Κακόβουλο λογισμικό

Νικόλαος Ε. Κολοκοτρώνης
Επίκουρος Καθηγητής

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Πελοποννήσου
Email: nkolok@uop.gr
Web: http://www.uop.gr/~nkolok/

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

Περιεχόμενα

Περιεχόμενα

- Types of malicious software (malware)
- Propagation
  - Infected content (viruses)
  - Vulnerability exploit (worms)
  - Social engineering (spam e-mail, trojans)
- Payload
  - Attack agent (zombie, bots)
  - Information theft (key loggers, phishing, spyware)
  - Stealthing (backdoors, rootkits)
- Countermeasures

Malicious Software

Terminology

Name	Description
Virus	Malware that, when executed, tries to replicate itself into other executable 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.
Logic bomb	A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.
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 the Trojan horse program.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality.
Mobile code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Kit (virus generator)	Set of tools for generating new viruses automatically.
Spammer programs	Used to send large volumes of unwanted e-mail.
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.
Spyware	Software that collects information from a computer and transmits it to another system.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

Malware classification

- Can be 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

Malware classification

- Propagation mechanisms
  - Include infection of existing executable or interpreted content by viruses that is subsequently spread to other system
  - Exploit of software vulnerabilities either locally or over a network 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

Malware classification

- Earlier approaches to malware classification distinguished between
  - Those that need a host program, being parasitic code such as viruses
  - Those that are independent, self-contained programs run on the system such as worms, trojans, and bots
- Another distinction used was
  - Malware that does not replicate, such as trojans and spam e-mail
  - Malware that does, including viruses and worms

Malware classification

- Payload actions performed by malware once it reaches a target system can include
  - Corruption of system or data files
  - Theft of service (makes the system a zombie, part of a botnet
  - Theft of information (especially logins, passwords, or other personal details by keylogging or spyware programs)
  - Stealthing (malware hides its presence on the system from attempts to detect and block it)
- Blended attack uses many infection/propagation methods
  - To maximize contagion speed and attack's severity

Malware case: mirai

Mirai systems in Europe (July 2017)

Attack kits

- Initially, the development and deployment of malware required considerable technical skill by software authors
- This changed with the development of virus-creation toolkits (1990s) and more general attack kits (2000s)
  - These toolkits are often known as *crime-ware*
  - Include a variety of propagation mechanisms and payload modules that even novices can combine, select, and deploy
  - Can easily be customized with the latest discovered vulnerabilities
    - Exploit the opportunity window: weakness publication vs. patch deployment
  - Increased the population of attackers able to deploy malware

Attack sources

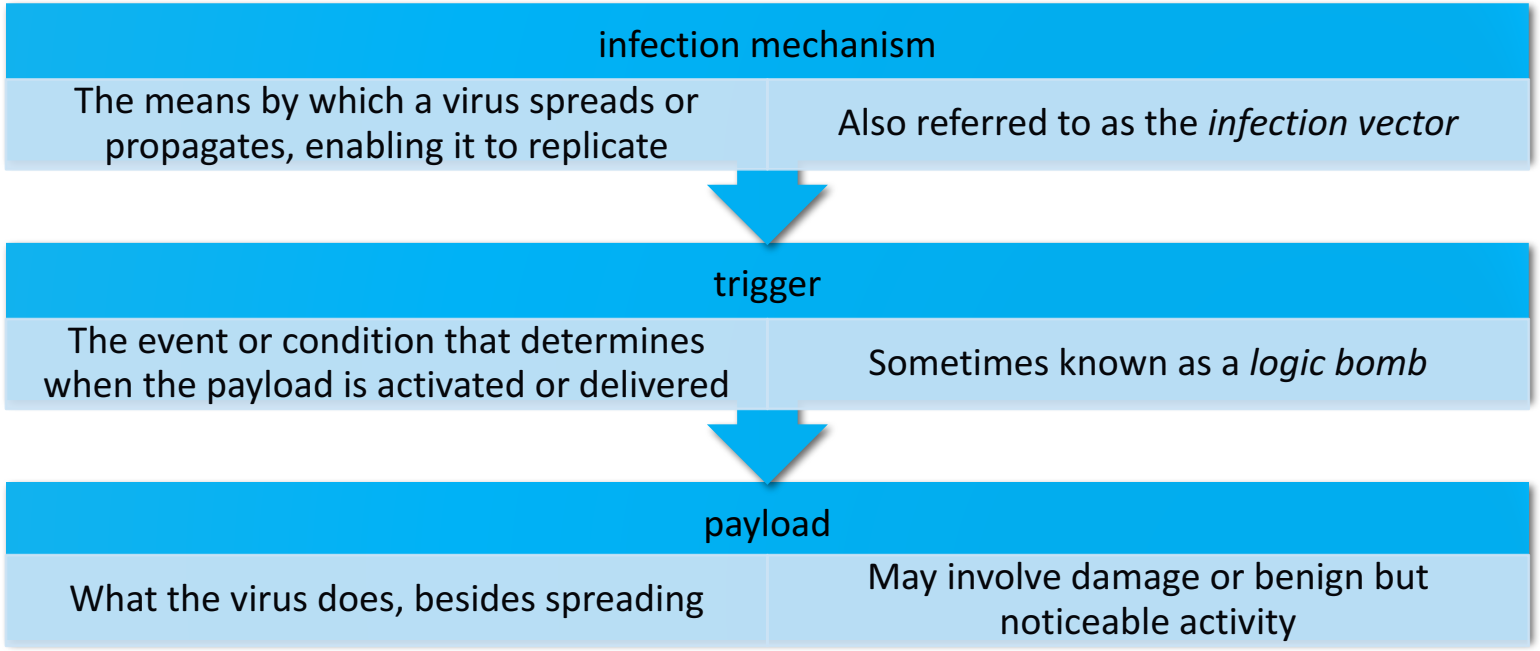
- A significant malware development is the change from individual attackers to organized and dangerous attack sources
  - These include politically motivated attackers, criminals, organized crime, organizations that sell their services to companies and nations, and national government agencies
- This has significantly changed 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

