The Hack on Sony Group Pictures Entertainment

The Anatomy of One of the Most Devastating Attacks in History

How The Lazarus Group Executed the Compromise

secure OPS

THE LAZARUS GROUP'S 2014 HACK ON SONY PICTURES ENTERTAINMENT

Over the past few years, hacks against companies and governments have continued to grow, and their methods become more varied and effective. Memorable hacks include the attack against Yahoo!, which compromised every active account—a total of 3 billion,[1] the Wannacry ransomware attacks which struck across the globe, most notably affecting England and Scotland's National Health Service Hospital's computers, forcing hospitals to turn away patients,[2] and the 2014 Sony hack, which unlike many other hacks caused actual physical damage, and appeared to have been directed by a nation state to achieve its political ends.[3]

While these attacks initially captured the attention of the world, they have become less interesting as time has passed, but past hacks can offer insights into dealing with IT security in the future. For example, the Sony hack has at least three very good lessons: first, it was one of the first times actual physical damage was done using a cyberattack, and it forecasts some of the greater damage some experts fear a cyberattack could wreak, second, the Sony attack used pieces of the Wannacry ransomware, which shows how hackers can use old attacks to formulate new efforts. Third, some of the steps, like strong password protocols and data encryption or deletion, that would have helped to protect against the Sony hack are still important today, and still are not properly administrated. For these reasons, the Sony hack is a valuable case study, and it is worth a close examination.

In September 2014, unbeknownst to Sony Pictures Entertainment (Sony), hackers broke into Sony's networks and stole significant amounts of confidential data and planted malware.[4] On the Monday before Thanksgiving, when Sony employees tried to log into their computers a picture of a red skeleton appeared on their computer screens with the words "'#Hacked by GOP#'" and a threat to release data later.[5] In the coming weeks the hackers posted statements online containing links to data from Sony networks[6] including emails, salary information, movies that had not yet been released, as well as additional information.[7] The malware also destroyed 70 percent of Sony's laptops and computers.[8] In an historic move, the United States government formally attributed the hack to North Korea and charged a North Korean government hacker with the crime, based on a variety of indicators.[9] These included the hacker's call for Sony to not release the movie, "The Interview," which was a comedy about the assassination of Kim Jong-Un (Sony eventually bent under the pressure and only released the movie for download).[10] This paper provides an overview of how the hackers, members of what is commonly called the Lazarus Group,[11] carried out the hack and how the hack was traced to North Korea.

Phishing for Access

There are two technical ways for hackers to obtained data that belongs to people or organizations: break in and take it or intercept their data as it is transmitted and then decrypt it.[12] Social engineering is another way to get data—the hacker just asks for it in a way that tricks the users into believing they should give their information to the hacker. Often, before conducting a phishing attack, hackers will search online for information about individuals whose information they hope to steal, and then use that information to specifically target that person, a method called spear-phishing.[13] Often, hackers will copy legitimate emails, but then replace the hyperlinks in those emails "with hyperlinks that would re-direct potential victims to infrastructure under the [hacker's] control" where the hacker would then deliver malware to the victim's computer.[14] The methods of tricking users into handing over their data are only limited by hackers' ingenuity and users' credulity.

The hackers who participated in the 2014 Sony hack had a variety of possibilities for phishing attacks, according to the FBI investigation. For example, Facebook sends emails to users to alert them when a computer with a new IP address signs into their account, and contain links to follow-up on the sign-in.[15] In this instance, the hackers copied these legitimate emails, but changed the hyperlinked text for logging in to Facebook to the link http://www.fancug.com/link/facebok_en.html, which likely would have sent the user to malicious infrastructure (although the hyperlink was not active by the time the FBI obtained access to the email).[16] The hackers also created emails that looked like they came from Google to try to gain access to Sony workers' computers, one email, for example, purported to "welcome a recipient to Google's Drive service" but included a link to http://.[[DOMAIN REDACTED].com/x/o?u=2cfb0877-eaa9-4061-bf7e-a2ade6a30d32&c=374814 which was also likely to have sent the user to a malicious file.[17] Another email claimed to be from Google, alerting the user that "'malicious activities are detected'" but the Google hyperlinks offering information about how to mitigate malicious activities and Google's terms of service contained URLs that were not related to Google, and instead were likely malicious.[18]

A private researcher found a number of Sony employees, including Michael Lynton, Sony CEO,[19] had received phishing emails emails pretending to be from Apple.[20] These emails asked users to verify their Apple IDs because of supposed unauthorized activity and provided them with a link to click on that took them to a form that appeared to be from Apple but were fake, when the Sony employees typed their credentials into the fake forms the credentials fell into the hands of the individuals who sent the fake emails.[21] It appeared that the phishing emails were especially directed at Sony employees who had "broad access to the company's networks," information the hackers may have gathered by conducting surveillance about Sony employees via LinkedIn.[22]

Although experts cannot point to one specific set of spear-phishing emails that gave the hackers the access they needed to infiltrate Sony's networks, it is quite clear the hackers used spear-phishing to gain the initial information necessary to stage the hack.

Infrastructure Used in the Hack

To carry out the Sony hack, the actors used various infrastructure components including certain IP addresses, compromised hop point computers, proxy IP address services, and Dynamic Domain Name System, or DDNS. An IP address (Internet Protocol address) is "a set of four numbers…ranging from 0 to 255 and separated by a period…that is used to route traffic on the internet."[23] Each device that uses the internet has an IP address that can be used to identify it and send data to the device. The FBI investigation of the Sony hack found malicious activity related to the hack originating from several IP addresses assigned to North Korea.[24] The IP addresses associated with the activity come in two blocks: the first, "is a block of IP addresses, 175.45.176.0-175.45.179.255," and are registered to a company in North Korean, and the second is a block of addresses, "210.52.109.0—210.52.109.255" which are registered to a Chinese company, but have been used or leased by North Korean since before 2009.[25] From the devices associated with these addresses, the hackers carried out activity directed against Sony.

