Practical Malware Analysis

MAASEC

Content

01 Malware Stages

02 Malware Types

03 Detection

04 BREAK

05 Obfuscation Techniques

06 Competitive Obfuscation

07 BREAK

08 Protective Approaches

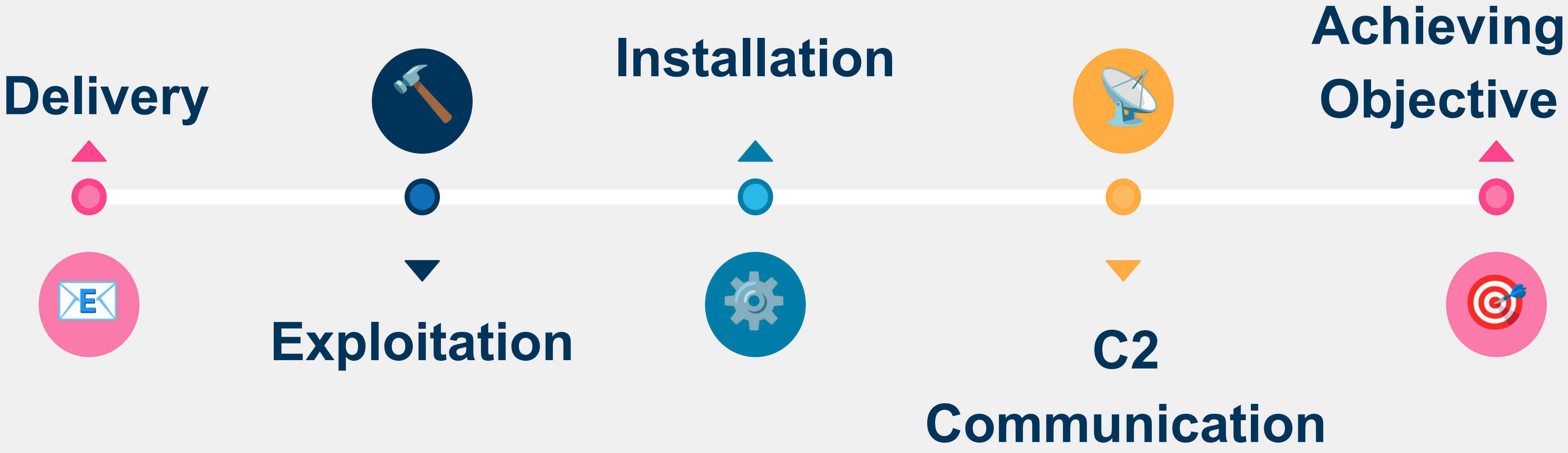
Malware - Definition

Malware is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.

MALWARE STAGES

Malware - Stages

The process of a malware's execution can be broken down into five stages:



Delivery

Exploitation

Installation

C2 Communication

Achieving Objective

Malware - Stages - Delivery 📧

The Delivery stage represents the process, and manner, through which an attacker gains access to a system or network. Attacks can be random or targeted, and the form of this stage reflects the attackers’ intentions.

Malware - Stages - Delivery - Types

Random (Opportunistic):

- Drive-by Download
- Scanning and Exploiting Vulnerabilities

Targeted:

- Social Engineering (Phishing)
- Compromised Credentials

Malware - Stages - Exploitation 🔨

Exploitation is the action(s) needed for the malware to be activated, via the Entry point, to gain privileges on the system. This can be done without user intervention, by exploiting vulnerabilities in the network or the system, or through user action.

Malware - Stages - Installation ⚙️

Once the malware is on the system, it needs to configure itself, and the system, to allow for its final objective to be achieved. This can include downloading additional parts of itself, and changing the settings of the system, such as disabling Malware Detection measures.

Malware - Stages - C2 📡

In the C2 stage, the malware sets up network-based communication with the system of the attacker. This connection allows the attacker to control and communicate with the malware, achieving tasks such as data gathering and remote control.

Malware - Stages - Actions on Objectives 🎯

When everything has been set-up, the malware is able to achieve the task for which it was created. This depends entirely on the developer of the malware, and may include data theft, system disruption, or even damage to hardware.

MALWARE TYPES

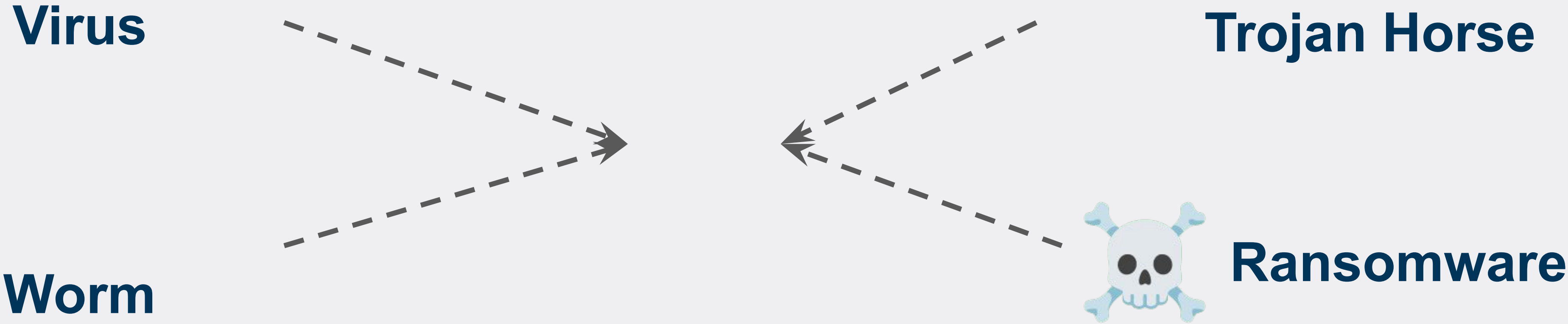
Malware - Types

Not all malware follow the same architecture. We can classify malware based on a few factors:

- Behavior / Functionality
- Propagation
- Delivery Method
- Payload Type
- Stealth Techniques

Malware - Types

We can classify malware based on those factors. There are many different categories, but most malware fall into one of four:



Virus

Trojan Horse

☠️ Ransomware

Worm

Malware - Types - Virus

A virus, is a type of malware. Its definition is limited to a program or code that self-replicates or copies itself in order to spread to other devices or areas of the network.

Malware - Types - Worm

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it.

Malware - Types - Trojan Horse

A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

Malware - Types - Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid.

MALWARE DETECTION MECHANISMS

Detection

Malware Detection is the process of analysing files and identifying malicious software on a computer to prevent (further) harm.

Detection - Types

There are multiple ways to detect malware:

1. Signature-Based Detection
2. Manual Analysis (Static and Dynamic)
3. Machine Learning

Detection - Types - Manual Analysis

Manual Analysis of malware happens when a malware analyst uses static and dynamic analysis to determine if a program can be considered malware. Most new releases of malware can only be detected through manual analysis.

Detection - Types - Signature-Based

Signature-Based Detection requires a database of past malware, and compares the program being currently analyzed against the stored ones. This technique is cheaper and faster than manual analysis, but is incapable of detecting all malware.

Detection - Types - Machine Learning

Modern machine learning algorithms are able to combine the Manual and Signature-Based approaches to provide faster and cheaper malware analysis. The functionality depends on the model, but they are able to use features extracted from program behavior, structure, or code patterns to determine if a program is malware.

BREAK

Obfuscation Techniques

Obfuscation

Obfuscation means to make something difficult to understand. Programming code is often obfuscated to protect intellectual property or trade secrets, and to prevent an attacker from reverse engineering a proprietary software program.

Obfuscation - Types

There is no standard as how to how categorize them, but we can group them up into three categories:

1. Encryption (Packing)
2. Complexification
3. Modification

Obfuscation - Types - Encryption

Through encryption the payload of the malware is hidden from the detection mechanism during analysis. When the malware wants to use the payload, it decrypts it, and encrypts it or deletes it after it’s done using it. This makes effective static analysis impossible, but can be overcome through dynamic analysis.

Obfuscation - Types - Complexification

Complexification is not a single technique, but rather a family of them. It encompasses every design choice and feature that makes understanding the execution of the program more difficult. This can include dummy code, using more lines of code than needed and opaque predicates (conditionals that are evaluated the same way each time).

Obfuscation - Types - Modification

Software has the capacity to modify itself. Sections of code and payloads can be stored as data inside the program and randomly selected each time the malware is spread. This makes signature based detection impossible, since the amount of signatures is increased.

COMPETITIVE OBFUSCATION

Competitive Obfuscation

Form a team of **5 members**, and create a flag of the format **MAAS{---}**.

Then use the obfuscation the obfuscation techniques mentioned, or your own ones, to **hide the flag**.

At the end share the executable in the Discord channel of the workshop, and try to find the flags of other teams.

MALWARE PROTECTION MEASURES

Protection Approaches

There are a few different philosophical approaches to keeping a system secure:

1. Prevention
2. Detection and Removal
3. Resilience

Protection Approaches - Prevention

Prevention focuses on reducing the likelihood of an infection occurring on a system. There’s two ways to do this:

1. Reinforcing the system
2. Educating the people

Protection Approaches - Prevention

Reinforcing the system is typically done by introducing measures that prevent or eliminate malware during the early stages of its lifecycle. Using well-tested Firewall and Antivirus software can detect and block threats before they become a problem.

Protection Approaches - Prevention

Educating the people that are part of a system is an effective, yet difficult to implement safety measure. This is because attackers are constantly developing new ways to trick their victims. Nevertheless, educating individuals on cyber risks, can reduce the likelihood of them occurring by up to 70%.

Protection Approaches - Detection/Removal

Detection and Removal is focused on handling Malware after it has been installed on a system. Detection has already been covered, and removal can be performed manually (with no guarantees of success) and automatically, with tools like certain Antiviruses.

Protection Approaches - Resilience

In some cases, the previous two approaches might both fail. In that case the resilience approach is used to minimize damage and promote quick recovery. Performing regular back-ups of a system and composing a disaster recovery plan, ensure that important data is not lost, or its loss is minimized.

What can YOU do?

- Keep your software updated
  Regularly patch your operating system and applications to fix vulnerabilities.

- Think before you click
  Avoid suspicious links, email attachments, and pop-ups.

- Back up your data regularly
  Use local and cloud backups to protect important files.

- Stay informed
  Learn about common threats like phishing, ransomware, and scams.

DO NOT TRY AT HOME >:(

Destroying a VM with Malware