**Part 1: Individual Research**

1. Create a group of 5 students maximum.
   * A group of fewer than 5 will require double work.
   * A group of more than 5 is not permitted.
   * Select your group members for reliability and collaboration skills.
2. Assign each member of your group a malware type topic from the list below.
   * Viruses & Worms
   * Trojans, Rootkits & Botnets
   * Ransomware
   * Adware, Malvertising & Spam
   * Spyware
3. Provide the names of your group members and their assigned topic to Mr. Nestor.
4. Information to get you started for each topic is provided at the end of this lesson document.
5. Create a portfolio about your topic. A portfolio is a collection of high quality web resources that includes the following:
   * References to web pages from trusted sources.
   * Links to informative videos that are specific to one idea or topic.
   * Links to news reports or journalistic articles
   * Links to infographics, images, or other graphic elements
   * The resources must be of high-quality
   * Links to the resources may be stored in a Word or PowerPoint document, etc.
6. Note: You do not have to summarize or write your own content. Your assignment will be evaluated on your selection of high-quality resources
7. The audience for your portfolio will be to teach your other group members about your topic.
   * It will be uploaded to GitHub in Part 2 of this assignment
   * **Be Prepared To Teach Your Malware Topic To Other Members Of Your Group**

**An outline for your portfolio is as follows:**

1. Introduction To Your Malware Type. You should have at least one quality resource for each topic.
   1. What it does to an infected computer / user

<https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>

<https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html>

<https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html>

* 1. How it infects a computer

<https://enterprise.comodo.com/how-do-you-get-trojan-virus.php>

<https://www.guidingtech.com/4467/what-is-a-rootkit/>

<https://www.pandasecurity.com/mediacenter/security/what-is-a-botnet/>

* 1. How it spreads

<https://enterprise.comodo.com/how-are-trojan-horses-spread.php>

<https://securingtomorrow.mcafee.com/consumer/identity-protection/what-is-rootkit/>

<https://techtalk.gfi.com/explaining-botnets/>

* 1. How it is different from other types of malware

<https://www.webopedia.com/DidYouKnow/Internet/virus.asp>

<https://www.quora.com/What-is-the-difference-between-malware-a-virus-trojans-rootkits-etc>

<https://staysafeonline.org/stay-safe-online/online-safety-basics/malware-and-botnets/>

* 1. How to detect this type of malware

<https://enterprise.comodo.com/forensic-analysis/how-to-detect-trojan-virus-on-computer.php>

<https://www.varonis.com/blog/rootkit/>

<https://www.welivesecurity.com/2014/10/22/botnet-malware-fight/>

* 1. How to remove this type of malware

<https://enterprise.comodo.com/what-to-do-if-you-get-a-trojan-virus.php>

<https://www.wikihow.com/Remove-a-Rootkit>

<https://www.technadu.com/how-to-detect-prevent-and-remove-botnet-malware/28381/>

1. News report(s) of specific case/outbreak of your malware
   1. Summarize what happened

**Kovter** is a Trojan, which has been observed acting as click fraud malware or a ransomware downloader. It is disseminated via malspam email attachments containing malicious office macros. Kovter is fileless malware that evades detection by hiding in registry keys. Some reports indicate that Kovter infections have received updated instructions from command and control infrastructure to serve as a remote access backdoor.

* 1. When and where it happened

Kovter first appeared in 2016 in the online browsers [**Google Chrome**](http://www.securityweek.com/kovter-trojan-gets-new-persistence-mechanism) and [**Mozilla Firefox**](http://www.securityweek.com/fileless-trojan-kovter-poses-firefox-update)’s updates.

* 1. Its affects: computers infected / countries attacked / financial damage

Originally, Kovter was distributed as a ransomware variant that locked victims' and threatened law enforcement response. In more recent campaigns, Kovter has been used for click-fraud and malicious advertising to generate funds for its developers.

* 1. Who was responsible (if available)

N/A