Introduction to Malware

Brought to you by Assemble You.

It's time to work on YOU. So, sit back and listen to practical, actionable advice to secure yourself.

Today we are discussing malware. We've all fantasized about throwing our computer or laptop out of the window. It could be the system suddenly slowing down, or it might be encountering unusual errors and crashes. It's pretty common to discover unrecognized programs installed on our system. But is it okay? Well, not really. Even though a system can slow down, a sudden slowdown or the discovery of software you can't explain should alert you. These issues can be indicative of malware on your system.

So, what is malware, and why should we be worried about it?

Malware is a portmanteau, a combination of the words – "malicious" and "software." It's malicious software that is designed to cause harm to a system. It could be simply deleting data or, even more perniciously, hiding like a spy in the system, monitoring our activities. It can capture your keystrokes and send them to the person, the hacker, who planted the malware in our system. This means that if we are entering a password somewhere, let's say in our online bank account, that person controlling the malware also gets to know it. Almost everything is visible to the hacker: our data, confidential files, photographs... almost everything.

Sounds scary, right? It is, but that doesn't mean we're helpless. Over the next few minutes, we'll go through some of the different types of malware and what you can do to protect yourself against them.

Malware itself is not an entity but a broad term often used interchangeably with "virus." Many of us would call all malicious software **either** malware **or** virus, but this isn't accurate. A virus is just one subset of malware.

We need to understand each type to differentiate between them, as they all have unique characteristics.

So, let's take a look at them, starting with...

Virus

A virus alters the behavior of an existing application. When a virus does this, the existing application may start behaving strangely. For example, suppose a Word file is infected with a virus. The virus won't execute until we open the file. Once it is opened, the virus triggers itself. The result may be for the virus to add random text or delete the existing file content.

Next up, the worm.

A worm is another variant of malware that crawls from one system to another. It uses email or file sharing to traverse through a network. For example, if a malicious attachment comes via email and we double-click to open it, the worm is triggered. It will then start replicating itself on the network, infecting as many systems as possible. Unlike a virus, it does not cause any damage to the data, but it can slow down the network performance.

Onto the next type of malware, the Trojan.

In the famous story, the Greek army laid siege to the city of Troy for 10 years. Eventually, one morning the Greek troops retreated from their camp, leaving a large wooden horse outside the gates of Troy. After much debate, the Trojans pulled the mysterious gift into the city. When night fell, the horse opened up, and a group of Greek warriors climbed out and sacked the Troy from within.

So, as you might expect, a *Trojan* horse in computing is any malware that misleads users of its true intent. It disguises itself as a regular program, and when clicked, it triggers to cause damage, like deleting data.

Another form of malware is Keyloggers.

We almost all need type to use our systems, and hackers are desperate to know what we're typing. They aim to acquire sensitive information, such as passwords, by capturing keystrokes using a keylogger. Every key that is pressed, the keylogger captures and sends to the hacker. For example, suppose we enter user credentials to log on to our bank account. In that case, the keylogger will capture all the keystrokes and send them to the hacker. This means your user credentials are now known to the hacker.

Moving on from keyloggers, another type of malware is spyware

Hackers watch our activities on a system by planting spyware on our system. Spyware tracks every action we perform and reports it to the hacker. Spyware can also be

designed to steal data and gather sensitive and confidential information. For example, it will send copies of your files to the hacker.

Ransomware is next on the agenda.
A ransom is a demand made by a criminal in exchange for a captive or a hostage. In computing, the ransom is demanded not for the captive but for the system and its data. A hacker can encrypt our files using ransomware and demand ransom. The hacker encrypts the files, and they can only be decrypted with the decryption key that the hacker has. Even once we've paid the ransom, the hacker may or may not decrypt the files. We can never be sure.

Next on the agenda is backdoor malware.
When programmers develop software, they usually want an easy way to get into an application. To do this, they leave a backdoor opening into the applications. Hackers use this method to get an easy entry into the system.

For a hacker, it is difficult to hack into a system again and again. The easiest method is to hack once and leave a backdoor. That allows them to go in and out of the system without problems.

Logic Bomb
A logic bomb works on predefined conditions, such as time or date. It may exist in the system but triggers only when predefined conditions are met. For example, a hacker may create a small script executed at a specific date and time. Once executed, it can cause severe damage, including inflicting harm via file deletion. One of the most famous logic bombs attacks was The Siemens Corporation spreadsheet debacle. It involved contract employee David Tinley, who provided software to Siemens' Monroeville PA offices. He was a trusted employee for nearly a decade and would create spreadsheets to manage equipment orders. However, Tinely planted a logic bomb within one of the spreadsheets. The bomb went undetected for two years. Whenever a script would malfunction, Siemens would have to call Tinley, who would "fix it" for a fee. However, the scheme eventually ended when Tinley was out of town and gave the spreadsheet password to Siemens' IT staff during another crash. The logic bomb was found, and Tinley pled guilty in May 2019.

Moving on from the logic bomb attack, we have the Fileless Virus.
Almost all types of malware exist in the form of some file. Fileless malware, on the other hand, exists only in a computer's random-access memory (RAM), meaning that nothing is ever written directly to the hard drive. This makes it more difficult to detect as there are no stored files for defensive security software to scan. It becomes even more difficult if forensic processes are performed on the system. Since memory is volatile and does not retain information, then if the system is rebooted, the fileless virus disappears.

All of this is why, as reported by the Ponemon Institute, 77% of all breaches in 2017 used fileless techniques, which are also ten times more likely to succeed than file-based attacks.

Protecting Yourself
So, now we know the different types of malware. But how do we safeguard ourselves?

One of the most straightforward tips is to avoid opening attachments from unknown email senders. If you receive an email about million-dollar prize money and need to download the attached PDF file, remember that no one gives out a million dollars for free! The attached PDF file is likely infected with malware, so don't open it.

Our next tip is to keep your systems and applications updated. You should also install only legitimate and licensed programs to avoid licensing and malware issues.

Next, ensure that you have a SPAM filter on all incoming emails.

Finally, your systems must be equipped with a firewall with rules configured to filter the incoming and outgoing traffic.

Other than this, we should have antimalware or antivirus programs installed with the updated signatures. A virus signature (also known as a virus definition) is **a file or multiple files downloaded by a security program to identify a computer virus**. The files enable malware detection by the antivirus (and other antimalware) software in conventional file scanning and breach detection systems. Remember that antimalware is only effective if updated with the latest signatures. Every day, thousands of malware get released, and therefore, the antimalware or antivirus vendors keep releasing the updates regularly.

So, that's a lot of information to digest. But now is time to take action. Check your system and determine whether you have an antivirus or antimalware installed. If there's an update available, install it.

That's all for today. Thanks for listening, and remember: keep building the best you.

Reading List

- [Video] Malware: Difference Between Computer Viruses, Worms and Trojans
- [Video] 10 Signs of Malware on Computer | How to Know if you're Infected?
- [Video] 6 Signs Your Computer Is Affected By Malware, Spyware, Or Virus
- [Article] Introduction to Malware: Definition, Attacks, Types, and Analysis
- [Article] Fileless Malware, Awake Security
- [Article] Malware | What is Malware & How to Stay Protected from Malware Attacks