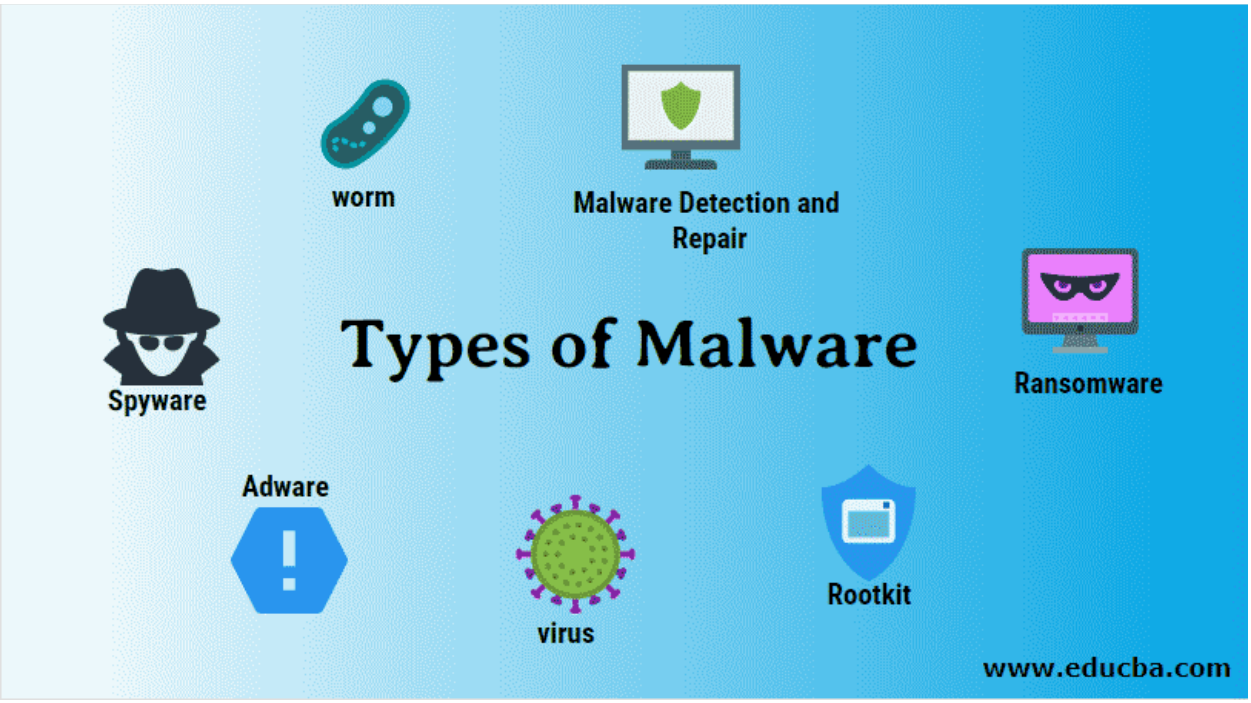
DEPI WEEK 1 REPORT

MALWARE ANALYSIS

ABSTRACT

This report explains the different types of malwares and their projection across the MITRE ATT&CK framework

What is Malware?



Malware, or “malicious software,” is an umbrella term that describes any malicious program or code that is harmful to systems.

Hostile, intrusive, and intentionally nasty, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device’s operations. Like the human flu, it interferes with normal functioning.

The motives behind malware vary. Malware can be about making money off you, sabotaging your ability to get work done, making a political statement, or just bragging rights. Although malware cannot damage the physical hardware of systems or network equipment (with one known exception—see the Google Android section below), it can steal, encrypt, or delete your data, alter or hijack core computer functions, and spy on your computer activity without your knowledge or permission.

Types of malwares

Adware

Adware is unwanted software designed to throw advertisements up on your screen, most often within a web browser.

Spyware

Spyware is malware that secretly observes the computer user's activities without permission and reports it to the software's author.

Worms

Worms are a type of malware similar to viruses. Like viruses, worms are self-replicating. The big difference is that worms can spread across systems on their own, whereas viruses need some sort of action from a user to initiate the infection.

