The 49th Annual IEEE International Carnahan Conference on Security Technology

Comparative Analysis of Governmental Countermeasures to Cyber attacks

Lee Heon Soo (*Author*)
Policy dept.
The Attached Institute of ETRI
Daejeon, KOREA
lhs@ensec.re.kr

Abstract— Sony in United States and KHNP in South Korea were hit by a series of cyberattacks late in 2014 that were blamed on North Korea.

U.S. president Obama responded strongly and positively as control tower, and led Sony do not surrender to hacker's demand. U.S government demonstrated retaliatory action against North Korea under the proportional principle, blacklisted 3 North Korean entities and 10 officials. That days, there was the outrage of internet of North Korea. In order to enhance the cyber security response capability, U.S created a new office, CTIIC and encouraged the development of ISAOs, and made Sanctions EO, Information Sharing EO etc.

KHNP and the Ministry of Industry rectified incidents itself early period when cyber incident arose, and the situation did not recovered as quickly as desired. S. Korea had not retaliation actions, otherwise called for closer global cooperation against cyber-attacks. To enhance national cyber security and resilience, S. Korea government created the new post of presidential secretary for cyber security and draw up 'Strengthening National Cyber Security Posture' initiative.

Keywords— Governmental Countermeasures; Cyber-attacks; South Korea; United States; North Korea; Comparative Analysis

I. INTRODUCTION

As internet and cyberspace are evolving rapidly, cyber threats and hacking incidents arise more frequent and become cross-border disputes in many cases.

In late 2014 the U.S. Sony and Korea Hydro & Nuclear Power(KHNP) suffered a series of cyber-attacks from attackers suspected to North Korea. Sony hack attacker's demand included not to show the film 'The Interview', otherwise KHNP hack attacker's demand included the shut-down of three nuclear plant. In many ways, the cyber-attack to KHNP Dec. 2015 in S. Korea bears hallmarks of the attack on Sony Pictures Nov. 2105.

When a large scale cyber incident arise, or when a major national values or national infrastructure is being breached, government are to take cyber countermeasures for national cyber security. Governments need to take appropriate countermeasures through investigation, attribution, blocking, resilience, and punishment of cyber-attack or incidents. And, Governments need to identify the characteristics of circumstance and damage well, and if necessary, to seek the prevention of future incidents through proper legal and institutional improvements.

In this paper, U.S. Sony and KHNP hacking cases would be analyzed by focusing on the process and results of the national countermeasures. Also, this paper would seek ways and suggestions for improving and enhancing national capabilities to respond to future hacking incidents better.

II. KHNP HACK IN S.KOREA

A. Overview

The suspect has threatened to publicize more data held by the Korea Hydro & Nuclear Power Co.(KHNP) on the Internet if the government does not close down three of Korea's 23 reactors by Dec. 25. The two investigative agencies, i.e. the prosecution and police have been put on emergency alert.

It appears the hackers first tried to hamper nuclear power plant operations by attacking e-mail messages of KHNP employees and attempting to destroy the computer hard disks. The officials noted that when that failed, the hackers went on to reveal the stolen information in order to cause social chaos.

B. The E-mail Attack(2014.12.9.~12.12.)

The malware used in the attack was spread in a wave of 5,986 phishing attacks, sent in phishing e-mails to 3,571 KHNP employees. And the first release of data included personal information on 10,799 KHNP employees. Eight personal computers of KHNP employees were infected through e-mail attacks last year, and in five cases, the hard disks were initialized. But there has been no damage to plant operations or nuclear safety, said investigators. The hackers also said they still have 100,000 documents and they had transmitted 16,250 viruses.[1]

C. The stolen Data and threatening to destroying facilities(2014.12.15.~2015.3.12.)

The hacker first disclosed personal information of employees of the state-run KHNP in blog postings on Dec. 15. The cybercriminal later posted internal information on the nuclear reactors such as floor maps on Dec. 18 and 19 on Twitter, demanding the shutdown of Gori reactor units 1 and 3 and Wolseong reactor unit 3 for three months from Dec.25. In the post on Dec.21. the hacker revealed the designs and manuals of Gori reactor unit 2 and Wolseong reactor unit 1, taken from the KHNP.

March.12. 2015, the hacker renewed its threats by posting more files on Twitter that included documents concerning the country's indigenous advanced power reactor, while demanding money in exchange for not handing over sensitive information to third countries. This was the sixth posting of information since December 15 of last year.[2]

D. Attribution : incidents caused by an (unidentified) group of North Korean hackers

North Korea is believed to be linked to a series of recent leaks of data on South Korea's nuclear power plants, investigators said Mar.17. 2015.

