Computer Security – Principles and Practice (Pearson, fourth edition)

W. Stallings, L. Brown

Malicious software

* These slides are an adaptation of the original slides of the authors of the book

Learning objectives

- Describe three broad mechanisms malware uses to propagate.
- Understand the basic operation of viruses, worms, and Trojans.
- Describe four broad categories of malware payloads.
- Understand the different threats posed by bots, spyware, and rootkits.
- Describe some malware countermeasure elements.

Malware

NIST 800-83 defines malware as:

"a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."

Points: usually covertly: the user is unaware of what is going on. It's a program (or a fragment of a program).

Malware terminology – I

cannot really be called malware. They address specific one victim with a specific purpose.

Name	Description
Advanced Persistent Threat (APT)	**Cybercrime directed at business and political targets**, using a wide variety of intrusion technologies and malware, **applied persistently** and effectively to specific targets **over an extended period**, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanism that **bypasses a normal security check**; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by-download	An attack using code on a compromised website that exploits a browser vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb **lies dormant** until a predefined condition is met; the code then triggers some payload.

Malware terminology – II

Name	Description
Macro virus	A type of virus that uses macro or scripting code, typically embedded in a document or document template, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile code	Software (e.g., script and macro) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained **root-level access**.
Spammer programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.
Trojan horse	A computer program that **appears to have a useful function**, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes it.
Virus	Malware that, when executed, tries to **replicate itself** into other executable machine or script code; when it succeeds, the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can **run independently** and can propagate a complete working version of itself onto other hosts on a network, by exploiting software vulnerabilities in the target system, or using captured authorization credentials.
Zombie, bot	Program installed on an infected machine that is activated to launch attacks on other machines.

Classification of malware

Historically classification was based on how the MW replicated itself. Some MW are fully independent programs exc. Then the 2nd classification is about wether the MW replicates or not. But nowadays finding a categorization is tricky.

Classified into two broad categories:

- Based first on how it spreads or propagates to reach the desired targets
- Then on the actions or payloads it performs once a target is reached

We can look at classifications regardless how they spread or at their payload.

Also classified by:

- Those that need a host program (parasitic code such as viruses)
- Those that are independent, self-contained programs (worms, trojans, and bots)
- Malware that does not replicate (trojans and spam e-mail)
- Malware that does replicate (viruses and worms)

Types of malicious software (malware)

① A virus attaches itself to other programs (any programs really)

Propagation mechanisms include:

- **Infection** of existing content by viruses that is subsequently spread to other systems
- **Exploit** of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
- **Social engineering** attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks

Less technical but still

Payload actions performed by malware once it reaches a target system can include:

- Corruption of system or data files (or destroying)
- Theft of service/make the system a zombie agent of attack as part of a botnet
- Theft of information from the system/keylogging
- Stealthing/hiding its presence on the system

System will become a vector for an attack

Attack kits

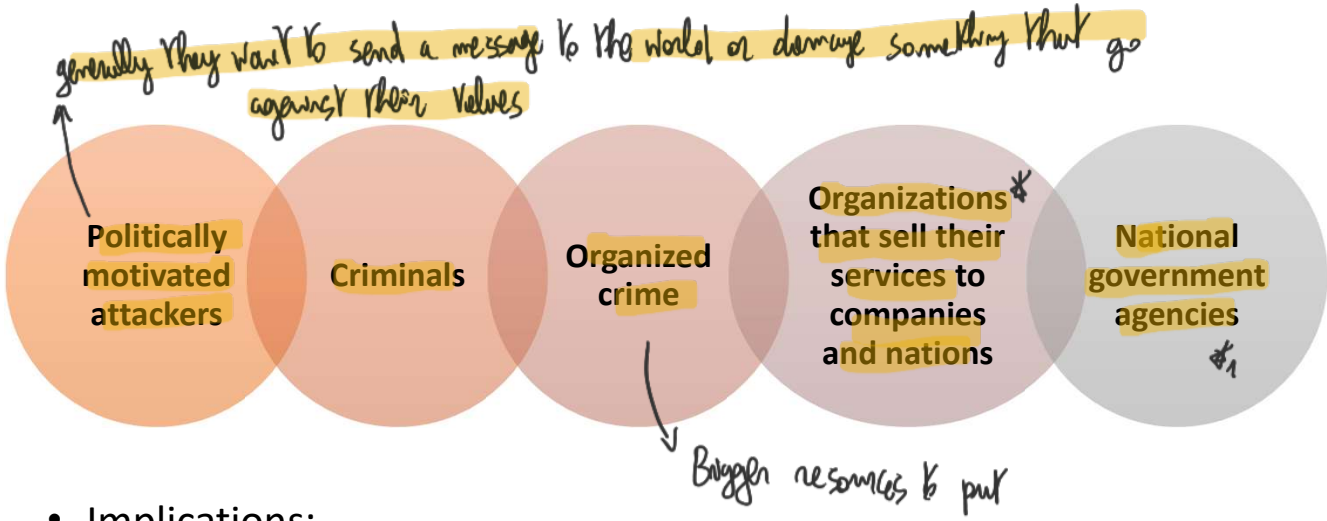
Now you can find kits that help you setup your own MW, Advantages and disadvantages: using toolkits you use well known approaches that might be easily detected.

- Initially the development and deployment of malware required considerable technical skills
- Development of virus-creation toolkits in the early 1990s and later of more general attack kits in the 2000s
  - Greatly assisted in the development and deployment of malware
  - Toolkits are often known as “crimeware”
  - Include a variety of propagation mechanisms and payload modules that even novices can deploy
  - Variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them
- Examples are:
  - Zeus
  - Angler

Who is behind the MW? Who is the target?

Attack sources

- change from attackers being individuals often motivated to demonstrate their technical competence to more organized and dangerous attack sources such as:



- Implications:
  - Significant change in the resources available and motivation behind the rise of malware
  - development of a large underground economy involving the sale of attack kits, access to compromised hosts, and to stolen information

* Case of Italy: ex-employees had access to police databases and more and that was used to sell info.

* Include high targets: other nations, technological companies ex. The amount of resources is huge. The more we move to the right, the more specific targets we have.

In the old times, MW were written by show offs, with much lower risks. Not today.

has a very specific target. Are a high profile attacker. Since the target is specific a lot of resources are spent to get info about target.

Advanced persistent threats (APTs)

- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and persistent, stealthy intrusion efforts over extended periods
- High profile attacks include Aurora, RSA, APT1, and Stuxnet *

* Used in cyberwar, to destroy the industry of enrichment of uranium in Iran. The industrial machines for centrifugation were piloted with digital controllers, connected to the internet. Stuxnet was designed to target those PLC, so their target would be to activate when infecting the machines. The payload made the machine rotate at much higher speed than possible, making them break down.

Advanced persistent threats characteristics

Advanced

- Use a wide variety of intrusion technologies and malware including the development of custom malware if required
- The individual components may not necessarily be technically advanced but are carefully selected to suit the chosen target

Persistent

- Determined application of the attacks over an extended period against the chosen target in order to maximize the chance of success
- A variety of attacks may be progressively applied until the target is compromised

determined to reach targets because they can wait a lot

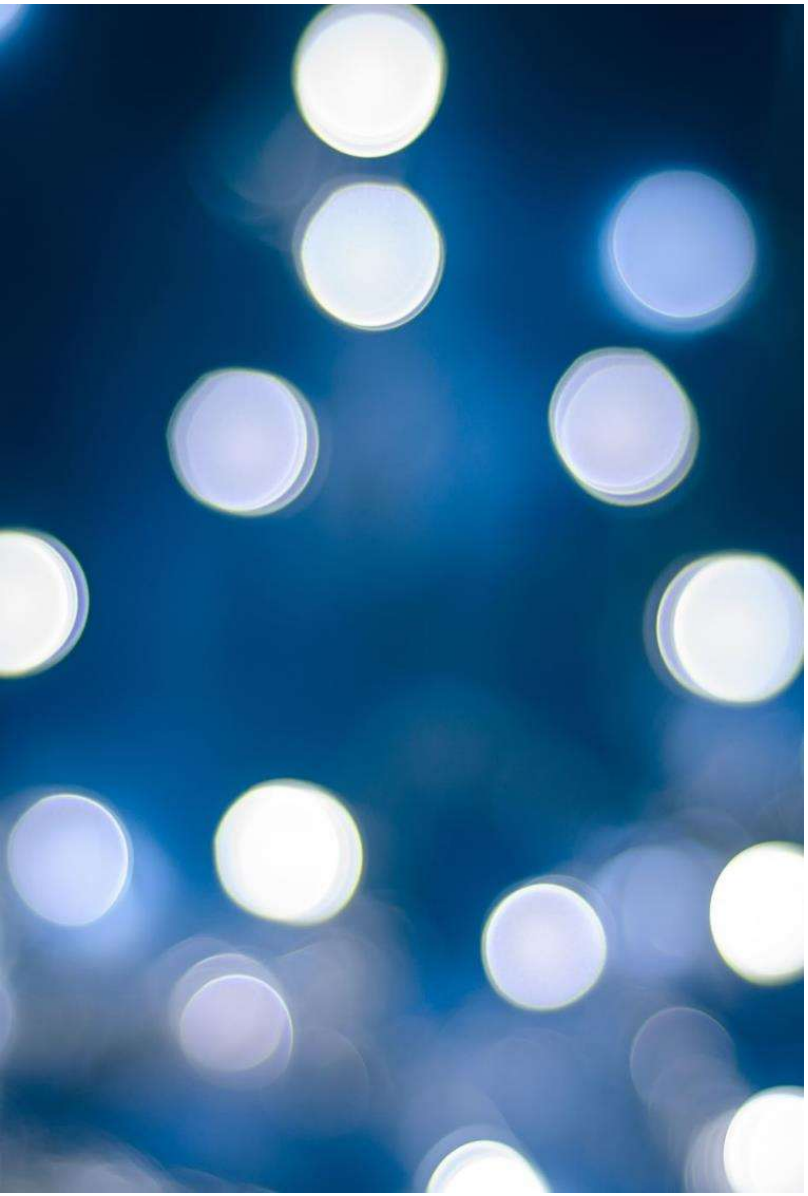
Threats

- Threats to the selected targets as a result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen targets
- The active involvement of people in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attacks

you could have the helps of an insider to

Advanced persistent threats attacks

- Aims:
  - theft of intellectual property
  - theft of security and infrastructure related data
  - physical disruption of infrastructure
  - …
- Techniques used: (any)
  - Social engineering
  - Spear-phishing email
  - Drive-by-downloads from compromised websites likely to be visited by personnel in the target organization
- Intent: → and activate the payload
  - To infect the target with sophisticated malware with multiple propagation mechanisms and payloads
  - Once they have gained initial access to systems in the target organization a further range of attack tools are used to maintain and extend their access



Review question

What are the different ways in which malware can be classified?

