**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](mailto: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
   * Provide: Year / Creator / Origin
   * Its classification: Virus / Worm / Trojan / DoS Attack / Email Phish, etc.

Cryptolocker is a Trojan horse that encrypts files on the infected computer and then prompts the user to purchase a key in order to decrypt the files. The malware was created in 2013. The virus was written by Russian hacker Evgeniy Bogachev. It’s classification is an Email phishing Trojan virus. Trojans are a virus that appears harmless at first but is actually malicious.

1. Any Other Interesting Facts

The creator Evgeniy Bogachev was involved with making another malware called GameOver Zeus. Many victims who paid the ransom claimed to not get their data back.

1. Its Targets
   * Target Hardware Type: e.g. PC, Network, Smartphone, etc.
   * Target Operating System: e.g. Windows, Mac, Android, etc.
   * Target Software Applications

Cryptolocker targets PCs that use the Windows operating system.

1. What it Did
   * What it did to Computer Hardware
   * What it did to Computer Software
   * What it did to Computer Data

Once the virus infected computers it encrypted the computer’s files and prompted users to send bitcoin to the hacker or their files would be deleted by a deadline.

1. How it Worked
   * How did it get into a computer
   * How did it spread between computers

It attacked computers by disguising itself in familiar file formats like .docx or .pdf but they included a hidden .exe that opens a downloader to infect your computer. It was spread through emails.

1. Its Effect
   * Summarize its Financial impact
   * Summarize its User Base impact

Cryptolocker infected over 500,000 PCs and made over 3 million dollars from the ransomware.

1. Its Control
   * How was it discovered
   * How was it stopped
   * How can it be removed

The virus was discovered in September 2013. The virus was stopped by security firms and they found the person responsible for the virus. A security firm called Fox-IT created a website called decryptcryptolocker.com for people with computers that got infected to get a free key to decrypt the virus.

Resources

<https://www.bbc.com/news/technology-28661463>

<https://www.symantec.com/security-center/writeup/2013-091122-3112-99>

<https://www.securityweek.com/cryptolocker-infections-rise-us-cert-issues-warning>