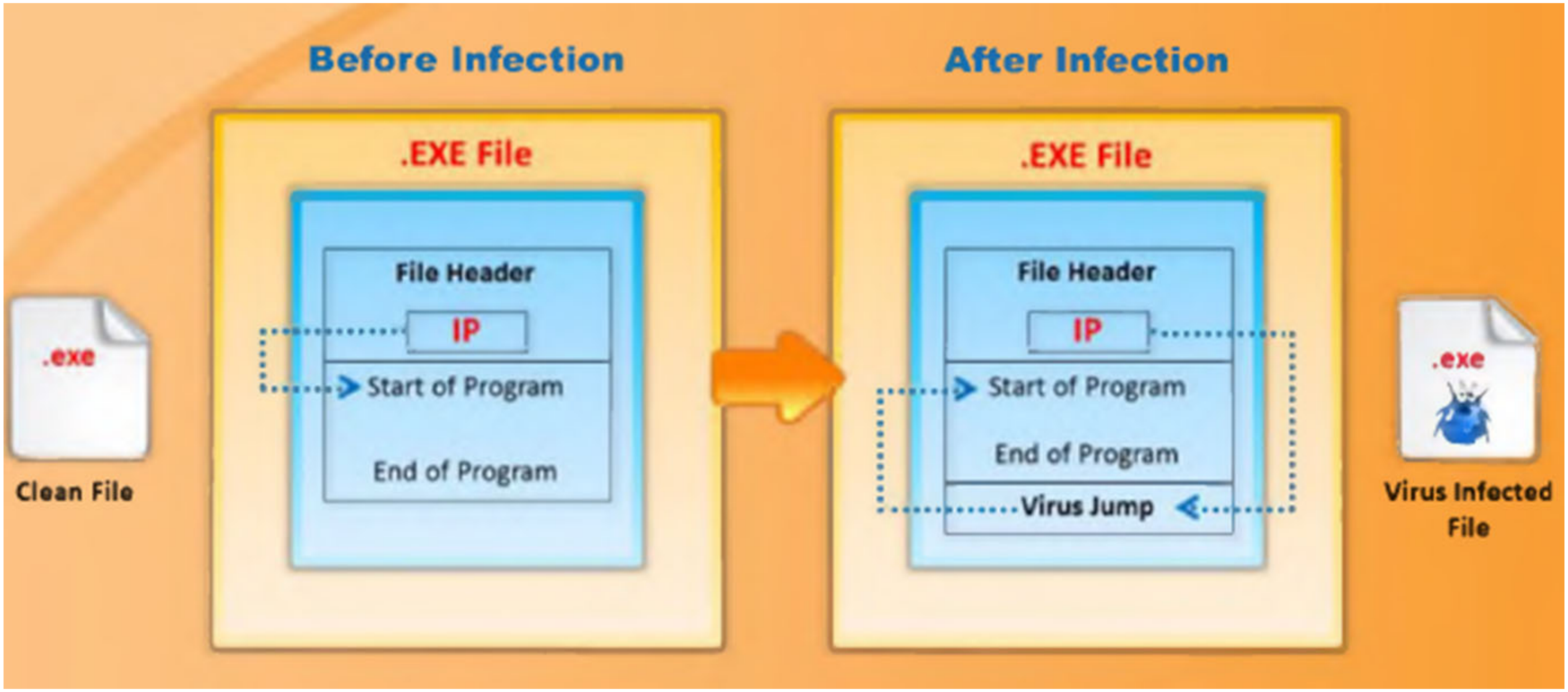
Virus

- A computer virus is a computer program written by attacker which is attached to another program or file like a PDF, word document, exe file enabling it to spread from one computer to another and infect them as it travels.



Virus cont…

- Some possible ways that cause computers get infected by virus are:
  - Downloading an infected file and executing it
  - Opening an infected E-mail attachment which causes virus to distribute itself out to all contacts on the victims email address book
  - Viewing E-mail in some versions of Microsoft Outlook
  - Viewing infected websites
  - …

Virus cont…

- Viruses need '2 factors' to operate:
  - Carrier: is the document or program to 'attach' itself to
  - user action: to initiate the propagation/triggering phase

Virus components

- Virus has three parts:
  - Trigger event: is the event or condition that determines when the payload is activated.
  - payload: what it does (its actions):
    - Data destruction or theft
    - Data encryption (ransomware)
    - Real-world damage such as Stuxnet that caused physical damage also (targeted to Siemens industrial control software)
    - Logic bomb: *"explodes" when a condition occurs*. Code inserted into malware by an intruder; lies dormant until a predefined condition is met
  - infection mechanism: enables replication/propagation

Phases of a virus

- The lifecycle of a virus includes:
  - Dormant phase: Virus is idle and waiting to get activated by a certain trigger event (such as date, presence of another program or file, …)
  - Triggering phase: Virus is activated by a trigger event to perform the function for which it was intended.
  - Execution phase: The intendent function is performed which can be:
    - harmless, such as a message on the screen
    - harmful, such as destruction of programs and data files
  - Propagation phase: Virus places a copy of itself (identical or not; it can morph to avoid detection) into other programs or certain system areas on disk. A virus will typically not propagate to another infected program.

