Case Study: 2014 Sony Pictures Entertainment cyber attack

Team: MORPHO-7470

Jesús Gabriel Ly Ponce
Pere Garau Burguera
Tahmid Quddus

Abstract

The present work is a case study where we analyze the cyber attack suffered by the North American company Sony Pictures Entertainment (SPE) in 2014 where its computer data base was compromised, personal data was stolen and movie material as well. This attack was perpetrated by a rogue unit from North Korea calling themselves as "The Guardians of Peace" (GOP) causing that SPE's networks and IT systems were offline, releasing publicly private information, e-mails, executives' salaries and personal data from the Sony's employees. This attack is considered as one of the worst corporate hacks in the history of the United States because it forced the company to cancel the release of the movie *The Interview*, to later develop into a national security crisis where the FBI and other U.S. government agencies were involved to deal with the attack, also movie theaters were threatened to suffer physical attacks. From the cyber security perspective we observe how the accident within one company triggers a serious national security crisis of cyber terrorism, involving presidents from two different nations (U.S and North Korea), leading to the involvement also of the U.S. Federal government.

Introduction

The computer database hack suffered by Sony Picture Entertainment on 2014 unleashed a storm of attention on cyber attacks and took SPE to the forefront of the media and public because it was not only a simple hack news, this event became a crisis of serious national security for the United States and was treated as an act of cyberterrorism. At the beginning of the attack, it was presumed that this was not real or was just a hoax, however, as the crisis was evolving, they realized that it was a serious issue, since e-mails and threats turned into concrete actions, and then the U.S. National Security had to take part into the event. For many of us, the idea of terrorism is associated with specific actions of violence in our heads and we are all in a way familiar with the concept, that according with the U.S civil code is defined as "the term terrorism means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents; the term terrorist group means any group practicing, or which has significant subgroups which practice, international terrorism" [1]. Nevertheless, we are living in a fully connected and technological era of the information where the Internet is the major enabler for most of our daily activities, for this reason, the definition of terrorism is no longer applicable only to the physical world or actions against it, now this terminology can also be extended to the "virtual" world or the "cyber space" and the violence can also be extended into

these areas, for this reason in our modern era the term “Cyberterrorism” is applicable in cases like the SPE’s cyber-attack, where a non-combatant party is attacked and the civil rights of the people are violated. Then, we can understand the term as “Cyberterrorism means premeditated, politically motivated attacks by sub national groups, clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets” [2], clearly we see that this term applies to our study case on SPE hack.

In recent years the cyberterrorism has been of a major concern for the nations, organizations and individuals in general because it represents a serious threat to the privacy, security, economics and freedom of the information, since precisely this information is available online and is always connected to the internet, being exposed to attacks on this network from any part of the world, but not only the vulnerability or disclose of private information could be considered an act of cyberterrorism, also the shut down of systems, damage of virtual environments, steal of the information or destruction of sensitive data falls in this category, for this reason is that this issue has serious consequences as we see in this case study. Furthermore, the SPE hack is an example of modern cyberterrorism in the information era and serves as a clear action that indicates towards this direction. This is because the perpetrators of this attack, identified themselves as “The Guardians of Peace”, were later linked to North Korea and sanctions were applied on that time [3].

This group (GOP) utilized the cyber-attack against SPE as an instrument of political intervention that was triggered by the release of a movie produced by SPE called “The Interview”, this movie depicted satirically the North Korean supreme leader. Because of this attack, i.e. the act of cyberterrorism, a national security crisis was unleashed in the United States, transforming a cyber-attack against a private organization into a national security crisis, that as we observed before, impacted negatively into the U.S. citizens civil rights by violating their privacy and freedom, moreover, according to the definition of terrorism, a non-combatant organization (in this case SPE) suffered a shut down of their IT systems, networks, destroyed information and sensitive data pertaining the U.S citizens (in this case the SPE employees) was disclosed unauthorized. Furthermore, we can see that the SPE hack as an example of a crisis triggered by cyberterrorism, since the attackers took control of the IT systems of a private organization through the Internet connection and affected a nation as a whole, in terms of cyber security.

In this case study, we will observe the time line of the events and how them evolved gradually into the aforementioned crisis, furthermore, we will observe how the interactions between a private organization and the U.S. federal government were conducted to later install security issue between two nations: United States and North Korea, we will also cover how the accusations against North Korea initiated based on the investigations of the Federal Bureau of Investigation (FBI), how were the reactions of this attack, not only from the SPE’s employees or the United States Federal Government, but also from former employees, actors, and other international authorities. Finally, we will review how the attack could be perpetrated and the data that was stolen.

What is SPE (Sony Pictures Entertainment)?

To understand SPE we need to first take a look over its parent company, Sony Corporation (Sony), which is a multinational conglomerate based in Tokyo, Japan and having its U.S. headquarters in

New York city. According to the webpage its mission is: *"at Sony, our mission is to be a company that inspires and fulfills your curiosity"* [5]. In terms of entertainment, Sony is considered as one of the biggest companies in the world with six big categories of business: Electronics and Mobile, Film and Television, Music, Games, Digital Services, and Other Businesses. SPE, which is included in the Film and Television sector, is responsible for motion picture production, television production, television networks [6]. In the case of SPE, this company was founded in 1987 and was launched as the purchase of the company Columbia Pictures by the Coca-Cola company in the late 80s, since then, Sony Pictures Entertainment was dedicated to the film and television industry production and distribution of motion pictures materials, having in their portfolio important business-success films like: Men in Black, Spider-Man, Stuart Little, Black Hawk Down, Mr. Deeds or The Da Vinci Code. Additionally, in the television business, SPE is responsible of classics series such as: Seinfield, The Dr. Oz Show and Breaking Bad [7].

