**Viruses and Worms**

**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**

Some computer viruses are programmed to harm your computer by damaging programs, deleting files, or reformatting the hard drive. Others simply replicate themselves or flood a network with traffic, making it impossible to perform any internet activity.

* 1. **How it infects a computer**

Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed. This means that a virus can remain dormant on your computer, without showing major sings or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do. While some viruses can be playful in intent and effect, others can have profound and damaging effects, such as erasing data or causing permanent damage to your hard disk, and worst yet, some are even design with financial gains in mind. (Norton)

* 1. **How it spreads**

In today’s constantly connected world you can contract a computer virus in many ways, some more obvious than others. Viruses can be spread through email and text message attachments, Internet file downloads, social media scam links, and even your mobile devices and smartphones can become infected with mobile viruses through shady App downloads. Viruses can hide disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files. To avoid contact with a virus it’s important to exercise caution when surfing the web, downloading files, and opening links or attachments. As a best practice, never download text or email attachments that you’re not expecting, or files from websites you don’t trust. (Norton)

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

Viruses are a specific type of malware (designed to replicate and spread), while malware is a broad term used to describe all sorts of unwanted or malicious code. Malware can include viruses, spyware, adware, nagware, trojans, worms, and more. However, because viruses (and to a lesser extent, trojans and worms) made headlines a few years ago, most security companies focused their marketing on them, which is why they're called "antivirus."

* 1. **How to detect this type of malware**
* A very slow running computer
* Pop-up messages that appear out of nowhere and are hard to get rid of
* Computer programs starting that you don’t recognize or didn’t start up yourself
* You can hear the sound of the hard drive in constant action
  1. **How to remove this type of malware**
* Install anti-virus software and firewall
* Track potential data exfiltration at the edge and attacks at the point of entry
* Remember to regularly install security patches
* Monitor and analyze file and user behavior
* Leverage security analytics to spot suspicious behavior
* Set up alerts to notify you automatically and immediately when an anomaly occurs

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

In 2017, the WannaCry worm attack caused damage worth hundreds of millions to billions of dollars. Also known as WannaCry ransomware, this attack is a hybrid of ransomware and a worm – specifically cryptoworm.

* 1. **When and where it happened**

The WannaCry attack affected NHS services in the week from 12 May to 19 May 2017.

It was a universal attack, which involved most countrys.

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

WannaCry searches for and encrypts 176 different file types and appends. WCRY to the end of the file name. It asks users to pay a US$300 ransom in bitcoins. The ransom note indicates that the payment amount will be doubled after three days. If payment is not made after seven days, it claims the encrypted files will be deleted. However, Symantec has not found any code within the ransomware which would cause files to be deleted.

* 1. **Who was responsible (if available)**

WannaCry was responsible for this attacked

The hack appears to have originally been discovered by the NSA, which allegedly kept it on file as a potential tool to use for surveillance or other issues. We found out about it because a group of hackers, known as Shadow Brokers, in April released a cache of stolen NSA documents on the internet, including details about the WannaCry vulnerability.

**RESOURCES**  
<https://www.kaspersky.co.in/resource-center/threats/viruses-worms>

<https://www.varonis.com/blog/what-is-a-computer-virus-and-computer-worm/>

<https://www.pandasecurity.com/mediacenter/malware/worms-vs-viruses-whats-difference/>

<https://ca.norton.com/internetsecurity-malware-what-is-a-computer-virus.html>

<https://www.avg.com/en/signal/how-to-get-rid-of-a-virus-or-malware-on-your-computer>

<https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack>

<https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/>

<https://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277>

<https://www.webroot.com/au/en/resources/tips-articles/computer-security-threats-computer-viruses>

<https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/>

**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.