Reyan Jan Samontanes **BSIT 3 – 2CP** **Info Assurance Task Performance**

Part 1:

1. Select five Malware from the following: Spyware, Adware, Rootkit, Ransomware, Worm, Trojan Horse, or Backdoor.
2. Search two examples for each of the five malware you have selected. Add a short description for each. Cite your references.

- Trojan Horse
    - Animal – was the first known trojan virus created by John Walker in 1974 (Dupont, 2019). It was a disguised as a harmless popular game called "guess the animal" and install in every directory where it is not present.
    - BashLite – In 2015 it was called bashdoor(Dupont, 2019) where it infected Linux systems around the world and launched DDoS attacks that reached 400GB per second.
- Adware
    - CoolWebSearch – A.K.A "About:Blank" or "CWS" (Gray, 2009) is a malicious application commonly attacked firefox users where it establishes its files on various windows OS platforms. It displays popup or pop-under ads and is known as Browser Hijacker or BHO.
    - Fake Player – When Android OS gained popularity(Thomas, Surendran, John, & Alazab, 2023), The first known malware in android emerged in 2010. This malware came disguised as a media player and it send messages to some premium number with each messages costing around 5 dollars.
- Rootkit
    - Regin Spying tool – A highly sophisticated and stealthy malware platform (Paganini, 2014) that has been link to state-sponsored cyber espionage campaign, discovered in 2014.
    - Machiavelli - Machiavelli smuggles itself into the Mach kernel (Ries, 2009), the foundation of Mac OS. It installs a local agent which, while nearly invisible to the user, can be controlled remotely via the network.
- Ransomware
    - CryptoLocker - Screen lockers virtually disappeared after the introduction of a ransomware group known as CryptoLocker in 2013. CryptoLocker ransomware was developed by the so-called BusinessClub that used the massive Gameover Zeus botnet with over a million infections (Baker, 2024).
    - MedusaLocker - a ransomware family that was first seen in the wild in early October 2019 (Baker, 2024). In January 2020, a fork of MedusaLocker named Ako was observed, which has been updated to support the use of a Tor hidden service to facilitate a RaaS model.
- Worm
    - Mirai – (Tanner, 2023) a botnet that targeted routers, as well as some internet-of-things (IoT) devices such as smart home systems. It scanned and targeted devices with a particular processor running a reduced version of Linux, which is very

common on routers and IoT technologies, and then gained access using default credentials, which unfortunately are often not changed by the user on setup or in some cases are hard-coded by developers.

- Stuxnet - is believed to have been developed jointly by U.S. and Israeli intelligence agencies. It used stealth as well as four separate zero-day exploits to spread because its objective was singular and very specific to infect SCADA systems that were part of Iran's nuclear program and destroy the centrifuges being used to enrich uranium into weapons-grade material (Tanner, 2023).

Part 2:

1. Search for an article regarding a cybersecurity attack using malware. The article should be published within the last five years by a credible sources.
2. Answer the following items based on the article you found.
   a. What is the title of the article?
      - The Risk of Accidental Data Exposure by Generative AI is Growing.

   b. Who wrote the article?
      - Paolo Passeri, a cyber intelligence principal, NetSkope.

   c. When was the article published?
      - August 16, 2023

   d. Give the link where you found the article?
      - https://www.infosecurity-magazine.com/blogs/accidental-data-exposure-gen-ai/

   e. Is it possible to prevent this kind of attack? How?
      - Yes, by being aware and being sensible to the type of data that we have to share on the internet. Also the company provided the preventive and security measures so that this kind of breach prevent.

   f. How extensive was the impact of the attack to the environment where it happened?
      - It very extensive because the widely confidential information is leaked. In 2023, OpenAI, the company of ChatGPT, provided details of a data breach, forcing it to temporarily take the generative AI app offline. The data breach exposed mostly source codes also some of the customers payment related information and allowed titles from some active user’s chat history to be viewed. Some of the company like Samsung ban the use of Generative AI because some of the users leaked their confidential and most sensitive data via CHAT GPT.

   g. How did the person or the company, who was attacked coped with the consequence and the effect of the incident?
      - Through this events happening that data breach and sources codes leaked via Generative AI. The platforms also collaborating with some of the biggest industries in technology that provide a granular approach based on DLP controls that detect sensitive information such as source code, users information and others sensitive data. Also implementing a security and accountability policy to be their top priority.

References

Baker, K. (2024, March 29). *Cybersecurity 101 › Ransomware › Ransomware Examples:*. Retrieved from CROWDSTRIKE: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-examples/

Dupont, J. (2019, April 30). *Fun & Lifestyle*. Retrieved from Dewvolutions: https://blog.devolutions.net/2019/04/a-history-of-major-computer-viruses-from-the-1970s-to-the-present/

Gray, D. (2009, May 06). *Removed CoolWebSearch Malware*. Retrieved from Article: https://www.syschat.com/how-to-remove-coolwebsearch-malware-4673.html

Paganini, P. (2014, December 01). *Regin: State-Sponsored Malware or Cybercrime?* Retrieved from InfoSec: https://www.infosecinstitute.com/resources/malware-analysis/regin-state-sponsored-malware-cybercrime/

Ries, U. (2009, July 31). *Black Hat: Machiavelli - Demo rootkit for Mac OS X*. Retrieved from The H security: http://www.h-online.com/security/news/item/Black-Hat-Machiavelli-Demo-rootkit-for-Mac-OS-X-742755.html

Tanner, J. (2023, June 6). *Malware 101: Worms and how they propagate*. Retrieved from Barracudas: https://blog.barracuda.com/2023/06/06/malware-101-worms

Thomas, T., Surendran, R., John, T. S., & Alazab, M. (2023). *Inteligent Mobile Malware Detection.* Broken Sound Parway NW: CRC Press.