Week 3 Task 3.2C

Task 1

a) Y2K Millennial reflections on computers as infrastructure.pdf Using the above paper and your own research, answer the following questions In your own words (up to 200 words), summaries Y2K.

- The way early computer systems maintained dates let to a severe problem known as the year 2000 problem, sometimes known as the millennium Bug or Y2K. In the early days of computing, memory was a valuable resource, thus programmers used two numbers to represent the year such as “99” for 1999.concerns about these systems misinterpreting the year 2000 as 1900 rather than 2000 as 2000 drew nearer intensified as it seemed more likely that massive system failures would result. These malfunctions could have unanticipated and perhaps disastrous effects on a number of vital infrastructures, such as the military, banking and transportation networks.

  Businesses and governments throughout the world scrambled to find and address Y2K-related problems in their embedded systems and software as the year 2000 drew closer. The problem was enormous in scope, encompassing millions of lines of code and multiple legacy systems, many of which lacked original programmers or had little documentation. Estimates of the cost of the remediation project worldwide approach billions of dollars.

  The transition to the year 2000 happened with very few major events, despite the anxieties and extensive preparations. This was partly because of the extensive efforts made to handle the issue in the years preceding the century.

  (203 words)

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

- Since Y2K was a bug in how dates were represented in computer systems and was not purposefully made to cause harm, it is not regarded as malware. Malware, on the other hand, is specifically created to harm or interfere with systems.

  (41 words)

c) 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.

- No, there was no computer security issue with the Year 2000 problem. Threats like illegal access, data breaches, or virus attacks—which purposefully damage systems by taking advantage of vulnerabilities—are examples of computer security issues. The widespread usage of two-digit year formats in date fields contributed to the Year 2000 problem, a technological issue that might have resulted in data processing issues when the year 2000 arrived. It was an anticipated, systemic issue that didn't involve criminal intent or the exploitation of security flaws but nevertheless needed to be fixed.

(90 Words)

Task 2

a) What type of malware was WannaCry? Support your answer referring to Week 2's lecture (i.e., it's X given that ...)
   - WannaCry was classified as a crypto-ransomware that relies on worms. This classification is based on how it behaves and functions:

     ✓ Ransomware: This type of malware essentially prevented users from accessing their own data by encrypting the files on compromised systems and requesting a Bitcoin ransom to unlock the decryption key.
     ✓ Worm: It possesses a worm component that enables it to propagate through networks on its own without human assistance. It used a Windows SMB (Server Message Block) protocol vulnerability known as EternalBlue to spread swiftly and autonomously amongst computers on the same network.

b) Could WannaCry move across different machines? Support your answer with up to 100 words.
   - Indeed, WannaCry could spread among various computers. It dispersed independently between machines connected to the same network by taking use of an EternalBlue vulnerability in the Windows SMB (Server Message Block) protocol. Because of its worm-like characteristics, WannaCry spread quickly and without the help of users, infecting other weak systems after it had taken control of one. Its impact was amplified by its mobility across computers and networks, which resulted in widespread infections throughout the world.

     (76 words)

c) How does WannaCry ensure persistency on a machine that has infected? (i.e., what actions does WannCry 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)
   - WannaCry makes sure the ransomware is persistent by generating a Windows registry key that permits it to execute at system startup. At "HKCU \Software \Microsoft \Windows} \CurrentVersion\Run\vyzrjjjywpoefn971," WannaCry generates a registry key. The last portion of the key is a randomly generated identifier that is specific to each compromised machine. This key ensures persistency by allowing the ransomware to run every time the machine reboots.
   - There are several scanning techniques to find such a worm;

     ✓ Process Monitor: Used to track and record activity on the file system in real time. It lets you keep an eye on processes, CPU use, memory, and other things, so you can identify any unusual spikes in memory usage. The Linux CLI's "htop" command can be used to access it.
     ✓ Wireshark is a vital tool for network traffic monitoring in order to identify unusual patterns or connections, like the ones that WannaCry used to compromise compromised servers. This can assist in determining the ransomware's communication efforts.

     (161 words)

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)

- No, WannaCry cannot infect Kali Linux. WannaCry targets Windows operating systems in particular by taking advantage of the EternalBlue vulnerability in the Windows SMB (Server Message Block) protocol. Kali Linux does not support the Windows SMB protocol in the same way as Debian because it is built on Debian and uses a different kernel architecture and protocols; as a result, the EternalBlue exploit cannot be used with Kali Linux. Furthermore, WannaCry's registry key persistence technique only works with Windows and is incompatible with Linux systems.

(85 words)

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

- It was not a guarantee that victims could unlock their computers even after paying the ransom to the hackers. Numerous victims who paid the ransom either did not receive a working decryption key or received one that was inoperable, underscoring the dangers associated with dealing with ransomware operators and the unpredictability of criminals' demands.

(54 words)

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)

- It was true that in certain circumstances it was feasible to unlock the encrypted data on a victim's computer without having to pay the ransom. The usage of static keys or the discovery of decryption keys still in memory on infected systems were two examples of the vulnerabilities in WannaCry's encryption implementation that were exploited by security researchers' tools, which permitted this.

(62 words)