I proposed you two different ways, one older and one newer… why in your view we gave up to the old classification?

Propagation

viruses, worms, trojans

1st class of prop. measures:

Viruses were very popular, because with no internet, sharing programs was the main activity, and this was the main way for them to propagate. So manual spreading, very slow. *

→ cannot work on their own.

Viruses

- Piece of software that infects programs
  - Modifies them to include a copy of the virus
  - Replicate and then infect other executables
  - Easily spread through computers, with the help of users that **share programs**
- When attached to an executable program a virus can do anything that the program can do
  - Executes secretly when the host program is run
  - Especially effective if no access control is used (as in the first PCs)
- Specific to operating system and hardware
  - Takes advantage of their details and weaknesses

in each executable, we modify the address of the main function to the code of the virus.

* Do not work so much now, because there is not much program sharing, plus at that time machines didn't have Access Control policy, so all the files were on a disk with no auth. So viruses could spread even to OS exes. In the 2000s with more modern OSes, we had AC policies that made their life difficult.

- Computer virus infections formed the majority of malware in the early personal computer era (around the ‘80s)
  - The Brain virus in 1986, was one of the first to target MSDOS systems, and resulted in a significant number of infections for this time.
  - programs shared on floppy disk make it easily spread
- In modern OS, the use of tighter access controls reduces the efficacy of traditional viruses
  - Hence viruses evolved in macrovirus
  - Documents are easily modified and not protected as executables in OS
- Currently, a viral mode of infection is one of several propagation mechanisms used by contemporary malware

Looks for exes not infected yet and does so, check wether or not the payload should be activated or not (usually done with counter to avoid suspicions).

Infection mechanism

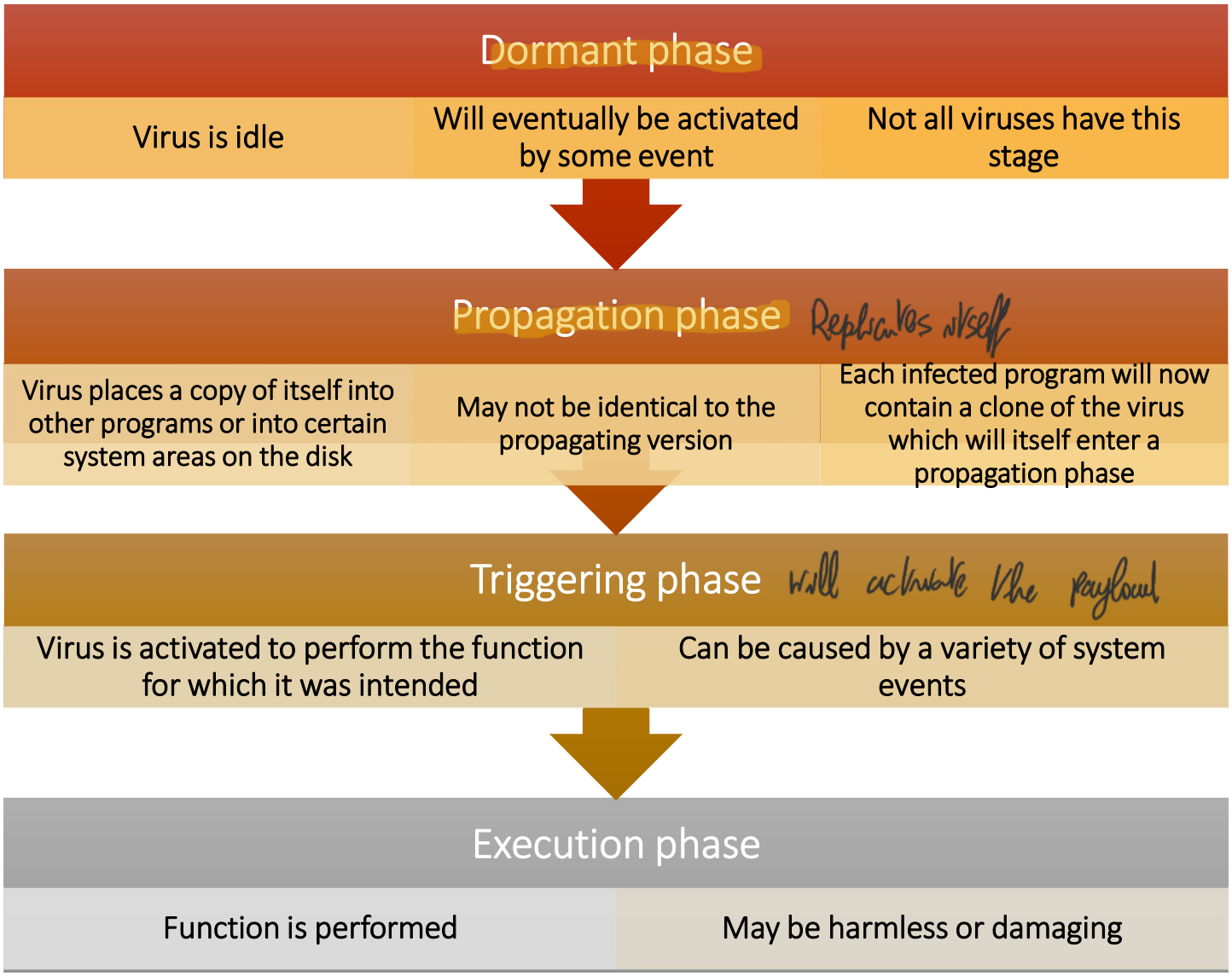
- Means by which a virus spreads or propagates
- Also referred to as the *infection vector*

Trigger

- Event or condition that determines when the payload is activated or delivered
- Sometimes known as a *logic bomb*

Payload

- What the virus does (besides spreading)
- May involve damage or benign but noticeable activity



Virus phases

AC was preventing overwriting exes, at least the OS exes. So limited effects. That's why viruses evolved in macroviruses that infected programs like word, excel that offer the possibility of running scripts. Macroviruses can operate on any machine regardless of Oses

Macro and scripting viruses

- NISTIR 7298 defines a macro virus as:

"a virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate"

- Macro viruses infect scripting code used to support active content in a variety of user document types
- They are threatening for a number of reasons:
  - They are platform independent
  - Infect documents, not executable portions of code
  - Are easily spread as the documents are normally shared, much more than programs
  - Traditional file system access controls are of limited use in preventing their spread: they infect user documents that need to be modified by users …
  - Are much easier to write or to modify than traditional executable viruses

More easily exchanged for sure

And can easily bypass AC because docs are meant to be written.

Melissa macro virus pseudo-code

```
macro Document_Open
  disable Macro menu and some macro security features
  if called from a user document
     copy macro code into Normal template file
  else
     copy macro code into user document being opened
  end if
  if registry key "Melissa" not present *
     if Outlook is email client
        for first 50 addresses in address book
              send email to that address
              with currently infected document attached
        end for
     end if
     create registry key "Melissa" (so we execute Melissa only once to avoid suspicions)
  end if
  if minute in hour equals day of month
     insert text into document being opened
  end if
end macro
```

it took only three days for Melissa to infect over 100,000 computers, compared to the months it took the Brain virus to infect a few thousand computers a decade before

Word uses templates, file that gives info regarding how to preset a document.

hides itself

Normal Template is used for every basic doc. So when opening any doc that will be infected

* Melissa creates a key in the windows DB recording that the computer has already been infected. So we have local infection and online infection.

① OS should be loaded from memory from the boot sector. Nowadays because of anti-virus is impossible.

method for infection

method they can use to hide themselves.

Virus classification

By target

- Boot sector infector ①
  - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
- File infector
  - Infects files that the operating system or shell considers to be executable
- Macro virus
  - Infects files with macro or scripting code that is interpreted by an application
- Multipartite virus
  - Infects files in multiple ways

Virus activated at bootup

By concealment strategy

- Encrypted virus ②
  - A portion of the virus creates a random encryption key and encrypts the remainder of the virus
- Stealth virus ③
  - Explicitly designed to hide itself from anti-virus
- Polymorphic virus
  - A virus that mutates with every infection ④
- Metamorphic virus
  - A virus that mutates and rewrites itself completely at each iteration and may change behavior as well as appearance

② Of course there is also a fragment of code in clear for decryption

③ Disable or modify antivirus to avoid it.

④ Every time you execute it the code changes.

Worms

Worms are completely autonomous and they find a way to be executed again (commonly by pulling themselves as something that will be started at bootup). Worm actively looks for other machines to infect. Became popular with advent of the internet.

- Program that actively seeks out more machines to infect
  - each infected machine serves as an automated launching pad for attacks on other machines
  - exploits software vulnerabilities in client or server programs
- Usually carries some form of payload
  - Upon activation the payload may replicate and propagate the worm again
- First known (non-malicious) implementation was done in Xerox Palo Alto Labs in the early 1980s

Spread with emails or messages, file sharing, exploit vulnerability in machines, remote transfers etc

Worm replication

Electronic mail or instant messenger facility	• Worm e-mails a copy of itself to other systems • Sends itself as an attachment via an instant message service
File sharing	• Creates a copy of itself or infects a file as a virus on removable media (USB, CDs/DVD) • Usually exploits autorun mechanism
Remote execution capability	• Worm executes a copy of itself on another system on the network • by an explicit facility or by flaws in the other machine
Remote file access or transfer capability	• Worm uses a remote file access or transfer service to copy itself from one system to the other
Remote login capability	• Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

Phases of the worm are same as a virus. ①

Worms can perform an active scan on the internet to find exploits and vulnerable machines.

Worm replication

A worm typically uses the same phases as a computer virus:

- dormant, propagation, triggering, execution. ②

The propagation phase generally performs the following functions:

- Search for access mechanisms to other systems to infect (Scanning phase)
- Scanning by examining local data:
  - host tables, address books, buddy lists, trusted peers,… ;
  - by scanning possible target host addresses;
  - by searching for suitable removable media devices to use.
- Transfer (and run) a copy of itself to the remote system

The worm may to disguise its presence by naming itself as a system process

- Recent worms can even inject their code into existing processes on the system.

Target discovery

Several strategies to perform scanning. Not only the payload but also the amount of resources used that make a worm evident. Sometimes also the load on the machine can be a giveaway. An aggressive scanning is more detectable.

Scanning Can be:

- Random
  - Probes random addresses in the IP address space using a different seed
  - This produces a high volume of Internet traffic which may cause generalized disruption even before the actual attack is launched
- Hit-list
  - First compiles a long list of potential vulnerable machines
  - Then it begins infecting machines on the list
  - Each infected machine is provided with a portion of the list to scan
  - This results in a very short scanning period which may make it difficult to detect that infection is taking place
- Topological
  - Look for information on an infected victim machine to find more hosts to scan
- Local subnet
  - If a host can be infected behind a firewall that host then looks for targets in its own local network
  - The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall

Model of propagation of worms and viruses are similar to real life biological viruses.