The hackers also used hop point computers to help hide their identity and location. A hop point conceals a user's original IP address because it acts as an intermediary between the

original IP address and the victim's network, so the victim can only see the address of the hop point computer.[26] Hop point computers usually belong to innocent users who are not involved in the hack, but use their devices without knowing hackers have compromised their computers.[27] In this case, the hackers used a particular piece of malware called the "Brambul" worm to compromise computers and use them as hop points.[28] Malware is a piece of software, or code, which is designed to take control away from the legitimate owner of the computer, and give it to another, usually without the legitimate owner knowing about it.[29] This piece of malware came in the form of a worm, which tries "to progressively infect computers, typically by exploiting a vulnerability in the victim's computers or by 'brute force' attacks upon victim computers.'"[30] The Brambul worm spread itself using "self-replication by infecting new victim systems via brute force attacks on the victim's Server Message Block ('SMB') Protocol."[31] A brute force attack is an attack that tries to log in to a computer using a list of combinations of usernames and passwords in an attempt to guess the correct credentials—the list of combinations is often in the thousands.[32] The SMB is a "network file sharing protocol" used by Microsoft,[33] i.e., a means of sharing files and more between computers.[34]

Once Brambul guessed the correct credentials and gained access to the computer it surveyed the computer and collected the machine's "IP address, system name, operating system, username last logged in, and last password used" and sent the information to one or more of the email addresses that the hackers hard-coded into the malware.[35] Using this information, the hackers could log in to one of the infected computers and use it as a hop-point to disguise the hackers' actual location.[36]

Proxy services were another infrastructure component the hackers used to hide their identity.[37] Proxy servers act much like hop points, in that they are an intermediary between the original user and the end computer, but unlike hop points which are formed using hacked computers, proxy servers are offered by businesses to consumers who want to avoid sending their IP address across the internet for good, or bad reasons.[38] The proxy service user can still use their original computer, but their request for data gets routed through another, intermediate server, who then contacts the end destination, effectively obscuring the original IP address.[39] The Sony hackers used proxy services as another way to disguise their identity.

The Sony hackers also used the dynamic domain name system (DDNS) to conceal their activities.[40] The Domain Name Service (DNS) is "a naming system for computers, services, or any other resources connected to the internet,"[41] it is often explained as "the phone book for the internet by 'resolving' human-friendly computer hostnames to IP addresses," for example, the domain name might be "www.justice.gov, and it may resolve to the IP address 149.101.146.50."[42] The DDNS allows users to control what IP address is assigned to their domain: the user can change the domain's associated IP address through the DDNS provider, and the changes will "propagate quickly across the internet," while it would take longer using a DNS service.[43]

The Sony hackers used a DDNS to help hide what they were doing: the malware they sent to computers would force the victim computer to look up the IP address assigned to a domain, but instead of connecting to that address, it would cause the computer to perform an "'XOR' operation using a specific hard-coded XOR key" to convert the original IP address into a new IP address,

and then the computer would connect to that address.[44] This meant that even with the domain embedded in the malware, investigators could not determine the location of computers the hackers controlled unless they had a detailed analysis of the malware and knew the XOR key.[45]

XOR, which is short for the phrase "exclusive-or," is a process in computer science where a binary key is applied to data to mix the two streams of data to form a new data stream:[46] if the input of either the key or data stream is 1 (and the other is 0), the new output will be 1, and if both the initial inputs are 1 or 0, then the output will be a zero, as demonstrated below.[47]

```
  01010111 01101001 01101011 01101001
⊕ 11110011 11110011 11110011 11110011
= ---------------------------------------
  10100100 10011010 10011000 10011010
```

Figure 1: XOR[48]

The combination of computers and their associated IP addresses, hop point computers and the malware used to gain access to them, proxy services, and DDNS provided the Sony hackers with the infrastructure they needed to support their intrusion into Sony's networks and to disguise their actions and identity.

The Malware

Phishing Success: How the Hackers got into Sony's Network

The FBI investigation found that the hackers tried to distribute the malware through spear-phishing emails and links posted on Facebook pages associated with Sony and actors involved in "The Interview," although it is not apparent if any of the malware on these pages led to a breach in the Sony network.[49] They did, however, find particular spear-phishing emails that appeared to have been successful in breaching Sony's network. Analysts found seven instances when Sony systems "'beaconed' to a specific Chinese IP address between September 26 and October 6, 2014," and in six of the seven times, the Sony user account used to connect to the IP address belonged to one specific Sony employee.[50] When a forensic team looked at that employee's hard drive they found a spear-phishing email sent from bluehotrain@hotmail.com on September 25, 2014.[51] Part of the text of the email read, "Here is the link," and then included a hyperlink to "http://1drv.ms/1rvZp.Fi.[52] Although the link was no longer active, the forensic analysts separately found a file named "'[REDACTED NAME OF BUSINESS] Advertising Video Clips (Adobe Flash).exe'"[53]

The use of the name, "Adobe Flash" in the title of the file was likely a way to distract the Sony employee and make it appear that the file was a media file that would play in Adobe Flash, when it was really an executable file, meaning it will download a program onto the computer.[54] Analysts determined that this file was malware, and when downloaded it caused the computer to connect to five hard-coded IP addresses (addresses that had been written directly into the malware), including the Chinese IP address that the Sony systems had beaconed to seven times between the end of September and beginning of October.[55] The malware had the ability to receive commands from the attackers that would then "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;" and it appeared to be the way the hackers were able to access Sony's network.[56]

How the Malware Spread

The malware used against Sony is specifically a Server Message Block (SMB) worm tool, and it included "a Listening Implant, Lightweight Backdoor, Proxy Tool, Destructive Hard Drive Tool, and Destructive Target Cleaning Tool."[57] The SMB worm tool is what gained initial access to the networks, which then allowed the other parts of the malware to complete their tasks. The SMB worm worked like the Brambul worm that

the hackers used to compromise computers to use as hop points: it used a "brute force authentication attack" to spread using Windows SMB shares (the purpose of Windows SMB is to allow information sharing, like files or printers).[58]

The worm had two threads of execution (thread refers to "the smallest unit of processing that can be performed in an operating system").[59] The first, involved the worm sending information back to the hackers in the form of logs: a log is a time-stamped list of certain events that are relevant to the particular system of program, for example, access logs for web servers, logs of changes made to databases, etc.[60] In this instance, every five minutes the worm would call home and send log data back to the command and control (C2) computer about whether it was successful at spreading to other computers running Windows.[61] In particular, the worm spread to other Windows hosts using port 445: a port is a channel or endpoint of communication for a computer or network, and port 445 is notoriously attack-prone because it is often open and available.[62]

The malware created a network file share and gave unrestricted access to that share, which meant any other computer on the network could access it. Then, it used the Windows Management Interface (WMB) command line to try to communicate to other network computers to launch code and spread itself.[63] Every process is launched using a command line, as the command line is used to "describe which application to run,"[64] so the hackers would have used the WMB command line to try to start new applications to contact other computers. Also, when the worm called back to C2 with information about its successes, it would accept new "scan tasking"—the hackers could send new commands to the worm, using a computer programming language.[65]

The second thread worked on a brute force attack against other computers' SMB connections.[66] A brute force attack means the program guesses over and over what the password is for a program, network, or other component, until it eventually guesses the right password and is granted access.[67] This demonstrates the need for strong passwords, which make it more difficult to guess a password, and other password protections, like multi-factor authentication, which requires more than a single password to grant access (it is also particularly helpful in protecting against breaches enabled by phishing attacks, because even if a person gives away one means of authentication, the other method has not been compromised).[68] These two threads provided the hackers access to the Sony network while updating them on it's actions, and spread the malware by connecting with other computers on the network.