Trojans

A trojan, or Trojan horse, is one of the most dangerous malware types. It usually represents itself as something useful to trick you. Once it's on your system, the attackers behind the Trojan gain unauthorized access to the affected computer. From there, Trojans can be used to steal financial information or install other forms of malware, often ransomware.

Ransomware

Ransomware is a form of malware that locks you out of your device and/or encrypts your files, then forces you to pay a ransom to regain access.

Rootkits

Rootkit is a form of malware that provides the attacker with administrator privileges on the infected system, also known as "root" access.

Keylogger

A keylogger is malware that records all the user's keystrokes on the keyboard, typically storing the gathered information and sending it to the attacker, who is seeking sensitive information like usernames, passwords, or credit card details.

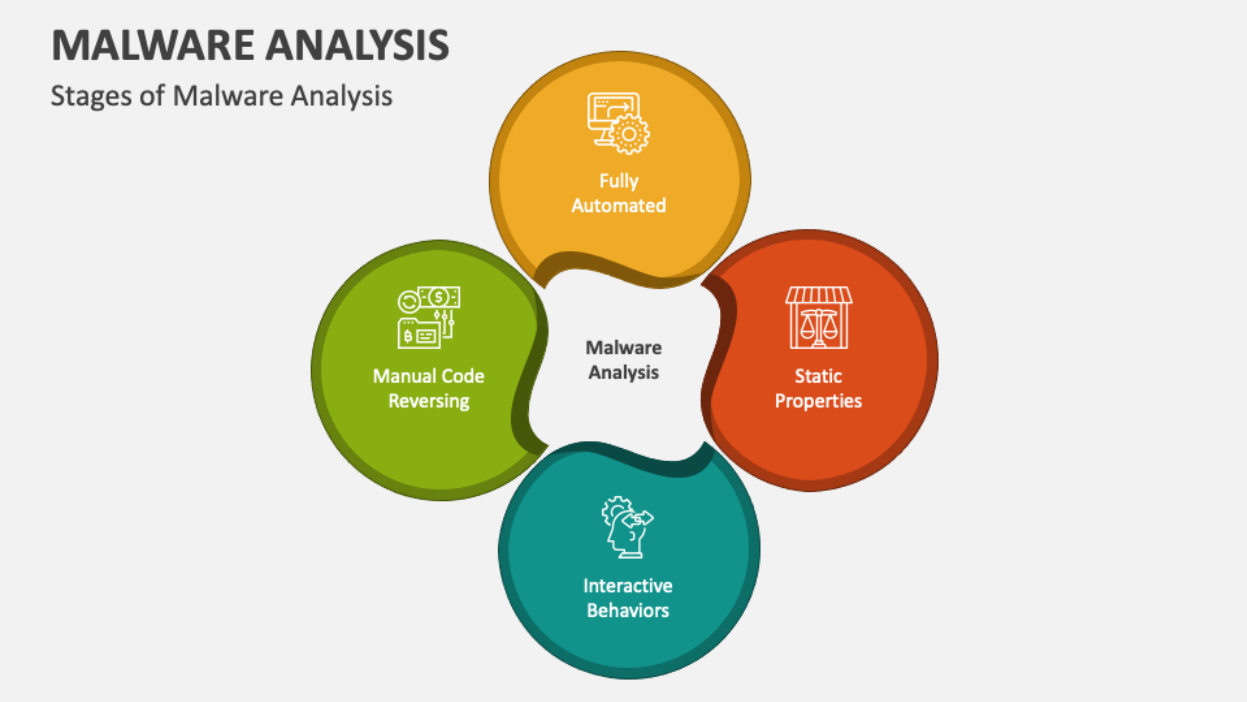
Malicious cryptomining

Malicious cryptomining, also sometimes called drive-by mining or cryptojacking , is an increasingly prevalent malware usually installed by a Trojan. It allows someone else to use your computer to mine cryptocurrency like Bitcoin or Monero.

What is malware analysis?

