**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.

Ritik – Ransomware

Ibrahim – Viruses & Worms

Harman – Spyware

Martin – Trojans, Rootkits & Botnets

Dinesh – Adware, Malvertising & Spam

1. Information to get you started for each topic is provided at the end of this lesson document.
2. 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.
3. Note: You do not have to summarize or write your own content. Your assignment will be evaluated on your selection of high-quality resources
4. 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

**Covers most of topics:** <https://security.berkeley.edu/faq/ransomware/>.

* 1. What it does to an infected computer / user

<https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html>

* 1. How it infects a computer

**(INFOGRAPHIC)** <https://enterprise.comodo.com/forensic-analysis/how-does-ransomware-get-on-your-computer.php>

* 1. How it spreads

<https://www.datto.com/blog/how-ransomware-is-spread>

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

<https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/malware-vs-viruses.html>

* 1. How to detect this type of malware

<https://enterprise.comodo.com/forensic-analysis/how-do-i-know-if-i-have-ransomware-in-my-pc.php>

* 1. How to remove this type of malware

**(VIDEO)** <https://www.youtube.com/watch?v=NKW64z7H9qE>

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

<https://fortune.com/2017/05/14/ransomware-wannacry-faq/>

* 1. Summarize what happened
  2. When and where it happened
  3. Its affects: computers infected / countries attacked / financial damage
  4. Who was responsible (if available)

**Part 2: Group Collaboration**

1. Create a folder in your GitHub repository for your group
   * The folder should be titled "Malware Types"
   * Upload all your group member presentations to this folder
   * Share this folder with all your group members
   * Note: This can be done by only person in your group an you can all share the one folder.
2. Use the five different presentations created by your group to complete part 2 of the lesson.
   * details are T.B.D.

**1. Viruses & Worms**

**Viruses**

Viruses were the most common type of malware in the 1990s with the introduction of Email attachments. One person would open an infected email and the entire company would be infected in short order.

A computer virus is what most of the media and regular end-users call every malware program reported in the news. Fortunately, most malware programs aren't viruses. Pure computer viruses are uncommon today, comprising less than 10 percent of all malware.

A computer virus is the only type of malware that "infects" other files and programs. A virus modifies legitimate data files (like a Word docs) in such a way that when a victim's file is executed (i.e. by opening it in Microsoft Word), the virus is also executed.

This makes viruses particularly hard to clean up because the malware is executed from a legitimate (i.e. non-infected) program. Even the best antivirus programs struggle with removing viruses correctly and in many (if not most) cases will simply quarantine or delete the infected file instead.

Viruses spread through script files, and documents (i.e. attachments) shared through the use of web apps. Viruses are also capable of copying themselves and spreading to other computers. Viruses often spread in this way by attaching themselves to programs and executing code when a user opens a document related to the infected programs.

Viruses can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.

**Worms**

Computer worms can be classified as a type of computer virus, but there are several characteristics that distinguish computer worms from regular viruses. A major difference is that computer worms have the ability to self-replicate and to spread by themselves while viruses rely on human activity to spread (i.e. running a program, opening a file, etc).

Although worms can spread through emails with infected attachments, they usually spread by themselves over computer networks by exploiting operating system vulnerabilities. These vulnerabilities are design weaknesses (logic errors) or bugs (run-time errors) in the code of legitimate programs (e.g. Microsoft Word) or operating systems (e.g. Microsoft Windows).  Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers.

Worms can also contain “payloads” that are intended to cause specific damage host computers. Payloads are pieces of code written to perform actions on affected computers beyond simply spreading the worm. Payloads are commonly designed to steal data, delete files, or create botnets.

**2. Trojans, Rootkits & Botnets**

**Trojans**

Computer worms have been replaced by [Trojan horse](https://www.csoonline.com/article/3403381/what-is-a-trojan-horse-how-this-tricky-malware-works.html) malware programs as the weapon of choice for hackers. Trojans are popular with cyber criminals for two reasons: They're easy to write and they are easy to spread by tricking end-users.

Trojans appear to be legitimate programs, but they contain malicious instructions. The most popular Trojan type is the fake antivirus program, which pops up and claims you're infected, then instructs you to run a program to clean your PC. Users swallow the bait and the Trojan takes root. Trojans also easily spread through web sites that encourage the downloading of pirated software, game patches, and video files. A Trojan must be executed by its victim to do its work.

A Trojan can give an attacker remote access to an infected computer. Once an attacker has access to an infected computer, it is possible for the attacker to steal data (logins, financial data, even electronic money), install more malware, modify files, monitor user activity (screen watching, keylogging, etc), use the computer in botnets, and anonymize internet activity by the attacker.

**Rootkits**

A [rootkit](https://www.veracode.com/security/rootkit) is a type of stealth program designed to remotely access or control a computer without being detected by users or security programs. A rootkit modifies the underlying operating system to take ultimate control of the computer. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer as part of a botnet.