The Malware's Listening Implant

As the listening implant is installed, it decrypts part of the computer's binaries (binaries are compiled versions of programs) using AES.[69] AES is short for Advanced Encryption Standard, and it is a widely used method of encryption.[70] AES is a block cipher, meaning the text is arranged into "blocks" of text, and it encrypts only 16 bytes of data at a time: it arranges the bytes into four rows with four columns, and it requires byte substitution, shifting rows, mixing columns, and adding a round key; although, to decrypt, the process would be reversed.[71]

Lightweight Backdoor

The malware used against Sony also contained a lightweight backdoor that functioned as a backdoor listener.[72] Lightweight means the software was relatively simple,[73] and a backdoor, in terms of hacking, is an illicit portal or point of entrance the hackers use or install on a system which gives them the ability "to come and go as they please and gives them remote access to the system."[74] This type of malware is often called a "remote access Trojan" or RAT, and can be used to "install other malware on the system or exfiltrate data."[75] In this case, the backdoor was a listener "designed as a service DLL."[76] DLL is short for Dynamic Link Library; it is "a library of code" and more than one program can use it at a time.[77] The creator could then "execute

commands on the command line" and "execute arbitrary code,"[78] meaning the hackers could run any command they wanted on the hacked system.[79] This meant the hackers could do a large number of things to advance their access to and knowledge of the computer system, as well as their ability to do damage; for example, the backdoor enabled "file transfer, system survey, process manipulation, file time matching, and proxy capability."[80] The file transfer and system survey abilities are particularly interesting, because the Lazarus Group hackers stole large amounts of data from Sony, and this may have been the piece of malware that allowed them to exfiltrate that data. It also means they could examine the computer system looking for other ways to gain more access or control or do other damage.

The backdoor also allows the hackers to open ports in the victim's firewall and use "universal Plug and Play (UPNP) mechanisms to discover routers and gateway devices, and add port mappings."[81] Essentially, it makes it easier for the hackers to find other devices, like computers and devices that are on the network, and connect to and communicate with them.

Proxy Tool

The malware also contained a proxy tool. It was likely installed as a service file, which might have been a .exe file, demonstrating one of the key characteristics of malware files—its executable nature. The proxy tool was "configured to listen on TCP port 443. TCP stands for Transmission Control Protocol, and is a protocol, or list of rules that governs how data is sent between two points of connection, either over the internet or via another network.[82] It works by taking a file that needs to be delivered, dividing it into packets of data and then sending each packet to the IP layer of program, which then delivers the data packets. Upon delivery, the TCP assembles the packets back in the original file and delivers it to the waiting application.[83]

Port 443 is the standard port or line of communication used by websites that use SSL, or secure sockets layer, a technology that establish a secure, encrypted link between a web server and browser, using an SSL certificate.[84] When a web server activates SSL, it creates a public and private cryptographic key. The public key goes into a Certificate Signing Request (CSR) and is submitted to the Certification Authority.[85] Once they issue an SSL certificate, the web server matches the certificate to the web server's public key, and the web server can establish an encrypted link between the server and a person's browser.[86] When a person's browser wants to connect to a site, it will retrieve the site's certificate and ensure that is has not expired, that it was issued by a trustworthy Certification Authority, and it is being used by the website the certificate was issued to, if these criteria are met, the browser will establish a secure connection, as indicated by a lock near the URL..[87] SSL was formerly used as the method of encryption for HTTPS, the protocol for communicating over the internet (TLS has since replaced it as the most updated version).[88] This proxy tool then, listened for traffic on port 443, which was reserved for data being transferred in what should be a secure way.

Destructive Hard Drive Tool

The hack on Sony destroyed about three-quarter's of the company's computers and servers at it's central location, and erased large amounts of data.[89] The malware that infected Sony's systems contained three components, each of which was capable of deleting data or rendering computers inoperable through changes to physical hard drives or the master boot record (MBR).[90] A destructive hard drive tool is the first of these components. This tool was designed to wipe the hard drive and destroy data past recovery, as well as make it more difficult to recover the infected machine.[91] A hard drive is a piece of equipment that stores data long-term,[92] and the MBR is a special boot sector of a hard drive: a boot sector is a physical sector of the hard drive that contains information about how to initiate the "boot" process and load the operating system.[93] Without the MBR, the computer isn't able to load the operating system.

The destructiveness of the tool depended on the level of privileges, or access to systems, the host computer had: if the host computer had administrative privileges, the tool could over-write portions of as many as four physical hard drives, and would "over-write the master boot record (MBR) with a program designed to cause further damage if the hard drive [were] rebooted."[94] If an individual had only "user-level access" then the malware would delete specific files and they would be "practically irrecoverable,"[95] but the computer would still be useable. Thus, by overwriting the MBR and deleting files, the malware was capable of both destroying data and rendering computers physically unusable. The difference in the level of destruction depending on the victim computer's access or privileges demonstrates why the hackers would have been interested in getting the login credentials of employees with high levels of access, as mentioned in the beginning of this report.

