Weighing the Threats: Current Trends in Cyberattacks

Adam Gardiner
Liberal Arts, Huachiew Chalermprakiet university
*Email : 13degreeslatitude@gmail.com

Abstract

The advent of advanced computer technology and the expansion of cyberspace has a two-pronged impact. On the one hand, it is increasingly useful for undertaking private and government activities in this digital era. On the other hand, the users of these advanced technologies are equally exposed to cybersecurity threats and attacks. This paper discusses the problem of the expanding threat of cyberattacks. It specifically discusses the nature of the trends of attacks especially during the pandemic, and also considers the role of cyber threat intelligence in helping to mitigate them. The discussion of trends shows that the cyber threat landscape is becoming more complex, becoming more resilient to traditional cyber security defences, and adapting faster to take advantage of new trends such as cloud computing and IoT. Therefore, more research into ways of improving cyber threat intelligence is required.

Keywords : cybersecurity, cyber threat intelligence, cyber security trend, threat actors

1. Introduction

Since the turn of the century, the world has witnessed a shift in the way daily life activities such as commercial, cultural, social and governmental activities and communications are carried out due to the advent of advanced technology and expansion of cyberspace (Li & Liu, 2021). However, in tandem with the cyberspace expansion there has been a significant increase in global cyberattacks in recent years. It is evident that both private companies and government organizations are facing challenges of cyberattacks and the threats of wireless communication (Lee, 2019). The targets of these attacks have included critical infrastructure, financial institutions, and government agencies (Kumar, 2016). There has been a trend from attacks that are only disruptive to those that are designed to cause physical damage or steal data. Further, the attackers are becoming more sophisticated and using more complex tools (Li & Liu, 2021; Ukwandu et al., 2022). Consequently, the attacks also are becoming more sophisticated and more likely to cause greater damage to the users affected by them. Thus, it is necessary to understand the nature of the trends of attacks, so users can have ways to mitigate them. To understand each trend of cyberattack at a deep level, it is essential to have effective cyber threat intelligence (CTI). Therefore, this paper discusses cyber threat intelligence in relation to some current trends of cyberspace attacks: Exploitations of Vulnerabilities, Phishing and Spear Phishing attacks, Cyber Espionage, Distributed Denial of Service (DDoS) attacks and Botnets. (Diwan, et al, 2021).

2. Objective

The goal of this research study is to discuss some common trends of cyberattacks and consider the role of cyberthreat intelligence in understanding and mitigating them.

3. Trends of Cyberattacks

It should be noted that not all cyberattacks fall neatly into one of the following types. Many cyberattacks are complicated, combining methods from more than one trend to achieve their goal. For example, in the case of espionage, cyber attackers may use various methods to penetrate a computer system in order to access government information. For all of the types, I am especially interested in the role of cyber threat intelligence in helping us to understand not only how the cyberattack is executed but also the behaviour and motives of the cyber attackers or threat actors. Cyber threat intelligence can usefully be divided into three overlapping levels: tactical which is technical intelligence that could lead to the identification of threat actors, operational which is details of the motivation of threat actors and strategic which concerns the high-level strategy to respond to threats (Bank of England, 2020),

3.1. Exploitation of vulnerabilities

This type of attack exploits a vulnerability, which is a flaw in a computer system that weakens its security. An example is the set of attacks that exploited Log4Shell (CVE-2021-44228) which was a zero-day vulnerability in Log4j, a popular Java logging framework. A zero-day vulnerability is a vulnerability that has been disclosed but not yet patched. The Log4Shell vulnerability was disclosed on 24 November, and a patch became available on 6 December.

