE's confidential data had been exfiltrated.

H. Targeting Movie Theater Chain

130. As noted above in paragraph 82, the subjects made threats directed at places where "The Interview" would be shown. The FBI has obtained other evidence showing that the subjects did in fact begin targeting movie theaters where "The Interview" was scheduled to be shown. The investigation identified numerous accounts that sent malware to employees of AMC Theatres, one of the theater companies that was scheduled to release and show "The Interview," including the following accounts.

a. [JG NAME REDACTED]@gmail.com:[7] I was first informed by AMC Theatres that this email account had sent an AMC Theatres employee a spear-phishing email on December 3, 2014. I later learned that [JG NAME REDACTED]@gmail.com sent spear-phishing messages to a total of five AMC Theatres employees on that same date. This particular email is characterized as a spear-phishing email because it was sent from an email address using the name of a real AMC Theatres employee to another employee. Moreover, the interests listed on the recipient employee's publicly facing social media accounts included art, and the subject who sent the spear-phishing email referred to art in the message, and asked the real AMC employee to open an attachment containing a screensaver with the sender's drawings. The screensaver was password protected, and the sender stated the password was simply "1." I know based on my training and experience that hackers often send password-protected files so that the files can be sent to targeted victims and, due to being password-protected, anti-virus scanners are often unable to detect malicious code contained in them.

[7] Where the name used to create an email address was the name of a real person, the full name of the person is redacted and the person's initials are used instead. In this instance, the redacted name was the name of a real employee of AMC Theatres.

b. agena316@gmail.com: Agena316@gmail.com was used as a recovery email account for the [JG NAME REDACTED]@gmail.com account. Like [JG NAME REDACTED]@gmail.com, agena316@gmail.com sent spear-phishing messages on December 2, 2014, to two AMC Theatres employees, as well as other emails showing the subjects' intent to target SPE. These messages sent by agena316@gmail.com in particular indicate that the same subjects were responsible for both the attack on SPE and for targeting AMC Theatres. Agena316@gmail.com was also used to register a Facebook account and the subject using it also conducted online reconnaissance regarding employees of AMC Theatres and other movie theaters. As noted above in paragraph 110, the Facebook page created using agena316@gmail.com was also accessed by the same device as the "Watson Henny" Facebook account and, as noted below in paragraph 159, the subject using the account researched banks in Bangladesh.

c. [JP NAME REDACTED]@hotmail.com: Provider records show that the user of this account had saved a spear-phishing message, but not yet sent it, and that message was addressed to an AMC Theatres employee and dated December 2, 2014. That is the same date that agena316@gmail.com sent spear-phishing emails to two AMC employees. This email address was also used to create a Facebook account, and that Facebook account was accessed from the same IP address that accessed Twitter account @erica_333u in late-2014.

d. mogbe123456@gmail.com: As noted in paragraph 108, a subject using this email account conducted online reconnaissance of SPE, its executives, and defacements of SPE's website. On December 11, 2014, mogbe123456@gmail.com sent messages to employees of AMC Theatres with malware attachments titled "MovieShow.zip" and "Attach_File.zip."

e. [JK NAME REDACTED]@gmail.com: On December 13 and 14, 2014, [JK NAME REDACTED]@gmail.com sent spear-phishing emails to employees

of AMC Theatres with malware attachments titled "reference_book.ppsx." This account was created on December 13, 2014 using [JK NAME REDACTED]@outlook.com as its alternate email address, which account was created from North Korean IP Address #2 on December 8, 2014 and accessed from North Korean IP Address #2 and Proxy Service IP addresses on later dates.

131. The FBI has not obtained any evidence from AMC Theatres itself nor from any other sources in the course of the investigation that show any of the subjects' unauthorized intrusion attempts at AMC Theatres were successful.

I. Intrusion at Mammoth Screen

132. In 2014, Mammoth Screen, a British production company, had been producing a show titled "Opposite Number," fictionally set in North Korea. In August 2014, it was announced that the series was "greenlit," meaning it would be financed and proceed towards production. According to Mammoth Screen's website, the show was a ten-part fictional series about a British nuclear scientist on a covert mission who was taken prisoner in North Korea.

133. According to multiple publicly available articles, a spokesman for the Policy Department of the National Defense Commission of the DPRK issued a statement on August 31, 2014, in which the spokesman derided the U.K. series and claimed that "[r]eckless anti-DPRK hysteria would only bring disgrace and self-destruction" and that "[i]t would be well advised to judge itself what consequences would be entailed if it ignores the DPRK's warning." These comments by the North Korean government are similar to comments made by the subjects prior to the November 2014 cyber-attack against SPE.

134. Between September 4 and 11, 2014, the subject using the "Andoson David" Facebook account conducted online reconnaissance about the "Opposite Number," including about the producers and other personnel listed on Mammoth

Screen's website (sometimes minutes or seconds before or after conducting online reconnaissance regarding SPE and "The Interview").

135. Between September 7 and 19, 2014, the subject using the "John Mogabe" Facebook account conducted some of the very same online reconnaissance that was conducted by the subject using the "Andoson David" Facebook account eight days earlier. "John Mogabe" also "liked" another production company associated with the "Opposite Number."

136. As of January 21, 2015, watsonhenny@gmail.com's stored address book had saved in its contacts seventeen email addresses for Mammoth Screen personnel (each using the domain mammothscreen.com). Those same seventeen Mammoth Screen email addresses were also stored in the South Korean email account jasmuttly@daum.net (*see* paragraphs 119–120).

137. Additionally, a subject created a LinkedIn account for "henny watson" using the email address watsonhenny@gmail.com, and used it to send multiple invitations to join "henny watson's" network. Among the recipients of those messages were the LinkedIn accounts subscribed using five of the Mammoth Screen email addresses saved in watsonhenny@gmail.com's address book.

138. Although evidence collected shows that an intrusion occurred, it was detected and subsequently remediated. However, as noted below in paragraph 166, an IP address registered to Mammoth Screen tried to look up a domain under the control of the subjects between January 23 and March 7, 2016.[8]

VIII. INTRUSIONS AT FINANCIAL INSTITUTIONS

139. As described below, at around the same time that the subjects were targeting and carrying out the attack and intrusions at SPE, Mammoth Screen, and AMC Theatres, they also began targeting financial institutions with the goal of

[8] I received information indicating that, after the "Opposite Number" was initially greenlit, the show was not produced because it was determined to be commercially unviable for reasons unrelated to the intrusion.

stealing money from those banks. These intrusions were carried out using some of the same accounts for spear-phishing and targeting, and used malware that shared similarities with the attacks on SPE and other victims, showing that that they were part of the same conspiracy by the same subjects, including PARK.

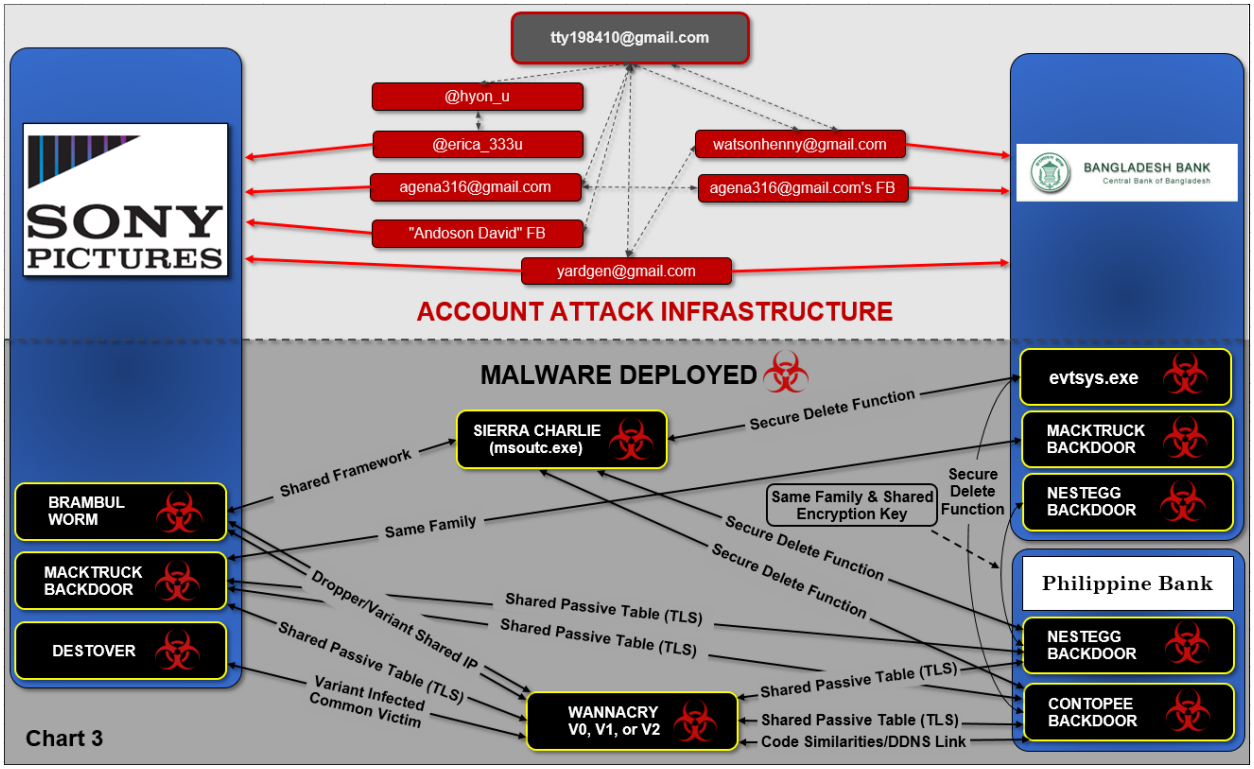
140. The intrusions generally proceeded by targeting the local networks of individual banks, which banks use the SWIFT system to communicate payment instructions. SWIFT is the Society for Worldwide Interbank Financial Telecommunication, a consortium of international financial institutions that manages a global communication network. SWIFT facilitates 24-hour secure international exchange of payment instructions between commercial banks, central banks and other financial institutions.

141. The intrusions of financial institutions generally began with online reconnaissance by the subjects related to an individual bank. The subjects would then send spear-phishing messages to employees of the bank, as well as email or social media addresses associated with that specific bank. Once a spear-phishing message had been successful and the subjects had gained access to the bank's computer network, they moved through the bank's network in order to access one or more computers that the bank used to send or receive messages via the SWIFT communication system. With access to that computer, the subjects were able to impersonate bank employees who were authorized to create and transmit messages through the SWIFT system on behalf of that bank, making those messages falsely appear as if they were authorized by employees of the bank.

142. The subjects executed the heists by crafting and sending real but fraudulent SWIFT messages—*i.e.*, authenticated messages sent from the victim bank's computer systems that were being remotely accessed to construct the messages, but which messages were not actually authorized by the victim bank. In addition to gaining access to the computers that interfaced with the SWIFT system

and then preparing and sending the fraudulent SWIFT messages, the subjects also took measures to conceal their activities and cover their tracks. Specifically, as part of transactions conducted using SWIFT, many financial institutions typically both generate a document confirmation (either in hard copy or as an Adobe PDF file) and use an Oracle database to retain a record of messages sent using SWIFT. The subjects here used malware that interfered with each of those processes at the victim banks (presumably to avoid alerting the victims of the subjects' activities), and then used other malware to delete evidence of those concealing activities. Some of those malware-based measures used to conceal their activities have connections to the malware used against SPE and other victims. Moreover, some of the very same accounts were used to target Bangladesh Bank as were used to target some of the other victims discussed above, including SPE.

143. Victims of these intrusions that have been linked to each other—and to the attack on SPE—have included Bangladesh Bank, as well as a bank Vietnam (the "Vietnamese Bank"), a bank in the Philippines (the "Philippine Bank"), a bank in Africa (the "African Bank"), and a bank in Southeast Asia (the "Southeast Asian Bank"). Connections between the attacks on SPE, the intrusions at Bangladesh Bank and the Philippine Bank, and the WannaCry ransomware malware (described below in Part X) are depicted in Chart 3, which connections include common accounts used for spear-phishing and common elements in the malware used in the intrusions.



A. Background Regarding Bangladesh Bank Cyber-Heist

144. In February 2016, Bangladesh Bank became the victim of a computer intrusion and cyber-heist that caused a loss of approximately $81,000,000, with an attempted theft that approached $1 billion. As a result of the intrusion, approximately $81,000,000 was routed to accounts in the Philippines, and $20,000,000 was routed to an account in Sri Lanka. The $20,000,000 sent to Sri Lanka was stopped by the recipient bank and the money never reached the intended recipient. The $81,000,000 that was successfully transferred to the accounts in the Philippines was subsequently laundered through multiple bank accounts, a money remitting business, and casino junkets.[9] The majority of the $81,000,000 has not been recovered to date.

[9] None of the accounts in the Philippines that received or laundered those fraudulently transferred funds were held at the Philippine Bank that was the victim of a computer intrusion that resembled the intrusion at Bangladesh Bank.

145. The hackers were able to gain access to Bangladesh Bank's computer terminals that interfaced with the SWIFT communication system, and then craft, authenticate, and send SWIFT messages that appeared to be authentic and originating from Bangladesh Bank's own computer system. Each of those SWIFT messages directed the Federal Reserve Bank of New York ("FRBNY") to transfer funds from Bangladesh Bank's account held in U.S. dollars there to the specified accounts in the Philippines (and Sri Lanka) via specific U.S. correspondent banks.

146. The $81,000,000 that was successfully transferred was sent to bank accounts that had been created in the Philippines in May 2015 in the names of fictitious persons. The fraudulent SWIFT messages sent from Bangladesh Bank's computer systems included the (fake) names and (real) account numbers of the specific accounts that had been created in May 2015.

147. Evidence subsequently discovered has shown that the targeting of banks in Bangladesh by the subjects began as early as October 7 and 8, 2014, *i.e.*, before the attack on SPE became overt and more than a year before the cyber-heist at Bangladesh Bank. The subject using [MONIKER 3 REDACTED]@gmail.com[10] conducted online reconnaissance regarding specific banks in Bangladesh that the subjects later targeted with spear-phishing messages, including by visiting some of their websites. A subject later did online research about the central bank of Bangladesh (*i.e.*, Bangladesh Bank) and on another bank in Bangladesh in February and October 2015, respectively, each of which were also targeted with spear-phishing emails by the subjects. Mobile devices that were connected to

[10] In April and May of 2015, a DPRK person who was not PARK used watsonhenny@gmail.com to communicate with an individual in Australia about shipments of certain commodities to North Korea. That person, at least at some points, also appears to have used the email account [MONIKER 3 REDACTED]@gmail.com. Some of those communications are described generally in paragraph 276.

[MONIKER 3 REDACTED]@gmail.com were accessed from North Korean IP Address #3 in July, August, September, October, and November 2014, and January 2015.

148. The FBI's investigation, including its analysis and examination of digital devices and electronic evidence received from Bangladesh Bank, identified four key accounts used to target and infiltrate Bangladesh Bank: watsonhenny@gmail.com, yardgen@gmail.com, and two accounts connected to them, rasel.aflam@gmail.com and rsaflam8808@gmail.com. The spear-phishing emails from each of those four accounts were nearly identical (in some versions the words "and cover letter" were removed, and the links varied, as noted in some of the descriptions below) and read as follows:

> I am Rasel Ahlam.
>
> I am extremely excited about the idea of becoming a part of your company and am hoping that you will give me an opportunity to present my case in further detail in a personal interview.
>
> Here is my resume and cover letter. Resume and cover letter <http://www.[DOMAIN REDACTED].com/CFDOCS/Allaire_Support/rasel/Resume.zip>
>
> Thank you in advance for your time and consideration.

149. As discussed below, these links may have hosted the malware that allowed the subjects to gain initial access to the computer network of Bangladesh Bank.

150. In addition to the similar spear-phishing messages sent from each account, the same or similar hyperlinks at the same domain used in each message, and the overlap of the banks in Bangladesh that were the intended recipients, there are other connections between these accounts and others described above that show they were used as part of the same overall conspiracy. Those connections, showing that the intrusion at Bangladesh Bank was part of a campaign targeting multiple

banks that was in turn part of the same overall conspiracy that had also attacked SPE, are discussed below.

B. Malicious Accounts Used

151. The following sections discuss the malicious email and social media accounts that the subjects used to target Bangladesh Bank, as well as the subjects' use of those accounts in the targeting of and intrusions at other victims.

1. watsonhenny@gmail.com

152. As discussed above (*e.g.*, paragraphs 110–110.b and 136), watsonhenny@gmail.com is the account that used tty198410@gmail.com as a secondary account and that was also accessed by the same device as tty198410@gmail.com. Further watsonhenny@gmail.com is also the account that signed up for an SPE file-sharing service, that saved contacts in its address book for Mammoth Screen employees, and that was used to create a LinkedIn account that sent invitation requests to Mammoth Screen employees.

153. In addition to the Mammoth Screen employees' email addresses stored in watsonhenny@gmail.com's address book, by June 24, 2015, the account also had thirty-seven email addresses of personnel at Bangladesh Bank saved in its address book. These email addresses ended with "@bb.org.bd," the domain of Bangladesh Bank domain.

154. Moreover, in addition to the LinkedIn invitations that watsonhenny@gmail.com's LinkedIn account sent to Mammoth Screen employees (*see* paragraph 136), that account also sent a LinkedIn invitation to the LinkedIn account associated with a Bangladesh Bank employee, whose contact was also stored in watsonhenny@gmail.com's address book.

2. yardgen@gmail.com

155. As discussed above, a subject using yardgen@gmail.com researched the email account of one of the actors in "The Interview," saved contacts in its address

book for two of the actors in "The Interview," and sent a test spear-phishing email addressed to the name of one of those actors to tty198410@gmail.com.

156. On January 29, 2015, a subject using yardgen@gmail.com conducted online research about cover letters and hacking-related topics like PDF exploits and certain CVEs.[11]

157. On January 29, 2015, yardgen@gmail.com sent 10 email messages to sixteen different email addresses of employees of Bangladesh Bank. Each of those messages purportedly sought an employment opportunity. In the emails, the following link was included, which purported to contain a résumé: http://www.[DOMAIN REDACTED].com/CFDOCS/Allaire_Support/ahlam/Resum.zip. Forensic analysis regarding that link is discussed in paragraph 164.a.

158. On February 23, 2015, yardgen@gmail.com sent two email messages to ten recipients at Bangladesh Bank, which were identical to the email described above in paragraph 148, except that the "linked" text displayed only "Resum.zip" (but if clicked on, it would take the computer to the same URL or website discussed in the previous paragraph).

159. Among the recipients of those emails sent by yardgen@gmail.com was a specific Bangladesh Bank email address (ending in bb.org.bd). On January 27, 2015 (*i.e.*, approximately one month earlier), a subject who used the Facebook account registered using agena316@gmail.com conducted online research about that email address and that Bangladesh Bank employee, along with online research related to Bangladesh Bank and bankers in Bangladesh. (As described above in paragraph 130.b, agena316@gmail.com sent spear-phishing email messages to recipients at both SPE and AMC Theatres.) Moreover, a subject using that same

[11] A person using the same account also conducted research that same day related to the Department of Justice and the Foreign Agents Registration Act (*i.e.*, FARA).

Facebook account—registered to agena316@gmail.com—also conducted online reconnaissance related to SPE during the previous month, on December 7, 2014, and AMC Theatres on November 30, 2014.

3. rsaflam8808@gmail.com

160. The email account rsaflam8808@gmail.com was registered using the name "Aflam Rasel" and used a recovery email address of watsonhenny@gmail.com, used the Korean language setting, had been accessed using a Proxy Service, and was disabled on August 12, 2015 (just after sending the spear-phishing emails described below). Rsaflam8808@gmail.com was also accessed from an Indian IP address on August 12, 2015, which IP address was also used to access mrwangchung01@gmail.com (one of the Brambul collector email accounts) on February 23, 2015. Additionally, the account rsaflam8808@gmail.com was accessed by a device that also accessed mrwangchung01@gmail.com (as noted below in paragraph 162).

161. On August 11, 2015, rsaflam8808@gmail.com sent a message to another Bangladesh-based bank (not Bangladesh Bank). The content of this email was the same as the emails sent by yardgen@gmail.com to employees of Bangladesh Bank, as discussed in paragraphs 157–158, but the link was as follows: http://[DOMAIN REDACTED].com/CFDOCS/Allaire_Support/Ahlam/Resume.zip (including the "e" after "Resum"). The name of the purported sender of this email, "Rasel Ahlam," appeared in the body of the email and appeared to be an inadvertent misspelling of "aflam," which was used in the email address itself.

4. rasel.aflam@gmail.com

162. Rasel.aflam@gmail.com was registered using the name "Rasel Aflam." On August 11, 2015, it was used to send what appeared to be two test spear-phishing emails to the email account mrwangchung01@gmail.com—the body of which appeared the same as the message quoted above in paragraph 148. As noted

above in paragraph 41, mrwangchung01@gmail.com is one of the Brambul collector email accounts, it was accessed from North Korean IP address #6, and it was accessed by the same device used to access rsaflam8808@gmail.com (and registered to "Aflam Rasel"), tty198410@gmail.com, and watsonhenny@gmail.com. Specifically, the day after the test spear-phishing email was sent, on August 12, 2015, a device used to log into watsonhenny@gmail.com was also used to log into mrwangchung01@gmail.com.

163. On August 11 and 12, 2015, rasel.aflam@gmail.com sent twenty-five spear-phishing messages to employees of multiple Bangladesh-based banks. The text of each of the emails was the same as the email quoted above in paragraph 148, but the linked text displayed "Resume and cover letter" and the hyperlink was updated to: http://www.[DOMAIN REDACTED].com/CFDOCS/Allaire_Support/rasel/Resume.zip (replacing "ahlam," which appeared in some of the messages described above, *e.g.*, paragraph 161, with "rasel").

C. Results of Forensic Analysis

164. After the compromise of and cyber-heist from Bangladesh Bank, forensic review and analysis revealed the following:

a. At least three Bangladesh Bank computers had attempted to download the file "http://www.[DOMAIN REDACTED].com/CFDOCS/Allaire_Support/Ahlam/Resum.zip"—*i.e.*, the same link sent by yardgen@gmail.com—between January 29 and February 24, 2015. The users of two of those computers corresponded to two of the addressees to which yardgen@gmail.com sent a spear-phishing email. The user of the third computer corresponded to one of the contacts saved in the address book of watsonhenny@gmail.com. This shows that, as with the subjects' cyber-attack on

SPE, the subjects were successful in causing recipients at Bangladesh Bank to download the payload from their spear-phishing emails.

b. Subsequently, in March 2015, that analysis showed that the subjects had moved within the Bangladesh Bank network and had saved a file that was a backdoor that communicated over a custom binary protocol designed to look like "TLS" traffic. That malware was capable of performing file transfers, creating .zip archives, and executing certain files. It had three IP addresses hard-coded (*i.e.*, programmed) into it.

i. I know, based on my training and experience, that "TLS" or "Transport Layer Security" is a cryptographic protocol that is used to increase the security of communications between computers. The "FakeTLS" signature that is referenced is a protocol that mimics authentic encrypted TLS traffic, but actually uses a different encryption method.

ii. By utilizing "fake" TLS, many computer network intrusion detection systems will ignore the traffic because they assume the contents cannot be decrypted and that the traffic is a common communication protocol, allowing the hackers to carry on communications without tripping security alerts.

iii. As discussed below in paragraphs 170.c and 183–183.d, a fake TLS communication protocol is a common technique used in Lazarus Group malware. Thus, the malware used in March 2015 shared this and other traits with the Lazarus Group, and the spear-phishing emails above that sent the link that was clicked on in January were sent by one or more subjects, *i.e.*, members of the Lazarus Group.

c. Nearly a year later, on January 29, 2016, days before the fraudulent transfers were made, the subjects engaged in a number of lateral movements throughout the network, including from the computer where they had installed a file that communicated by mimicking TLS traffic. One of those moves

was to Bangladesh Bank's SWIFTLIVE system. That system was the core component of Bangladesh Bank's SWIFT processing environment. It used the SWIFT Alliance Access application, which was a customer-managed gateway to the SWIFT network that transmitted and received messages from other banks that create and confirm financial transactions. As the application received SWIFT messages, it would record local copies of the messages, including by formatting and printing those messages to files or a printer and by entering information associated with them in a separate database.

d. As the hackers tried to move onto the Bangladesh Bank computer hosting the SWIFTLIVE system, they made at least four attempts to log-in to it. The subjects had successfully deleted some evidence of their attempts to log-in to Bangladesh Bank's SWIFTLIVE system, but left some evidence that was later found during the forensic examination. Significantly, one of those log-in attempts (that presumably was not successful) used the name of a specific currency exchange business in South America (the "South American currency exchange"). Bangladesh Bank has confirmed that no account or credentials with that name resided on its system.

165. Separately, that South American currency exchange had already been targeted by the same subjects, and thus the attempt to use credentials associated with it was likely an error by the subjects who were conducting or managing multiple intrusions at the same time and remotely accessing Bangladesh Bank's computer systems. As described below, this shows that the subjects who were carrying out the intrusion in Bangladesh Bank were the same ones targeting the South American currency exchange. Domains used to target both Bangladesh Bank and the South American currency exchange were managed by accounts that were controlled by the same device or group of devices, and that those DDNS domains were controlled by North Korean IP addresses.

a. Specifically, an IP address assigned to the South American currency exchange was observed trying to resolve or "look up" the specific domains mones.biz.tm, pubs.ignorelist.com, and lakers.crabdance.com, between December 11, 2015 and March 14, 2016. Those domains were controlled by a DDNS provider, and two particular accounts at that DDNS provider managed those and certain other domains. Moreover, that DDNS provider had identified a number of accounts that were accessed by the same device or devices, which each in turn controlled a number of domains. (Thus one computer was being used to manage dozens of domains.) Although the FBI's local legal attaché had notified the South American currency exchange of the possible breach through its local counterparts, it is not known precisely what caused the resolution request or the attempt to "look up" that domain—*e.g.*, a piece of malware being executed or used on the currency exchange's computer, or network or IT security personnel (or automated network security services) testing a link contained in a file found on its systems.

b. Two other domains, mlods.strangled.net and bepons.us.to, were, along with mones.biz.tm, pubs.ignorelist.com, and lakers.crabdance.com, under the control of DDNS accounts that were accessed (and thus controlled) by the same device. The former two domains were found in a forensic review of a computer at Bangladesh Bank that was compromised during the intrusion. The domains were found by the FBI in a memory "dump" that was captured as the result of an application that crashed or failed on January 27, 2016. The application likely crashed as a result of activity conducted by the hacker while he or she was removing some traces of malicious activity from the computer, and thus the manner in which the domains had been used could not be determined. But the fact that these domains—which are distinct and not commonly trafficked websites—were found on a Bangladesh Bank computer, which domains were being controlled by the same computer that also controlled the domain that the currency exchange tried to

"look up," shows that both Bangladesh Bank and the South American currency exchange were victims of the same group of subjects.

c. Also among the domains controlled by those DDNS accounts accessed from the same device were statis.ignorelist.com and repview.ignorelist.com. These two domains were embedded in malware found at the Philippine Bank. The Philippine Bank was the victim of an intrusion, but one that did not result in the fraudulent transfer of funds. The malware used in connection with that intrusion at the Philippine Bank was similar to the malware used against Bangladesh Bank, as discussed below in Part VIII.D.