Destructive Target Cleaning Tool

This tool was also designed to make computers inoperable by overwriting its MBR. The malware was installed via an executable file which contained three parts: an executable, a DLL, and an encoded command file.[96] The executable and DLL contained the code that overwrote the MBR, and the encoded command file contained "the actual destruction commands" that initiated the destructive code.[97]

Network Propagation Wiper

The final component that erased data was a network propagation wiper. This malware used "built-in Windows shares" to move throughout the Sony network.[98] Using usernames and passwords the hackers had, and the hostname and IP address of the systems they wanted to target, the hackers would "access remote network shares" and upload a copy of the malware to begin remotely wiping data in the computers.[99] The malware had two methods for accessing shared files on these remote systems. The first was to check for shared files that already existed, using the filenames "\\hostname\admin$\system32 and \\hostname\shared$\system32."[100] A hard drive does not distinguish between files, it only stores the data; a computer's operating system uses code to organize the space on the hard drive, and it allows programs to see the code through a "filesystem" where each file has a "file path" which is a textual way for programmers to point to or reference the location of a particular file.[101] File paths can be written in a variety of ways, but the filenames "\\hostname\admin$\system32 and \\hostname\shared$\system32" likely point first to the server the file is located one: hostname, then the user: admin or shared$,[102] and finally the type of file: a system file, in particular system32, which contains "Windows system files and software program files" that are "vital to the operation of the Windows operating system and software programs."[103] This shows that the malware hoped to infiltrate shared critical files on computers.

If no shared files existed, the malware created a new share using "cmd.exe /q /c net share shared$=%SystemRoot%/GRANT:everyone, FULL." And would then upload a copy of the wiper malware "taskhostXX.exe," another executable file, and start remotely wiping the computer.[104]

In Hindsight and Going Forward: Preventative Measures for Similar Hacks

Combined, the different pieces of malware involved in the hack against Sony enabled the hackers to exfiltrate large amounts of of data, delete data, and render a large portion of Sony's devices in their central location physically unusable. Although other hacks have compromised more data, or data belonging to a larger number of people, like the Yahoo! hack, which potentially exposed the information of three billion users,[105] the Sony hack gathered attention because it caused physical damage to the company's infrastructure and appeared to involve a nation-state hacking a private company to achieve political ends. Since the hack, there has been discussion about what went wrong in terms of Sony's computer security, and what Sony and other companies should do to protect themselves. There are three significant things that Sony could have done differently to increase their computer security: use better password protocols, delete or encrypt data, and segregate servers.

When the hackers began releasing the data they took from Sony systems the information included lists of password, some of the passwords were "s0ny123" and "password," which are very weak.[106] The leak also included a folder

that contained payroll spreadsheets; these were protected by a password, but there was another document in the folder named "passwords" that contained the passwords to unlock the spreadsheets.[107] Although the list of passwords may not have even been necessary, if it were, they should have been encrypted. To encrypt the passwords, Sony could have taken the passwords and added a random string of data to it, called "salt," designed to protect against rainbow table attacks which use tables of hashed passwords to guess passwords, and then run it through a secure cryptographic hash function which would change the text into a non-invertible number (it could not then be returned back to the original plain text), but stable, meaning the hash is the same for a particular password any time it is initially hashed.[108] The hash of the salt and password should then be run through the hashing function several times to help protect it from brute force attacks.[109] It also appears that Sony employees did not use two-factor authentication, which requires using a password and some other credential, like an SMS code, Google code, or key fob, and is a common method to protect access.[110]

When the hackers began to release the data they had stolen from Sony, it also showed that, in accordance with their email-retention policy, Sony had kept emails from the past seven years. This data was unencrypted, and it appeared that Sony "was essentially using email for long-term storage of business records, contracts, and documents saved in case of litigation."[111] Keeping less data and encrypting the data that was kept would help prevent hackers from stealing and using or releasing the information.

It also appears that data was not well segregated, which meant that once the hackers got inside the Sony network, they were able to move between systems easily, stealing data as they went.[112] By hardening the servers, Sony may have been able to better protect their networks and keep the hackers from gaining as much access. Some steps that may be included in hardening servers includes deleting unnecessary ports, turning off unnecessary services, not installing unnecessary applications, and disabling or deleting unnecessary accounts. This can make it more difficult to access data.[113] Although it is likely impossible to protect against every vulnerability, the changes listed above would add more security to a computer network.

Attribution of the Attack

The Sony hack is unusual because it is one of the few cases where the U.S. government publicly attributed the hack to a nation-state, as well as because of the rapidity of the attribution. On November 24 2014 Sony realized it had been hacked, and by December 3, 2014 the FBI attributed the hack to North Korea, making it "the first time that the United States has openly laid blame on a foreign government for a destructive cyberattack against an American corporation."[115] It is often difficult to trace cyberattacks, and linking the Sony hack to North Korean hackers required connecting multiple hacks that took place across the world and then connecting them to the Sony hack using knowledge about the other hacks and similarities between them determine the creators of the Sony malware.

WannaCry Ransomware FakeTLS Table, Bitcoin, and Connections to North Korea

The most convincing link tying the Sony hack to other hacks and back to North Korea, was the use of a FakeTLS table that appeared in intrusions at the Philippine bank and Southeast Asian bank.[116] The FakeTLS table appeared in three samples of malware called MACKTRUCK that appeared in the Sony hack, in malware called Contopee, which appeared in malware used against the Philippine bank and Southeast Asian Bank, and in the malware NESTEGG, which was used against the Philippine Bank.[117] The table was simply "a data table coded within the malware" and had no apparent purpose. The lack of purpose suggested that it was drawn from a "control or common library or database of malware" used repeatedly by the same hackers, thus supporting the argument that the same people were behind each hack.[118]

This data table also appeared in an early version of the "WannaCry" ransomware, but in that piece of malware it was a critical part of the code and was used to conduct FakeTLS communication.[119] Computers use the TLS (Transport Layer Security) handshake protocol to communicate securely by, among other things, choosing "which cipher suite will be used throughout their exchange."[120] The protocol provides a list of cryptographic algorithms that can encrypt the TLS communications, and each of these algorithms, or cipher suites, is "assigned a two-byte

identification code" (a byte of data consists of 8 bits of data, and each bit is either a zero or one) that the client computer sends to the server, to select a cipher to encrypt the rest of the TLS communication.[121] The malware contained a list of two-byte values that are used to help generate the cipher suites, this makes it harder for "network security software to distinguish between legitimate TLS traffic" and the malicious software that contained the FakeTLS code, which makes it harder to block malicious traffic without also blocking legitimate traffic.[122]

The fact that all of these pieces of malware contained the same data table is important because it shows "the authors of the malware samples very likely had access to the same collection of original source code"[123] which means that if the authors of one piece of malware can be traced, they can be linked to the other hacks, and the WannaCry ransomware attacks were linked to North Korea through IP addresses, language fonts, and time-stamps.[124]