SPE produces great amount of material for TV and Movies, and the film that unleashed the cyber attack against them and later the national security crisis was a film called "The Interview". This movie was released by SPE in the year 2014, which was a satire comedy film directed by the also actor Seth Rogen and Evan Goldberg. In this film James Franco and Seth Rogen, the main characters of the movie, impersonate two journalists that run a sensationalist show on TV, in some point they try to make their show bigger and in this sense they manage to get an interview with the supreme leader of North Korea that will take place in Pyongyang. When the CIA learns about this interview they recruit them for a top secret mission operated by the agency to assassinate the supreme leader. During their visit in Pyongyang they depicted the city and people in a satiric way overacting the limitations of the people and the country. The film content was not taken well by the North Koreans, triggering the aforementioned crisis between the two countries.

Timeline of the Cyber Attack on Sony Pictures Entertainment **[8] [9] [10] [11] [12] [13]**

Day-1: November 24, 2014 (Monday)

An ordinary week day begins at the Sony Pictures Entertainment's headquarter at Culver City, California. Everything was quite normal until the point when all the computers in the Los Angeles office started flashing a red graphic skull with long skeleton fingers, accompanying an intimidating massage that says "**This is just the beginning**", "**We've obtained all your internal data including your secrets and top secrets**" and ask to "**obey**" the demands they have and threats to release the data otherwise. Within around 10.50 in the morning, the news reaches to the media and it was reported instantly that, the global corporation is basically paralyzed with the digital infiltration and is in digital hibernation right now. All the computers in the California branch were turned down as a basic safeguard and proactive measures were taken immediately throughout all the branches around the world to deal with the breach.

The hacker group identified themselves as GOP (Guardians of Peace), which was visible on the flash screen and the total volume of the obtained data was roughly 100 Terabytes from Sony servers. To compare, if printed, the whole library of congress collection would require only 10 Terabytes of data space.

Day-2: November 25, 2014 (Tuesday)

The precaution continues and the digital equipment of Sony Pictures Entertainment remained shut down in their corporate branches of New York and Culver City. Although the news is flashed to the media, but the actual damage info is still remains as an inside news due to the involvement of SPE spokesperson Jean Guerin. Several estimation and theories build up among the news media and as per BBC the damage was assumed to be less intensive than the incident happened with Sony PlayStation back at 2011. Even, rumors append regarding the truth of the incident.

Day-3: November 26, 2014 (Wednesday)

It was the Thanksgiving eve and all the digital equipment remains turned off for Sony employees and they continue working without e-mails, voice mails and computers.

Day-4: November 27, 2014 (Thursday)

Repercussion starts with some of the films produces from the SPE banner goes public. Among these, '**Fury**' of Brad Pitt that was already released by that time, along with '**Annie**', '**To Write Love On Her Arms**', '**Still Alice**' and '**Mr. Turner**', which was waiting for its time to get to the theater, find its way to the public file sharing hub. Within the next one week, '**Fury**' would face illegal download issue for more than 1 million times.

Day-5: November 28, 2014 (Friday)

By this time, the first speculation arrives for North Korea to be behind the act as a reaction for the movie '**The Interview**' that showcases the lavish lifestyle and ultimately the assassination of the North Korean supreme leader **Kim Jong-un** in a comedic manner. Supporting this clause, a North Korean site refers the movie as an attempt of provocation. **Re/code**, first published report linking the attack to North Korea which was later further detailed by **NBC News**.

Day-6: November 29, 2014 (Saturday)

Still it remains a digital stampede for SPE employees without the privilege of computer, voice mail or e-mail.

Day-8: December 01, 2014 (Monday)

The salary figure (Pre-bonus) of 17 SPE higher executive along with 6000 employees and their dependent becomes public. Also, the personal information like e-mail addresses, home addresses were leaked. Many websites in the world wide web (Deadline, BBC) published the financial figures of the high officials. By this time, Sony approaches for the support from FBI cyber-security department (SealMandiant) for investigating the incident which was later on confirmed by the FBI spokesperson **Laura Emilier**.

Day-9: December 02, 2014 (Tuesday)

After 9 days of the breach, understanding the depth and gravity of the situation the SPE executive chief Michael Lynton and Amy Pascal issue statement regarding the incident throughout the company alerting about the attack- "It's apparent at present that a huge chunk of confidential Sony Pictures Entertainment data has been accessed and stolen by cyber attack from a hacker group called "GOP", including personnel, business and financial information. This is the result of a brazen cyber-attack on our company, our employees and our business partners. This theft of SPE

materials and the release of sensitive employee and other information are heinous criminal acts and we are working as closely as possible with the law enforcement (FBI)…While we are not yet sure of the full scope of information that the attackers have or might release, we unfortunately have to ask you to assume that information about you in the possession of the company might be in their possession. While we would hope that common decency might prevent disclosure, we of course cannot assume that… We can't overemphasize our appreciation to all of you for your extraordinary hard work, commitment and resolve" [Deadline; David Robb; December 22, 2014].

