Name: Ronit Singh **CDAD** **Date:** 12 September, 2021

CYBERWARFARE

Week 3 Reading Summary

The three PDFs "Cyber Threat Source Descriptions", "2019 State of Malware", and "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks", mention current trends, related statistics and predictions, and present situations in today's threat landscape and their possible mitigation techniques, respectively.

The first PDF "Cyber Threat Source Descriptions" talks about the various types of **threat actors** that pose a risk to the US Government and its critical infrastructures, categorizing them into high, medium or low risk based on their capabilities, access to resources and damage extent. The National cyber warfare programs by National Governments pose the maximum threat in cyberspace due to their availability to resources, fundings and extensive infrastructures. Others that comparatively pose relatively lesser risk include Terrorists (due to their lack of skill set in cyberspace and funding), Industrial Spies and Organized Crime Groups (mainly, profit and money oriented but access to money as well as cyber skills, so medium level risk), Hacktivists (political oriented; moderate to highly skilled but relatively lesser access to resources, funding), and Hackers and its various sub-types (relatively less capable, but still pose a threat to local businesses and people). The article also shows the GAO (Government Accountability Office) Threat Table that includes other threat actors i.e. Bot-network operators, Insiders, Phishers, Spammers, and Spyware/malware authors. If coordinated, these can be equally disruptive as well!

The second PDF "2019 State of Malware" compares, makes predictions, and talks about the cyber attack trends in 2018 and 2019. It deeply and accurately analyses the various **threat vectors** and **major incidents in cyberspace** in those years based on numbers i.e. statistics and charts. The article states that "Over the years, we have seen more attacks against businesses, more detections of malware on their endpoints, and a greater focus on what cybercriminals consider a more lucrative target." (Malwarebytes, 6). It also mentions the rise of ransomwares during 2017 and cites the famous and lucrative ones like SamSam and WannaCry as examples. After looking at the charts for most used malwares, I came to the conclusion that Trojan always remained in the top 3. Moreover, the article says that businesses and people in 'high economy' western countries are more likely to be targeted by cyber attacks as can be seen in the charts (Figure 10 and 11), where the US tops the list in both cases, and the UK is not close behind. Apart from that, there have also been cases of criminals targeting hardware devices, especially routers and IoT home devices. Attackers have an extra edge here because of outdated devices (lack of patches) and this scenario is difficult to combat for many security vendors. Hence, users should be aware of the risks and never take the security of your data or devices for granted.

The third PDF "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks" explores the concept behind semantic attacks. The article says that, keeping in mind these attacks, "researchers and engineers should aim to approach for both current and future semantic attacks by addressing core semantic attack characteristics rather than particular implementations. That is because a defence system designed for a particular set of characteristics can be applicable across all attack types that share it, thus making it a more efficient choice from the perspective of technical development." (R. Heartfield and G. Loukas, 37:3). The article lists out control stages 1-3 (Orchestration, Exploitation, Execution) and its several modes and vectors which help in separating and classifying the different attacks uniquely. Moreover, in this rapidly changing and evolving threat landscape, it is extremely important that the policies, procedures, rules, and regulations be flexible to "unknown and unforeseen attacks" (R. Heartfield and G. Loukas, 37:21).

What surprised me?

The methodology behind "sound loggers" was surprising to me. I already knew what keyloggers aimed to do, but didn't know that there could be programs or tools to record sounds and listen to the cadence and volume of tapping to determine which keys are struck on a keyboard.

Moreover, I found the concept of "middleware" proxy training portal to be interesting. According to "2019 State of Malware", it is "responsible for brokering a connection between the user and Internet access. Only after users successfully complete a training quiz/test for improving security education and risk awareness will access to remote resources is permitted." (R. Heartfield and G. Loukas, 37:22).

Questions?

1. Is polymorphism and AI generated attacks similar? What's the difference, if any?
2. What other methods do businesses use for their employees to become aware of the risks in cyberspace (like middleware training)?

Works Cited

CISA. Cyber Threat Source Descriptions | CISA. [online] Available at: <https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions>[Accessed 11 September 2021].

Heartfield, Ryan & Loukas, George. (2016). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. ACM Computing Surveys. 48. 10.1145/2835375.

MalwarebytesLabs., 2019. [online] Malwarebytes.com. Available at: <https://www.malwarebytes.com/resources/files/2019/01/malwarebytes-labs-2019-state-of-malware-report-2.pdf> [Accessed 11 September 2021].