Ransomware is a type of malware that once it infects a computer it encrypts the computer's files and requires the users to pay the hackers, usually through something like Bitcoin, to decrypt the data. The WannaCry ransomware exploited a Microsoft Server Message Block vulnerability called "CVE-2017-0144,"[125] and had three different versions, Version 0, Version, 1, and Version 2, some of which spread more widely than others.[126] Analysts determined that the different versions of "WannaCry" were created by the same author, based on factors that included nearly identical core components (even though the source code was not public), similar passwords through all three iterations, and similarities in how Bitcoin payments were processed.[127]

When a computer's files are encrypted by ransomware the computer's owner often pays to have the files decrypted using Bitcoin, an anonymous way of exchanging money. Bitcoin is "the name of the payment network on which the Bitcoin digital tokens are stored and moved," all without a central authority, instead it "is run by a decentralized network of computers around the world that keep track of all Bitcoin transactions."[128] The record that these computers update with Bitcoin transactions is called the blockchain.[129] The blockchain uses a ledger, or digital file, to document all transactions on Bitcoin; the ledger doesn't exist in a central location, but is distributed across private computers, called nodes, all over the world, and each computer has a copy of the ledger.[130] The ledger does not keep track of balances, but rather, records requested transactions, and users verify their balance by linking all previous transactions.[131]

When users want to send Bitcoins, they broadcast "a message to the network" saying their account should go down by a certain amount, and the other person's account should increase by the same amount, and each node updates their ledger accordingly.[132] To engage in Bitcoin transactions, users must have a wallet, and each wallet is protected using a public and private cryptographic key. The private key is used by the wallet owner to make sure no other person can use the wallet: the owner sends a message encrypted with the private key, and then the other node can ensure the message was sent by the wallet owner, using the public key to decrypt the message.[133] When users encrypt a message with their private key it creates a digital signature, which is "a string of text" generated "by the combination of [the] transaction request and [the] private key" and if another person changes any character in the string it changes the digital signature, which prevents another person from altering the transaction.[134] Transactions pass through the Bitcoin network and reach different nodes at different times, to order the transactions, the Bitcoin network groups transactions into blocks, and each block has a link to the block of transactions before it.[135]

The creators of Version 1 and 2 of WannaCry used Bitcoin for payment, and investigators found that when the Bitcoins were transferred from various wallets to another type of

cryptocurrency, the transfers took place using IP addresses that were TOR network exit nodes (TOR is an anonymous network that distributes traffic over multiple computers so users cannot be traced),[136] and transfers for payments from both Version 1 and 2 "used the same browser User-Agent string" which may be an "indication that the same user or computer" may have conducted the transfers.[137] This helps connect the different WannaCry versions.

Analysts found that an "IP address used for command and control in connection with Version 1, was accessed by North Korean IP addresses."[138] This means that one of the computers that controlled the WannaCry ransomware was also connected to a computer in North Korea, supporting the belief that North Korean hackers created and used the malware. Further, investigators found that individuals with a North Korean IP address had been researching how to develop code "that would exploit the CVE-2017-0144 vulnerability" that Version 2 of WannaCry used.[139] They found that the users of the same North Korean IP address mentioned above visited technet.microsoft.com, where Microsoft provided information about Microsoft products, including vulnerabilities, like the CVE-2017-0144, and other websites with information about the vulnerability.[140]

The FBI's Cyber Behavioral Analysis Center (CBAC) found that the computer that was used to "create the [WannaCry] ransomware language files had the Korean language fonts installed," because of the Rich Text Format tag "/fcharset129" which is not usually part of a default installation in the U.S., but is included in a Korean installation[141] (Rich Text Format is a file format for text and graphics).[142] The language files of each version of WannaCry had an RTF tag that contained a timestamp. The timestamps led the CBAC to think the computer may have been set to the time zone used in South Korea; the same time zone was also used in North Korea until 2015.[143] The above evidence, and other evidence that does not appear in this review, ties the different versions of WannaCry together and ties them to North Korea; in turn, the FakeTLS table used in WannaCry ties the Sony hack to the WannaCry ransomware and thus back to North Korea.

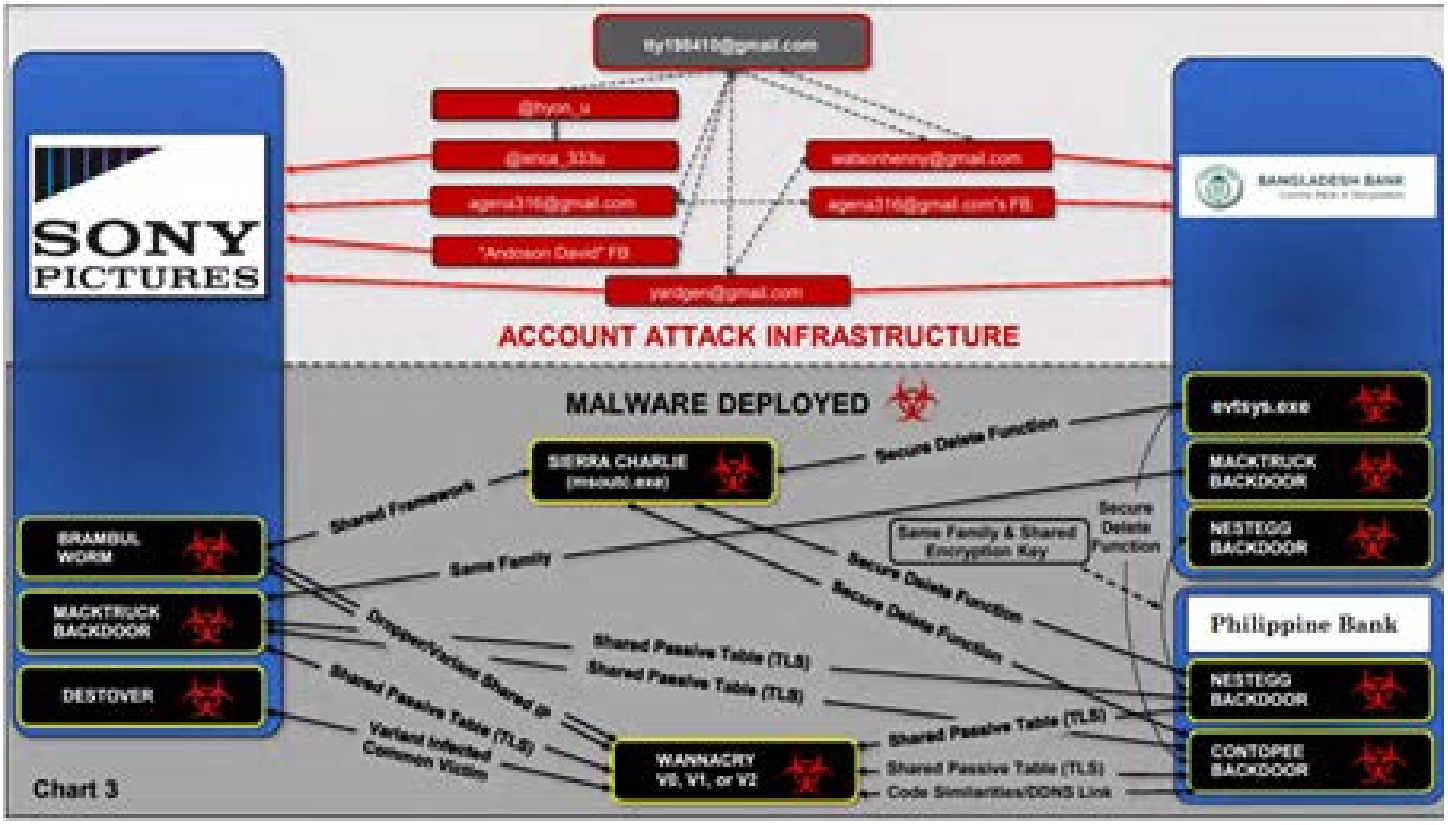
Other Connections Between the WannaCry Ransomware and the Sony Hack

