The SolarWinds Attack and Its Lessons

https://www.e-ir.info/2021/06/17/the-solarwinds-attack-and-its-lessons/

CHI TRAN, JUN 17 2021

In the late 2020 and early 2021, while strained by the Covid-19 pandemic and preparing for the transfer of power following the presidential election, the United States admitted that it suffered the biggest cyber-attack ever in terms of sophistication and extent of impact. The attack was conducted through SolarWinds, a large and reputable US cybersecurity company headquartered in Texas.[1] SolarWinds network and security products, as of the time of the attack, were used by more than 300,000 major customers worldwide, including various Fortune 500 companies, major telecom companies, military and government organizations such as the Pentagon, the United States Aeronautics and Space Administration (NASA), National Security Agency (NSA), State Department, Justice Department, and even the Executive Office of the President.[2] SolarWinds has made a statement that up to 18,000 out of more than 300,000 of their customers were infected with malicious code.[3] The attack was carried out in a very methodical manner with the participation of more than 1000 professional engineers believed to be sponsored by Russia.[4] Aiming at a very normal activity of service users, which is software updates, hackers began to try to insert malicious code into the SolarWinds Orion Platform software update from the end of 2019.[5] However, it was not until February 2020 that the intrusion and distribution of malicious code began to be carried out. The attack was completely undetected until December 13, 2020, by FireEye – a direct victim of the cyberattack.[6]

According to Deputy National Security Advisor for Cyber and Emerging Technology, Anne Neuberger, as of February 17, 2021, at least nine federal agencies and more than one-thousand private companies have been affected by the attack.[7] Although believed to have originated and backed by another country-Russia, hackers launched attacks from within the United States. The serious large-scale attack on SolarWinds has signaled the possibility of cyber warfare becoming more present and fierce than ever. Given the severity of a large-scale attack, concentrating resources on security agenda enhancement measures should be a top priority in the security agenda. Therefore, by analyzing the nature and characteristics of large-scale cyber-attacks like SolarWinds hack, this proposal will recommend possible precautions to prevent similar attacks from occurring as much as possible in the future. In addition, one of the factors contributing to the massive damage of an attack lies in the delay in detecting the behavior of this hacker group. That is, it took more than half a year since the SolarWinds attack was launched until it was discovered. Former Chief Information Officer Theresa Payton described the SolarWinds attack by comparing the hack with the situation of discovering somebody was in the house six months ago. He states "The forensic evidence get damage and destroyed."[8] This delay has created a chance for the group of hackers to erase their tracks and hide their own selves, making various obstacles to investigating identity, motives, and the intelligence stolen in the intrusion. The timely response of victims, including individuals, companies, and corporations, most importantly government headquarters has become one of the most important factors in minimizing damage caused by attacks. Therefore, besides protecting these agencies from attacks, the second central aspect of this paper is to minimize damage as well as maximum fixing of the system when these large-scale attacks occur.

The Nature of Cyber Security and Cyber Threats

Myriam Dunn Cavelty, a senior lecturer from the Center of Security Studies, has defined "Cyber Security" by referring it to what she called cyberspace or the "bioelectronic environment."[9] That is a universal network ecosystem created virtually and immaterially. It exists everywhere having computers, servers, telephone wires, or electromagnetic waves.[10] Cyber Security, simply, is to make this bioelectronic environment safe by establishing sets of both technical and non-technical activities to protect the system itself along with the information it possesses from being attacked, damaged, stolen, and other potential threats.[11] Similar to the physical world, threats in this bioelectronic environment might occur accidentally or intently with different levels of seriousness. Moreover, due to the closed linkage between these two environments, or in other words, the strong dependence of humanity on technology, damages occurring in cyberspace could lead to real breakages in the physical world. Cyberattacks, thus, might be considered as tools for cyber warriors and criminals to cause great damage on various dimensions of security. The diversity in methods, motives, and goals of these warriors means cyber-security falls under not only the national security category but also the individual and international level. More than 160 million personal credit card information stolen in a cyber-attack by five Russian and Ukrainian hackers in 2013 is an example of attacks targeting individuals.[12] National and international agencies are no exception as they were also victims and the SolarWinds is a prime example of the vulnerability of these agencies when facing large-scale cyber-attacks.

