RESEARCH ARTICLE OPEN ACCESS

Cyberwarfare History and APT Profiling

Azhar Ushmani

ABSTRACT

The cyberattack that occurred in 1998 called the Moonlight Maze has a significant impact on the cyber world, particularly in the United States. Although this is not the first cyberattack in history, its effect "led to a dramatic shift in US administration's approach to cybersecurity" (Haizler, 2017). The Moonlight Maze is a large-scale cyber-attack carried out to spy on some of the most prestigious departments in the US such as the Pentagon, NASA, and Energy Department. What makes this cyberattack even more noteworthy is that it was not discovered right away. It took nearly two years before the US officials discovered it. From then on, cyber capabilities have evolved. Two of these are malware and advanced persistent threats (APT).

Keywords:- cyberattack

I. INTRODUCTION

The malicious software can be grouped into three—the low-potential end, high-potential end, and the one in between (Rid & McBurney, 2012). The first two will be discussed in this section. The first group of malwares is not designed to create a direct harm but rather to disrupt operations on a specific target such as a Denial of Service (DoS) attack. This type of malicious software is easy to install yet also easy to detect and, thus, defend against. The one on the high-potential end aims to significantly harm a system—usually a well-protected one—and has embedded intelligence. It goes after a specific target and not just any system that appears vulnerable. However, this malware is complicated to set up because it needs stealth to be able to carry out its purpose like, for example, the malware that tricked the Syrian's air defense system that there were no approaching airplanes in it area (Rid & McBurney, 2012).

An APT, on the other hand, is characterized by the following according to Chen, Desmet, and Huygens (2014): First, it has specific targets and objectives such as obtaining confidential information or disrupting an organization's critical mission or program. According to a survey as mentioned in Chen et al.'s paper, the top most common victims are those in the education, energy, government, and finance industries. The goals of these attacks are mainly gaining access to data of value such as intellectual property or trade secrets. Second, it is well thought out and well planned by well-resourced attackers. The illegal infiltrators can be highly-skilled individuals working for another organization or hired mercenaries whose job is to hack into systems. These people are given ample resources and time to ensure a successful operation. Third, the attack is repeated and lasts for a long time. The preparation for this attack is extensive, and the goal is clear; hence, attackers ensure that they get what they need. If the first attempt fails, they will modify the plan until they reach the goal originally set. For example, they may infiltrate a less secure system first. This may go on for months or years until successful. Last, it is concealed. One of the reasons an advanced persistent threat lasts for a long time is its stealth. Hackers use evasive techniques so that the activity remains undetected. They slowly infiltrate a system, as opposed to the highly detectable malware, particularly the one on the low-potential end. As of this writing, there's no specific countermeasure for APT because it is complex and stealthy.

To carry out APT, the hackers go through six phases (Chen et al., 2014). The first one is the gathering of information also referred to as the reconnaissance and weaponization. The information can come from the publicly available sources then devising a manipulation scheme based on this information to entice the target to take action. The next phase is the delivery of the attack tool such as phishing. Once the tool is in place, the next phase is the initial intrusion where the hackers obtain credentials usually from commonly used programs with vulnerabilities such as Microsoft Office and installs malware. The following phase is called the command and control phase, where the attacker uses the installed malware to control the infected device then communicates with attacker's machine. Once communication between the two devices is established, it conducts the gathering of information once again so that it can infiltrate more systems and create a clearer map for the success of the process. After enough information has been collected about the target, it will then start stealing the data needed.

Because of the characteristics of APT and the complexity of how it is carried out, it is different from the attacks before the proliferation of the internet. For one, APT is successful mainly because of internet. The data gathered by the attackers about their targets come from publicly available sources. If there were no or little access to the internet, data gathering would take a very long time, if not impossible. Also, APT uses programs that are commonly used by the target users such as Microsoft Office and vulnerable browsers. Perhaps, these programs did not collect much data from its users before; hence, the reconnaissance would, again, be challenging. Also, before the internet, the cloud was not a common storage; hence, the trade secrets or intellectual properties of value may not be there.

An APT can originate in supervisory control and data acquisition (SCADA) systems in Critical Infrastructure Systems. SCADA systems are the main controllers of the entire power grid. They are composed of computers and communication networks installed in different locations to monitor and control critical infrastructures (Ten, Manimaran, and Liu, 2010). Because the SCADA is the heart and brain of a power plant's operations and it is connected to the internet, it is the most susceptible to an APT attack. In 2000, a SCADA breach occurred in Queensland, Australia in Maroochy Shire. The attacker took control of the SCADA system in Maroochy plant and spilled raw sewage in rivers, parks, and even famous establishments such as the Hyatt Regency Hotel (Rid & McBurney, 2012).

II. CONCLUSION

Regarding the profile of a possible attacker on the Western Interconnection power grid, here is what Vianna (2016) writes: The Western Interconnection power grid is one of the three major interconnected systems in North America. The other two are the Eastern Interconnection and the Texas Interconnection. Of these three, only Texas Interconnection has an independent energy systems that will not be affected by a black out in any of the other power grids. This means that the attackers are non-state actors. Their resources are the internet and computers. These will be used for reconnaissance, weaponization, and writing of malicious codes to be installed in the Western Interconnection's SCADA systems. Based on the Ukrainian attack on energy plants, the attackers may have the capabilities to log out staff's access and overwrite its credentials, create phishing emails, and manipulate Microsoft office documents (Vianna, 2016). The attackers may not have physical access to the site because they only need to control the SCADA systems to be able to carry out their attack plans. Their main target could be the black start unit which provides emergency power if a black out occurs. There are black start units that have not actually undergone a re-start of power; hence, their function is not a hundred percent reliable. Also, according to Vianna (2016), aside from the black start unit, the Western Interconnection and the Eastern Interconnection do not have other backup plans. Therefore, attacking this may result in prolonged black outs.

REFERENCES

[1] Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security*, 63-72. Retrieved from https://link.springer.com/content/pdf/10.1007/978-3-662-44885-4_5.pdf

[2] 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. Retrieved from https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/The%20United%20States%E2%80%99%20Cyber%20Warfare%20History%20Implications%20on.pdf

[3] Rid, T. & McBurney, P. (2012). Cyber-weapons. *The RUSI Journal*, 157(1), 6-13. Retrieved from https://doi.org/10.1080/03071847.2012.664354

[4] Ten, C.W., Manimaran, G., & Liu, C.C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics*, 40(4), 853-865. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/downl

oad?doi=10.1.1.475.2858&rep=rep1&type=pdf

[5] Vianna, G. (2016). Vulnerabilities in the North American power grid. *Global Security Studies*, 7(4). Retrieved from http://www.globalsecuritystudies.com/Vianna%20Electric%20Grid.pdf