Analysts found many other links between the WannaCry ransomware, other hacks, the Sony hack, and North Korea. For example, A report from Symantec, a cybersecurity company, reported that they found three pieces of malware on a victim's computer from WannaCry version 0, and found two variants of the malware "Backdoor.Destover" which was also used against Sony.[144] Also, a sample of the WannaCry malware used the IP address "84.92.36.96 as a command-and-control address," and in February and March of 2016, a North Korean IP address connected to that IP address and connected to a compromised computer that was infected with malware connected to the Sony hack.[145] These similarities, and others that are beyond the scope of this discussion, are convincing evidence to connect the Lazarus group to the Sony hack, and in turn connect the Lazarus group to North Korea.

The graphic below showcases in more detail the connections between malware and email accounts that help attribute the Sony hack to the Lazarus group.[146]

Conclusion

The 2014 Sony hack caught the attention of the world because of the damage it did to a large company, both in terms of stealing data, and, more unusually, making physical infrastructure unusable. The hack became even more unusual when the U.S. government took the step of publicly attributing the hack to North Korean hackers. This paper reviews some of the technical details behind the hack on Sony and a portion of the work investigators and analysts undertook to attribute the hack to the Lazarus group and North Korea, demonstrating the variety of knowledge and skill that went into carrying out the hack, and the methods used to trace it.



References and Resources

1: Selena Larson, "Every Single Yahoo Account Was Hacked – 3 Billion in All," CNN Business, October 4, 2017, accessed June 8, 2019, https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.
2: "Global Cyberattack Strikes Dozens of Countries, Cripples U.K. Hospitals," CBS News, May 12, 2017, accessed June 6, 2019, https://www.cbsnews.com/news/hospitals-across-britain-hit-by-ransomware-cyberattack/.
3: Alert (TA14-353A): Targeted Destructive Malware," US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A and Ellen Nakashima, Craig Timberg, and Andrea Peterson, "Sony Pictures Hack Appears to be Linked to North Korea, Investigators Say," Washington Post, December 3, 2014, accessed December 10, 2018, https://www.washingtonpost.com/world/national-security/hack-at-sony-pictures-appears-linked-to-north-korea/2014/12/03/6c3c7e3e-7b25-11e4-b821-503cc7efed9e_story.html?utm_term=.a21e2ffc8b96.
4: David E. Sanger, David D. Kirkpatrick, and Nicole, "The World Once Laughed at North Korean Cyberpower. No More," The New York Times, October 15, 2017, accessed December 10, 2018, Perlrothhttps://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html
5: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.39300b4eb387.
6: Andrea Peterson, "The Sony Pictures Hack Explained," Washington Post, December 18, 2014, accessed December 10, 2018, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.39300b4eb387.
7: Gabi Siboni and David Siman-Tov, Cyberspace Extortion: North Korea versus the United States, INSS Insight No. 646, (p. 1) December 23, 2014.
8: David E. Sanger, David D. Kirkpatrick, and Nicole, "The World Once Laughed at North Korean Cyberpower. No More," The New York Times, October 15, 2017, accessed December 10, 2018, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.
9: Ellen Nakashima and Devlin Barrett, "U.S. Charges North Korean Operative in Conspiracy to Hack Sony Pictures, Banks," Washington Post, September 6, 2018, accessed December 10, 2018, https://www.washingtonpost.com/world/national-security/justice-department-to-announce-hacking-charges-against-north-korean-operative-the-charge--stemming-from-the-2014-sony-pictures-case--is-the-first-against-a-pyongyang-spy/2018/09/06/f477bfb2-b1d0-11e8-9a6a-565d92a3585d_story.html?utm_term=.51a4bb2ea79b.
10: David E. Sanger, David D. Kirkpatrick, and Nicole, "The World Once Laughed at North Korean Cyberpower. No More," The New York Times, October 15, 2017, accessed December 10, 2018, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.
11: "Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 5.
12: Matthew Tait, "Cybersecurity Foundations: Social Engineering," (lecture, University of Texas at Austin, Austin, TX, November 26, 2018).
13: "Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 20.
14: "Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 20-21.
15: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 21.
16: Complaint, 21.
17: "Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 22-23
18: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 23.
19: Collen Kriel, "Sony Hackers Used Fake Apple ID Emails to Steal Passwords, Says Researcher, Silicon Angle, Aprik 22, 2015, accessed December 10, 2018, https://siliconangle.com/2015/04/22/sony-hackers-used-fake-apple-id-emails-to-steal-passwords-says-researcher/.
20: Gregg Keizer, "Sony Hackers Targeted Employees with Fake Apple ID Emails, Computer World, April 23, 2015, accessed December 10, 2018, https://www.computerworld.com/article/2913805/cybercrime-hacking/sony-hackers-targeted-employees-with-fake-apple-id-emails.html.
21: Gregg Keizer, "Sony Hackers Targeted Employees with Fake Apple ID Emails, Computer World, April 23, 2015, accessed December 10, 2018, https://www.computerworld.com/article/2913805/cybercrime-hacking/sony-hackers-targeted-employees-with-fake-apple-id-emails.html.
22: Gregg Keizer, "Sony Hackers Targeted Employees with Fake Apple ID Emails, Computer World, April 23, 2015, accessed December 10, 2018, https://www.computerworld.com/article/2913805/cybercrime-hacking/sony-hackers-targeted-employees-with-fake-apple-id-emails.html.
23: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 10.
24: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 13.
25: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 10.
26: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 9.
27: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 9.
28: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 14.
29: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 10.
30: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 35.
31: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:, 15.
32: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 13.