Virus classification

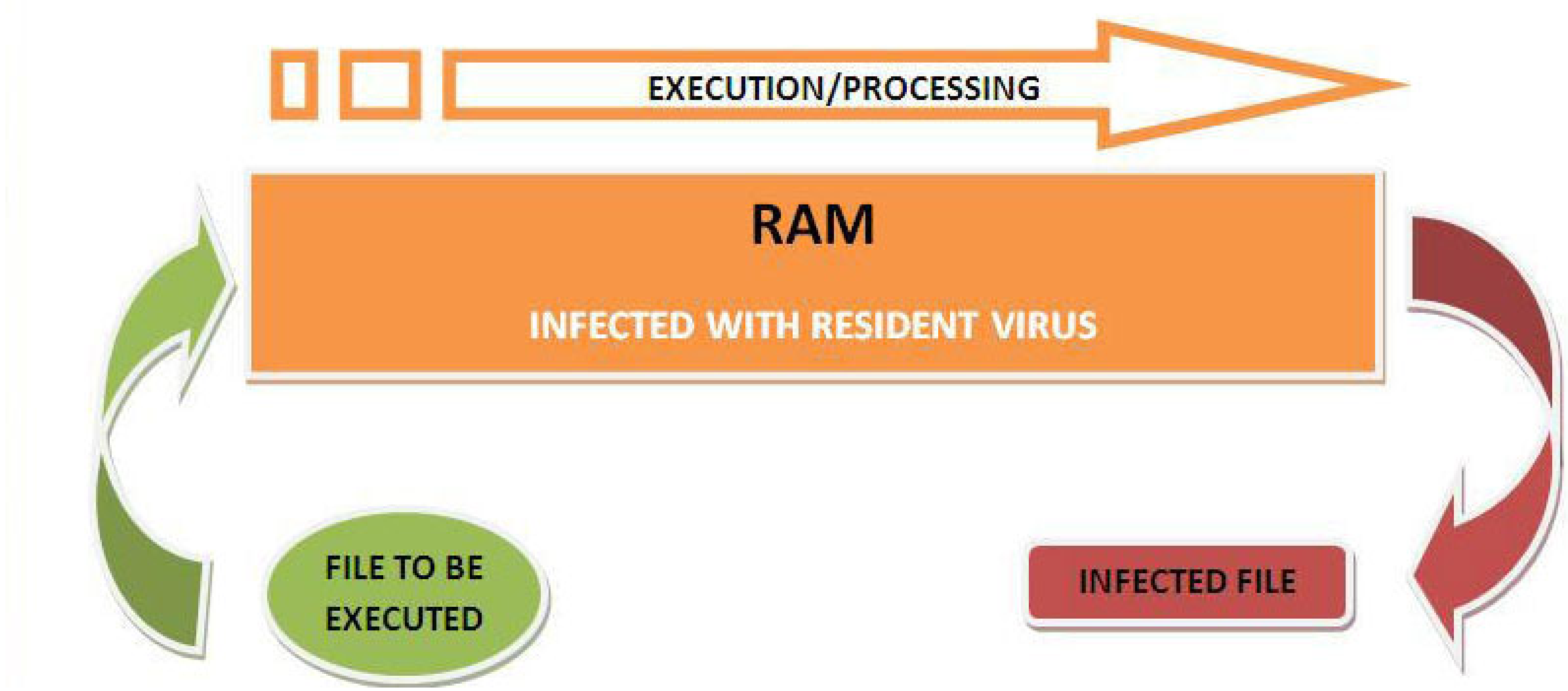
- By target:
  - Macro/scripting virus
  - multipartite: infects multiple ways
  - boot sector: infects a master boot record and spreads when a system is booted from the disk containing the virus
  - Bootkit
  - file infector: infects files that the OS considers executable

Virus classification cont…

- By concealment strategy:
  - Encrypted virus: a portion of the virus creates a random encryption key and encrypts the remainder of the virus and stores the key with the virus.
  - Stealth virus (مخفیانه): explicitly designed to hide itself (e.g., compression) from detection by antivirus software
  - Parasitic virus (انگلی): attaches itself to executable files **to replicate**. When the infected program is executed, by finding other executable files to infect
  - Memory-resident virus
  - polymorphic (چند ریختی) virus
  - metamorphic (دگرگونی) virus

Memory-resident virus

- Memory-resident virus places itself inside the memory as part of a system program.
- The virus gets activated whenever the OS runs and from that point on, the virus infects every program that opens and executes.



polymorphic (چند ریختی) virus

- Polymorphic is a virus in which the same code takes many forms as the virus can encrypt itself with a variable encryption key so that each copy of the virus looks different because it's encrypted with a different key (but the functionality the same).

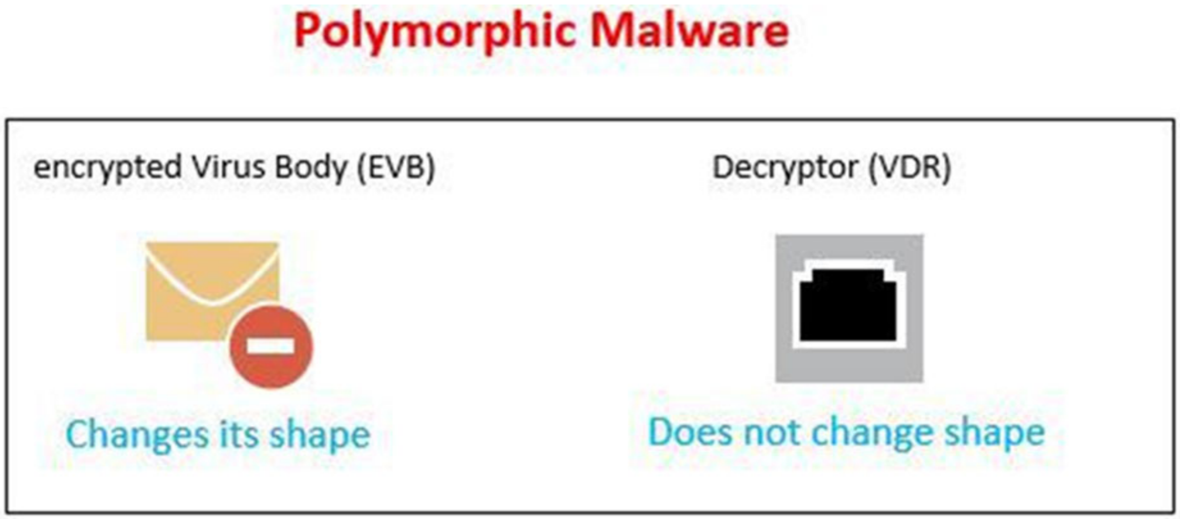
- A polymorphic virus decrypts its code, runs that code, and then when propagating itself, encrypts the decrypted code (to bypass signature detection) with a different key. Thus, the executed code is different on every machine its propagated to.

- Not all of the virus is encrypted.

polymorphic virus cont…

- Polymorphic virus has two parts:
  1. encrypted virus body (EVB): is the core malware code which changes its shape.
  2. virus decryption routine (VDR): is the code that is used to decrypt and encrypt the other part. This part does not change its shape and remains the same with each iteration. This makes the virus easier to identify.