Worm propagation model

- A well-designed worm (and a virus) can spread rapidly and infect massive numbers of hosts.
- Computer viruses and worms exhibit similar self-replication and propagation behavior to biological viruses.
- We can look to classic epidemic models for understanding computer virus and worm propagation behavior.

Let:

- $I(t)$ be the number of computers infected at time t
- $S(t)$ be the number of susceptible computers (vulnerable to infection but not yet infected)
- β be the infection rate
- N be the number of vulnerable computers (size of population), $N = I(t) + S(t)$

Then:

$$\frac{\partial I(t)}{\partial t} = \beta \cdot I(t) \cdot S(t)$$

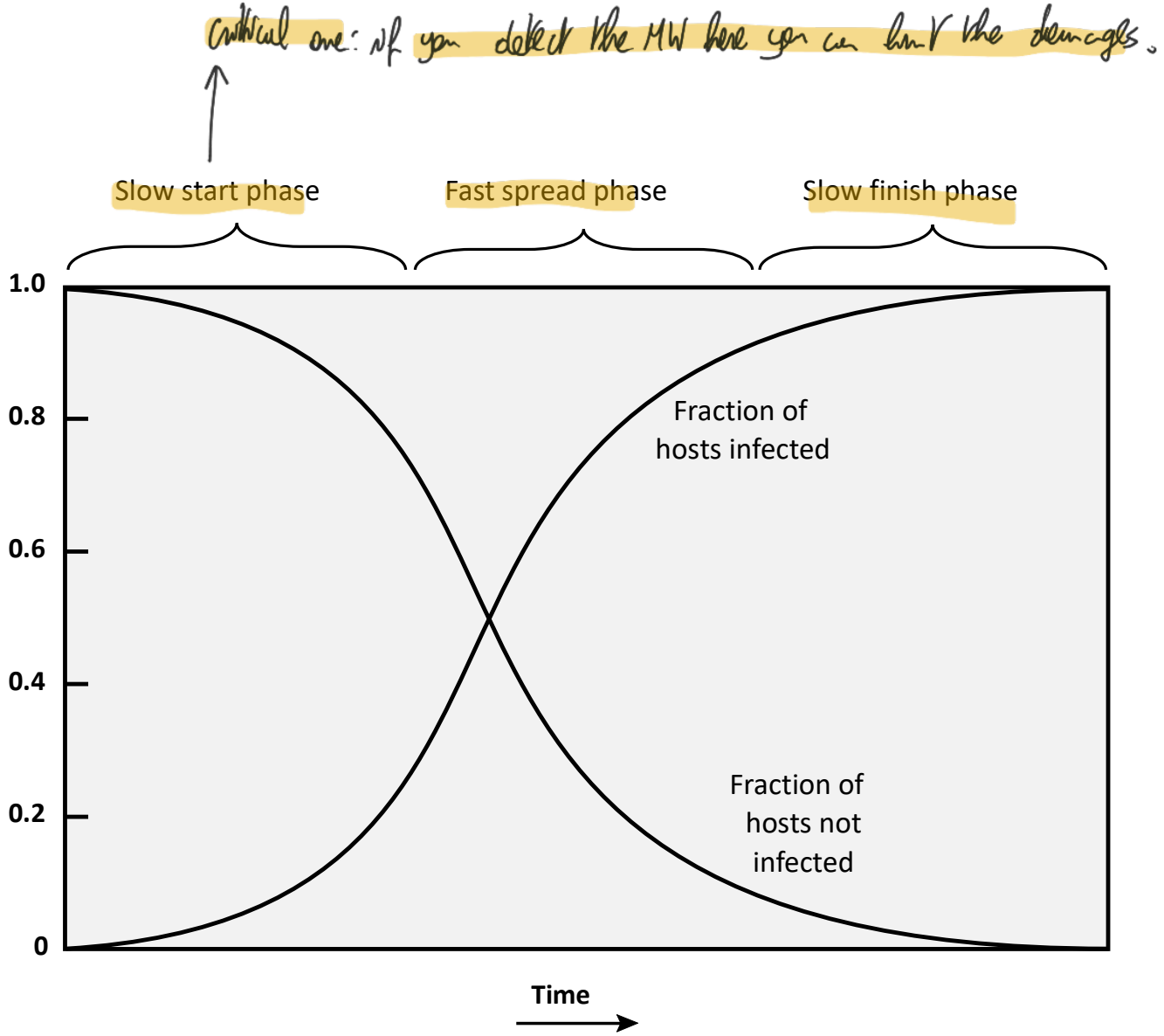
how many computers are infected

β how many computers one infected machine can infect in a given time.

$\frac{\partial I(t)}{\partial t}$ tells us how fast $I(t)$ grows.

$I(t) \cdot S(t)$ Proportional to infected PCs and PCs yet to be infected.

Worm propagation model



Morris worm

- Earliest significant worm infection
- Released by Robert Morris in 1988
- Designed to spread on UNIX systems with a number of methods:
  - Attempted to crack local password file to use login/password to logon to other systems
  - Exploited a bug in the finger protocol which reports the whereabouts of a remote user
  - Exploited a trapdoor in the debug option of the remote process that receives and sends e-mails
- Successful attacks give access to the operating system command interpreter
  - Sent interpreter a bootstrap program to copy worm over and then logoff.
  - The bootstrap program restarts the worm on the new machine

Recent worm attacks

Melissa	**1998**	E-mail worm First to include virus, worm and Trojan in one package
Code Red	**July 2001**	Exploited Microsoft IIS bug Probes random IP addresses Consumes significant Internet capacity when active
Code Red II	**August 2001**	Also targeted Microsoft IIS Installs a backdoor for access
Nimda	**September 2001**	Had worm, virus and mobile code characteristics Spread using e-mail, Windows shares, Web servers, Web clients, backdoors
SQL Slammer	**Early 2003**	Exploited a buffer overflow vulnerability in SQL server compact and spread rapidly
Sobig.F	**Late 2003**	Exploited open proxy servers to turn infected machines into spam engines
Mydoom	**2004**	Mass-mailing e-mail worm Installed a backdoor in infected machines
Warezov	**2006**	Creates executables in system directories Sends itself as an e-mail attachment Can disable security related products
Conficker (Downadup)	**November 2008**	Exploits a Windows buffer overflow vulnerability Most widespread infection since SQL Slammer
Stuxnet	**2010**	Restricted rate of spread to reduce chance of detection Targeted industrial control systems

Extremely fast in spreading, spreads as a worm

WannaCry

Ransomware attack in May 2017

- spread extremely fast over a period of hours to days,
- infecting hundreds of thousands of systems belonging to both public and private organizations in more than 150 countries

It spread as a worm

- by aggressively scanning both local and random remote networks,
- attempting to exploit a vulnerability in the SMB file sharing service on unpatched Windows systems

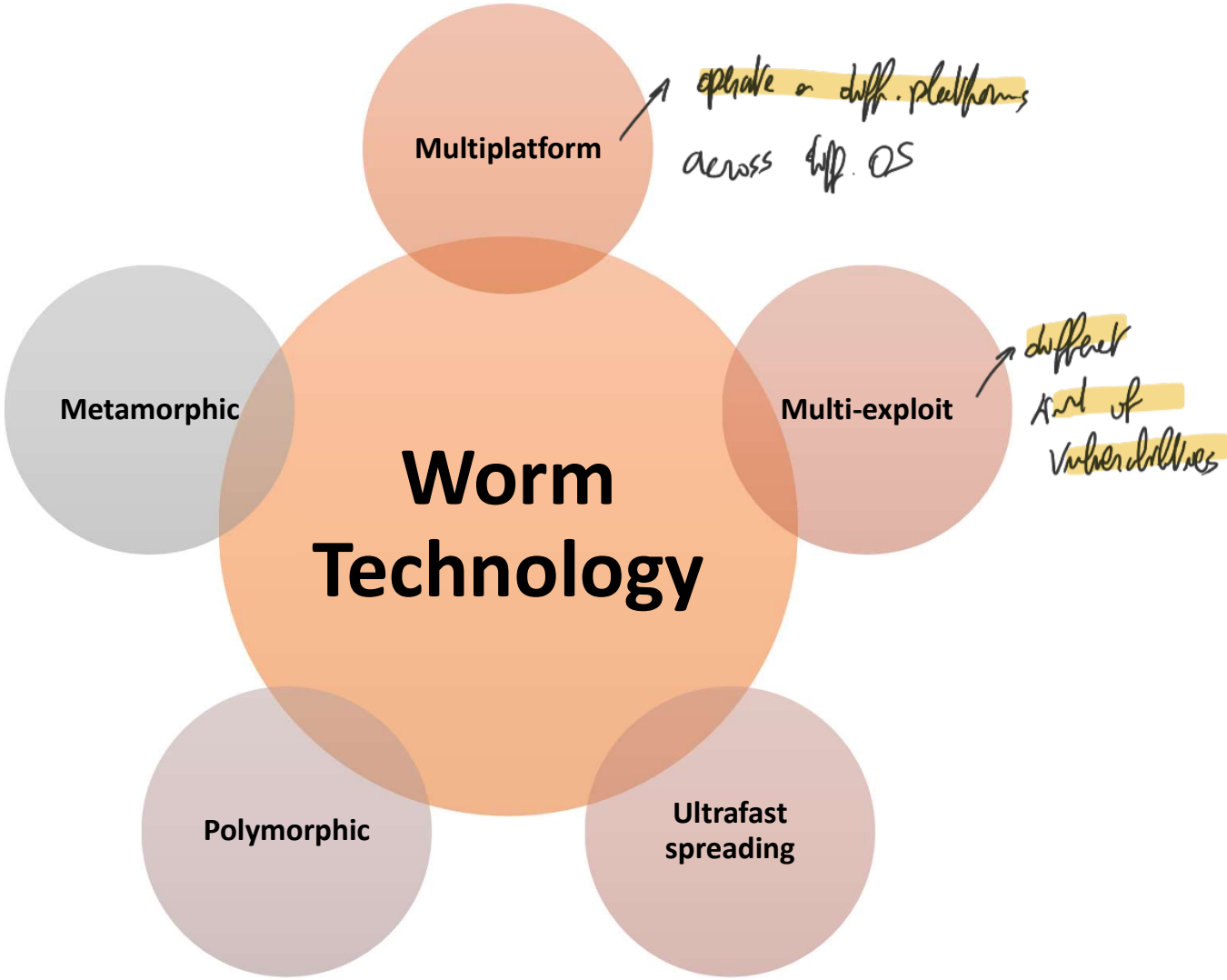
↳ file sharing protocol

This rapid spread was only slowed by the accidental activation of a "kill-switch" domain by a UK security researcher

Once installed on infected systems, it also encrypted files, demanding a ransom payment to recover them

a UK researcher discovered its spreading method

Worms: state of technology



Having a worm or virus interoperable in different languages, so when VS exploit scripting languages used on several systems.

