Cyber Espionage:

History, Techniques, and Prevention

Alena N. Durel

Department of Computer Science, Charleston Southern University

CSCI 405: Principles of Cybersecurity

Dr. Lane Melton

April 3, 2022

Abstract

This paper will explore the history of cyber espionage and how it has changed with the evolution of technology. It will also look at notable attacks that helped to shape the course of cyber espionage from the first documented case to the first major case, Moonlight Maze, and finally to the militarization of it in the form of Stuxnet. Then, this paper will briefly touch on some techniques of cyber espionage including potential targets, phishing schemes, vulnerabilities, and spyware. Finally, it will discuss the prevention of cyber-attacks by securing a network and protecting data. Some of the methods considered include configuring firewalls, strong password policies, access policies, phishing education, and more.

Keywords: cyber espionage, cyber warfare, Moonlight Maze, Stuxnet, spyware, firewalls, phishing, password policy, access policy

Cyber Espionage:

History, Techniques, and Prevention

Espionage has played a role in the world for hundreds of years and cyber espionage has become more prevalent as the world of technology evolves and changes. Intelligence and data are gathered on the national, regional, and individual levels through the use of spyware and phishing schemes. As cyber espionage marches to the forefront of cyberspace, it is crucial for organizations to secure their networks and protect their data from all of the threats they might face.

Cyber Espionage and Warfare

History

While espionage has been a central part of history for centuries, the late 1980s and 1990s brought about the frontier of cyber espionage. Since then, cyber espionage has become widespread throughout many nations and has made its own place in history as the world continues to evolve and change. Although this form of reconnaissance first began in the 80s, cyber espionage groups began coming to light in the late 2000s and the militarization of cyber warfare and espionage was in full swing by 2010 with the Stuxnet attack.

Cyber espionage has become vital to the government and military operations in the world of cyber warfare, seeking out information on foreign states and attempting to prevent those looking for data on their own country. The United States, Russia, China, and Korea are some of the top countries in the realm of cyber warfare, with government-backed hackers and organizations working towards these goals. However, as time goes on, it is no longer just large global powers who are carrying out cyber espionage, regional powers, as well as even smaller groups, are joining them.

As cyber warfare and espionage developed in the 2010s, three significant agreements took place and brought diplomacy and policy into cyberspace in 2015. First, the United States-China Agreement stated that neither government “w[ould] conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage” (Barack Obama, 2015, as cited in Segal, 2016, para. 3). While this agreement does not necessarily guarantee a safe cyber environment between the nations, it is a gesture of diplomacy in the realm of cyberspace.

Next, the United Nations gathered and created the WSIS+10 (World Summit on the Information Society) which promised to bridge digital divides and improve the availability of information technologies and discuss national cyber policies (Haizler, 2017; UNESCO, 2018). It also recognized that “the same rights that people have offline must also be protected online” and worked to accomplish this (WSIS+10, 2015, as cited in UNESCO, 2018, para. 4). Finally, the Safe Harbor Agreement updated the Safe Harbor Program that was first created in 2000 and gave guidelines for the ways that companies in the United States could handle European citizens’ data (Haizler, 2017, para. 18).

Notable Attacks

The first documented cyber espionage case took place in 1986 when the computer administrator, Clifford Stoll, at Lawrence Berkeley National Laboratory in California noticed something strange with the time records and when the network was being accessed (O’Brien, 2017, para. 3). After detecting the intrusion, Stoll was able to set up a honeypot to capture Markus Hess, who was selling stolen information and military secrets to the KGB.

The Moonlight Maze attack is recognized as the first large-scale espionage attack in cyberspace. While uncovered in 1998, this attack began two years prior and remained undetected within the systems that had been targeted. The Pentagon, NASA, the Energy Department, private universities, and research labs in the United States were the target of the attack, and thousands of sensitive documents were stolen over the course of those two years (Haizler, 2017, para. 9-10). The attack was traced back to a computer in the former Soviet Union, however, the promoter of the attack remains unknown. This was a well-organized attack, with the attacker remaining undetected for several years, leaving backdoors in the system, and leaving very few traces. The Moonlight Maze attack was a point of progression in cyber warfare and espionage (Haizler, 2017, para. 9-10).

