Malware Threats and Cyber Risks in IoT & OT

Prepared by: PalCyberSec Team

TABLE OF CONTENTS

Software

Software is a set of instructions or programs used to operate computers and perform tasks.

Main categories:

•System Software: manages hardware.

•Application Software: performs specific tasks for users.

WHAT IS MALWARE?

The word "malware" comes from the combination of "malicious" and "software."

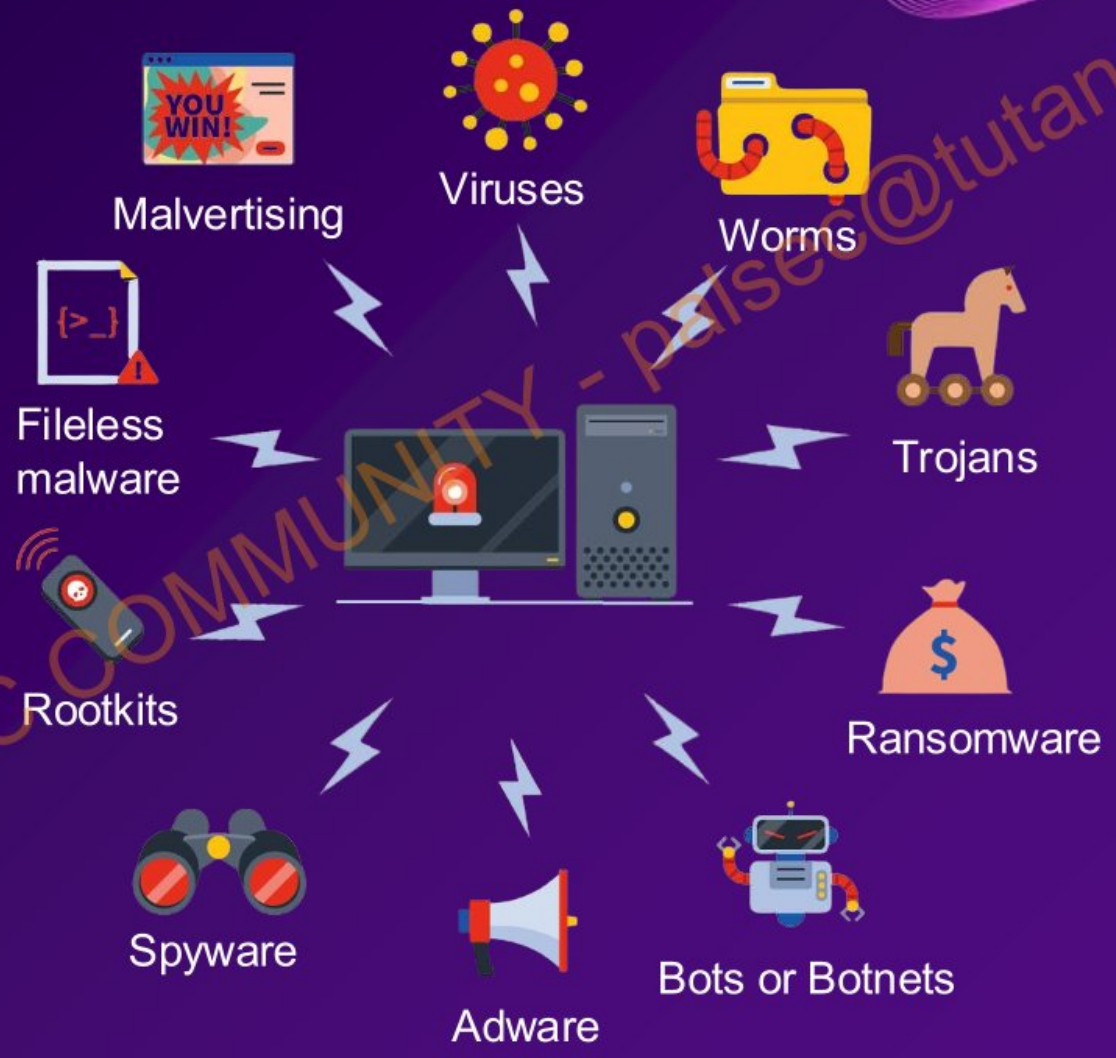
In Spanish, "mal" means "bad," making the term "bad software."

Malware is software that is intentionally created to:

1. Gain unauthorized access to or cause damage to a computer system.
2. Steal sensitive information such as personal, financial, or business data.
3. Exploit system resources for malicious activities, like launching attacks or mining cryptocurrency.

Each type of malware has a specific purpose and properties.

Types of Malware



Malware Defense Strategies

- Antivirus Software: Scans and removes malware.
- Firewalls: Blocks unauthorized access to systems.
- Regular Updates: Keeps software and operating systems patched.
- Safe Practices: Avoiding suspicious links, attachments, and downloads.
- Backup Solutions: Ensures data recovery in case of malware attacks

Social Engineering as a Tool for Spreading Malware

Most malware spread through social engineering

Social engineering is the psychological manipulation of individuals to perform actions or disclosure confidential information.

Most common type of social engineering:

Phishing emails: Fake emails that appear to come from trusted sources, tricking users to providing sensitive information or downloading malware.

Detecting Malicious Content: Email Analysis

Email is one of the most common vectors for delivering malicious content.

Someone has been trying to access your account. Is this a legitimate email or a malicious attempt to deliver malware?

Why is this malicious?

From Malware to IoT & OT Security Risks

IoT and OT systems face unique security challenges, making them prime attack targets.

Next, we'll explore their risks and how to secure them.

Internet of Things(IOT)

Devices with sensors, software, and technology that can connect to the internet or other networks to share data with other devices and systems.

These devices can "talk" to each other and work together without human interaction.

Example: Smart Refrigerator

Operational Technology(OT)

The hardware and software used to control and monitor machines, systems, in industries like manufacturing, energy, and transportation.

Example: Car Manufacturing

OT vs. IoT

Aspect	OT (Operational Technology)	IoT (Internet of Things)
Main Purpose	Ensures safety, reliability, and stability in industries.	Enhances automation, efficiency.
Examples - Usage	Chemical factories	Smart homes, Smart cities, Smart buildings

IOT Risks

- Low processing power
- Physical vulnerabilities
- Shared network access

IoT security breaches

Mirai botnet

In 2016, the Mirai Botnet exploited unsecured IoT devices to create a botnet of 145,000 devices, to perform DDoS attacks on services like Netflix and Twitter.

OT Risks

- Malware infiltration
- Lost revenue
- Loss of human life

OT security breaches

Stuxnet

Stuxnet is the first targeted cyberattack on OT, discovered in 2010, designed to target industrial control systems, specifically to destroy Iran's nuclear enrichment facilities.

Secure your IoT devices

- Physical security
- Encrypted data transfer
- Network firewall

Secure your OT

- Implement multifactor authentication (MFA)
- Network segmentation
- Limit access to the internet

THANKS