Rootkit prevention, detection, and removal can be difficult due to their stealthy operation. Because a rootkit continually hides its presence, typical security products are not effective in detecting and removing rootkits. As a result, rootkit detection relies on manual methods such as monitoring computer behavior for irregular activity. Organizations and users can protect themselves from rootkits by regularly patching vulnerabilities in software, applications, and operating systems, updating virus definitions, avoiding suspicious downloads, and performing static analysis scans.

**Botnets**

Bots are infected computers that become part of a larger malicious network. [Botnets](https://www.csoonline.com/article/3240364/hacking/what-is-a-botnet-and-why-they-arent-going-away-anytime-soon.html) range in size from a few thousand compromised computers to huge networks with hundreds of thousands of systems under the control of a single botnet master. These botnets are often rented out to other criminals who then use them for their own criminal purposes.

Botmasters have one or more "command and control" servers that send out instructions to infected bot computers. Bots can be used for DDoS (Distributed Denial of Service) attacks, as spambots that render advertisements on websites, as web spiders that scrape server data, and for distributing malware disguised as popular search items on download sites. Websites can guard against bots with CAPTCHA tests that verify users as human.

**3. Ransomware**

Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom. Ransomware is now the most common type of malware because of its pay off using cryptocurrency and due to its ability to attack large companies, hospitals, police departments, and [even entire cities](https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html).

Ransomware typically spreads like a normal computer worm ending up on a computer via a downloaded file or through some other vulnerability in a network service. The malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove the restrictions and regain access to their computer.

A typical ransomware programs look for and encrypt users’ files within a few minutes of infection. However, some more advanced programs are appearing that take a “wait-and-see” approach. By watching the user for a few hours before setting off the encryption routine, the malware admin can figure out exactly how much ransom the victim can afford and also be sure to delete or encrypt other supposedly safe backups.

Ransomware can be prevented just like every other type of malware program, but once executed, it can be hard to reverse the damage without a good, validated backup. According to some studies, about a quarter of the victims pay the ransom, and of those, about 30 percent still do not get their files unlocked. Either way, unlocking the encrypted files, if even possible, takes particular tools, decryption keys and more than a bit of luck. The best advice is to make sure you have a good, offline backup of all critical files.

**4. Adware, Malvertising & Spam**

**Adware**

A[dware](https://www.csoonline.com/article/3406422/what-is-adware-how-it-works-and-how-to-protect-against-it.html) is a form of malware which attempts to expose the end-user to unwanted and potentially malicious advertising. A common adware program might redirect a user's browser searches to look-alike web pages that contain other product promotions.

Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements. Common examples of adware include pop-up ads on websites and advertisements that are displayed by software. Often times software and applications offer “free” versions that come bundled with adware. Most adware is sponsored or authored by advertisers and serves as a revenue generating tool. While some adware is solely designed to deliver advertisements, it is not uncommon for adware to come bundled with spyware that is capable of tracking user activity and stealing information. Due to the added capabilities of spyware, adware/spyware bundles are significantly more dangerous than adware on its own.

**Malvertising**

M[alvertising](https://www.csoonline.com/article/3373647/what-is-malvertising-and-how-you-can-protect-against-it.html) is the use of legitimate ads or ad networks to secretly deliver malware to unsuspecting users’ computers. For example, a cybercriminal might pay to place an ad on a legitimate website. When a user clicks on the ad, code in the ad either redirects them to a malicious website or installs malware on their computer. In some cases, the malware embedded in an ad might execute automatically without any action from the user, a technique referred to as a “drive-by download.”

Cybercriminals have also been known to compromise legitimate ad networks that deliver ads to many websites. That’s often how popular websites such as the New York Times, Spotify and the London Stock Exchange have been vectors for malicious ads, putting their users in jeopardy.

The goal of cybercriminals who use malvertising is to make money. Malvertising can deliver any type of money-making malware, including ransomware, cryptomining scripts or banking Trojans.

**Spam**

Spam is the electronic sending of large numbers of unwanted messages. The most common medium for spam is email, but it is not uncommon for spammers to use instant messages, texting, blogs, web forums, search engines, and social media. While spam is not actually a type of malware, it is very common for malware to spread through spamming. This happens when computers that are infected with viruses, worms, or other malware are used to distribute spam messages containing more malware. Users can prevent getting spammed by avoiding unfamiliar emails and keeping their email addresses as private as possible.

**5. Spyware**

[Spyware](https://www.csoonline.com/article/3384100/what-is-spyware-how-it-works-and-how-to-prevent-it.html) is most often used by people who want to check on the computer activities of loved ones. Criminals can also use spyware to log the keystrokes of victims and gain access to passwords / account information or financial / intellectual property. Spyware often has additional capabilities as well, ranging from modifying security settings of software or browsers to interfering with network connections.

Spyware spreads by exploiting software vulnerabilities, bundling itself with legitimate software, or in Trojans. Spyware programs are usually the easiest to remove, often because they aren't nearly as hidden in their intentions as other types of malware. A much bigger concern than the actual spyware is the mechanism it used to exploit the computer or user. This is because the presence of a spyware program should serve as a warning that the computer has a weakness that could be exploited by other types of malware.