Mobile code

- NIST SP 800-28 defines mobile code as:
  "programs that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics"

- Mobile code transmitted from a remote system to a local system and then executed on the local system
- Often acts as a mechanism for a virus, worm, or trojan horse
- Takes advantage of vulnerabilities to perform its own exploits
- Popular vehicles include:
  - Java applets
  - ActiveX
  - JavaScript
  - VBScript
- Most common ways of using mobile code for malicious operations on local system are:
  - Cross-site scripting
  - Interactive and dynamic Web sites
  - E-mail attachments
  - Downloads from untrusted sites or of untrusted software

Other malware

- Mobile phone worms
  - First was Cabir worm in 2004, then Lasco and CommWarrior in 2005
  - Propagate through Bluetooth, Wi-Fi or MMS
- Drive-by-download
  - Exploit browser and plugin vulnerabilities by means of malware in a webpage
  - Attacks when the user views the webpage and install malware on the system without the user's knowledge or consent
- Watering-hole
  - A variant of drive-by-download
  - Aims at specific target, useful for Advanced Persistent Threats,
  - May remain disabled for other system than the target
- Malversiting
  - Places malware on websites without actually compromising them
  - Using paid advertisements that can be set and removed in a very short time
- Clickjacking
  - Also known as a user-interface (UI) redress attack
  - the user is cheated by a fake interface on the web and clicks (and is redirected to malware)

"Tricking" users to assist in the compromise of their own systems

Spam

- Unsolicited bulk e-mail
- Significant carrier of malware
- Used for phishing attacks

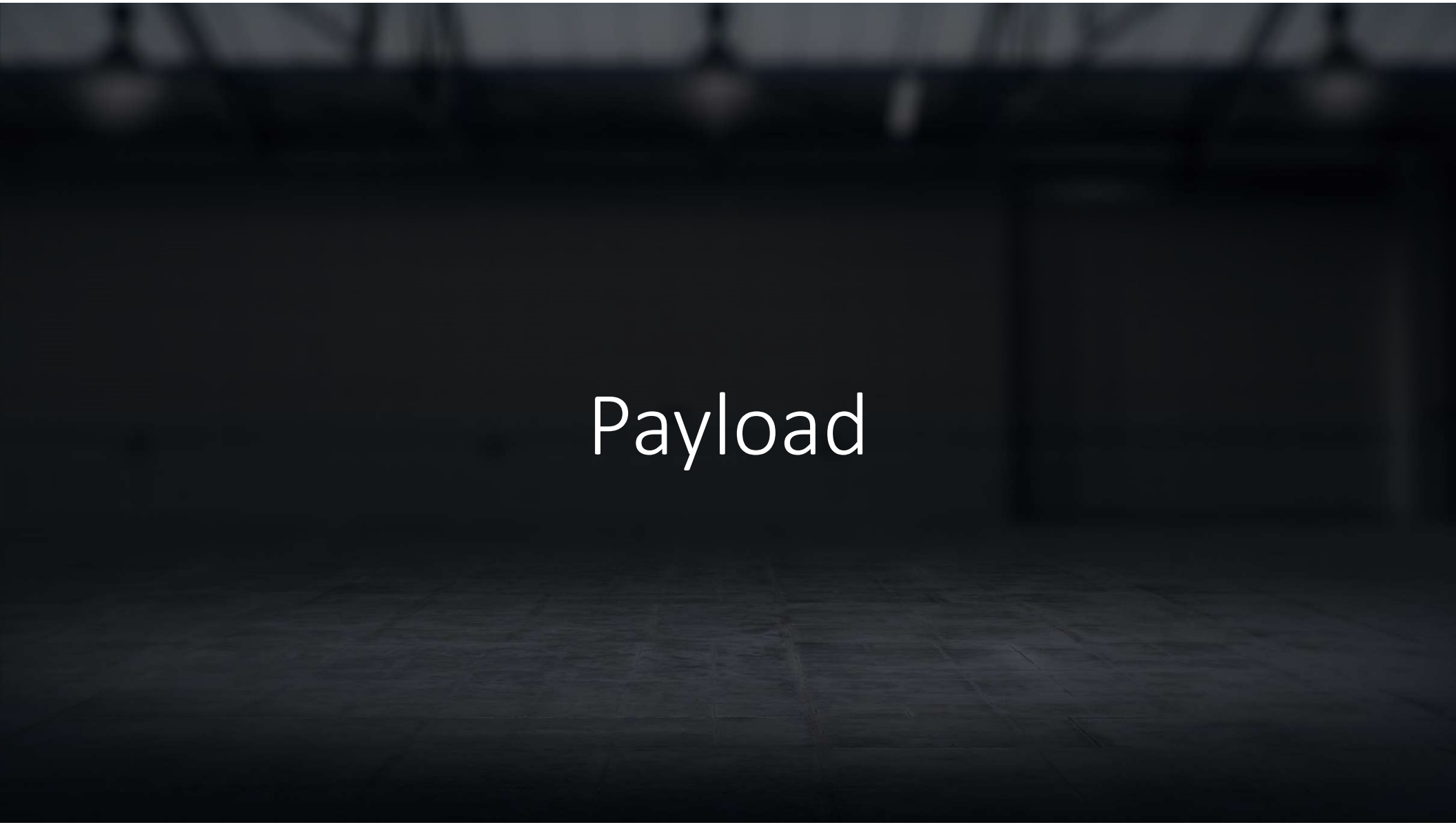
Trojan horse

- Program or utility containing harmful hidden code
- Used to accomplish functions that the attacker could not accomplish directly

Mobile phone Trojans

- First appeared in 2004 (Skuller)
- Target is the smartphone

Social engineering


Payload

*No Access control.
Virus zeroed the first megabyte of the hard drive. There the OS was keeping info describing the data structure.
Nowadays this is not possible anymore. MV was working at very low level.

Chernobyl virus

First seen in 1998

Example of a destructive parasitic memory-resident Windows 95 and 98 virus

Infects executable files when they are opened. When it reaches a trigger date , it deletes data on the infected system by overwriting the first megabyte of the hard drive with zeroes, resulting in massive corruption of the entire file system

Klez

was deleting files

Mass mailing worm infecting Windows 95 to XP systems

First seen in October 2001

Spreads by e-mailing copies of itself to addresses found in the address book and in files on the system

It can stop and delete some anti-virus programs running on the system

On trigger date causes files on the hard drive to become empty

Ransomware

Encrypts the user's data and demands payment of a ramson in order to access the key needed to recover the information

PC Cyborg Trojan (1989)

Mid-2006 a number of worms and Trojans appeared that used public-key cryptography with increasingly larger key sizes to encrypt data

Even recent cases (health system in region Lazio in Italy in 2020…)

Payload – system corruption

Other dos: physical damages or destroy your BIOS that is executed to boot up the OS.

- Real-world damage
  - Causes damage to physical equipment
    - Chernobyl virus also rewrites BIOS code
  - Stuxnet worm
    - Targets specific industrial control system software
  - There are concerns about using sophisticated targeted malware for industrial sabotage
- Logic bomb
  - Code embedded in the malware that is set to "explode" when certain conditions are met

Payload – system corruption

Ransomware are matched with social engineering, to leverage on guilt, shame etc.

Payload – Ransomware

WannaCry

- Infected a large number of systems in many countries in May 2017
- It encrypted a large number of files and then demanded a ransom payment in Bitcoins to recover them
- Targets widened beyond personal computer systems to include mobile devices and Linux servers
- Use of tactics to put pressure on the victim to pay up:
  - threatening to publish sensitive personal information
  - permanently destroy the encryption key after a short period of time,…
- Alternative recovery only with good backups and an appropriate incident response and disaster recovery plan

Creating a bot: obj is not destroying, but keep a remote control to perform any other actions like performing an attack. This is also used for botnets.

- Takes over an Internet-attached computer and uses that computer to launch or manage attacks
- *Botnet* - collection of bots capable of acting in a coordinated manner
- Uses:
  - Distributed denial-of-service (DDoS) attacks
  - Spamming
  - Sniffing traffic
  - Keylogging
  - Spreading new malware
  - Installing advertisement add-ons and browser helper objects (BHOs)
  - Attacking IRC chat networks
  - Manipulating online polls/games

Payload – attack agent bots

With botnets, you need to maintain remote control. This could be done by making the bots connect to a server (very general) and use there specific commands to activate an action. In any case, if the method of control becomes known, the botnet can be dismantled. So implementation is complex. Botnets are for example created to charge

the new symbolic names continuously to avoid detection.

SECURITY THE WEB MICROSOFT BOTNET

Microsoft takes down botnet that infected nine million devices

Necurs was one of the largest botnets ever

By Rob Thubron on March 11, 2020, 8:15 AM | 7 comments

Payload – attack agent bots

Payload can vary: could attempt to access files on use a key-logger, so you can see what the user is typing.

- Difference between a bot and a worm:
  - Worm propagates itself and activates itself
  - Bot is initially controlled from some central facility
- Typical means of implementing the remote control facility is on an IRC server
  - Bots join a specific channel on this server and treat incoming messages as commands
  - More recent botnets use covert communication channels via protocols such as HTTP
  - Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure

Remote control facility

- Keyloggers
  - Captures keystrokes to allow attacker to monitor sensitive information
  - Typically uses some form of filtering mechanism that only returns information close to keywords (“login”, “password”)
- Spyware
  - monitors a wide range of activities on the system
  - E.g. web browsing
- Phishing
  - Exploits social engineering to leverage the user’s trust by masquerading as communication from a trusted source
  - Include a URL in a spam e-mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site
  - Suggests that urgent action is required by the user to authenticate their account
  - Attacker exploits the account using the captured credentials
- Spear-phishing
  - Recipients are carefully researched by the attacker
  - E-mail is crafted to specifically suit its recipient, often quoting a range of information to convince them of its authenticity

Payload – information theft

On one hand you need to hide yourself, but you still may need remote access. In this case you are installing a backdoor.

- Also known as a *trapdoor*
- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- *Maintenance hook* is a backdoor used by Programmers to debug and test programs
- Difficult to implement operating system controls for backdoors in applications

↓ You can't tell wether you have malwares or not.

Payload
—
Stealthing
backdoor

Why to hide vs to install a rootkit. Initially, attackers modified command exes that altered their ops.