166. Another domain under the control of the connected DDNS accounts controlled by the subjects was bitdefs.ignorelist.com. Among the IP addresses that had tried to resolve or "look up" that domain was an IP address assigned to Mammoth Screen, the U.K. production company, between January 23 and March 7, 2016.

D. Comparison of Malware Used and Other Targeted Banks

167. Aside from Bangladesh Bank, the subjects targeted and in some instances were successful in gaining access to multiple other banks in multiple countries. This Part describes the connections between some of those other victims and intended victims, including through the malware that was used to carry out the intrusions. There have been multiple different types of connections between the malware used at some or most of the victims, including use of the same family of malware at different victims, a shared "framework" used for different types of malware used in the intrusions, a "secure delete" function that appeared in different types of malware at different victims, a common data table embedded in the malware used in connection with multiple victims, a DNS function that calculated a command and control IP address based on the result of "looking up" an IP address assigned to a domain the subjects controlled, similar encryption keys, and domains

under the common control of the subjects to which they caused their victims' computers to connect.

168. The malware files used against each of the victims did not share all of these traits. Moreover, each trait examined alone might not foreclose the possibility that source code had been shared or sold. But when evaluated collectively, the number and strength of the connections between the malware used against these victims shows that the malware used in these intrusions was the work of a group of persons who had access to the same library of source code and were thus working collaboratively and in concert. These connections are separate from, and in addition to, the overlap in the accounts used to target victims through reconnaissance and spear-phish some of the same victims, and the overlap in the other infrastructure used to control and carry out the intrusions.

1. Families of Malware

169. The subjects of the investigation have used several distinct "families" of malware to conduct their computer intrusions. That is, although samples of malware within these families are not identical to each other, cyber security companies have identified key features and characteristics that allow the specific classification of malware into narrowly defined categories, each of which has been given a name by the company analyzing it. Malware samples belonging to the same family are likely created by the same group of programmers with access to the same source code.

170. I know the following about families of malware used by the subjects of the investigation based on both public and private reports written by cyber security companies, as well as from analysis by an FBI computer scientist of the malware and forensic images of computers from victims:

a. "Contopee" is a backdoor observed in several computer intrusions of banks, including the intrusions at the Philippine Bank and the same

Southeast Asian Bank referenced in paragraph 143. Contopee can gather information about a compromised computer, as well as to start and stop other programs on the computer, and upload files to and download files from the computer. Many Contopee samples communicate with a DDNS domain for command and control via port 443.[12] In such samples that have been identified by the FBI, the DDNS domains used were linked to accounts controlled by the subjects of the investigation, as described in paragraph 48. Examples of DDNS domains found to be embedded in Contopee samples analyzed by the FBI are tbs.fartit.com, ovhelp.mrbasic.com, and onlink.epac.to.

b. "NESTEGG" is a backdoor that was used in connection with intrusions at financial institutions, including at Bangladesh Bank. NESTEGG exists "in memory"; that is, the malware runs in the computer's memory without existing on the hard drive. In order to install NESTEGG, the hacker first places an executable program (generically called a "dropper") that contains an encrypted payload on the target system's hard drive. The hacker then runs the dropper with a command that includes a password, instructing the dropper to decrypt the payload using the MD5 hash of the password, store it on the hard drive, register it as a Windows service (a type of program that runs outside the user's view), and start the service. This service is a second dropper that contains another encrypted payload; the second dropper decrypts its payload using the same MD5 hash and loads it into the memory of the computer. This second decrypted payload continues to run as an

[12] In addition to the IP addresses used to route traffic on the internet, internet traffic also includes a "port." Once the right IP address is located and the traffic is routed there, the port is effectively a channel that allows the computer to separate different kinds of internet traffic based on different types of communication protocols. For example, web browsers often communicate over port 80 or 8080, secure web browsing often occurs over port 443, and certain email protocols use port 25, 110, or 143. Traffic to port 443 may be legitimate TLS traffic or it may appear to be TLS traffic when in fact it is not.

executable program from the computer's memory, and functions as the NESTEGG backdoor. Furthermore, the program copies the second dropper to the computer's memory before securely erasing it from the computer's hard drive and deregistering the service so that it is difficult for cyber security experts, forensic examiners, or security software to detect its existence. Once NESTEGG is running on a system, it listens for commands on a specific port. It is capable of acting as a proxy to send commands to other infected systems, and accepts commands to upload and download files, list and delete files, and list, start, and terminate processes. Because a computer's memory is cleared when the computer is shut down, NESTEGG attempts to detect when the computer is being shut down. In that case, NESTEGG will copy the second dropper from the computer's memory to the hard drive and register it as a Windows service again, to ensure that the second dropper is re-run the next time that the computer is powered on so that it reinstalls NESTEGG.

c. "MACKTRUCK" is a backdoor, and variants of it were used in both the attacks against SPE and Bangladesh Bank. It uses the FakeTLS protocol referenced above in paragraph 164.b.i and described in more detail below in paragraphs 183–183.d to communicate with a hardcoded list of servers via port 443 for command and control.

171. In addition to the shared code used in the malware discussed below, an analysis of the malware found on the computer systems of financial institutions that were victims of the subjects, and of the connection logs at those victims, has shown that the subjects used a number of IP addresses as command-and-control IP addresses to carry out the intrusions. In addition to those banks mentioned here, the subjects have targeted and in some cases successfully infiltrated other banks, but in those cases the intrusions were detected before the subjects were able to

effect fraudulent transfers from those victim banks or the fraudulent transactions were eventually reversed.

2. Use of NESTEGG

172. One of the pieces of malware found on Bangladesh Bank's network that the subjects used in the heist was NESTEGG. Throughout the intrusion, the NESTEGG dropper was consistently named "hkcmd.exe." I know based on my training and experience that hackers will often name a malicious file with the same name as a non-malicious file that is routinely found on computers in order to attempt to conceal that the file is malicious. Here, hkcmd.exe is also the name of a legitimate utility file published by Intel Corporation that is deliberately and legitimately placed on many computers during the process of their manufacture.

173. Forensic analysis at Bangladesh Bank showed that NESTEGG was used on January 20, 2016—specifically, that a task was scheduled to install NESTEGG (hkcmd.exe) using the password nf300karjfs9e8rhtQJ3u9gh. According to the command syntax, the password was then "hashed" using the MD5 algorithm, and the result was used as a key to decrypt two specific resources. Forensic analysis showed that, about 30 seconds later, the firewall was modified to allow inbound access using a specific port, and then shortly afterward malware used that port to begin accepting commands.

174. The FBI has received information from a foreign investigative agency indicating that the command used to install the particular NESTEGG dropper (hkcmd.exe) used in Bangladesh Bank matched a piece of malware with the same name (hkcmd.exe) that the foreign investigative agency had obtained from an investigation of a separate hacking incident by North Korean subjects. Both hkcmd.exe files decrypt another piece of malware, and then execute it in memory, rather than storing it as a file on the hard drive of the compromised computer.

175. Most significantly, the hkcmd.exe file found by the foreign investigative agency in the other North Korean hacking incident used a lengthy password, and the majority of the password was identical to the password used in the Bangladesh Bank intrusion. Specifically, the password (which is hashed to generate the key) that was used to install NESTEGG at Bangladesh Bank was nf300karjfs9e8rhtQJ3u9gh, and the password used in the hkcmd.exe file found in the separate North Korean hacking incident was f200karjfs9e8rhtQJ3u9gh (underlining added for emphasis). This password is a value that can be chosen by the hacker and, as noted in paragraph 188.a, had not been publicly published on the internet or through other publicly available sources at the time of either incident; it is therefore highly improbable that the two passwords would randomly contain that identical string of characters. Furthermore, as detailed below in paragraph 188.a, the same password as the one used at Bangladesh Bank was used to install NESTEGG at the African Bank, and another sample of the NESTEGG dropper that used the same password was recovered from a bank—the same Southeast Asian Bank referenced in paragraph 143—that was a victim of a computer intrusion in late 2016.

176. The FBI's examination of the computers that were compromised at the Vietnamese Bank in late 2015 found forensic artifacts on the computers left behind from the subjects' activity that showed that a file with the name hkcmd.exe had been executed on the compromised computer. That is the same name of the NESTEGG dropper that was used in the intrusion at Bangladesh Bank and in the separate North Korean computer intrusion discussed above in paragraphs 174–175. The file was no longer stored on the computer, indicating that the subjects had deleted it in an attempt to conceal their activities, and it had also been securely deleted, likely using the procedure discussed below in paragraph 179.b. Although, as detailed above in paragraph 172, hkcmd.exe is the name of a file that can serve a

legitimate function on Windows systems, because it was executed from a non-standard location on the computer and was securely deleted, it likely contained malware used in furtherance of the intrusion.

177. It should be noted that the malware used is not the only connection to be drawn between the intrusions at the Vietnamese Bank, Bangladesh Bank, and elsewhere carried out by the subjects. Specifically, the user of an account that was accessed from North Korean IP Address #5 previously researched the Vietnamese Bank, visited the Vietnamese Bank's website, researched the BIC code for the Vietnamese Bank, and researched the BIC code used by a correspondent bank needed to carry out one of the intended fraudulent transfers from the Vietnamese Bank.[13] That research was conducted in late 2015 before the unauthorized SWIFT messages were sent in December 2015. The user of the account also researched the time zone of a correspondent bank that the subjects intended and attempted to use for a fraudulent transfer from a victim bank in 2016, days before the cyber-heist there. The user of the account also visited a SWIFT online user guide and conducted research on various hacking-related topics, including brute force attacks and hacking banks.

3. Secure Delete Function: Connections Between Intrusions at Bank Victims and SPE

178. Separate from the use of NESTEGG, multiple private cyber security researchers have published reports explaining that the malware used in connection

[13] A BIC is a "business identifier code" that is used by the SWIFT system to uniquely identify banks and financial institutions (including the sending and recipient bank). A correspondent bank is a bank that is used as an intermediate bank to effect a transfer between two other banks, often by holding accounts in different currencies on behalf of other banks. Thus the fact that the subjects were researching the BIC code for their intended victim as well as for a correspondent bank needed to route fraudulently transferred funds shows that they understood correspondent banking and were preparing to—and did—incorporate those details into the unauthorized SWIFT messages they generated and sent.

with the intrusion at Bangladesh Bank shared other distinct code with the malware used against other banks in Asia.[14] Furthermore, other malware that was used in the intrusions at the Vietnamese Bank and the Philippine Bank shared significant similarities to malware used by the group that attacked SPE.

179. Forensic analysis of compromised computers at Bangladesh Bank and other banks has revealed links to the attack against SPE's network. In particular, a specific "secure delete" function was found in malware on the compromised networks of multiple financial institution victims, linking those intrusions together. That secure delete function was also found in a piece of malware (SierraCharlie) uploaded to VirusTotal.com ("VirusTotal")[15] (an online repository of malware) from

---

[14] *See, e.g.*, https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html; http://baesystemsai.blogspot.com/2016/05/cyber-heist-attribution.html; and https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks.

[15] VirusTotal, which is owned by Google, is an online service that analyzes files and URLs enabling the identification of viruses, worms, Trojans, and other kinds of malicious content detected by antivirus engines and website scanners. VirusTotal does not distribute or advertise any products belonging to third-parties. VirusTotal aggregates dozens of antivirus engines and scanners to scan each file submitted and provides the detection results of these engines, free of charge. VirusTotal also allows users of its subscription service to run Yara rules across approximately the last 75-80 TB of data submitted, which typically results in searching approximately the last 90 days of files submitted, based on a typical month.

A Yara rule is a tool that can assist with identifying and classifying digital files, including malware. A Yara rule essentially contains a description of patterns of text or binary (zero or one) numbers. This pattern can then be used to search digital files or databases to quickly find instances in which the pattern is found. Specifically, a pattern tailored to match a particular feature in a piece of malware can be used to identify related files, or "families," that might have been written from the same base of source code. That "pattern" can be based on a set of commands that the malware will perform, or it can be based on stored values or static data kept in the contents of the malware, or on other features. Typically, malware samples recovered from victims or from publicly available sources are in "binary" or "machine" code, and Yara rules are designed to detect whatever pattern they are seeking in machine code.

an unknown source, but which shared a framework with the Brambul worm samples found on SPE's compromised network. In addition to the information obtained from Bangladesh Bank, I learned the following from other FBI agents, an FBI computer scientist, information received from SPE, a private cyber security firm—Mandiant—retained by the U.S. Attorney's Office and the FBI to analyze the malware that the FBI has collected from multiple sources, and other private cyber security firms publicly available reporting:

a. Three samples of the Brambul worm described in Part V.B were recovered from SPE's network. Forensic analysis determined that these samples' code shared substantial similarities to the code of a different family of malware that was dubbed "SierraCharlie" by private cyber security company Novetta in a publicly available report titled "Operation Blockbuster." Further analysis determined that these similarities are due to the fact that both types of malware (Brambul and SierraCharlie) were likely created from the same code framework; that is, both share one generic, reusable body of code with components that a programmer can selectively interchange to create new pieces of software, without having to rewrite redundant code segments for each piece of software. Researchers have been unable to identify this specific framework in other software or malware, which strongly suggests that the same programmers who created the Brambul and SierraCharlie malware also created the framework underlying each of those types of malware.

b. A particular sample of SierraCharlie named "msoutc.exe," uploaded to VirusTotal on March 4, 2016 by an unidentified person, contains a unique function to securely delete a file from a computer's hard drive in a manner that makes it extremely difficult, if not impossible, to recover in a subsequent forensic examination. Although the source of this SierraCharlie sample is not known, this file is significant because it contains both a secure delete function (that was seen in malware found at Bangladesh Bank and a bank infected in Vietnam)

and shared the same overall framework of the Brambul malware recovered from SPE's network that was used during the intrusion (as discussed above in paragraph 179.a).

i. The particular secure delete function's characteristics are that it first generates random data to over-write the part of the hard drive that was allocated to store the file that is to be deleted (making the file irrecoverable). It then renames the file to a random name that is all lowercase letters that has the same number of letters as the original filename. Finally, it performs a regular Windows deletion of that file with the new random filename.

ii. This secure deletion function existed in a nearly identical form in a piece of malware named "evtsys.exe" that performed a role in the cyber-heist from Bangladesh Bank. Specifically, one piece of malware named "evtdiag.exe" was configured to access the database that stored records of messages on the SWIFT server at Bangladesh Bank. That malware (evtdiag.exe) was used to delete the specific messages that instructed the fraudulent transactions in the theft, in essence covering some of the subjects' tracks. The malware evtdiag.exe was also designed to send an instruction to evtsys.exe to securely delete itself (evtdiag.exe) on February 6, 2016, at 6:00 a.m. per the computer's local time (even further covering their tracks, by deleting the malware used to delete the messages). However, Bangladesh Bank personnel shut down the server on February 5, 2016. When the server was started again on February 6, 2016, evtdiag.exe failed to send its deletion instruction, resulting in an apparently inadvertent preservation of the malware. According to multiple private sector security researchers, the secure delete function present in evtsys.exe has only been observed in malware samples that are tools linked to North Korea, and specifically to the Lazarus Group.

c. The same secure delete function in msoutc.exe described above that was used by SierraCharlie and evtdiag.exe was also found in a piece of

malware (FoxItReader.exe) recovered from a computer at the Vietnamese Bank. Officials at the Vietnamese Bank have informed the FBI that the SWIFT messages that were sent were fraudulently created as a result of a computer intrusion. This piece of malware was also designed to conceal evidence of specific SWIFT messages, although in a somewhat different way than the evtdiag.exe malware did at Bangladesh Bank, as discussed in paragraph 179.b.ii.

i. The manner in which the malware found at the Vietnamese Bank conducted this concealment was tailored to unique aspects of the Vietnamese Bank's business processes. Specifically, the Vietnamese Bank's connectivity to the SWIFT network was managed by a third-party company. Each SWIFT message sent to or from the Vietnamese Bank was memorialized in an individual PDF document stored on the third-party's server, whereas Bangladesh Bank printed paper copies of the SWIFT messages. Vietnamese Bank employees in general would remotely connect to the third-party's server and use a program called FoxIt Reader in order to review the documents containing records of the SWIFT messages.

ii. The malware used against the Vietnamese Bank was designed in such a manner that when the Vietnamese Bank employees attempted to open these PDF documents in FoxIt Reader, they would instead inadvertently initiate the malware. The malware would analyze the document being opened to determine whether it met certain criteria designed to determine if the PDF document being opened would contain evidence of the fraudulent messages. If the document did meet the criteria, then the malware would first make certain modifications to the document, then instruct the legitimate FoxIt Reader software to open the modified document so that the user would be unaware that anything unusual had occurred. The end result was that documents that contained records of the fraudulent SWIFT messages sent by the subjects would be modified so that the

bank employee viewing the record would remain unaware of the fraudulent message.

d. This same secure delete function was further identified within a malware sample belonging to the Contopee family—specifically, a sample of Contopee that was recovered from the network of the Philippine Bank. It utilized a specific DDNS domain, onlink.epac.to, in the manner described in paragraphs 47–48. This domain was managed by an account at a DDNS provider; this same account was accessed on October 6, 2015 from a North Korean IP address. Furthermore, the NESTEGG backdoor malware—that was also found at Bangladesh Bank—was deployed throughout the Philippine Bank's network in a computer intrusion from November 2015 to January 2016, shortly before the subjects sent the fraudulent SWIFT messages from Bangladesh Bank.

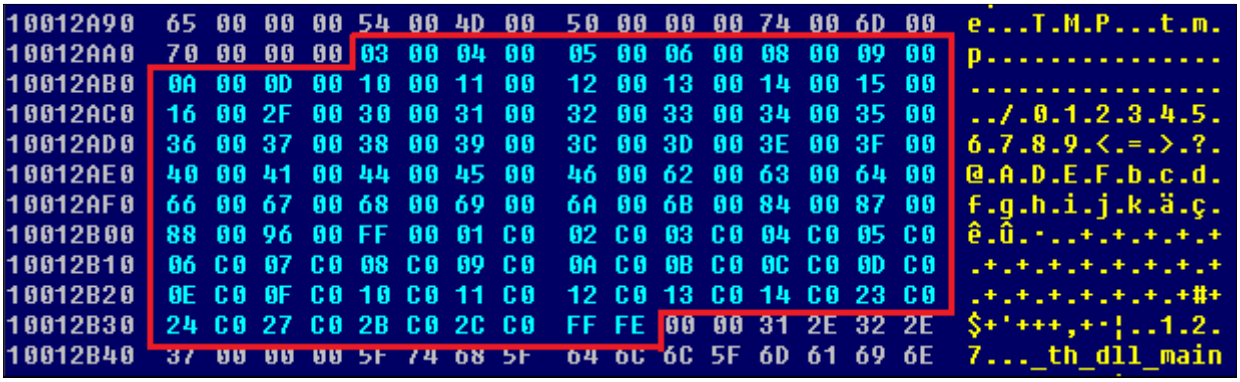
4. FakeTLS Data Table

180. I learned from those same sources referenced in paragraph 179 that further forensic analysis revealed that all three samples of the MACKTRUCK malware used in the attack on SPE were linked to the NESTEGG sample found at the Philippine Bank as well as to the Contopee backdoor malware used in the intrusions at the Philippine Bank and the Southeast Asian Bank (the same bank referred to above in paragraphs 143 and 175) by way of a data table coded within the malware. The purpose of the data table was previously unknown, because although many samples of MACKTRUCK (including those used at SPE), Contopee (including those used at the Philippine Bank and the Southeast Asian Bank), and NESTEGG (the one used at the Philippine Bank) contained this data table, none were known to contain any code that actually referenced the table (*i.e.*, made any use of it). In other words, in these samples the data table was unused, static code that served no function, and thus its presence was not readily apparent when the malware was analyzed.

181. The fact that this data table existed in the malware used in each of those intrusions is, however, of significance because that alone suggests that the same subject or subjects were responsible for these intrusions, given that the static data table had not been seen in other malware. Moreover, the fact that the static data table was inactive in these malware variants further suggests that the subject or subjects who authored the malware were drawing code from a central or common library or database of malware. In other words, the static data table was likely an inadvertent artifact that resulted when the subjects compiled multiple pieces of malware from source code to machine code using that common library. I know, based on my training and experience, that programming mistakes can result in the inadvertent inclusion (during the compilation process) of parts of a code library that are not always necessary in the finished piece of software. Given that the static data table had no discernable function in the multiple pieces of malware referenced above, this appears to be the most plausible explanation for its presence in those malware files.

182. I learned from those same sources that that same static data table was also found in an early version of a ransomware worm malware dubbed "WannaCry" (from approximately February 2017, "Version 0" discussed below). The table, as used in that early version of WannaCry, is pictured below.[16] (The WannaCry worm is further discussed below in Part X.)

[16] *See* http://baesystemsai.blogspot.com/2017/05/wanacrypt0r-ransomworm.html



183. Notably, however, in both the sample of WannaCry and one particular sample of Contopee that had been uploaded to VirusTotal, the static data table was critical to the malware's functioning—specifically, as to conducting FakeTLS communication. Subsequently, the FBI has identified a total of nineteen samples, including samples of NESTEGG, that contain this function that actually makes use of the static data table, all of which are either directly related to WannaCry or otherwise linked to the Lazarus Group based on one or more other attributes in the malware. Those nineteen samples—including the samples of WannaCry and Contopee described above—used the identical static data table in the same way: in the process of randomly generating certain information to send while initiating a FakeTLS communication, as follows:

a. The TLS Handshake Protocol is used by computers establishing a secure connection with each other to (1) choose which cipher suite will be used throughout their exchange, (2) authenticate the server to the client, and (3) exchange session key information.

b. A standard, legitimate TLS handshake is initiated when a client sends a "ClientHello" network data packet to a server. This packet is intended to transmit certain pieces of information about the client to the server in order for both systems to establish a mutually intelligible communication channel; this

information includes the TLS Protocol Version, Session ID, Cipher Suite, and Compression Method. Of particular note, for reasons discussed below, is the cipher suite field. The TLS protocol, in versions 1.2 and older, specifies a list of cryptographic algorithms, or cipher suites, which can be used to encrypt TLS communications. Each cipher suite is assigned a two-byte identification code for reference purposes. When a client initiates a TLS communication, it sends the server a list of these codes to indicate which cipher suites it is capable of supporting. The server can then compare this to the cipher suites that it supports, in order to choose an appropriate cipher suite to use to encrypt the remainder of the TLS communication.

c. As noted above in paragraphs 164.b–164.c and 183, several pieces of malware closely resembling those used in previous Lazarus Group intrusions contain a function that generates a packet resembling the TLS ClientHello packet in order to initiate a FakeTLS communication with a command and control server operated by the subjects. These pieces of malware contain a hardcoded data structure that contains a list of 75 two-byte values, which is the data table referred to above. These two-byte values correspond to valid TLS cipher suites as described above. The function randomly selects one of the following numbers: 12, 18, 24, 30, and 36. It then selects that same number of cipher suite identifiers from the TLS data table. These identifiers are then input into the cipher suite field of the ClientHello packet that the function generates.

d. As a result, the ClientHello packet has a randomly selected list of cipher suites with a variable length. This makes it more difficult for network security software to accurately distinguish between legitimate TLS traffic and malicious network traffic generated by malware that contains this FakeTLS code, and thus more difficult to effectively block malicious network traffic without inadvertently blocking legitimate network traffic.

184. The similarities between different samples of malware described above in paragraphs 180–183 are significant because they demonstrate that the authors of all of the malware samples very likely had access to the same collection of original source code, including the static table used for FakeTLS traffic. As noted below, it is highly unlikely that disparate groups of persons independently created these various malware variants. Instead, the most likely explanation is that a single group of subjects created all the malware or, at a minimum, had direct access to the source code used in these malware variants—source code that was not publicly available.

a. Although minimal, targeted changes to the binary code of an executable program (also called "patching" it, as described below in paragraph 188.b) are relatively easy to make, it is much more difficult to make substantial changes or additions to binary code of an executable program. This is because the process of compiling source code (that human programmers compose and revise) to binary code (or "machine code" that computers process) automatically generates references to virtual memory addresses throughout the binary code that the program uses to store and manipulate information. Any modifications to the binary code that would change the relative position of these virtual memory references within the file would invalidate them. It would therefore likely take a substantial amount of effort to recalculate these references in order to restore the functionality of the program if one were trying to make major or even minor changes but preserve the functionality of the program.

b. Alternately, if a person wanted to make substantial changes or additions to binary code, a programmer could hypothetically reverse-engineer, or "decompile," the binary code of a piece of malware to its original source code, then modify that source code and recompile it into a new program. However, the compilation process involves many steps wherein the code is automatically modified

and reorganized to optimize it so that a computer can run the program more efficiently, as compared to the manner in which a human originally wrote the source code. Thus, decompiling the binary code would result in the creation of a product that appears to be substantially different than the original source code. If that decompiled source code were then recompiled, the optimization procedures applied to it would further modify it, resulting in binary code that would be different from the original program. The degree of similarity in the functions repeated between the malware samples noted above largely precludes this hypothetical scenario, rendering this alternative similarly implausible. Therefore, it is likely that the creators of each of the pieces of malware discussed above had access to the same source code for each of the unique functions described above.

