Malware Analysis: Task 2.2C

Name of Student

Institutional Affiliation

**Question 1**

**a) Was Y2K a malware? Support your answer with a short answer of up to 50 words (refer to Week 2’s lecture).**

Y2K was not a malware but a bug. It was also known as the Year 2000 bug or Millennium Bug, a problem with computer systems coding that was planned at the beginning of 2000 to cause chaos in computers and computer nets worldwide (Raymond & Lawrence, 2000).

**b) Was Y2K a computer security problem? (refer to Week 1’s lecture where we define what is a computer security problem) Support your answer with a short answer of up to 100 words.**

Yes, it was a major security problem. Private and government organisations invested $100 billion to tackle the Y2K problem. In preparation for Y2K, devices were available and mis-coded programmes did not result in failure of energy or the disappearance of bank accounts. In the course of this period, the creation and development of new technology tools specifically developed for cyber security purposes has hit the market. As vendors began to produce and to sell applications which collects and collects events across all systems in the network, Y2 K helped form the Security Information and Event Management (SIEM) market.

**c) In your own words (up to 200 words), summaries what caused Y2K.**

In the 1960s and 1980s, computer engineers used a two-digit code for the year when complex computer programmes were written. The "19" has been denied. It read 70 instead of a date of 1970. The dates were shortened by engineers because computer data storage was expensive and space-taking. Save significant quantities of storage space just two digits during the year. Storing was unbelievably costly (Simon, 2019). For instance, more money was saved by banks, which have stored thousands of transactions every day. Y2K was both a challenge with software and hardware. Software is used to say what to do to a machine by electronic programmes. Hardware is the computer's own equipment. Computer and hardware companies have been able to patch the bug and have developed support services for "Y2K compliant."

When these programmes were written, programmers had no concern for what would happen when 2000 walked in, as all the systems had been antiquated and new systems had taken over by that time. However, these systems have never been completely eliminated and the newer systems were actually designed to be compatible with the older systems. In this way, the issue was exacerbated.

**Question 2**

**a) What type of malware was WannaCry? Support your answer referring to Week 2’s lecture**

WannaCry is a type of ransomware.

**b) Could WannaCry move across different machines? Support your answer with up to 100 words.**

In May 2017, WannaCry quickly spread across many computer networks. After a Windows device has been infected, it encrypts files on a PC's hard drive, prevents user access, then needs a ranking in bitcoin payment to decrypt them (Buchanan, 2020).

**c) How does WannaCry ensure persistency on a machine that has infected? (i.e., what actions does WannaCry take to achieve persistency on victim machine) List the tools from Task 2.1P that you could use to detect each action. (up to 200 words)**

It is crucial to understand the characteristics and the actions of various forms of ransomware in order to establish effective defence mechanisms. In the case of malicious binaries in controlled environment, dynamic analysis techniques are usually utilised to accomplish that objective. They are then observed. In this paper, dynamic findings are presented which concentrate on the infamous WannaCry ransomware.

WannaCry will not actually start encryption even if a PC is successfully infected. As mentioned above, it will try to access a gibberish URL for a very long time before it is going to function. WannaCry shuts itself off if it can access this domain. The intent of this feature is not fully clear. Some researchers thought that this should be a way to pull the plug on the attack from malware developers (Michelson, 2020). Any Windows PC that is not patched can be WannaCry-friendly. The capacity of organisations to spread across networks is especially at risk. A variety of organisations, the majority of which are in Europe, were affected worldwide. However, individuals can also be affected.

**d) Is Kali Linux vulnerable to WannaCry? Support your answer by referring to characteristics of the malware as discussed in question 2.c (up to 100 words)**

Instead of attacking only on Windows XP, Vista and later Windows OSs, there are no witnesses in GNU/Linux OSs and derived OSs. This is even due to poor safety patches.

In addition, WannaCry Ransomware focuses on businesses, corporations and even individuals whose data (for obvious reasons like databases, research projects) are very, very valuable for them who can make payments in order to preserve their data. The news reports have shown that only a limited number of people have been affected.

**e) If victims paid the ransom to hackers, could they unlock their machine? (~50 words)**

Yes, that's right. Persons or organisations, as this does not guarantee that files are released, are discouraged from payment of the ranch (Watters, 2018). However, the FBI has cautioned that the victim cannot recover their data without paying a ransom if sophisticated ransomware was involved.

**f) Without paying ransom to hackers, was it possible to decrypt the encrypted content of victim’s machine? If so, what made that possible? (~50 words)**

Yes. Some people were able to retrieve the files by using a ransomware decryptor. The decryption software was created a while after the ransomware had spread. The software decrypts content encrypted by the ransomware. However, the software decryptor arrived late which meant that people with sensitive data mostly paid to have their data back.

# **References**

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Harvard University Press.

Michelson, D. (2020). *Wannacry Ransomware Attack: Learning the Essentials.* First Rank Publishing.

Raymond, F., & Lawrence, J. (2000). *Y2K Aftermath--crisis Averted: Final Committee Report.* The Committee.

Simon, F. (2019). *The Y2K Bug: A Novel Review.* Broadman & Holman.

Watters, P. (2018). *Defeating Ransomware: Wannacry and Other Challenges.* CreateSpace Independent Publishing Platform.