Malware analysis is defined as “the process of breaking down malware into its core components and source code, investigating its characteristics, functionality, origin, and impact to mitigate the threat and prevent future occurrences.” This article will touch upon the types of malware analysis, best practices, and key stages.

Stages of malware analysis



Static properties analysis

Static properties refer to strings of code embedded inside the malware file, hashes, header details, and metadata. Static properties analysis provides a quick and easy way to gather helpful information about malware because the malware does not have to be executed for you to study it.

Interactive behavior analysis

Interactive behavior analysis involves a security analyst interacting with malware running in a lab, making observations regarding its behavior. In this way, you can better understand how malware uses different elements of a computer system, such as its memory.

Fully automated analysis

Fully automated analysis scans suspected malware files using automated tools, focusing on what the malware can do once inside your system. After the analysis, you get a report outlining the potential damage to assets connected to your network.

Manual code reversing

Manual code reversing breaks down the code used to build the malware to learn how it works and what it is capable of doing. This is a time-consuming process that requires significant skill. However, when used correctly, manual code reversing can reveal valuable information about the malware.

Types of malware analysis

Static malware analysis

Static malware analysis looks for files that may harm your system without actively running the malware code, making it a safe tool for exposing malicious libraries or packaged files. Static malware analysis can uncover clues regarding the nature of the malware, such as filenames, hashes, IP addresses, domains, and file header data. The malware can be observed using a variety of tools, such as network analyzers.

Dynamic malware analysis

Dynamic malware analysis uses a **sandbox**, which is a secure, isolated, virtual environment where you can run suspected dangerous code. Security professionals can closely monitor the malware in the sandbox without worrying about infecting the rest of the system or network, allowing them to gather more information about the malware.

What's a Trojan

A Trojan is a type of malware that hides within a legitimate file or program to gain access to your device. Because Trojan malware is delivered inside a legitimate app or file, it's very difficult to detect. Trojans are used to spy on victims, steal data, infect other programs, and inflict other harm.

Types of Trojans

Backdoor Trojans

They are one of the simplest but potentially most dangerous types of Trojan. This is because they can either load all sorts of malware onto your system in their role as a gateway, or at least ensure that your computer is vulnerable to attack. A backdoor is often used to set up botnets.

Remote Access Trojan (RAT)

This Trojan gives the attacker complete control over the victim's computer, effectively turning it into a tool for cybercriminals to exploit.

Banking Trojans

Banking Trojans are among the most widespread Trojans. Given the increasing acceptance of online banking, as well as the carelessness of some users, this is no wonder – they are a promising method for attackers to get their hands on money quickly. Their goal is to obtain the access credentials to bank accounts. To do this they use phishing techniques, for example by sending the alleged victims to a manipulated page where they are supposed to enter their access credentials.

DDoS Trojan

These Trojans perform DDoS attacks, flooding a network with traffic to overwhelm and crash it.

Trojan-Ransom

This type of Trojan can modify data on your computer so that your computer doesn't run correctly or you can no longer use specific data. The criminal will only restore your computer's performance or unblock your data after you have paid them the ransom money that they demand

How do Trojans actually work?

Unlike computer viruses, a Trojan horse cannot manifest by itself, so it needs a user to download the server side of the application for it to work. This means the executable (.exe) file should be implemented and the program installed for Trojan to attack a device's system.

A Trojan virus spreads through legitimate-looking emails and files attached to emails, which are spammed to reach the inboxes of as many people as possible. When the email is opened and the

malicious attachment is downloaded, the Trojan server will install and automatically run every time the infected device is turned on.

Devices can also be infected by a Trojan through social engineering tactics, which cyber criminals use to coerce users into downloading a malicious application. The malicious file could be hidden in banner advertisements, pop-up advertisements, or links on websites.

A computer infected by Trojan malware can also spread it to other computers. A cyber criminal turns the device into a zombie computer, which means they have remote control of it without the user knowing. Hackers can then use the zombie computer to continue sharing malware across a network of devices, known as a botnet.