Viruses

- Parasitic software fragments that attach themselves to some existing executable content
- Can “infect” other programs or any type of executable content and modify them
- The modification includes injecting the original code with a routine to make copies of the virus code, which can then go on to infect other content
- One reason viruses dominated the malware scene in earlier years was the lack of user authentication and access controls on personal computer systems

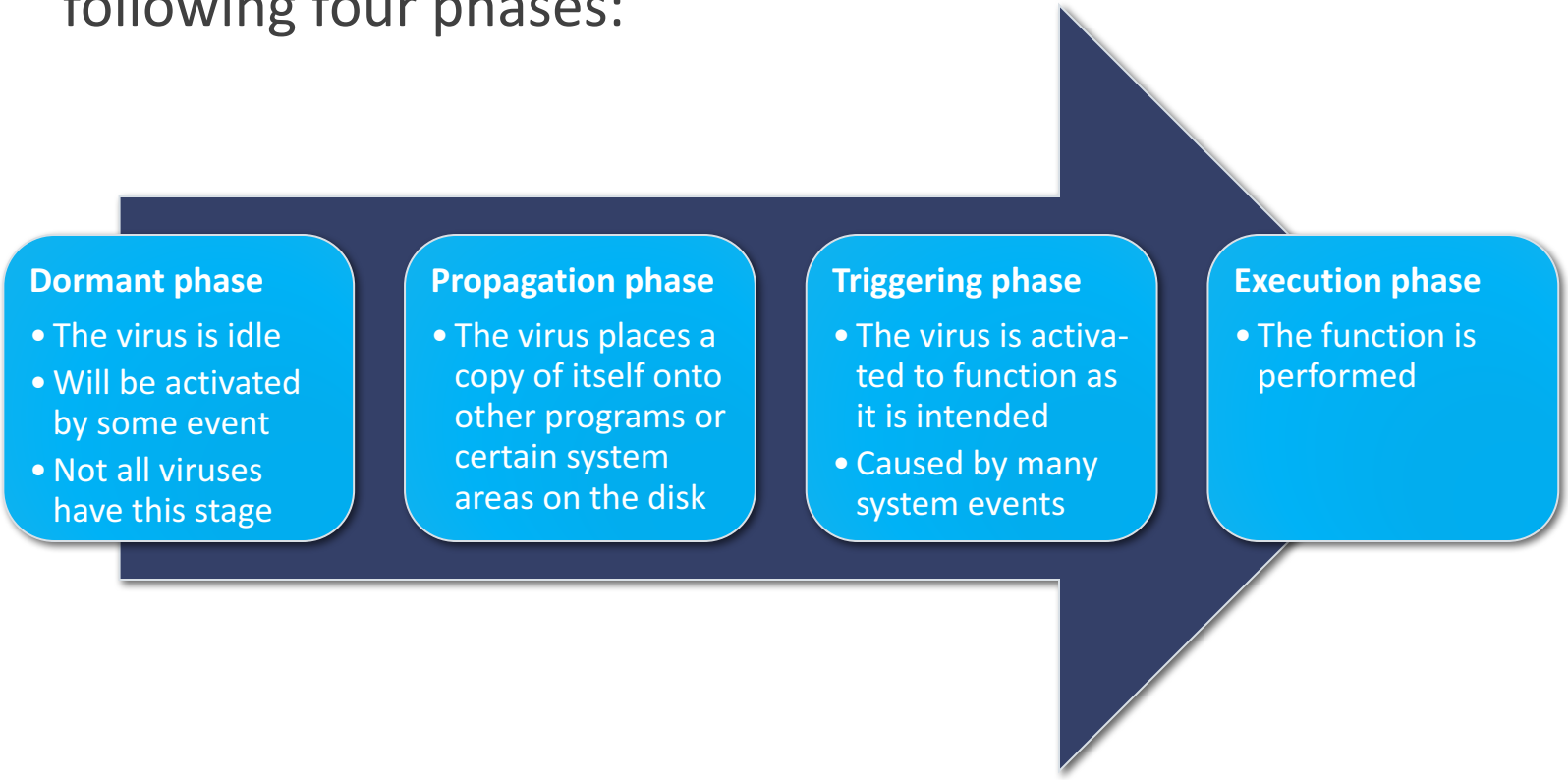
Virus structure

- A virus and many contemporary types of malware includes one or more variants of each of these components:



Virus phases

- During its lifetime, a typical virus goes through the following four phases:



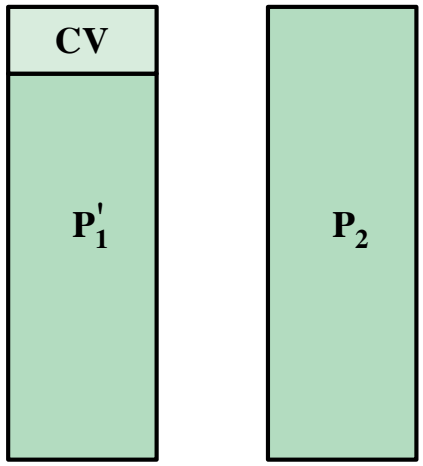
Simple virus

```
   program V :=

{goto main;
   1234567;

   subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
             then goto loop
             else prepend V to file; }

   subroutine do-damage :=
        {whatever damage is to be done}

   subroutine trigger-pulled :=
        {return true if some condition holds}

main:    main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

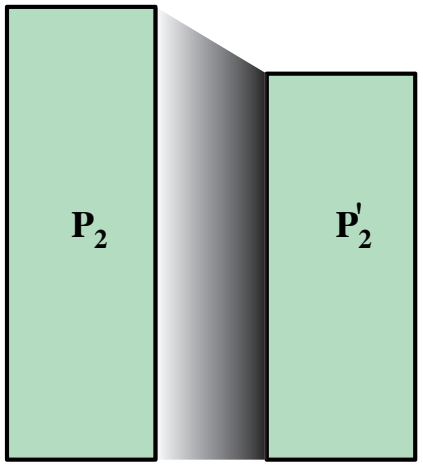
Compression virus

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
            {loop:
                file := get-random-executable-file;
            if (first-line-of-file = 01234567) then goto loop;
(1)         compress file;
(2)         prepend CV to file;
        }

main: main-program :=
            {if ask-permission then infect-executable;
(3)         uncompress rest-of-file;
(4)         run uncompressed file;}
        }
```

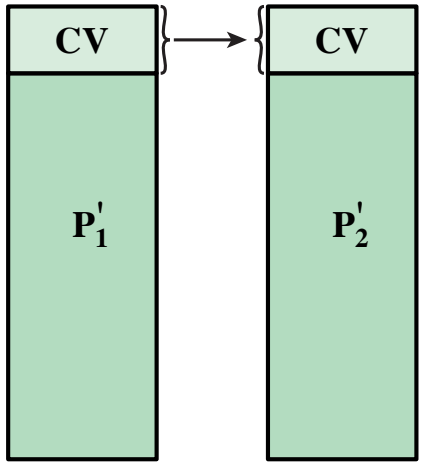
Compression virus



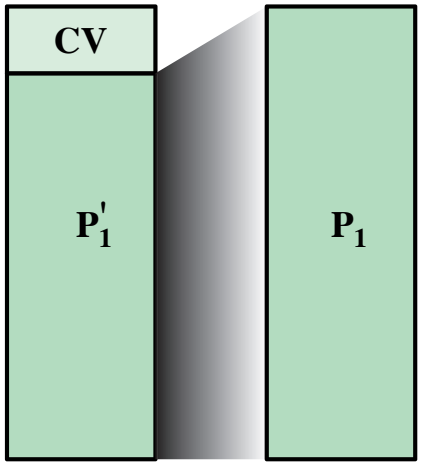
t_0: P_1' is infected version of P_1; P_2 is clean



t_1: P_2 is compressed into P_2'



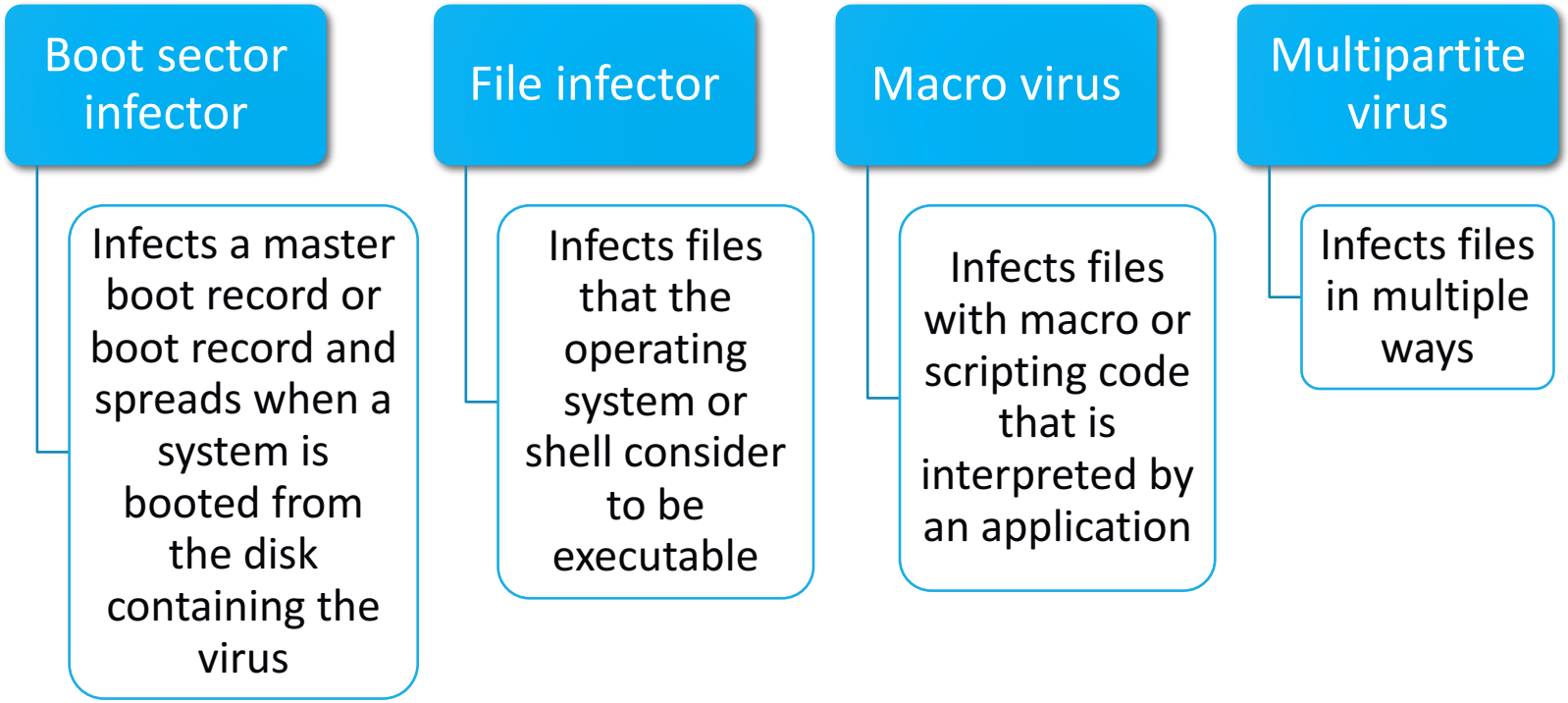
t_2: CV attaches itself to P_2'