Announcing the interim results of its probe into the high-profile case, a special investigation team said the series of incidents "is believed to have been caused by an (unidentified) group of North Korean hackers who aimed at causing social unrest and agitating the people."

Investigators said that nine digits out of one of the 12-digit internet addresses used by the perpetrators matched a previous attack by North Korean malicious code called "Kimsuky." They also said that many of the internet addresses the hackers used to steal data, attack e-mail accounts and post threatening messages were found to have passed through a company in Shenyang, China, the same firm used in the past for the cyber-attack against the South by agents from the North's Reconnaissance General Bureau.[3]

North Korea, which has a track record of waging 3.20 cyberattacks on major financial institutions, 6.25 cyberattacks on government websites and media organizations in the South, has denied any involvement in the cases.

E. KHNP' reaction to attack

KHNP was slow to respond to the leak, and when it did respond it was mostly concerned with covering up the scandal. KHNP downplayed the significance of the documents that the group had already leaked.[4]

KHNP and the Ministry of Trade, Industry and Energy, the government ministry charged with overseeing KHNP had an emergency meeting to check in the Dec.18. night and ordered public energy institutions to strengthen cyber alert. The next day, The Ministry of Industry configured the emergency squad.

Korea Hydro and Nuclear Power Co Ltd(KHNP) conducted large-scale drills at four nuclear power plant complexes on 12.22.~23. The National Security Council at Cheong Wa Dae held an emergency meeting on cyberterrorism, Dec.25. pm., in a gesture that the office was taking the recent threats seriously.

III. SONY HACK IN U.S.

A. Overview

In 2015 late November, Sony Pictures Entertainment (SPE) confirmed that it was the victim of a cyber-attack that destroyed systems and stole large quantities of personal and commercial data. A group calling itself the "Guardians of Peace" claimed responsibility for the attack and subsequently issued threats against SPE, its employees, and theaters that distribute its movies.

B. Data and computer breach

Computers have been downed and email have been frozen, Movies have been leaked, and internal documents have exposed private company memos, along with employees' salaries, Social Security numbers and health information.

In Sony's case, it looks like more than 100 terabytes of data were stolen. That's equivalent to about 50,000 full-length HD movies. Hackers have exposed the Social Security numbers of Conan O'Brien, Sylvester Stallone, Rebel Wilson and 47,423 other people as part of the massive Sony Pictures breach.

For 15,231 Sony Pictures employees and contractors, there's enough information made public to open bank accounts, credit cards and claim tax refunds in their names. Movie scripts, entire films and internal memos was also being shared online.

C. Vulnerability of Sony

Sony broke a basic rule about sensitive data, that is Keep it in one place, and protect it. The vast majority of the files weren't even password-protected. In fact, Sony broke a lot of common sense rules. Workers also kept password lists, which gives hackers access to even more data going forward.

Sony should have known better. The 2011 hack of Sony's PlayStation Network devastated the company and cost it more than $170 million. One interview with someone purportedly from GOP said they had been stealing data from Sony for a year.

D. Attribution

As a result of FBI investigation, and in close collaboration with other U.S. government departments and agencies, the FBI had enough information to conclude that the North Korean government was responsible for these actions.

North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves. FBI had seen that this cyber threats pose one of the gravest national security dangers to the United States.

FBI conclusion is based, in part, on the following.[5]:

- Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed.

- The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea.
- Separately, the tools used in the SPE attack have similarities to a cyber-attack in March of year 2013 against South Korean banks and media outlets, which was carried out by North Korea.

But many security researchers have found that evidence to be thin and unconvincing.[6]

- Security expert Bruce Schneier called the evidence "circumstantial at best" and considered a number of other possible explanations.
- CloudFlare principal researcher and DefCon official Marc Rogers wrote that the FBI's indicators seem to rely on malware that is widely available for purchase and IP addresses easily hijacked by any bad guy.

The company Norse narrowed the list of suspects to a group of six people, including at least one Sony veteran with the necessary technical background to carry out the attack, said Kurt Stammberger, senior vice president at Norse.

But the doubters leave open the possibility that the government has other intelligence supporting the idea that it's North Korea that they don't have access to, and a U.S. official told POLITICO it is likely the U.S. has access to information it is choosing to not release

The evidence gathered by the "early warning radar" of software painstakingly hidden to monitor North Korea's activities proved critical in persuading President Obama to accuse the government of Kim Jong-un of ordering the Sony attack.[7]

E. Sony's Reaction to Hack

1) quick reporting

After discovering the intrusion into its network, SPE requested the FBI's assistance. Since then, the FBI has been working closely with the company throughout the investigation. Sony's quick reporting facilitated the investigators' ability to do their jobs, and ultimately to identify the source of these attacks.

