

Lesson 7

Malicious Codes (Malware)

Outline

1. What is a malware?
2. Common types of malware
3. How to detect & prevent them?

What is a malware?

- **A malware** is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.
- **Malware** can be classified into several categories, depending on propagation and concealment.

What is a malware?

- **Propagation**
 - **Virus**: human-assisted propagation
 - **Worm**: automatic propagation without human assistance
- **Concealment**
 - **Rootkit**: modifies operating system to hide its existence
 - **Trojan**: provides desirable functionality but hides malicious operation
- Various types of payloads

Malware Goals



Data

- Company IP
- Personally Identifiable Information (PII)



Money

- Cryptocoins!
- Financial Info



Damage

- Destroy Facilities
- Cause Harm

Delivery & Techniques



Delivery & Techniques



Malware Types

- Basic types:
 - Virus
 - Worms
 - Trojan Horse
- Several variants of the basic types exist:
 - Time Bomb
 - Logic Bomb
 - Keylogger
 - Rootkit
 - Adware
 - Spyware
 - ...

Keylogger

Work Examiner keylogger software: you should know what they do on computer!



Why Work Examiner Keylogger?

- keystrokes, emails and chats logs
- screenshots in real-time and history mode
- websites and programs usage reports
- easy installation
- stealth work mode

DOWNLOAD NOW
free 30-day trial

More than 20+ computers?
[Try Pro version](#)

WannaCry Ransomware Screenshot:



CryptoLocker Ransomware Screenshots:



Cryptowall Screenshot example:

Your files are encrypted.


To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **10/06/14 - 09:14** the cost of decrypting files will increase **2 times** and will be **1000 USD/EUR**.

Prior to increasing the amount left:
119h 58m 24s

Your system: **Windows 7 (x64)** First conned IP: **[redacted]** Total encrypted **28** files.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?



1. You should register Bitcoin wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:

- [Coin.mx](#) - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
- [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- [coinmr.com](#) - Another fast way to buy bitcoins
- [bitquick.co](#) - Buy Bitcoins Instantly for Cash
- [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
- [Cash Into Coins](#) - Bitcoin for cash.
- [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
- [anxpro.com](#)
- [bitylicious.com](#)
- [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 0.79 BTC to Bitcoin address: 1L7SLmazb6cy614zsD5Lwz4bxx1anJvDeV [Get QR code](#)

4. Enter the Transaction ID and select amount:

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386d929c40bf34f19a27c42f07f5cd3e2aa08114c4d1f2)



NSA INTERNET SURVEILLANCE PROGRAM

PRISM

COMPUTER CRIME PROSECUTION SECTION



YOUR COMPUTER HAS BEEN LOCKED!

Your computer has been locked due to suspicion of illegal content downloading and distribution.

The illegal content (414 Mb of photo and video files) was automatically classified as child pornographic materials.

The downloading and distribution of illegal content, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251 Sexual exploitation of children (Production of child pornography)

18 U.S.C. § 2252 Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A Certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 6 months to 10 years and shall be fined up to \$250,000.

Collected technical data

Your IP address: [REDACTED]
Your host name: [REDACTED]
Source or intermediary sites: [REDACTED]
Location: [REDACTED]

Illegal content found:



ALL INFORMATION FILED FROM YOUR COMPUTER WERE TRANSMITTED TO A SPECIAL SERVER AND SHALL BE DELETED IMMEDIATELY. DON'T TRY TO CORRUPT ANY DATA OR DAMAGE YOUR COMPUTER IN AN UNAUTHORIZED WAY.