For example, a user might receive an email from someone they know, which includes an attachment that also looks legitimate. However, the attachment contains malicious code that executes and installs the Trojan on their device. The user often will not know anything untoward has occurred, as their computer may continue to work normally with no signs of it having been infected.

Prevention and mitigation

Preventing and mitigating Trojan infections is essential to maintaining the security of your systems and data. Here are some key strategies to protect against and mitigate Trojans.

Use Antivirus and Anti-Malware Software

Ensure that you have reputable antivirus or anti-malware software installed on your system. Enable real-time protection and schedule regular scans to detect and remove Trojans before they cause harm.

Do not download from untrusted sources

Never download or introduce any product program from a site or source that you don't completely trust. user-level files and processes.

Avoid phishing assaults

Do not open a connection or snap a connection in an email that was simply shipped off you from an arbitrary individual.

Update your Operating framework and any introduced security conventions

Regularly update your OS to ensure that the product is progressively equipped for battling off dangers. Updates normally incorporate security patches on the most recent dangers.

Do not visit dangerous sites

Be watching out for any sites that don't have security testaments – their URL ought to incorporate https://rather than HTTP://. The 's' represents secure and there ought to likewise be a lock close to the URL in the location bar.

MITRE ATT&CK projection on Trojans

MITRE ATT&CK is a comprehensive framework that categorizes the tactics, techniques, and procedures (TTPs) used by cyber adversaries, including Trojans. By mapping Trojans to the MITRE ATT&CK framework, you can understand the different stages and behaviors associated with Trojan attacks. Here's a high-level breakdown of how Trojans relate to the different tactics and techniques within the MITRE ATT&CK framework.

T1547.001(Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder)

Trojan-Karagany can create a link to itself in the Startup folder to automatically start itself upon system restart.

T1059.003(Command and Scripting Interpreter: Windows Command Shell)

Trojan-Karagany can perform reconnaissance commands on a victim machine via a cmd.exe process.
can survive operating system reinstalls and even hard drive replacements, they are

What's ransomware

Ransomware is a type of malware that holds a victim's sensitive data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker.The earliest ransomware attacks simply demanded a ransom in exchange for the encryption key needed to regain access to the affected data or use of the infected device.

Types of ransomware

Leakware or doxware

Leakware or doxware is ransomware that steals, or exfiltrates, sensitive data and threatens to publish it. While earlier forms of leakware or doxware often stole data without encrypting it, today's variants usually do both.

Mobile ransomware

Mobile ransomware includes all ransomware that affects mobile devices. Delivered through malicious apps or drive-by downloads, most mobile ransomware is non-encrypting ransomware. Hackers prefer screen-lockers for mobile attacks because automated cloud data backups, standard on many mobile devices, make it easy to reverse encryption attacks.

Wipers

Wipers, or destructive ransomware, threaten to destroy data if the victim does not pay the ransom. In some cases, the ransomware destroys the data even if the victim pays. This latter type of wiper is often deployed by nation-state actors or hacktivists rather than common cybercriminals.

Scareware

Scareware is just what it sounds like—ransomware that tries to scare users into paying a ransom. Scareware might pose as a message from a law enforcement agency, accusing the victim of a crime and demanding a fine. Alternatively, it might spoof a legitimate virus infection alert, encouraging the victim to purchase ransomware disguised as antivirus software.

How does Ransomware actually work?

The ransomware lifecycle has six general stages: malware distribution and infection; command and control; discovery and lateral movement; malicious theft and file encryption; extortion; and resolution.

Stage 1 : Malware distribution and infection

Before attackers can demand a ransom, they must infiltrate their victims' systems and infect them with malware. The most common ransomware attack vectors are phishing, Remote Desktop Protocol (RDP) and credential abuse, and exploitable software vulnerabilities

Stage 2 : Command and Control

A command-and-control (C&C) server set up and operated by the ransomware attackers sends encryption keys to the target system, installs additional malware and facilitates other stages of the ransomware lifecycle.