t_3: P_1' is decompressed into the original program P_1

Virus types by target

- Includes the following categories



Virus types by concealment

- Encrypted virus
  - Portion of the virus creates a random encryption key and encrypts the remainder of the virus
  - When an infected program is invoked, the virus uses the stored random key to decrypt the virus
  - When the virus replicates, a different random key is selected
  - Because the bulk of the virus is encrypted with a different key for each instance, there is no constant bit pattern to observe
  - Examples:

Virus types by concealment

- Stealth virus
  - A form of virus explicitly designed to hide itself from detection by antivirus software
  - The entire virus, not just a payload is hidden
  - Examples:
- Polymorphic virus
  - A virus that mutates with every infection, making detection by the “signature” of the virus impossible
  - Examples:

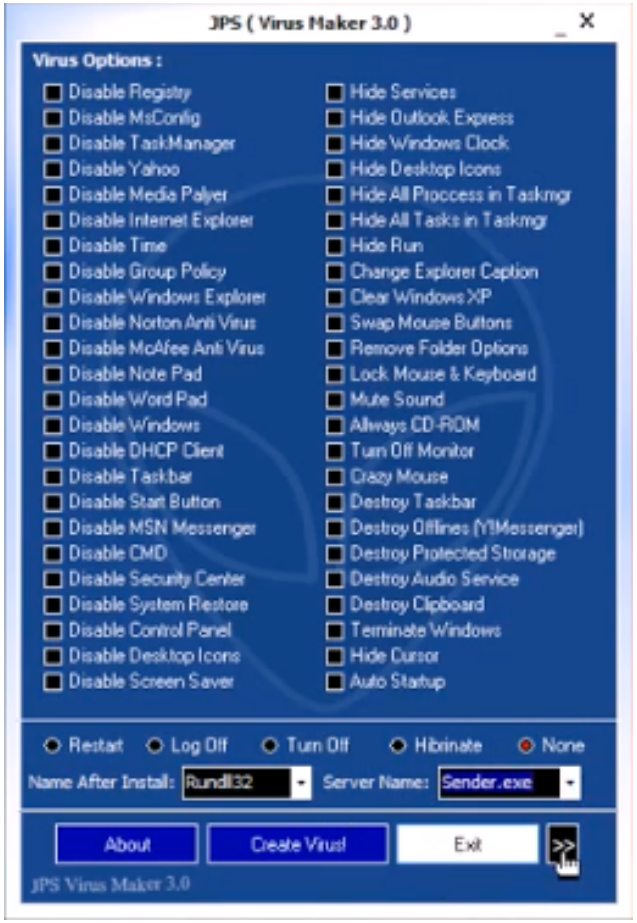
Virus types by concealment

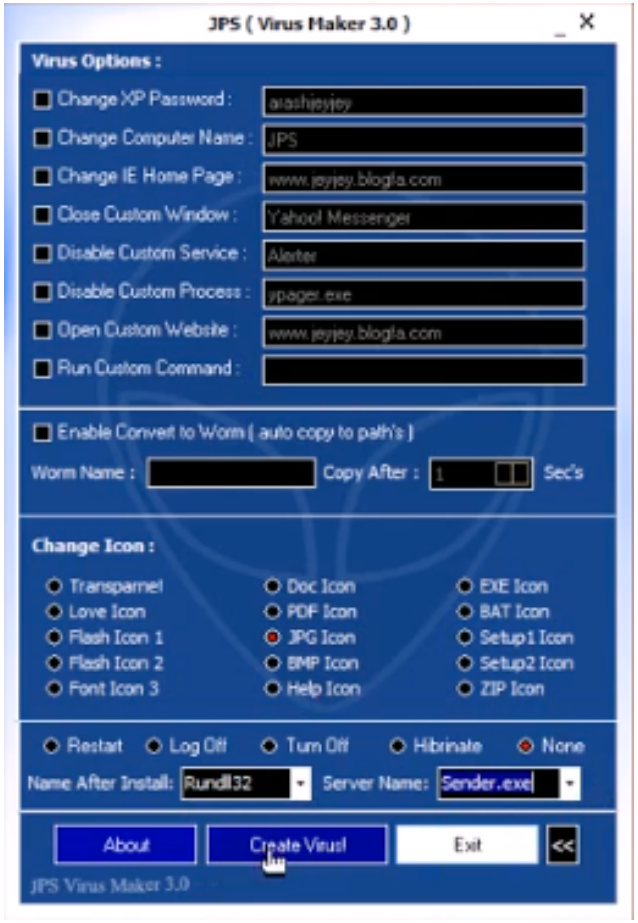
- Metamorphic virus
  - Mutates with every infection
  - Rewrites itself completely at each iteration, increasing the difficulty of detection
  - May change their behavior as well as their appearance
  - Examples:

Macro and scripting viruses

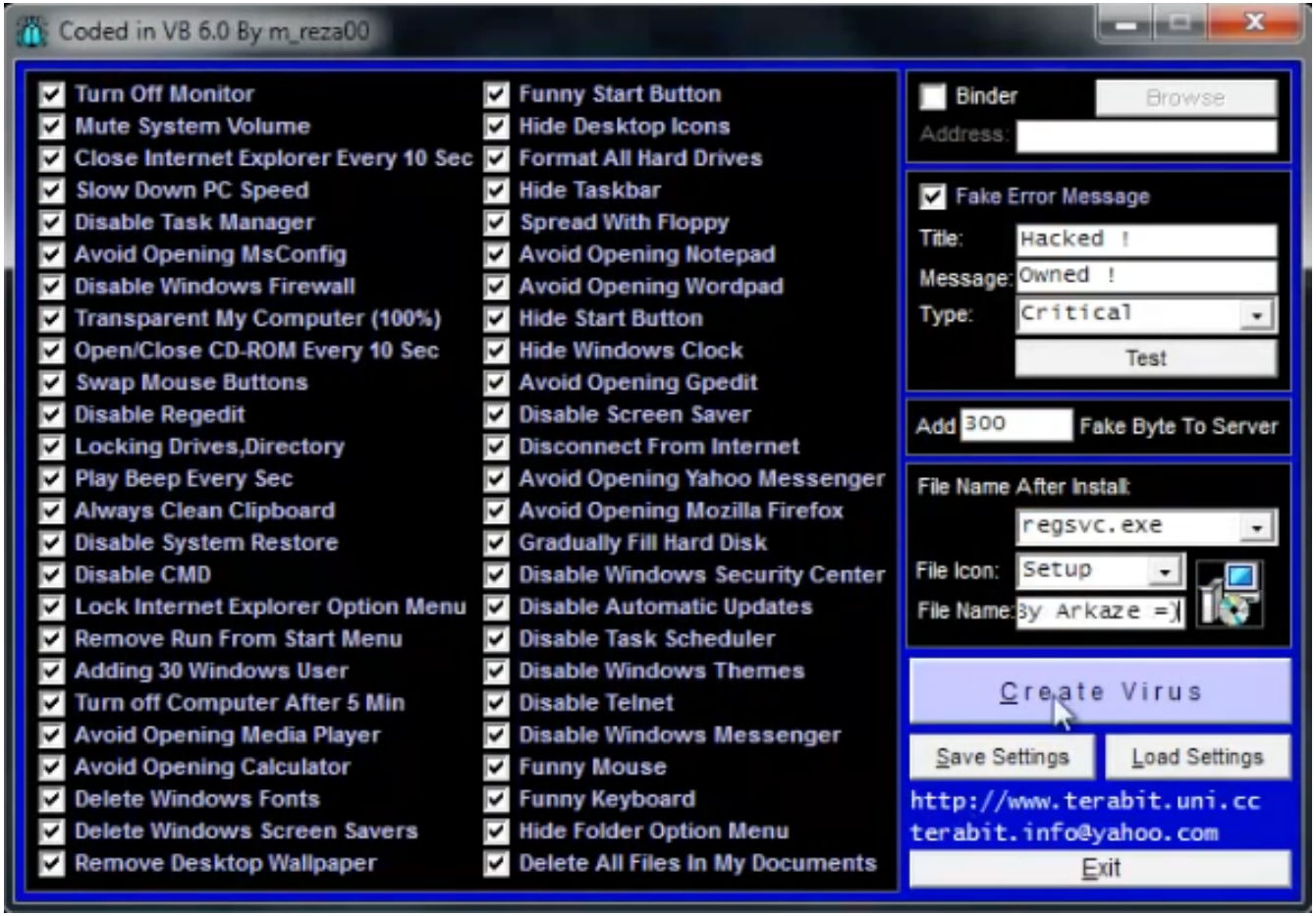
- Macro viruses infect scripting code used to support active content in a variety of user document types
- Threatening for a number of reasons
  - A macro virus is platform independent
  - Macro viruses infect documents, not executable portions of code
  - Macro viruses are easily spread, as the documents they exploit are shared in normal use
  - Because macro viruses infect user documents rather than system programs, traditional file system access controls are of limited use in preventing their spread

Virus makers: JPS





Virus makers: TeraBIT



Worms

- A program that actively seeks out more machines to infect
  - Upon activation, the worm may replicate and propagate again
- To replicate itself, a worm uses some means to access remote systems
  - Electronic mail or instant messenger facility
  - File sharing
  - Remote execution/login capability
  - Remote file access or transfer capability

Worm phases

- A worm typically uses the same phases as a virus
  - Dormant / Propagation / Triggering / Execution
- The propagation phase generally performs the following functions
  - Search for proper access mechanisms to other systems to infect
    - examine host tables, address books, buddy lists, trusted peers, and other similar repositories of remote system access details
  - Use the access mechanisms found to transfer a copy of itself to the remote system and cause the copy to be run

Target discovery

- Scanning/fingerprinting

  The function in the propagation phase for a network worm to search for other systems to infect

- Worm network scanning strategies:
  - Random
  - Hit list
  - Topological
  - Local subnet