Your case can be classified as occasional/unmotivated, according to 17 (U.S. Code) §512

Thus it may be closed without prosecution.
Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of \$300



MoneyPak

Exchange your cash for a MoneyPak voucher and use your voucher code in the form below:

Code: 1 2 3 4 5 6 7 8 9 0

Status: Waiting for payment

Permanent lock on 09/28/2013 8:45 pm EST



Where can I buy MoneyPak:



http://localhost/shell/email_us.aspx localhost

Address	Current : C:\inetpub\wwwroot\shell\ Use Reset Form	
Login	Do it : <input type="text"/>	Do it
Command	Process : cmd.exe	Execute
	Command : <input type="text"/>	
Upload	File name : <input type="text"/> Browse...	<input type="checkbox"/> Is virtual path Upload
	Save as : <input type="text"/>	
	New File name : <input type="text"/>	
Download	File name : <input type="text"/>	Download
Upload Base64	Base64 File : <input type="text"/>	<input type="checkbox"/> Is virtual path Upload
	File Path and Name : <input type="text"/>	
Sql Server	<input type="button" value="Standard Connection Sample"/> <input type="button" value="Trusted Connectin Sample"/>	
	Connection String : <input type="text"/>	Run
	Query : <input type="text"/>	
Change Creation Time	File name : <input type="text"/>	Get
	From This File : <input type="text"/>	Set
	New Time : <input type="text"/>	Set

Computer Virus

- ***Virus***: a program that attaches copies of itself into other programs.
 - Propagates and performs some **unwanted functions**
 - Viruses are not programs
 - *Definition from RFC 1135: A virus is a piece of code that inserts itself into a host [program], including operating systems, to propagate. It cannot run independently.* It requires that its host program be run to activate it.

Four Phases of a Virus

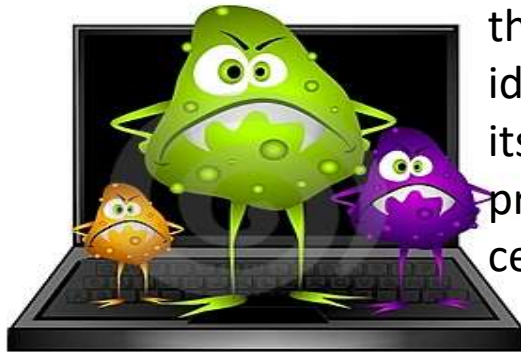
The virus is activated to perform the function for which it was created

1. Dormant Phase



- The virus is idle
- Not all viruses have this stage

2. Propagation Phase



the virus places an identical copy of itself into other programs or into certain system areas

3. Triggering Phase



4. Execution Phase



- The function is performed
- The function may be harmless or damaging

Virus Types

- *Parasitic virus – ký sinh:*
 - Attaches itself to a file and replicates when the infected program is executed
 - most common form
- *Memory resident virus:*
 - lodged in main memory as part of a resident system program
 - Virus may infect every program that executes

Virus Types

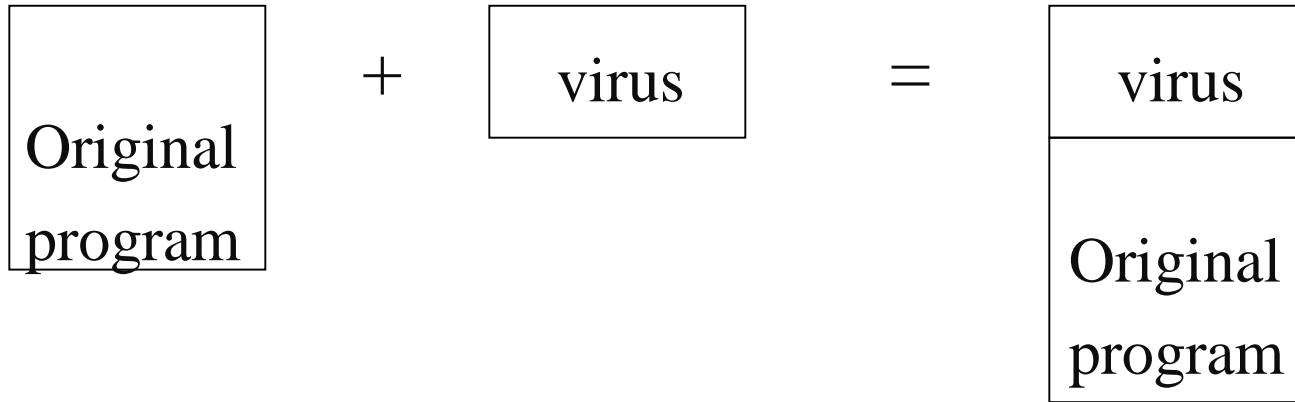
- *Boot Sector Viruses:*
 - Infects the boot record and spreads when system is booted
 - Gains control of machine before the virus detection tools
 - Very hard to notice
- Macro Virus:
 - virus is part of the macro associated with a document