Apache then gave Log4Shell a CVSS severity rating of 10 which is the highest available score (Apache Software Foundation, 2021). Even though Log4Shell is no longer a zero-day vulnerability, it is still a severe threat because of the huge number of devices that run Java, many of which have not yet been patched. Charlie Gero, CTO of Akamai Technologies, emphasizes the severity of the threat posed by the Log4Shell vulnerability: “To understand just how bad this vulnerability is, we must consider that Java runs on billions of devices around the world, and that Log4j is one of the most widely used logging libraries for it.” (Akamai Blog, 2022 March 8). These devices include not only web servers but embedded and IoT devices. The severity rating also reflects the harmful activities that follow an exploit. After an attacker exploits the vulnerability to execute arbitrary Java code on a server or other computer, they can use the victim’s computer for cryptocurrency mining, creating botnets, sending spam, and ransomware attacks.

3.2 Phishing and Spear Phishing

Phishing is a type of social engineering where a hacker creates a fake email that appears to be from a legitimate source such as a bank. The email contains a link to a fake website that prompts the recipient to enter personal data, or an attachment that, when clicked, downloads malware onto the victim's computer. The malware then allows the hacker to gain access to the victim's personal data, such as passwords or financial information. Spear phishing is a sub-type of phishing where an attacker directly targets a specific person or organization with customized fake communications. Phishing appears to be the type of cyberattack that has benefitted most from the trends resulting from the Covid-19 pandemic, especially remote working and the increasing number of people whose economic situation was adversely affected by the pandemic. One of the many examples catalogued by Laille (2021) is an email purporting to be from the UK government, offering job retention payments.

3.3. Cyber Espionage

Cyber espionage is the activity of stealing information or trade secrets from another person or organization by using computers and the internet. Usually this is done by hacking into the target's computer system and accessing their files. The hacking methods are various, including the use of proxy servers, cracking techniques and malicious software including Trojan horses and spyware. Corporations and governments are most likely to be affected by this kind of cyberattack. Threat actors may be individuals or groups working independently, but the sophistication required for a successful cyberattack against a government usually requires the backing of another government. In December 2020, FireEye, a cybersecurity consulting firm, discovered and disclosed the massive “SolarWinds operation.” Hackers inserted malicious code into an update for Orion, a network management platform provided by Solar Winds. Customers downloaded what they thought was a legitimate update to the Orion software but in reality downloaded a virus that infected their computer. This cyberattack, suspected to have been planned and executed by a group backed by the Russian government, affected many corporations besides Solar Winds and led to data breaches of many branches of the United States federal government (Emerald Expert Briefings, 2020). Regarding cyber threat intelligence, various public and private sector organizations, such as Mandiant, accumulate their own intelligence data relating to cyber espionage and release it in publicly available reports.

3.4. Denial of Service attack or Distributed Denial of Service (DDoS) attack

As the words imply, a Denial of Service attack has the objective of making a network service temporarily or permanently unavailable. The attacker achieves this objective by launching a large number of requests to the target machine, typically a website or online service. thus overwhelming it with traffic. Consequently, the target machine becomes slower and less responsive, and users may be unable to access it while the attack is ongoing. There are different types of DDoS attack depending on which of the seven layers of the network connection is targeted. A distributed denial of service (DDoS) attack has the same objective as a DoS attack, but uses a network of multiple compromised systems to implement the attack. These systems could include computers and IoT devices. They are coordinated by the attacker to overwhelm the target machine. This network of machines is known as a "botnet."

There appears to have been an increase in DoS and DDoS attacks globally during the COVID-19 pandemic. The number of Denial of Service attacks in the UK increased by 28.57% from May 2019 to May 2020 (Buil-Gil et al, 2021).

3.5 Botnets

A botnet is a network of computers that are infected with a bot, which is a type of malware that allows an attacker to send commands to the computers and control them remotely. A botnet may be used for launching DDoS attacks as described in the previous section, or for other purposes such as sending spam. Regarding cyber threat intelligence, the tactical level is of most relevance here. Various network tools and technical data such as IP addresses or server logs can be used to help in the identification of cyber attackers behind a botnet. It must be emphasized that this is a very complex process which could lead to false identification, especially in the case of a botnet, since the IP addresses will probably belong to machines that have been hijacked by the cyber attacker. If the nature of the attack was not understood, the organization that owns the computer would be wrongly implicated in the attack.

