**Part 1: Individual Research**

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

It runs in the back and allows the hacker access to your personal information, email, bank account, passwords, internet history, ip address, photos etc. You may not know that your computer is under attack by spy ware so you should always run an anti-virus program. Spyware can also make your computer slower causing it to crash, overheat , making it unusable <https://www.youtube.com/watch?v=-Z3pp14oUiA>

* 1. How it infects a computer

Spyware is sneaky. It finds its way on to your computer without your knowledge or permission, attaching itself to your operating system. You might even inadvertently permit spyware to install itself when you agree to the terms and conditions of a seemingly legitimate program without reading the fine print. Spy ware can also enter your system through phishing, hackers may send emails to you with links that may be enticing to click, when you click those links the spyware downloads into your computer. Spyware authors love to present their spyware programs as useful tools to download. It might be an Internet accelerator, new download manager, hard disk drive cleaner, or an alternative web search service <https://www.malwarebytes.com/spyware/>

* 1. How it spreads

Spyware does not necessarily spread through out the computer instead when it is installed into your computer it is able to track all of your files, and personal information. Although the way it spreads onto computers is through downloads, phishing emails, legitimate applications and sketchy websites

<https://www.nortonsecurityonline.com/security-center/spyware.html>

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

Spyware and adware  collect information about you without appropriate notice and consent. Whereas    A computer virus spreads software, usually malicious in nature, from computer to computer. In short, spyware is a specific type of unwanted software that covertly collects your information. A virus is a specific way software can be covertly distributed, often by e-mail.  Both spyware and viruses can cause damage to your computer or cause you to lose important data but specifically spy virus like to collect you data.

<https://www.microsoft.com/security/blog/2006/11/02/whats-the-difference-between-spyware-and-a-virus/>

* 1. How to detect this type of malware?

Spyware is designed not to cause computer glitches, so it can go undetected for a long time because there’s usually no warning sign of an infection. The victim will never have a knowledge that spyware is lurking in the computer until the personal details are used for unauthorized transactions.  StartUp by typing Msconfig in the Windows search bar. If you notice any suspicious software running in StartUp consuming a substantial amount for memory, temporarily terminate its process. If you’re unsure what the program is, search for it online. Also you will notice that your computer has a spyware virus when it starts to become slower, spyware runs in the back and usually effects the performance of your computer.

<https://enterprise.comodo.com/check-for-spyware.php>

**How to remove this type of malware**  
**Spyware** is any sort of application that hides in the background and either manipulates or tracks your Web browsing experience. Spyware that tracks you in order to serve up advertising is also called **adware**. To remove this virus you will have to use a anti-spyware software will scan your computer and look for evidence of spyware applications. Most anti-spyware applications will quarantine anything they identify as spyware automa tically. Next, most of the applications will allow you to review the spyware applications found on your machine before you delete them. It's usually a good idea to delete spyware once you detect it.

<https://electronics.howstuffworks.com/how-to-tech/how-to-scan-for-and-remove-spyware1.htm>

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

A spyware attack has impacted approximately 1,400 mobile devices. Citizen Lab for [its part said](https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/) that during its investigation it identified over 100. After the attack the [WhatsApp’s owner Facebook is filing a lawsuit against the NSO Group](https://threatpost.com/facebook-sues-nso-whatsapp-hack/149661/) for allegedly hacking WhatsApp back in May.

* 1. When and where it happened

This attack had occurred earlier in 2019 and cyber security experts at the Citizen Lab, an academic research group based at the University of Toronto’s Munk School, helped them launch the investigation into the alleged hack. Overall it attacked whatsapp users in 20 different countries.

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

Since consumers trust Whatsapp with there personal text message so they will possibly being sued by those consumers since their information is now out there. There is also a lawsuit against the NSO group that has an undisclosed amount of money. There were 20 countries attacked.

* 1. Who was responsible (if available)

The NSO group is responsible for the attack on whatsapps 1400 users.

**Part 2: Group Collaboration**

1. Create a folder in your GitHub repository for your group.
   * Note: He following instructions can be done by only person in your group.
   * All of your group members can share the one folder.
   * The folder should be named "***Malware Types***".
   * All group member portfolios will be uploaded to this folder.
   * Share this folder with all your group members
2. Save your portfolio with the name “***Your First Name – Malware Type***”   
   (e.g. MrNestor – Ransomware.doc)
3. Upload your portfolio to the Malware Types folder created for your group.
   * Your folder should contain 5 different portfolios created by 5 members of your group
4. Record the GitHub link to your “Malware Types” folder.
   * Write the link down on the template handout provided in class
5. Use the five different portfolios created by your group to complete the table of questions in the template handout.
   * Work together as a group to complete each malware type in order
   * The ***author*** of the malware type portfolio teaches other group members about what they have found out.
   * The ***learner*** group members summarize (in words) their answers to the template questions.
   * The roles are switched for each malware type portfolio.
6. Hand in the completed template for individual evaluation.

**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.