Virus Types

- *Stealth virus*
 - A form of virus explicitly designed to hide from detection by antivirus software
- *Polymorphic virus:*
 - A virus that mutates with every infection making detection by the “signature” of the virus difficult

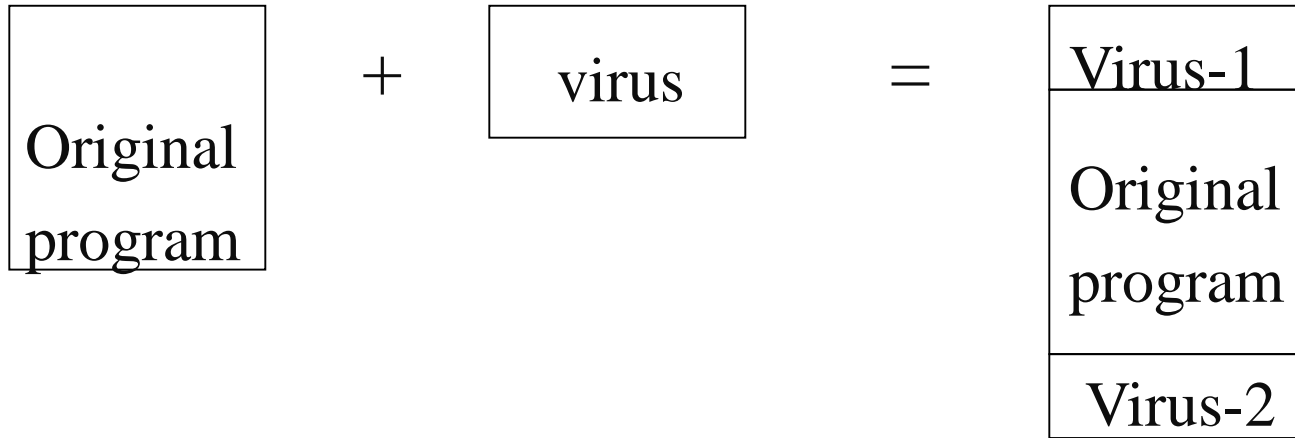
Mutate: đột biến

How Viruses Append



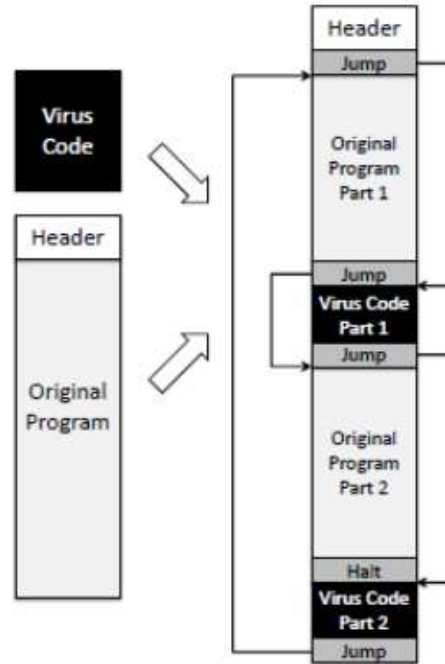
Virus appended to program

How Viruses Append



Virus surrounding a program

How Viruses Append



Virus integrated into program

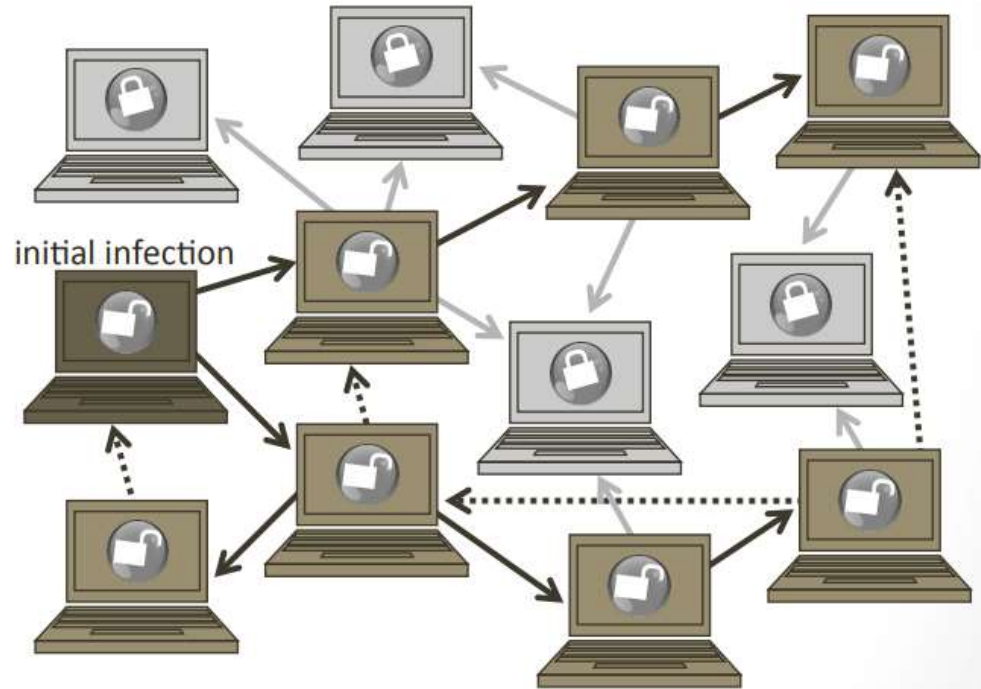
Computer Worms