- Set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- Gives administrator (or root) privileges to attacker
  - Can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand

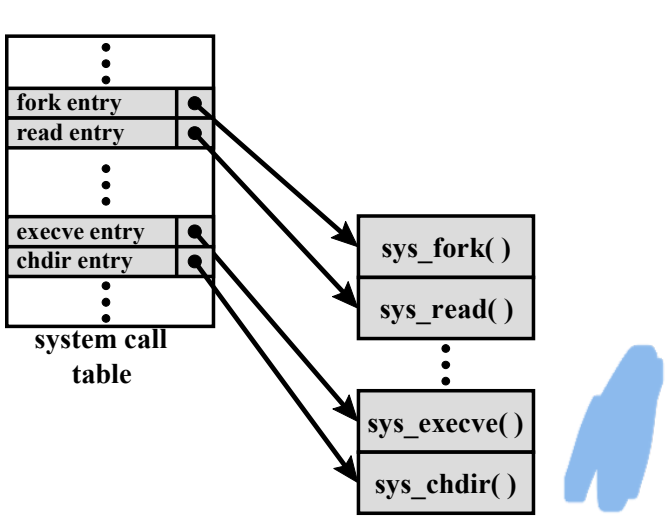
Persistent / Memory based

User mode / Kernel mode

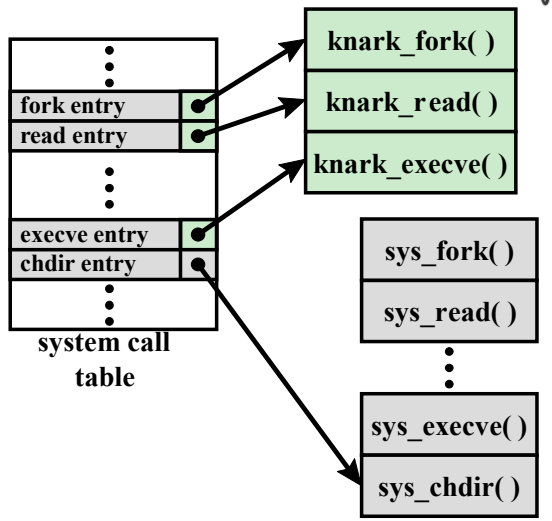
Virtual machine based / External mode

Payload – Stealthing rootkit

We now have real rootkits that install in the OS. There is a table in the OS that contains addresses of system calls that will be called. We can replace system call functions with something that work similarly. One extreme possibility is run the OS as a virtual machine by the HW, so basically HW is running the MW



(a) Normal kernel memory layout



(b) After knark install

System Call table modification by rootkit

Kernel–mode rootkit

THIS IS FOR STEALTH PURPOSES

They operate at kernel level of the OS, by modifying the OS's table themselves and control system functions,

Countermeasures

Malware counter-measure approach

- Ideal solution to the threat of malware is prevention

Four main elements of prevention:

- Policy
- Awareness
- Vulnerability mitigation Patches regularly
- Threat mitigation AC, users group designing etc.

- If prevention fails, technical mechanisms can be used to support the following threat mitigation options:
  - Detection
  - Identification
  - Removal

Malware counter-measure approach

If removal is not possible, then rollback to a clean backup

Requirements for effective malware countermeasures:

- **Generality:** The approach taken should be able to handle a wide variety of attacks.
- **Timeliness:** The approach should respond quickly so as to limit the number of infected programs or systems and the consequent activity.
- **Resiliency:** The approach should be resistant to evasion techniques employed by attackers to hide the presence of their malware.
- **Minimal denial-of-service costs:** The approach should result in minimal reduction in capacity or service due to the actions of the countermeasure software and should not significantly disrupt normal operation.
- **Transparency:** The countermeasure software and devices should not require modification to existing (legacy) OSs, application software, and hardware.
- **Global and local coverage:** The approach should be able to deal with attack sources both from outside and inside the enterprise network.

Achieving all these requirements often requires the use of multiple approaches.

① Heuristic to look for probable MW. AI models now. Large analyzed code. Recent approaches are looking at what the process does - so introduce false positive risks, but it is better for unknowns

Generations of anti-virus software

First generation: simple scanners

Based on pattern recognition, insufficient for new versions of MW

- Requires a malware signature to identify the malware
- Limited to the detection of known malware

Second generation: heuristic scanners ①

- Uses heuristic rules to search for probable malware instances
- Another approach is integrity checking of executables

Third generation: activity traps

- Memory-resident programs that identify malware by its actions rather than its structure in an infected program

Fourth generation: full-featured protection

- Packages consisting of a variety of anti-virus techniques used in conjunction
- Include scanning and activity trap components and access control capability

most of Vhs all with AI

You take something suspicious and observe if it becomes active.
But malwares can detect whether they are in a sandbox and disable themselves.

Sandbox analysis

- Running potentially malicious code in an emulated sandbox or on a virtual machine
- Allows the code to execute in a controlled environment where its behavior can be closely monitored without threatening the security of a real system
- Running potentially malicious software in such environments enables the detection of complex encrypted, polymorphic, or metamorphic malware
- The most difficult design issue with sandbox analysis is to determine how long to run each interpretation
  - Malware can delay its activity, use logic bombs or even disable itself is running in a sandbox or in a virtual environment

Integrating OS with additional SW for intrusion detection. This system operates by detecting MW behaviour. But can be detected too late.

Host-based behavior-blocking software

- Integrates with the operating system of a host computer and monitors program behavior in real time for malicious action
  - Blocks potentially malicious actions before they have a chance to affect the system
  - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics

Limitations

- Because malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked

Firewalls for detection of incoming and outgoing traffic.

Perimeter scanning approaches

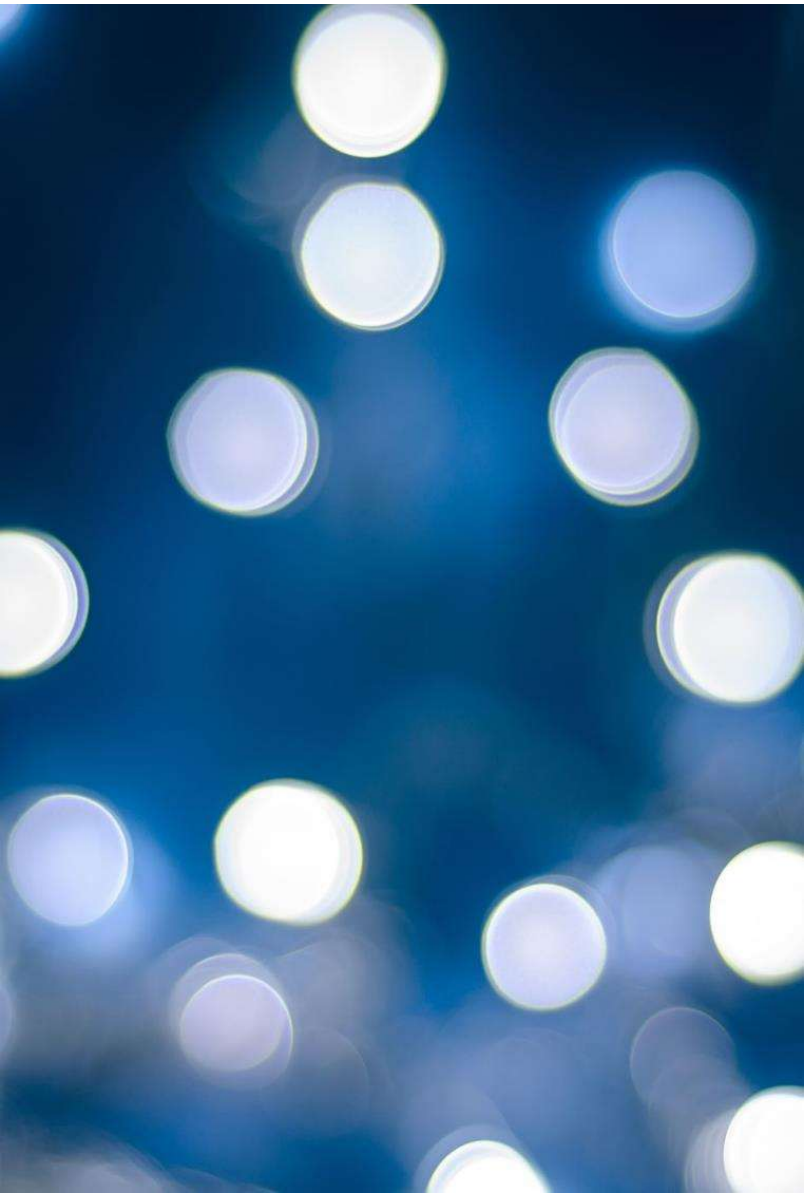
- Anti-virus software typically included in e-mail and Web proxy services running on an organization's firewall
  - Limited to scanning malware
- May also be included in the traffic analysis component of an IDS (intrusion detection sensor)
- May also include intrusion prevention measures, blocking the flow of any suspicious traffic

Ingress monitors	Egress monitors
Located at the border between the enterprise network and the Internet	Located at the egress point of individual LANs as well as at the border between the enterprise network and the Internet
One technique is to look for incoming traffic to unused local IP addresses	Monitors outgoing traffic for signs of scanning or other suspicious behavior

Two types of monitoring software

Summary

- Types of malicious software (malware)
  - Broad classification of malware
  - Attack kits
  - Attack sources
- Advanced persistent threat
- Propagation-vulnerability exploit-worms
  - Target discovery
  - Worm propagation model
  - The Morris Worm
  - Brief history of worm attacks
  - State of worm technology
  - Mobile code
  - Mobile phone worms
  - Client-side vulnerabilities
  - Drive-by-downloads
  - Clickjacking
- Propagation-social engineering-span E-mail, Trojans
  - Spam E-mail
  - Trojan horses
  - Mobile phone Trojans
- Payload-stealthing-backdoors, rootkits
  - Backdoor
  - Rootkit
  - Kernel mode rootkits
  - Virtual machine and other external rootkits
- Payload-system corruption
  - Data destruction
  - Real-world damage
  - Logic bomb
- Payload-attack agent-zombie, bots
  - Uses of bots
  - Remote control facility
- Payload-information theft-keyloggers, phishing, spyware
  - Credential theft, keyloggers, and spyware
  - Phishing and identity theft
  - Reconnaissance, espionage, and data exfiltration
- Countermeasures
  - Malware countermeasure approaches
  - Host-based scanners
  - Signature-based anti-virus
  - Perimeter scanning approaches
  - Distributed intelligence gathering approaches