- When an infected application launches, the VDR decrypt the EVB so it can execute and then re-encrypt it again.



polymorphic virus cont…

- The virus can be easier to be detected by AV because:
  - There is a decryption stub which is responsible to decrypt and run the encrypted virus. The decryption stub remains unencrypted and in the simplest polymorphic viruses this stub also remains constant (that part of it always looks the same) so it can be used to detect the presence of the virus.
  - Because the virus has to decrypt itself in order to operate, and because the unencrypted form of the virus doesn't change, AV products are often able to recognize the virus by emulating its execution for long enough that it will decrypt itself and then examining the result.

metamorphic (دگرگونی) virus

- Metamorphic is a virus in which the code mutates, so the code itself is different in each execution (but the functionality the same).
- A metamorphic virus can translate and rewrite it’s own code so that, once again, each copy of the virus looks different.
- Unlike polymorphic viruses, metamorphic viruses don’t really require a decryption stub because they aren’t encrypted. When the virus creates a new copy of itself it translates it is existing instructions into functionally equivalent instructions. Thus, no part of the virus remains constant and the virus is never returned to it’s original form during execution, which makes it more difficult for AV products to recognize.

metamorphic virus cont…

- The author may use multiple transformation techniques, including register renaming, code permutation, code expansion, code shrinking and garbage code insertion.
- In spite of the permanent changes to code, each iteration of metamorphic malware functions the same way. The longer the virus stays in a computer, the more iterations it produces and the more sophisticated the iterations are, making it increasingly hard for antivirus applications to detect, quarantine and disinfect.

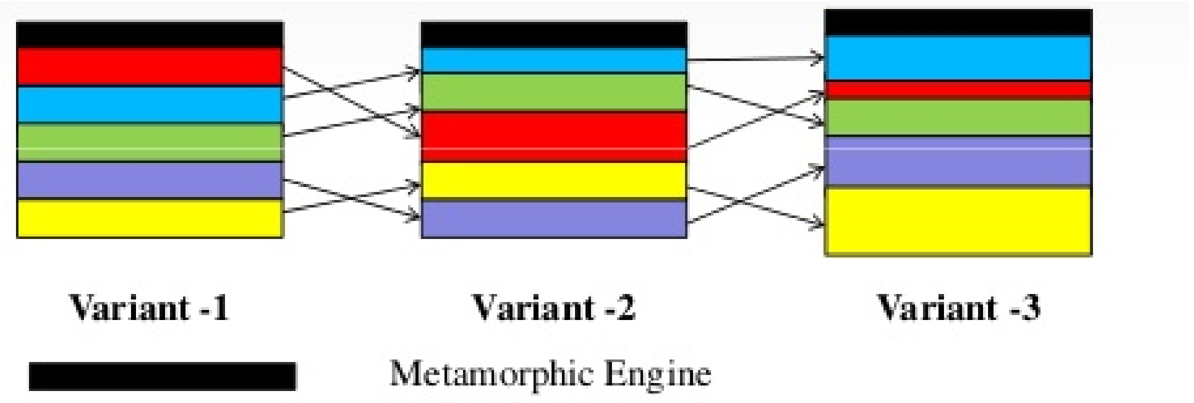
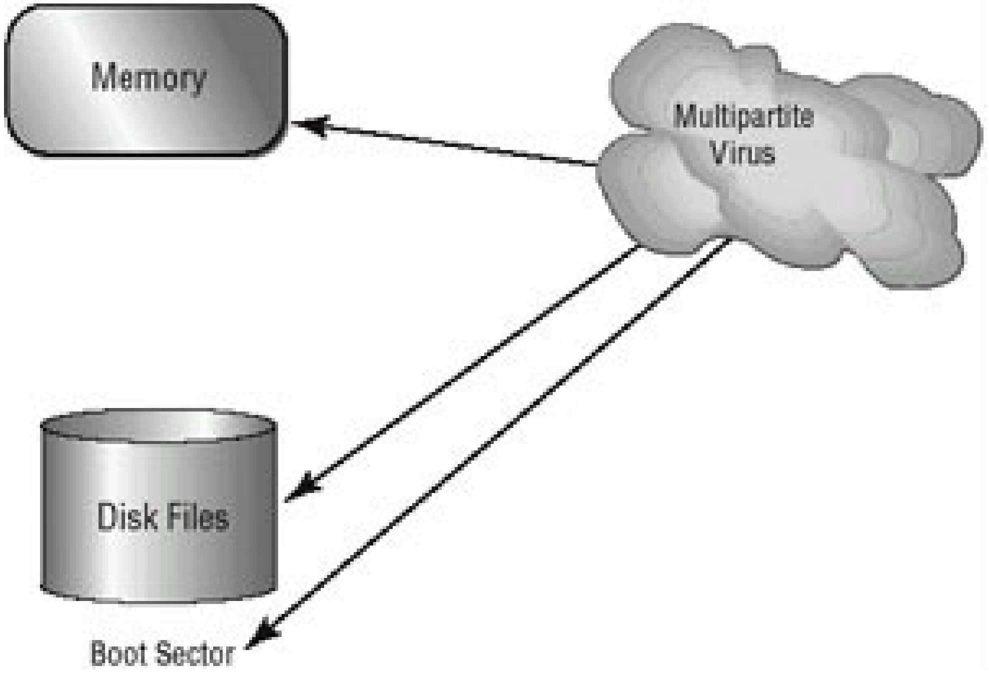