- A computer worm is a malware program that spreads copies of itself without the need to inject itself in other programs, and usually without human interaction.
- In most cases, a computer worm will carry a malicious payload, such as deleting files or installing a backdoor.

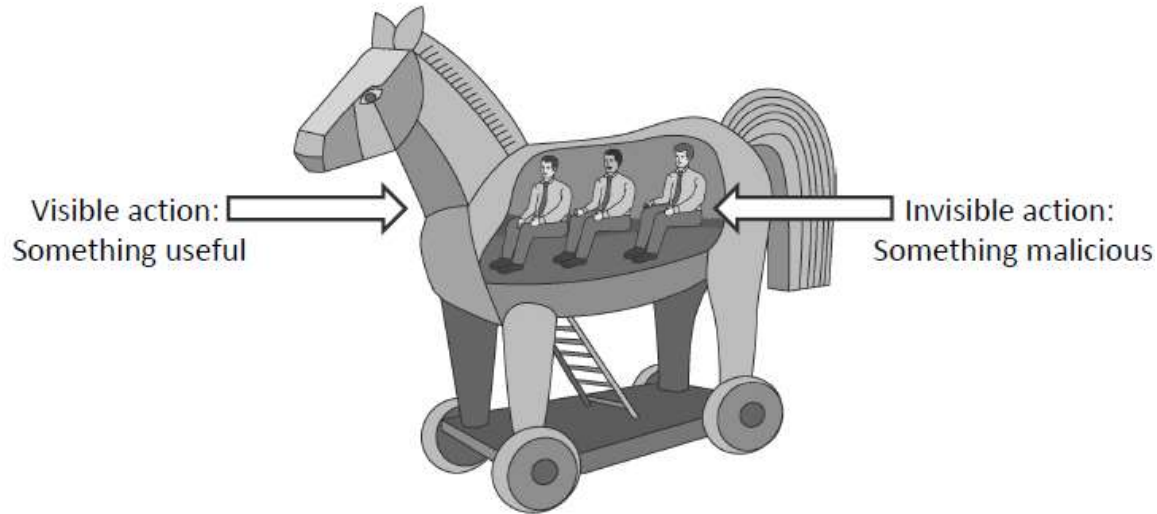
Worm Propagation

- Worm propagation by finding and infecting **vulnerable hosts**



Trojan Horses

- A Trojan horse is a malware program that appears to perform some **useful tasks**, but which also does something with **negative consequences**.