It's so devastating that the FBI warned other companies about the malicious software that infected Sony's computers.

2) Sony cancels release

The GOP threatened on Dec.16 to attack screenings of The Interview. Since the threats were made public, all major US theater chains declined to show the film. Sony therefore canceled The Interview's theatrical release and confirmed there were no plans to release it at all.

3) Sony backpedals

President Obama said on Dec.19 that Sony made mistake of cancelling its plans to release "The Interview". After that, Sony eventually backpedaled on releasing The Interview.

A group of indie theaters showed it on Christmas Day. The studio released it digitally as well on platforms including YouTube, Google Play, Microsoft's Xbox Video, and Sony's own dedicated website. The film eventually went to Netflix as well. As of January 18, The Interview had grossed more $40 million in cable, satellite, telecom, and online VOD sales, and $6 million through its limited theatrical release.

IV. COUNTERMEASURES OF GOVERNMENT

A. S. Korea Government in KHNP hack

1) President Park orders to step up cyber security

South Korea's President Park told officials to step up the country's cyber security following leaks of nuclear power plant data.[8] Her order came as the hackers posted more data online on Dec.23. President Park has reiterated the importance of enhancing the nation's cybersecurity capabilities, stressing that the security situation on the peninsula has become unpredictable.

2) The new post of presidential secretary

President Park and her Cabinet approved a proposal to launch a team under Cheong Wa Dae(the executive office and official residence of the President of the Republic of Korea)'s National Security Office to counter North Korean cyberattacks on Mar.31, 2015.

The new post of presidential secretary for cyber security is designed to strengthen the country's control tower over cyber security. Park's new security team is expected to build a new response system by recruiting top experts on cyberterrorism.

3) 'Strengthening National Cyber Security Posture' initiative

In the wake of hacking incidents of KHNP, to secure cyberspace more than now the S. Korea government draw up 'Strengthening National Cyber Security Posture' initiative.

In order to carry out this initiative, the government agreed to enhance the overall capabilities of cyber security control tower, that is the national cyber security center in Cheong Wa Dae, on Mar.17, 2015.[9]

4) Initiate proactive operations in cyber warfare

In the wake of growing security threats online, South Korea has decided to drop its long-held defensive tactics in cyber warfare and instead initiate proactive operations. To better guard against enemies' online infiltrations, it is pushing to establish a new team in charge of cyber operations under the Joint Chiefs of Staff (JCS) while increasing its personnel from the current 600 to 1,000.[10]

5) Global cooperation against cyber-attacks

Foreign Minister called for closer global cooperation against cyber-attacks, citing the hacking of Sony Pictures and South Korea's nuclear power plant operator by North Korea. Minister Yun said on Apr.2015, the two cases vividly showed the gravity of the cyber threat, so we should set up prompt and timely judicial cooperation and information sharing between countries, while delivering a keynote speech at the Global

Conference on Cyberspace underway in the Hague, the Netherlands.

B. U.S. Government in Sony hack

1) U.S. and President Obama's reaction

US officially confirmed on 19 December that North Korea was behind the hack. The White House press secretary said the US plans to take action and that the action would be "proportional" to the crime. Obama had said his staff was weighing all the options and he would choose what he feels was appropriate.

2) Outrage of North Korea

Dec.22's Web blackout lasted more than 9 hours. Web disruption came amid escalating war of words between the U.S., North Korea

The timing of North Korea's latest internet issues made them significant. They come days after the U.S. government blamed Pyongyang for being behind the hacking of Sony Pictures over that company's production of "The Interview" as well as threats against anyone who dared watch the movie.

The reason exactly why the outrage of Internet of North Korea was not confirmed. North Korea did not mention much about this incident. Also, the US government would not even confirm of deny (NCND).

3) U.S. slaps new sanctions on N. Korea in response to Sony hack

Early January 2015, the U.S. announced retaliatory sanctions in response to the North's alleged cyber-attack on Sony Pictures, blacklisting 3 North Korean entities and 10 officials, including the Reconnaissance General Bureau, Pyongyang's top spy agency.[11]

The U.S. sanctions on North Korea are "pretty light and symbolic at best," a former CIA director has said, calling for tougher restrictions to make life harder for leaders of the communist regime.

4) Sanctions Excutive Order(EO)

It's focused on attacks by people or organizations, which directly are responsible for or benefit from a cyber-attack against the nation's critical infrastructure, a wide scale disruption of computer networks, the theft of trade secrets, or aiding or embedding those stolen goods or as part of the other two attack vectors.

