**ICS2O0 Slides C.4 Virus Presentation Name:**

**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

-[Peer-to-peer (P2P)](https://searchnetworking.techtarget.com/definition/peer-to-peer) botnets have a random organization and operate without a C&C server.

Today its ones of the largest botnets, infecting up to a computer population of 1.9 million.

-The primary motivation of this threat is to make money through [pay per click](http://en.wikipedia.org/wiki/Pay_per_click) advertising. It does this by downloading an application that conducts Web searches and clicks on the results. This is known as [click](http://en.wikipedia.org/wiki/Click_fraud) fraud, which is a highly lucrative business for malware creators.

-downloading other threats on to the compromised computer, some of which may be Misleading Applications that display bogus information about threats found on the computer and scare the user into purchasing [fake antivirus software](http://www.symantec.com/security_response/writeup.jsp?docid=2007-101013-3606-99) to remove the bogus threats. It is also capable of downloading updates of itself to improve and/or fix the functionality of the threat.

- download software onto compromised computers in order to mine [bitcoins](http://en.wikipedia.org/wiki/Protocol_of_Bitcoin) for the malware creators. Bitcoin mining with a single computer is a futile activity, but when it is performed by leveraging the combined processing power of a massive botnet, the sums that can be generated is considerable.

-it opens a back door and connects to a command and control (C&C) server, which allows the remote attacker access to the compromised computer. The attacker is then able to perform any number of actions on the computer, and the computer may then become part of a wider botnet.

-It is able to achieve the above functions silently as it infects a system driver that acts as a rootkit hiding all of its components on the computer. The threat creates an encrypted hidden volume in the computer's file system where it stores all of its components. Not only does it store all of its components in the hidden volume, but it can also hide any other malicious software that it downloads onto the computer there as well.

-There are primarily two types of payload, both aimed at revenue generating activities; click fraud and bitcoin mining. Click fraud modules download online advertisements onto the computer and then generate artificial clicks on the ads as though they were generated by legitimate users. Bitcoin mining is based on performing mathematical operations on computing hardware. This activity has a direct value to the botmaster and a cost to unsuspecting victims.

-The primary motivation behind ZeroAccess is financial fraud through pay-per-click (PPC) advertising.

* + Provide: Year / Creator / Origin

It was first released in May 2011 but that was the first version. The second version came out in 2012. However, this malware was at its peak in August 2013 infecting up to 1.9 million computers, whereas the first version only infected up 30 thousand.

* + It's classification:

Trojan- A Trojan hides malware in files that seem to be normal. This virus usually targets at taking control of the computer, stealing information and inserting more malware onto the computer.

1. It's Targets
   * Target Hardware Type: e.g. PC, Network, Smartphone, etc.
   * Target Operating System:
   * Target Software Applications

Its target hardware type is mainly just regular desktops and laptops due to their vulnerability in the operating system. The operating system that the Trojan only affects is only Windows. This means that anyone with a windows computer will be vulnerable to the virus. Its target Software application is online browsers like Firefox, Google Chrome and Internet Explorer. This means that you can be easily infected with the Trojan if you are not careful of what browse on the internet or emails. It can also spread across your network as it can search extensively for files to encrypt.

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

Cryptolocker does not affect any hardware parts or computer software. Once the Trojan is implemented, then you will be having a warning screen with a time limit. This time limit is the time which is when the ransom should be paid by and when your flies will be deleted. Data is heavily affected as if the ransom is not paid, all of your computer data will be deleted. Furthermore, hackers could encrypt the data which means they can use your data for other uses.

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

The most common method of infection is via emails with unknown attachments. Although the attachments often appear to be familiar file types such as \*.doc or \*.pdf, they, in fact, contain a double extension — a hidden executable (\*.exe). Once opened, the attachment creates a window and activates a downloader, which infects your computer. Because the program is a Trojan, it cannot self-replicate, meaning it must be downloaded to infect your computer. In addition to malicious email attachments, this malware may also come from websites that prompt you to download a plug-in or video player. Typically, you will see nothing wrong with your computer until all files have been encrypted. Then, a warning will pop up indicating that you have been infected and showing a countdown timer until all your data is destroyed. Many antivirus programs can remove this Trojan but are unable to decrypt your data. In some cases, users have re-installed the Trojan after removal in order to pay the ransom and unlock their data. Cryptolocker can cause serious damage to personal and business computers. By always creating a physically separate backup of critical files, regularly running antivirus scans and avoiding unknown email attachments, you can minimize the chance of infection.

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

Between September 2013 and June 2014, a virus known as CryptoLocker infected around **500,000 computers** around the world. Designed to lock data on a victim's computer and hold it for ransom, it ended up extorting an estimated $3 million from victims who agreed to pay rather than lose their files.

1. It's Control
   * How was it discovered

The CryptoLocker ransomware attack was a cyber attack using the CryptoLocker [ransomware](https://en.wikipedia.org/wiki/Ransomware) that occurred from 5 September 2013 to late May 2014. The attack utilized a [trojan](https://en.wikipedia.org/wiki/Trojan_horse_(computing)) that targeted computers running [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows)and was believed to have first been posted to the Internet on 5 September 2013.It propagated via infected email attachments, and via an existing [Gameover ZeuS](https://en.wikipedia.org/wiki/Gameover_ZeuS) [botnet](https://en.wikipedia.org/wiki/Botnet). When activated, the malware [encrypted](https://en.wikipedia.org/wiki/Encryption) certain types of files stored on local and mounted network drives using RSA [public-key cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography), with the private key stored only on the malware's control servers. The malware then displayed a message which offered to decrypt the data if a payment (through either [bitcoin](https://en.wikipedia.org/wiki/Bitcoin) or a pre-paid cash voucher) was made by a stated deadline, and it threatened to delete the private key if the deadline passes. If the deadline was not met, the malware offered to decrypt data via an online service provided by the malware's operators, for a significantly higher price in bitcoin. There was no guarantee that payment would release the encrypted content.

* + How was it stopped

CryptoLocker was isolated in late May 2014 via [Operation Tovar](https://en.wikipedia.org/wiki/Operation_Tovar), which took down the [Gameover](https://en.wikipedia.org/wiki/Gameover_ZeuS) Zeus [botnet](https://en.wikipedia.org/wiki/Botnet) that had been used to distribute the malware. During the operation, a security firm involved in the process obtained the database of private keys used by CryptoLocker, which was in turn used to build an online tool for recovering the keys and files without paying the ransom. It is believed that the operators of CryptoLocker successfully extorted a total of around $3 million from victims of the trojan. Other instances of encryption-based ransomware that have followed have used the "CryptoLocker" name (or variations), but are otherwise unrelated.

* + How can it be removed

Although CryptoLocker itself was easily removed, the affected files remained encrypted in a way which researchers considered hard to break. Many said that the [ransom](https://en.wikipedia.org/wiki/Ransom) should not be paid, but did not offer any way to recover files; others said that paying the ransom was the only way to recover files that had not been [backed up](https://en.wikipedia.org/wiki/Backup). Some victims claimed that paying the ransom did not always lead to the files being decrypted.