Logic/Time Bomb

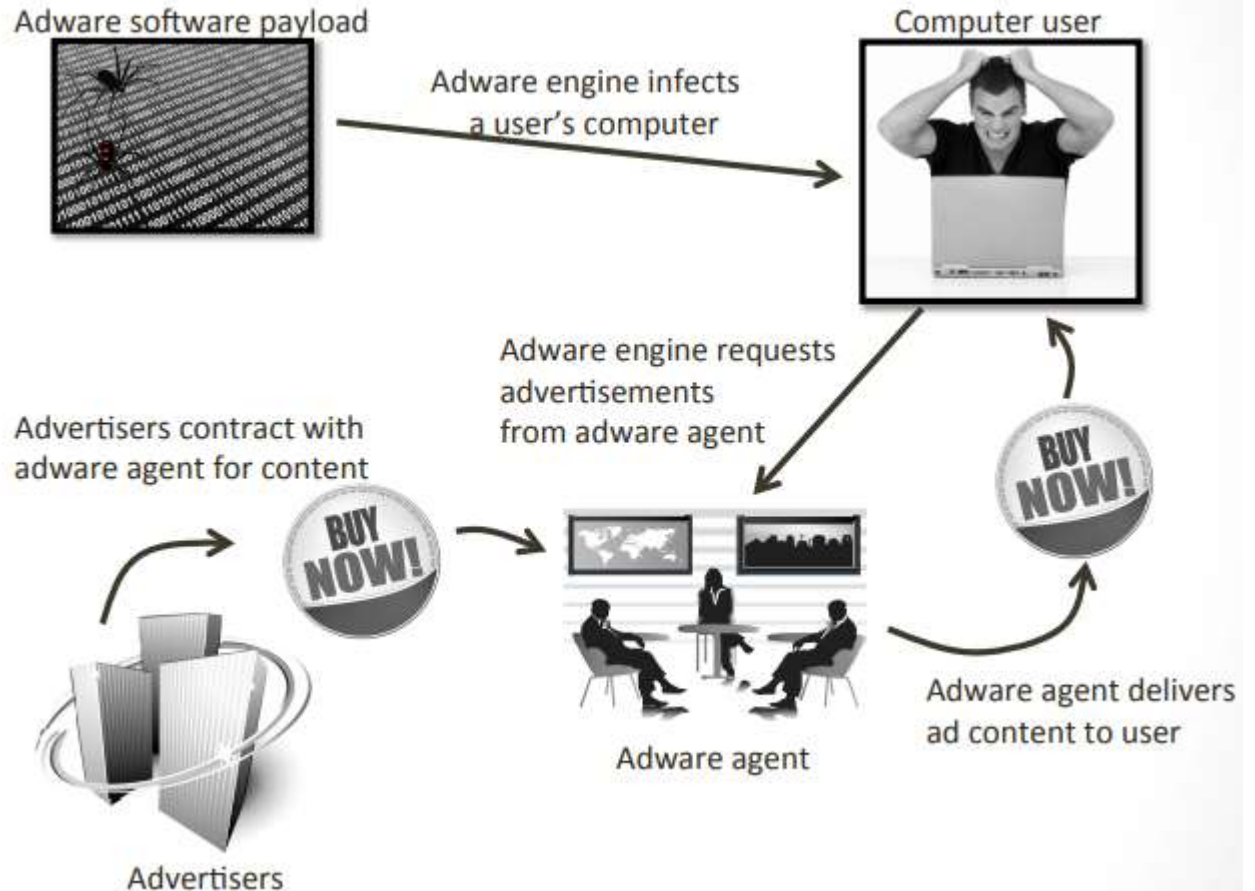
- programmed threats that lie dormant for an extended period of time until they are triggered
 - When triggered, malicious code is executed



Rootkit

- ***Rootkit:*** Rootkits are designed to conceal certain objects or activities in your system. Often their main purpose is to prevent malicious programs being detected – in order to extend the period in which programs can run on an infected computer