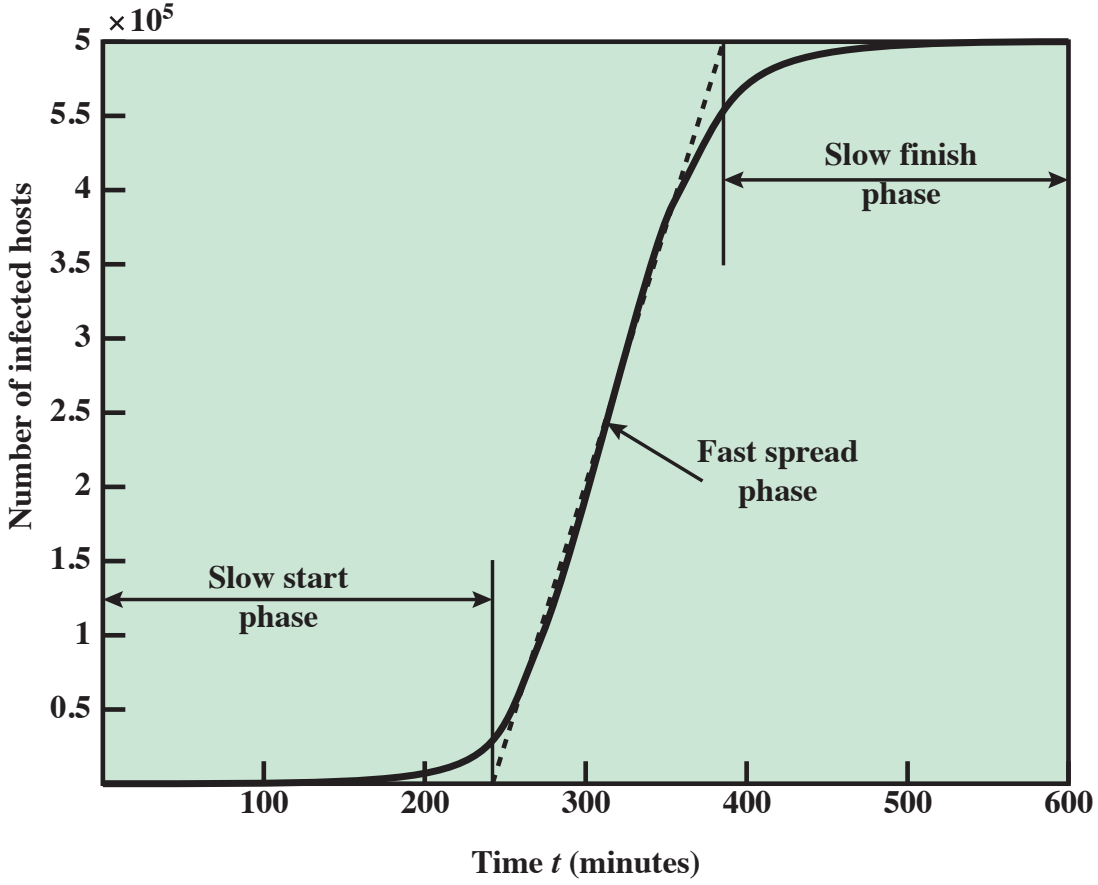
Target discovery

- Random
  - Each compromised host probes random addresses in the IP address space, using a different seed
  - Produces a high volume of Internet traffic, which may cause generalized disruption even before the actual attack is lunched
- Hit list
  - The attacker compiles a list of potential vulnerable machines
  - Then, the attacker begins infecting machines on the list
  - Each infected machine is given a portion of the list to scan
  - Results in a very short scanning period that makes it difficult to detect an infection is taking place

Target discovery

- Topological
  - Uses information contained on an infected victim machine to find more hosts to scan
  - Based on the network's topology
- Local subnet
  - If a host is 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

Worm propagation model



The Morris worm

- Released onto the Internet by Robert Morris in 1988
- Designed to spread on UNIX systems and used a number of different techniques for propagation
  - exploited known vulnerabilities in sendmail, finger, rsh/rexec and weak passwords
- When a copy began execution its first task was to discover other hosts known to this host that would allow entry from this host

The Morris worm

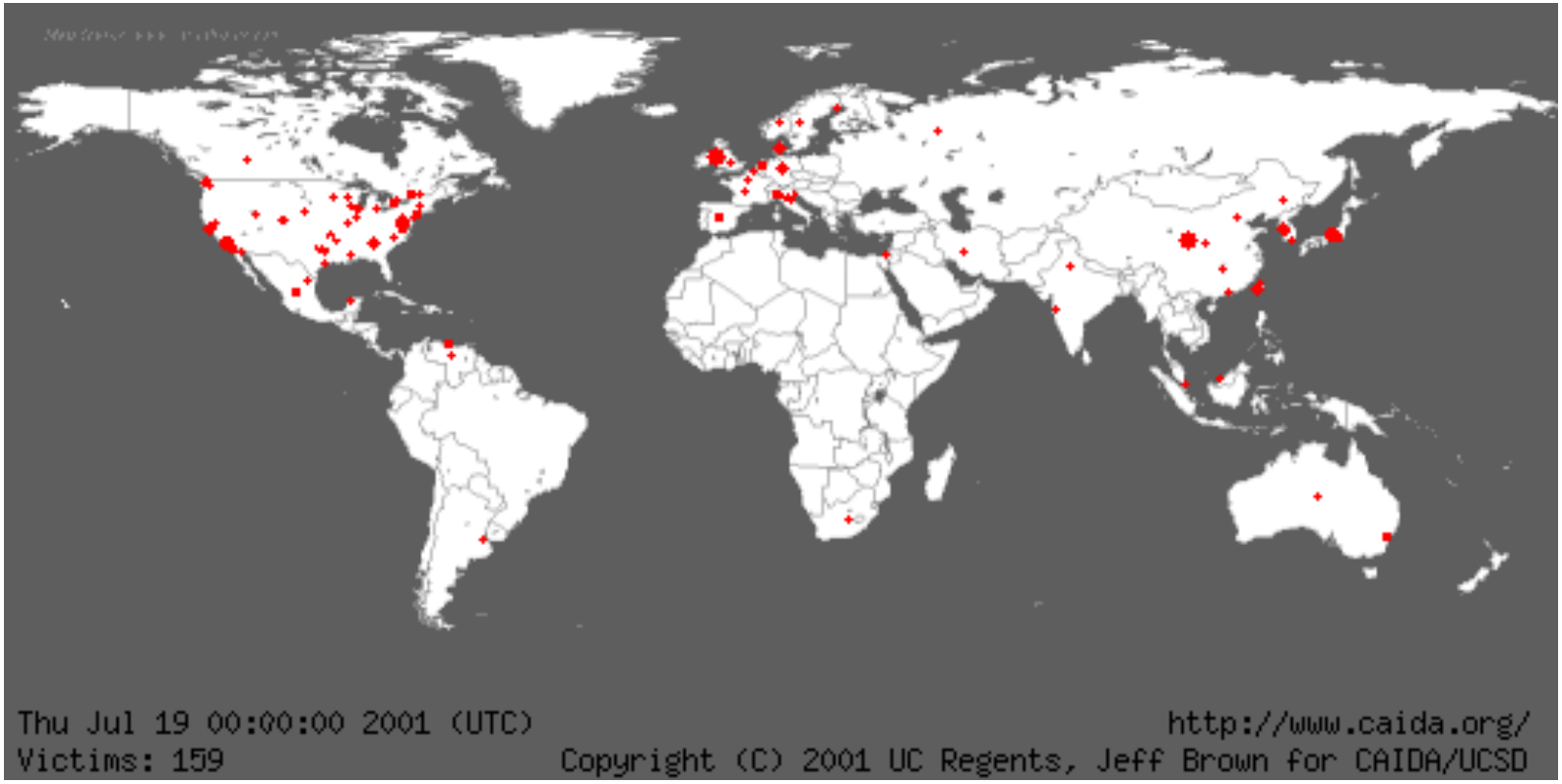
- For each discovered host, the worm tried a number of methods for gaining access
  - It attempted to log on to a remote host as a legitimate user
    - Used 432 built-in passwords
  - It exploited a bug in the UNIX finger protocol, which reports the whereabouts of a remote user
  - It exploited a trapdoor in the debug option of the remote process that receives and sends mail