Stage 3 : Discovery and lateral movement

This two-step stage involves attackers first gathering information about the victim network to help them better understand how to launch a successful attack, and then spreading the infection to other devices and elevating their access privileges to seek out valuable data.

Stage 4 : Malicious theft and file encryption

In this stage, attackers exfiltrate data to the C&C server to use in extortion attacks down the line. Attackers then encrypt the data and systems using the keys sent from their C&C server.

Stage 5 : Extortion

The attackers demand a ransom payment. The organization now knows it is a victim of a ransomware attack.

Stage 6 : Resolution

The victim organization must go into action to address and recover from the attack. This could involve restoring backups, implementing a ransomware recovery plan, paying the ransom, negotiating with attackers or rebuilding systems from the ground up.

Prevention and mitigation

Never click on unverified links

If a link is in a spam email or on a strange website, you should avoid it. Often, hackers spread ransomware through a malicious link that initiates a malware download. Once the malware is on your computer, it can encrypt your data, holding it hostage, only allowing someone with a decryption key to access it.

Scan emails for malware

Typically, the malware in the email will be embedded in an attachment or inside a file within the body of the email. Hackers have been known to insert images that appear innocent, but when you click on the image, it installs ransomware on your computer. Scanning for emails with these kinds of files can prevent your device—or others on your network—from getting infected.

Use firewalls

Firewalls can be a good solution as you figure out how to stop ransomware attacks. Firewalls scan the traffic coming from both sides, examining it for malware and other threats. In this way, a firewall can ascertain where a file came from, where it is headed, and other information about how it traveled and then use that to know whether it is likely to contain ransomware.

Only download from trusted sites

In many cases, the link itself may look innocent. If you are not familiar with the site or if its Uniform Resource Locator (URL) looks suspicious even though it appears to be a trusted site, you should steer clear. Cybercriminals often create fake sites that look like a trusted one. Always double-check the URL of a site before downloading anything from it.

Keep backups of important data

If your data is backed up to a device or location you do not need your computer to access, you can simply restore the data you need if an attack is successful. It is important to make sure you

back up all critical data frequently because if enough time goes by, the data you have may be insufficient to support your business's continuity.

Use security software

Security software can be a powerful tool in ransomware prevention. Therefore, it is often listed among the best practices to prevent ransomware. Security software checks the files coming into your computer from the internet. When a malicious file has been detected, the software prevents it from getting into your computer.

Do not use unfamiliar USB devices

A Universal Serial Bus (USB) device can be used to store a malicious file that could contain ransomware. Whether the USB has an executable file on it that can infect your computer or the file is launched automatically when you insert the USB device, it can take very little time for an apparently benevolent USB to capture your computer.

Avoid giving out personal data

With the right personal data, a cybercriminal can set a variety of traps to get ransomware on your computer or trick you into installing it on your device yourself. People often use the same passwords for their computers as they do for websites and accounts. A cybercriminal can use your personal data to gain access to an account, and then use that password to get into your computer and install ransomware.

MITRE ATT&CK projection on Ransomwares

The MITRE ATT&CK framework, which is a comprehensive model of adversarial techniques used in cyber intrusions, provides a valuable lens to understand how rootkits operate within broader attack chains.

Rootkits are generally classified under Defense Evasion techniques within the MITRE ATT&CK matrix. One of the core techniques that directly maps to rootkit behavior is T1014: Rootkit. This technique highlights how attackers use rootkits to hide the presence of malicious software or processes from detection tools, such as antivirus or intrusion detection systems (IDS). Rootkits can subvert core OS functions to provide attackers with privileged access while keeping their actions concealed. In practice,

several sub-techniques under other tactics within the ATT&CK framework may also involve rootkit-like behavior. For instance:

T1486 - Data Encypted for impact

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted

T1135 - Network share discovery

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

What's a rootkit

A rootkit is a type of malicious software designed to gain unauthorized access to a computer system and remain undetected. Rootkits typically hide their presence by modifying system-level files and processes, allowing an attacker to maintain control of the system for a long time. They often run with root (administrator) privileges, hence the name "rootkit."