Adware



Spyware

Spyware software payload



1. Spyware engine infects a user's computer.



Computer user



2. Spyware process collects keystrokes, passwords, and screen captures.



3. Spyware process periodically sends collected data to spyware data collection agent.

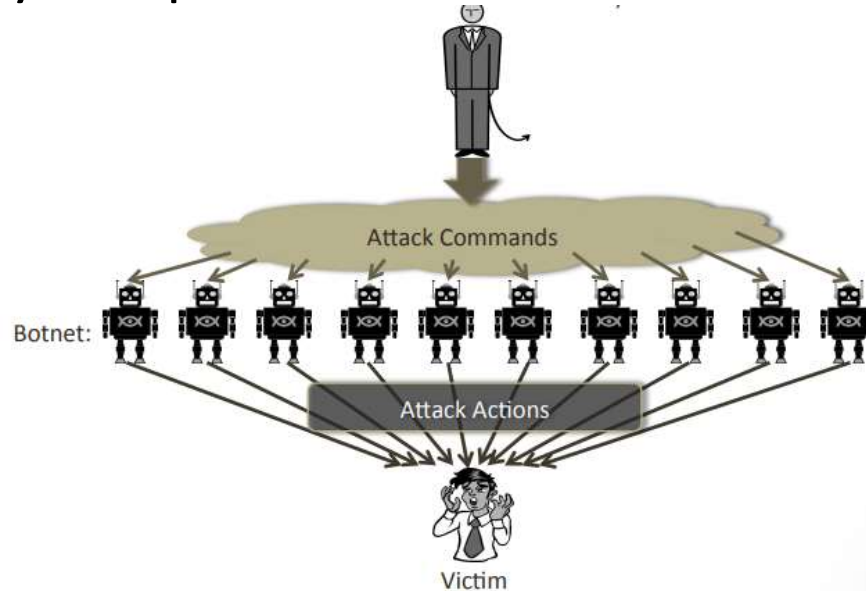


Spyware data collection agent

Software which sends information to its creators about a user's activities (e.g., passwords, credit card numbers, and other information that can be sold on the black market.

Malware Zombies

- Malware can turn a computer into a zombie, which is a machine that is controlled externally to perform malicious attacks, usually as a part of a **botnet**.



Where does Malicious Code Hide?

1. Email
2. Web Content
3. Legitimate Sites
4. File Downloads

....

How to detect & prevention them

- A **detection system** may detect *suspicious activities*.
- A **prevention system** must *identify* and *stop malicious attacks* before they do damage and have a chance to infect a system.

Malware Countermeasures

- **Signatures**
 - Find a string that can **identity the virus**
- **Heuristics Analysis -**
 - Useful to identify new and “zero day” malware
 - **Analyze program behavior** (network access, file open, attempt to delete file, attempt to modify the boot sector,...)
 - Heuristic methods can trigger false alarms
- **Sandbox analysis**
 - Running the executable in a VM
 - Observe it (file activity, network, memory,...)
- **White/Black listing**

Signatures

- Scan compare the analyzed object with a database of signatures
- A signature is a virus fingerprint (*E.g., a string with a sequence of instructions specific for each virus*)
- A file is infected if there is a signature inside its code (*Fast pattern matching techniques to search for signatures*)
- All the signatures together create the malware database that usually is proprietary

Antivirus Approaches

- *Detection*
 - determine infection and locate the virus
- *Identification*
 - identify the specific virus
- *Removal*
 - remove the virus from all infected systems, so the disease cannot spread further
- *Recovery*
 - restore the system to its original state

Preventing Virus Infection

- **Prevention:**
 - Good source of software installed
 - Isolated testing phase
 - Use virus detectors
- **Limit damage:**
 - Make and retain backup copies important resources

Preventing Malicious Attacks on the Internet

- Up-to-date
- Install a firewall
- **Scanning systems**

Malware analysis

- There are two fundamental approaches to malware analysis
 - **Static analysis**, which involves examining and analyzing the malware without executing it
 - **Dynamic analysis**, which involves executing the malware on the system and analyzing it.

Q & A