**Outline**

· This is an individual assignment.

· You will be assigned one of the following virus topics.

· Research your topic to learn about computer malware and to prepare a presentation about your topic.

· Suggested Slide Topics and layout for your presentation is provided below.

· The presentation should be between 5-10 minutes and will be given in front of the class.

· Slides should be shared with Mr. Nestor (p0079141@pdsb.net) via. Google drive.

**Virus Topics**

1. CIH Virus – 1998

2. Melissa Worm – 1999

3. Code Red Worm – 2001

4. Slammer Worm – 2003

5. SoBig.F Worm – 2003

6. My Doom Worm – 2004

7. Stuxnet Worm – 2010

8. Cryptolocker Trojan – 2013

9. ZeroAccess Botnet – 2013

10. Superfish Adware – 2014

11. Locky Ransomware – 2016

12. WannaCry Ransomware - 2017

**Suggested Slide Layout**

1. Overview

· Summarize what is known about the malware

Slammer worm is a ransomware that had spread through internet usage, and has infected 75,000 servers within the first 10 minutes of being released. It slowed down internet traffic and denied access to major sites across the network.

· Provide: Year / Creator / Origin

David Litchfield created Slammer worm in 2002. He created 2 bypasses to the mechanisms built into the Microsoft SQL server.

· Its classification: Virus / Worm / Trojan / DDOS Attack / Email Phish, etc.

This ransomware is a DDOS attack that had spread through internet traffic and infected network traffic.

2. Any Other Interesting Facts

· This will be topic dependent

This worm infected 75,000 servers in a short span of ten minutes. Reports of the worm were sent in to microsoft in 2002, but the official launch of the worm was 2003 when the worm infected a lot of victims. About 250,000 computers were infected globally by the ransomware.

3. Its Targets

· Target Hardware Type: e.g. PC, Network, Smartphone, etc.

The target hardware that slammer worm was targeting to execute the worm, was in servers and did not impact home computers as much. Since slammer worm had very few lines of code, this allowed the worm to stay in the memory of the device.

· Target Operating System: e.g. Windows, Mac, Android, etc.

Any server or computer operating system. This worm can operate in servers, as well as infect any device that has access to that server and receives data from.

· Target Software Applications

This worm did not target any software applications, mainly because its purpose was to slow down internet traffic, and make pages unresponsive to use. This worm can be easily removed, and it is a RAM based worm.

4. What it Did

· What it did to Computer Hardware

This worm was not of any harm to any computer or server hardware.

· What it did to Computer Software

This worm was not of any harm to any computer software or programs running in the machines.

· What it did to Computer Data

This worm did not produce any harm to any computer data, since this worm dealt with slowing down the transfer of data, and not altering it in any way.

5. How it Worked

· How did it get into a computer

It got into a computer by receiving data from the servers that got infected by the ransomware.

· How did it spread between computers

Slammer worm spread between computers because slammer worm infected servers. This then connected to computers and infected them. Slammer worm would replicate itself inside the servers to infect other servers in milliseconds.

6. Its Effect

· Summarize its Financial impact

This worm slowed down network traffic, and then that would make companies lose a bit of money, but not alot as users realize that it wasn’t the company’s fault. This also made business for other companies, offering to remove the worm by clearing the cache from the RAM that was installed in the computer.

· Summarize its User Base impact

This worm slowed down network traffic, and so users experienced delays that would not be a hassle to deal with if the worm wasn’t there in the first place. Users had to reboot their computer with the new microsoft update with the patch, in order for things to go back to normal.

7. Its Control

· How was it discovered

It was discovered by the people who had their servers slowed down tremendously by the worm. This caused a great commotion and so microsoft had to implement a fix to stop the worm.

· How was it stopped

Microsoft implemented a patch into their operating system, and when the servers were restarted or rebooted, the fix was executed which got rid of the slammer worm.

· How can it be removed

It can be removed by rebooting the servers or computers, and having the microsoft update implemented into the system when the computer or server was rebooted.

Resources

<https://www.symantec.com/connect/blogs/bios-threat-showing-again>

<https://www.symantec.com/security-center/writeup/2000-122113-1425-99>

<https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/zeroaccess-indepth-13-en.pdf>