Day-10: December 03, 2014 (Wednesday)

GOP posts internal mail communication of SPE employees in **pastebin**, a text storage service embedded in a web application, criticizing Adam Sandler, Angelina Jolie, Jonah Hill and Barack Obama along with the passport and Visa information of the whole crew members in PDF format. The nature of the criticism was sensitive,extreme and harsh where the US president was portrayed as "Racist" and Angelina Jolie was referred to as "Spoiled Brat" which took the web like a flood and opened some true nature and beliefs of some front-runners in the entertainment business. There was also leaked information found on some fringe media sites regarding budgeterial information of several films, their contracts and credentials of the members.

A long list of 25 pages that contains the complaints of the employees goes online. As per the tech site re/code, Sony is also pursuing it's best effort to take counteroffensive measures to activate "Denial of Services" if an attempt is carried out to publish or access the stolen data online anywhere. Still by this point, SPE denies any allegations against North Korea regarding the attack. The same day, another victim was found from the same hackers as the financial information of almost 30,000 employees of the corporate leader in auditing- "Deloitte", found available in **Pastebin** also.

Day-12: December 05, 2014 (Friday)

Allegations against North Korea gets stronger as to the uncanny similarity that is found in between the codes of the SPE hack and the ones that targeted several companies and government agencies in South Korea at 2013 which was supposedly initiated by North Korea. Also, the very same day, another demand form GOP arrives which threats to hurt the company employees, their families and other subordinates if they refuse to abandon Sony. This was done by asking to sign their names in a provided mail address if they are willing to come forward with the falsification that Sony had been doing over the years.

Day-13: December 06, 2014 (Saturday)

James Franco and **Seth Rogen**, two of the main characters of the film "**The Interview**", who was also hosting the celebrity talk show- 'Saturday Night Live', become witty in their opening monologue regarding the hack incident on Sony. Franco says- "Something pretty crazy happened this week. I have this movie called *The Interview* coming out at Sony and this week Sony Studios got all their computers hacked. This is true. These hackers have leaked real personal information about everybody that works at Sony. Social security numbers, e-mails, and I know eventually they're going to start leaking out stuff about me. So before you hear it from someone else, I thought it would be better if you hear it from me. Soon you'll know that my e-mail is

CuterThanDaveFranco@AOL.com. My password is LittleJamesyCutiePie — and this is all just a real violation of my personal life" [BUSINESS INSIDER; Aly Weisman; Dec 7, 2014].

Day-15: December 08, 2014 (Monday)

The first ever response documented from North Korea regarding the incident where they allegedly denies the responsibility, though they openly praised the work and referred it as 'Righteous Deed'. Another message pops up from GOP in the Pastebin, where they ask for the immediate halt of the movie in the theaters that is causing turmoil in regional peace and friendship. They also refuses any link to the life threats of the Sony employees and their families made last Friday. Some unclear and opaque demands from GOP along with a long list of celebrity aliases were uploaded at github.

Day-17: December 11, 2014 (Thursday)

Scott Rudin, the producer to make insensitive comments on Angelina Jolie apologizes in public stating that the comment was not made in a formal manner, rather the intention was to make funny comment between friends. **Amy Pascal,** chairperson of SPE, also talks about the racially inappropriate comments made for Barack Obama in an interview with Deadline's Mike Fleming and states that it was all a momentary impulse which was not definitely meant to take seriously. MPAA (Motion Pictures Association of America) also releases their statement saying at this moment, they are not involved with the investigation or with the incident.

The premier of the movie "The Interview" takes place in Los Angeles, California, at the Ace Hotel's theater with maximum security provisioning.

Day-18: December 12, 2014 (Friday)

Media comes forward with the news regarding additional leaked documents such as medical records of the employees, medical bills attained by several employees under insurance for their dependents. Although, there was no trace of the leaked documents found online. The next day, GOP releases the seventh largest dump of SPE documents and issue a promise to bid a "**Christmas gift**" that evidently will put Sony Pictures Entertainment "**into the worst state**."

Day-20: December 14, 2014 (Sunday)

One prematured script of the next upcoming James Bond film, "Spectre" is released online which had copyright and owned by MGM and Danjaq who, after this incident, was onboard with Sony on their fight against the hackers and made public statement regarding protecting their rights against this kind of violation which caused money, privacy and fame . Eventually, it was clear that although the attack was intended against SPE, but it was spreading like a virus and affecting everyone associated with Sony. MPAA issues their second statement where they put their sympathy for Sony and their associations and also agrees to provide support to handle the situation in rigorous manner.

Sony takes steps as the company litigator, David Boies, issues for justification against publication of the leaked material online and in the media and also demands immediate removal of the possessed documents by anywhome as SPE does not consent with any kind of publication or ownership.

Day-21: December 15, 2014 (Monday)

During the monthly Town Hall meeting held at the SPE corporate headquarter, its CEO **Michael Lynton** fails to reassure the employees regarding the gravity, priority and the progress of the ongoing investigation as the employees peruse a class action law-suite against SPE on the accusation that Sony has incredibly failed to protect the confidential information of the employees which violets the basic propriety measures.

