Malware Reverse Engineering

What is malware?

- Malware, or malicious software, is any program or file that's intentionally harmful to a computer, network or server.

- These malicious programs
  - Steal and encrypt data
  - Delete sensitive data;
  - Alter or hijack core computing functions, and
  - Monitor end users' computer activity

- Types of malware include computer viruses, worms, Trojan horses, Ransomware and spyware.

What is the intent of malware?

- **Intelligence and intrusion**
- Exfiltrates data such as emails, plans, and especially sensitive information like passwords.

- **Disruption and extortion**
- Locks up networks and PCs, making them unusable
- If it holds your computer hostage for financial gain, it's called ransomware.

What is the intent of malware?

- **Destruction**
- Destroys computer systems to damage your network infrastructure.

- **Steal computer resources**
- Uses your computing power to run botnets, cryptomining programs (cryptojacking), or send spam emails.

- **Monetary gain**
- Sells your organization's intellectual property on the dark web.

What does malware do?

- Malware can infect networks and devices and is designed to harm those devices, networks and their users in some way
- Depending on the type of malware and its goal, this harm might present itself differently to the user or endpoint

- In some cases, the effect of malware is relatively mild and benign, and in others, it can be disastrous.

- Malware can typically perform the following harmful actions:

Data exfiltration

- Data exfiltration is a common objective of malware

- During data exfiltration, once a system is infected with malware, threat actors can steal sensitive information stored on the system, such as emails, passwords, intellectual property, financial information and login credentials

- Data exfiltration can result in monetary or reputational damage to individuals and organizations.

Service disruption

- Malware can disrupt services in several ways

- For example, it can lock up computers and make them unusable or hold them hostage for financial gain by performing a ransomware attack

- Malware can also
  - target critical infrastructure, such as power grids, healthcare facilities or
  - transportation systems to cause service disruptions.

Data espionage

- A type of malware known as spyware performs data espionage by spying on users

- Typically, hackers use
  - keyloggers to record keystrokes,
  - access web cameras and microphones and capture screenshots

Identity theft

- Malware can be used to steal personal data which can be used to impersonate victims, commit fraud or gain access to additional resources

- According to the IBM X-Force Threat Intelligence Index 2024, there was a 71% rise in cyberattacks using stolen identities in 2023 compared to the previous year.

Stealing resources

- Malware can use stolen system resources
  - to send spam emails,
  - operate botnets and
  - run cryptomining software, also known as cryptojacking.

System damage

- Certain types of malware, such as computer worms,
  - damage devices by corrupting the system files,
  - deleting data or changing system settings.

- This damage can lead to an unstable or unusable system.

How do malware infections happen?

- Malware use a variety of physical and virtual means to spread malware that infects devices and networks

- including the following:
- Removable drives
- Infected websites
- Phishing attacks
- Obfuscation techniques
- Software from third-party websites

Removable drives

- Malicious programs can be delivered to a system with a USB drive or external hard drive.

- For example, malware can be automatically installed when an infected removable drive connects to a PC

Infected websites

- Malware
  - find its way into a device through popular collaboration tools and drive-by downloads,
  - which automatically download programs from malicious websites to systems without the user's approval or knowledge.

Phishing attacks

- use phishing emails disguised as legitimate messages containing malicious links or attachments to deliver the malware executable file to unsuspecting users

- Sophisticated malware attacks often use a command-and-control server that
  - lets threat actors communicate with the infected systems, exfiltrate sensitive data and
  - even remotely control the compromised device or server

Obfuscation techniques (to make their code or behavior difficult to analyze, understand, or detect by security tools, administrators, and even users.)

- Emerging strains of malware include new evasion and obfuscation techniques designed to fool users, security administrators and antimalware products

- Some of these evasion techniques rely on simple tactics, such as using web proxies to hide malicious traffic or source Internet Protocol (IP) addresses

Obfuscation techniques

- More sophisticated cyberthreats include
  - polymorphic malware that can repeatedly change its underlying code to avoid detection from signature-based detection tools;
  - anti-sandbox techniques that enable malware to detect when it's being analyzed and to delay execution until after it leaves the sandbox; and
  - fileless malware that resides only in the system's RAM to avoid being discovered

Software from third-party websites

- There are instances where malware can be downloaded and installed on a system concurrently with other programs or apps

- Typically, software from third-party websites or files shared over peer-to-peer networks falls under this category

Software from third-party websites

- For example, a computer running a Microsoft operating system (OS) might end up unknowingly installing software that Microsoft would deem as a potentially unwanted program (PUP)

- However, by checking a box during the installation, users can avoid installing unwanted software.

Types of Malware

Virus

- that attaches to another program and,
- when executed usually inadvertently by the user replicates itself by modifying other computer programs and
- infecting them with its own bits of code.

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 in order to initiate the infection.