Diagram depicts metamorphic malware variants with reordered code

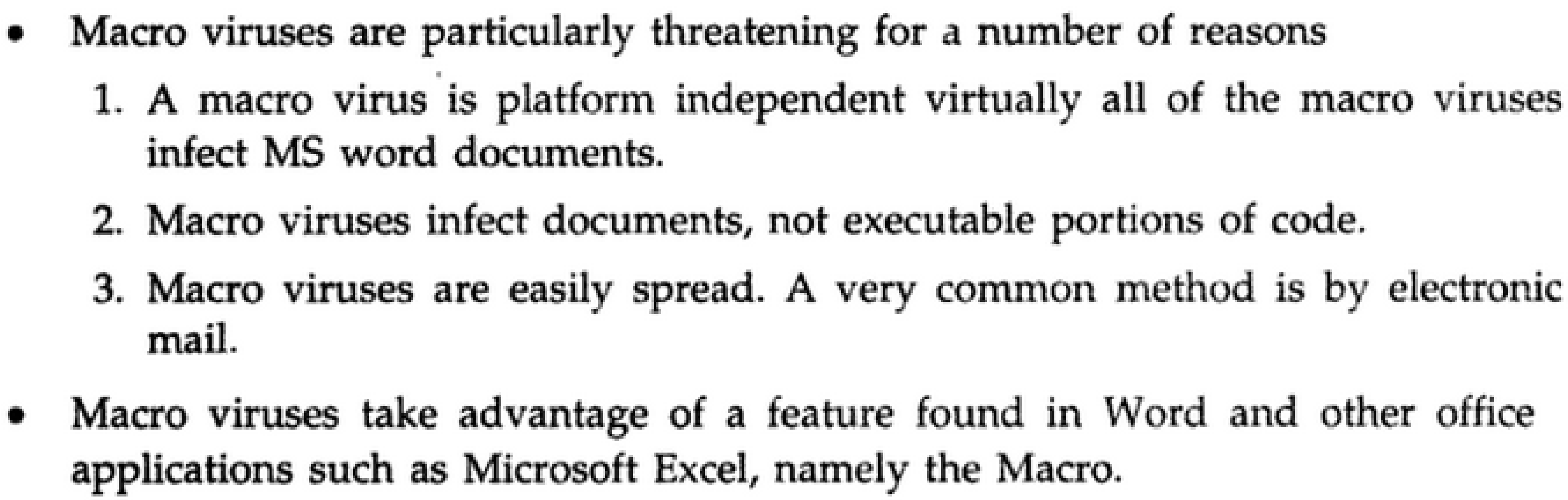
multipartite virus

- A Multi-part/Multipartite virus is a virus that attempts to attack and spreads in multiple ways.
- For example, it attacks both the boot sector and the executable files at the same time.

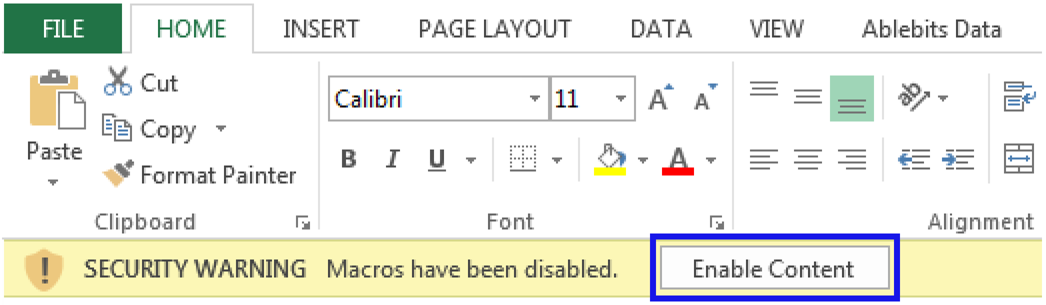


Macro virus

- Macro virus infects the files that have been created using some applications or programs that contain macros like doc, ppt, xls. It can hide itself in documents and triggered when document is viewed or edited



- Macro viruses are particularly threatening for a number of reasons
  1. A macro virus is platform independent virtually all of the macro viruses infect MS word documents.
  2. Macro viruses infect documents, not executable portions of code.
  3. Macro viruses are easily spread. A very common method is by electronic mail.
- Macro viruses take advantage of a feature found in Word and other office applications such as Microsoft Excel, namely the Macro.



SECURITY WARNING Macros have been disabled.

Rootkit/Listener

- The rootkit term comes from the two component words, “root” and “kit”, where “root” is the equivalent of the Windows Administrator, while “kits” are software designed to take root/administrator control of a PC, without informing the user.

- Rootkits are computer programs that are designed by attackers to gain root or administrative access to your computer by hiding deep inside your system.

- Once a rootkit installs itself on your computer, it will boot up at the same time as your PC. On top of that, by having administrator access, it can track everything you do on the device, scan your traffic, install programs without your consent, hijacker your computer’s resources.

Rootkit cont…

- Unlike viruses, it is not directly destructive and unlike worms, its objective is not to spread infection as wide as possible.

- Most often, rootkits are used to control and not to destroy. Of course, this control could be used to delete data files.

- rootkits run at the same privilege levels as most antivirus programs. This makes them that much harder to remove as the computer cannot decide on which program has a greater authority to shut down the other.

- Rootkits generally go much deeper than the average virus. They may even infect your BIOS – the part of your computer that's independent of the OS, making them harder to remove.

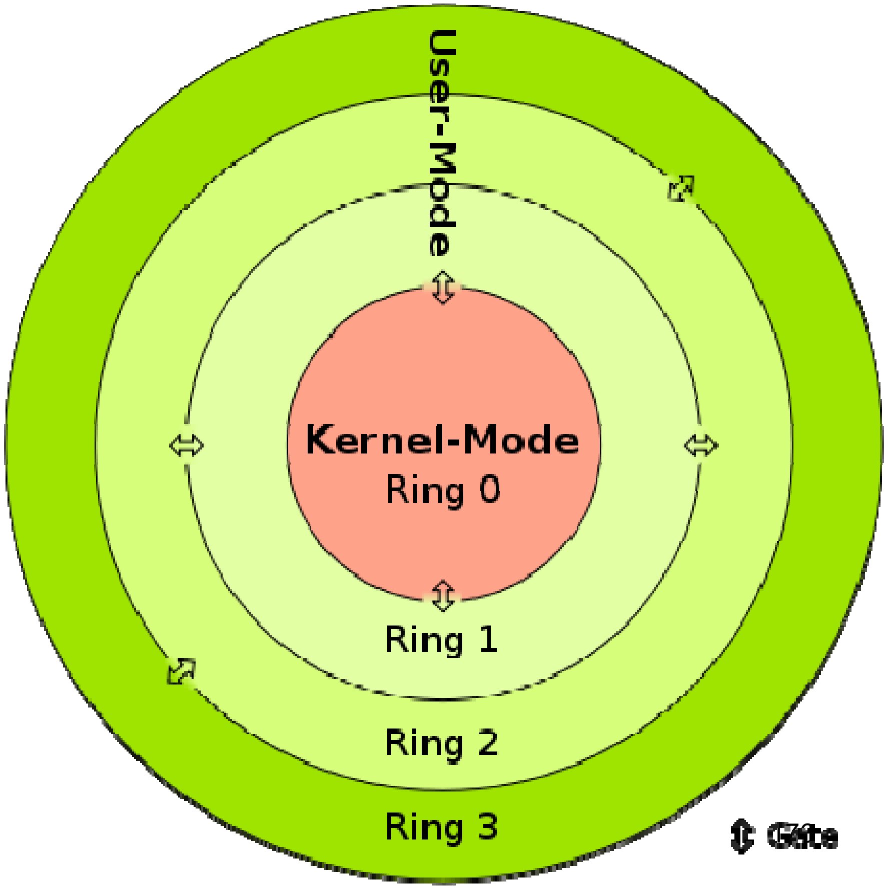
Rootkit cont…

- Rootkits are usually composed of three components:
  - Dropper: the dropper code starts the rootkit installation and can be activated by clicking a malicious link on a website or Email, or opening an infected PDF file, device driver, or shared libraries (DLL). The dropper launches the loader program and then deletes itself.
  - Loader: the loader loads the rootkit into memory. At this point the computer has been compromised.
  - rootkit itself