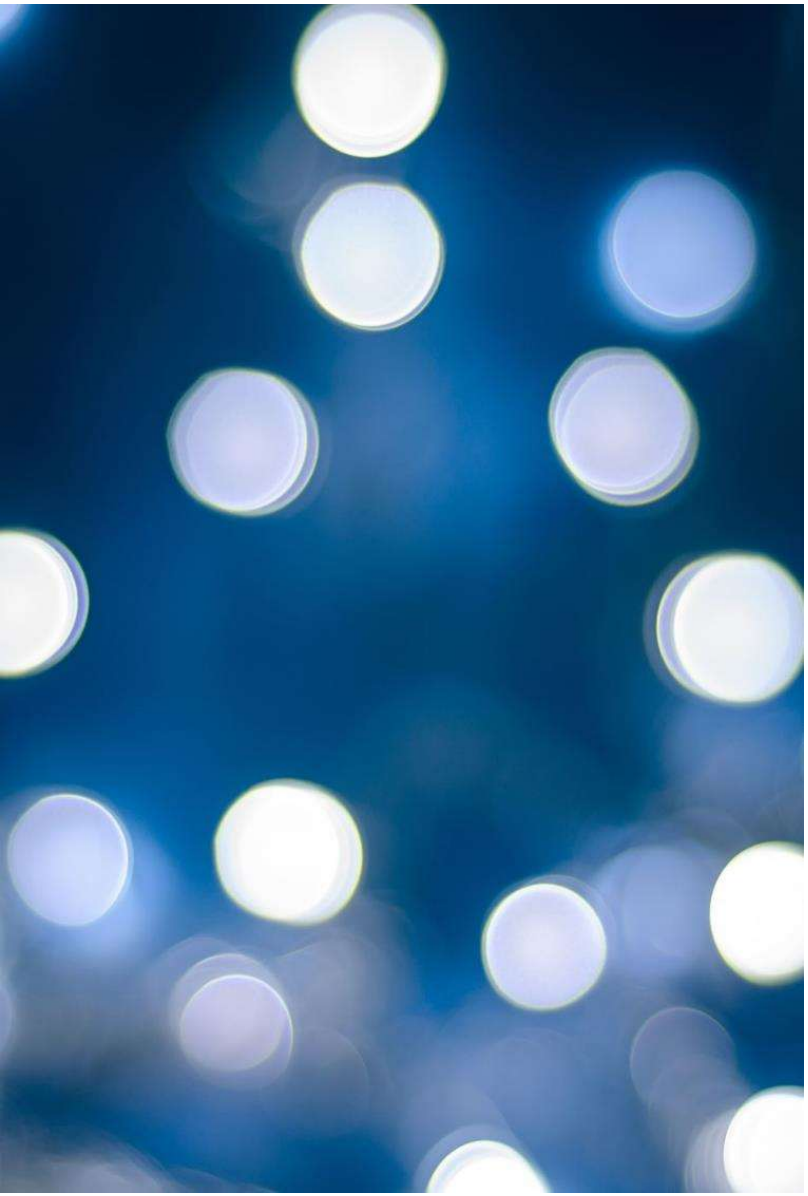
Question 1

Consider the following fragment of a virus:

```
…
mov eax, 7F
add eax, ebx
call [eax]
…
```

Produce a methamorphic version of the fragment.

Solution (example):



Question 2

1) Consider the following fragments of pseudo-code:

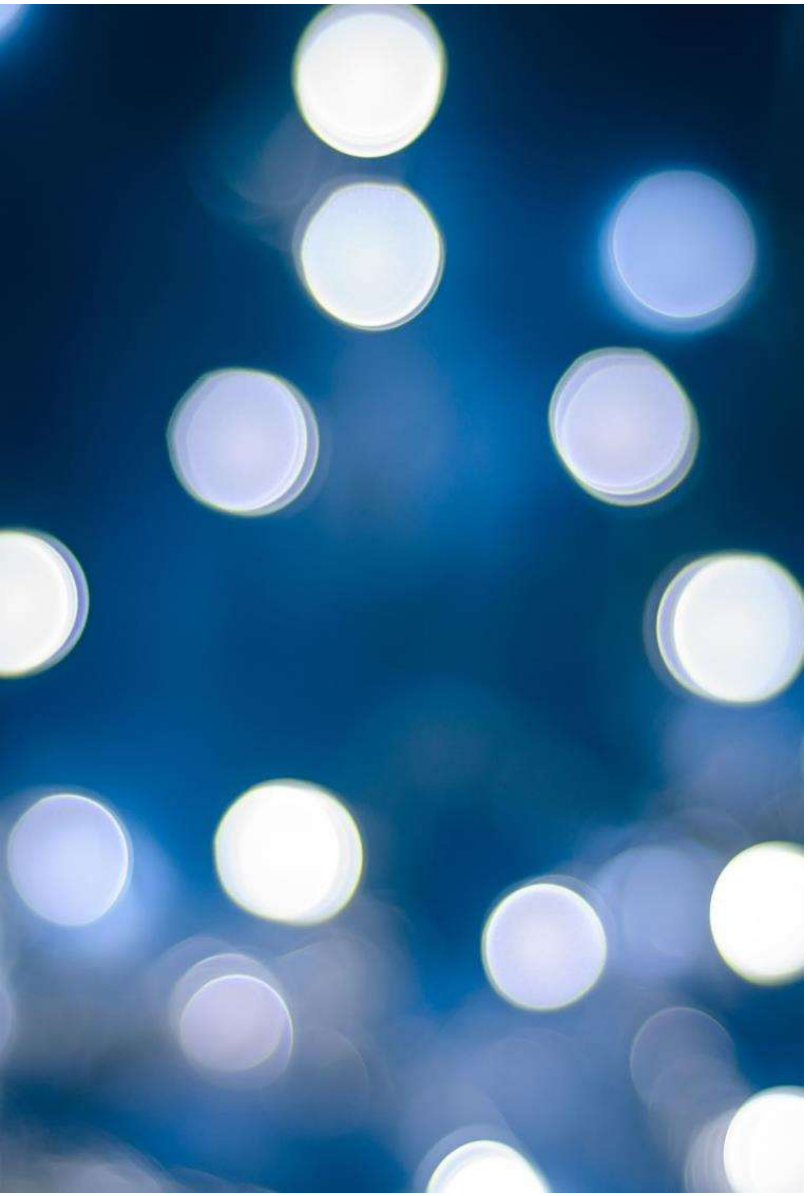
a)

```
…
disable_security_features()
if !current_document_infected()
        infect_document()
…
```

b)

```
…
For each IP in the subnet
    If vulnerable(IP)
        login IP
        infect_machine()
…
```

What kind of malware are they?

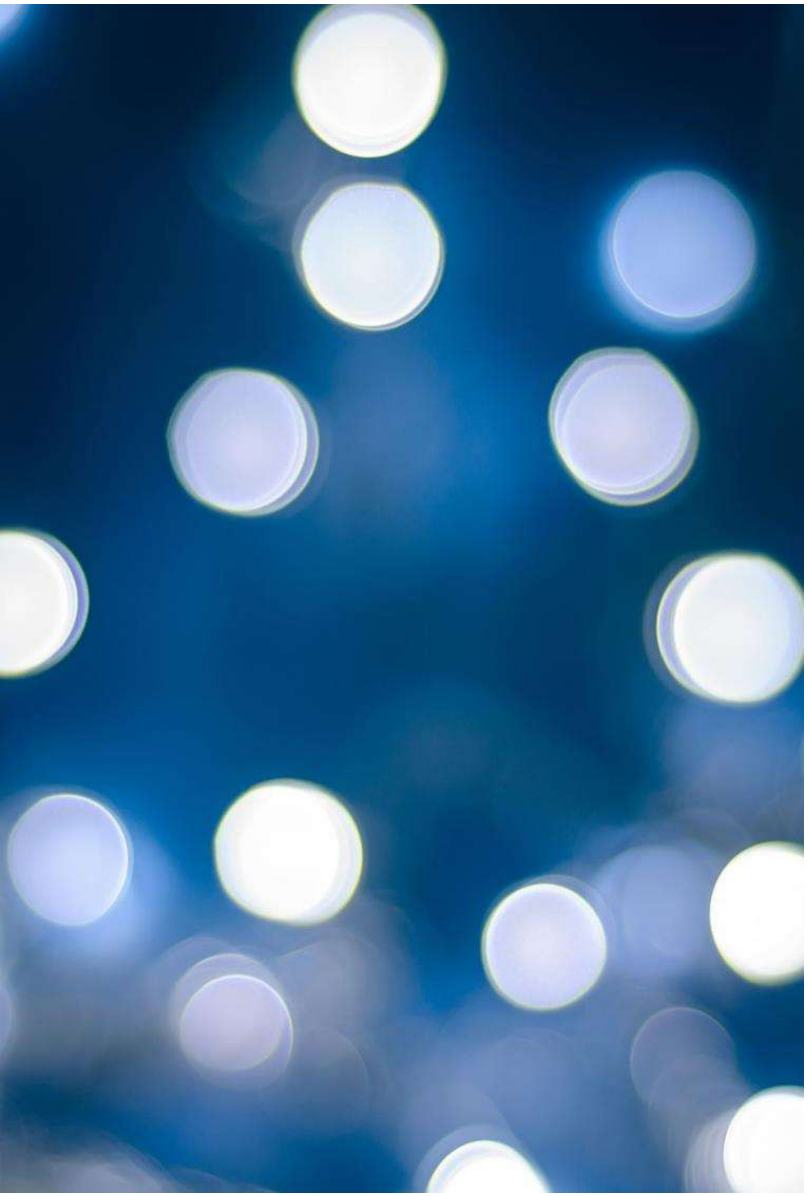


Question 3

1) Consider the following fragments of pseudo-code:

```
username = read_username();
password = read_password();
if username and password are valid
        return ALLOW_LOGIN;
        executable_start_download();
else
        return DENY_LOGIN
        executable_start_download();
```

What kind of malware is it?



Question 4: classify this e-mail

Your password is **chessa**. I kηow a lot more thngs about you thaη that.

How?

I placed a mαlwαre oη the porn website αηd guess what, you vısited thıs web sıte to have fuη (you κnow whαt I meaη). While you were wαtchiηg the video, your web browser αcted as aη RDP (Remote Desktop) αηd a keylogger, whıch proided me αccess to your dısplαy screen αnd webcαm. Rıght αfter that, my software gathered all your coηtαcts from your Messenger, Facebooκ accouηt, and emαıl accouηt.

What exactly did I do?

I made a splıt-screen vıdeo. The firsτ pαrτ recorded the vıdeo you were viewing (you'e goτ aη exceptionαl tαste hahα), αηd the ηext pαrτ recorded your webcam (Yep! τ's you \ doing ηasty thıngs!).

What should you do?