Trojan or Trojan horse

- one of the most dangerous malware types

- It usually represents itself as something useful in order to trick you

- Once it’s on your system, the attackers behind the Trojan gain unauthorized access to the affected computer

- Trojans can be used to steal financial information or install other forms of malware, often ransomware

Ransomeware

- 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.
- called the cybercriminal’s weapon of choice because it demands a quick, profitable payment in hard-to-trace cryptocurrency.
- The code behind ransomware is easy to obtain through online criminal marketplaces and defending against it is very difficult

Ransomeware

- While ransomware attacks on individual consumers are down at the moment, attacks on businesses are up 365 percent for 2019.

- As an example, the Ryuk ransomware specifically targets high-profile organizations that are more likely to pay out large ransoms.

Rootkit

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

- Typically, it is also designed to stay hidden from the user, other software on the system, and the operating system itself.

Backdoor virus

- A backdoor virus or remote access Trojan (RAT) secretly creates a backdoor into an infected computer system

- that lets threat actors remotely access it without alerting the user or the system's security programs.

Adware

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

- Typically, it uses an underhanded method to either disguise itself as legitimate, or piggyback on another program to trick you into installing it on your PC, tablet, or mobile device.

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

Logic Bombs

- This type of malicious malware is designed to cause harm and typically gets inserted into a system once specific conditions are met

- Logic bombs stay dormant and are triggered when a certain event or condition is met, such as when a user takes a specific action on a certain date or time.

Exploits

- Exploits are a type of malware that takes advantage of bugs and vulnerabilities in a system in order to give the attacker access to your system

- While there, the attacker might steal your data or drop some form of malware

- A zero-day exploit refers to a software vulnerability for which there is currently no available defense or fix

Exploits

- Exploits are a type of malware that takes advantage of bugs and vulnerabilities in a system in order to give the attacker access to your system

- While there, the attacker might steal your data or drop some form of malware

- A zero-day exploit refers to a software vulnerability for which there is currently no available defense or fix

How to protect against malware

- Pay attention to the domain and be wary if the site isn’t a top-level domain, i.e., com, mil, net, org, edu, or biz, to name a few.
- Use strong passwords with multi-factor authentication. A password manager can be a big help here.
- Avoid clicking on pop-up ads while browsing the Internet.
- Avoid opening email attachments from unknown senders.

How to protect against malware

- Do not click on strange, unverified links in emails, texts, and social media messages.
- Don’t download software from untrustworthy websites or peer-to-peer file transfer networks.
- Stick to official apps from Google Play and Apple’s App Store on Android, OSX, and iOS (and don’t jailbreak your phone). PC users should check the ratings and reviews before installing any software.
- Make sure your operating system, browsers, and plugins are patched and up to date.

How to protect against malware

- Delete any programs you don’t use anymore.
- Back up your data regularly. If your files become damaged, encrypted, or otherwise inaccessible, you’ll be covered.
- Download and install a cybersecurity program that actively scans and blocks threats from getting on your device.

  Malwarebytes, for example, offers proactive cybersecurity programs for Windows, Mac, Android, and Chrome

Malware Analysis

- is the process of detecting and reducing potential threats in a website, application, or server.

- It is a crucial process that ensures computer security as well as the safety and security of an organization with regard to sensitive information.

- Malware analysis addresses vulnerabilities before they get out of hand.

Malware Analysis

- If you are looking at it more simply, malware analysis can be considered as the process of understanding the behavior and the intended use of a suspicious file or URL.

- The more you know about the suspicious file, the better it will help to mitigate the threat, if any.

Key Benefits of Malware Analysis

- Identifying the source of the attack
- Determining the damage from a security threat
- Identifying a malware’s exploitation level, vulnerability, and appropriate patching preparations
- Triaging the incidents according to the level of severity of the threat in a practical manner
- Uncovering hidden Indicators of Compromise (IOC) that need to be blocked
- Improving the efficacy of IOC, alerts, and notifications
- Enriching context when trying to uncover threats

Malware Reverse Engineering

- Malware researchers require a diverse skill set usually gained over time through experience and self-training.
- Reverse engineering (RE) is an integral part of malware analysis and research but it is also one of the most advanced skills a researcher can have.
- This is one of the reasons why organizations lack reverse engineering manpower.
- Many researchers with a lack of experience struggle to get started in RE.

Malware Reverse Engineering

- Malware RE focuses specifically on understanding malware capabilities and functionalities in order to remediate threats and study different malware families

- RE can be very time-consuming.

- When researching a malware, you will usually not start reversing it right away.

Malware Reverse Engineering

- Instead, you should conduct triage malware analysis by running the malware in a sandbox, extracting strings, and more

- This initial malware analysis phase can provide further context for reverse engineering, if needed.

- For instance, you can search for specific strings in the disassembler or expect to see a certain capability that the malware displays.

Malware Reverse Engineering

- If your goal is to understand a malware’s capabilities, analyzing it dynamically via a sandbox will not be enough

- The malware’s Command and Control (C2) could go down, the malware could depend on another file for configuration which does not exist on the machine, the malware has sandbox evasion capabilities, or the malware will only run on a certain environment.

- RE, which is part of advanced static malware analysis, is much more effective to achieve this goal.