**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
13. Overwrite Virus

**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.

This Virus spreads to computers and rewrites random data over existing documents. The Virus usually infects files within the systems memory where all the important system information is stored. The virus may infect images, files, documents, and videos by overwriting it with random data. Once infected, the file is no longer available and you cannot recover anything as all the data has been erased. The virus can only be removed by deleting all infected files thus, losing all your work. The only way to recover your files is too redownload all original files from a backup source.

1. Any Other Interesting Facts
   * This will be topic dependent
2. Its Targets
   * Target Hardware Type: e.g. PC, Network, Smartphone, etc.
   * Target Operating System: e.g. Windows, Mac, Android, etc.
   * Target Software Applications

The Virus has been known to exploit a wide range of operating systems including Linux, Macintosh, Windows and DOS platforms. It enters your system by USB or by downloads off the internet. Someone may leave a USB which contains the Virus out in the open for someone to  pick up. Someone may take the USB home and plug it into their computer. Once plugged in the Virus spread to the system memory and rewrites many files with random data. Another way this Virus can enter your system is if you download an unknown file from the internet. Virus hosts have become creative and may use a popup ad to make you download their file. The ad may look something like this which makes you download the virus thinking your downloading something to protect you from it.

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

What this Virus does is that it takes existing files, images, videos and documents and rewrites random data over them. The files which have been infected by this virus are unrecoverable as the virus rewrites data but does not save the previous codes.

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

This gets into computers either if you download a file from the internet which contains this virus, or if you plug in a USB chip which contains the virus.

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

This has a big effect on who ever downloads this virus. This is because tall the files that get effected are unrecoverable and are lost forever. If someone has a work computer with important information on it, they can lose all documents and if so, may have a financional impact. This is one of the most dangerous viruses.

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

This virus was discovered in 1992 when people began losing files they had saved on their computers. This Virus was not known about and was new at the time. Files began getting infected and OS’s started to get damaged which led to the discovery of this virus. This virus can only be removed if you delete all infected files. This will lead to you lose documents or files that you need. The files can only be recovered if they were saved on an external backup source.

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>