5. DNS Function

185. A malware sample belonging to the NESTEGG family of backdoors containing the same FakeTLS ClientHello function and data table described above in paragraphs 180–183 also contained a function that looked up a domain in the same manner described in paragraph 49. This particular function of the malware (1) queries a domain passed to it by the malware (*i.e.*, from a different section of the malware), (2) receives a response from that DNS "look-up," (3) then performs a mathematical manipulation (specifically, an "XOR," or "exclusive OR,"[17] operation) on the result using a hardcoded value in order to generate a new IP address to contact, and then (4) releases the memory space allocated to temporarily store the result of the DNS query.

[17] An XOR is a simple operation that, in binary code (consisting of 0s and 1s), combines two strings of code sequentially with each other, here (a) the code corresponding to the IP address assigned to the domain and (b) the hard-coded key value. When the values of each position are the same (either both 0s, or both 1s), the result is 0; when the values are both different (either 1 and 0, or 0 and 1), the result is 1.

a. Releasing memory space is a common procedure required in most programming languages. It is designed to ensure that the program uses a minimal amount of the computer's memory. Specifically, temporary data that has been stored in the memory needs to be "released" or "deallocated," which does not necessarily erase the data, but allows the computer to reuse that memory space for another purpose. (This type of memory is commonly referred to as "RAM" or random access memory, which is used while the computer is executing processes and running applications, and is separate from the storage capacity of a hard drive or other medium where most files are stored.)

b. In general, one of two functions may be available on a Windows system that a program can use in order to release the memory from the results of a DNS query. One function exists in the Windows XP and later versions of the Windows operating system (Windows XP was released in 2001), whereas the other exists in earlier versions of Windows and is now deprecated, meaning that it is only currently implemented to ensure that older software written to use this function remain compatible with newer versions of Windows. In the specific case of the NESTEGG DNS query function, both of these Windows functions are implemented, meaning that the portion of the code designed to work with Windows versions earlier than Windows XP is surplus and unnecessary in most cases except for when it is used on extremely old versions of the Windows operating system.

c. I learned from Mandiant that many code samples published in open sources contain references to both of these DNS deallocation functions in the same manner. However, these code samples do not contain an ability to manipulate the result of the DNS query (here, by using the XOR function described in paragraph 49). Thus, although the subjects do appear at times to use open-source code to create their malware, they sometimes also appear to modify that code in a unique and telltale manner.

186. An FBI computer scientist searched a repository of malware samples compiled in the course of this investigation using a Yara rule (*see* footnote 15) designed to identify samples of malware that conducted the following three actions in the exact manner as the NESTEGG sample described above in paragraph 185: that is, malware samples that (1) performed a DNS look-up or resolution request, (2) manipulated the result of that request, and (3) contained this pre- and post-Windows XP manner of releasing or de-allocating memory. The search yielded four files that contain these features. Two were Contopee samples, one was the NESTEGG sample discussed above in paragraph 185 and one was the msoutc.exe file (*i.e.*, SierraCharlie) discussed above in paragraph 179.c. The fact that these samples performed those three actions in the same exact manner further demonstrates that these families of malware were likely authored by the same programmers that are the subjects of this investigation. A third Contopee sample found at the Southeast Asian Bank shared all of the same attributes, except it was a 64-bit, Visual C++ 10.0 sample, indicating it may have been created using portions of the same source code but compiled in a different environment. That Contopee sample also contained the data table described in Part VIII.D.4. This is the same Southeast Asian Bank referred to in paragraph 175, where NESTEGG was used with the same encryption key used at Bangladesh Bank and the African Bank.

187. In sum, an early WannaCry sample and that NESTEGG sample contained the TLS function; that NESTEGG sample also contained the DNS function described in this Part, as did msoutc.exe (SierraCharlie); and msoutc.exe in turn is connected to both Brambul (found at SPE) via a shared framework and to evtsys.exe (found at Bangladesh Bank) via the secure delete function.

6. Intrusion at the African Bank: Connections to Bangladesh Bank

188. In 2016, the aforementioned African Bank became the victim of a computer intrusion and cyber-heist that initially resulted in the theft of approximately $100,000,000. The subjects routed the funds to accounts in multiple countries in Asia, but those funds were ultimately returned by those banks at the request of the African Bank. I learned the following from an FBI computer scientist based on his and others' forensic analysis of devices that were recovered from that intrusion, which devices contained artifacts consistent with both the use of malware and malicious activity at the subjects' other victims:

a. Forensic analysis of the SWIFT server at the African Bank shows that, early in 2016, several entries were created in a specific part of the Windows Registry (a database of Windows software settings) that is characteristic of NESTEGG. The data stored in these entries include the MD5 hash of the password nf300karjfs9e8rhtQJ3u9gh, which, as mentioned above in paragraphs 173–175, is the same as the password used to execute the NESTEGG dropper at Bangladesh Bank. As noted in paragraph 173, the MD5 hash of the password was generated in order to generate the key used to decrypt the resources, and as noted in paragraph 175, this password had not, to my knowledge or the knowledge of the FBI computer scientist or other researchers with whom he consulted, been publicly published on the internet or through other open sources at the time of either incident.

b. On the day of the unauthorized transfers, the subjects modified several files that formed components of the SWIFT Alliance Access software on the African Bank's SWIFT server. Later forensic analysis recovered an executable program named fpat.exe from the African Bank's SWIFT server. The program fpat.exe was capable of making targeted modifications to otherwise legitimate Alliance Access files. In particular, the forensic analysis and analysis of the

malware determined that one SWIFT Alliance Access file that had been modified was "patched," meaning that a very small portion of its binary instructions were overwritten. That particular file would ordinarily prevent changes to the database that recorded all SWIFT messages exchanged by the bank, but once it was modified or "patched," the subjects were able to access and modify the database. This modification was done in a way that was nearly identical to the intrusion at Bangladesh Bank, except that in the intrusion of Bangladesh Bank, the modification was only conducted on a copy of the Alliance Access file as it was loaded into the computer's memory, while in the intrusion of the African Bank, the modification was implemented on the file as it was stored on the server's hard drive.

c. Forensic analysis further revealed that a file named nroff.exe had been placed on the African Bank's SWIFT server on the day the unauthorized messages were sent. Although artifacts of the file's use were found, the file itself had been deleted by the time a forensic copy of the server was obtained, and therefore the malware sample itself was not recovered from the African Bank. The file named nroff.exe is typically a legitimate software tool used by Alliance Access to format the text of a SWIFT message in preparation for printing. The fact that a file with that same name was created in the Alliance Access program folder on the same date that the fraudulent messages were sent suggests that this particular file named nroff.exe was not the legitimate SWIFT Alliance Access file, but instead was malware with that name specifically placed on the African Bank's SWIFT server by the subjects. Later on the same day, the same file was erased in a manner likely intended to prevent forensic recovery and analysis (although not the same way as discussed above in paragraph 179.b). Of note, the intrusion at Bangladesh Bank used a piece of malware also called nroff.exe to intercept and modify fraudulent transactions that would have otherwise been automatically printed for the bank's

records. Thus, it is likely that the nroff.exe file observed at the African Bank was also malware designed to accomplish a similar purpose.

d. Moreover, forensic analysis identified three text files on the server that contained Structured Query Language ("SQL") statements, which are specially formatted instructions to query a database for information.

i. These statements contained generic instructions that configured how the output of the database query should be formatted. The statements also contained specific instructions to retrieve information from the bank's database of SWIFT messages related to a SWIFT message that contained a specified Transaction Reference Number ("TRN"). (A TRN uniquely identifies a transaction within a bank's records.) These text files containing the SQL statements were created on the same day that the fraudulent messages were sent from the African Bank, and they specified the same TRN that was used in one of the fraudulent SWIFT messages sent from the bank on that date.

ii. Further forensic analysis uncovered artifacts showing the existence of other text files with the same naming convention as those three text files, but those files had been "zeroed" out, *i.e.*, the allocated space on the hard drive for them had been replaced with all zeroes. Zeroing out a file is not something that is done when a user tries to delete a file using the Windows operating system, and this therefore likely shows that the subjects intended to conceal the contents of those files. Given that they had the same naming convention and were zeroed out, those files may have contained the SQL statements designed to query for the TRNs for the other fraudulent transactions originating from the African Bank.

iii. Furthermore, the evtdiag.exe malware described in paragraph 179.b.ii, which was identified on Bangladesh Bank's SWIFT server, contained a feature designed to create nearly identical text files (to those discussed above) containing SQL statements. These SQL statements that the Bangladesh

Bank malware was designed to create were identical to the ones actually found on the African Bank's SWIFT server, except for several data fields that were specific to the bank and to the specific transactions that the SQL statements were intended to retrieve. (The SQL statements were generally identical, except for the BICs and the TRNs.) This is significant because the SQL statements contained very specific and apparently idiosyncratic instructions to retrieve and format the data. In other words, those SQL statements were not just a generic methodology for querying the database, rather they represent a unique signature of activity.

7. Watering Hole Campaign Targeting Financial Institutions

189. In January 2017, the FBI learned of a malicious cyber campaign that targeted the Polish banking sector and affected multiple victims, including Polish financial institutions. I have reviewed numerous reports regarding the campaign, received information from the Polish National Police, and spoken with individuals involved in the response to this campaign. The series of intrusions has been characterized as one of the most serious information security incidents, if not the most serious information security incident, that has occurred in Poland. The intrusion was likely discovered before the hackers could successfully steal any funds, as the FBI has not obtained any evidence indicating that any fraudulent monetary transfers occurred in the incident. The subjects executed similar schemes in Mexico and a South American country (discussed below). As discussed below, artifacts indicating that NESTEGG was used in Poland and the use of North Korean IP Address #5 both show that the subjects of this affidavit were also responsible for these intrusions.

190. Specifically, the subjects behind the computer intrusions spread malware by infecting the website of the Polish Financial Supervision Authority, www.knf.gov.pl, with malware and used the compromised website in what is known as a "watering hole" attack. A watering hole attack occurs when a hacker

compromises a website that is known to be visited by intended victims. As the intended victims visit the website, typically as part of their normal business practices, the intended victims (and sometimes unintended victims) are infected with malware that gives the hacker access to the intended victim networks. In this case, the subjects likely assumed numerous banks would regularly visit the website of the Polish Financial Supervision Authority, making that website an ideal candidate to be used as a watering hole to infect banks in Poland.

191. The investigation into the campaign has revealed that the watering hole was likely in place from October 5, 2016 through February 2, 2017. The malware on the watering hole was configured to verify if any visitor to the website was one in whom the subjects were interested, by using an IP address "whitelist" that would only infect computers coming from selected ranges of IP addresses—many of which were IP addresses assigned to banks. The whitelisted victims would then be re-directed to one of two legitimate, but compromised, websites: http://sap.[DOMAIN REDACTED].ch/vishop/view.jsp?pagenum=1 or http://www.[DOMAIN REDACTED].in/design/fancybox/images.jsp?pagenum=1.

a. Multiple private cyber security research companies reported discovering evidence indicating that the website of a Mexican financial regulator had also referred traffic to one of the domains redacted in the previous paragraph, although to a different resource on the domain, on November 8, 2016.[18] This was also reflected in the logs received by the FBI showing which computers accessed the domain.

b. An additional website of a bank in South America (the "South American Bank") also appeared to have communicated with that same domain

[18] *E.g.*, http://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html

(redacted above), based on data that had been submitted to VirusTotal.[19] Specifically, that data showed that on approximately October 26, 2016, when a person visited the website of the South American Bank, the person's computer was directed to request data from that same compromised domain. Thus, while in Poland and Mexico the subjects used a regulatory authority's website as a watering hole, in the South American country it appears that the subjects used an individual bank's website as the watering hole.

c. A malware sample with a file name Winslui.exe, which also used the compromised domain referenced above, was uploaded to VirusTotal on October 27, 2016 from the same country as the South American Bank. (The fact that the malware sample used the same domain as the known domain of the watering hole and was uploaded from the same South American country strongly suggests that it was uploaded by a victim of, or cyber security researcher investigating, the South American Bank watering hole campaign.) Microsoft and Symantec each identified it as a backdoor, and Symantec reported it was linked to the Lazarus Group based on unique strings of text contained in the malware.[20] Specifically, it concealed elements of its functionality by storing text in an encrypted form that could be decrypted at the time that the malware was executed. These exact same strings of text were identified in a sample of Brambul that was uploaded to VirusTotal on November 30, 2011, which used xiake722@gmail.com as a collector email account (*see* paragraph 41).

192. The FBI has confirmed that NESTEGG was found on the victim computer network at one of the victim banks in Poland, and forensic analysis

---

[19] Although VirusTotal is commonly used as a repository of malware samples, here the data uploaded to VirusTotal was the traffic between the South American Bank site and an unidentified person's web browser.

[20] https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0.

conducted and published by Kaspersky has identified that hosts inside the victim environment contained a file "gpsvc.exe," which is known to the FBI to be a version of NESTEGG based on its structure and behavior, and based on separate analysis by another private cyber security company.[21] Although the FBI has not had direct access to the computers that were compromised, the investigators who were involved in responding to that incident found forensic artifacts that revealed that that NESTEGG sample was directly linked to the watering hole involving the Polish banking regulator. The malware used in the intrusion included a configuration file named srsservice.hlp that included two DDNS domains: tradeboard.mefound.com and movis-es.ignorelist.com.[22] The victim computer would resolve one of these two DDNS domains to determine the IP address assigned to the domains, and—as described in paragraph 49—use that IP address to calculate a new IP address via an XOR operation. This newly calculated IP address would then be used as the "real" command and control node.

193. Any IP addresses attempting to resolve these DDNS domains are likely victims or intended victims of intrusions by the subjects. An IP address assigned to the Polish victim bank referenced above connected to tradeboard.mefound.com hundreds of times between January 12 and February 2, 2017, and an IP address assigned to a different Polish financial services company connected to the same domain dozens of times between October 26, 2016 and January 21, 2017.

---

[21] https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf

[22] Records obtained by the FBI show that the account that created tradeboard.mefound.com also created the DDNS domains shareboard.mrbonus.com, wconsult.longmusic.com, and paystore.onedumb.com, and that the account that created movis-es.ignorelist.com also created the DDNS domain lcgmd.strangled.net and is linked to the account that created geodb.ignorelist.com and vnistudio.mooo.com.

194. As noted above in paragraph 191.a–191.b, while the watering hole website in Poland was directing intended victims to the two compromised redacted domains, those compromised domains were also receiving connections from victims in Mexico and the South American country.

a. An IP address assigned to a Mexican bank connected to tradeboard.mefound.com multiple times between December 23, 2016 and January 19, 2017; connected to movis-es.ignorelist.com dozens of times between December 21, 2016 and February 9, 2017; and connected to geodb.ignorelist.com between February 10 and 13, 2017.

b. An IP address assigned to a second Mexican bank connected to tradeboard.mefound.com on January 18, 2017 and movis-es.ignorelist.com multiple times between January 14 and 19, 2017.

c. An IP address assigned to a third Mexican bank connected to movis-es.ignorelist.com dozens of times between February 1 and 15, 2017.

d. Eight different IP addresses from the country where the South American Bank is located connected to movis-es.ignorelist.com nearly 100 times between December 22, 2016 and January 16, 2017, and seven different IP addresses from that country connected to tradeboard.mefound.com approximately 15 times between October 31, 2016 and January 15, 2017. Based on WHOIS records for these IP addresses it was not possible to determine who or what the specific victim(s) were that tried to "look up" or resolve the domains.[23] (WHOIS is a protocol to query regionally-managed publicly available databases of domain registry

[23] Large internet service providers that serve a large number of customers will occasionally use a "name server" that will both perform DNS "look ups" when the provider's customers try to look up domains, and caches or locally stores the IP addresses assigned to those domains. In those instances, the name server actually performs the resolution request on behalf of its customer (here, the victim trying to look up a domain under the control of the subjects).

information, showing who registered the use of a particular domain or IP address, his/her/its contact information, and the IP address assigned to a particular domain.)

195. In May 2017, Russian cyber security firm Group IB published a detailed report[24] that analyzed computer intrusions on the financial sector that included the Bangladesh Bank heist and the watering hole attack in Poland. The key finding of the report was that two North Korean IP addresses (one of which was North Korean IP Address #5) were using a complex three-layer series of hop points in order to command-and-control the malware being used in these intrusions in the financial sector.

196. While the Group IB report did not explain all of the evidence on which it relied, its findings are corroborated by the findings in the ongoing investigation by the FBI—specifically, that this same North Korean IP Address #5 has been used by the subjects in connection with their attempts to infiltrate financial institutions (as noted in paragraph 177). Additionally, its findings regarding the use of multiple proxies is corroborated by the FBI and Department of Homeland Security's public release regarding a North Korean backdoor malware called FALLCHILL.[25]

197. North Korean IP Address #5 shares other connections to the subjects, as described in the following paragraphs.

a. On multiple days in March 2015, North Korean IP Address #1 (its predecessor, as described in paragraph 36) was used to access a DDNS account that created the DDNS domain tbs.fartit.com. As mentioned in paragraph 170.a, a Contopee sample analyzed by the FBI contained the DDNS domain tbs.fartit.com. That Contopee sample was compiled on February 23, 2015. Notably, the first time that the tbs.fartit.com domain was under the control of the subjects was also on

[24] https://www.group-ib.com/blog/lazarus

[25] https://www.us-cert.gov/ncas/alerts/TA17-318A

February 23, 2015, and, after using a Proxy Service IP to begin managing it, it was also controlled using North Korean IP Address #1 on March 4 and 26, 2015.

b. The same device used to access the DDNS account managing tbs.fartit.com also was used to access the DDNS account that registered the use of the domain cloud.edns.biz. The Compromised Web Server (discussed above in Part VII, used in connection with the attack on SPE) was observed connecting hundreds of thousands of times between April 2016 and June 2017 to the domain cloud.edns.biz.

c. This same Compromised Web Server, which was resolving cloud.edns.biz—which, in turn, was controlled by a subject who had used North Korean IP Address #1—was observed by the FBI being accessed by North Korean IP Address #2 in February, April, May, June, July, and December 2015, and by North Korean IP Address #6 on March 22, 2016. (As mentioned in Part V.A, there was a shift in activity associated with certain North Korean IP addresses used by the subjects in March 2016, such that, for example, activities that were in 2014 and 2015 associated with North Korean IP Addresses #1–#4 shifted to North Korean IP Addresses #5–#8, respectively.)

d. This shows that the subjects of this investigation have access to both the computer networks assigned North Korean IP Addresses #5 (formerly #1) and North Korean IP Address #6 (formerly #2) and have used both in furtherance of their computer intrusions.

198. This use of the same North Korean IP addresses, in addition to the use of NESTEGG in the intrusions at Bangladesh Bank (and elsewhere) and the Polish financial sector, shows that the subjects at issue in this affidavit were also responsible for carrying out these watering hole attacks.

IX. TARGETING OF OTHER VICTIMS

199. In addition to the subjects' cyber-targeting and intrusions of SPE and financial institutions worldwide, the evidence indicates that the subjects have also targeted and attempted to penetrate U.S. defense contractors, at least one U.S. university, U.S. academic researchers, U.S. energy companies, and virtual currency exchanges worldwide using spear-phishing emails. In particular, the connections between those previously discussed attacks/intrusions and the targeting of U.S. defense contractors includes use of the same social media and email accounts; the same monikers; and the same operational infrastructure, such as IP addresses. Facts related to some of these intrusions and attempted intrusions are discussed below.

A. Initial Discovery of Defense Contractor Targeting

200. The email account MrDavid0818@gmail.com was created on October 29, 2015 using the name "David andoson" (the "Andoson David" alias, reversed) and using tty198410@gmail.com as its recovery email. The same device accessed both MrDavid0818@gmail.com and watsonhenny@gmail.com between December 14, 2015, and May 13, 2016. On March 12, 2016, a LinkedIn account was created using the email address MrDavid0818@gmail.com and the name "Andoson David." That LinkedIn account then sent LinkedIn invitation requests to dozens of individuals, including employees at aerospace companies in the United States and Israel, including specifically Lockheed Martin Corporation ("Lockheed Martin").

a. Later in 2016, the user of the email account [J NAME REDACTED]@yandex.com sent an email to MrDavid0818@gmail.com asking about what appeared to be source code for a particular business project. [J NAME REDACTED]@yandex.com then also contacted [Z NAME REDACTED]@yandex.com about having arrived and seeking help.

201. Lockheed Martin is the prime contractor for the Terminal High Altitude Area Defense ("THAAD") system, a missile-defense system. As was publicly reported, in July 2016, the United States and the South Korean military agreed to deploy a THAAD system in South Korea, and multiple media outlets publicly reported that a part of the THAAD system arrived in South Korea in March 2017. Evidence collected by the FBI indicates that spear-phishing emails were sent to various employees of defense contractors at various times through 2016 and 2017, at least some of which contained explicit references to THAAD. As discussed below, although the subjects have continued to target Lockheed Martin with repeated waves of spear-phishing, the FBI has not obtained any evidence from Lockheed Martin itself nor from any other sources in the course of the investigation that show any of the subjects' unauthorized intrusion attempts at Lockheed Martin have been successful.

202. The FBI alerted Lockheed Martin to this apparent targeting, and a cyber analyst at Lockheed Martin in turn informed the FBI of other email accounts that Lockheed Martin had observed being used to send spear-phishing messages to its employees between April 29 and May 20, 2016. The analyst later informed me of subsequent waves of spear-phishing messages beginning in early-July 2016 and late-August 2016. The subjects' accounts that were used to send spear-phishing messages to Lockheed Martin included campbelldavid793@gmail.com, goo19874@gmail.com, stevegell77@gmail.com, and uiwon0608@daum.net, among other purported Lockheed Martin employees (discussed below). In some instances, the same accounts were used to send spear-phishing messages in more than one "wave." In other instances, the subjects registered new social media accounts using email accounts from a previous wave of targeting Lockheed Martin employees, and in still other instances the subjects used entirely new accounts to send spear-phishing messages.

203. That same Lockheed Martin analyst also indicated that he was confident that the spear-phishing messages originated from the same group identified in the publicly available "Operation Blockbuster" report[26] that discussed an attack on SPE. One factor that he pointed to was his analysis of the malware used to target Lockheed Martin, which showed it tried to communicate using a FakeTLS signature, a common feature of malware identified in the "Operation Blockbuster" report and a tactic also employed in the intrusion at Bangladesh Bank.

204. Other Lockheed Martin cyber analysts provided further information regarding spear-phishing campaigns between February 2017 and May 2017, which originated from numerous accounts that purported to be from persons who worked in the recruiting and in the executive search industries, in an apparent attempt by the subjects to craft convincing spear-phishing emails.

B. Connections Between Accounts Used to Target Defense Contractors, and with Accounts Used to Target SPE

205. I and others at the FBI conducted internet research for information connected to the email accounts that had been used by the subjects to send spear-phishing emails to Lockheed employees. Based on those searches, I learned the following:

a. On December 4, 2015, a user named "hwa5403" posted on the website hackforums.net that he or she was "looking for a silent doc exploit," and requested that responsive information be sent to campbelldavid793@gmail.com.

b. The same user, hwa5403, also posted on hackforums.net on December 22, 2015: "I am testing phishing gmail but it goes to spam directly. Can anybody send me a sample phishing mail doesn't go to spam directory? My mail

[26] https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

addr is gooteam1000@gmail.com."

206. Campbelldavid793@gmail.com was created by "Campbell David" on November 11, 2015, using the recovery email address hwa5403@daum.net, and was accessed from North Korean IP Address #6. This account received emails from adobesystems.com and wordzen.com in August and September 2016. The user of the account also showed interest in aerospace companies and technologies, and read a Washington Post article on the North Korean military threat. The address book for campbelldavid793@gmail.com had also saved in its contacts dozens of Lockheed Martin employees' email addresses.

207. Provider records show the email account hwa5403@daum.net, a South Korean email account, was used in November 2015 to send spear-phishing emails to numerous individuals that focus on East Asia and Korean policy matters and, in 2016, the account sent spear-phishing messages to employees of two South Korean technology companies. (The email address hwa5403@daum.net was also used to create an account at a DDNS provider and registered a DDNS domain.) Those records also showed the account hwa5403@daum.net was accessed from North Korean IP Address #6 and North Korean IP Address #7 in 2016. North Korean IP Address #7 in particular was used to access hwa5403@daum.net and send spear-phishing messages on November 14, 2016, the same day that same IP address—North Korean IP Address #7—was used to access South Korean email addresses bangsong8519@daum.net and uiwon0608@daum.net (discussed in paragraphs 209 and 210, and paragraphs 202 and 219, respectively). (The three South Korean email accounts were also accessed from North Korean IP Address #6 on other days throughout 2016, with all three accounts accessed from North Korean IP Address #6 on August 31, 2016, and overlapping log-ins on other days as well.) As discussed below in paragraphs 307 and 314, North Korean IP Address #7 was used to access

Chosun Expo Accounts approximately two weeks later on December 1 and 2, 2016, and has been used since then as well.

208. A series of emails in July 2016 revealed additional tactics used by the subjects, as well as connections between the accounts used to target Lockheed Martin and the accounts used in the previously discussed cyber-attack on SPE and cyber-heist from Bangladesh Bank and intrusions at other financial institutions.

a. First, "David Campbell" sent an email from campbelldavid793@gmail.com titled "Invitation to dinner" to multiple email addresses, including gooteam73@gmail.com, diver.jacker@gmail.com (a Brambul collector email account, *see* paragraph 41) and [FC NAME REDACTED]@gmail.com (an email address that, like campbelldavid793@gmail.com, used hwa5403@daum.net as its recovery email). In August 2016, [FC NAME REDACTED]@gmail.com, which was accessed during that same month from North Korean IP address #6, exchanged what appear to be test spear-phishing emails with tty198410@gmail.com.

b. Several days later, gooteam73@gmail.com sent an email titled "Welcome to drive" to campbelldavid793@gmail.com that contained an embedded link to "http://www.[DOMAIN REDACTED].com/x/o?u=2cfb0877-eaa9-4061-bf7e-a2ade6a30d32&c=374814." (As described above, Google Drive is a remote file storage service, and this email was likely drafted as a test to see how the link might appear to an unknowing victim, while the subject line was one that might appear as if the email had been sent by Google. The domain corresponded to the email tracking service referred to above in paragraph 58.)

c. An apparent test spear-phishing email was also sent from campbelldavid793@gmail.com to gooteam1612@gmail.com on July 22, 2016, with a subject of "Malicious activities are detected" and multiple non-Google (and likely malicious) hyperlinks were embedded in the email in places where Google would

normally provide links to "Terms of Service" and instructions on how to mitigate these "malicious activities."