33: “Microsoft SMB Protocol and CIFS Protocol Overview,” Microsoft, accessed December 10, 2018, https://docs.microsoft.com/en-us/windows/desktop/FileIO/microsoft-smb-protocol-and-cifs-protocol-overview.
34: Why and How to Disable Windows SMB1 on Windows 10/8/7,” The Windows Club, accessed December 10, 2018, https://www.thewindowsclub.com/disable-smb1-windows.f
35: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 15.
36: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 16.
37: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 16.
38: “Proxy Server,” What is My IP Address, accessed December 10, 2018, https://whatismyipaddress.com/proxy-server.
39: “Proxy Server,” What is My IP Address, accessed December 10, 2018, https://whatismyipaddress.com/proxy-server.
40: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018:, 18.
41: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 7.
42: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 8.
43: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 8.
44: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 18.
45: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 18.
46: Matthew Tait, “Cybersecurity Foundations: Intro to Tech: Block Ciphers (lecture, University of Texas at Austin, Austin, Tx).
47: “Binary XOR Operation,” xcprod, accessed December 10, 2018, http://xcprod.com/titan/XCSB-DOC/binary_xor.html.
48: “XOR Cipher,” Wikipedia, accessed December 10, 2018, https://en.wikipedia.org/wiki/XOR_cipher.
49: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 33-39.
50: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 45.
51: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 45.
52: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 45
53: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018:, 45.
54: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 45-46.
55: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 46.
56: Criminal Complaint: United States of America v. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park,” aka “Pak Jin, Hek,” U.S. District Court for the Central District of California, June 8, 2018: 46.
57: “Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
58: “SMB Protocol and CIFS Protocol Overview,” Microsoft, May 30, 2018, accessed December 10, 2018, https://docs.microsoft.com/en-us/windows/desktop/fileio/microsoft-smb-protocol-and-cifs-protocol-overview.
59: “Thread,” Techopedia, accessed December 10, 2018, https://www.techopedia.com/definition/27857/thread-operating-systems.
60: “Definition: Log (log file),” Tech Target, accessed December 10, 2018, https://whatis.techtarget.com/definition/log-log-file.
61: “Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
62: Kevin Beaver, “How to Detect and Defend Against a TCP Port 445 Exploit,” accessed December 10, 2018, https://searchsecurity.techtarget.com/answer/Detecting-and-defending-against-TCP-port-445-attacks.
63: Sean Gallagher, “Inside the ‘Wiper’ Malware that Brought Sony Pictures to its Knees [Update],” Ars Technica, December 3, 2014, accessed December 10, 2018, https://arstechnica.com/information-technology/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/.
64: Matthew Tait, “Cybersecurity Foundations: Intro to Tech: Command Lines,” (lecture, The University of Texas at Austin, Austin, TX.
65: “Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
66: “Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
67: Aimee O’Driscoll, “What A Brute Force Attack is (With Examples) and How you Can Protect Against One,” CompariTech, May 9, 2018, accessed December 10, 2018, https://www.comparitech.com/blog/information-security/brute-force-attack/.
68: Matthew Tait, “Cybersecurity Foundations: Social Engineering,” (lecture, University of Texas at Austin, Austin, TX, November 26, 2018).
69: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
70: “Advanced Encryption Answers,” TutorialsPoint, accessed December 10, 2018, https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm.
71: “Advanced Encryption Answers,” TutorialsPoint, accessed December 10, 2018, https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm,
and Matthew Tait, “Cybersecurity Foundations: Tech Intro: Block Ciphers,” (lecture, The University of Texas at Austin, Austin, TX).
72: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
73:“Definition: Lightweight,” TechTarget, accessed December 10, 2018, https://whatis.techtarget.com/definition/lightweight.

