Old Dominion University

Major Cyber Attacks and Prevention

Nathan Cosendine

CYSE280

Professor Malik A. Gladden

06 Apr. 2023

Introduction

A cyber attack is an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm. Cyber attacks can occur for many different purposes such as financial gain and destroying or stealing confidential data. By looking at past major cyber attacks, we can learn the best means to prevent other similar major attacks from happening in the future. Three major cyber attacks that will be looked at in this paper are the Stuxnet, WannaCry, and SolarWinds attacks, with the goal of seeing potential dangers in the future, and also seeing how these attacks could have been prevented.

Research Overview

Major Cyber Attacks

Stuxnet. In June 2010, the Stuxnet attack was launched by the combined efforts of the United States and Israel. The attack was aimed at an Iranian nuclear plant and uranium enrichment site in Natanz and was originally signed off by the Bush administration and would continue to be carried out after President Barak Obama was elected. Years before the Stuxnet attack, in President Bush's State of the Union address on January 29, 2002, the President would describe North Korea, Iran, and Iraq as an "Axis of evil" for seeking to develop weapons of mass destruction. The motive behind the Stuxnet attack was to prevent or delay Iran from developing these weapons of mass destruction by delaying the uranium-enriching program while simultaneously avoiding a war between Iran and Israel (Baezner & Robin, 2017).

The Stuxnet attack was carried out by unleashing a worm called Stuxnet on the nuclear plant. "A computer worm is a subset of the Trojan horse malware that can propagate or self-replicate from one computer to another without human activation after breaching a system

(Malwarebytes).” This worm was believed to be transmitted through a USB drive, as the plant did not have internet access. The Stuxnet worm was designed to target the plant’s centrifuges and change the speed of the rotors, which would then cause the centrifuges to not function properly or be destroyed. This attack had caused damage to Iran directly, by damaging and destroying nearly 1000 centrifuges, but also caused damage on the political level by discrediting the Iranian government and their new nuclear program. The attack also had economic effects because Iran could not simply buy new centrifuges due to international embargoes. This meant they had to build the replacement centrifuges themselves using foreign materials. Stuxnet also put pressure on Iran to have to buy enriched uranium from outside countries, due to the poor gains they were getting from Natanz.

In terms of prevention and avoiding situations like Stuxnet in the future, States can put a bigger emphasis on cyber security and spreading cyber security awareness. Stuxnet is believed to have been transmitted through a USB drive, and if the employee was more aware they would have known not to have taken it into the facility and plugged it in. Stuxnet also emphasizes creating better monitoring and verification systems, as Stuxnet was able to go undetected for a long time before being discovered.

Stuxnet would prove to be an important event in history and a turning point for Countries using Cyber warfare weapons against other countries (Langner, 2011). Stuxnet was more complex than any other malware seen before, and would “provoke a vast change in states’ cyber policies and strategies (Baezner & Robin, 2017).”

WannaCry. WannaCry was a major cyber attack that took place in May 2017 and affected more than 150 countries, notably hospitals in the United Kingdom. A few months later the US government would blame North Korea for the attack on December 19, 2017. On September 6, 2018, the United States also charged Park Jin Hyok, a member of the North Korean hacking group called Lazarus, for launching the WannaCry attack.

WannaCry was a form of zero-day Ransomware that made use of the EternalBlue vulnerability on Windows machines. Ransomware is a type of malware that "prevents users from accessing their system or personal files and demands a ransom payment to regain access." [N6] It was first planted in organizations through phishing emails containing a malicious file or link. Once a machine is infected, WannaCry would then spread to other machines on the network, soon infecting every computer and even spreading outside of the network. Unlike normal Ransomware, it is believed that WannaCry was a cyber weapon that was aimed at destruction and was not done for monetary gain. This is believed because there were no reports of systems being decrypted after the ransom had been paid, and there are reports of payments being made and no decryption key being sent in return. The attack caused damage to 100,000 organizations in the 150 countries it spread to and caused $4 Billion in damages globally with some estimates going up to $8 Billion. One of the organizations that got hit hard by the Ransomware was UK hospitals. The UK hospital system had to cancel 13,500 outpatient appointments but luckily no deaths were reported to have been caused by the attack.

The best means of prevention for Malware, including Ransomware, is to most importantly keep all software up to date. This is because updates, like Microsoft Windows updates, can patch out vulnerabilities before hackers can exploit them. Other good practices to implement are not opening suspicious emails and do not visit unsafe websites. The last means of prevention is to use antivirus programs and Windows firewall. It is advised by the FBI to NOT pay the ransom if your computer has been infected by Ransomware. Instead, use free decryptors or scans that also will remove the threat, or do a full system restore.

WannaCry is notable for the scale of the attack and how much economic damage it caused. WannaCry is also notable because of its destructive nature which made it stand out from other Ransomware attacks that had monetary gain as their motive.

SolarWinds. The SolarWinds attack was a major cyber data breach that occurred on September 4, 2019. The attack continued for a year after being launched and was discovered by FireEye on December 8, 2020. The attack was aimed at the company SolarWinds, which distrusted software to many companies and clients. Due to this attack, over 18,000 SolarWinds clients were affected by the data breach. The SolarWinds attacker's identity was up for debate after the attack, but after his election President Joe Biden would accuse Russia of being responsible, with their motive being data collection.