Somewhere else, **Aaron Sorkin,** a renowned writer and columnist who was also the creator of several TV series like 'The Newsroom' , motion pictures like 'The Social Network', 'Steve Jobs' publishes a column in the esteemed **The New York Times** where he allegedly calls the journalists responsible for this disaster who disclosed the leaked information in media. He accuses them to bear most of the responsibility for this entropy following that, "Hackers just hacked, but the rest of the part was done by us, the journalists" [Aaron Sorkin, The New York Times; Dec 15, 2014].

Day-22: December 16, 2014 (Tuesday)

This is the day the cyber terrorists states their named on calling directly the name of the movies confirming the theories that had been building up for the last 20 days. In direct mail communication to several media reporters, the hackers demand to immediately stop all the premiers of the movie or to face '**Doom**' referring to the mass attack that happened at 9/11, 2011. FBI further explained that the thread posses for the people not to be near any crowded movie theater and for the first time, although statement from the Homeland Security denies confirmation of any active terrorist activity. It seemed like this incident it going past the entertainment domain and rather entering to the political domain.

Both the main characters of the film, **Seth Rogan** and **James Franco** cancels there promotional activities for the film for that week. Sony provides option for the owners of theater considering the situation to pull the movie back which was first responded by **Carmike**. Several other theaters cancel the first premier shifting the venue and the date.

Whilst all this, another dump of mail correspondence between the **Lynton** and **Pascal** drops by which was named as the duly stated '**Christmas Gift**' by the hacker. Meanwhile, Sony faces a second class-action lawsuit from the former employees of Sony as to the negligence in protecting their rights.

Day-23: December 17, 2014 (Wednesday)

In response to the terrorist threat to cause havoc on the theaters and the theater-goers that premiers the film, SPE postpones the release of the film considering the safety and the security of the employees, the theater owners and above all the viewers and the audiences. **National Association of the Theater Owners** also provides to go signal in lieu of not releasing the film at Christmas day. Press screening at several major cities for Wednesday night at Cincinnati, New York, Austing is cancelled accordingly along with all the TVC regarding the release of the movies.

Another dump of mail is released which shows there was ideas roaming around for the possible merger of **Lionsgate** and **SPE**. At this point, the US government takes step for formal accusation against North Korea for the cybercrime.

Day-24: December 18, 2014 (Thursday)

White House shares press release focusing on the ongoing activities against the incident naming it as a national security issue blaming North Korea behind the job and also ensures a tempered and appropriate response. During the slot of the movie, in its previous release date, the Theater Association agrees to protest the attack by showcasing "Team America: World Police", a 2004 mockery of North Korea created by the makers of South Park, which was ultimately denied by Paramount Pictures for security reasons.

In parallel, with an interview renowned actor George Clooney reveals that, in a effort with his agent to circulate a letter supporting the cause of Sony Pictures Entertainment, none of the Hollywood's major executives agreed out of sheer fear, which left him with an awe of unfathomable surprise and insecurity for the future of this industry. Meanwhile, SPE receives the third class-action lawsuit from their former employees in the light of keeping them dark.

Day-25: December 19, 2014 (Friday)

The hackers contact SPE and assure them there will be no other damage as long as the movie is not out in the theaters as well as warns them that if it has a new release, the previous incident will continue further on. The US President Barack Obama in his annual year end press conference berates SPE for caving under threats which later on, was refused by the SPE CEO who says that Sony did not make any decisions of postponing the release. Whereas, it merely respected the decision of the theater owners who did not want to show the picture due to understandable security issues. Barrack Obama also says U.S.A does not render recognition to any dictatorship, nor it will allow any foreign interference in its freedom of speech & media and the U.S.A will respond proportionally.

Day-26: December 20, 2014 (Saturday)

In response to US president, North Korea invites U.S.A forming a joint investigation group to investigate the attack at SPE and threats to attack the U.S mainland including White House, Pentagon and others, if U.S.A refuses to do so. The U.S Government asks for the compensation from North Korea for the damages caused to SPE due to the attack which is approximately more than 100 million USD, which was later on, laughed at by the opposing party.

Day-29: December 23, 2014 (Tuesday)

Sony announces the film will be released as per the previous plan, during the Christmas Day, which was hugely acclaimed by the U.S President. As well as they announces the release of film to be available on homes on VOD and it also allowed rental options for this movie from YouTube, Google Play and also from a dedicated website operated by the studio.

International reactions to the attack on Sony Pictures Entertainment

Background: North Korea – United States relations

In order to analyze how events unfolded after the attack, especially after the United States formally accused North Korea, it is important to know the status of the relations between the two nations involved, and to know the events which led to that situation.

Since the end of the Korean War and the signing of the Korean Armistice Agreement in 1953, which ceased all hostilities, relations between the United States and North Korea have been rather hostile. Since the decease of the North Korean leader, Kim Jong-il, in late 2011, and the coming to the power of his son, Kim Jong-un, relations continued to deteriorate. They were motivated by the successive long-range missile launch tests, the development of its nuclear program and threats against the United States and its allies. In 2013, tensions escalated, motivated by the UN Security Council Resolution 2087, which condemned North Korea for the launch of their first satellite, named Kwangmyŏngsŏng-3 Unit 2, in December of 2012. The resolution was adopted unanimously, and it also imposed some travel bans and asset freezes to several North Korean officials and companies. [14]