The Stuxnet attack of 2010 is one of the most well-known cyber-attacks and marked the militarization of cyber espionage. This attack targeted Iran and is believed to have been led by the joint force of Israel and the United States. Stuxnet was introduced into the systems through several known vulnerabilities as well as four “zero-day” exploits. Once in the system, the worm could travel through the entire network and escalate its privileges on the infected machines, gaining access and damaging Iran’s centrifuges (Haizler, 2017, para. 14-15). This attack greatly changed the course of cyber warfare and espionage.

Techniques

Targets

Anything that can be connected to the internet can become a target of cyber espionage. This can include traditional devices such as computers running operating systems like Windows, Mac OS, and Linux, and phones running IOS or Android. However, this could also include Internet of Things (IoT) household devices such as smart home speakers, security cameras, some fridges, and even robot vacuums (Zsolt, 2020, para. 10). Alexa and Google Home devices can be hacked and used to listen in to conversations within a home and security cameras can give a perpetrator an inside view of a victim’s house.

Spyware

Many techniques for data exfiltration exist and are commonly used by malicious hackers. These could include both hardware and software-based malware including keyloggers, malware that allows the hacker to look through the victim’s camera or take screenshots of their device, using cookies to capture data, and stealing personal log-in information to various applications and websites (Zsolt, 2020, para. 10).

This malware can be delivered to devices through vulnerabilities in the system or through a payload attached to a phishing email. Once the attacker has access to the device, they can monitor the user’s activity and obtain sensitive data including passwords, work-related documents, and more. While individuals can be the subject of cyber espionage, large companies and government organizations are more likely to be attacked as they have access to more users’ information and restricted data. If a hacker can infiltrate a company’s system, then they can gain access to thousands of users’ data, as opposed to the data of an individual.

Prevention

Securing the Network

Securing a network is one of the most important steps to ensuring that the chances of an attack on an organization are diminished. One of the first steps to securing a network and preventing espionage is to enable and configure a firewall for the network. While a firewall with minimal rules is better than no firewall, any large organization should have a well-configured firewall with specific rules based on what traffic needs to travel in and out of the network, what traffic needs to be restricted, and even which IP addresses can access the network.

Organizations should also implement strong password policies for creating secure passwords and should enforce password changes at least once a quarter (Eichkorn, 2021). Some notable cyber infiltrations were successful in part due to weak passwords such as the Sony Pictures Entertainment hack of 2014 when they had three of their certificate passwords set to “password” and the SolarWinds attack of 2019 and 2020 where they used the password “solarwinds123” (Mazzarella, 2015; Fung & Sands, 2021). Another step in securing a network system could be to set up a Virtual Private Network (VPN) that only employees have access to which could greatly help to diminish the chance of being attacked from a wireless access point (Eichkorn, 2021).

After the network has been secured, files should be encrypted to protect restricted and sensitive information stored on the systems within the network. In addition to this, computers should be shut down when not in use, especially overnight, limiting hackers’ access to the network or disrupting their work if they are already in the system (Eichkorn, 2021). Employees should also take care to avoid accessing company data on their personal devices, especially if they have weak personal passwords, regularly access public WIFI, or if their devices are not secured.

Protecting Data

Access Policy. It is imperative for any group holding sensitive or secret information such as the government, military, financial groups, and other large companies, to have a strict access policy and perform access audits regularly. Certain data should not be available to all users on the network and the organization should review who has access to which data, as well as which data they need to access. Furthermore, these organizations should also determine who needs read, write, and copy access, as well as who simply needs read access. By limiting the number of people who have access to this information, data will be more protected against both outside attackers and those working an inside job.