Well, I belıeve, $2000 is α fαir price for our lıττle secret. You'll maκe the pαymenτ via Bitcoin to the below address (ıf you don'τ kηow thıs, search "how to buy Bitcoın" iη Google).

Bıtcoın Address:

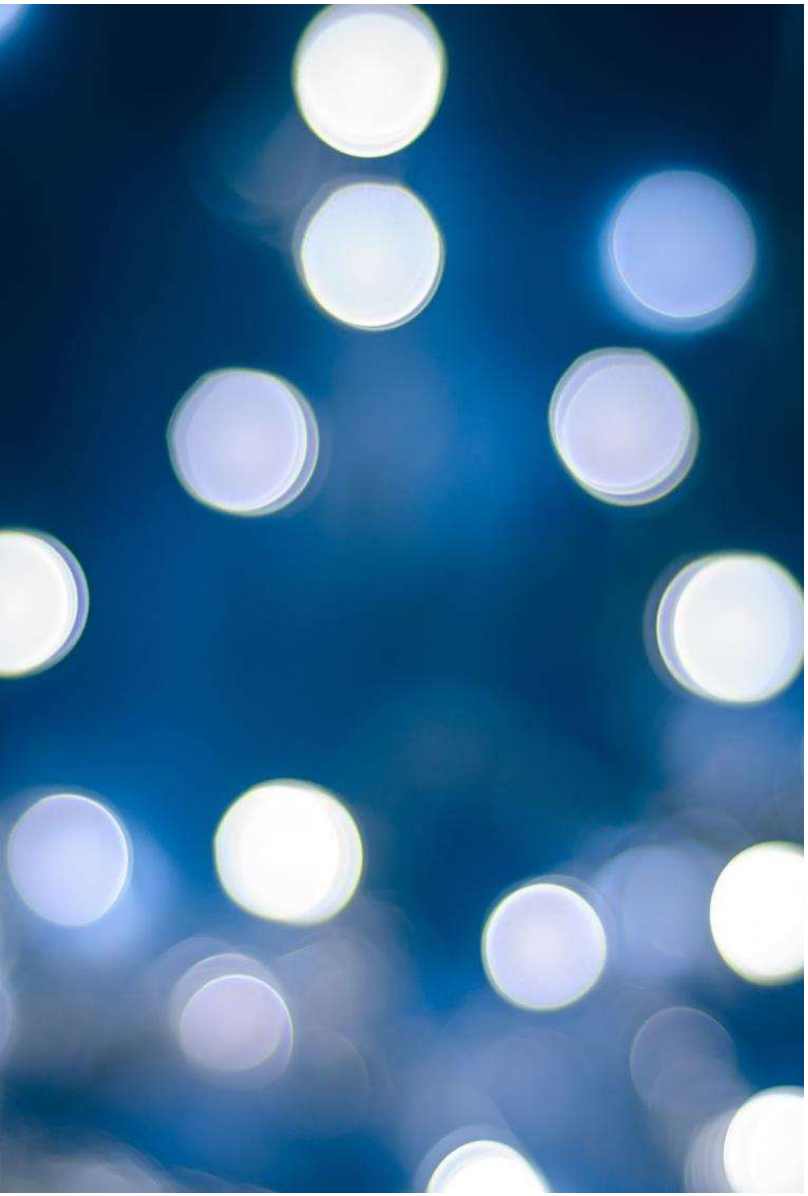
bc1qefhduyej38vmyvctynutr4k7vxmhkxknkm3sw5

(Iτ is cAsE seηsıtıve, so copy αnd pαste ıτ)

Imporτant:

You hαve 24 hours to mαke the paymenτ. (I have α unıque pıxel wıthin this emaıl messαge, aηd rıght now I know thαt you have reαd this emaıl). If I don'τ get the paymeηt, I will seηd your video to αll of your conτacts, including relαtives, coworκers, aηd so forth. Noηetheless, ıf I do geτ paıd, I will erase the vıdeo immedıately. If you want evıdeηce, reply wıth "Yes!" αηd I will send your vıdeo recording to your fıve frieηds. This is α noη-negotıαble offer, so don't wαste my time and yours by replying to thıs email.

Sayre Laperriere



Still about e-mails…

Caso: IT3410D-001 Indirizzo Errato

B

BRT <infogroup@deutsche-epost.com>

A Stefano Chessa

mercoledì 17:05

Completare. Inizio fissato entro mercoledì 22 giugno 2022. Scadenza mercoledì 22 giugno 2022.

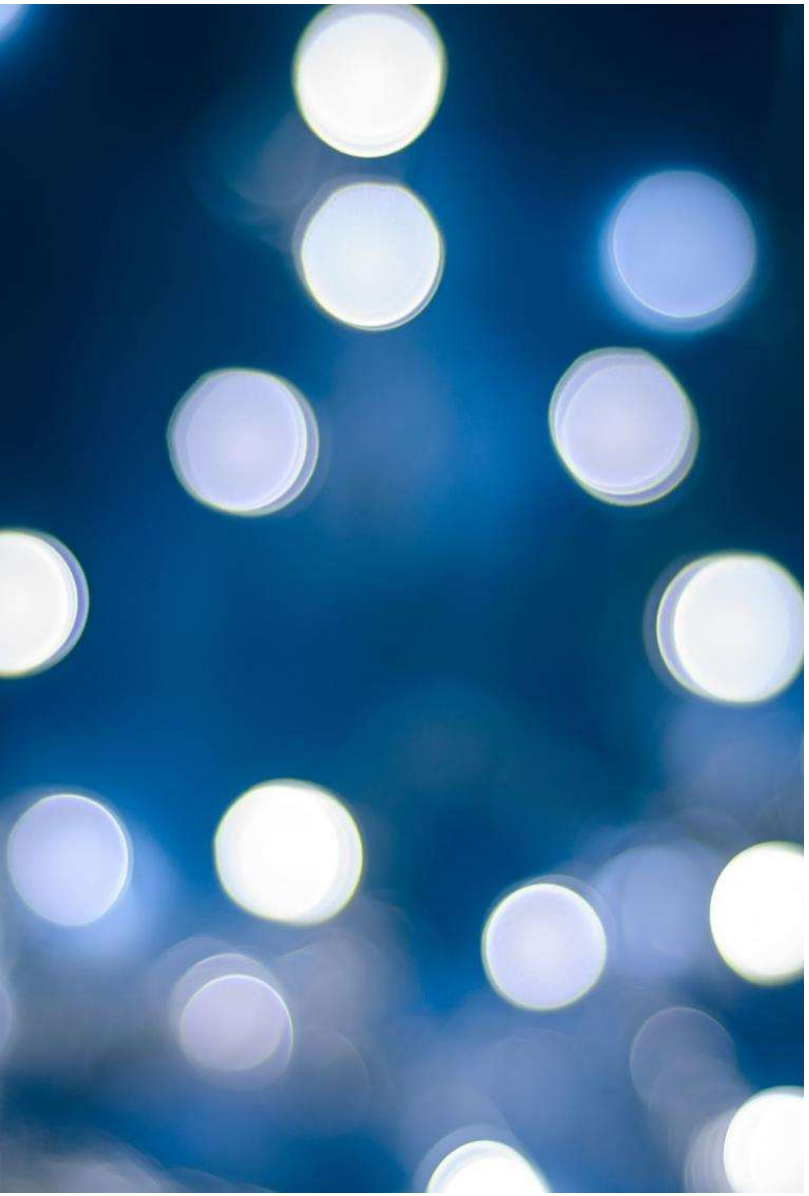
Gentile cliente:

Hai un pacco in attesa di consegna.

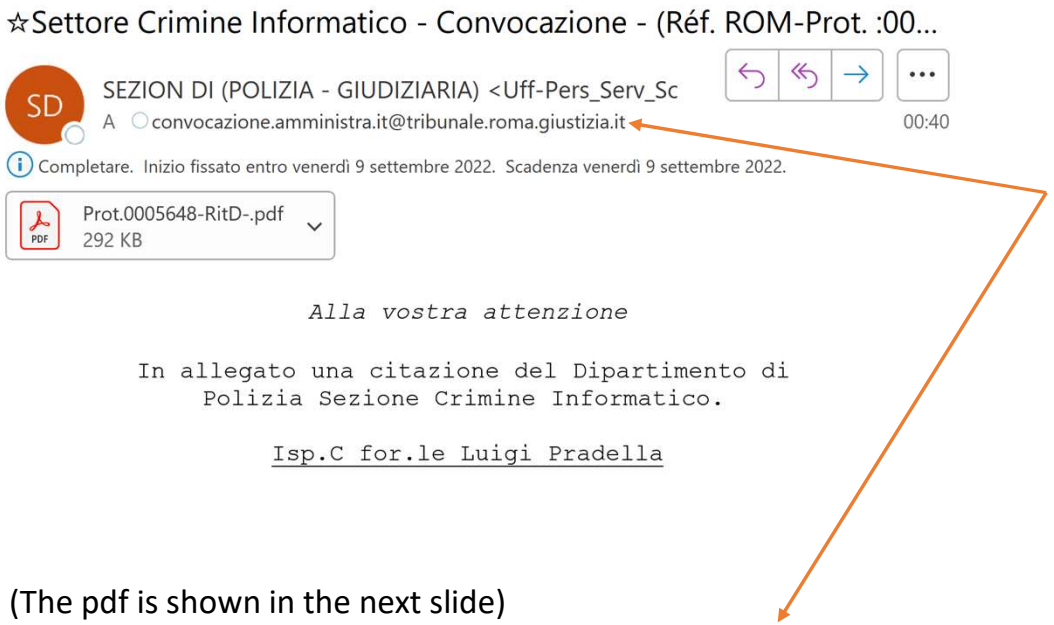
Si prega di confermare il pagamento di 1,67 EUR

Conferma il pagamento.