Types of Rootkits

- Different levels of control are illustrated in the protection ring model.
- The severity of a rootkit infection can be measured depending on how deep into the system it goes. The lower the ring, the higher the privilege the controller has.

Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner.

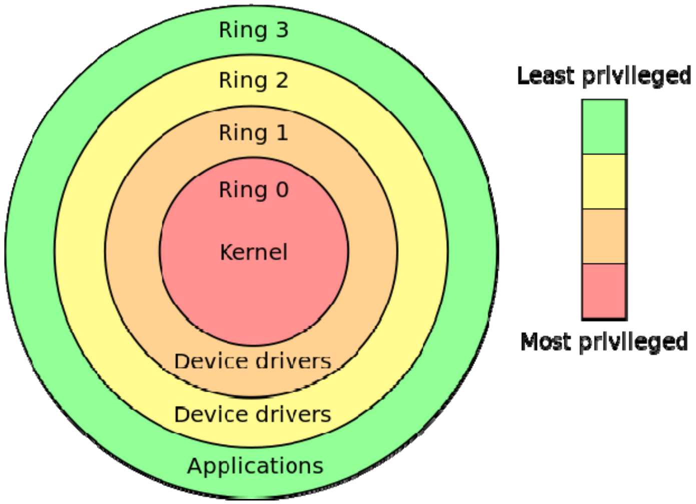


Types of Rootkits cont…

- Infections at the Ring 3 levels are fairly superficial, since these only infect applications such as Microsoft Office, Photoshop or other similar software.

- Ring 1 and 2 are deeper layers, such as the drivers for the video graphics card or your sound system.

- Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory. Since this type of rootkit is designed to function at the level of the OS itself, it can effectively add new code to the OS, or even delete and replace OS code. The kernel rootkits are deepest and hardest to remove since an antivirus (which mostly operates at Ring 3) doesn't have full access to Ring 0.

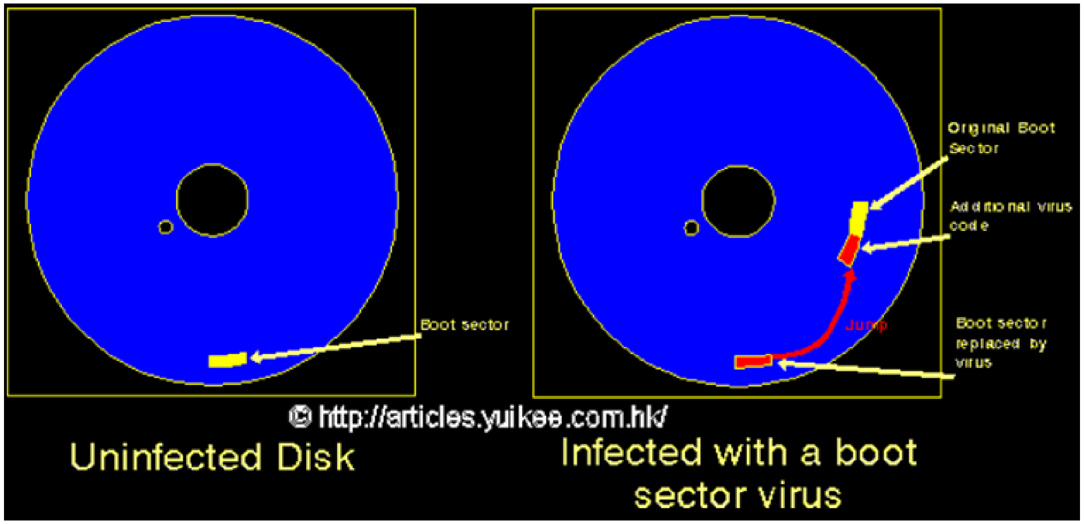


Ways of infection by rootkit

- There are different ways that we might get infected with a rootkit:
  - A rootkit may piggyback along with software that you thought you trusted. When you give this software permission to install on your computer, it also inserts a process that waits silently in the background for a command. And, since to give permission you need administrative access, this means that your rootkit is already in a sensitive location on the computer.
  - Another way to get infected is by standard infection techniques – either through shared disks and drives with infected web content. This infection may not easily get spotted because of the silent nature of rootkits.
  - There have also been cases where rootkits came pre-installed on purchased computers. The intentions behind such software may be good – for example, anti-theft identification or remote diagnosis – but it has been shown that the mere presence of such a path to the system itself is a vulnerability.
  - etc.

Boot sector virus

- A boot sector virus usually infects the computer by altering the master boot sector program. The virus replaces the default program with its own corrupted version.
- The virus runs each time the system boots.
- A boot sector virus is able to infect a computer only if the virus is used to boot up the computer. The computer will not be infected if the virus is introduced after the boot-up process or when the computer is running the OS.

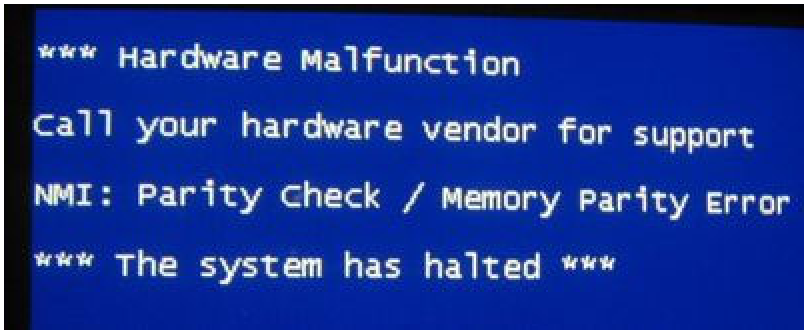

Boot sector
Original Boot Sector
Additional virus code
Jump
Boot sector replaced by virus
© http://articles.yuikee.com.hk/
Uninfected Disk
Infected with a boot sector virus

Boot sector virus cont…

- An example of a boot sector virus is Parity Boot. This virus's payload displays the message PARITY CHECK and freezes the OS, rendering the computer useless.

