EUROPOL | EC3 European Cybercrime Centre

MALWARE BASICS

Malware is short for ***mal***icious soft***ware***. It is designed to infiltrate a computer system or mobile device without the owner's consent to gain control over the device, steal valuable information or damage the data. Malware remains a key threat both for private citizens and businesses. There are many types of malware, and they can complement each other when performing an attack.

TROJAN

It poses as a legitimate programme (or is embedded within one), but has malicious intentions. The damage it can cause depends on the motivation of the attacker: spying, stealing data, deleting files, expanding a botnet, performing DDoS attacks, etc.

BACKDOOR/ RAT

*Remote Access Trojan

It allows remote and unauthorised access to a computer system. Backdoors can be detected (if they already exist) or installed via another piece of malware. It gives almost total control to the attacker, who can perform a wide range of actions: monitoring, interfering, intercepting, modifying, etc.

RANSOMWARE

It either partially or completely prevents users from accessing their electronic devices, demanding them to pay a ransom by a certain deadline to regain control. There are two well-known types: WINLOCKER locks the device screen and restricts access to the whole system, while CRYPTOLOCKER encrypts relevant files (documents, photos or databases).

ROOTKIT

A collection of programmes that enable administrator-level access to a computer or computer network. Once installed, it masks the fact that a system has been compromised, allowing the attacker to gain root or privileged access to the computer and, possibly, other machines on the network.

FAKE ANTIVIRUS

Fake applications that pretend to scan and find malware/security threats on a user's device, misleading them into paying for the simulated removal. Besides the standard payload (50-100 EUR) to remove the malware, they normally contain a Trojan.

COMPUTER WORM

It replicates itself over a computer network with no user interaction, via email, file sharing and links to infected websites. It can perform different actions, exploiting vulnerabilities automatically without further guidance.

ADWARE

Applications displaying advertising banners or pop-up windows, usually integrated into another programme offered at no charge or low cost. It tracks users' behaviour on the internet without their knowledge (visited websites) for advertising purposes.

SPYWARE

Applications unwittingly installed on a computer that monitor users' activity and transmit the information to a third party. They can get into a computer in various ways: as a software virus, as the result of installing a new (genuine) programme or by visiting malicious websites, among other ways.

FILE INFECTOR VIRUS

It infects executable files (such as .COM and .EXE) by inserting infected code or overwriting them, with the intention of causing permanent damage or making them unstable. When the executable file runs, so does the file infector virus.

Malware remains one of the key threats in cybercrime

Among the different types, ransomware remains a top threat for EU law enforcement

The volume of malware in mobile platforms is increasing

Email spam continues to be one of the most common methods of malware distribution

Phishing attacks are shifting to other distribution channels, like social media

source: IOCTA 2015

Links and attachments in unsolicited emails, visits to unreliable websites, pop-up windows, open Wi-Fi networks, pirated software, peer-to-peer sharing websites and removable storage devices, paired up with the use of social engineering are common ways to get infected with malware!

TIPS & ADVICE

Keep your devices' operating system and all software current

Install and keep antivirus and firewall software updated on your devices

Back up the data stored on your computer regurlarly, on a separate storage device and offline

Think before you click on banners and links without knowing their true origin and avoid websites with pirated material

Only download files, software and apps from trusted sources

Beware of unusual looking messages received through email, social networks or instant messaging tools, even from someone you know

Created by Europol

UNDERSTANDING MALWARE

Malware is short for ***mal***icious soft***ware***. It is designed to infiltrate a computer system or mobile device without the owner's consent to gain control over the machine, steal valuable information or damage the data. There are many types of malware, and they can complement each other when performing an attack

Malware remains one of the key threats in cybercrime

Among the different types, ransomware remains a top threat for EU law enforcement

The volume of malware in mobile platforms is increasing

Email spam continues to be one of the most common methods of malware distribution

Phishing attacks are shifting to other distribution channels, like social media

source: IOCTA 2015

Created by Europol

EUROPOL
EC3 | European Cybercrime Centre

MALWARE: COMMON SOURCES OF INFECTION

EMAIL: Opening suspicious or unsolicited attachments or clicking on links from spam/phishing emails and unknown senders