209. The email account goo19874@gmail.com (which was one of the accounts that had sent spear-phishing messages to Lockheed Martin employees) was created on December 9, 2015, used the name "Google Info" and the South Korean recovery email address of bangsong8519@daum.net (which email address was accessed from North Korean IP Address #6 and North Korean IP Address #7 during 2016), and was used to register other email accounts that sent spear-phishing messages to Lockheed Martin, including stevegell77@gmail.com and diver.jacker@gmail.com). The account was accessed from North Korean IP Address #6, and its user had conducted online research into Lockheed Martin and hacking Gmail accounts. Its address book had saved in its contacts Lockheed Martin employees' email addresses. The account was accessed by the same device as campbelldavid793@gmail.com, among others. The account had sent numerous spear-phishing emails to alumni of universities in southern California, and received emails from an email tracking service used by the subjects (a service referred to in paragraph 58).

1. Connection to mrwangchung01@gmail.com

210. As noted above, stevegell77@gmail.com sent spear-phishing emails to Lockheed Martin, and shared a common subscriber email (the South Korean email account bangsong8519@daum.net) with other email accounts that did the same. It was also accessed by the same device as mrwangchung01@gmail.com.

a. As discussed above, mrwangchung01@gmail.com is the Brambul collector email account that (i) was accessed by the same device as watsonhenny@gmail.com, as well as a device that accessed tty198410@gmail.com, (ii) used watsonhenny@gmail.com as its secondary email account, (iii) received test spear-phishing emails from rasel.aflam@gmail.com just before the spear-phishing

emails were sent to Bangladesh Bank employees, and (iv) was accessed by North Korean IP Address #6.

b. Closer in time to the most recent spear-phishing campaign targeting Lockheed Martin, on February 9, 2017, mrwangchung01@gmail.com was accessed from North Korean IP Address #6.

211. Moreover, [FC NAME REDACTED]@gmail.com—one of the email addresses that exchanged test spear-phishing emails with tty198410@gmail.com and campbelldavid793@gmail.com (used to target Lockheed Martin) and which was accessed from North Korean IP Address #6 in August 2016, as discussed above in paragraph 208.a—sent an email to [K NAME REDACTED]@163.com in 2016. That email was opened by [K NAME REDACTED]@163.com and its user clicked on a link that resulted in a connection with an IP address in Peru. Just hours before that occurred, multiple connections were made from North Korean IP Address #6 to the Peruvian IP address. Earlier in 2016, the user of mrwangchung01@gmail.com, a Brambul collector email account, obtained what appeared to be administrator credentials for that same Peruvian IP address.

2. Connection to @erica_333u

212. As discussed above in paragraph 111, the Twitter account @erica_333u posted the same link to malware that the "Andoson David" and "John Mogabe" Facebook accounts did on Facebook pages related to "The Interview." One of the registered email addresses for the Twitter account @erica_333u was goffman_david2@aol.com.

213. Goffman_david2@aol.com and [FC NAME REDACTED]@gmail.com used hwa5403@daum.net as their recovery email address, which was the same address that was used to register campbelldavid793@gmail.com. Goffman_david2@aol.com was used to send spear-phishing messages to academic professors and other individuals, at least some of whom had written about North

Korea. It also appears that emails sent from goffman_david2@aol.com were designed by the subjects to appear as if they were sent by someone who was assigned to "USFK," which is a common abbreviation for U.S. Forces Korea. Based on emails received by goffman_david2@aol.com, the subjects had also used the email account to register with the website of another U.S. aerospace firm.

214. Thus, the same email account, goffman_david2@aol.com, was used to subscribe a Twitter account (@erica_333u) that posted a link to malware targeting SPE, and also shared a common recovery email address with an email account that sent spear-phishing messages to Lockheed Martin.

215. Moreover, goffman_david2@aol.com sent a spear-phishing email to what appeared to be an email address affiliated with a policy expert on North Korea, and attached to that email was a version of MACKTRUCK that contained the same static table that was found in versions of MACKTRUCK, Contopee, and WannaCry, as described above in paragraphs 180 through 183.

3. Connection to jongdada02@gmail.com

216. By way of background, jongdada02@gmail.com was accessed most days between May 5 and June 8, 2015 from North Korean IP Address #2. In one instance, on May 28, 2015, that North Korean IP address was also used to access the Compromised Web Server (that was used to disseminate SPE's data via email, and which stored some of the malware used to target SPE) thirty minutes before it was used to access jongdada02@gmail.com. Provider records indicate that the subject using jongdada02@gmail.com had an interest in topics related to software and computer hacking, and conducted internet research regarding numerous

hacking-related topics, including as to specific CVEs and exploits and vulnerabilities in certain fonts.[27]

217. Multiple email accounts that sent messages during the February 2017 "wave" of spear-phishing targeting Lockheed Martin had been registered using jongdada02@gmail.com as the recovery email address. Those accounts included the accounts described in the following paragraphs. Of these email accounts, many used the email tracking service referred to above in paragraph 58, which is used to manage and track emails that are often sent as a part of a campaign and that informs the user when emails are opened.

a. One email address, [SW NAME REDACTED]@gmail.com, used the name of a television network and a journalist who appears on that network, in an apparent attempt to trick potential victims into believing that they were receiving emails from that journalist. That email account sent approximately 80 emails with subject lines such as "Consulting Request – Fighter Jet Software," and "Your Opinion" on February 3 and 9, 2017, to approximately 79 Lockheed Martin email accounts. Other email campaigns, likely test campaigns, were sent to other email accounts used by the subjects on February 3, 2017.

b. [DJ NAME REDACTED]@gmail.com sent approximately 47 emails on February 21, 2017 to employees of Lockheed Martin with subject lines purporting to be from a "Hiring Director" at other defense contractors.

---

[27] A related account, amazonriver1990@gmail.com (discussed in paragraph 96), was registered on May 19, 2015 from the same IP address, North Korean IP Address #2, which was used to access the account frequently between May 2015 and August 2015, including in one instance approximately three minutes after the same North Korean IP address was also used to access the Compromised Web Server. The user of that email account, amazonriver1990@gmail.com, also conducted similar internet research.

c. [ER NAME REDACTED]@gmail.com sent an email on February 9, 2017 with a subject of "Leadership role opportunity?" and the name of another defense contractor to approximately 17 Lockheed Martin employees.

d. [JB NAME REDACTED]413@gmail.com sent approximately six email campaigns (*i.e.*, each campaign was a separate email to one or multiple recipients),[28] with subjects such as "Leadership role opportunity?" and the name of another defense contractor between February 9 and 13, 2017. Those campaigns were sent to more than 80 accounts in total, including to Lockheed Martin employees.

e. [JC NAME REDACTED]@gmail.com sent more than 48 emails with subjects such as "Hiring Director" and the name of another defense contractor to approximately 49 Lockheed Martin employees between February 6 and 23, 2017.

f. skyfriend202@gmail.com sent emails with a subject of "Reaching Out!" on February 2, 2017 to approximately 25 Lockheed Martin employees.

218. The subjects have also created additional spear-phishing email accounts that purported to be from Lockheed Martin recruiters for use in spear-phishing campaigns targeting employees at other defense contractors. For instance, in May and June 2017 the subjects created two email accounts purporting to be recruiters at Lockheed Martin ([BM NAME REDACTED]@gmail.com and [MP NAME REDACTED]@gmail.com), and used those accounts to send numerous emails to employees of another defense contractor. Notably, the subjects accessed both email accounts from North Korean IP Address #6.

---

[28] Email campaigns are typically used in marketing, and each email in a campaign is typically sent to numerous recipients with a seemingly identical subject and body. Each recipient in a campaign might be unaware of who the other recipients are. The emails often contain tracking features that inform the sender when activities related to the email are conducted by the recipient, such as when an email is opened or when embedded links are clicked.

219. As with the email accounts mentioned in the previous paragraph, most of these targeting accounts were accessed from North Korean IP Address #6. Those accounts include campbelldavid793@gmail.com, [BM NAME REDACTED]@gmail.com, [MP NAME REDACTED]@gmail.com, [ER NAME REDACTED]@gmail.com, goo19874@gmail.com, [JB NAME REDACTED]@gmail.com, [JC NAME REDACTED]@gmail.com, [SW NAME REDACTED]@gmail.com, [KB NAME REDACTED]@gmail.com [KK NAME REDACTED]@gmail.com, [LB NAME REDACTED]@gmail.com, skyfriend202@gmail.com, and stevegell77@gmail.com, among others, many of which were impersonating the names of real persons who are journalists or employees at defense contractors. Likewise, uiwon0608@daum.net, the South Korean email address used to send spear-phishing emails, was accessed from North Korean IP Address #6 and North Korean IP Address #7 at various points in 2016.

C. Targeting of South Korean Entities

220. Evidence obtained in the investigation indicates that the subjects have a significant interest in South Korean companies and government entities, and have used spear-phishing and social engineering to try to compromise these entities. For example, a Facebook account that was accessed by the same device that was used to access the Facebook account registered to mogbe123456@gmail.com was used to either send friend requests or messages to three South Korean individuals who, based on internet research, appear to be employed by a South Korean secure software provider and on other occasions has sent messages to employees of a major South Korean technology company. Other evidence indicates that the subjects conducted significant internet reconnaissance for employees of United States and South Korean military entities, including for employees of specific fleets and divisions within each.

X. WANNACRY GLOBAL RANSOMWARE

A. WannaCry Ransomware Attacks

221. On March 14, 2017, Microsoft released a patch for a Server Message Block (SMB) vulnerability that was identified as CVE-2017-0144 on its website, https://technet.microsoft.com/en-us/library/security/ms17-010.aspx. Microsoft attempted to remedy the vulnerability by releasing patches to versions of Microsoft Windows operating systems that Microsoft supported at the time. Patches were not initially released for older versions of Windows that were no longer supported, such as Windows XP and Windows 8.

222. The next month, on April 15, 2017, an exploit that targeted the CVE-2017-0144 vulnerability (herein the "CVE-2017-0144 exploit") was publicly released by a group calling itself the "Shadow Brokers."

223. On April 18, 2017 and April 21, 2017, a senior security analyst at private cyber security company RiskSense, Inc. ("RiskSense") posted research on that exploit on his website: https://zerosum0x0.blogspot.com.

224. On May 9, 2017, RiskSense released code on the website github.com with the stated purpose of allowing legal "white hat" penetration testers to test the CVE-2017-0144 exploit on unpatched systems. Essentially, RiskSense posted source code that its employees had reverse-engineered for the CVE-2017-0144 exploit, which cyber security researchers could then use to test vulnerabilities in client computer systems. I know based on my training and experience that penetration testers regularly seek to exploit vulnerabilities with their customers' consent as a proof-of-concept to demonstrate how hackers could illegally access their customers' systems.

225. On May 12, 2017, a ransomware attack called "WannaCry" (later identified as "WannaCry Version 2," as discussed below) began affecting computers around the globe. Those infected computers included many at the United

Kingdom's National Health Service ("NHS"), as I have learned from officers at the United Kingdom's National Crime Agency ("NCA"), and numerous victims in the United States. According to information provided to the FBI by the NCA, at least 80 out of 236 NHS trusts (organizations serving a particular function or geographic area) across England were affected either because they were infected or because they had to disconnect as a precaution; at least 37 NHS "trusts" were in fact infected with WannaCry. An additional 603 primary care or other NHS organizations were infected. National coordination was undertaken during this major incident and remedial action was taken by local organizations to address the vulnerability and the spread of the malware to prevent further infections. There was no patient harm reported during the incident, but the effects included 6,912 appointments that were cancelled (and subsequently re-scheduled) between May 12 and 18, 2017, and 1,220 (approximately 1%) pieces of diagnostic equipment across the NHS that were affected by WannaCry. No NHS organizations paid the ransom, consistent with advice not to do so that was given by NHS during the incident. Other reports, including those by Europol, have indicated that hundreds of thousands of computers in more than 150 countries have been affected by the WannaCry Version 2 ransomware. Numerous victims within the Central District of California were infected with the WannaCry Version 2 ransomware in the days immediately after it was released, based on records relating to the IP addresses that tried to resolve a lengthy domain embedded in the code of the malware during that period of time. Based on how WannaCry operates, those computers would not have tried to resolve that domain unless the malware had infected their computers.[29]

[29] Although some security researchers began "self-infecting" their computers and/or analyzing the malware and the domain contained within it, those occurrences were a very slim fraction of the total instances of infection or traffic to the domain in the days immediately after the attack began.

226. Unlike most ransomware, which typically encrypts important files on a computer and then charges the victim a ransom to recover the files, it does not appear that victims of the WannaCry Version 2 ransomware have been able to actually decrypt their files by paying the ransom; instead, the files remain encrypted and inaccessible. The WannaCry Version 2 ransomware was also different from most other ransomware attacks in that—at least after the initial computer was infected—it does not appear that it was targeting any particular victim(s) as it spread. Instead, it was designed to self-propagate as a worm (using the SMB CVE-2017-0144 vulnerability) and continually infect additional vulnerable computers. Specifically, the malware contained separate functions to identify and infect computers vulnerable to the CVE-2017-0144 exploit on the computer's Local Area Network ("LAN"), as well as computers accessible over the internet.

a. The malware targeted other computers on each victim computer's LAN by querying the victim computer's network configuration to determine the range of IP addresses that constituted the LAN, then iteratively attempted to connect to each IP address in the LAN to determine whether there was a vulnerable computer located at that address. If there was, the malware would attempt to infect that computer.

b. The malware further targeted computers on the internet by randomly generating a target IP address outside the victim's LAN and attempting to connect to it. If the connection was successful, the malware would then iteratively attempt to connect to IP addresses with a number near the target IP address's (*i.e.*, an IP address that may be in the same network). For each successful connection, the malware would determine whether there was a vulnerable computer available, and if so, attempt to infect it. The malware further contained a timer mechanism to slowly change the range of IP addresses that it targeted in order to continually, randomly seek out new victims on the internet.

227. Private cyber security company BAE Systems conducted research on this version of WannaCry, and reported[30] that at least part of the code released by RiskSense on May 9, 2017 was likely duplicated into the WannaCry Version 2 ransomware, suggesting the hackers behind WannaCry Version 2 were aware of and had accessed the code provided by RiskSense.

228. In the days following the WannaCry Version 2 infections on May 12, 2017, security researchers from multiple companies (such as Symantec, BAE Systems, and Kaspersky) publicly identified previous versions of the WannaCry ransomware that did not include the self-propagation component. In other words, those earlier versions of the ransomware did not use the SMB vulnerability to spread. Those earlier versions thus did not spread widely, nor had they gained the notoriety of the May 12, 2017 version (*i.e.*, Version 2), given that they affected relatively few victims.

229. For example, according to a May 22, 2017 report by Symantec,[31] these earlier WannaCry attacks occurred in February 2017 (referred to therein as "Version 0" and previously mentioned in Part VIII.D.4) and March and April 2017 (referred to therein as "Version 1"). These earlier WannaCry versions were nearly identical to the May 12, 2017 self-propagating version (referred to as "Version 2"), with the most notable difference being the way the malware spreads. Versions 0 and 1 did spread, but only across infected victim networks by using stolen user credentials, meaning that the attackers would need to have already compromised a network and obtained user credentials to allow either Version 0 or 1 to spread; the malware did not propagate across the internet. Version 2, the only WannaCry version that used the SMB CVE-2017-0144 exploit described above, was able to

---

[30] http://baesystemsai.blogspot.com/2017/05/wanacrypt0r-ransomworm.html

[31] https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

spread to any unpatched computer on the internet that was allowing inbound connections via vulnerable Microsoft SMB versions, or to computers that were connected to a network in which another computer was allowing these inbound connections to vulnerable SMB versions. This new CVE-2017-0144 exploit is why WannaCry Version 2 spread so quickly, affected computers in so many countries, and was thus so widely publicized. As described below, Symantec also reported that earlier versions of the WannaCry ransomware were linked to the Lazarus Group.

230. The following sections discuss two key points.

a. First, as described in more detail in Part X.B below, evidence indicates that the same author or authors created WannaCry Versions 0, 1, and 2. This is based on the facts that:

i. most core components of Versions 1 and 2, excluding the propagation capability, are nearly identical to each other; and Version 0 is also largely similar to Versions 1 and 2;

ii. the source code for Versions 0 and 1 does not appear to be currently publicly available, let alone to have been publicly available at the time that Version 2 was released;

iii. similar passwords were used in all three versions;

iv. several forensic artifacts link the three versions; and

v. Bitcoins that victims of Versions 1 and 2 paid the subjects to decrypt their computers were subsequently cashed out and transferred using browsers with the same exact User-Agent string,[32] and the Bitcoin "cashouts" followed a similar pattern of laundering.

---

[32] In internet web browsing using HTTP, a User-Agent string is used to detect specific information about the client system, software, and browser making the request, which allows the web server to choose how to optimally provide data back to the client. For example, the website may present a slightly different version for a computer visiting that site when it is using a Mac operating system versus when the computer visiting the site is using a Windows operating system.

b. Second, as discussed in more detail in Parts X.C–X.D below, evidence indicates that all three WannaCry versions were authored by the North Korean subjects of this investigation. This is based on the facts that:

i. Version 0 used the identical FakeTLS table (discussed above) that was found in a passive state in malware used by the subjects in the other intrusions discussed in this affidavit, suggesting that these different pieces of malware were compiled by author(s) who had access to the same library of code;

ii. Version 0 (which did not spread widely) and two variants of the "Destover" malware—malware that the Symantec report indicated was related to the malware used in connection with the SPE cyber-attack—were found infecting the computer network of a single victim;

iii. an IP used for command and control by the malware that spread Version 1 (a dropper referred to as Backdoor.Bravonc or Trojan.Bravonc) was also compromised by the Brambul worm and used by the subjects of this investigation to access an account (*i.e.,* rasel.aflam@gmail.com) used in connection with intrusions at other victims discussed in this affidavit;

iv. the above-mentioned malware that spread Version 1 and other malware attributed to the Lazarus Group have similarities and also use similar infrastructure;

v. an IP address used for command-and-control in connection with Version 1 was accessed by North Korean IP addresses in 2016; and

vi. subjects using North Korean IP Address #6 were reading information regarding the development of code that would exploit the CVE-2017-0144 vulnerability that was used in WannaCry Version 2.

B. Similarities in the Three Versions of WannaCry

231. I learned from an FBI computer scientist and several private sector security companies' published reporting that most components of WannaCry

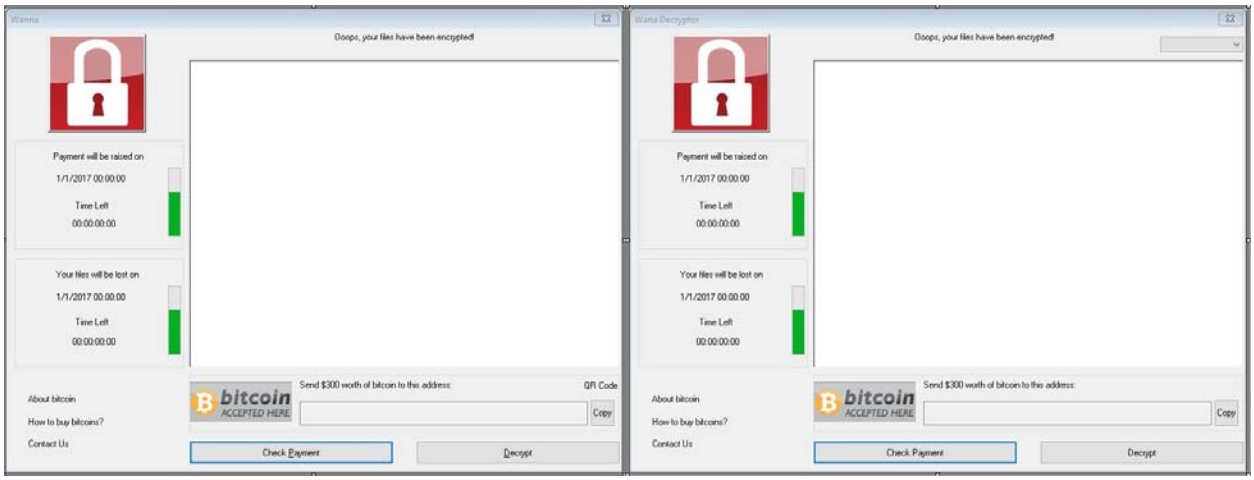
Versions 0, 1, and 2 are substantively identical in both form and function across the different versions. In function, each version encrypts the files on a victim's computer and presents a demand for Bitcoin. In form, the operation of the programming components of each version work in the same way. This alone is a strong indication that the author(s) of WannaCry Version 2 were also the author(s) of WannaCry Version 1.

a. Both Versions 1 and 2 encrypt a victim's files using a piece of malware (the "encryption tool") that is stored on the victim computer's hard drive in an encrypted state, then decrypted and executed from the computer's memory by another piece of malware (the "installer tool"). The encrypted form of the encryption tool in Version 1 is named "t.wry," whereas in Version 2 it is named "t.wnry." Most of the functions are nearly identical in each version of the encryption tool, with only minor changes that do not affect the overall manner in which it functions to encrypt victims' files. Version 0 does not have a separate encryption tool, but instead implements the encryption capability directly in the installer tool. However, the portions of the Version 0 installer tool implement the encryption functions in a nearly identical fashion to the encryption tools in Versions 1 and 2.

b. The installer tools of Versions 0, 1, and 2 deploy a piece of malware (the "decryption tool") purportedly to decrypt the files of users who paid the ransom. The installer tool for Version 1 initially deploys the decryption tool with the filename "u.wry" before changing it to "!WannaDecryptor!.exe," whereas Version 2 initially names it "u.wnry" before changing it to "@WannaDecryptor@.exe." The decryption tool is implemented in a nearly identical fashion in each version, with only minor changes that do not affect the overall manner in which it functions to decrypt files of victims who have been confirmed to

have paid the ransom.[33] Although the Version 0 decryption tool is somewhat simpler in certain respects, it contains very similar code to Versions 1 and 2 to decrypt files, and large portions of it are identical to portions of the later versions of the decryption tool. Furthermore, unlike other components of WannaCry that run in the background without the victim's awareness, the decryption tool has a visible user interface. As illustrated below, Versions 1 and 2 have a nearly identical interface.

Decryption tool – Version 1 **Decryption tool – Version 2**



c. The source code for Versions 0 and 1 had not been publicly found or released before Version 2 was found infecting computers on May 12, 2017, based on my searches and searches by other FBI personnel of malware repositories, my communications with cyber security and antivirus companies who investigated WannaCry, and my review of published reports about WannaCry (which in the aggregate are the conclusions of companies that have significant visibility into the

[33] Some anecdotal reports indicate that victims of WannaCry Version 2 were able to decrypt their files. *E.g.,* https://qz.com/985093/inside-the-digital-heist-that-terrorized-the-world-and-made-less-than-100k/. A private sector security researcher reporting in open sources has confirmed that the malware is technically capable of decrypting a victim's files upon presenting the correct value of the decryption key. However, no automatic mechanism exists to associate a victim's payment information with her or his decryption key; the victims who were able to decrypt their files could only do so after contacting the actor(s) to provide proof of their payment. *See*: securingtomorrow.mcafee.com/executive-perspectives/wannacry-really-ransomware/.

presence and use of malware and some of which have monitored criminal forums). Consequently, for the reasons described above in paragraphs 184–184.b, it is likely that the authors of Versions 0, 1, and 2 were either the same person or persons who shared access to the same source code.

d. While the three versions of WannaCry (first observed in February, April, and May 2017, respectively) have some differences (hence, they are different versions), the versions are generally very similar to each other. The changes that have been made reflect "improvements" in sophistication of the software. For example, Version 0 implemented essentially no safeguards to conceal its file encryption capabilities from either cyber security researchers or antivirus software, whereas Version 1 placed its encryption capabilities in a separate, encrypted module that is only decrypted when it is temporarily stored in the victim computer's memory in order to execute; Version 2 followed the exact paradigm as Version 1 in this respect.[34] These changes, which involved more than simply minor modifications to the source code, would have been difficult to make without access to the source code, for the reasons discussed in paragraph 184–184.b. The changes made in WannaCry Versions 1 and 2, made while retaining the common form and function attributes described above, are thus consistent with having been made by a person or persons with access to the source code for each earlier version, rather than by separate individuals or groups who had reverse-engineered it.

232. The three WannaCry versions also used similar passwords inside the malware: "wcry@123"; "wcry@2016"; and "WNcry@2ol7". While this itself is not

---

[34] While antivirus companies scan for known malicious files, many also employ heuristic analyses that seek to discover patterns of malware behavior that may indicate malicious activity, even if the specific file in which the behavior is exhibited is not already known. Here, because Version 1 placed its encryption capabilities into a separate, encrypted module, that module could not be examined as easily by many antivirus programs. In contrast, in Version 0 the encryption capabilities (*i.e.*, that it would encrypt large portions of the victim's computer) were more "exposed" to antivirus analysis.

conclusive, the fact that there are similarities in the passwords used is another factor suggesting that the same person(s) were responsible for each version of the malware.

233. Moreover, the FBI's Cyber Behavioral Analysis Center ("CBAC") conducted a detailed analysis of the malware and associated files used in the WannaCry attack and found the following, concluding that all three versions of WannaCry were likely created by the same author(s):

a. The WannaCry Versions 0, 1, and 2 were all compiled using Visual C++ 6.0.

b. The computer used to create the ransomware language files had the Korean language fonts installed, as evidenced by the Rich Text Format ("RTF") tag "\fcharset129," which is not typically included on a RTF file from a default Windows U.S. installation, but would be included on a RTF file from a default Windows Korean installation. Specifically, this tag indicates the presence of a Hangul (Korean) character set on the computer. In contrast, other character sets are accompanied by different \fcharset numerical tags.

c. The language files of each version contained an RTF tag "\datastore" that held pertinent metadata in the form of hidden UTC timestamp "ModifyTime," which is stored as an 18-digit Lightweight Directory Access Protocol ("LDAP") timestamp. A comparative analysis of this UTC timestamp against the standard RTF revision time "\revtime" timestamp led the CBAC to conclude that the computer used to author the ransomware language files may have been set to the UTC +09:00 time zone, which is the time zone used in South Korea and formerly in North Korea.

i. According to publicly available information, until August 2015, North Korea used the same time zone as South Korea, UTC +09:00. On August 15, 2015, the 70th anniversary of North Korea's liberation from Japan, the

government of North Korea began using Pyongyang Time (PYT), which is UTC +08:30.

d. The ransomware language files were likely authored in English by a non-native English speaker.

e. The ransom notes for Versions 1 and 2 were created using Microsoft Word 2007 or later, and the author and last person to edit the ransom note files in each of those Versions was listed as "Messi." There were only slight differences in the verbiage and formatting between the two, and the metadata associated with the ransom note in Version 1 indicated that it had been edited for 156 minutes, while the metadata for the ransom note in Version 2 indicated it had been edited for only four minutes, suggesting that the ransom note for Version 1 had been used to create the ransom note for Version 2.