In the same year as the cyber-attack, the United States House of Representatives voted to pass the North Korea Sanctions Enforcement Act of 2013, which increased sanctions against the Democratic People's Republic of Korea, in order to increase punishment and deterrence from the pursuit of nuclear development. The bill, however, was never passed by the US Senate. Rep. Edward R. Royce, sponsor of the bill and Chairman of the House Foreign Affairs Committee, declared: "By shutting down North Korea's illicit activities, we deprive the Kim regime of the money he needs to pay his generals and to conduct nuclear weapons research". [15] [16]

Accusations against North Korea

On December 17th 2014, American officials concluded that North Korea was "centrally involved" in the attack. They announced that the White House was debating whether to publicly accuse North Korea. The response that the United States would take against North Korea was not clear at that point, and that they were considering a range of options in weighing a potential response. While some officials argued that the North Korean government had to be confronted directly, others claimed such response would provide North Korea with their long coveted dispute, and possibly interfere in diplomatic negotiations held at that time between Japan and North Korea. [17]

The following day, White House Press Secretary Josh Earnest, confirmed that the Federal Bureau of Investigation (FBI) and the Department of Defense were investigating the hack, and that the situation was being treated as a "serious national security matter". [18]

On December 19, the FBI provided an update on the status of the investigation. Upon discovering the intrusion into their network, Sony Pictures Entertainment requested the FBI's assistance. Both the company and the federal agency had since worked closely. It also stated that Sony's quick reporting facilitated the FBI's ability to do its job and eventually identify the source of the attacks. Furthermore, the agency encouraged all companies to act quickly, like Sony Pictures did, in case they were the target of a cyber attack.

Most importantly, the FBI announced that they had enough information to conclude that the responsible of the attacks was the North Korean government, and proceeded to give part of the reasons that brought them to such conclusion (while not releasing sensitive information). After

conducting technical analyses of the data deletion malware which infected Sony Pictures' systems, the FBI found similarities to other malware which the FBI knew it had been developed by North Korean actors. The similarities were, for instance, specific lines of code, encryption algorithms and data deletion methods. Furthermore, similarities were found in terms of the infrastructure used. Several IP addresses that were known to originate from North Korean infrastructure were hard-coded into the malware used in the attack. Finally, the FBI found that the tools used in this attack were similar to those used in a cyber attack against South Korean banks and media outlets, carried out by North Korea in March of 2013. [19]

The same day, the Secretary of the US Department of Homeland security, Jeh Johnson, released a brief statement, in which he did not consider the attack as solely being against a company and its employees, but also against the freedom of expression and way of life of the US. He also commented about the importance of good cyber security practices and encouraged companies to assess their company's cyber security, as well as offering help from his Department and other agencies in the prevention against cyber attacks. [20]

Also the same day, US Secretary of State John Kerry, criticized North Korea for the attacks and the physical threats against the moviegoers, and encouraged their allies and partners to "defend the values of all our people in the face of state-sponsored intimidation". [21]

President Obama said that the US would respond to the attack, although he declined to specify what sort of actions would be taken. [22]

US officials reported that the issue had been discussed with Chinese government officials, "to share information, express our concerns about this attack and to ask for their cooperation". [22]

The next day, North Korea, to its foreign ministry, offered to hold a joint inquiry into clarifying the origin of the attack, and threatened the United States if they refused to collaborate and continued their allegations against North Korea, claiming they would face "serious consequences". [23]

In a report of December 7, the North Korean News Agency carried a statement from North Korea's National Defense Commission, in which they denied the "wild rumors" of their involvement, but strongly criticizing Sony Pictures for the production of The Interview, "a film abetting a terrorist act while hurting the dignity of the supreme leadership of the DPRK by taking advantage of the hostile policy of the US administration against the DPRK". [24] It is important to note that North Korea had previously expressed concerns to the UN for the production of the movie. [25]

On January 2, 2015, the United States installed additional economic sanctions against North Korea, under an Executive Order issued by President Obama. The sanction was imposed on 10 North Korean officials and 3 organizations, including the regime's main intelligence agency and a state-run arms dealer. The President also said that the United States was considering the inclusion of North Korea back onto their list of states that sponsor and promote terrorism. [26] [27] The North Korean regime quickly denounced the United States for imposing such sanctions. The regime's foreign minister claimed they did not have anything to do with the attacks, accusing the US of rising up hostility towards his nation, and stating that the sanctions would not undermine the country's strong military. [28]

On January 7, 2015, the FBI's director, James B. Comey, slightly clarified more details of the attacks, and defended the claim that North Korea was responsible, with "high confidence". He stated that the attackers –qualified as "sloppy"- had sent the attacks and messages directly from North Korean internet addresses, instead of routing them through decoy servers. Also, he reported that it had been found out that the hackers logged into their Facebook account and Sony's servers from North Korean addresses. The attackers seemed to realize of their mistakes and quickly proceeded to reroute their attacks through servers located abroad, Mr. Comey said. [29] [30] [31]

The next day, the National Security Agency (NSA) director, Admiral Michael Rogers agreed to the consideration that the attack had originated from North Korea. He considered the attack against Sony Pictures as a "game changer" for cybersecurity. He endorsed the US response to the attack. The NSA had partaken in the investigation, examining the malware used in the attacks and helping determine its origins. [32] In a NSA document disclosed in 2015, it appeared that the NSA had gained access to North Korean networks in 2010, and that the information gathered from such access was essential to support the accusations against North Korea. [33]

Doubts about accusations against North Korea and other investigations

Even before the official accusations by United States officials against North Korea, numerous cyber security experts and other personalities expressed their doubts and started to believe North Korea was not behind the attacks, claiming that the accusations did not have a strong base.