Similar to threats in the physical world, cyber threats also become more preventable if the identity, goals, motives, and mechanism of execution of these cyber warriors and criminals can be determined. Determining the attack lies in which type, cyber-crime, cyber warfare, cyber terrorism, or cyber espionage, are the first steps to addressing the crisis that these attacks cause.[13] Based on this information, the necessary steps include determining the extent of damage, then punishment and deterrence measures for the attackers to prevent similar events from occurring in the future. However, identifying the origins of these attacks is never an easy task, even with the help of computer and internet experts.[14] Fortunately, hard does not mean impossible. Two of the most effective determinations is based on the scale of the damage and the attack targets of these hackers. First, the size and sophistication of the attack are, in many ways, proportional to the resources and funding these hackers have, both professionally and financially. In fact, companies, businesses, government agencies, and even individuals using technology devices have certain perceptions of their own cyber-security, despite the level of understanding of each actor has a significant difference. Companies, large businesses, and government agencies, usually spend large amounts of their annual budget on cyber-security and protection.[15] This makes finding a security flaw in the system and attacking it completely difficult, which require a long time of research and the necessary supporting equipment. These groups of hackers, therefore, are more likely to have the financial resources and strong support to spend their time researching and planning large-scale attacks like the SolarWinds. Second, the target of attack might somehow help the government to find out the motive of warriors and criminals. Hackers might be divided into two types basing on the purpose of their actions. They might “seek to reveal, manipulate, or otherwise exploit the vulnerabilities in computer operating systems and other software.”[16] For those hackers who try to break into the system and attack its vulnerability simply for personal challenges without any political agendas is somehow easier to deal with than those having political purposes.[17] Those hackers, because their purpose is merely to show their persona professionalism, many of them do not even erase their tracks and conceal their own actions in cyberspace. Even when discovered, they are more likely to cooperate with investigative agencies and technology companies to address the security vulnerability. Big technology companies, in fact, are somewhat interested in this type of hacker and desire to have those people work for them. For example, at the end of 2019, Google also awarded prizes of up to 1.5 million dollars to any hacker who could find out how to hack the Titan M security chip on Pixel smartphones and then take control of the device.[18] On the contrary hacktivists are those who combine cyber-attacking activities with political activism. Dealing with this type of hacker often encounters significant difficulties. When it comes to political agendas, the actions of these hacker groups are often system destruction, stealing information, causing heavy damage to the economy, society, and political situation.[19] Due to the seriousness and illegal motivations of these attacks, hackers often try to hide their identity, making it harder for investigative agencies to track down the perpetrators as in the case of the SolarWinds attack. Therefore, unlike the first type of hackers, hacktivists become a major concern for cyber-security paradigm.

Based on the two identifications discussed, large-scale and high-damage attacks targeting large businesses and political institutions such as the SolarWinds hack will typically have two primary characteristics. First, they are more likely to be sponsored by governments or political organizations, or even extreme terrorist groups since cyberspace is the ideal environment for these organizations to make huge impacts on the world with the low chance of being attributed responsibilities and facing jurisdiction.[20] Second, since these attacks are usually planned carefully, whenever they happen, they will cause huge damage to the system and it is extremely hard to determine the hackers’ identities and the information controlled or lost. As a result, it is significantly important to pay attention to cyber threats, especially large-scale attacks, in the security agenda. It is not only because these threats might have huge negative impacts on all three aspects of the paradigm: individual, national and international security. But also because of the difficulty and complexity of this problem. Unlike other traditional threats, such as the military, which leaves the state with quite complete mechanisms to deal with after centuries of developing the agenda, cyber-security is new with many undiscovered threats that states have never faced before. If states and corporations do not want to be vulnerable victims of these potential threats, it is required to have a comprehensive discussion of effective measures in preventing and dealing with cyber-attacks in the modern era.

Policy Recommendations

To address problems related to cyber-security, it is necessary to have a clear clarification of the two types of policy: prevention and problem-solving. Prevention policies are implemented at a time when large-scale cyber-attacks have not yet occurred or have not been undetected in order to predict, alert, and block these attacks from happening. Examples of this type of policy might include the establishment of defenses for technology devices such as firewalls, or the establishment of intelligence agencies to detect and prevent individuals and organizations intending to attack the system. In contrast, problem solving policy will only be executed when attacks have been identified to minimize their negative effects. These policies may include patching security holes, investigating the cause and purpose of hackers' attacks. Each of these policy types will have its own characteristics that are appropriate for its purpose of creation.

As for the precautionary policy, its effectiveness is determined by the degree to which attacks are prevented from occurring at the first place. These policies are also known as defensive regulations that follow at various levels.[21] To ensure cyber-security at both the individual, national and international levels, there is a requirement for technology equipment suppliers to provide with their products a certain level of security in order to protect the personal information of customers. This security mechanism must effectively prevent various types of large-scale cyber-attacks, including viruses, phishing attacks, Trojan horses, worms, ransomware, and spyware.[22] Two significant ways to ensure security in a networked computer system are the use of firewalls and third-party products such as anti-malware software, intrusion detection and prevention systems. It is a fact that individuals, companies, corporations, and even government agencies rarely build by themselves a defensive security system for their devices and information. Instead, they buy and use services from a third party, usually, companies that provide security services, such as SolarWinds. Therefore, these cyber-security companies play a very significant role in preventing risks. Whether they can become a strong fortress against hackers depends entirely on the quality of the products and services they provide. When this great wall is defeated, all objects they protect become vulnerable targets of the cyber warriors and criminals. That is why just by hacking and injecting malware into a SolarWinds Orion Platform update software of SolarWinds, the hackers have affected more than 18,000 major corporate customers, including important agencies of the United States government include the Pentagon and the National Security Agency. Despite also being a victim of this large-scale attack, SolarWinds' responsibility is significant since it was completely unable to detect the malware in its own software for nearly a year. Even worse, the one who identified this security vulnerability was not SolarWinds, but FireEye, one of its clients. The failure of cyber-security companies such as SolarWinds to test the security of their own programs requires stricter United States domestic legal systems to ensure the quality of cyber-security services. Regular checking and scanning technological flaws should be given more attention by these software company.

