**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.

Superfish Adware is classified as a spyware and adware that was preinstalled onto some Lenovo laptops. It was installed onto laptops between September 2014 and February 2015. It has the ability to break the HTTPS encryption. It also produces self-signed certificates that can possibly allow any malicious third person to intercept the SSL or TLS connections. It also gets access to your information, such as personal information, knows what you are viewing, and tracks user’s website traffic.

1. Any Other Interesting Facts
   * This will be topic dependent

Lenovo had preinstalled it onto their computers. Lenovo was tricked by Superfish about what the program actually does. Superfish said that it’ll analyze images on the web and present lower prices. There were certificates that issued by themselves, not by the Bank of America.

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

The targets by Superfish were the computers sold by Lenovo between September 2014 and February 2015. It affected all their window computers. Browsing applications, such as Google Chrome, Internet Explorer, and Safari, were targeted. Some affected models were: E10-30. Flex2 14, Flex2 15, Flex 2 14D, Flex2 15D, Flex2 Pro, Yoga2-11, Yoga2-13, Yoga2Pro-13, Yoga3 Pro.

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

The computer hardware wasn’t really affected. The data stored inside the computer was taken and used by the owners of Superfish Adware. All personal information, such as credit card information, full name, address, and email address and passwords, were leaked to the owners.

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

The program was pre-installed onto the computer. Then the information would be taken by the owners. Lots of models were infected and Lenovo was being tricked.

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

Lenovo had to spend money to remove it. Users were worried about personal information as their money could be stolen. They can purchase things from credit cards users own. Lenovo may have been sued for the big mistake that they had made by trusting Superfish.

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

People started discovering it early 2015. It was removed by the user themselves. You had to delete the program from the program list, the certificate of the program from the certificate list, and then you would be safe. Lenovo offered users a program that uninstalls Superfish Adware on their website. They also provided manual instructions for users who want to do it themselves.

**Works Cited**

<https://malware.wikia.org/wiki/Superfish>

<https://www.tripwire.com/state-of-security/security-data-protection/superfish-lenovo-adware-faq/>

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>