Researchers from cyber the security company Norse said that their own investigation of the Sony attack did not point to North Korea at all, and instead indicated that some Sony Pictures employees and hackers belonging to piracy groups were behind the cyber attack. Cyber security expert Kurt Stammberger criticized the FBI, since in his opinion, they had drawn their conclusions too quick. He said that the company was collaborating with the FBI to share their findings about the case, although he expected the agency to share more information. [34]

Cyber security expert Marc Rogers, said that he found unlikely that North Korea was behind the cyber attack, and went on to provide his own thoughts as to why he was making such a claim. He stated that he thought the perpetrator was some Sony employee (either current at the time or former), and that accusations against North Korea were only politically motivated. [35]

Former Anonymous hacker Hector Monsegur, said on a television interview, that he believed North Korea did not have an infrastructure capable of conducting such an attack. Again, his suspicions were focused on it being an inside job, meaning that employees or other individuals closely related to the company were behind the attack. [36]

Kim Zetter, award-winning cyber security reporter at Wired, said in an article that the evidence that North Korea was behind the attack was "flimsy". The article was published before the FBI announced that North Korea was "centrally involved" in the attacks. In his opinion, and based on his experience and technical details of the hack, he stated that attributing these kinds of attacks is difficult, sometimes impossible. His belief was that this attack had been conducted by hacktivists, rather heterogeneous groups of various actors who act based on their common interests. [37]

Despite many cyber security researchers concluding that the North Korean link to the attack did not exist, others found that the FBI investigation was being conducted thoroughly and in a serious manner, and came to support the official position of the US government.

Months after the attack, Kevin Mandia, president of the security firm FireEye, who had been called in to help investigate the hack, stated that the attacker was “definitely not an insider”, and that the attack had been the work of a government. In his opinion, it was highly remarkable that it was the first time a US president had publicly blamed another country for a cyber attack, and that went to indicate that the US government had strong evidence to support such a claim. Mandia also reminded the fact that the NSA had breached into North Korean networks, and that had given them part of the evidence to claim that North Korea was actually behind the hack. [38]

In 2016, security vendor Novetta, working together with Kaspersky Labs, Symantec and AlienVault, wrote an extensive report about the attack, in which it is said that the cybercrime group called “Lazarous Group” was behind the attack. The investigation, coined “Operation Blockbuster”, had as an objective to analyze malware samples from several cyber attacks in order to find potential links among them. Despite several cyber security researchers had doubted about the FBI’s accusations against North Korea and gave weight to the idea of insiders, these security companies stated in their report that the FBI’s claims were supported by their findings. [39] [40]

The Lazarous Group

The Lazarous Group is a cybercrime group to which researchers have attributed many cyber attacks over the last years. It is not clear how many people made up the group, which is reported to have perpetrated some of the most impactful cyber attacks of the last decade, aside from the Sony hack which, among others, include:

- DDos attacks against South Korean targets, starting in 2009. [41]
- Several bank cyber heists from 2015 to 2018, including that of the Bangladesh Central Bank. [42]
- The WannaCry ransomware attack of 2017. [42]
- Cyber attacks against cryptocurrency users in South Korea and elsewhere. [43]

The origins of the group are unclear, but some experts, including the group led by Novetta, have reported it has links to North Korea.

On June 8, 2018, the US department of justice officially charged a North Korean individual named Park Jin Hyok, purportedly member of the Lazarous Group, for his role in the Sony hack, the WannaCry ransomware outbreak, several bank cyber heists and more. The charges filed against him were “a violation for conspiring to commit unauthorized access to computer and obtaining information, with intent to defraud, and causing damage, and extortion related to computer intrusion, and a violation for conspiring to commit wire fraud”. [44] [45] A federal arrest warrant for this person was issued on the same day. [46]

Conclusion

The most relevant aspect of the events that unfolded after this cyber attack is, surely, the diplomatic and international involvement, that eventually led the United States to officially make

accusations against North Korea. The tension between these countries has always been at a high level, and there have been moments where the US invasion in North Korea was seen as not only a remote possibility.

It is still not well known who the perpetrators were, what their motivation was, or how much data they managed to steal. Furthermore, there are some experts that, soon after the attack was noticed, claimed it did not look like North Korea was behind. At this point we might never know exactly what happened, and if the FBI really had enough evidence to make such a claim, and to do it in such a short period of time. SPE's response was excellent, informing the law enforcement authorities right after becoming aware of the attack. This attack did not only involve a cyber attack and a theft of private and sensitive information, but physical threats against people going to the movies to watch the movie *The Interview.* Regardless of the credibility or the actual possibilities of a physical attack, it makes this case different from others. One thing to be said, however, is that the cancellation of the release of the movie was, perhaps, a mistake. The United States has always kept the same policy of not negotiating with terrorists, and has given the image of a country whose citizens are resilient to attacks, and that those do not change people's way of life. President Obama considered that the company's decision was "a mistake", and that dictatorial regimes should not be able to impose censorship in the US. [47]

Regardless of who conducted the cyber attack, whether it was North Korean state-sponsored hackers, Sony employees, a combination of both, or someone else, it is very likely that the attack was politically motivated, and that the perpetrators were trying to have some kind of international political response back. The response from the United States, launching accusations against their long-time enemy seems to be what North Korea wanted, not only to disrupt or cease diplomatic negotiations with US allies, but to possibly give North Korea some way of justifying some of its future acts in retaliation of the accusations against them. The attackers were aware that North Korea would look as the main suspect, and this could have been a reason for them (if it turns out they were not linked to that country) to conduct the attack with most eyes turned away from them.