The sanctions, which would name the targets, seize their U.S. funds and ban them from the American financial system, would also apply to "a corporation that knowingly profits from stolen trade secrets," the White House said on April 1, 2015. [12]

5) Promoting Private Sector Cybersecurity Information Sharing EO

Private companies, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

The Secretary of Homeland Security shall strongly encourage the development and formation of Information Sharing and Analysis Organizations(ISAOs), said Obama, Feb.13, 2015.[13]

6) Relisting North Korea as a state sponsor of terrorism

The U.S. House of Representatives passed the defense budget bill for next year, on May, 2105 after attaching a clause that brands North Korea as a terrorism sponsor.

U.S. Congress saw a bill May 2015 calling for relisting North Korea as a state sponsor of terrorism and levying further sanctions as tension rises.

7) Cyber Threat Intelligence Integration Center

The White House had said Feb. 2015, it was creating a new office to sort through intelligence data about cyber threats, reflecting the government's latest attempt to buttress defenses against the rising threat of sophisticated hackers.

The Cyber Threat Intelligence Integration Center(CTIIC) have the job of analyzing and integrating intelligence from various agencies such as the CIA and NSA, and distributing information more broadly to other federal agencies.[14]

C. Calling for a joint probe of N. Korea

The N. Korea's unidentified Foreign Ministry spokesperson denied responsibility for the cyberattack, calling for a joint probe with S. Korea, into KHNP hack, and the U.S. into Sony hack incident.

The spokesperson said. "Anyone, if he or she wants to level criminal charges against a sovereign state, he or she should put forward clear evidence. We have means to establish our innocence. " The N. Korea applauded Sony hack attack as "a righteous deed of the supporters and sympathizers with the N. Korea", on Dec. 7. 2104.[15]

V. Comparative Analysis

A. Similarities of circumstance and responsive actions between two countries

In many ways, the cyber-attack to KHNP Dec. 2015 in S. Korea bears hallmarks of the attack on Sony Pictures Nov. 2105. The hackers demanded an unspecified amount of money, claimed to be part of an activist group, and are threatening the release of more data if their demands are not met.

Security experts have come to agree that the hacking method that extracted staff information and secret information of KHNP is the same as that of Advanced Persistent Threat(APT) used when Sony Pictures Entertainment was hacked.

Sony hack attacker's demand included not to show the film 'The Interview', otherwise KHNP hack attacker's demand included the shut-down of three nuclear plant.

Hacker's request was somewhat satisfied. That is, the movie 'interview' was not screened on regular theater in U.S, and in

S.Korea, some national, social anxiety was spread, as hackers desired.

There were several institution building and legislation development for national cyber defend system against hacking in both countries, but the details are different.

B. Difference

1) Control tower of managing North Korea's provocative threat.

Despite Sony hack is the case of attack to private companies, U.S. president Obama responded strongly and positively, opened the press conference, rebuked Sony' cancel of release due to attacker's threatening.

KHNP hack in Korea is the case of national critical infrastructure, but KHNP rectify incidents itself early period. Ongoing disclosure of the hacker eventually made the Ministry of Industry the center of managing incidents lately.

2) Victims action in the early days

Sony's quick reporting facilitated the investigators' ability to do their jobs, and ultimately to identify the source of these attacks. But KHNP was slow to respond to the leak, and when it did respond it was mostly concerned with covering up the scandal.

3) Diversity in Attribution

In U.S. Many security researchers have found that evidence to be thin and unconvincing, and considered a number of other possible explanations. But some doubters leave open the possibility that the government has other intelligence supporting the idea that it's North Korea that they don't have access to.

In S. Korea, Many security researchers considered that the North Korean government was responsible allowedly for attack actions. A small portion of people thought that guess could be wrong.

4) Retaliation actions and attacks on North Korea

The United States had a thorough and varied retaliation actions and attacks on North Korea alleged Sony hacking.

The U.S. announced retaliatory sanctions in response to the North's alleged cyber-attack on Sony Pictures, blacklisting 3 North Korean entities and 10 officials, and made Sanctions EO which would name the targets, seize their U.S. funds and ban them from the American financial system.

Outrage of North Korea lasted more than 9 hours. The US government would not even confirm of deny (NCND).

S. Korea had not retaliation actions, otherwise called for closer global cooperation against cyber-attacks, citing the hacking of South Korea's nuclear power plant operator by North Korea.

5) Institution building and legislation development

The White House created a new office to sort through intelligence data about cyber threats, CTIIC that is The Cyber Threat Intelligence Integration Center, and DHS is encouraging the development and formation of Information Sharing and Analysis Organizations(ISAOs). The White House announced several EO, that is Retaliatory Sanctions on North Korea, Sanctions EO, Information Sharing EO.