234. Finally, the Bitcoin ransom payments by victims of WannaCry Versions 1 and 2 were both transferred from a Bitcoin wallet to a cryptocurrency exchange using a browser with the same User-Agent string, and Bitcoin from victims of Version 1 and Version 2 were both transferred through some of the same cryptocurrency exchanges and ultimately converted to another cryptocurrency, Monero. Specifically, the subjects undertook the following transactions.

a. Ransoms paid by victims of WannaCry Version 1 were paid into Bitcoin wallets. On July 20, 2017, a series of transactions occurred that moved all of the ransom payment proceeds from the Bitcoin wallets associated with WannaCry Version 1. After the funds were sent to a currency exchange, the funds were converted to Monero, another cryptocurrency. At least some of the transactions occurred from five IP addresses that have been identified as exit nodes

for the TOR network,[35] and used the same browser User-Agent string "Mozilla/5.0 (Windows NT 6.1.; rv:52.0.) Gecko/20100101 Firefox/52.0."

b. As with Version 1, ransoms paid by victims of WannaCry Version 2 were also paid into Bitcoin wallets. Estimates as of early-August 2017 indicate that approximately 330 victims paid the ransom demanded by WannaCry Version 2 totaling over $140,000. On August 3, 2017, the ransom payments from the victims of the WannaCry Version 2 ransomware were transferred from the original Bitcoin addresses to other cryptocurrency addresses in a series of transactions. As with the laundering of the ransoms associated with Version 1, following the Version 2 ransoms being sent to currency exchanges, the funds were converted to Monero. At least some of those transfers used IP addresses that have been identified as exit nodes for the TOR network, and used the same browser User-Agent string, "Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0."

c. While a User-Agent string is not a particularly distinct identifier (like a fingerprint or a hash value would be), when User-Agent strings match across certain web activities, it can be an indication that the same user or computer may be conducting them. The specific User-Agent string observed in conducting the transfers (noted in paragraph 234.a) corresponds to the same browser used in an "alpha" release of the TOR application at the time of the activity (meaning it was not fully tested and could be unstable), but it does not correspond to the browser then used in what is referred to as the "stable" version of the TOR application. The "stable" version is more widely used and is the version a user ordinarily downloads through the TOR website. Thus, while the IP addresses used to transfer the bitcoins were both TOR nodes, the User-Agent string shows that the computer(s)

---

[35] "The Onion Router," also known as "TOR" or "Tor," is an anonymizing software that directs users' internet traffic through a random series of servers or nodes in order to obfuscate the origin of traffic.

used to effect the transfers from Version 1 and Version 2 used the same, less-common version of the TOR application to do so.[36]

235. Taken in sum, the evidence described above indicates that WannaCry Versions 0 and 1 were likely created by the same person or persons who created Version 2.

C. Links Between WannaCry and Other Intrusions Described Above

236. The evidence also suggests that the person(s) who created WannaCry Versions 0 and 1 (and therefore WannaCry Version 2) were the same subjects responsible for other intrusions discussed in this affidavit, including the cyber-attack on SPE, intrusions at Bangladesh Bank and other financial institutions, and targeting of U.S. defense contractors. That evidence is discussed below.

237. First, the FakeTLS table discussed above in Part VIII.D.4 provides one of the strongest links between the subjects discussed in this affidavit and WannaCry. Specifically, the same FakeTLS table in WannaCry Version 0 was also found in all three samples of MACKTRUCK malware found at SPE, the MACKTRUCK malware found in a spear-phishing document sent to an individual who dealt with North Korean policy by one of the accounts that was linked to the targeting of Lockheed Martin, the Contopee backdoor used in the intrusions at the Philippine Bank,[37] the Contopee backdoor used at the Southeast Asian Bank, and

---

[36] That User-Agent string would also be generated by a user who happened to choose that specific version of Firefox, but the fact that it is a version used by the TOR application and a TOR IP address was used to effect the transfers indicates it is more likely the result of using the same version of the TOR application.

[37] As noted in paragraph 179.d, there is a strong connection between the intrusions at the Philippine Bank and Bangladesh Bank. Specifically, the NESTEGG backdoor malware—also found at Bangladesh Bank—was deployed throughout the Philippine Bank's network in a computer intrusion from November of 2015 to January of 2016, shortly before the subjects sent the fraudulent SWIFT messages from Bangladesh Bank. These intrusions are also linked to the subjects,

the NESTEGG sample found at the Philippine Bank. For the reasons discussed in paragraphs 184–184.b above, it is unlikely that the FakeTLS table would be in these versions of malware if the authors were not the same person or persons.

238. Second, in the May 22, 2017 Symantec research report, noted in paragraph 229, Symantec analyzed the first WannaCry-related attack it had identified from February 2017 (a WannaCry Version 0 attack) based in part on evidence obtained from the computer network of a victim. The report contained the following information:

a. *First*, Symantec identified three samples of Lazarus Group malware on the victim's network, including two variants of Backdoor.Destover, which was also used against SPE (*see* paragraph 89), and one variant of Trojan.Volgmer, which Symantec identified in a December 2014 blog post[38] as being used against South Korean victims and linked to malware used against SPE.

b. *Second*, WannaCry Version 1 was observed by Symantec as being spread by malware called Trojan.Alphanc and Trojan.Bravonc, which Symantec described as a modified version of Backdoor.Duuzer, a common Lazarus Group malware family. Several tools that were used in the February 2017 WannaCry Version 0 attack were also used in the March to April 2017 WannaCry Version 1 attacks, including a credential dumper called mks.exe and a dropper tool that was renamed from hptasks.exe to bcremote.exe.

c. *Third*, the above-mentioned Trojan.Bravonc associated with WannaCry Version 1 used a Saudi Arabian IP address, 87.101.243.252, for command-and-control purposes. That same Saudi Arabian IP address was also used by some samples of the aforementioned Lazarus Group tools Backdoor.Duuzer

---

and thus together, by the DDNS accounts managed by the same device or devices, which were discussed in paragraphs 165–166.

[38] https://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea

and Backdoor.Destover. (As discussed in more detail in paragraph 240.b, that same Saudi Arabian IP address, and others used by WannaCry Version 1, were compromised by the Brambul worm and used by the subjects of the investigation.)

d. *Fourth*, Trojan.Bravonc, which was used to spread WannaCry Version 1, obfuscated parts of its code in a way similar to WannaCry Version 1. Those two samples—Trojan.Bravonc and WannaCry Version 1—also obfuscated their code in a similar way to Infostealer.Fakepude, which Symantec previously identified as being used by the Lazarus Group. (For example, obfuscating code can include concealing the types of "system calls" to cause particular functions in the operating system to be performed, so that what the executable file is doing is more difficult to discern.) A malware report[39] on Infostealer.Fakepude shows that this malware used the DDNS domains checkupdates.flashserv.net, download.ns360.info, and update.craftx.biz.

i. These three domains were previously identified by Symantec in July 2016 as being related to the Contopee backdoor used in the intrusions of financial institutions. They were all hosted by a DDNS provider, where one or more had been controlled at one time or another by accounts registered using four different email addresses since at least November 2013.

ii. Those same four email accounts also had all been used to register for accounts at a different DDNS provider, which accounts were accessed using the same device or devices that were used to access the accounts that controlled the domains used in the intrusions at multiple banks, identified above in paragraphs 165–166. For example, an email account that controlled two of the above domains used in Infostealer.Fakepude (download.ns360.info and

[39] https://www.symantec.com/security_response/writeup.jsp?docid=2016-040409-4542-99&tabid=2

update.craftx.biz) was also in control of two domains (repview.ignorelist.com and statis.ignorelist.com) used in a version of Contopee found at the Philippine Bank.

e. *Fifth*, Symantec and BAE Systems identified shared code between WannaCry Version 0 and the Contopee sample referenced in paragraph 183 (used by the Lazarus Group) in reports dated May 22, 2016 and May 16, 2017, respectively.[40] Symantec identified one version of Contopee that used a custom communication protocol that was intended to look like Secure Socket Layer ("SSL") or TLS that used an identical cipher suite as WannaCry Version 0. (Although one report referred to a single cipher suite, the malware generates a list of cipher suites, as described in more detail in paragraph 183–183.d.)

i. The cipher suite is what is generated using the FakeTLS data table discussed above in Part VIII.D.4. Thus, the Symantec report cited not only the existence of the FakeTLS data table within the code, but also that WannaCry Version 0 uses the data table for FakeTLS communications, as does a version of Contopee.

ii. In Version 0, this FakeTLS communication protocol was used to report back to the subjects' command-and-control infrastructure, for example to confirm and identify a victim that had been infected and to upload private keys. Subsequent versions of WannaCry used the TOR network for this function instead of FakeTLS.

239. The links between toolsets and shared code identified by Symantec and other researchers are significant and demonstrate an evolution of the attack tools used by the subjects over the course of several years. For the same reasons described above in paragraph 184–184.b, it would be difficult for a new malware

[40] https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group; http://baesystemsai.blogspot.com/2017/05/wanacrypt0r-ransomworm.html.

author(s) to simply cannibalize or re-use portions of existing WannaCry code even if the author(s) had access to the earlier versions of WannaCry, making it unlikely that new author(s) are responsible for these similarities. Rather, it is much more likely that the same persons with access to the same common library of source code generated each malware. Additionally, many of the sections of code used in these malware versions have been analyzed for uniqueness, and one private security company has stated to the FBI that particular snippets of code used in WannaCry only appear in malware that has been used by or attributed to the Lazarus Group.

240. Third, as discussed below, malware discussed above that is connected to WannaCry Version 1 has also used IP addresses that the particular subjects of this investigation have successfully compromised and used for malicious purposes. Specifically:

a. Both a WannaCry sample and Trojan.Alphanc used IP address 84.92.36.96 as a command-and-control IP address, according to Appendix A of the May 22, 2017 Symantec report. (That IP address was also a command-and-control address for a sample of malware obtained by the FBI that drops a malware payload in a similar way to how other malware that private cyber security companies have attributed to the Lazarus Group,[41] as well as malware that the subjects used to target Lockheed Martin.) On February 29 and March 1, 2016, a North Korean IP Address connected to that IP address. This North Korean IP address, the same IP address referenced in footnote 1, was used during the shift in IP addresses from January 2016–March 2016. Specifically, this North Korean IP address was used to access the Compromised Web Server, on January 8, 2016; on January 22 and 27, 2016, it also connected to a compromised computer in North Carolina that was infected with malware linked to the attack on SPE; and, on March 10, 2016, it was

[41] https://researchcenter.paloaltonetworks.com/2017/04/unit42-the-blockbuster-sequel/

used to access a Facebook profile that previously had been accessed from North Korean IP Address #2 on December 13, 2015.

b. As noted above in paragraph 238.c, Trojan.Bravonc was used in connection with WannaCry Version 1 and it used as a command-and-control server a Saudi Arabian IP address, 87.101.243.252; this same IP address was used by Backdoor.Duuzer and Backdoor.Destover, which have been linked to the Lazarus Group. Of note, this Saudi Arabian IP address had been compromised by the Brambul worm and thus was accessible to the subjects of this investigation since at least April 2015. Specifically, on April 9, 2015, whiat1001@gmail.com, one of the Brambul collector email accounts, received an email with a subject of "87.101.243.252|[USERNAME REDACTED]|[PASSWORD REDACTED]," and on June 25, 2015, mrwangchung01@gmail.com, another Brambul collector email account, received an email with a subject of "87.101.243.252|[USERNAME REDACTED]|[PASSWORD REDACTED]|[OPERATING SYSTEM AND OTHER SYSTEM DETAILS REDACTED]." On August 12, 2015, the subjects used the same compromised IP address to create the email account rasel.aflam@gmail.com, which was used to send spear-phishing emails to numerous banks in Bangladesh. These spear-phishing emails were virtually identical to those sent to Bangladesh Bank in August 2015. (*See* paragraphs 148–149 and 162–163.)

c. The U.S. IP address 184.74.243.67, which is listed in Appendix A of the May 22, 2017 Symantec report, is identified as a command-and-control IP address for Trojan.Alphanc, which was used to spread WannaCry Version 1. This U.S. IP address was also used to access the email account jonnie.jemison@gmail.com on nine separate days between August and November 2016. During roughly the same period of time (September to November 2016), North Korean IP Address #6 was also used to access jonnie.jemison@gmail.com. Jonnie.jemison@gmail.com used a recovery email address of

changtony1989@hanmail.net, which was used to create a Facebook account used by the subjects for reconnaissance. That particular Facebook account was also accessed by an IP address that appeared in the subject line of an email received by a Brambul collector email account (meaning that Brambul had compromised that IP address), and had been accessed by two other IP addresses that were used to directly access one of the Brambul collector email accounts.

d. The South African IP address 196.45.177.52 is listed in Appendix A of the May 22, 2017 Symantec report as one used by a backdoor and as making up part of the "WannaCry and Lazarus shared network infrastructure." That IP address, along with a compromised username and password, appeared in the subject of an email sent on June 23, 2015 to xiake722@gmail.com (a Brambul collector email account) indicating the subjects had access to that IP address since June 2015.

241. Fourth, as mentioned above, FBI's CBAC determined that WannaCry Versions 0, 1, and 2 were all created using Visual C++ 6.0. Moreover, BAE Systems[42] has determined that this same development environment—Visual C++ 6.0—was used to create malware used in the Bangladesh Bank cyber-heist and the intrusion at the Vietnamese Bank. This alone is not a dispositive link, as Visual C++ 6.0, released in 1998, still has proponents mostly because it does not require the installation of Microsoft's .NET framework in order to run, as later versions of Visual C++ do. However, based on my own review of malware and my communications with FBI computer scientists and private security companies, I know that the majority of malware attributed to North Korea was created using Visual C++ 6.0 when the malware is 32-bit, as the WannaCry versions are (and is created using Visual C++ 10.0 when the malware is 64-bit). (As noted below in

[42] https://baesystemsai.blogspot.com/2017/05/wanacrypt0r-ransomware.html

paragraph 282, PARK's résumé indicated that he was skilled in Visual C++.) This is thus another similarity between all versions of WannaCry and the other malware discussed in this affidavit.

D. Evidence Shows Subjects Were Following Exploit Development

242. Records that I have obtained show that the subjects of this investigation were monitoring the release of the CVE-2017-0144 exploit and the efforts by cyber researchers to develop the source code that was later packaged into WannaCry Version 2:

a. On numerous days between March 23 and May 12, 2017, a subject using North Korean IP Address #6 visited technet.microsoft.com, the general domain where Microsoft hosted specific webpages that provide information about Microsoft products, including information on Windows vulnerabilities (including CVE-2017-0144), although the exact URL or whether the information on this particular CVE was being accessed is not known.

b. On April 23, April 26, May 10, May 11, and May 12, 2017, a subject using North Korean IP Address #6 visited the blog website zerosum0x0.blogspot.com, where, on April 18, 2017 and 21, 2017, a RiskSense researcher had posted information about research into the CVE-2017-0144 exploit and progress on reverse-engineering the exploit; RiskSense subsequently released the exploit code on GitHub.com.

243. Finally, as noted above in paragraph 233.e, the name of the authors listed in the metadata of ransomware language files for both Version 1 and Version 2 was "Messi." The subjects of this investigation have also used the name of soccer star Lionel Messi—specifically, in the creation of an email account messilionel.messi2015@yandex.com, which was used as a recovery email address for jamesmartin20162016@gmail.com. According to records from Google, jamesmartin20162016@gmail.com used the Korean language setting.

a. Jamesmartin20162016@gmail.com was created on October 22, 2015 from North Korean IP Address #2. As noted above in paragraph 197.c, the Compromised Web Server was accessed from North Korean IP Address #2 in February, April, May, June, July, and December 2015, both before and after it was used to create jamesmartin20162016@gmail.com. That North Korean IP address had also been used to access the email account jongdada02@gmail.com in May 2015 and August 2015. (*See* paragraphs 216–217.)

b. Jamesmartin20162016@gmail.com was accessed on May 24, 2016 from North Korean IP Address #6. That same North Korean IP address was used the next two days, May 25 and 26, 2016, to access the @erica_333u Twitter account that posted a malicious link targeting "The Interview" and actors in it (*see* paragraph 111). As noted above in paragraph 197.c., the Compromised Web Server was accessed from North Korean IP Address #6 on March 22, 2016, two months before it was used to access jamesmartin20162016@gmail.com.

244. Taken in sum, this evidence indicates that the subjects discussed in this affidavit were responsible for the cyber-attack against SPE, computer intrusions of Bangladesh Bank and other financial institutions, and targeting of U.S. defense contractors, as well as for authoring WannaCry Versions 0, 1, and 2.

XI. THE "KIM HYON WOO" PERSONA

245. This Part discusses the subjects' use of the persona of "Kim Hyon Woo," and variants of that name, in opening numerous email and social media accounts. The subjects of the investigation have used those accounts (and that persona) in connection with the attack on SPE, cyber-heists against financial institutions, and targeting of U.S. defense contractors. While this Part (Part XI) describes the accounts using the alias "Kim Hyon Woo" and their connections to some of the operational infrastructure described above, the following Part (Part XII) describes Chosun Expo Accounts used by or connected to PARK. Part XII details

the connections between the "Kim Hyon Woo" accounts and the Chosun Expo Accounts that in turn are connected to PARK.

246. It is important to note that according to FBI Korean linguists, the Korean character "우" can be translated to English as "Woo," "Wu," or "U." As described in this section, the subjects have used both the Korean character "우" and the English transliterations "Woo," "Wu," and "U"—sometimes interchangeably—when making "Kim Hyon Woo" alias accounts. Given the multiple possible transliterations, where this affidavit describes evidence containing the character "우," it is translated as "Woo."

A. tty198410@gmail.com

247. As discussed above, tty198410@gmail.com was used to subscribe the "Andoson David" Facebook account, watsonhenny@gmail.com, MrDavid0818@gmail.com, and @hyon_u. It was accessed by the same device as watsonhenny@gmail.com, yardgen@gmail.com, and the Brambul collector account mrwangchung01@gmail.com. And it exchanged test spear-phishing messages with yardgen@gmail.com and jasmuttly@daum.net.

248. Provider records show that tty198410@gmail.com was created on September 1, 2011, using the name "K YM," and a recovery email address of hyon_u@hotmail.com, and from September 2014 through May 2015 was accessed exclusively from Proxy Service IP addresses. The time zone settings in the account's calendar were set to Asia / Pyongyang (the capital of North Korea).

249. Provider records show that the account was consistently used with the name "Kim Hyon Woo" and variants thereof. For example, in November 2013, tty198410@gmail.com was used to sign-up for an account at Rapid 7—a security and analytics company that offers the widely-used network penetration testing platform Metasploit—under the names "kim hyonw" and "kim hyon woo." At one point, Rapid 7 terminated connections for the tty198410@gmail.com account because the

connections originated from a North Korean IP address and from an IP address in the Chinese block 210.52.109.0–210.52.109.255 that is used by North Korea. A later connection was allowed from an IP address that was not in the North Korean IP block or this Chinese IP block. In another example, tty198410@gmail.com was used to create a profile at a cyber security company's website with a user name of "Kim HyonWu."

B. hyon_u@hotmail.com

250. Hyon_u@hotmail.com was used as the recovery email for tty198410@gmail.com. It was created on April 13, 2007, used Korean language resources, listed a location of Seoul, Korea, and used a name of 현우 김, which translates to "Hyon Woo Kim" or "Kim Hyon Woo."

251. The FBI discovered that hyon_u@hotmail.com was used to subscribe an account at a foreign software development website on April 23, 2007, where it used the name "김현우," which translates to "Kim Hyon Woo." That account was accessed using several North Korean IP addresses. Provider records show that the account at that website, hosted in a foreign country, was accessed primarily from North Korean IP addresses (including North Korean IP Address #2 on February 25, 2014) or the Proxy Services, and that it viewed articles on topics related to hacking and computer software, like injecting code into a portable executable file, and hiding executable code within an image file. (Tty198410@gmail.com also created an account with the same website in June 2014 and only used it during that month. The name used to create that account shared similarities with the names of multiple other email addresses used by the subjects for spear-phishing, including [JG NAME REDACTED]@gmail.com and agena316@gmail.com (*see* paragraph 130.a and 130.b).)

C. hyonwoo01@gmail.com

252. Two other accounts besides tty198410@gmail.com are known to have used hyon_u@hotmail.com in their subscriber records. The first was hyonwoo01@gmail.com, which was created in 2011 using the previously mentioned Korean name that translates to "Kim Hyon Woo." The subject using that account conducted internet research regarding computer programming-related terms, including in March 2011 related to VC++, which appears to be a reference to the Visual C++ software development environment, discussed above in paragraph 241.

253. Significantly, on March 16, 2011, hyonwoo01@gmail.com received a series of emails from a spoofed email account (xxxx@gmail.com) that attached a number of files. An FBI computer scientist was able to reconstruct the files attached to those separate emails into one database, which the computer scientist was able to determine had contained a significant amount of deleted data that was able to be recovered using a data recovery tool. The recovered database contained tables labeled Agent, Object, Proxy, and Server. The "Agent" table appeared to contain names/identifiers of computers controlling other computers (*i.e.*, a command-and-control computer). The "Object" and "Server" tables contained a number of columns about individual computers (such as a MAC address) which seemingly reflected compromised computers; a column titled "TroyVersion," and the Server table contained a column titled "TroyPort." These columns "TroyVersion" and "TroyPort" appear to contain data related to particular versions or computer port numbers used by the installed malware, and the values were either blank, 0, 1, 153, 163, 65537, 65538, or 131074. In a column of the Server table called "Special," several entries in the database have what appear to be notes written by the database author, with some entries containing notes such as "vnc worm, proxymini-3128(sqlsrv32.exe)," "proxymini-443(ccEvtSrv.exe)," and "ver 1.0,

ccEvtSrv.exe(proxymini), reproxy-443(nod32krn.exe)." ("Proxymini," is a legitimate proxy server application, and is discussed further in paragraph 333.g.)

254. In 2013, two years after these emails containing the tables were sent to hyonwoo01@gmail.com, cyber security researchers at McAfee Labs authored a report on multiple cyber-attacks between 2009 and 2013 targeting victims in South Korea that included victims in the financial, media, and defense sectors, culminating with a destructive malware attack against South Korean financial companies known in the cyber security industry as "Dark Seoul." McAfee Labs referred to the attack campaigns as "Operation Troy" because there were numerous references to "Troy"—such as "Make Troy"—directly in the malware used in the attacks. As a result of the Dark Seoul attack, tens of thousands of computers in South Korea were rendered inoperable.

255. I have consulted with an anti-virus company about the contents of this database, and out of the 679 IP addresses listed in it, 46 were known to the anti-virus company through malware it had identified. Those malware samples were compiled in September 2010 and March 2 and 3, 2011 (just before hyonwoo01@gmail.com received the emails with the database on March 16, 2011). Of those malware samples, three of them (their hash values) were referenced in the public report and indicators of compromise published by McAfee about Operation Troy.

256. Given that DarkSeoul was carried out using malware with references to "Troy," and the database containing lists of infrastructure sent to hyonwoo01@gmail.com contained references to "Troy" and an apparent list of compromised computers along with IP addresses that were used in connection with the DarkSeoul attack, this evidence suggests that the subject or subjects using hyonwoo01@gmail.com was also involved in carrying out the DarkSeoul attack and maintained the list of infrastructure needed for it.

257. Further, there are stylistic similarities between the computer defacement graphics used in both the DarkSeoul and SPE attacks. Below is a side-by-side depiction of the defacements—that is, the images that appeared on computers that were attacked during DarkSeoul (on the left) and SPE computers (on the right).

a. Furthermore, examination of the metadata embedded within the Photoshop image(s) composing the SPE defacement, showed that it was created (2014-11-23T10:37:41 +09:00), modified (2014-11-23T11:29+09:00), converted from .bmp to .jpeg (2014-11-23T11:28:20+9:00), and saved (2014-11-23T11:29+09:00) all in a time zone that was UTC +09:00.

b. This is the time zone used by North Korea at the time that the Dark Seoul and SPE cyber-attacks were launched. This same time zone was also referenced in the WannaCry ransomware. (*See* paragraph 233.c.)

D. hyonwu@gmail.com

258. Hyonwu@gmail.com also used hyon_u@hotmail.com as its recovery account. It was created on April 29, 2007, using the same Korean name that

translates to "Kim Hyon Woo." In 2007, the user of that account read an article that appeared to be related to North Korean food rationing.

E. @hyon_u

259. The first Twitter account to follow @erica_333u, which sent a link to malware hosted on the Compromised Web Server, was @hyon_u. The email account used to register it was tty198410@gmail.com, which, as discussed above and in more detail below, has numerous connections to the Chosun Expo Accounts. Moreover, the name initially associated with the Twitter account @hyon_u was "Kim hyon wu," but it was later changed to "Infosec."

260. Twitter account @hyon_u was accessed by a North Korean IP address in March 2016. Furthermore, watsonhenny@gmail.com, the LinkedIn account registered using watsonhenny@gmail.com, and the Twitter account @hyon_u were each accessed by the same two Proxy Service IP addresses between July 30 and August 4, 2015.

F. Brambul Collector Accounts

261. One of the Brambul collector accounts was xiake722@gmail.com. It was created on September 28, 2009, from a North Korean IP address, using the name "Kim HyonWoo." (A malware sample using this email account was mentioned in paragraph 191.c as sharing strings of text that matched malware used in the watering hole attacks.)

262. Another of the Brambul collector accounts, laohu1985@gmail.com, was created on October 14, 2009, from the same North Korean IP address. The name appearing in subscriber records is "Kim HyonWoo."