Cyber attacks are now one more element of warfare. In this case, a cyber attack was not conducted for economic or hacktivist reasons (or at least these were not the main motivations behind it). The people behind it wanted to make the whole world see what they were capable of, and not only steal and delete an important company's information, but to attack the freedom of the country whose main motto is freedom and liberty. It is a complicated case, unlike some others in which the motivation appears to be very clear. For this reason, and since this case led to an escalation of tensions between two countries, in an attack which was considered for some an act of war, we believe that so many things can be learned from it, specially related to the political and diplomatic side of the cyber world, which might sometimes be overlooked by regular people.

All in all, it is hard to analyze who came victorious after this "battle". Most importantly, because the actors are not completely defined, and also since the goal of the attack is unclear. This, perhaps, makes this case more interesting and fun to analyze and discuss. For the same reason, this case had unprecedented media coverage and even regular citizens discussed about the matter. More interestingly, it had a very crucial international diplomacy aspect, which not only raised tensions between two enemies, but changed people's views about the North Korean regime

and its leadership –which were probably not the best anyway, especially in the United States and its allies.

References

[1] 22 U.S. Code § 2656f. Annual country reports on terrorism https://www.law.cornell.edu/uscode/text/22/2656f

[2] L. J. Janczewski and A. M. Colarik, Cyber Warfare And Cyber Terrorism, Information Science Reference, 2008.

[3] Letter -- Imposing Additional Sanctions with Respect to North Korea. 2015 [Press release] https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/letter-imposing-additional-sanctions-respect-north-korea

[4] Sony Pictures Cyber-Attack Timeline. [Accessed on 14/05/2019] https://www.bankinfosecurity.com/sony-pictures-cyber-attack-timeline-a-7710

[5] Sony Corporation website. [Accessed on 14/05/2019] http://corporate.sony.ca/html/sonyinfo/index.html

[6] Sony Pictures. [Accessed on 14/05/2019] https://en.wikipedia.org/wiki/Sony_Pictures

[7] SONY Pictures Entertainment – Hack of the Century (2016). [Accessed on 14/05/2019]. http://www.colinhautman.com/wp-content/uploads/2016/02/Arthur-Page-Submission_SONY-Hacking-case.pdf

[8] David Robb (2014). "Sony Hack: A Timeline". Available from: https://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ [Access at 14th May, 2019]

[9] Ryan J. Reilly (2018). "Feds Charge North Korean Programmer In Sony Hack Over Seth Rogen's 'The Interview'. Available from: https://www.huffpost.com/entry/north-korea-sony-hack-the-interview_n_5b914031e4b0511db3dff9c5?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABedxBbhq4id-Lg77eMbA-1o4wDY9z8IREFANY1NKRAu9lSshtmutqHEdALl57cMNP6osPmvV14sdDu22Bh7bGQc0IqoelkT3F0SbRkbHKlll2zxwu1reWuKlsfrB47HgCF0nTrTvSYiwWN3eFqnCatjT7-V1RCYO6NSmFNi6pPI [Access at 14th May, 2019]

[10] Alex Altman (2014). "Everything We Know About Sony, *The Interview* and North Korea". Available from: http://time.com/3639275/the-interview-sony-hack-north-korea/ [Access at 14th May, 2019]

[11] Wikipedia (2015). "Sony Pictures Hack". Available from: https://en.wikipedia.org/wiki/Sony_Pictures_hack [Access at 14th May, 2019]

[12] BBC News (2014). "The Interview: A guide to the cyber attack on Hollywood". Available from: https://www.bbc.com/news/entertainment-arts-30512032 [Access at 14th May, 2019]

[13] Aly Weisman (2014). “Seth Rogen Crashes James Franco's 'SNL' Monologue To Address Sony Hack”. Available from: https://www.businessinsider.com/james-franco-seth-rogen-snl-monologue-sony-hack-2014-12?r=US&IR=T [Access at 14th May, 2019]

[14] United Nations Security Council, “Resolution 2087 (2013)”. Adopted on January 22, 2013. Available online: https://undocs.org/S/RES/2087(2013)

[15] The Hill, “House passes bill to toughen North Korea sanctions”. July 28, 2014. Available online: https://thehill.com/blogs/floor-action/house/213553-house-passes-bill-to-toughen-north-korea-sanctions

[16] US Congress. H.R. 1771 – North Korea Sanctions Enforcement Act of 2014. Referred in Senate 29 July 2014. Available online: https://www.congress.gov/113/bills/hr1771/BILLS-113hr1771rfs.pdf

[17] The New York Times, “U.S. said to Find North Korea Ordered Cyber Attack on Sony”. December 17, 2014. Available online: https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0

[18] Entertainment Weekly, “White House treating Sony hack as ‘serious national security matter’”. December 18, 2014. Available online: https://ew.com/article/2014/12/18/white-house-sony-interview-north-korea/?#

[19] Federal Bureau of Investigation, “Update on Sony’s Investigation”. December 19, 2014. Available online: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

[20] US Department of Homeland Security, “Statement By Secretary Johnson On Cyber Attack On Sony Pictures Entertainment”. December 19, 2014. Available online: https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment

[21] Reuters, “Kerry condemns North Korea for Sony cyber attack”. December 19, 2014. Available online: https://www.reuters.com/article/us-sony-cybersecurity-kerry/kerry-condemns-north-korea-for-sony-cyber-attack-idUSKBN0JX2AC20141219

[22] Los Angeles Times, “North Korea decries U.S. allegations on Sony hack; U.S. turns to China”. December 20, 2014. Available online: https://www.latimes.com/world/asia/la-fg-north-korea-proposes-joint-investigation-into-sony-hack-20141220-story.html

[23] BBC, “North Korea proposes joint Sony hack inquiry with US”. December 20, 2014. Available online: https://www.bbc.com/news/world-us-canada-30560712

[24] North Korea Tech, “Pyongyang breaks silence on Sony hack”. December 8, 2014. Available online: https://www.northkoreatech.org/2014/12/08/pyongyang-breaks-silence-on-sony-hack/

[25] North Korea Tech, “DPRK takes “The Interview” movie complaint to the UN”. July 10, 2014. Available online: https://www.northkoreatech.org/2014/07/10/dprk-takes-the-interview-movie-complaint-to-the-un/

[26] The Guardian, “Obama imposes new sanctions against North Korea in response to Sony hack”. January 2, 2015. Available online: https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview

[27] Time, “U.S. Sanctions North Korea Over Sony Hack”. January 2, 2015. Available online: http://time.com/3652479/sony-hack-north-korea-the-interview-obama-sanctions/

[28] The Guardian, “North Korea responds with fury to US sanctions over Sony Pictures hack”. January 5, 2015. Available online: https://www.theguardian.com/world/2015/jan/04/north-korea-fury-us-sanctions-sony

[29] The New York Times, “F.B.I Says Little Doubt North Korea Hit Sony”. January 7, 2015. Available online: https://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html

[30] The Verge, “FBI Director Comey reveals new details on the Sony hack”. January 7, 2015. Available online: https://www.theverge.com/2015/1/7/7507981/fbi-director-comey-reveals-new-details-on-the-sony-hack

[31] CNBC, “FBI details North Korean attack on Sony”. January 8, 2015. Available online: https://www.cnbc.com/2015/01/08/fbi-details-north-korean-attack-on-sony.html#.

[32] Time, “NSA Director on Sony Hack: The Entire World is Watching”. January 9, 2015. Available online: http://time.com/3660757/nsa-michael-rogers-sony-hack/

[33] The New York Times, “N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say”. January 18, 2015. Available online: https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

[34] Politico, “U.S.: No alternate leads in Sony hack”. December 29, 2014. Available online: https://www.politico.com/story/2014/12/fbi-briefed-on-alternate-sony-hack-theory-113866

[35] Marc Rogers, “Why the Sony hack is unlikely to be the work of North Korea”. December 18, 2014. Available online: http://marcrogers.org/2014/12/18/why-the-sony-hack-is-unlikely-to-be-the-work-of-north-korea/

[36] CBS News, “Ex-Anonymous hacker questions North Korea’s role in Sony hack”. December 18, 2014. Available online: https://www.cbsnews.com/news/sony-hack-former-anonymous-hacker-not-convinced-north-korea-is-responsible/

[37] Kim Zetter, “The evidence that North Korea hacked Sony is flimsy”. Published on Wire, December 17, 2014. Available online: https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/

[38] Vox, “Sony Hack Was Not an Inside Job, Says Security Expert Kevin Mandia”. April 21, 2015. Available online: https://www.vox.com/2015/4/21/11561700/sony-hack-was-not-an-inside-job-says-security-expert-kevin-mandia

[39] iTnews, “North Korea linked to Sony hack attack: researchers”. February 25, 2015. Available online: https://www.itnews.com.au/news/north-korea-linked-to-sony-hack-attack-researchers-415603

[40] Novetta, “Operation Blockbuster: Unravelling the Long Thread of the Sony Attack”. February 2015. Available online: http://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

[41] Kim Zetter, “The Sony hackers were causing mayhem years before they hit the company”. Published on Wire, February 24, 2016. Available online: https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/

[42] ZDNet, “How US authorities tracked down the North Korean hacker behind WannaCry”. September 6, 2018. Available online: https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/

[43] Coindesk, “North Korean Hacking Group Lazarous Stole $571 million in Cryptos: Report”. October 19, 2018. Available online: https://www.coindesk.com/north-korean-hacking-group-lazarus-stole-571-million-in-cryptos-report

[44] SearchSecurity, “Lazarous Group hacker charged in WannaCry, Sony attacks”. September 8, 2018. Available online: https://searchsecurity.techtarget.com/news/252448325/Lazarus-Group-hacker-charged-in-Wannacry-Sony-attacks

[45] United States of America v. Park Jin Hyok, filed on June 8, 2018. Available online: https://www.justice.gov/opa/press-release/file/1092091/download

[46] Most Wanted, FBI, “Park Jin Hyok”. June 8, 2018. Available online: https://www.fbi.gov/wanted/cyber/park-jin-hyok/download.pdf

[47] The Guardian, December 20, 2014. “Sony pulling The Interview was ‘a mistake’ says Obama”. Available online: https://www.theguardian.com/us-news/2014/dec/19/obama-sony-the-interview-mistake-north-korea