Types of rootkits

User-Mode Rootkits

These rootkits operate in the user space of the operating system, which is less privileged than the kernel level. They can modify or replace system binaries, processes, or libraries to hide files, processes, or network connections.

Kernel-Mode Rootkits

These rootkits operate in the user space of the operating system, which is less privileged than the kernel level. They can modify or replace system binaries, processes, or libraries to hide files, processes, or network connections.

Bootloader (Bootkit) Rootkits

These infect the Master Boot Record (MBR) or bootloader, allowing them to execute before the operating system loads. Bootkits can alter the boot process, making it difficult for antivirus software to detect their presence. They can re-install malicious components each time the system boots up.

Firmware Rootkits

These target the firmware of hardware components like hard drives, network cards, or even the BIOS/UEFI. They persist across operating system reinstallation, as they reside in non-volatile memory. Extremely hard to detect since they are outside the operating system's control.

Hypervisor Rootkits (Virtualized Rootkits)

These rootkits create a virtualized environment in which the operating system runs, essentially creating a hypervisor layer between the hardware and the OS. The operating system becomes unaware that it's running inside a virtual machine, giving the rootkit full control. Difficult to detect because the rootkit can monitor and control the operating system's actions from outside the OS.

How does Rootkits actually work?

Rootkits are a particularly sneaky form of malware that work by taking control of the underlying operations of a computer, making them almost invisible to users and even most security tools. Imagine they're like someone quietly slipping behind the scenes of a theater, controlling what the audience sees without anyone noticing. In the case of a rootkit, it intercepts or modifies how the system normally functions. For example, it might prevent certain programs from showing up in the task manager, hide files from view, or even stop your antivirus software from running properly.

One of the most common tricks rootkits uses is to alter the very core of the operating system, known as the kernel. This is like changing the foundation of a house so that any damage is covered up—things look fine on the surface, but underneath, the system is compromised. By modifying these critical files, the rootkit ensures that any normal detection tools, like antivirus programs or system monitors, simply can't see the malicious activities going on. To the average user, everything looks perfectly normal, when in reality, the system has been compromised.

Rootkits are designed to stay hidden for as long as possible, often going so far as to block security software from updating or scanning the system entirely. They can also make sure that any malicious network traffic or suspicious activities are masked, allowing an attacker to remotely access the system undetected. What makes rootkits even scarier is that some can infect the computer's bootloader, the software that runs before the operating system starts. This means they can survive even if the computer is restarted or the operating system is reinstalled.

These tools give attackers long-term access to systems without the user having any idea that their data might be at risk. Rootkits can be used for all sorts of malicious activities, from stealing sensitive information to turning the computer into part of a botnet—a network of compromised computers used for large-scale cyberattacks. In the worst cases, rootkits can be so deeply embedded that the only way to fully remove them is to completely wipe and reinstall the system, or even replace the hardware itself if the rootkit has infected the computer's firmware.

Because rootkits are so stealthy, traditional antivirus programs often aren't enough to detect them. Many organizations now use advanced security tools that look for unusual behavior in the system—things like unexpected network traffic or strange process activities—to catch rootkits in action. Rootkits remind us that not all threats are obvious, and they require a more thoughtful and vigilant approach to keeping systems secure.

Prevention and mitigation

Detecting rootkits can be extremely challenging, particularly when they operate at the kernel or firmware level, where they have deep access to system processes and can remain hidden from traditional antivirus solutions. Rootkits are designed to evade detection by altering system components, making them difficult to identify using standard security measures. However, several advanced methods can be employed to improve the chances of detecting and mitigating rootkits:

Behavioral Analysis

One of the most effective ways to detect rootkits is through behavioral analysis, where system activity is continuously monitored for anomalies. Rootkits often cause unexplained network traffic, increased CPU or memory usage, or unusual system calls. For example, a kernel-level rootkit may bypass security controls or open hidden communication channels, leading to performance degradation or suspicious network connections. Monitoring these behaviors can help security teams identify irregularities indicative of rootkit activity.