- This virus message is taken from an actual error message which is displayed to users when a computer's memory is faulty.

- As a result, a user whose computer is infected with the Parity Boot virus is led to believe that the machine has a memory fault rather than an disruptive virus infection.



```
*** Hardware Malfunction

Call your hardware vendor for support

NMI: Parity Check / Memory Parity Error

*** The system has halted ***
```

Worm

- Like the virus:
  - Worm is self-replicating program
  - Worm can spread from computer to computer

- Unlike the virus:
  - Worm is standalone software and does not need to attach itself to an existing program
  - Worm has capability to replicate/copy itself and travel/spread automatically **without need of any human action** (running a program, opening a file, etc.). To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them.
  - The worm infection is network-based while the virus infection is usually host-based (target computer).

Worm cont…

- Worm exploits computers in a network that contain security holes. Once a security hole is found, the worm will attempt to replicate itself from computer to computer (Stuxnet).

- One example is that worm can send a copy of itself to everyone listed in your contact list or email address book. Then the worm replicate and send itself out to everyone listed in each of the receiver contact list or email address book and it continues.

- A worm always seeks for network loopholes to replicate from computer to computer and thus most common way of intrusion are emails attachments.

Worm cont…

- Due to the copying nature of the worm and its capability to travel across the network, the end result is that the worm consume too much system memory and network bandwidth causing the computer and network servers stop responding.

- Worms almost always cause some harm to the network, by taking lots of bandwidth or anything else. And after infecting a computer, they can delete files or use the computer as a botnet and use its computer resources for illegal activities, send spams or even blackmail companies by threatening about DoS attacks.

Signs of a computer worm

- Users should be familiar with the symptoms of a computer worm so that they can quickly recognize infections and begin the process of computer worm removal. Here are some of the typical symptoms of a computer worm:
  - Slow computer performance
  - Freezing/crashing
  - Programs opening and running automatically
  - Irregular web browser performance
  - Unusual computer behavior (messages, images, sounds, etc)
  - Firewall warnings
  - Missing/modified files
  - Appearance of strange/unintended desktop files or icons
  - Operating system errors and system error messages
  - Emails sent to contacts without the user's knowledge
  - …

Worm phases

- Worm has phases like a virus:
  - Dormant
  - Triggering
  - execution
  - Propagation

Worm technology

- Worm technology include:
  - Multiplatform: target a variety of OS
  - Multi-exploit: penetrate systems in a variety of ways (through email, browsers, file sharing, …)
  - Ultrafast spreading: use various techniques to identify as many vulnerable machines in a short period of time
  - Polymorphic
  - Metamorphic
  - Multi-Transport vehicles: can carry a variety of payloads (rootkits, spam generators, bots, etc.)
  - Zero-day: try to exploit new/unknown vulnerabilities

Zero-day

- A zero-day attack happens once the software/hardware vulnerability is exploited by attackers before a developer has an opportunity to create a patch to fix the vulnerability—hence “zero-day.”
- Let’s break down the steps of the vulnerability:
  - A company’s developers create software, but they do not know it contains a vulnerability.
  - The attackers find that vulnerability either before the developer does or acts on it before the developer has a chance to fix it.
  - The attacker writes and implements exploit code while the vulnerability is still open and available.
  - After releasing the exploit, either the public recognizes it in the form of identity or information theft or the developer catches it and creates a patch to staunch the cyber-bleeding.
- Once a patch is written and used, the exploit is no longer called a zero-day exploit. These attacks are rarely discovered right away. In fact, it often takes not just days but months and sometimes years before a developer learns of the vulnerability that led to an attack.

Trojan

- A Trojan is a destructive program that pretends to be a harmless or useful application such as computer game, free screen savers, or even an anti-virus in foreground, but in reality it is working silently in background without your knowledge to harm your computer

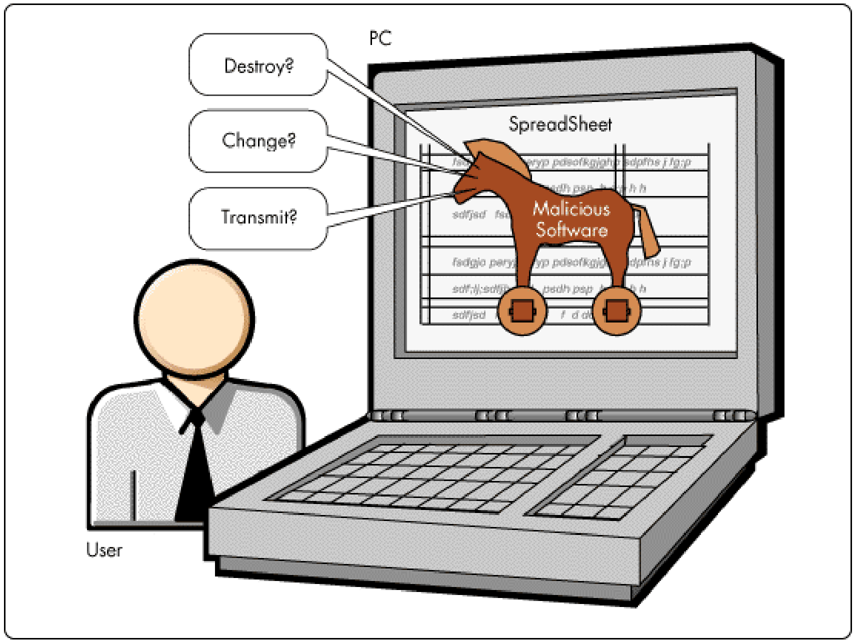
- Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host such as:
  - irritating the user (popping up windows or changing desktops).
  - damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses).
  - creating back doors to give malicious users access to the system.
  - …

