**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

-A peer-to-peer [botnet](https://searchsecurity.techtarget.com/definition/botnet) is a decentralized group of [malware](https://searchsecurity.techtarget.com/definition/malware)-compromised machines working together for an attacker’s purpose without their owners’ knowledge.

-[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 fraud](http://en.wikipedia.org/wiki/Click_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 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, 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.

* + Its 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. Any Other Interesting Facts
   * This will be topic dependent
2. Its Targets
   * Target Hardware Type: e.g. PC, Network, Smartphone, etc.

It targeted computers

* + Target Operating System: e.g. Windows, Mac, Android, etc.
  + Target Software Applications

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

It was able to steal, encrypt, and delete data off of a computer.

1. How it Worked
   * How did it get into a computer
   * How did it spread between computers
2. Its Effect
   * Summarize its Financial impact
   * Summarize its User Base impact
3. Its Control
   * How was it discovered
   * How was it stopped
   * How can it be removed