WEBSITES: Clicking on links to unknown websites or just by visiting them (i.e. websites featuring adult content)

POP-UP WINDOWS: Clicking on them to download software or to view compromised advertisements

OPEN WI-FI: Cybercriminals use these networks to harvest your personal data and access your electronic systems

SOFTWARE: Downloading pirated or free software (games, screen savers, etc.) or downloading files via peer-to-peer networks

REMOVABLE STORAGE DEVICES: Malware can spread by copying itself to any removable device connected to a computer system

Cybercriminals will use social engineering and phishing techniques to trick you into performing any of the described actions and obtain your personal information

EUROPOL
EC3 | European Cybercrime Centre

Created by Europol

TROJAN

WHAT IS IT?

A legitimate or useful-looking computer programme (or embedded within one) but with malicious intentions

WHAT DOES IT DO?

It depends on the attacker's motivation: spying, stealing data, deleting files, expanding a botnet, performing DDoS attacks, etc.

HOW DOES IT SPREAD?

It requires user interaction, normally by opening an email attachment or downloading/running a file from a website; social engineering is common

EUROPOL
EC3 | European Cybercrime Centre

Created by Europol

RANSOMWARE

WHAT IS IT?

It prevents or limits users from accessing their system or devices, demanding them to pay a ransom through certain online payment methods (and by an established deadline), in order to regain control of their data

HOW DOES IT SPREAD?

It can be downloaded through fake application updates or by visiting compromised websites. It can also be delivered as email attachments in spam or dropped/downloaded via other malware (i.e. a Trojan)

TWO WELL-KNOWN TYPES

WINLOCKER: locks the device screen and restricts access to the whole system
CRYPTOLOCKER: encrypts relevant files (documents, photos or databases)

ADVICE

Never pay.
There is no guarantee that you will regain access to the device/files

EUROPOL
EC3 | European Cybercrime Centre

Created by Europol

POLICE RANSOMWARE

WHAT IS IT?

A variant of the ransomware winlocker which uses law enforcement symbols to lend authority to the message and to coerce victims into making the payment

HOW DOES IT SPREAD?

It can be downloaded through fake application updates or by visiting compromised websites. It can also be delivered as email attachments in spam or dropped/downloaded via other malware (i.e. a Trojan)

HOW TO RECOGNISE IT?

The message is alleged to be police action against illegal online behaviour of the victim, such as illegal file-sharing, downloading or accessing online child abuse material, or visiting terrorist websites

New cases of police ransomware haven't been detected in the last years

EUROPOL
EC3 | European Cybercrime Centre

Created by Europol

BACKDOOR/RAT *

*Remote Access Trojan

WHAT IS IT?

An application that allows remote and unauthorised access to a computer system

WHAT DOES IT DO?

It gives almost total control to the attacker, who can perform a wide range of actions: monitoring, interfering, intercepting, modifying, capturing, etc.

HOW DOES IT SPREAD?

Backdoors can be detected (if they already exist) or installed via another piece of malware. Remote Administration Trojans (RATs) are both Trojan and Backdoor: a seemingly legitimate application that provides access to the system

EUROPOL
EC3 | European Cybercrime Centre

SPYWARE

WHAT IS IT?

An application that is unwittingly installed on a computer to monitor users' activity and transmit the information to a third party

WHAT DOES IT DO?

It tracks users' behaviour on the internet and it gathers information without their knowledge (visited websites, personal data, passwords, etc.). It takes up a considerable amount of bandwidth and it may cause your computer to operate slowly

HOW DOES IT SPREAD?

Spyware can get in a computer in various ways: as a software virus, as the result of installing a new (genuine) programme or by visiting malicious websites, among other ways

EUROPOL
EC3 | European Cybercrime Centre

Created by Europol

ADWARE

WHAT IS IT?

An application that displays advertising banners or pop-up windows while a programme is running

WHAT DOES IT DO?

It often includes code that tracks users' behaviour on the internet and it gathers information without their knowledge (visited websites) usually for advertising purposes

HOW DOES IT SPREAD?