Top computer worms

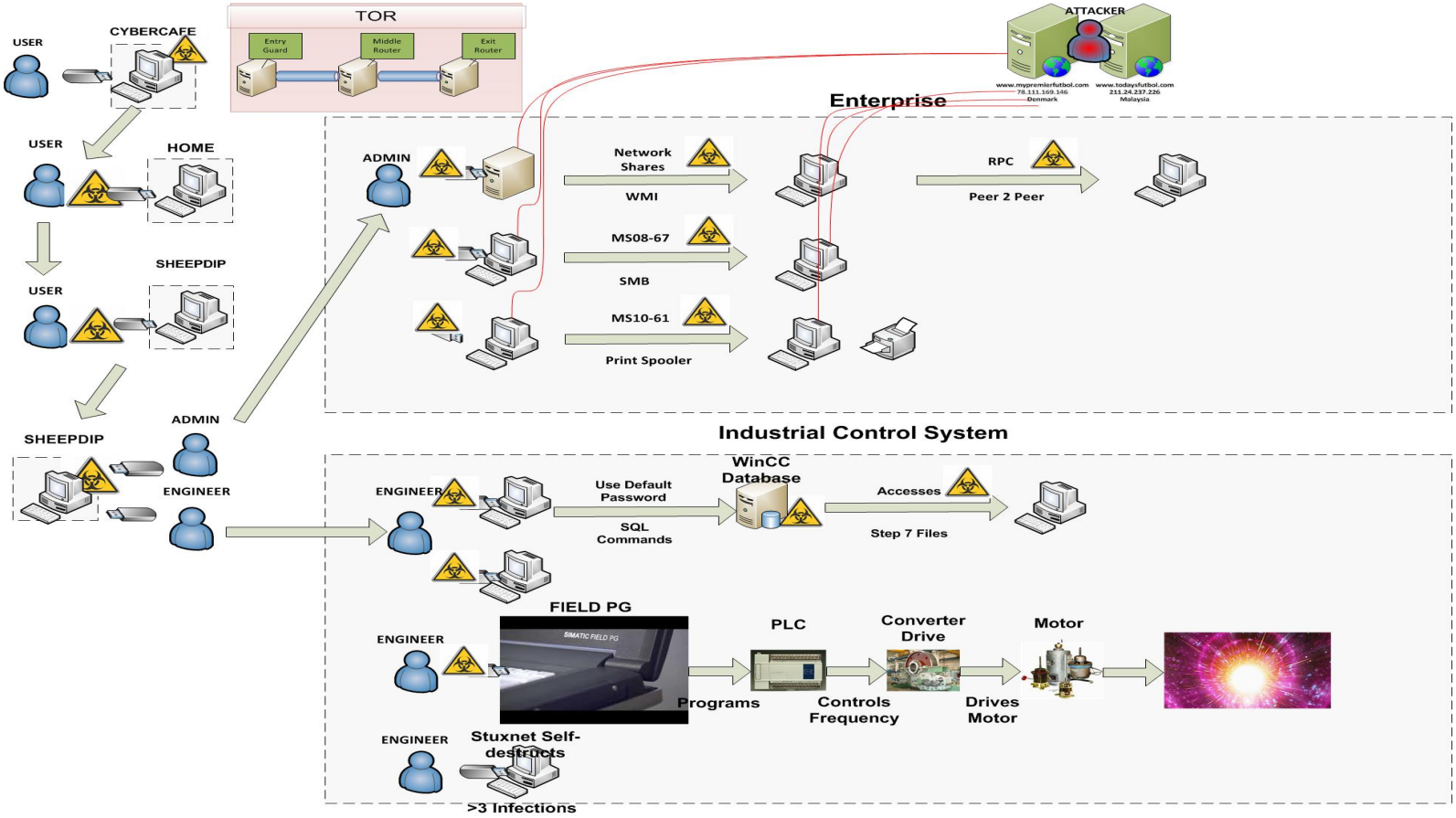
https://cyberwarfaremag.wordpress.com/tag/code-red/