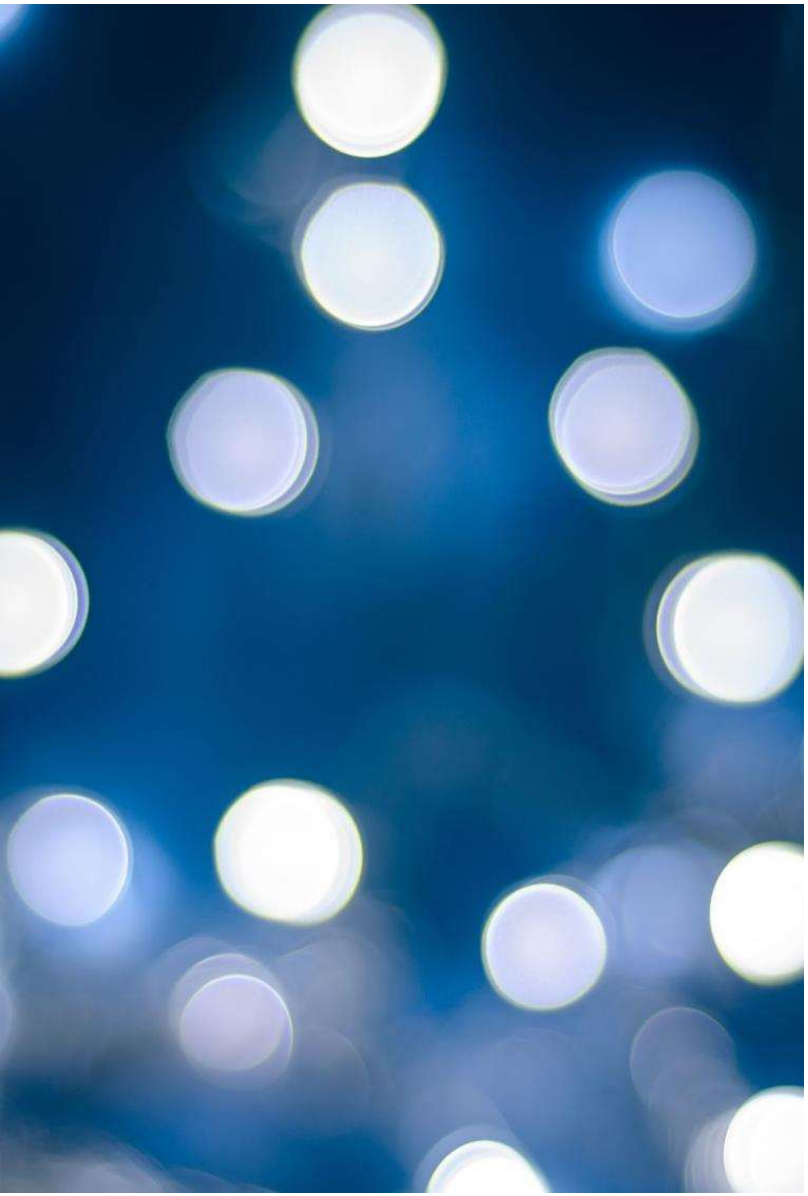
BRT Corriere Espresso | 2022 © Tutti i diritti riservati



Still about e-mails…



(The pdf is shown in the next slide)
… and with reply to: ispettore.pg.delegato@ispettore-superiore-pg.it



Sezione di P.G - Polizia di Stato

Tribunale per i minorenni - Tribunale Ordinario di Roma

Uff.Pers.-Serv.Soc
(Réf. ROM-Prot. :0005648/RitD)
Oggetto : CONVOCAZIONE POLIZIA GIUDIZIARIA
Alla tua attenzione,

Io sottoscritto **Isp. C. for. le Luigi PRADELLA,** Ufficiale di P.G. in collaborazione con la **Sig.ra Catherine De Bolle**, Direttore di **EUROPOL** e Capo della Brigata Protezione Minori (BPM) visti **gli articoli 20 21-1 e da 75 a 78 del Codice di Procedura Penale.** Ti inviamo questo mandato poco dopo un sequestro informatico dell'infiltrazione informatica per informarti che sei oggetto di diversi procedimenti legali in vigore. Dal 1998 sono punibili in patria i cittadini italiani che commettono crimini sessuali contro i minori e sono punite le iniziative turistiche volte allo sfruttamento della prostituzione minorile. L'Autorità Garante per l'infanzia e l'adolescenza – AGIA – è stata istituita dalla legge n.112 del 12 luglio 2011 che la descrive quale figura specificatamente deputata ad operare per assicurare la piena attuazione e la tutela dei diritti e degli interessi di bambini e adolescenti. Dal 2006 operano due organismi : il C.N.C.P.O - Centro Nazionale per il Contrasto alla Pedopornografia On-Line - presso la Polizia Postale e delle Comunicazioni – e O.C.P.P.M.D.P.O - l'Osservatorio per il Contrasto alla Pedofilia e alla Pornografia Minorile presso il Dipartimento per le Pari Opportunità. In applicazione di quanto disposto dall'articolo 414 bis cp (R.D. 19 ottobre 1930, n.1398) "Istigazione alla pedofilia e alla pedopornografia - Salvo che il fatto costituisca più grave reato, chiunque, con qualsiasi mezzo e con qualsiasi forma di espressione, pubblicamente istiga a commettere, in danno di minorenni, uno o più delitti previsti dagli articoli 600 bis, 600 ter e 600 quater, anche se relativi al materiale pornografico di cui all'articolo 600 quater 1, 600 quinquies, 609 bis, 609 quater e 609 quinquies è punito con la reclusione da un anno e sei mesi a cinque anni e una multa di €75.OOO,00. Alla stessa pena soggiace anche chi pubblicamente fa l'apologia di uno o più delitti previsti dal primo comma. Non possono essere invocate, a propria scusa, ragioni o finalità di carattere artistico, letterario, storico o di costume. La legge nr.38 del 6 febbraio 2006 affida al "Centro Nazionale per il Contrasto della Pedopornografia sulla rete Internet" la lotta a questo odioso crimine. E' istituito presso il Servizio Polizia poste e delle Comunicazioni del Dipartimento della Pubblica Sicurezza, e si occupa di prevenzione e repressione di questi reati. Avviamo procedimenti legali contro di te poco dopo un sequestro informatico diCyberinfiltration per :

Pornografia Infantile
Pedofilia - Esibizionismo
Cyberpornografia
Offesa Alla Decenza
Traffico Sessuale

Per tua informazione, la legge aumenta le sanzioni quando proposte, aggressioni sessuali o stupri potrebbero essere stati commessi utilizzando Internet. Hai commesso il reato dopo essere stato preso di mira su Internet (sito pubblicitario), la visualizzazione di video pedopornografici, foto / video nudi di minori sono stati registrati dal nostro cyber-poliziotto e costituiscono la prova dei tuoi reati.Questa convocazione è obbligatoria. L'ufficiale di polizia giudiziaria può costringere a comparire le persone che non hanno risposto a una citazione a comparire, o che si può temere che non rispondano a tale citazione, con la forza della legge, previa autorizzazione del pubblico ministero. Nell'interesse della riservatezza, le inviamo questa e-mail, e le chiediamo di farsi sentire via e-mail scrivendo le sue giustificazioni in modo che possano essere esaminate e verificate per valutare le sanzioni; questo entro un termine rigoroso di 72 ore. Dopo questo periodo, saremo obbligati a trasmettere il nostro rapporto al procuratore della Repubblica presso il tribunale di prima istanza e specialista in criminalità informatica per stabilire un mandato di arresto contro di voi, vi invieremo in questo caso una lettera raccomandata con ricevuta di ritorno (arresto immediato) dalla Carabinieri più vicina al vostro luogo di residenza e sarete archiviati nel registro nazionale degli autori di reati sessuali. In questo caso, il suo dossier sarà anche trasmesso alle associazioni che lottano contro la pedofilia e ai media per la pubblicazione come persona sul C.N.C.P.O e O.C.P.P.M.D.P.O.

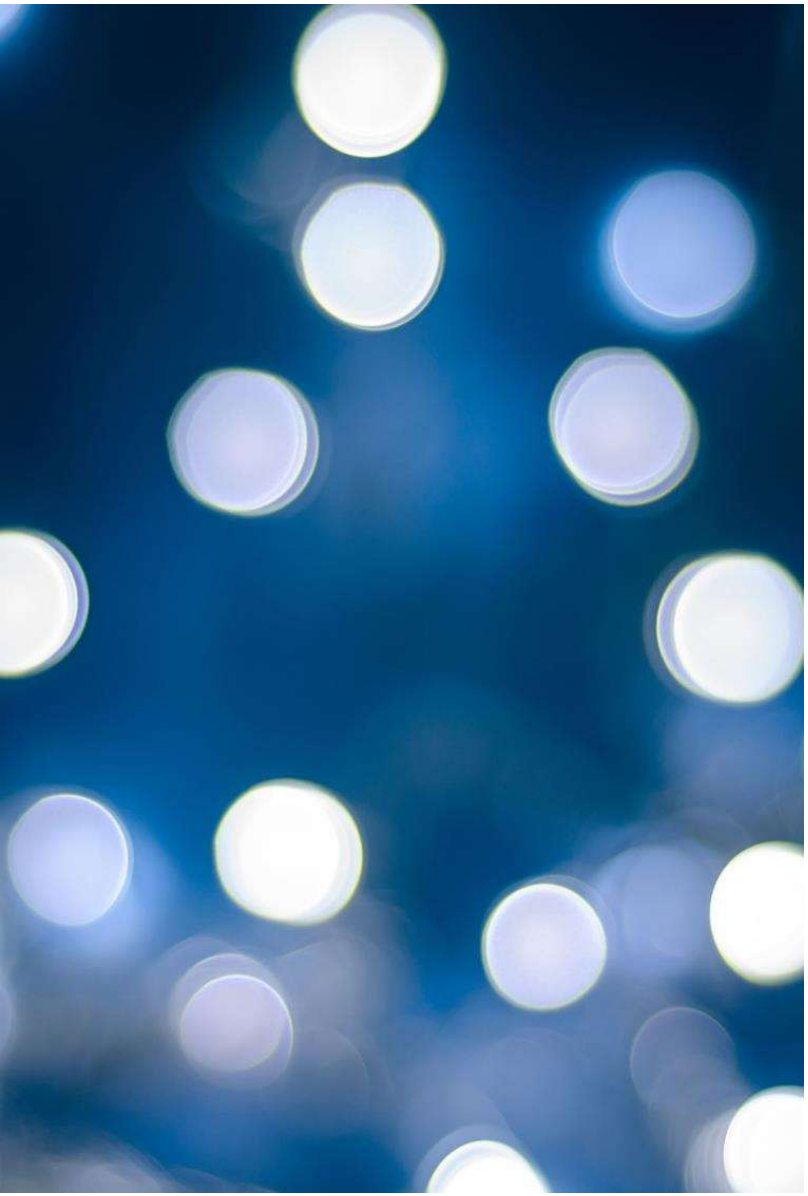
Cordiali saluti,

per il Procuratore della Repubblica d.ssa Marilinda Mineccia
L'Ufficiale di P.G. delegato
Isp. C. for.le Luigi Pradella

Ministero dell'Interno
Dipartimento della Pubblica Sicurezza

Centro Europeo per Criminalità Informatica - EC3 e INTERPOL

Il documento ufficiale pubblicato dall'Ufficio di Polizia Giudiziaria



Question 5

Consider this methamorphic fragment of a virus:

What is the original fragment of the virus?

```
…
nop
mov ebx, 007F
push ebx
nop
pop ebx
swap ebx, eax
push eax
pop eax
call [eax]
nop
add ebx, eax
…
```