Trojan analogy

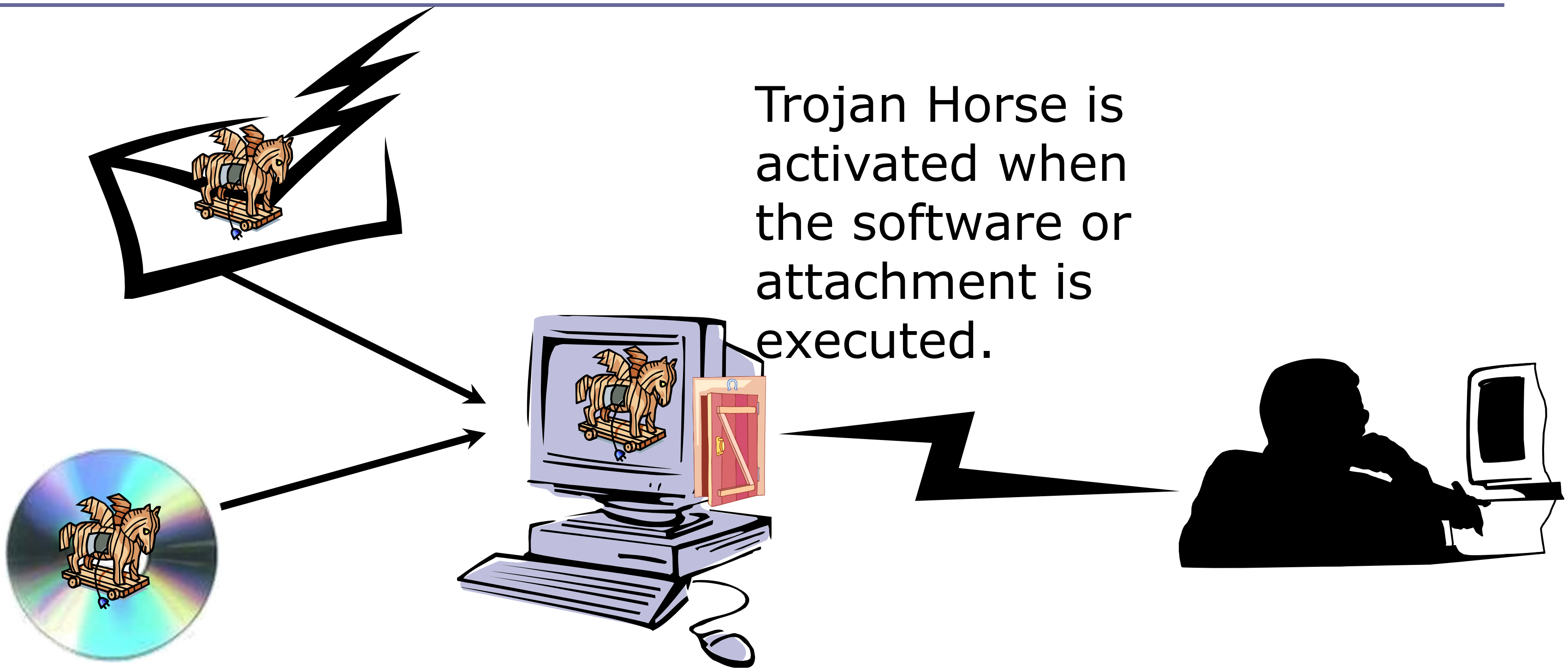
- Suppose you are the CEO of a company and there is an employee you think is a valuable asset because of some initial success he gave your company.
- In reality the employee is working for your competitor and destroying your company from within.
- Now these kinds of employees can be considered as a Trojan horses if you consider the company as your computer.

Trojan cont…

- Trojans open backdoor/trapdoor on you computer that give the attacker access to you system.
- Backdoor/trapdoor is secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures.
-
-



Trojan cont…



Trojan Horse is activated when the software or attachment is executed.

Trojan Horse arrives via email or software like free games.

Trojan cont…

- Some types of Trojans:
  - **remote access**: designed to give an attacker control over a victim’s system (client-server model)
  - data sending: designed to capture and redirect data (keystrokes, passwords, …) to an attacker
  - Destructive: designed to destroy data or kill the system
  - Denial of Service: designed to conduct a DoS attack on a predefined IP address
  - FTP: designed to set up the infected system to serve as an FTP server for illegal software, pirated movies and music, etc.
  - …

Malware Actions

- Once malware is in your computer, it can do many things:
  - Spyware
  - Adware
  - Rootkit
  - Ransomware
  - Scareware

Spyware

- Spyware is a type of software that secretively collects user information, and sends that information back to the creator so they can use your personal information in some nefarious way.

- This could include keylogging to learn your passwords, watching your searching habits, changing out your browser home and search pages, adding unwanted browser toolbars, stealing your passwords and credit card numbers.

- Spyware can be installed even via your browser using banners, ads, pop-ups, etc.

Spyware cont…

- Since spyware is primarily meant to make money at your expense, it doesn't usually kill your PC—in fact, many people have spyware running without even realizing it, but generally those that have one spyware application installed also have a dozen more. Once you've got that many pieces of software spying on you, your PC is going to become slow.

- Note that not every antivirus software is designed to catch spyware.

Adware

- Adware (advertising-supported software) is unwanted software designed to throw advertisements up on your screen, most often within a web browser.

- Sometimes the way that advertisements are delivered can be deceptive in that they track or reveal more information about you than you would like.

- Most of the time, you agree to the adware tracking you when you install the software that the adware comes with. Generally, it can be removed by uninstalling the software it was attached to.

Ransomware

- Ransomware holds you PC hostage and demands money. It locks you computer and threatening to destroy data demanding ransom or payment for release of your data and regain the ability to use your files of computer again.