74: Kim Zetter, “Hacker Lexicon: What is a Backdoor?” December 11, 2014, accessed December 10, 2018, https://www.wired.com/2014/12/hacker-lexicon-backdoor/.
75: Kim Zetter, “Hacker Lexicon: What is a Backdoor?” December 11, 2014, accessed December 10, 2018, https://www.wired.com/2014/12/hacker-lexicon-backdoor/.
76: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
77: “What is a DLL,” Microsoft, accessed December 10, 2018, https://support.microsoft.com/en-us/help/815065/what-is-a-dll.
78: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
79: “Problem Solve: How Does ‘Arbitrary Code’ Exploit a Device?” TechTarget, accessed December 10, 2018, https://searchsecurity.techtarget.com/answer/How-does-arbitrary-code-exploit-a-device.
80: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
81:Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
82:Angie Beal, “TCP – Transmission Control Protocol,” Webopedia, accessed December 10, 2018, https://www.webopedia.com/TERM/T/TCP.html.
83:“Definition: TCP (Transmission Control Protocol), TechTarget, accessed December 10, 2018, https://searchnetworking.techtarget.com/definition/TCP.
84: “Q10241—FAQ: What is SSL?” SSL.com, accessed December 10, 2018, http://info.ssl.com/article.aspx?id=10241.
85: “Q10241—FAQ: What is SSL?” SSL.com, accessed December 10, 2018, http://info.ssl.com/article.aspx?id=10241.
86: “Q10241—FAQ: What is SSL?” SSL.com, accessed December 10, 2018, http://info.ssl.com/article.aspx?id=10241.
87: “Q10241—FAQ: What is SSL?” SSL.com, accessed December 10, 2018, http://info.ssl.com/article.aspx?id=10241.
88: “What is an SSL Certificate?” Symantec, accessed December 10, 2018, https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https.
89: David E. Sanger and Michael S. Schmidt, “More Sanctions on North Korea After Sony Case,” The New York Times, January 2, 2015, accessed December 10, 2018, https://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html?referrer=.
90: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
91: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
92: Tyler Lacoma, “What is a Hard Drive?” Digital Trends, March 19, 2018, accessed December 10, 2018, https://www.digitaltrends.com/computing/what-is-a-hard-drive-your-guide-to-computer-storage/.
93: Tim Fisher, “What is a Boot Sector,” March 12, 2017, accessed December 10, 2018, https://www.lifewire.com/what-is-a-boot-sector-2625815.
94: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
95: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
96: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
97: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
98: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
99: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
100: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
101: Matthew Tait, “Cybersecurity Foundations: Introduction to Tech: Websites and NUL-Byte Injections,” (lecture, University of Texas at Austin, Austin, TX).
102: “Path (Computing)” Wikipedia, accessed December 10, 2018, https://en.wikipedia.org/wiki/Path_(computing)
103: “System32” Computer Hope, September 22, 2017, accessed December 10, 2018, https://www.computerhope.com/jargon/s/system32.htm.
104: Alert (TA14-353A): Targeted Destructive Malware,” US-CERT, September 30, 2016, accessed December 10, 2018, https://www.us-cert.gov/ncas/alerts/TA14-353A.
105: Alina Selyukh, “Every Yahoo Account that Existed in Mid-2013 was Likely Hacked,” October 3, 2017, accessed December 10, 2018, https://www.npr.org/sections/thetwo-way/2017/10/03/555016024/every-yahoo-account-that-existed-in-mid-2013-was-likely-hacked.
106: Lorenzo Francheschi-Bicchierai “Sony Picture Leak Shows Employees Used Worst Passwords Ever,” December 2, 2014, accessed December 10, 2018, https://mashable.com/2014/12/02/sony-hack-passwords/#KBKClQBuR5qu.
107: Lorenzo Francheschi-Bicchierai “Sony Picture Leak Shows Employees Used Worst Passwords Ever,” December 2, 2014, accessed December 10, 2018,https://mashable.com/2014/12/02/sony-hack-passwords/#KBKClQBuR5qu.
108: Matthew Tait, “Cybersecurity Foundations: Intro to Tech: Stream Ciphers,” (lecture, University of Texas at Austin, Austin, TX).
109: Matthew Tait, “Cybersecurity Foundations: Intro to Tech: Passwords and Intro to Crypto,” (lecture, University of Texas at Austin).
110: Matthew Tait, “Cybersecurity Foundations: Intro to Tech: Phishing and Social Engineering,” (lecture, University of Texas at Austin, Austin, TX).
111: Peter Elkind, “Sony Hack Part Two: The Storm Builds,” Fortune, June 26, 2015, accessed December 10, 2018, http://fortune.com/sony-hack-part-two/.
112: Mike Gillespie, “think Tank: Lessons to be Learned from Sony Breach,” Computer Weekly, accessed December 10, 2018, https://www.computerweekly.com/opinion/Security-Think-Tank-Lessons-to-be-learned-from-Sony-breach-on-limiting-attacks.
113: Sandra Kay Miller, “Five Ways to Harden Windows Server,” Computer Weekly, accessed December 10, 2018, https://www.computerweekly.com/news/2240020779/Five-ways-to-harden-Windows-Server.

114: Ellen Nakashima, Craig Timberg, and Andrea Peterson, "Sony Pictures Hack Appears to be Linked to North Korea, Investigators Say," Washington Post, December 3, 2014, accessed December 10, 2018, https://www.washingtonpost.com/world/national-security/hack-at-sony-pictures-appears-linked-to-north-korea/2014/12/03/6c3c7e3e-7b25-11e4-b821-503cc7efed9e_story.html?utm_term=.a21e2ffc8b96.
115: Ellen Nakashima, "US Attributes Cyberattack on Sony to North Korea," December 19, 2014, accessed December 10, 2018, https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html?utm_term=.831d67544d1f.
116: C Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:118
117: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:77.
118: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:77-78.
119: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:79
120: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:63, 79.
121: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:80.
122: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:80.
123: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:81.
124: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:111 and 115.
125: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:106
126: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:109 and 110.
127: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:110.
128: Nathaniel Popper, "What is Bitcoin, and how Does it Work?" The New York Times, October 1, 2017, accessed December 10, 2018, https://www.nytimes.com/2017/10/01/technology/what-is-bitcoin-price.html.
129: Nathaniel Popper, "What is Bitcoin, and how Does it Work?" The New York Times, October 1, 2017, accessed December 10, 2018, https://www.nytimes.com/2017/10/01/technology/what-is-bitcoin-price.html.
130: Michele D'Aliessi, "How Does the Blockchain Work? The Blockchain Technology Explained in Simple Words," Medium, June 1, 2016, accessed December 10, 2018, https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae.
131: Michele D'Aliessi, "How Does the Blockchain Work? The Blockchain Technology Explained in Simple Words," Medium, June 1, 2016, accessed December 10, 2018, https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae.
132: Michele D'Aliessi, "How Does the Blockchain Work? The Blockchain Technology Explained in Simple Words," Medium, June 1, 2016, accessed December 10, 2018, https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae.
133: Michele D'Aliessi, "How Does the Blockchain Work? The Blockchain Technology Explained in Simple Words," Medium, June 1, 2016, accessed December 10, 2018, https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae.
134: Michele D'Aliessi, "How Does the Blockchain Work? The Blockchain Technology Explained in Simple Words," Medium, June 1, 2016, accessed December 10, 2018, https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae.
135: Michele D'Aliessi, "How Does the Blockchain Work? The Blockchain Technology Explained in Simple Words," Medium, June 1, 2016, accessed December 10, 2018, https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae.
136: "Tor: Overview," Tor Project, accessed December 10, 2018, https://www.torproject.org/about/overview.html.en
137: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:, 117
138: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:111
139: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018: 111.
140: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:125
141: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:115.
142: http://accessproject.colostate.edu/udl/modules/word/tut_rtf.php
143: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:115.
144: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:121.
145: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:122.
146: Criminal Complaint: United States of America v. Park Jin Hyok, also known as ("aka") "Jin Hyok Park," aka "Pak Jin, Hek," U.S. District Court for the Central District of California, June 8, 2018:175.