Chapter 3 Malicious Code

# Malware

Wide range of software that is intentionally designed to cause harm to a system, device, network, or user.

## Ransomware

Malware that takes over a computer and demands a ransom. It can be for crypto and or to expose someone’s private information.

Usually used in phishing campaigns or by direct methods (Remote Desktop Protocol, vulnerable services, or front-facing applications that they can compromise).

Indicators of Compromise (IoCs):

* Command and Control (C&C) traffic and/or contact to known malicious IP addresses.
* Use of legitimate tools in abnormal way.
* Lateral movement processes that seek to attack or gain information.
* Encryption files.
* Notices to end users of the encryption process with demands for ransom.
* Data exfiltration behaviors, including large file transfers

Defenses:

* Effective backup system that stores files in a separate location from the infected system.
* Having antivirus or antimalware programs downloaded.

Paying the ransom is not always the answer.

## Trojans

Type of malware that is disguised as legitimate software.

An example is Triada Trojan, which is often distributed in the guise of a modified, feature-enhanced Whatsapp version.

When the application is launched the Trojan gathers information about the host devices (device IDs, subscriber IDs, and device’s hardware address). The information is sent to a device on a remote server. Then the malicious actor can do what they want with the downloaded information.

IoCs of Trojans:

* Signatures for specific malware applications or downloadable files.
* C&C system hostnames and IP addresses.
* Folders or files created on target devices.

Remote Access Trojan (RAT) provides attackers with access to remote attacks. Organizations have an issue, because remote access tools also use RAT. Malware detection programs will call a false positive. To combat RAT don’t download untrusted software and antimalware or Endpoint Detection and Response (EDR) tools that detect Trojan and RAT behaviors.

Mitigating practices:

* Awareness of downloaded and running applications.
* Controlling the applications users can download.
* Downloading Anti-malware and EDR.

**Bot:** Automated program.

**Botnet:** A network compromised computer by bots.

**Command & Control (C&C):** The central server that communicates with all the bots in a botnet.

## Worms

Attacks on vulnerable services that spread themselves. Worms can be attached to email attachments, network file shares, IoT (internet to things), phones, etc. Worms are self-install.

To defend from worms:

* Firewalls
* Network-Level Controls

Example of a worm is Raspberry Robin, which is used as part of pre-ransomware activity. It spreads from an infected USB using LNK files. Once running it uses built-in Windows tools to accomplish tasks and stay living.

IoCs of Worms:

* Know malicious files.
* Downloads of additional components from remote server.
* C&C contact to remote system.
* Malicious behaviors using system commands for injections and other activities, including use of cmd.exe.msiexec,exe, and others.
* Hands-on-keyboard attacker activity.

Mitigating Worms:

* Effective network-level controls focused on preventing infection traffic.
* Firewalls, IPS devices, network segmentation, and similar controls are the first layer of defense.
* Patching and configuring services to limit attack surfaces.

After the infection:

* Use of antimalware, EDR, and similar tools to stop and potentially remove infections.
* Reinstallation or resetting to original firmware on the device.
* Removal may be impossible.

## Spyware

Designed to obtain information about a person, organization, or system. Spyware can track browsing habits, installations, or similar information. Spyware goal is to target sensitive data, access webcam, or have unlimited access to a device.

Combat Spyware:

* Antimalware tools with antispyware capabilities.
* User awareness includes control of software that is being downloaded on a device.

IoCs of Spyware:

* Remote-access and remote-control-related indicators.
* Know software file fingerprint.
* Malicious processes, often disguised as system processes.
* Injection attacks against browsers.

Spyware can use Trojan, worm, or virus-style attacks to access a device.

## Bloatware

Unwanted applications installed on system by manufacturers. It is unintentional but caused by poorly written code with information about the system or usage or may even provide a way for attackers to access a device.

Mitigation is by uninstalling the unwanted pre-installed applications.

## Viruses

Malicious programs that self-copy and self-replicate once they are activated. Viruses look to spread to multiple devices. The virus needs a **trigger** to start so it can infect the computer which is known as the **payload**.

Virus Types:

* Memory-resident virus which remains in the memory.
* Non-memory-resident viruses which execute, spread, and then shut down.
* Boot Sector viruses which reside in the boot sector of a drive or media storage.
* Email viruses which spread via email as an attachment or as part of the email itself.

Fileless viruses’ attacks are like regular viruses. They spread via email or websites and exploit flaws in browsers, plug-ins, and websites. Once they find a way into the system, they inject themselves into the memory.

Mitigation:

* User awareness of what they are clicking on or downloading.
* Downloading antimalware.
* Having virus removal tools.
* Wipe hard drive or discard hard drive.

## Keyloggers

Captures keystrokes from keyboard. It may also collect mouse movement, touch screen inputs, and credit card swipes.

Works in different ways, ranging from tools that capture data from the kernel, via APIs or scripts, or even directly from memory. Goal is to capture user input.

Preventions:

* Malware with keylogger detection.
* Multifactor authentication.

IoCs of Keylogger:

* File hashes and signatures.
* Exfiltration activity to C&C systems.
* Process names.
* Known reference URLs.

## Logic Bombs

Functions or code placed inside other programs that will be activated when set conditions are met.

Logic bombs are a consideration in software development and systems management and have a significant impact if they successfully activate.

IoCs is to analyze the code and logic and from there build a defense.

### Analyzing Malware

* Online analysis tools can check if the malware is a known tool and see if it identified by multiple AV tools.
* Sandbox tools can analyze malware behavior in a protected environment.
* Manual code analysis.

## Rootkits

Designed to allow attackers to access a system through a backdoor.

Rootkits also conceal the rootkit from detection from multiple techniques ranging from hooking file-system drivers to ensure that users cannot see the rootkit files to infecting startup code in the Master Boot Record (MBR) of a disk, allowing attacks against full-disk encryption systems.

To detect a rootkit, you can:

* Test the suspected system from a trusted device.
* Rootkit detection tools.
* Integrity checking with data validation.

It is also recommended to rebuild the system or to restore it from a well-known backup.

Prevention:

* Patching
* Use of a secure configuration.
* Ensuring that privilege management is used.

IoCs:

* File hashes and signatures.
* C&C domains, IP addresses, and systems.
* Behavior-based identification like the creation of services, executables, configuration changes, file access, and command innovation.
* Opening ports or creation of reverse proxy tunnels.