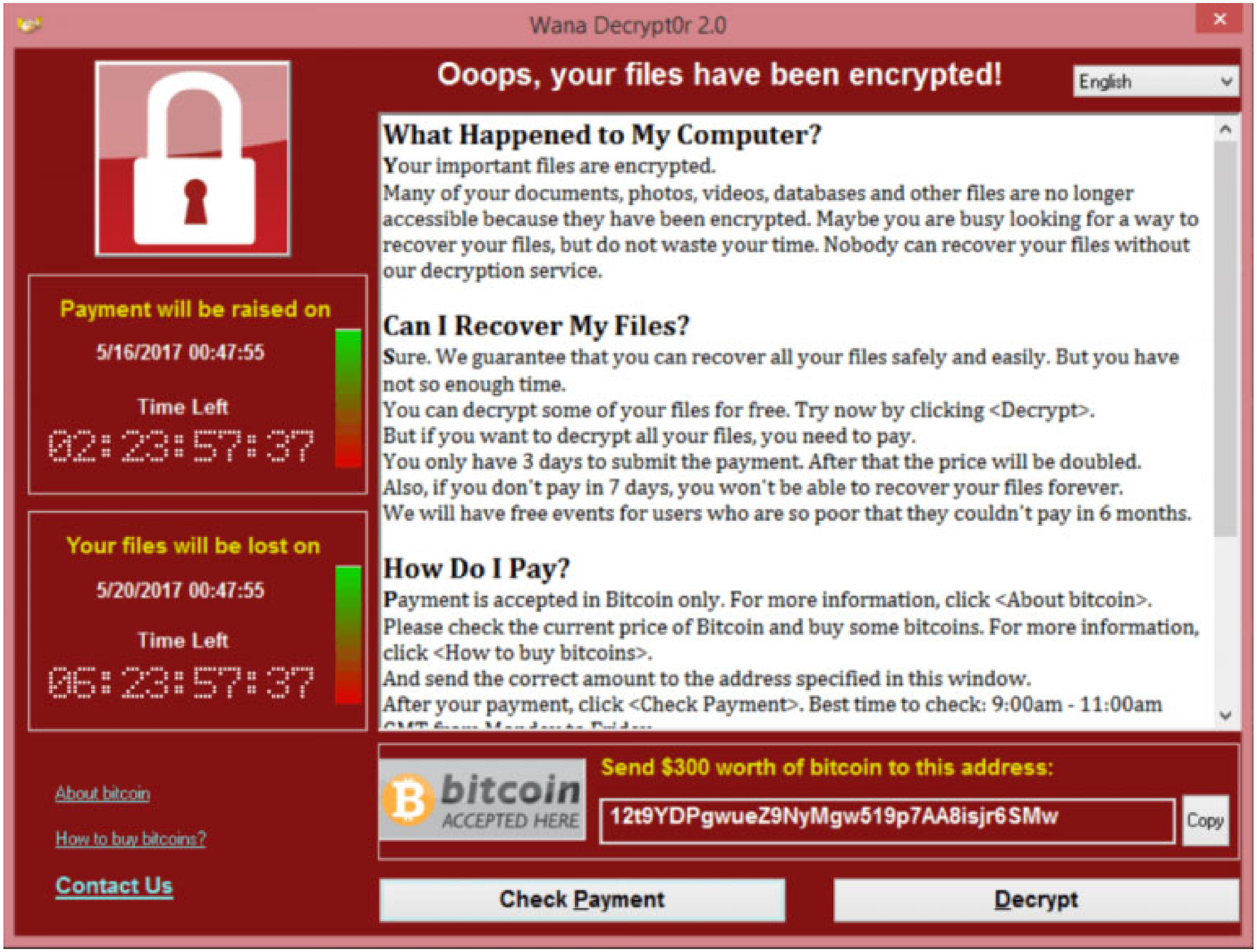
- While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

- Ransomware is lately a very popular way for Internet criminals to make money.

Ransomware cont…

- The subcategories of ransomware based on implementation include:
  - CryptoLockers: encrypts victim's data or the entire hard-drive
  - ScreenLockers: user is locked out and denied login to the system

Ransomware cont…



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

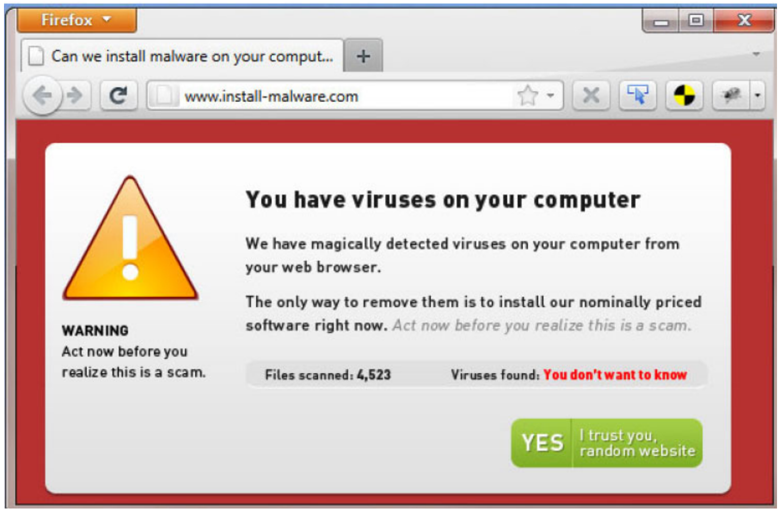
06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Scareware

- Scareware is malicious program that aim to scare users into installing a program and sometimes even paying for it.
- The program is 'supposed' to solve a problem that does not exist.
- Scareware is software that appears to be something legit (usually masquerading as some tool to help fix your computer) but when it runs it tells you that your system is either infected or broken in some way. This message is generally delivered in a manner that is meant to frighten you into doing something. The software claims to be able to fix your problems if you pay them.
- Scareware is also referred to as "rogue" software – like rogue antivirus.


Firefox
Can we install malware on your comput...
www.install-malware.com
YES
I trust you, random website

You have viruses on your computer

We have magically detected viruses on your computer from your web browser.

The only way to remove them is to install our nominally priced software right now. *Act now before you realize this is a scam.*

WARNING
Act now before you realize this is a scam.

Files scanned: 4,523 Viruses found: You don't want to know

Physical attack

- An attacker (might be an employee) can get physical access to a computer system to:
  - Find passwords to log in computer
  - Install back door, virus, Trojan, or keystroke logger
  - Steal USB drives, laptop, computers, CDs, etc.
  - …

Password cracking attacks

- types of password cracking attacks
  - brute force: every possible combination for password is tried
  - Dictionary: a list of commonly used passwords (the dictionary) is used
  - Guessing: the attacker uses his/her knowledge of the user’s personal information and tries to guess the password

SQL injection

- A SQL injection involves a threat actor inserting malicious code into the entry field of an application, causing that code to execute if entries have not been sanitized. SQL injections are among the most dangerous and common exploits affecting websites. A SQL injection into a media company’s CMS could enable a cyber actor access