File Integrity Monitoring (FIM)

Rootkits frequently modify or replace system files to conceal their presence. File integrity monitoring tools continuously check critical system files (such as system binaries and configuration files) for unexpected changes. This method relies on cryptographic hashing to create a baseline of the system files and then checks for any alterations. Changes to these files without legitimate updates may indicate rootkit activity. This technique is particularly useful against user-mode rootkits that focus on modifying user-level files and processes.

Boot-Time Scans

Rootkits that load before the operating system, known as bootkits, are particularly dangerous because they can modify the OS at its most vulnerable state. Standard antivirus programs may not be able to detect these rootkits during normal operations. Boot-time scanning techniques address this by performing deep scans before the OS fully loads, examining system components such as the Master Boot Record (MBR), UEFI/BIOS, and startup drivers. This can catch rootkits that hide within boot processes, as they cannot interfere with the scanner before it starts.

Hardware-Based Detection

For rootkits that compromise firmware or BIOS/UEFI, software-level detection may not be sufficient. Hardware-based security solutions, such as Trusted Platform Modules (TPM) and Secure Boot, can help detect unauthorized changes to firmware or the boot process. These hardware components store cryptographic signatures of firmware and boot loaders, ensuring that only trusted code is executed during the boot process. If a rootkit attempts to modify the firmware or boot sequence, these systems can detect and block it before the OS loads.

Digital Signatures

Code-signing ensures that software and drivers loaded into the system are from trusted sources. Rootkits often attempt to load unauthorized drivers or modify existing system files. Monitoring for unsigned or improperly signed drivers can help detect rootkits attempting to operate at the kernel level.

MITRE ATT&CK projection on Rootkits

The MITRE ATT&CK framework, which is a comprehensive model of adversarial techniques used in cyber intrusions, provides a valuable lens to understand how rootkits operate within broader attack chains.

Rootkits are generally classified under Defense Evasion techniques within the MITRE ATT&CK matrix. One of the core techniques that directly maps to rootkit behavior is T1014: Rootkit. This technique highlights how attackers use rootkits to hide the presence of malicious software or processes from detection tools, such as antivirus or intrusion detection systems (IDS). Rootkits can subvert core OS functions to provide attackers with privileged access while keeping their actions concealed. In practice, several sub-techniques under other tactics within the ATT&CK framework may also involve rootkit-like behavior. For instance:

T1547.001 - Boot or Logon AutoStart Execution

Registry Run Keys/Startup Folder Some rootkits inject themselves into the boot process, modifying the boot sector or registry entries to persist across reboots. A rootkit embedded this way is often nearly impossible to detect, as it starts executing before most security mechanisms are even loaded.

T1215 - Kernel Modules and Extensions

Attackers can exploit the OS kernel by injecting malicious modules or drivers. This is common with more sophisticated rootkits, which are often referred to as "kernel-mode" rootkits. Kernel-mode rootkits have direct access to hardware and critical system functions, making them highly effective at hiding malicious processes and altering system outputs to evade detection.

APTs and Groups used rootkits

Several advanced persistent threat (APT) groups have deployed rootkits as a part of their toolsets. One notable example is APT28 (also known as Fancy Bear), a Russian cyber espionage group. APT28 has been linked to rootkits like LoJax, which was designed to target the Unified Extensible Firmware Interface (UEFI), effectively embedding itself within the firmware of compromised systems. Since UEFI-level rootkits can survive operating system reinstalls and even hard drive replacements, they are incredibly resilient and dangerous tools.

Another instance is the Equation Group, believed to be associated with the U.S. National Security Agency (NSA). Their use of the EquationDrug and GrayFish malware families included sophisticated rootkit components that targeted the hard drive firmware of infected machines. These rootkits were designed to persist and operate even in highly controlled environments, where standard detection methods would likely fail.

The Turla group (also known as Snake or Uroburos), a cyber-espionage group believed to be tied to Russian intelligence, is another example. Turla has made extensive use of rootkits in their campaigns, including the notorious Snake rootkit, which allowed the group to carry out stealthy, long-term surveillance on high-profile targets.