S. Korea created the new post of presidential secretary for cyber security, which is designed to strengthen the country's control tower over cyber security. S. Korea government draw up 'Strengthening National Cyber Security Posture' initiative, which comprise of strengthening cybersecurity capabilities of the pan-government, expansion of organization and human resources for cyber-response operations, international cooperation, cyber security-related statute promotion.

VI. CONCLUSION

United States and South Korea were hit by a series of cyberattacks in Nov., in Dec., 2014, that were blamed on North Korea. It appears the hackers first tried to hamper target organization operations by attacking e-mail messages of employees and attempting to destroy the computer system. Next, the hackers went on to reveal the stolen information sources in order to achieve their requirements.

Two governments took respectively countermeasures such as investigation, attribution, blocking, resilience, and punishment. There were similarities in institution building and legislation development for national cyber defend system against hacking in both countries, but the details are different. There were differences in the control tower's actions coping with the attacker's threat, the attribution, and the retaliation attacks on the attackers, North Korea, etc.

It was once again confirmed the importance of the role of the control tower, in responding effectively in a large national cyber incident. U.S. president Obama responded strongly and positively as control tower, and led Sony the victim, FBI the investigator both well, and S. Korea created the new post of presidential secretary for cyber security, which is designed to strengthen the country's control tower over cyber security.

Throughout the incident it became more sense of the importance of information sharing. In U.S., the White House announced Information Sharing EO, and DHS is encouraging the development and formation of Information Sharing and Analysis Organizations(ISAOs).

Through quick and accurate investigation and attribution of hacking incidents, the retaliatory measures is required to stave off the spread of hacking and warn of similar future accidents. And international cooperation is thought effective in the remedy and prevention of grand hack incidents. U.S government announced retaliatory action against North Korea under the proportional principle, and several days later there was the outrage of internet of North Korea. S. Korea called for closer global cooperation against cyber-attacks, citing the hacking of South Korea's nuclear power plant operator by North Korea.

In order to respond effectively to cyber incidents it requires comprehensive efforts at the national level based on a well-appointed cybersecurity legislation and institutional building.

U.S created a new office, CTIIC and encouraged the development of ISAOs, and made Sanctions EO, Information Sharing EO etc. S. Korea government created the new post of presidential secretary for cyber security and draw up 'Strengthening National Cyber Security Posture' initiative.

The government need to sometimes support and sometimes force the institutions to reduce the vulnerabilities. In order not to be the victim of cyber-attacks, individual institutions is recommended to lower vulnerabilities as much as possible. There are several alternatives to lower vulnerabilities such as, thorough management of e-mail ID and password, the widespread use of two-factor authentication, blocking unwanted Internet connections, encrypting the server, strengthening information security management and supervision of the major supplier cooperator, increasing investment on security systems and education of cybersecurity expert.

REFERENCES

[1] Kim Yon-se, Korea seeks U.S. help in reactor hacking probe, koreaherald, Dec.22, 2014

[2] Sean Gallagher, South Korea claims North hacked nuclear data, arstechnica, Mar.18, 2015

[3] Gov't Probe Team, Interim probe results of KHNP Hacking Incident, Press release, Mar.17, 2015

[4] Nuke plant internal documents leaked in presumed hacking attack, hani, Dec.22, 2014

[5] FBI National Press Office, Update on Sony Investigation, Washington, D.C. Dec. 19, 2014

[6] Tal Kopan, U.S.: No alternate leads in Sony hack, POLITICO Pro, Dec. 29, 2014

[7] David E. Sanger and Martin Fackler, N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say, nytimes, Jan. 18, 2015

[8] South Korea's Park Geun-hye orders cyber security boost, Asia BBC, Dec.23, 2014

[9] Korean Government, Significantly strengthens'National cyber security posture competence', Press release, Mar.17. 2015.

[10] Yonhap, N. Korea boosts cyber operations capabilities, May.10, 2015

[11] The White House, Executive Order - Imposing Additional Sanctions with Respect to North Korea , Jan. 02, 2015

[12] The White House, Executive Order - "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", Apr. 01, 2015

[13] The White House, Executive Order - Promoting Private Sector Cybersecurity Information Sharing, Feb. 13, 2015

[14] Damian Paletta and Danny Yadron, White House to Create New Division to Streamline Cyberthreat Intelligence, wsj, Feb. 10, 2015

[15] Choe Sang-Hun, North Korea Denies Role in Sony Pictures Hacking, The Newyork Times, Dec. 7, 2014