263. Moreover, a single Proxy Service IP address also was used to access mrwangchung01@gmail.com, a Brambul collector account, on May 18, 2015, just nine minutes before it accessed watsonhenny@gmail.com and less than three hours

after it was used to access tty198410@gmail.com. The same device was used to access all of those email accounts that day.

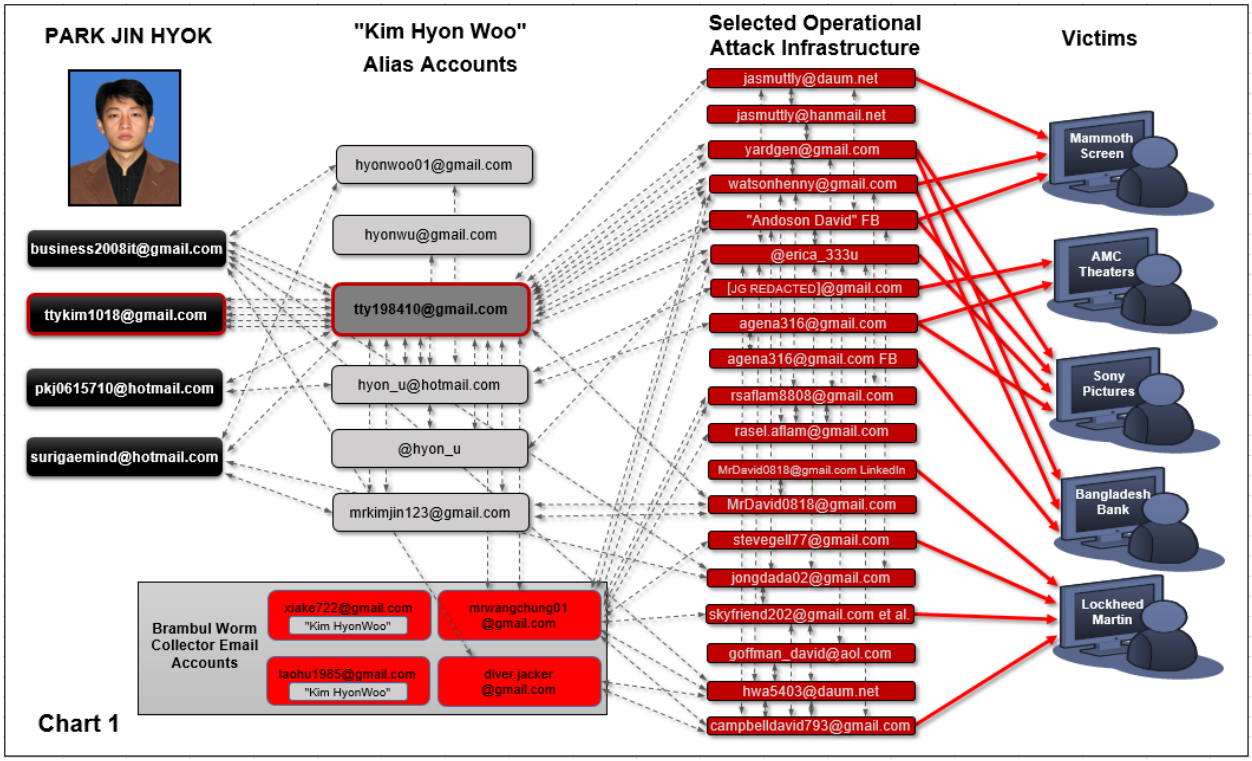
XII. PARK JIN HYOK

264. Although the name "Kim Hyon Woo" appeared in many of the operational accounts, the evidence gathered to date shows it is likely an alias that served as another layer to conceal the subjects' true identities. One of the identified subjects is PARK JIN HYOK, a North Korean programmer who was dispatched to Dalian, China,[43] where he worked for Chosun Expo until apparently returning to North Korea shortly before the attack at SPE. As described below, Chosun Expo, which is also known as "Korea Expo Joint Venture," is a North Korean government front company, and specifically one that generated currency for one of the North Korean government's hacking organizations that is sometimes known as "Lab 110." PARK accessed accounts that he used in his true name from China during the time he worked for Chosun Expo, and those accounts—the Chosun Expo Accounts—were accessed from North Korea after it appears he returned.

265. That PARK worked for Chosun Expo is itself significant—but PARK also has numerous connections to the operational accounts used in the name of the persona "Kim Hyon Woo" to carry out the computer intrusions discussed in this Affidavit. Those connections between PARK's Chosun Expo Accounts and "Kim Hyon Woo" accounts include shared access to an encrypted .rar archive, saving the "Kim Hyon Woo" accounts in Chosun Expo Accounts' address books, using read receipts between the two sets of accounts, using common names and monikers, and accessing accounts from common IP addresses, among others. These connections show that PARK was one of the persons—along with his co-conspirators—who had access to the operational infrastructure used to carry out the computer intrusions

[43] Dalian is a city in China's Liaoning province, which borders North Korea.

described herein. I know, based on my training and experience, that hackers generally do not allow strangers or other persons beyond their circle of trusted associates who are complicit and witting in their hacking to have access to their operational accounts or infrastructure. Those many connections, described in detail below and illustrated in part below in Chart 1, show that PARK was a member of the conspiracies:[44]



[44] Chart 1 contains connections between (1) the Chosun Expo Accounts used by PARK, (2) accounts used by the alias "Kim Hyon Woo," and (3) some of the accounts that were used as part of the subjects' attack infrastructure. Not all of the attack infrastructure accounts discovered throughout the investigation are included, rather only those with certain connections to Chosun Expo Accounts tied to PARK. The connections between the accounts include: the same device being used to access accounts; when one email was used to subscribe another account; common subscriber information or biographical information used; shared access to an encrypted file; "followed" using Twitter; stored contacts; shared alias or moniker; access using common or overlapping IP address; exchanging a test spear-phishing message or sending nearly identical spear-phishing messages to similar targets; using the same operational infrastructure to host malware; and other connections detailed herein.

266. I know, based on my training and experience, that sophisticated and well-resourced hackers will go to great lengths to conceal their locations and identities. They will often, as the subjects of the investigation did here, use various measures to avoid detection and identification, including: using layers of accounts and aliases to distance their identities and "true name" accounts from accounts or infrastructure that are used for criminal purposes; using different sets of IP addresses to access operational versus true name accounts; and avoiding accessing both operational and true name accounts from the same computer—at least without taking other measures to obscure their identities—so as not to reveal that the same person was using each.

267. Although the subjects were often successful in separating Chosun Expo Accounts and other true name accounts from the "Kim Hyon Woo" alias accounts and other operational accounts that made up their attack infrastructure, the numerous connections between the Chosun Expo Accounts and these other operational accounts that accumulated are significant and strong, and they suggest that the same individual or group of individuals accessed and controlled those accounts. Indeed, not only are these connections between the Chosun Expo Accounts and the "Kim Hyon Woo" accounts too numerous and significant to be a coincidence, they are meaningful and conclusive for the very reason that well-resourced hackers generally go to great lengths to separate their true identities from their alias identities and operational accounts.

268. Taken in sum, this evidence—enumerated in detail in the Parts that follow—shows that PARK was a member of the conspiracies described in this Affidavit that were responsible for the cyber-attacks and intrusions described above.

A. PARK's Work for Chosun Expo, a DPRK Government Front Company

1. Chosun Expo

269. As set forth below, Chosun Expo is a front for the North Korean government, based on: the account of a witness who had first-hand dealings with Chosun Expo; information provided to the FBI by a foreign investigative agency; the use of an operational email account by a North Korean government representative, which operational account was used maliciously for targeting victims and was also connected to Chosun Expo Accounts; the use of common IP addresses to access Chosun Expo's website and the Chosun Expo Accounts, as well as certain operational accounts; and the fact that both these Chosun Expo Accounts and operational accounts connected to them were used from North Korea.

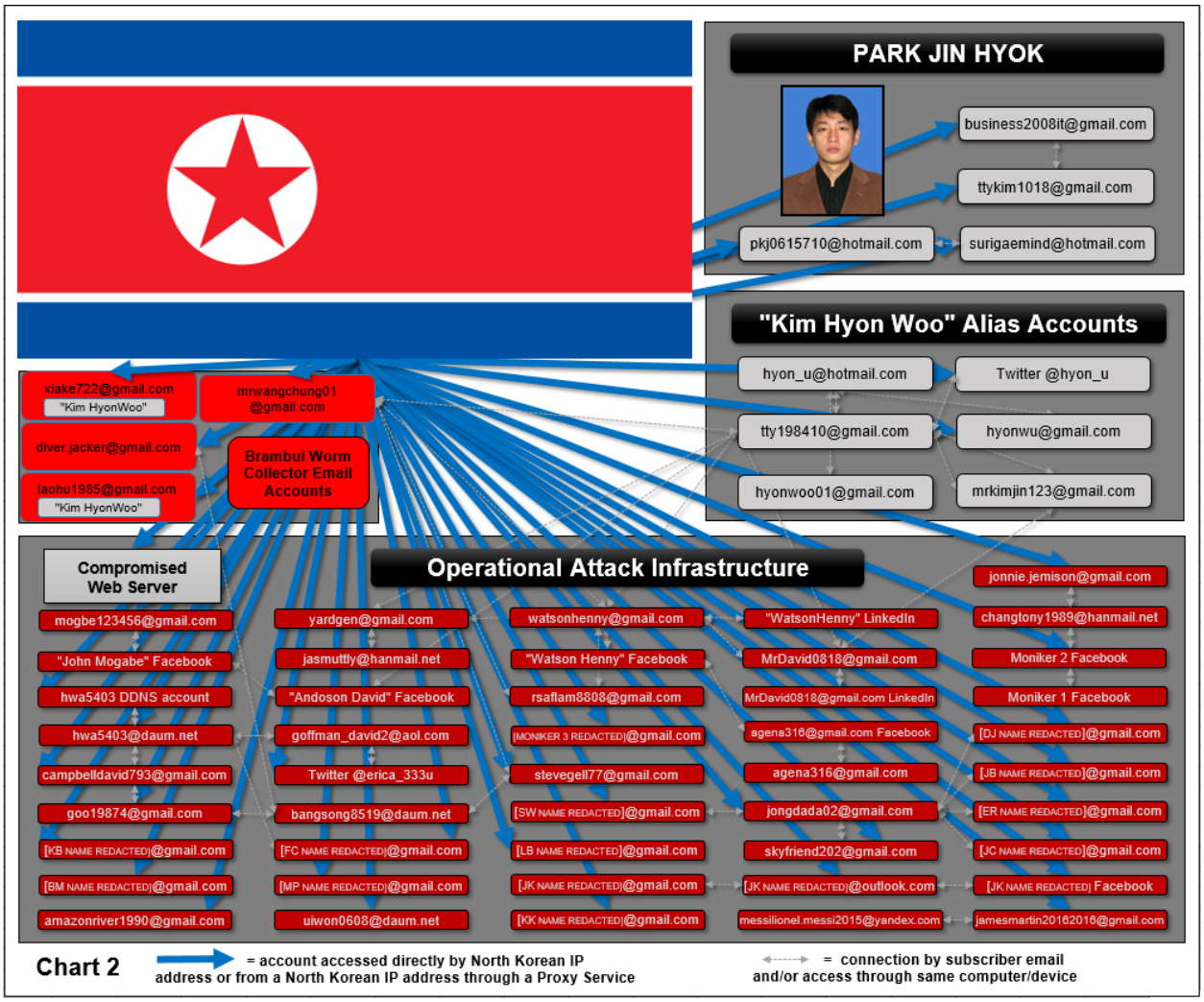
270. I have spoken with an expert on Korean matters who is cooperating with the FBI, who informed me that Chosun Expo was originally a joint venture between North Korea and South Korea established to be a Korean e-commerce and lottery website. Eventually, South Korea withdrew from the venture and North Korea maintained the business, which is known to supply various goods and services, including software, freelancing software development, and gambling-related products, some of which were offered through its website.

271. Emails in the Chosun Expo Accounts (discussed below in Part XII.B) show that PARK worked on these types of projects, and that at least some of the individuals who used the services of PARK and others working for Chosun Expo knew that they were North Korean computer programmers connected to the government. Based on information from a witness who had direct dealings with Chosun Expo, some employees of Chosun Expo who were dispatched to China kept only a very small fraction of their salary, remitting the rest to the government of

North Korea. While a Chosun Expo manager oversaw the work of those employees, they also had a separate political attaché monitoring them as well while in China.

272. I have spoken with experts on North Korean culture who have interviewed North Korean defectors, and have also read numerous articles on the ability of ordinary North Korean citizens to access the internet. My understanding, based on such articles[45] and interviews, is that only social "elites," government entities, certain university students with special permissions, and foreign visitors in North Korea have open access to the internet. And even those people and entities that might have access to the internet operate under the assumptions that (a) their internet use is heavily-monitored, often times by an individual who is physically present and watching their activities, and (b) any attempts to access information that might undermine or contradict the government regime will be swiftly punished. Most North Korean citizens do not have access to global websites and social media such as Google, Facebook, or Twitter. Accordingly, the use of accounts identified herein as accessed from inside North Korea was likely regime-sanctioned and approved, for these reasons and for others described in the paragraphs that follow. Chart 2 depicts the numerous email and social media accounts discussed in this affidavit that were accessed from North Korean IP addresses, as well as the other accounts accessed by the same devices or through email addresses used in subscriber records.

[45] *E.g.*, http://www.bbc.com/news/technology-20445632; http://www.slate.com/articles/technology/future_tense/2016/11/how_the_internet_works_in_north_korea.html



273. I have reviewed published reporting indicating North Korean cyber operations have been carried out using front companies, including ones operating in China. I have also learned from other agents and experts on North Korea that North Korean companies that operate abroad are under the control of the North Korean government.

274. According to information provided by a foreign investigative agency (*see* paragraphs 174 and 175), Chosun Expo, the North Korean government front company that employed PARK, registered the domain chosunexpo.com and earns foreign currency for an entity sometimes known as Lab 110, a North Korean

government hacking organization. An article published by an organization of North Korean dissidents resident in South Korea also identified Chosun Expo as providing cover for North Korean government officers.

275. Connections between Chosun Expo and the Chosun Expo Accounts, on the one hand, and malicious accounts used for cyber operations, on the other hand, support this conclusion. These connections include the use of the same IP addresses to access both malicious, operational accounts and accounts connected to Chosun Expo.

a. On September 25, 2013 and March 30, 2014, a particular U.K. IP address accessed the account used to register the domain for the Chosun Expo website and, on November 18, 2016, that IP address was also used to access Chosun Expo Account business2008it@gmail.com. The same U.K. IP address accessed a Facebook account registered to [JK NAME REDACTED]@outlook.com on June 12, 2015 and January 4, 2016. Both [JK NAME REDACTED]@outlook.com (the recovery account for [JK NAME REDACTED]@gmail.com, which spear-phished AMC Theatres employees on December 13 and 14, 2014 (*see* paragraph 130.e)) and the Facebook account registered to it were created from North Korean IP Address #2 on December 8, 2014. As discussed above, North Korean IP Address #2 has been consistently used to conduct malicious cyber activity, including being used in the cyber-attack on SPE, to access the Compromised Web Server, in the spear-phishing of Lockheed Martin, and to access "Kim Hyon Woo" alias accounts. (*See* paragraphs 75, 85, 96, 109, 216, and 251.)

b. On several days in October 2012, North Korean IP Address #3 accessed the account used to register the domain for the Chosun Expo website (chosunexpo.com), and it also accessed the Chosun Expo Account surigaemind@hotmail.com on March 2, 2015. As discussed in paragraph 147, North Korean IP Address #3 was used to access mobile devices connected to [MONIKER 3

REDACTED]@gmail.com in July, August, September, October, and November 2014, and January 2015. The user of that account conducted online reconnaissance regarding specific banks in Bangladesh, including Bangladesh Bank, that the subjects later targeted with spear-phishing messages.

c. As discussed more in paragraphs 308–308.f, on May 18, 2015 and August 10, 2015, Chosun Expo Accounts business2008it@gmail.com and surigaemind@hotmail.com, respectively, were accessed by a particular Switzerland IP address that was also used to access accounts used for spear-phishing in that same timeframe.

276. There are other specific connections between the DPRK government and the Chosun Expo Accounts. As already noted above, both the Chosun Expo Accounts and other malicious, operational accounts discussed in this affidavit were accessed or shared by multiple persons, including persons who have direct connections to the North Korean government. For example, in April and May 2015 (as noted in footnote 10), a person who was not PARK repeatedly used watsonhenny@gmail.com and [MONIKER 3 REDACTED]@gmail.com to communicate with an individual in Australia about shipments of certain commodities to North Korea. As described above in Parts VII.F and VIII.B.1, the email account watsonhenny@gmail.com is one of the most prolific operational accounts that was used in connection with targeting SPE, Bangladesh Bank, and other victims. As described in more detail below, that other person who shared the use of watsonhenny@gmail.com (the "North Korean Government Representative") explicitly claimed to have ties to the North Korean government.

a. In an email sent in October 2013, the North Korean Government Representative said he had spoken to the former ambassador of the DPRK to Kuwait about a transaction involving the person in Australia, and in that email listed his own title as "Ex-Counselor to Myanmar & Bangladesh."

b. In an email sent in January 2015 regarding setting up a "Joint Venture" project, the North Korean Government Representative wrote that the "Counselor for Foreign Affairs, Presidium, SPA, Pyongyang, DPRK (Former Ambassador to GCC countries)" had requested that he contact the recipients of the email about a business proposal.

277. Moreover, the person with whom the North Korean Government Representative was communicating in Australia (referenced above in paragraph 276) was also tied to the government of North Korea. Emails between the North Korean Government Representative and the person in Australia discussed negotiations and transactions regarding various commodities, such as coal and certain metals, and in 2017 the latter person was arrested in Australia for procuring missile components on behalf of the North Korean government. The following are examples of emails from the person in Australia.

a. In an email sent in July 2015, the person in Australia wrote in the context of negotiating a coal contract that he (the person in Australia) was a "recognized strategist that has favour with Kim Jong Eun," and that his "reports go directly to Kim Jong Eun."

b. In an email sent in December 2014, he said he was "currently looking after North Korea's overseas economics" and that North Korea was seeking to invest in specific types of infrastructure "from the direct orders of Mr Kim Jong un," and he asked for the recipient's "highest discretion on this matter."

c. In an email sent in August 2015, he said that a "sample" of a commodity had "been received and we have notified the government, this will be procured by a government entity." In that email he said he was "the liaison for NK international commerce, and that the particular deal "has already been approved for by the Commander in chief Mr Kim Jong Un himself" (sic). He also said that if necessary he would "utilize the NK government in liaison with" another foreign

government. In an earlier email that appeared to relate to the same commodity transaction being negotiated, he wrote to the same recipient that he was pleased to "become acquainted with you through the North Korean Embassy's" personnel.

d. In an email sent in November 2013, he wrote in regard to arranging an upcoming business trip to another country that his position should be listed as "CEO of DPR Korea foreign economy."

278. As explained above, PARK is one of the subjects under investigation in the overall scheme and numerous other co-conspirators are still being investigated. I know, based on my training and experience and on evidence found during the course of the investigation (such as the hard-coding of all of the workstations into the malware found on SPE's network), that the scale of the attacks on SPE, Bangladesh Bank, and others required significant resources and were likely the work of multiple persons working in concert. Attacks of this magnitude would likely require a team of persons, each performing different tasks, such as: developing malware tools; completing language translations or using developed foreign language skills; coordinating social engineering and spear-phishing; network reconnaissance; analyzing stolen information; and other jobs related to targeting specific employees of a company. The evidence discussed below shows that PARK is a member of the conspiracy, though he is not the only subject of the investigation.

279. The following sections discuss PARK's work for Chosun Expo as well as other personal details about PARK.

2. PARK JIN HYOK's Work in Dalian, China

280. PARK was at times dispatched to China, along with others, to work for Chosun Expo for paying clients on non-malicious software and information technology projects. The Chosun Expo Accounts included email accounts that he used while conducting this fee-generating business. On January 10, 2011, an email

was sent from an email account used by PARK's "Department Head" to the head of a non-DPRK company that provided financial market information services. That non-DPRK company employed programmers in Dalian, China, and later in North Korea, and the head of the non-DPRK company had met with military personnel in North Korea.

281. This particular email on January 10, 2011 said that a new developer, "Pak Jin Hek," was going to be replacing another developer on a programming team. (I was informed by an FBI linguist that both "Pak Jin Hek" and "Jin Hyok Park" are variants of how the same name in Korean would be written in English, given both variations in transliteration and conventions regarding whether surnames or given names are written first (*see* footnote 47 below).

282. Attached to the email was a biography or résumé, for "Pak Jin Hek" that showed the following: PARK's date of birth was listed as August 15, 1984; he listed his address simply as "Korea Expo Joint Venture," *i.e.*, Chosun Expo, where he was a "developer" and where he had been employed starting in 2002 as an "Online game developer"; he graduated from Kim Chaek University of Technology (a prestigious university in Pyongyang, North Korea); and he had programming language skills in "Vc++" (*i.e.*, Visual C++, the language discussed as being used in numerous malware samples including WannaCry and nearly all 32-bit North Korean malware samples), Java, php, jsp, and flash, and foreign language skills in English and Chinese.

283. Additionally, the résumé included the following photograph of PARK:

284. In addition to this January 10, 2011 email, other evidence in the Chosun Expo Accounts used by PARK (among others) also indicates that PARK arrived in Dalian to work for Chosun Expo in late-2010 or early-2011 and continued to work in Dalian until late-2013 or early-2014. The Chosun Expo Accounts—surigaemind@hotmail.com, ttykim1018@gmail.com, pkj0615710@hotmail.com, and business2008it@gmail.com—and their connections to PARK specifically are each discussed below in Part XII.B. That evidence in the Chosun Expo Accounts showing PARK was in Dalian during that period of time includes the following:

a. A Chosun Expo Account (surigaemind@hotmail.com), which was subscribed to "Jin Hyok Park," was created from an IP address registered to China Unicom Liaoning, in Dalian, on September 23, 2010.

b. On January 21 and 28, 2011, and June 22, 2011, a Facebook account registered to "Jin Hyok Park," using that same Chosun Expo Account (surigaemind@hotmail.com), was accessed using a Canadian IP address. That Canadian IP address was one that other subjects who were PARK's associates at Chosun Expo used in connection with work for the non-DPRK company referenced in paragraph 280. That Chosun Expo Account (surigaemind@hotmail.com) also used that Canadian IP address to send an email to itself on July 8, 2011.

c. On March 6, 2011 (one minute before surigaemind@hotmail.com emailed itself a file titled proxymini.zip, *see* paragraph 333.g), an email about a messenger application with a subject line translating to "Jin Hyok" was sent from surigaemind@hotmail.com to PARK's associate at Chosun Expo. (*See* paragraph 311.) Both emails were sent using the same IP address registered to China Unicom Liaoning, in Dalian.

d. On April 29, 2011, an unsigned email was sent by surigaemind@hotmail.com to itself with a subject of "My Current Location" and a body that contained an embedded hyperlink titled "Donglian Rd & Lianhe Rd." The hyperlink was to a Google Maps GPS location of 38.923981, 121.598053, which is located in Dalian, Liaoning, China, the province that borders North Korea.

e. In a translated May 2011 exchange between "Mr. Jin Hyok" and another person saved in ttykim1018@gmail.com, "Mr. Jin Hyok" wrote that he would have been "residing" in Dalian for "one year in September [2011]," and that before that he "went back and forth for three years for work." (*See* paragraph 299.) He further stated that he would be returning to North Korea in September 2011 to be married to his fiancée, whom he referred to as a "comrade," but that he was

"looking for a way to return home permanently." Later, on September 7, 2011, "Mr. Jin Hyok" informed the same person that he would be returning to the "motherland" "next week," the same timeframe he had previously discussed for his wedding.

f. Between 2012 and 2013, numerous Korean-language emails sent from surigaemind@hotmail.com either contained a subject line translating to "From Jin Hyok," or were signed with Korean characters translating to "Jin Hyok." (*See* paragraph 310.d.) Most of those emails, which related to programming projects for paying clients, were sent using IP addresses registered to China Unicom Liaoning, in Dalian, although one of them was sent using a Proxy Service IP address. (*See* paragraph 311).

285. Then, on September 4, 2013, an email was sent from another North Korean computer programmer (and subject of this investigation) to the person who ran the non-DPRK company in Dalian. The email stated that "Pak, Jin Hyok" and a second individual were "dismissed personnel." The email also attached a letter addressed to another individual, which reflected that "Pak, Jin Hyok" used DPRK passport number 290333974. A subsequent email on September 13, 2013 indicated that "mr.Park Jin Hyok" would continue working for Chosun Expo on projects for the non-DPRK company for a while longer, but a later email on February 21, 2014, referred to "Pak" as having already been dismissed. In other words, at some point between September 13, 2013 and February 21, 2014, PARK's rotation working for Chosun Expo in Dalian ended.

286. As noted above, PARK's résumé stated that he was employed as a developer by Chosun Expo. Messages in Chosun Expo Accounts also show PARK's connections to that company. First, multiple emails were auto-forwarded in 2009 and 2010 from webmaster@chosunexpo.com to the Chosun Expo Account pkj0615710@hotmail.com (another account connected to Chosun Expo and PARK,

discussed below). Second, on March 27, 2015, the Chosun Expo Account surigaemind@hotmail.com (which was registered using the name "Jin Hyok Park") sent two emails to webmaster@chosunexpo.com with a subject of "test." (The first email was sent from North Korean IP Address #4, while the second was sent from a Netherlands IP address.) Third, another email account connected to Chosun Expo had stored the email contact admin@chosunexpo.com as a saved contact with the name "Park Jin Hyok." These show that the persons using those Chosun Expo Accounts also used or operated the email accounts directly associated with Chosun Expo, which employed PARK as a developer.

B. The Chosun Expo Accounts

287. As noted above in Part III and elsewhere, both the operational accounts and the Chosun Expo Accounts were seemingly shared or accessed by more than one North Korean person.[46] PARK's use of the Chosun Expo Accounts was overt, in that he used his name in connection with the accounts and in that communications to or from several of those accounts also included Chosun Expo's name and website.