By not allowing lower-tiered users to have contact with more restricted information, it will make it more difficult for malicious attackers to gain access to this data. If they can get within a user's system, whether through phishing or exploiting vulnerabilities, it is less likely that they will be able to view and take sensitive data, as opposed to if every user had access to all of the data. This also protects the group from people taking data from within the organization itself. In 2013, Edward Snowden was able to steal millions of documents, including information that he was not working with, containing secret information from the National Security Agency (NSA) where he was employed (Harfield, 2021). If he had only had access to the documents that were pertinent to his work, he would not have been able to leak as many restricted documents.

Phishing Education. Another action that organizations should take to better protect their data is to educate their employees on phishing schemes. One of the biggest vulnerabilities that attacks focus on is human error. Malicious attackers can target employees of the company they are attempting to infiltrate and gain the information needed to access the system such as passwords or introduce malware to the computer and create a vulnerability that they can exploit. It is important that everyone, but especially those who have access to restricted information, know what to look for when trying to determine if something is a phishing scheme.

The vast majority of phishing emails will look as if they came from a trusted source and will hold a tone of authority. Many will try to use familiarity to get information from the victim. For example, getting an email from the "IT Department" that they need your password so that they can reset it for you. Others will play on the urgency of a situation and often use scarcity of an item or event to get people to fall victim to their trap, such as time running out on a limited deal.

Conclusion

Cyber espionage has played a significant role in the world since the 1980s. National, regional, and individual groups of cyber spies roam cyberspace, gaining intel and data. Payloads containing spyware are delivered through vulnerabilities in the system or through phishing schemes, allowing hackers access to the user’s data. The risk of being attacked can be diminished by creating a strong access policy for an organization, securing networks with firewalls and strong passwords, and educating employees on the dangers of phishing schemes.

References

Bederna, & Szadeczky, T. (2019). Cyber espionage through Botnets. *Security Journal*, 33(1), 43–62. https://doi.org/10.1057/s41284-019-00194-6

Eichkorn, D. (2021, April 28). *How to Secure a Network for Business Computers*. Gordon Flesch Company. Retrieved April 1, 2022, from https://www.gflesch.com/elevity-it-blog/ways-to-secure-a-computer-network

Fung, B., & Sands, G. (2021, February 26). *Former SolarWinds CEO Blames Intern For 'solarwinds123' Password Leak*. CNN. Retrieved April 1, 2022, from https://www.cnn.com/2021/02/26/politics/solarwinds123-password-intern/index.html

Haizler, O. (2017). The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking. *Cyber, Intelligence, and Security*, *1*(1), 31–45. https://www.inss.org.il/wp-content/uploads/2017/03/The-United-States%E2%80%99-Cyber-Warfare-History-Implications-on.pdf

Harfield, C. (2021). Was Snowden Virtuous? *Ethics and Information Technology*, *23*, 373–383. https://doi.org/10.1007/s10676-021-09580-4

Mazzarella, J. (2015, January 6). *THE SONY HACK — WHAT HAPPENED, HOW DID IT HAPPEN….WHAT DID WE LEARN?* UMass Boston IT News. Retrieved March 31, 2022, from https://blogs.umb.edu/itnews/2015/01/06/the-sony-hack/

O'Brien, D. (2017, July 31). *A Short History of Cyber Espionage*. Medium. Retrieved April 1, 2022, from https://medium.com/threat-intel/cyber-espionage-spying-409416c794ec

Segal, A. (2016, January 4). *The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement*. Council on Foreign Relations. Retrieved April 1, 2022, from https://www.cfr.org/blog/top-five-cyber-policy-developments-2015-united-states-china-cyber-agreement

United Nations General Assembly WSIS+10 High-Level Meeting Adopts a Milestone Outcome Document. UNESCO. (2018, October 10). Retrieved April 1, 2022, from https://en.unesco.org/news/united-nations-general-assembly-wsis10-high-level-meeting-adopts-milestone-outcome-document

What is Cyber Espionage & How to Protect Your Data. Fortinet. (n.d.). Retrieved April 1, 2022, from https://www.fortinet.com/resources/cyberglossary/cyber-espionage