The SolarWinds attack is a supply chain attack. Supply chain attacks are when attackers target weak points in an organization's supply chain to damage the actual organization. Vendors and their software are targeted in these attacks because since the "software is built and released by trusted vendors, the apps and updates are signed and certified (Microsoft)." In the case of the SolarWinds attack, the attackers damaged SolarWinds by targeting Orion, who was a supplier for SolarWinds. By targeting Orion they were able to gain access to a larger network of Organizations.

Data breach damage can be harder to quantify compared to a normal cyber attack, so it can be split into three different categories: direct, indirect, and hidden costs. Direct costs include the money spent detecting the breach, as well as the cost of any legal services. Indirect costs are linked to a company's reputation and how they are viewed by the public. In the case of SolarWinds, their reputation was greatly decreased along with the trust they had between themselves and their clients. Hidden costs come in the form of time spent on responding to the breach that could have been used to expand the company (Alkhadra et al., 2021).

To prevent supply chain attacks like SolarWinds, companies can implement third-party Risks analysis by being careful of which vendors they choose. Organizations should also be aware of their supply chain and use "endpoint detection and response solutions that can automatically detect and remediate suspicious activities (Alkhadra et al., 2021)." Any way to prevent supply chain attacks is to look at components of third-party software for any vulnerability or bug and modify the source code into a more secure version.

The SolarWinds attack is notable for being one of if not the biggest cyber attacks aimed towards the United States. In the end, the attackers were able to collect data undetected for a long time and there might be unforeseeable consequences from this breach in the future.

Methodology

The main method of researching and collecting data was by using keywords with the ODU library and Google Scholar search features. From the selected literary sources, the information was gathered by condensing the sources into the criteria below.

- Name:
- Date:
- Attacker:
- Victim:
- Motive:
- Attacker Methods Used:
- Prevention Methods:
- Damage Done:

Results

Prevention. By looking at previous major cyber attacks we can learn the attackers motives, how they did the attack, and most importantly, means of prevention. The means of prevention will vary based on what methods the attackers use, but I will detail best practices that can be incorporated by businesses based on previous attacks.

From these attacks, it seems the most important prevention method is cyber security awareness. In the Stuxnet, WannaCry, and SolarWinds attacks each one could have possibly been prevented by employees knowing basic cyber security practices. These practices include not opening random emails or clicking unfamiliar links, and employees should not plug in unauthorized devices like USB drives into company computers. Another important preventative measure is ensuring that all computer systems are kept up to date. This is an important step that should be implemented across all organizations to ensure that vulnerabilities are patched and ensure that any new security features that the developer pushes out are on the system.

Organizations should also implement thorough system scans that can detect suspicious activities; this can stop the spread of any damage that may occur. Ideally companies should also search third-party software for any vulnerabilities before implementing it, instead of blindly trusting the software because it’s from a trusted vendor.

Conclusion

There is a lot that can be learned from the Stuxnet attack of 2010, the WannaCry attack of 2017, and the SolarWinds attack of 2019. Each is historically notable and we will probably see attacks like these again in the future. Each of the motives were for political reasons; stopping Iran from developing nuclear weapons, attacking foreign businesses and institutions with WannaCry, and Russia stealing sensitive US company data with SolarWinds. I believe that we will see even bigger cyber weapons being used as war is being translated into the cyberspace. By looking at what went wrong in each case, it will help to prevent future incidents from occurring. I believe the main means of prevention should be increasing cyber security awareness for all organization workers and ideally the public as a whole.

Works Cited

Alkhadra, R., Abuzaid, J., AlShammari, M., & Mohammad, N. (2021). Solar winds hack: In-depth analysis and countermeasures. 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). From https://doi.org/10.1109/icccnt51525.2021.9579611

Alraddadi, W., & Sarvotham, H. (n.d.). A Comprehensive Analysis of WannaCry: Technical Analysis, Reverse Engineering, and Motivation. ECE 646 applied cryptography. Retrieved April 6, 2023, from https://people-ece.vse.gmu.edu/coursewebpages/ECE/ECE646/F19/project/F18_presentations/Session_III/Session_III_Report_3.pdf

Askarifar, S., Rahman, N., & Osman, H. (2018, July). A review of latest WANNACRY ransomware: Actions and preventions - taylor's. Retrieved from http://jestec.taylors.edu.my/Special%20Issue%20ICCSIT%202018/ICCSIT18_03.pdf

Baezner, M., & Robin, P. (2017, October 18). Stuxnet. CSS Cyberdefense Hotspot Analyses. Retrieved from https:/doi.org/10.3929/ethz-b-000200661

Branquinho, M. (2017, June). Ransomware in Industrial Control Systems. What Comes After Wannacry and Petya Global Attacks? Retrieved from https://www.witpress.com/Secure/elibrary/papers/SAFE17/SAFE17005FU1.pdf

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy Magazine, 9(3), 49–51. Retrieved from https://ieeexplore-ieee-org.proxy.lib.odu.edu/document/5772960

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science. Retrieved from https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

Supply chain attacks. Microsoft Learn. (2023, February 6). Retrieved April 6, 2023, from https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware?view=o365-worldwide

Wan, K. S. (2020). Notpetya, Not Warfare: Rethinking The Insurance War Exclusion In The Context Of International Cyberattacks. Washington Law Review, 95(3), 1595-1620,1595A. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/notpetya-not-warfare-rethinking-insurance-war/docview/2458775765/se-2

What is a computer worm? Malwarebytes. (n.d.). Retrieved April 6, 2023, from https://www.malwarebytes.com/computer-worm

What is ransomware?: How to protect against Ransomware. Malwarebytes. (n.d.). Retrieved April 6, 2023, from https://www.malwarebytes.com/ransomware