Usually integrated into another programme offered at no charge or at low cost

EUROPOL
EC3 | European Cybercrime Centre

Created by Europol

FAKE ANTI-VIRUS
ROGUE ANTI-VIRUS
SCAREWARE

WHAT IS IT?

A fake application that pretends to scan and find malware/security threats on a user's device, misleading them into paying for the simulated removal

WHAT DOES IT DO?

Besides the standard payload (50-100 EUR) to remove the malware, they normally contain a Trojan. If the user pays, the credit card details will probably be stolen

HOW DOES IT SPREAD?

Various tactics to convince the user: spam email, social media messages with the software installer attached or compromised websites displaying fake security warnings

EUROPOL
EC3 | European Cybercrime Centre

Created by Europol

COMPUTER WORM

WHAT IS IT?

A programme that replicates itself over a computer network and usually performs malicious actions, exploiting vulnerabilities automatically without further guidance

WHAT DOES IT DO?

They can cause harm by consuming bandwidth, taking up the computer's memory or hard disk space, deleting files or sending documents via email. They can be used to download and install other kinds of malware, such as backdoors. Another purpose could be enlarging a botnet network

HOW DOES IT SPREAD?

No user action needed. They spread exponentially through a network via email, a file sharing network, removable media exchange and links to infected websites

EUROPOL
EC3 | European Cybercrime Centre

Created by Europol

FILE INFECTOR VIRUS

WHAT IS IT?

A type of malware that infects executable files (such as .COM and .EXE) by overwriting them or inserting infected code, with the intention of causing permanent damage or making them unusable

WHAT DOES IT DO?

Consequences may vary from small disturbances to damaging the data on the machine. Bigger problems may require the complete reformatting of the device

HOW DOES IT SPREAD?

By self-replication and by attaching itself to executable files. When the executable file runs, so does the File Infector Virus

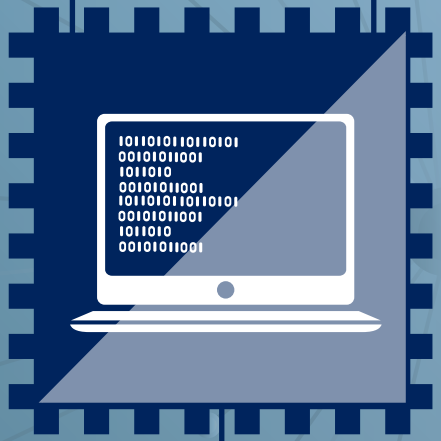
EUROPOL
EC3 | European Cybercrime Centre

Created by Europol

ROOTKIT

WHAT IS IT?

A collection of programmes that enable administrator-level access to a computer or computer network. Once installed, it masks the fact that a system has been compromised, allowing the attacker to gain root or privileged access to the computer and, possibly, other machines on the network



WHAT DOES IT DO?

A rootkit may consist of spyware and other programmes that monitor traffic and keystrokes, create a backdoor into the system, alter log files, attack other machines on the network, alter existing system tools to escape detection, etc.

HOW DOES IT SPREAD?

It requires user interaction to be installed in the system. It can be part of a payload of another type of malware

REMOVAL

If a rootkit is detected, you may have to erase the computer's hard drive and reinstall the operating system

EUROPOL
EC3 | European Cybercrime Centre

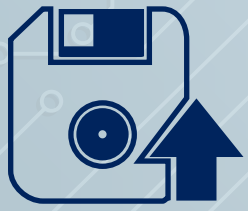
Created by Europol

MALWARE: TIPS & ADVICE

Install and keep antivirus and firewall software updated on your devices

Keep your devices' operating system and all software current

Only download files, software and apps from trusted sources



Back up the data stored on your computer regularly, on a separate storage device and offline

Beware of unusual looking messages received through email, social networks or other tools, even from someone you know

Think before you click on banners and links without knowing their true origin and avoid websites with pirated material

EUROPOL
EC3 | European Cybercrime Centre

****

Don't forget to use multiple and strong passwords in all your accounts!

Created by Europol