Particularly for government agencies, being aware that possessed information is very important to national security, ensuring the safety of the system must be a top priority. The establishment of security standards for government networks was announced by President George W. Bush with his Comprehensive National Cyber-security Initiative (CNCI) in 2008.[23] This is a necessary step towards securing a government intranet, but subsequent attacks require these standards to be updated and tested regularly to address the existing vulnerabilities. In addition, for large-scale and well-prepared attacks, intelligence will become very important for governments in order to preempt and prevent these attacks from happening. International agreements to limit the use of cyber weapons might be effective measures in dealing with large-scale cyber-attacks sponsored by governments or terrorist groups. However, these agreements have two significant weaknesses. First, it is difficult to determine cyber weapons in reality since the technologies used for creating these weapons are dual-use.[24] For example, a computer might be used to create a harmful virus for the internet system while also be used for doing good things such as creating an educational program. Second, signing these agreements and using intelligence might conflict with the privacy rights of both individuals and corporations.[25] The paradoxical situation of trying to gain more cyber-security would lead to further more insecurity has been illustrated by Myriam Dunn Cavelty. She describes this cyber-security dilemma by referring to the circumstance when national security strongly conflicts with individual security.[26] The state-focused security agenda to prevent large-scale attacks might lead to the militarization of cyber-security, and "(re-)assert their power in cyberspace, thereby overriding the different security needs of human beings in that space."[27] Therefore, in the process of establishing such an effective mechanism to protect the government and society from being targeting by well-planned cyber-attacks, it is vital to ethically take into consideration privacy and data protection rights.

Of course, there will still be exceptions when the above measures do not completely prevent cyber-attacks from occurring. In the worst-case scenario when they do happen, countermeasures or the and problem solving policy are of paramount importance to minimizing the damage caused by these attacks and stopping it as soon as possible. In this case, it is necessary to compel the cooperation of companies and corporations to cooperate with investigative agencies and the government to identify the target of the attack, and the purpose of the attack to be the shortest time. The cyber-security dilemma still occurs in those situations when the private information of individuals and companies might be important for investigating process. Another potential effective policy for dealing with cyber-attacks might include the new bill of the presidential administration Joe Biden that "require many software vendors to notify their federal government customers when the companies have a cyber-security breach."[28] The reason behind this requirement came from negative effects from the disruption and delay in the investigation of the SolarWinds attack. The National Security Council spokeswoman said "the federal government needs to be able to investigate and remediate threats to the services it provides the American people early and quickly. Simply put, you can't fix what you don't know about."[29] The importance of identifying and addressing large-scale attacks on cyber-security at any level indicates the necessity for cooperation between security companies and government agencies.

Conclusion

Due to the complexity and uniqueness of cyber-space, large-scale cyber-attacks are attractive tools for governments, political groups, and terrorist extremist groups. The increase in sophisticated and complex cyber-attacks like SolarWinds requires a change in the traditional security paradigm by increasing the priority of cyber-security and policies. Two types of policies have been introduced, including the prevention and problem-solving policies. The preventional policies including raising and ensuring the security standards of the security services provided by software companies, and the government internal networks. In terms of foreign affairs, agreements on cyber-weapons control are deserved concentration. On the other hand, problem-solving policies also play vital roles in dealing with existing cyber-attacks. The compulsory of providing information to the federal government if needed in case of being targeted by cyber warriors and criminals is necessary for effectively solving these harmful attacks. However, the cyber-security dilemma is also needed to be taken into consideration when establishing these policies. The possibility of the state's militarization of cyber-security will be higher if the governments fully focus on national cyber-security. Individual and corporation privacy, therefore, should be paid attention to in the cyber-security discussion.

Bibliography

Cavelty, Myriam Dunn. 2014. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science & Engineering Ethíc* 20 (3): 701.

Cavelty, Myriam Dunn. n.d. "Cyber Security." *The Routledge Handbook of New Security* 155.

Dan Caldwell, Robert Williams. 2012. *Seeking Security in An Insecure World.* Rowman & Littlefield Publishers.