288. While affirmative connections between PARK and each of the Chosun Expo Accounts are described below, at least one other name—one with the English initials "P.K.J."—in particular was also frequently associated with these Chosun Expo Accounts. Although the translation of Korean names means that a particular name can have multiple possible English-language spellings and initials, regardless of the translation, the "P.K.J." name shares the names "Park" and "Jin" (when

[46] As one example, in 2015, a person with the initials Y.Y.M. signed an email from business2008it@gmail.com, and as noted in footnote 10 and discussed in greater detail in the previous section, watsonhenny@gmail.com was used by a person who appeared to represent himself as a North Korean diplomat.

written in English and in Korean characters) with PARK JIN HYOK.[47] Some of the messages within the Chosun Expo Accounts referred specifically to that "P.K.J." name or variations of that name, and in at least one instance a message was sent with that name using an IP address that PARK used a couple months later to access the same account. Others referenced "Park Jin" or "Jin Park," or just the handle "pkj," which was often used in the Chosun Expo Accounts. Whether those references to "pkj," "Park Jin," or "Jin Park" were meant to refer to PARK or not is often not clear. Therefore, while references in the Chosun Expo Accounts to the "P.K.J." name, the "pkj" handle, and those other names each demonstrate connections between those accounts, this affidavit does not discuss many of those references. The evidence set forth below instead focuses primarily on the connections between PARK JIN HYOK and the Chosun Expo Accounts.

289. As referenced above, the Chosun Expo Accounts were used to communicate with customers for whom the subjects performed programing projects in exchange for payment, as well as to communicate with other subjects who at times referred to each other as "comrade." Records show that the subjects operating out of Dalian, China under the auspices and direction of Chosun Expo, the North Korean government front company, shared the use of multiple IP addresses (in Dalian, China, and sometimes infrastructure in other countries). Records also indicate that these Chosun Expo Accounts connected to PARK were accessed from

---

[47] According to FBI Korean linguists, "Pak" is a more common representation for the name by North Koreans and "Park" by South Koreans when translating from English to Korean, or vice versa. Likewise, "Chin" is a common representation of "Jin," and "Hyok" is sometimes spelled "Hek." I have also observed that the name PARK JIN HYOK, is sometimes spelled "Jin Hyok Pak" or "Pak Jin Hek," which FBI linguists have informed me is not unexpected, given the variations in transliteration and the conventions regarding whether surnames or given names are written first.

Given that the Korean character "진" can translate to "Jin" or "Chin" and "박" can translate to "Park" or "Pak," where this affidavit describes evidence containing those characters "진" will be translated as "Jin" and "박" will be translated as "Park."

Dalian, China between 2011 and 2013, and then from North Korea in 2014 and thereafter, which is consistent with evidence described above regarding PARK's time in Dalian, China and his return to North Korea.

1. ttykim1018@gmail.com

290. Provider records show a number of connections between tty198410@gmail.com—one of the malicious, operational accounts, *see* paragraphs 102, 110.a, 112, 116–120, 162, and 208.a—and another similarly named account, ttykim1018@gmail.com. The connections between those accounts show that a user of ttykim1018@gmail.com was at least one of the persons who was using tty198410@gmail.com, and other evidence discussed below shows PARK's connections to ttykim1018@gmail.com.

291. For instance, a remote file-storage service associated with tty198410@gmail.com contained a 5.1 megabyte password-protected file titled "203-8-24.rar," and ttykim1018@gmail.com was the only other account that had access to the password-protected file, as discussed below.

a. A .rar file is a compressed digital archive that can contain one or several files inside it in a compressed form, similar to a "ZIP" file.

b. The file-storage service allowed a user to upload, store, share, and edit files with collaborators. Based on my experience, a user can authorize other users or accounts to have permission to read or to write to (or edit) files. An account with the ability to write to the file has all the permissions that the file owner has, with the exception of being able to delete the file or folder.

c. Provider records showed that the file "203-8-24.rar" was created on August 27, 2013, and the file's metadata revealed that the account ttykim1018@gmail.com was listed as one of the writers of the file. As explained above, this shows that ttykim1018@gmail.com had write-access to the file and thus had privileges to read or change the file in any way short of deletion. It is

significant that both accounts shared privileges to edit the file, particularly given that the .rar file was password protected, meaning that the user of tty198410@gmail.com and ttykim1018@gmail.com would both need to know the password to access it. This suggests that a user of the ttykim1018@gmail.com email account was the same person as, or, at a minimum, a close associate of, a person controlling tty198410@gmail.com.

292. In addition to being on the .rar archive as a writer, ttykim1018@gmail.com was also listed as one of only two accounts in the contacts list of tty198410@gmail.com.

293. Although there were 41 email addresses saved in contacts list of ttykim1018@gmail.com, tty198410@gmail.com was one of only two contacts that had a GetNotify.com suffix in the domain, the other being surigaemind@hotmail.com, another Chosun Expo Account used by PARK. (That suffix permitted the sender to receive read-receipt notifications when the email was read. This connection is further discussed in paragraphs 313–313.a.)

294. Notably, on July 30, 2013, approximately a month before ttykim1018@gmail.com was listed as one of the two "writers" on the .rar file discussed above, ttykim1018@gmail.com sent an email to surigaemind@hotmail.com with the subject "test" and the text "track?" Evidence indicates that email was sent through the GetNotify tracking service.

295. Aside from sharing a similarly named email address and each account being saved in the other's contacts list, provider records show that both tty198410@gmail.com and ttykim1018@gmail.com were used to create accounts with a video service, and each of those accounts listed the same distinct piece of biographical information. (The video service account subscribed by tty198410@gmail.com was created from a Proxy Service IP address in March 2013.) Other records for payment accounts associated with both ttykim1018@gmail.com

and business2008it@gmail.com (another Chosun Expo Account discussed below) also listed that same biographical information. (This biographical information was not consistent with information listed in PARK's résumé, nor with biographical information in other Chosun Expo Account correspondence, but it shows a connection between tty198410@gmail.com and ttykim1018@gmail.com.)

296. The evidence set forth in the preceding paragraphs shows that ttykim1018@gmail.com has strong connections to the operational account tty198410@gmail.com, suggesting that the same person or persons used them. The evidence set forth below in this section indicates that PARK was among the persons who used the Chosun Expo Account ttykim1018@gmail.com.

297. The name appearing in subscriber records for ttykim1018@gmail.com was "Geonov Ruski Jk," but some emails received by the account were addressed to "Park," "Jin," and "Jin Park," and records from Facebook show that the Facebook account registered using ttykim1018@gmail.com used the name "Jin Park" (as did other accounts connected to Chosun Expo Accounts, as discussed below).

298. Ttykim1018@gmail.com was created on October 27, 2008, and listed a recovery email address of business2006@naver.com, which was also used as the recovery email for business2008it@gmail.com, which was subscribed using the name "Jin Hyok Park," as discussed below.

299. In an exchange on or about May 24, 2011 in ttykim1018@gmail.com, one user introduced himself as "Jin Hyok." Later in the exchange, he was asked "Are you KCC, Mr. Jin Hyok?," and he answered that he was not KCC. (Based on information available from multiple publicly available sources, "KCC" may be a reference to the Korea Computer Center, which is a North Korean government information technology research center established in 1990.) He also wrote that his Skype ID was pkj615. In that same exchange, "Jin Hyok" discussed being engaged to get married, and indicated that he had been in Dalian for close to a year, since

the prior September. As discussed above in Part XII.A.2, other evidence indicates that PARK also traveled to Dalian, China during that period.

300. Access logs show that ttykim1018@gmail.com has been accessed by IP addresses located in the United States, the United Kingdom, Germany, and other countries, which likely indicate that the user of that account accessed it by proxy services, VPNs, or hop points. (I have not seen any evidence to indicate that PARK has traveled to any of those three countries, for example.) Some of these IP addresses were also used to access other Chosun Expo Accounts, including surigaemind@hotmail.com and business2008it@gmail.com, sometimes at the same time as it was used to access ttykim1018@gmail.com, as discussed below in paragraphs 331–331.e.

301. Ttykim1018@gmail.com, however, was also accessed on August 14, August 18, and September 6, 2014 from North Korean IP Address #4, and provider records show that this North Korean IP address was also used to access five different mobile devices associated with the ttykim1018@gmail.com account. The account was also accessed from North Korean IP Address #8 in 2015 and 2016. Analysis of messages stored in ttykim1018@gmail.com by an FBI analyst fluent in Korean indicated that the account made frequent use of words and language styles that are commonly used in North Korea, but rarely used in South Korea.

2. business2008it@gmail.com

302. The name used to subscribe business2008it@gmail.com was "Jin Hyok Park," and the account was created on March 4, 2008 from a North Korean IP address. Business2008it@gmail.com, which shared a common recovery email address (business2006@naver.com) with ttykim1018@gmail.com, was also accessed by the same device as ttykim1018@gmail.com on an unidentified date. Among the names used to address emails sent to business2008it@gmail.com between December

1, 2012 and June 2015 were "Jin," "Park Jin," "Jin Hyok Park," and the above-described "P.K.J." name. (*See* paragraph 288.)

303. Header information from emails sent in 2012, 2014, 2016, and 2017 used the name "Jin Hyok Park" for business2008it@gmail.com. One email sent by business2008it@gmail.com on January 24, 2015, responding to a referral that appeared to relate to a technology project, stated in Korean characters: "My name is Jin Hyok Park." In business2008it@gmail.com's address book, the account itself was saved with the name "Jin Hyok Park."

304. On February 4, 2015, business2008it@gmail.com sent an email to surigaemind@hotmail.com, another Chosun Expo Account (discussed below in Part XII.B.3), with a subject and body that only read "test." That email, the January 24, 2015 "Jin Hyok Park" email, and another email signed with the "P.K.J." name were all sent using a specific IP address located in the Netherlands. That same Netherlands IP address had also been used (a) to access the account in November 2014 and January 2015, (b) to access ttykim1018@gmail.com in February 2015, and (c) to access another Chosun Expo Account (surigaemind@hotmail.com, discussed below) in February 2015. (*See* paragraph 331.b.)[48]

305. The email accounts ttykim1018@gmail.com and business2008it@gmail.com were also each accessed from the same IP address minutes apart on multiple days between August 27 and November 24, 2014. While in each of these instances the accounts were accessed from a common IP address, in each of those instances the IP address used to access the two accounts was different—and in a different country—on each date. For example, one of the IP addresses was in Germany, one was in the United Kingdom, and two were in the United States. Thus, these accounts were not only accessed by the same IP address,

[48] This is a different Netherlands IP address than the one discussed in paragraph 286.

but they were accessed from IP addresses in multiple countries around the world, indicating that the person using them was also using the same set of VPNs, compromised computers or hop points, or anonymizing proxy services to conceal that person's true location.

306. During the same period, on November 6, 2014, business2008it@gmail.com was accessed from North Korean IP Address #4. On several dates in 2016, including in March, April, and November, the account was accessed from North Korean IP Address #8 as well as another North Korean IP address.

307. In particular, on November 14, 2016, business2008it@gmail.com was accessed from North Korean IP Address #8, and on December 1 and 2, 2016, the account was accessed from North Korean IP Address #7. Likewise, another Chosun Expo Account described below—pkj0615710@hotmail.com—was accessed by North Korean IP Address #7 on November 17 and December 1, 2016. These connections from North Korean IP Address #7 are significant because, as mentioned in paragraphs 41 and 207, on November 14, 2016, North Korean IP Address #7 was used to create an account at a DDNS provider using the malicious email address hwa5403@daum.net and to access Brambul collector email account diver.jacker@gmail.com. This shows that these same computer networks that were being used to access Chosun Expo Accounts were also being used to create and maintain the malicious infrastructure being used in the computer intrusions discussed herein.

308. One of the IP addresses used to access business2008it@gmail.com was also used to access other operational accounts, as well as another Chosun Expo Account, surigaemind@hotmail.com, within days, as discussed below. Specifically, the IP address, which is located in Switzerland, was used to access the following accounts on the following days:

a. March 27, June 11, and August 27, 2015: accessed the Facebook account registered to [JK NAME REDACTED]@outlook.com (which account was accessed from North Korean IP Address #2, and which was the recovery email for the [JK NAME REDACTED]@gmail.com email account that spear-phished AMC Theatres employees, *see* paragraphs 130.e and 275.a);

b. May 18, 2015: accessed business2008it@gmail.com, a Chosun Expo Account;

c. July 13, 2015: accessed the Twitter account @amazonriver1990, which was registered using amazonriver1990@gmail.com (which account was accessed using North Korean IP Address #2, the user of which conducted online research for hacking-related topics between May 19, 2015 and September 10, 2015, *see* paragraph 96 and footnote 27);

d. August 10, 2015: accessed surigaemind@hotmail.com, a Chosun Expo Account;

e. August 20, 2015: accessed jongdada02@gmail.com, the recovery email for many accounts targeting Lockheed Martin; and

f. August 25, 2015: accessed otohokyasaco@gmail.com, which used jongdada02@gmail.com as its recovery email and which was also accessed from North Korean IP Address #2 on numerous occasions in August and September 2015.

309. Although these log-ins were separated by days, the fact that this IP address was used to access both operational accounts and Chosun Expo Accounts, as well as the fact that the IP address was located in Switzerland, indicate it is unlikely a coincidence that the same IP address happened to be used to access operational accounts and Chosun Expo Accounts. Rather, it more likely reflects the use of common infrastructure by the subjects to access both operational accounts and Chosun Expo Accounts, during the period when PARK appears to have returned to North Korea.

3. surigaemind@hotmail.com

310. Multiple pieces of evidence show that the email address surigaemind@hotmail.com was used by PARK. (Emails in the account were also at times addressed to or signed by the "P.K.J." name and/or the handle "pkj."[49]) Those connections to PARK include the following:

a. The name used to subscribe surigaemind@hotmail.com was "Jin Hyok Park," and the account was registered on September 23, 2010, when PARK appears to have been in Dalian, as discussed in paragraph 299. The IP address used to create the email account was registered to China Unicom Liaoning, in Dalian.

b. On November 29, 2010, a Facebook profile was subscribed using surigaemind@hotmail.com and using the name "Jin Hyok Park."

c. On the same day, Twitter account @ttypkj was created using surigaemind@hotmail.com and the name "Park Jin Hyok." (*See* paragraph 312 for further discussion of these accounts.)

d. Multiple emails sent from surigaemind@hotmail.com about various software projects for Chosun Expo clients were signed using Korean characters that translated to "Jin Hyok" or had a subject line translating to "Jin Hyok" or "From Jin Hyok." For example, one such email sent from surigaemind@hotmail.com to an associate at Chosun Expo using an IP address registered to China Unicom Liaoning, in Dalian, on March 6, 2011, contained the subject line translating to "Jin Hyok" and indicated that PARK was having trouble logging into an instant messenger application, and thus was providing an update by email. Multiple other emails from "Jin Hyok" were sent by

[49] For example, on November 3, 2010, two emails were sent from surigaemind@hotmail.com to a potential freelance customer. The name in the header information corresponding to surigaemind@hotmail.com (the sender) was "ParkJin Hyok," and the emails were signed "PKJ" and "pkj." Both emails were sent from Chinese IP addresses registered to China Unicom Liaoning, in Dalian.

surigaemind@hotmail.com in 2012 and 2013, many of which were sent using IP addresses registered to China Unicom Liaoning, in Dalian.

e. In an email on December 1, 2011 from PARK's "Department Head" to the non-DPRK company (both mentioned above in paragraph 280), the "Department Head" informed a client that surigaemind@hotmail.com was the contact email for "Mr. Jin."

f. An email on July 6, 2011, from a moderator of a website that connects freelance information technology employers and employees for discrete projects addressed surigaemind@hotmail.com as "JinHyok Park."

311. Not all of those "Jin Hyok" emails referenced in paragraph 310.d were sent from Chinese IP addresses. One of the emails—which was sent on September 30, 2012, referred to a messenger application, and had a subject of line that translated to "From Jin Hyok"—was sent using a Proxy Service IP address. This shows that the same operational infrastructure used to access spear-phishing and alias accounts was also used—even if inadvertently—to access an account used by PARK in his true name.

312. Aside from the email account itself, social media accounts registered using surigaemind@hotmail.com shared IP address access with other accounts connected to PARK and his associates. For example, in November 2010, the same Canadian IP address was used to access: (a) the Facebook account registered using surigaemind@hotmail.com (registered using the name "Jin Hyok Park"); (b) the Facebook account registered using the email addresses ttykim1018@gmail.com (with the name "Jin Park"); and (c) the @ttypkj Twitter account subscribed using surigaemind@hotmail.com (with the name "Park Jin Hyok") in 2010. The same

Canadian IP address was also used to access the email account of an associate of PARK at Chosun Expo during the same period.[50]

313. Similar to the connections between tty198410@gmail.com and ttykim1018@gmail.com, surigaemind@hotmail.com was connected to ttykim1018@gmail.com and business2008it@gmail.com in other significant ways: (a) it was one of two email addresses stored in ttykim1018@gmail.com's contacts with a GetNotify.com suffix in the domain (that suffix permitted the sender to receive read-receipt notifications when the email was read), the other email account saved with that suffix being tty198410@gmail.com, which (as discussed above) is an account used to register other accounts used for spear-phishing; (b) it was one of business2008it@gmail.com's approximately 23 stored contacts; (c) as described above, it received a "test" email from business2008it@gmail.com on February 4, 2015; and (d) these three accounts were often accessed by the same IP addresses, sometimes on the same day, as discussed below in Part XII.B.6.

a. In particular, ttykim1018@gmail.com had approximately 41 contacts saved, of which two had an email address that was appended with the domain ".getnotify.com," which is used as part of a read-receipt service. These two accounts were surigaemind@hotmail.com (as noted above, a Chosun Expo Account) and tty198410@gmail.com. (To be clear, "surigaemind@hotmail.com.getnotify.com" is the address listed as a contact that contains "getnotify.com" after the email address.) Thus, one Chosun Expo Account connected to PARK (ttykim1018@gmail.com) used read receipts with only two other accounts: another Chosun Expo Account connected to PARK (surigaemind@hotmail.com) and a central account used in the attacks described above (tty198410@gmail.com).

[50] This is a different Canadian IP address as the one referenced in paragraph 284.b.

314. Access logs for surigaemind@hotmail.com show that it was accessed on multiple occasions from North Korean IP addresses during and after 2014.

a. An online service account that was subscribed using surigaemind@hotmail.com was accessed using multiple North Korean IP addresses, including specifically North Korean IP Address #4 on November 20, 21, 22, and 27, 2014. The log-ins using North Korean IP Address #4 on November 20 through 27, 2014 occurred on the days immediately before and after the cyber-attack on SPE became overt, a time when PARK is believed to have been in North Korea.[51]

b. The surigaemind@hotmail.com email account itself (not the above-mentioned online service account subscribed using it) was accessed in March 2015 using North Korean IP Address #3 (the same North Korean IP address used by [MONIKER 3 REDACTED]@gmail.com in 2015, as discussed in paragraph 147) and in March and April 2015 using North Korean IP Address #4.

c. The surigaemind@hotmail.com email account itself was also accessed using North Korean IP Address #7 on February 6, February 10, March 28, April 11, and June 2, 2018.

4. pkj0615710@hotmail.com

315. Pkj0615710@hotmail.com is another Chosun Expo Account that shares numerous connections to surigaemind@hotmail.com and to PARK.[52]

316. The account was created on April 18, 2007 using North Korean IP Address #9, and it used a first name of "Jin" and the Korean character "박" for the

---

[51] As mentioned in Part V.A, in March 2016, a distinct shift occurred across numerous accounts that were under investigation. For example, accounts that had been accessed from North Korean IP Address #3 began being accessed by North Korean IP Address #7. Similarly, Chosun Expo Accounts that were accessed using North Korean IP Addresses #3 and #4 in 2014 and 2015 began being accessed from North Korean IP Addresses #7 and #8 in approximately late March of 2016.

[52] As with other Chosun Expo Accounts, pkj0615710@hotmail.com also has connections to the "P.K.J." name and the "pkj" handle, but those connections are not discussed in detail in this section.

last name, which translates to "Park." The account's calendar had been set to Korea Standard Time (currently 30 minutes ahead of "Pyongyang Time," but until August 2015 it was the time zone used by North Korea (*see* paragraph 233.c)), and it had been accessed using North Korean IP addresses.

317. The Facebook profile subscribed using pkj0615710@hotmail.com used the name "Jin Park" as well. That Facebook account also shared a distinct piece of biographical information with the "Jin Park" Facebook account subscribed to ttykim1018@gmail.com and the "Jin Hyok Park" Facebook account subscribed to surigaemind@hotmail.com (different from the biographical information described in paragraph 295), as did a user of ttykim1018@gmail.com using the name "Jin," according to an email sent in 2013.

318. Emails addressed to pkj0615710@hotmail.com in December 2009 and January 2010 contained Korean characters translating to "Park Jin Hyok," in the email header information identifying the account. There was no salutation in the body of the email.

319. Subscriber records for surigaemind@hotmail.com show that the account used pkj0615710@hotmail.com as an alternative email. Likely because it was listed as the alternative email account, pkj0615710@hotmail.com received emails about log-in activity for surigaemind@hotmail.com between 2013 and 2015.

320. Access logs show that the account was accessed from North Korean IP Address #4 on March 26, 2014 and March 2, 2015. On June 19, 2015, pkj0615710@hotmail.com received an email regarding a suspicious log-in to surigaemind@hotmail.com from a Namibian IP address. On that same date, provider records indicate that a video service account registered to business2008it@gmail.com was accessed from that same Namibian IP address, which was the only log-in to the account. Access logs also show that, more recently, North Korean IP Address #7 was used to access pkj0615710@hotmail.com on

November 17 and December 1, 2016, and North Korean IP Address #8 was used on June 22, 2016.

321. In addition to surigaemind@hotmail.com using pkj0615710@hotmail.com as an alternative email, the two accounts shared other connections, including registering for accounts at the same freelance service one day apart. On September 24, 2010, the day after surigaemind@hotmail.com was registered, the email account was used to register two profiles at an information technology freelancing website in the name "Park Jin" claiming to be from Dalian. On September 25, 2010, the next day, the email address for one of the accounts was changed to pkj0615710@hotmail.com.

a. Between September 2010 and August 2013, both freelance accounts were logged into primarily from IP addresses registered to China Unicom Liaoning, in Dalian, which is a period when PARK appears to have been in Dalian, China, and at times the same IP addresses used to log into both accounts overlapped.

b. One non-Chinese IP address that was used to access both freelance accounts was a specific United States IP address. That specific United States IP address was used by PARK's associates at Chosun Expo in March 2013 when working on a website coding project for a paying client. Specifically, an email sent on March 10, 2013 from an associate of PARK's at Chosun Expo (who also is a subject of the government's investigation) indicated that this United States IP address was the IP address for a "Windows server" that Chosun Expo employees in Dalian had set up in connection with the project for that client. The United States IP address was later used to register and access their email and social media accounts connected to the Chosun Expo Accounts on a number of occasions:

i. May 16–20, 2013: accessed the freelance account (described in paragraph 321) registered to surigaemind@hotmail.com;

ii. May 21–22, 2013: accessed the payment account associated with ttykim1018@gmail.com, which shared a distinct piece of biographical information with (a) the payment account associated with business2008it@gmail.com, (b) the video service account created by tty198410@gmail.com, and (c) the video service account created by ttykim1018@gmail.com (*see* paragraph 295);

iii. May 22, 2013–August 31, 2013: accessed the payment account associated with business2008it@gmail.com;

iv. May 28, 2013: created the video service account registered to ttykim1018@gmail.com;

v. May 31, 2013: accessed the Facebook account subscribed to "Jin Park" using the email address ttykim1018@gmail.com;

vi. June 30, 2013: accessed the freelance account registered to pkj0615710@hotmail.com;

vii. September 4, 2014–October 2, 2016: accessed business2008it@gmail.com (the last log-in of which occurred a few seconds after business2008it@gmail.com logged out from North Korean IP Address #8); and

viii. March 21, 2015, September 24, 2016, and October 1 and 2, 2016: accessed ttykim1018@gmail.com (at the same time the IP address was used to access business2008it@gmail.com).

322. The use of this United States IP address indicates that subjects of the investigation would on occasion use the infrastructure belonging to clients of Chosun Expo, a North Korean government front company, to access their own email and social media accounts, and it shows additional connections between the Chosun Expo Accounts used by PARK.

323. Aside from these connections to PARK and the other Chosun Expo Accounts, pkj0615710@hotmail.com is also connected to operational "Kim Hyon Woo" accounts.

a. Significantly, the saved contacts in pkj0615710@hotmail.com's address book included hyon_u@hotmail.com, one of the accounts used in the name "Kim Hyon Woo" discussed above in Part XI.B.

b. Pkj0615710@hotmail.com was also used to subscribe an email account with the handle "kym10180615." Relatedly, business2008it@gmail.com was used to register an account at a website using the name or handle "kym1018." "K YM" is also the name used to subscribe the operational "Kim Hyon Woo" account tty198410@gmail.com.

324. Moreover, North Korean IP Address #9 has been used to access pkj0615710@hotmail.com, ttykim1018@gmail.com, and the account created at a particular software development website using the email address hyon_u@hotmail.com that was stored in pkj0615710@hotmail's contacts. (Multiple operational email accounts, including tty198410@gmail.com and mogbe123456@gmail.com, had created accounts at that website.) Specifically:

a. On April 18, 2007, North Korean IP Address #9 was used to create the pkj0615710@hotmail.com email account.

b. On October 16, 2009, North Korean IP Address #9 was used to create the Skype account with Skype ID ttykim1018, which was registered using pkj0615710@hotmail.com and which shared the same "handle" (ttykim1018) with ttykim1018@gmail.com.

c. On April 7, 2010, North Korean IP Address #9 was used to access an account at a software development website that had been created using the email address hyon_u@hotmail.com and the name "김현우," which translates to Kim Hyon Woo.

d. On June 22, 2010, North Korean IP Address #9 was used twice to access Facebook ID 100000923415121, which account was created using the Chosun Expo Account ttykim1018@gmail.com and which was registered using the name "Jin Park." When this Facebook account was created, it was accessed exclusively from South Korean IP addresses between March and July 2010, with the exception of these two log-ins from North Korea during that time; this same account was accessed using a Chosun Expo client's infrastructure in May 2013 (*see* paragraph 321.b.v).

e. On July 5, 2010, North Korean IP Address #9 was used to access the same "Kim Hyon Woo" account at the software development website described above in this paragraph.

f. Between July 16, 2008 and November 26, 2010 (and on certain earlier dates as well) North Korean IP Address #9 accessed the account used to register chosunexpo.com, the domain for Chosun Expo.

