#Malware

##What is Malware

Before we get into the intricacies of what malware we can examine, we first need to ask ourselves, “What falls under the category of Malware?” As Cisco defines it, it “refers to any intrusive software developed by cybercriminals to steal data and damage or destroy computers and computer systems” [^1]. With the potential damage caused by the misuse of the data we’d be working with, it’s essential to know what’s at stake. So legal disclaimer, any damage that this does is not our responsibility. Don’t rip the learning module out and use it for your purposes. You could damage yourself and others severely if you’re not careful.

There are a lot of different kinds of malware that we need to keep our heads on a swivel for. These include but are not limited to:

* Viruses
* Worms
* Trojans
* Spyware
* Adware
* Ransomware

Then we have the special ones:

* Fileless Malware
* Bots

For this lesson, I’ll be explaining all of these in-depth. It might seem a little long but bear with me.

###Viruses

Viruses are constructed programs that usually run off a prescripted command or program that is set to exploit vulnerabilities within a machine. More often than not, these types of malicious software are executed entirely by accident as they require some form of human interaction. It can do anything from corrupt, encrypt, delete, or move your data files. The number one defense that you can provide for your computer against these types of programs is to maintain some form of antiviral software and ensure that the virus definitions for your computer stay up to date.

Another way of preventing virus-caused destruction is to ensure that you frequently scan your computer. Best times to do this include after surfing the internet and whenever you suspect that your computer may be compromised.[^2]

###Worms

Worms are nasty little bugs that like to spread inside your computer. They don't infect other programs[^3]. Worms are simple to deal with and prevent. You want to ensure your devices are updated with the best definitions and have active firewalls and email filtering.

###Trojans

Trojans are like the rogues of the virus world. They mask themselves as legitimate programs but secretly run executable programs in the background that damage and exploit the computer.[^4] You won’t realize they are often running unless you specifically look for them. They will look like random windows system programs but will be drilling into your computer looking for sensitive or private information.

You can defend against Trojans by simply not downloading from unknown sources. If you run Windows in S Mode, you can only download Microsoft-approved applications. If you’re like me and need the ability to download applications, then be sure that those MSI or EXE files come from trusted sources.

###Spyware

I would argue that spyware is the most dangerous of all the viruses as it can directly log the keystrokes of an unsuspecting victim. Typically, your most up-to-date antivirus software should be able to track, detect, and eliminate spyware to ensure that your computer is staying as up to date as humanly possible.

###Adware

Have you ever traveled on a site, clicked a link to another part of that site, and a webpage you didn’t click on opened up instead? Or a pop-up window opens up when you didn’t want it to or even know it was going to. Those annoying minor instances come from malicious websites littered with adware. More often than not, it’s not the fault of the website. Malicious actors can reprogram links in a site to perform a series of redirects that trap users in a cycle of malicious websites. As Arcticwolf states, “these ads may lead users to download more harmful types of malware inadvertently.”[^5]

###Ransomware

Ransomware is by far the most costly of all forms of malware. It’s also the most well-known, making headlines in news outlets worldwide because of the damages caused. Instances such as (WannaCry)[[https://en.wikipedia.org/wiki/WannaCry\_ransomware\_attack][^6](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack%5D%5B%5E6)] can cause chaos all over the world and lock computers from being accessed by their owners. In most cases, the demands result in monetary gain for the people using the ransomware.

The best way to protect against ransomware is to have a current backup of your systems and critical infrastructure to minimize downtime and teach your family or employees about safe surfing habits.

##The Special Category

This section is dedicated to the particular category, mainly because they are executed in unusual ways than traditional means. This unique classification can be concerning replication, design, or execution. The two primary categories that fall within this are Fileless Malware and Bots.

###Fileless Malware

Type 1 fileless malware consists of malware that doesn’t perform file activity. This malware can include firmware, USB peripheral, or network card attacks. This malware is hearty and can survive multiple attempts to remove it via reboots, disk reformats, and OS reinstalls.[^7] The other vulnerability to these attacks is the inability of antivirus software to be able to read firmware for viruses. The saving grace of this type of attack is that it is so sophisticated that it is uncommon.[^8]

Type 2 malware is run through the execution of files indirectly. Suppose you can execute these commands via PowerShell. In that case, you should be able to perform edits to files without ever touching the file system but indirectly use the files within the system.[^9] This is usually done by using repositories built into the OS to look at registry information and gain deeper access to the network.

There’s a type 3 that deals specifically with the idea of running scripts through tools found in the operating system. Still, more often than not, this method needs to be coupled with other ways to gain access to sensitive infrastructure and cause heavy amounts of damage.

###Bots

Bots have the potential to do severe damage, but they are not malware. More often than not, bots are used in distributed denial of service attacks, aka DDOS attacks. You can also use them to deliver spam and ultimately function more as a tool to execute malicious code rather than the malicious code itself. However, Bots have the privilege of being either hostile takeovers or constructed on purpose.

##Malware Collection

How do we collect malicious code, and why? The solution, make a closed-off honeypot. (Honeynet)[<https://www.honeynet.org/>]. This site allows a glimpse into what it means to collect and research different attack strategies on web-based applications. The main goal of the research project has been “to fight against malware and malicious hacking attacks and has the leading security professional among members and alumni.[^10] By examing the tactics used, we can find solutions to ongoing attacks and ensure that future instances fail miserably.

I’ve attached a video that you can watch if you still have questions concerning honeypots:

([](https://www.youtube.com/watch?v=gtk2qphHKmA))[https://www.youtube.com/watch?v=gtk2qphHKmA]

\*\*Works Cited\*\*

[^1][^2][^3][^4][^5][^6]Systems, C. (2022, April 1). *What is malware? - definition and examples*. Cisco. Retrieved April 12, 2022, from https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

[^7][^8][^9]Simpson, D., & Davis, C. (2022, April 5). *Fileless threats*. Microsoft Docs. Retrieved April 12, 2022, from https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/fileless-threats?view=o365-worldwide

[^10]Honeynet. (n.d.). *About Us*. The Honeynet Project. Retrieved April 12, 2022, from https://www.honeynet.org/about/