Ellen Nakashima, Craig Timberg. 2020. "Russian government hackers are behind a broad espionage campaign that has compromised U.S. angencies, uncluding Treasury and Commerce." *The Washington Post*, December.

Esther Dyson, George Gilder, George Keyworth, Alvin Toffler. 1996. "Cyberspace and the American Dream: A

Magna Carta for the Knowledge Age.” *The Information Society* 12 (3): 295-308.

Hannah Murphy, Helen Warrell, Demetri Sevastopulo. 2020. “The Great Hack Attack: SolarWinds breach exposes big gaps in cyber security.” *Financial Times*, December. https://www.ft.com/content/c13dbb51-907b-4db7-8347-30921ef931c2.

Holmes, Aaron. 2019. “Google is offering a $1.5 million reward to anyone who can pull off a complex Android hack.” *Business Insider*, November.

JangiralaSrinivasa, Ashok Kumar Dasb, Neeraj Kumar. 2019. “Government regulations in cyber security: Framework, standards and recommendations.” *Future Generation Computer System* 92: 178-188.

Joseph Menn, Christopher Bing, Nandita Bose. 2021. “Exclusive: Software vendors would have to disclose breaches to U.S. government users under new order: draft.” *Reuters.*

Knake, Robert. 2021. “Why the SolarWinds Hack is a Wake-Up Call.” *Council on Foreign Relations*, March. https://www.cfr.org/article/why-solarwinds-hack-wake-call#:~:text=The%20SolarWinds%20hacking%20campaign%E2%80%94one,behind%2C%20is%20far%20from%20over.

Morgan, Steven. 2019. “Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021.” *Cybercrime Magazine*, June.

Neuberger, Anne. 2021. Interview, The White House.

Richard Harknett, James Stever. 2011. “The New Policy World of Cybersecurity.” *Public Administration Review* 71 (3): 456-459.

Steven Henn, Robert Siegel. 2013. “Russian Hackers Stole More Than 160 Million Credit Cards.”*NPR: National Public Radio*, July.

Notes

[1] Robert Knake, “Why the SolarWinds Hack Is a Wake-Up Call,” *Council on Foreign Relations,* March 2021.

[2] Ellen Nakashima and Craig Timberg, “Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce,” *The Washington Post*, December 2020.

[3] Nakashima and Timberg.

[4] Knake, “Why the SolarWinds Hack Is a Wake-Up Call.”

[5] Knake.

[6] Knake.

[7] Anne Neuberger, interview by Jen Psaki, *The White House*, February 17, 2021.

[8] Hannah Murphy et al, “The Great Hack Attack: SolarWinds breach exposes big gaps in cyber security,”*Financial Times*, December 2020.

[9] Dyson Esther et al, “Cyberspace and the American Dream: A Magna Carta for the Knowledge Age,”*The Information Society* 12, no. 3 (1996): 295-308.

[10] Dyson Esther et al, 296.

[11] Myriam Dunn Cavelty, “Cyber-Security,” *The Routledge Handbook of*

New Security Studies, 155.

[12] Steven Henn and Robert Siegel, “Russian Hackers Stole More Than 160 Million Credit Cards,”*NPR : National Public Radio,* July 2013.

[13] Dan Caldwell et al, *Seeking Security in An Insecure World* (Rowman & Littlefield Publishers, INC: 2012), 159-172.

[14] Caldwell et al, 154.

[15] Steve Morgan, “Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021,”*Cybercrime Magazine,* June 2019.

[16] Caldwell et al, *Seeking Security in An Insecure World,* 162.

[17] Caldwell et al, 162.

[18] Aaron Holmes, “Google is offering a $1.5 million reward to anyone who can pull off a complex Android hack,” *Business Insider*, November 2019.

[19] Caldwell et al, *Seeking Security in an Insecure World,* 162

[20] Caldwell et al, 154.

[21] Caldwell et al, 162-163.

[22] Jangirala Srinivas et al, “Government regulations in cyber security: Framework, standards and recommendations,” *Future Generation Computer Systems* 92 (2019), 178-188.

[23] Richard Harknett and James Stever, “The New Policy World of Cybersecurity,” *Public Administration Review* 71, no. 3 (2011), 456-459.

[24] Caldwell et al, *Seeking Security in An Insecure World,* 173.

[25] Caldwell et al, 173.

[26] Myriam Dunn Cavelty, “Breaking the Cyber-Security Dilemma: Aligning

Security Needs and Removing Vulnerabilities,” *Science & Engineering Ethics* 20, no. 3 (2014), 701.

[27] Cavelty, 701.

[28] Joshep Menn et al, “Exclusive: Software vendors would have to disclose breaches to U.S. government users under new order: draft,” *Reuters,* March 2021.

[29] Menn.