5. mrkimjin123@gmail.com

325. Mrkimjin123@gmail.com is an alias-name account, but it also is an account that bridges the Chosun Expo Accounts and the operational accounts: it was registered using an operational account (tty198410@gmail.com), but the "Mr. Kim Jin" moniker was used in communications that a Chosun Expo Account (surigaemind@hotmail.com) had with a technology company.

326. Mrkimjin123@gmail.com uses both "kim" and "jin" in its address, and the name used to subscribe the account was a Korean name that translates to "Kim Jin-woo." The account was created on November 21, 2011. Emails received by surigaemind@hotmail.com during roughly that same period in 2011 (October 11, 2011 through December 7, 2011) were addressed to "Kim Jin."

327. The name "Kim Jin" has been used more recently in connection with surigaemind@hotmail.com as well. On February 3, 2015, a "Mr. Kim Jin," who

claimed to be located in China but was using the specific Netherlands IP address discussed in paragraph 304, submitted a request to a U.S. technology company using surigaemind@hotmail.com as the contact email address. On February 4, 2015, an email was sent from surigaemind@hotmail.com by "Jin" to the Chinese affiliate of that U.S. technology company, using the same Netherlands IP address, asking essentially the same question. Besides its use to contact the U.S. technology company on behalf of "Kim Jin" and "Jin" and using surigaemind@hotmail.com, the Netherlands IP address has other connections to the Chosun Expo Accounts:

a. Between November 19, 2014 and September 27, 2016, business2008it@gmail.com was accessed from the Netherlands IP address repeatedly (*see* paragraph 331.a), during which time an email was sent on January 24, 2015 from the account that identified the author as "Jin Hyok Park."

b. On February 5 and 28, 2015, ttykim1018@gmail.com was accessed from the Netherlands IP address.

c. On September 18, 2016, pkj0615710@hotmail.com was accessed from the Netherlands IP address.

328. In addition to these connections to Chosun Expo Accounts—the similarity in the substance of communications, and the names used—mrkimjin123@gmail.com also has connections to the "Kim Hyon Woo" accounts described above, showing that the same person or persons had access to each. Mrkimjin123@gmail.com was registered using the operational email account tty198410@gmail.com (an account used by "Kim Hyon Woo," *see* paragraph 249) and those two accounts were also accessed by the same device on November 13, 2014. The next day, November 14, 2014, mrkimjin123@gmail.com was accessed from a Proxy Service IP address, as was tty198410@gmail.com. Mrkimjin123@gmail.com was also accessed by the same device as MrDavid0818@gmail.com, which was used by the subjects to target defense contractors (*see* paragraph 200). At points in 2016,

mrkimjin123@gmail.com, mrdavid0818@gmail.com, and tty198410@gmail.com were all accessed by the same IP addresses located in Singapore that appear to belong to a VPN and cloud computing service (in some instances log-ins to these accounts were within a minute of each other, and in others within days).

329. Thus, mrkimjin123@gmail.com is in part a "Kim Hyon Woo" account in that it was registered using tty198410@gmail.com and accessed by a common device as that account, but its common use of "Kim Jin" with surigaemind@hotmail.com and access from the same Proxy Service used to access surigaemind@hotmail.com on September 30, 2012 show its connections to the Chosun Expo Accounts. These connections show that mrkimjin123@gmail.com likely was accessed both by one or more persons who had access to "Kim Hyon Woo" accounts and likely was also accessed by one or more persons who had access to Chosun Expo Accounts.

6. Access to Chosun Expo Accounts by North Korean IP Addresses

330. As discussed above, PARK has numerous connections to the Chosun Expo Accounts, and evidence indicates that PARK returned to North Korea in 2014, prior to the cyber-attack on SPE. Consistent with this, Chosun Expo Accounts were accessed from North Korean IP addresses in 2014 and afterward on several occasions. For example:

a. ttykim1018@gmail.com: accessed from North Korean IP Address #4 on August 14, August 18, and September 6, 2014; and North Korean IP Address #8 on April 1 and 7, 2016;

b. business2008it@gmail.com: accessed from North Korean IP Address #4 on November 6, 2014; another North Korean IP address on March 2, 2016; North Korean IP Address #8 on March 22, April 1, October 2, and November 14, 2016; and North Korean IP Address #7 on December 1 and 2, 2016;

c. surigaemind@hotmail.com: accessed from North Korean IP Address #3 on March 2, 2015; North Korean IP Address #4 on March 1, March 2,

March 27, and April 17, 2015; and North Korean IP Address #7 on February 6, February 10, March 28, April 11, and June 2, 2018; and

d. pkj0615710@hotmail.com: accessed from North Korean IP Address #4 on March 26, 2014 and March 2, 2015; North Korean IP Address #7 on November 17 and December 1, 2016; and North Korean IP Address #8 on June 22, 2016.

331. Additionally, rather than being accessed regularly from IP addresses registered to China Unicom Liaoning, in Dalian or elsewhere in China when they were not being accessed by North Korean IP addresses, the non-North Korean IP addresses that accessed the Chosun Expo Accounts in 2014 and later were from a variety of locations—places to which there is no evidence to date indicating PARK or his close associates have traveled. It thus appears that those log-ins from non-North Korean IP addresses occurred through use of other infrastructure to which the subjects had access, such as VPNs or their clients' infrastructure, which concealed their location. Those log-ins included the following:

a. A Netherlands IP address (discussed in paragraphs 327–327.b, among others) was used to access ttykim1018@gmail.com on February 5 and 28, 2015. That same IP address was used to access business2008it@gmail.com on November 19, 20, 21, 22, 23, and 28, 2014; December 2, 5, and 7, 2014; January 24, 25, 27, 28, 29, 30, and 31, 2015; February 3, 4, 11, and 28, 2015; July 14, 2016; and September 22, 23, 25, 26, and 27, 2016. It also accessed surigaemind@hotmail.com on February 2, 3, and 4, 2015, and pkj0615710@hotmail.com on September 18, 2016.

b. A Netherlands IP address (discussed in paragraph 286) was used to access ttykim1018@gmail.com on November 5, 2014. The same IP address was used to access business2008it@gmail.com on October 17, 2014 and November 5, 2015, and surigaemind@hotmail.com on March 27, 2015.

c. A United States IP address associated with a client of Chosun Expo (discussed in paragraphs 321.b–321.b.viii) was used to access business2008it@gmail.com on September 5, 2014; January 3, 2015; March 21 and 22, 2015; April 7, 8, 9, 10, and 24, 2015; June 8, 2015; July 27, 2015; October 10, 2015; June 12, 2016; September 7, 2016; and October 1 and 2, 2016 (the latter of which was a few seconds after a logout from North Korean IP Address #8). The same IP address was used to access ttykim1018@gmail.com on March 21, 2015; September 24, 2016; and October 1 and 2, 2016 (on all those dates, it was used at the same time to access business2008it@gmail.com).

d. Another United States IP address was used to access business2008it@gmail.com on November 15 and 26, 2014; December 15, 2014; February 6, 11, 14, and 23, 2015; and October 1, 2016. That IP address was also used to access ttykim1018@gmail.com on some of the same dates: November 15, 2014, and February 8 and 11, 2015. And it was used to access surigaemind@hotmail.com on February 6, 7, & 10, 2015, some of which overlapped with the log-ins by business2008it@gmail.com.

e. A Namibian IP address (discussed in paragraph 320) was used to access surigaemind@hotmail.com on June 19, 2015, and on that same date to access a video service account registered to business2008it@gmail.com.

332. These were just some of the numerous log-ins to Chosun Expo Accounts from non-North Korean IP addresses from 2014 through 2016. The log-ins from the non-North Korean IP addresses outnumbered the log-ins from North Korean IP addresses, suggesting that the subjects using those Chosun Expo Accounts, including PARK, often took affirmative steps to access the internet from proxy infrastructure to conceal their identities and locations. These measures taken when accessing Chosun Expo Accounts were different than those taken by the subjects when accessing operational accounts, which included the use of computers

compromised by the Brambul worm and use of the Proxy Services. But, as noted above in paragraph 266, sophisticated hackers will go to great lengths to separate their use of accounts that they use in their true names from operational accounts that they use in alias names. In that context, it is significant that on at least one occasion, PARK accessed surigaemind@hotmail.com using that same Proxy Service (*see* paragraph 311) that the subjects used to hide their locations and IP addresses when accessing malicious, operational accounts, including the "Kim Hyon Woo" persona accounts.

7. Summary of Connections Between "Kim Hyon Woo" Persona and Chosun Expo Accounts Connected to PARK

333. The evidence discussed above indicates that PARK returned to North Korea in 2014, before the cyber-attack on SPE. Other evidence discussed shows that "Kim Hyon Woo," the name used in subscriber records for an email account programmed into the Brambul worm and for accounts closely related to targeting of SPE, Bangladesh Bank, Lockheed Martin, Mammoth Screen, AMC Theatres and other victims (and thus likely to be discovered) is an alias and that PARK is either the person or, at a minimum, one of the persons who had access to the accounts in the name "Kim Hyon Woo." That evidence includes the following:

a. Tty198410@gmail.com had saved ttykim1018@gmail.com as a contact in its address book.

b. Tty198410@gmail.com was one of only two accounts saved in the address book of the Chosun Expo Account ttykim1018@gmail.com with a "getnotify.com" read receipt suffix, the second account being surigaemind@hotmail.com, another Chosun Expo Account.

c. Ttykim1018@gmail.com was the only account allowed access to a .rar file saved in tty198410@gmail.com's remote file-storage account. That .rar file was encrypted with a password, meaning that the user(s) of ttykim1018@gmail.com

and tty198410@gmail.com also must have known the same password in order to access it.

d. Tty198410@gmail.com registered a video account that shared a distinct piece of biographical information with a video account created by ttykim1018@gmail.com, a payment account created by ttykim1018@gmail.com, and a payment account associated with business2008it@gmail.com.

e. Hyon_u@hotmail.com was saved as a contact in the address book of the Chosun Expo Account pkj0615710@hotmail.com.

f. The username for mrkimjin123@gmail.com contains both "kim" and "jin" and connects the "Kim Hyon Woo" persona and PARK: it was subscribed using the "Kim Hyon Woo" account tty198410@gmail.com, and it was accessed by the same device that was used to access that account (tty198410@gmail.com) on November 13, 2014, shortly before the cyber-attack on SPE became overt. It was subscribed, however, using a Korean name that translates to "Kim Jin-woo," and the user of Chosun Expo Account surigaemind@hotmail.com used the name "Mr. Kim Jin" and "Kim Jin" in email correspondence.

g. On March 6, 2011, the Chosun Expo Account surigaemind@hotmail.com emailed itself a file titled proxymini.zip from an IP address registered to China Unicom Liaoning, in Dalian. Proxymini is an open source, downloadable tool that sets up a proxy server. (This was sent one minute after surigaemind@hotmail.com sent an email from "Jin Hyok" indicating that "Jin Hyok" was having difficulty accessing a messaging application on March 6, 2011, *see* paragraph 310.d.) As discussed in paragraph 253, the term "proxymini" appeared in the Operation Troy Access database found in the hyonwoo01@gmail.com account emailed ten days later on March 16, 2011.

h. Certain Brambul collector email accounts used the name "Kim Hyon Woo," and those and other Brambul collector email accounts were accessed

from North Korean IP addresses. Diver.jacker@gmail.com was a Brambul collector email account accessed from North Korean IP Address #7 in November 2016. During roughly the same time, North Korean IP Address #7 was also used to create an account at a DDNS provider using malicious email address hwa5403@daum.net and to log-in to Chosun Expo Accounts business2008it@gmail.com and pkj0615710@hotmail.com.

i. The Swiss IP address referenced in paragraph 308 was used to access both operational accounts used for, *e.g.*, conducing online reconnaissance and registering other accounts that sent spear-phishing messages (amazonriver1990@gmail.com, jongdada02@gmail.com, otohokyasaco@gmail.com, and the Facebook account subscribed to [JK NAME REDACTED]@outlook.com), as well as Chosun Expo Accounts (surigaemind@hotmail.com and business2008it@gmail.com) between May and August 2015.

j. As discussed at length in Part XII.B.4, North Korean IP Address #9 was used extensively to access Chosun Expo Accounts used by PARK, by "Kim Hyon Woo" accounts, and to access infrastructure registered to Chosun Expo.

XIII. CONCLUSION

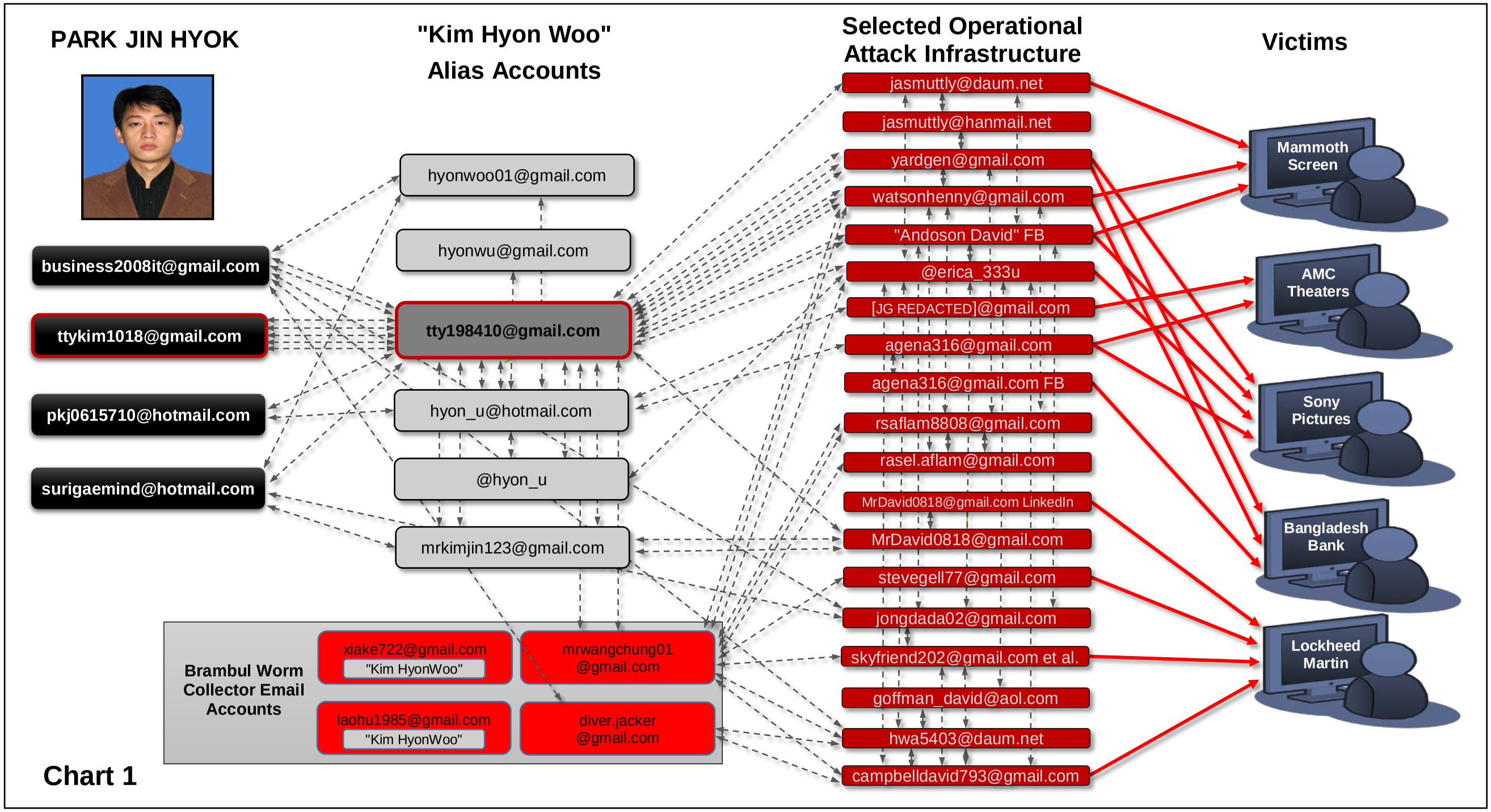
334. In the period shortly before the cyber-attacks discussed in this Affidavit, PARK was stationed in a Chinese border city working for Chosun Expo, a North Korean government front company for a North Korean hacking organization sometimes known as Lab 110, and evidence indicates that he returned to North Korea before the cyber-attack on SPE. As noted, the attacks and intrusions described in this Affidavit would have each required the efforts of a well-resourced team of persons working in concert, each performing different tasks. The technical evidence described above shows that those attacks and intrusions were carried out by a group of persons with access to the same email and social media accounts, computer infrastructure, and source code. Tracing connections back through the

operational infrastructure reveals numerous connections between PARK, his true-name email and social media accounts, and the operational accounts used to conduct the cyber-attacks and computer intrusions described herein. PARK's employment by a front company for a North Korean hacking organization and the connections between his true-name accounts and the operational accounts used by the subjects are therefore significant precisely because criminal hackers typically go to great lengths to separate their operational accounts from their true-name accounts and to conceal their identities. While PARK is not the only North Korean subject of the investigation, or the only person to use some of the accounts discussed above, the evidence set forth shows that PARK was a member of the conspiracies described here. For all the reasons described above, there is probable cause to believe that PARK has committed violations of 18 U.S.C. § 371 (Conspiracy) and 18 U.S.C. § 1349 (Conspiracy).

/s/
NATHAN P. SHIELDS
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me this
8th day of June, 2018.

ROZELLA A. OLIVER
HONORABLE ROZELLA A. OLIVER
UNITED STATES MAGISTRATE JUDGE


PARK JIN HYOK
"Kim Hyon Woo"
Alias Accounts
Selected Operational
Attack Infrastructure
Victims
business2008it@gmail.com
ttykim1018@gmail.com
pkj0615710@hotmail.com
surigaemind@hotmail.com
hyonwoo01@gmail.com
hyonwu@gmail.com
tty198410@gmail.com
hyon_u@hotmail.com
@hyon_u
mrkimjin123@gmail.com
jasmuttly@daum.net
jasmuttly@hanmail.net
yardgen@gmail.com
watsonhenny@gmail.com
"Andoson David" FB
@erica_333u
[JG REDACTED]@gmail.com
agena316@gmail.com
agena316@gmail.com FB
rsaflam8808@gmail.com
rasel.aflam@gmail.com
MrDavid0818@gmail.com LinkedIn
MrDavid0818@gmail.com
stevegell77@gmail.com
jongdada02@gmail.com
skyfriend202@gmail.com et al.
goffman_david@aol.com
hwa5403@daum.net
campbelldavid793@gmail.com
Mammoth Screen
AMC Theaters
Sony Pictures
Bangladesh Bank
Lockheed Martin
Brambul Worm Collector Email Accounts
xiake722@gmail.com
"Kim HyonWoo"
mrwangchung01 @gmail.com
laohu1985@gmail.com
"Kim HyonWoo"
diver.jacker @gmail.com
Chart 1

PARK JIN HYOK

business2008it@gmail.com

ttykim1018@gmail.com

pkj0615710@hotmail.com

surigaemind@hotmail.com

"Kim Hyon Woo" Alias Accounts

hyon_u@hotmail.com

Twitter @hyon_u

tty198410@gmail.com

hyonwu@gmail.com

hyonwoo01@gmail.com

mrkimjin123@gmail.com

xiake722@gmail.com

"Kim HyonWoo"

mrwangchung01 @gmail.com

diver.jacker@gmail.com

laohu1985@gmail.com

"Kim HyonWoo"

Brambul Worm Collector Email Accounts

Compromised Web Server

Operational Attack Infrastructure

mogbe123456@gmail.com

"John Mogabe" Facebook

hwa5403 DDNS account

hwa5403@daum.net

campbelldavid793@gmail.com

goo19874@gmail.com

[KB NAME REDACTED]@gmail.com

[BM NAME REDACTED]@gmail.com

amazonriver1990@gmail.com

yardgen@gmail.com

jasmuttly@hanmail.net

"Andoson David" Facebook

goffman_david2@aol.com

Twitter @erica_333u

bangsong8519@daum.net

[FC NAME REDACTED]@gmail.com

[MP NAME REDACTED]@gmail.com

uiwon0608@daum.net

watsonhenny@gmail.com

"Watson Henny" Facebook

rsaflam8808@gmail.com

[MONIKER 3 REDACTED]@gmail.com

stevegell77@gmail.com

[SW NAME REDACTED]@gmail.com

[LB NAME REDACTED]@gmail.com

[JK NAME REDACTED]@gmail.com

[KK NAME REDACTED]@gmail.com

"WatsonHenny" LinkedIn

MrDavid0818@gmail.com

MrDavid0818@gmail.com LinkedIn

agena316@gmail.com Facebook

agena316@gmail.com

jongdada02@gmail.com

skyfriend202@gmail.com

[JK NAME REDACTED]@outlook.com

messilionel.messi2015@yandex.com

jonnie.jemison@gmail.com

changtony1989@hanmail.net

Moniker 2 Facebook

Moniker 1 Facebook

[DJ NAME REDACTED]@gmail.com

[JB NAME REDACTED]@gmail.com

[ER NAME REDACTED]@gmail.com

[JC NAME REDACTED]@gmail.com

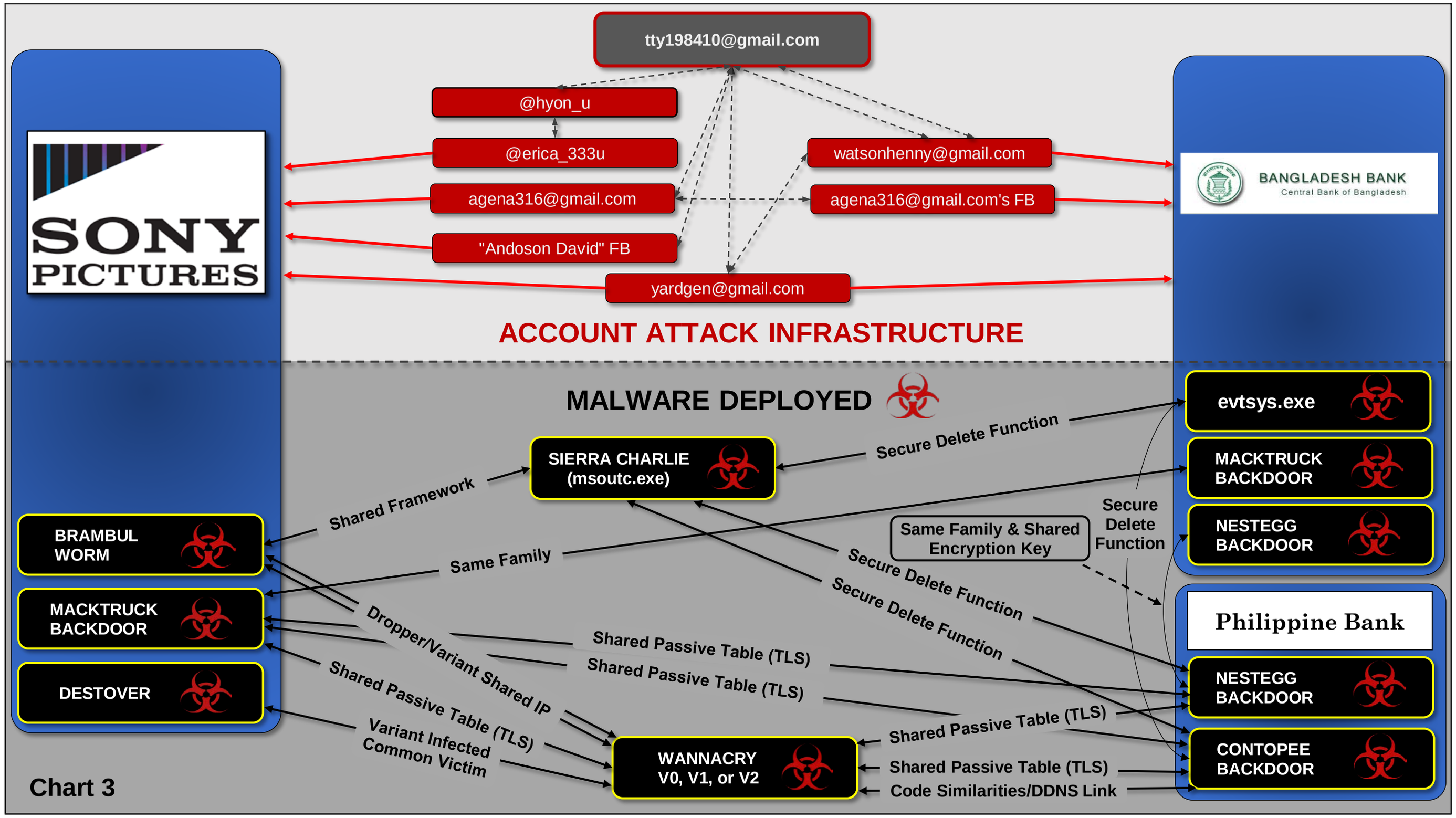
[JK NAME REDACTED] Facebook

jamesmartin20162016@gmail.com

Chart 2

= account accessed directly by North Korean IP address or from a North Korean IP address through a Proxy Service

= connection by subscriber email and/or access through same computer/device


tty198410@gmail.com
@hyon_u
@erica_333u
agena316@gmail.com
"Andoson David" FB
yardgen@gmail.com
watsonhenny@gmail.com
agena316@gmail.com's FB
SONY PICTURES
BANGLADESH BANK
Central Bank of Bangladesh
ACCOUNT ATTACK INFRASTRUCTURE
MALWARE DEPLOYED
SIERRA CHARLIE
(msoutc.exe)
BRAMBUL
WORM
MACKTRUCK
BACKDOOR
DESTOVER
WANNACRY
V0, V1, or V2
evtsys.exe
MACKTRUCK
BACKDOOR
NESTEGG
BACKDOOR
Philippine Bank
NESTEGG
BACKDOOR
CONTOPEE
BACKDOOR
Same Family & Shared
Encryption Key
Secure
Delete
Function
Secure Delete Function
Shared Framework
Same Family
Dropper/Variant Shared IP
Shared Passive Table (TLS)
Variant Infected
Common Victim
Shared Passive Table (TLS)
Code Similarities/DDNS Link
Chart 3