4. Conclusion

The above survey of current trends in cyberattacks shows that the cyberthreat landscape is becoming more complex as it exploits new trends in computing, especially IoT (internet of things) and cloud computing. Owing to the coincidence of these trends with the COVID-19 pandemic, the negative impacts of cyberattacks have accelerated over the last two years. Even though the COVID-19 pandemic appears to be waning in most countries, the trends of cloud computing and IoT will continue. Also, new trends are emerging which may threaten computer security. An example is quantum computing, which might be used in the future to break encryption algorithms that are currently unbreakable with classical computers. Therefore, the importance of cyber threat intelligence has never been greater. However, the quality of cyber defence is only as good as the quality of the available threat intelligence. The growing number of attacks during the pandemic indicates that more research needs to be done in improving the quality of CTI at the tactical, operational and strategic levels. In this context, I am interested in the innovative approach of CrowdSec, which uses tens of thousands of users throughout the world to "identify bad cybersecurity actors and create a database of rogue IPs for all community members to block, generating a real-time crowdsourced CTI (cyber threat intelligence database)" (CrowdSec, 2022). So I plan to critically assess the effectiveness of a crowdsourcing strategy in mitigating cyberattacks.

References

Apache Software Foundation (2021, Dec 12). *Apache Log4j Security Vulnerabilities.* Retrieved June 8, 2022, from https://logging.apache.org/log4j/2.x/security.html

Bank of England. (n.d.). *CBEST intelligence-led testing - Bank of England*. Bank of England. Retrieved June 15, 2022, from https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.

Cherqi, O., Hammouchi, H., Ghogho, M., & Benbrahim, H. (2021, November). Leveraging Open Threat Exchange (OTX) to Understand Spatio-Temporal Trends of Cyber

Threats: Covid-19 Case Study. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 1-6). IEEE.

Crowdsec. (2022, May 30). *CrowdSec, the open-source & collaborative IPS*. The open-source & collaborative IPS. Retrieved June 5, 2022, from https://crowdsec.net/

Diwan, T. D. (2021). AN INVESTIGATION AND ANALYSIS OF CYBER SECURITY INFORMATION SYSTEMS: LATEST TRENDS AND FUTURE SUGGESTION. *INFORMATION TECHNOLOGY IN INDUSTRY*, *9*(2), 477-492.

Fallout of solarwinds hack could last for years. (2020). *Emerald Expert Briefings*. https://doi.org/10.1108/oxan-es258390

Gero, C. (2022, March 8). *A Log4j retrospective part 2: Data Exfiltration and remote code execution exploits*. Akamai Blog. Retrieved June 6, 2022, from https://www.akamai.com/blog/security/a-log4j-retrospective-part-2-data-exfiltration-and-remote-code-execution-exploits

Kaur, J., & Ramkumar, K. R. (2021). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*.

Khan, I., Farrelly, W., & Curran, K. (2020). A demonstration of practical DNS attacks and their mitigation using DNSSEC. *International Journal of Wireless Networks and Broadband Technologies*, *9*(1), 56–78. https://doi.org/10.4018/ijwnbt.2020010104

Kumar, S., Benigni, M., & Carley, K. M. (2016, September). The impact of US cyber policies on cyber-attacks trend. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 181-186). IEEE.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Lee, D. (2019). The Trends of Next Generation Cyber Security. *Journal of the Korea Institute of Information and Communication Engineering*, *23*(11), 1478-1481.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

McNab, C. (2017). *Network security assessment: Know your network*. Sebastopol: O'Reilly Media, Inc.

Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., ... & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, *3*(1), 1-21.

Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020, December). Cyber security challenges and its emerging trends on latest technologies. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 2, p. 022062). IOP Publishing.

Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. *Computer Fraud & Security*, *2021*(1), 14-19.

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: a review of current and future trends. *Information*, *13*(3), 146.