Worm	Year	Damage
CIH	1998	$20-80m
Melissa	1999	$1bn
ILoveYou	2000	$5.5-8.7bn; 10% of all Internet connected PCs hit
Code Red	2001	$2bn
SQL Slammer	2003	Affected 500K servers globally; buffer overflaw
Blaster	2003	$2-10bn; hundreds of thousands of infected PCs
Sobig	2003	$1bn; 500K PCs globally
Sasser	2004	Tens of millions; shut down many companies' systems globally
MyDoom	2004	Slowed Internet by 10% and web load times by 50%
Bagle	2004	Tens of millions

The code red worm spreading



Worm: stuxnet



Worm: stuxnet

- Stuxnet worm ca be identified by antivirus programs as
  - *Symantec:* W32.Temphid
  - *F-Secure:* Trojan-Dropper:W32/Stuxnet
  - *Kaspersky:* Rootkit.Win32.Stuxnet.a (or .b)
  - *McAfee:* Stuxnet
  - *Sophos:* Troj/Stuxnet-A or W32/Stuxnet-B
  - *Norman:* W32/Stuxnet.A
  - *Trend Micro:* WORM_STUXNET.A

Worm technology

Multiplatform

- Newer worms can attack a variety of platforms

Multi-exploit

- Penetrate systems in a many ways, using exploits against web servers, e-mail, file sharing or via shared media

Ultrafast spreading

- Many techniques to optimize the rate of spread to max. its chance of locating as many vulnerable PCs as possible

Polymorphic

- Each copy has new code generated on the fly using equivalent instructions and encryption methods

Metamorphic

- They have a repertoire of behavior patterns that are unleashed at different stages of propagation

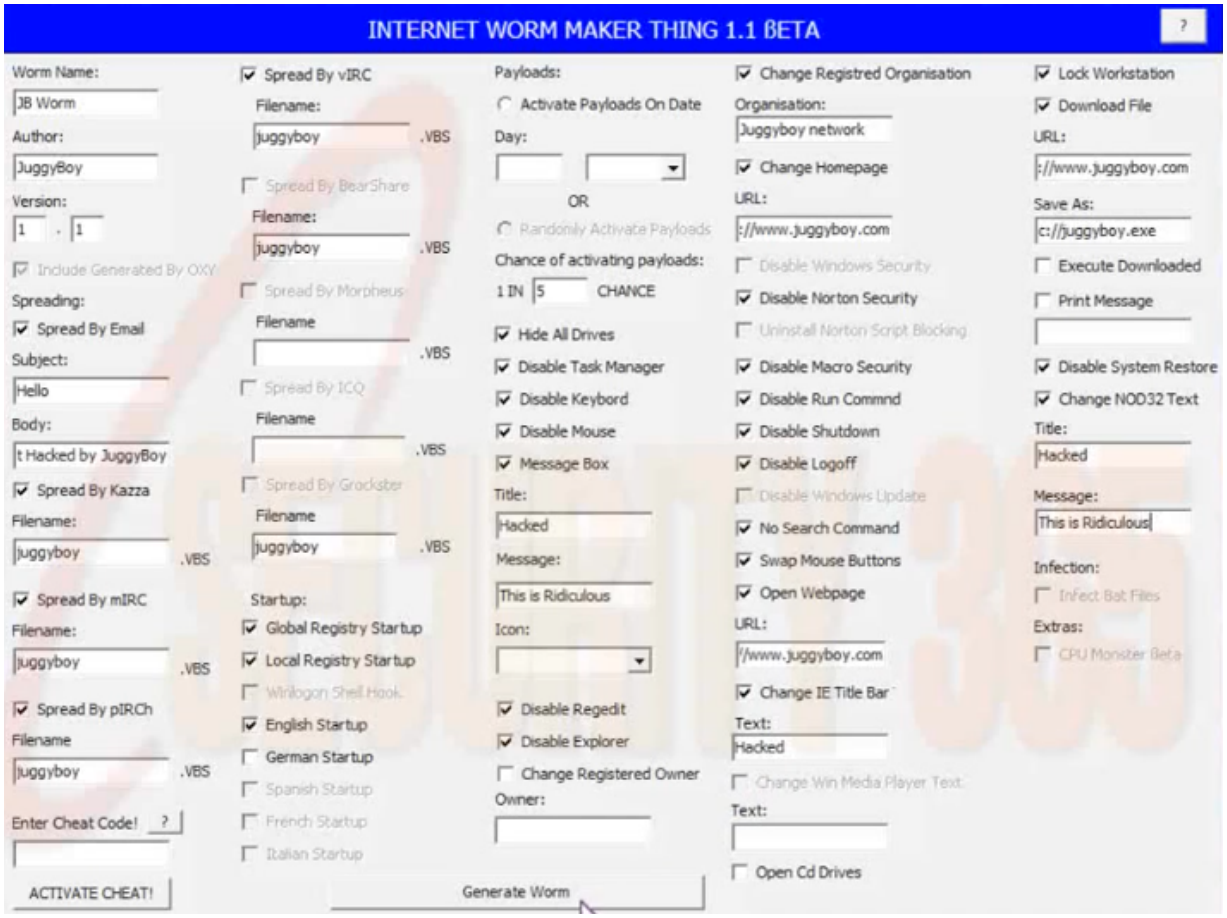
Transport vehicles

- Due to rapidly compromising a large number of systems, they are ideal for spreading many malicious payloads

Zero-day exploit

- A worm can exploit unknown vulnerability that is only discovered after the worm is launched

Internet worm maker thing

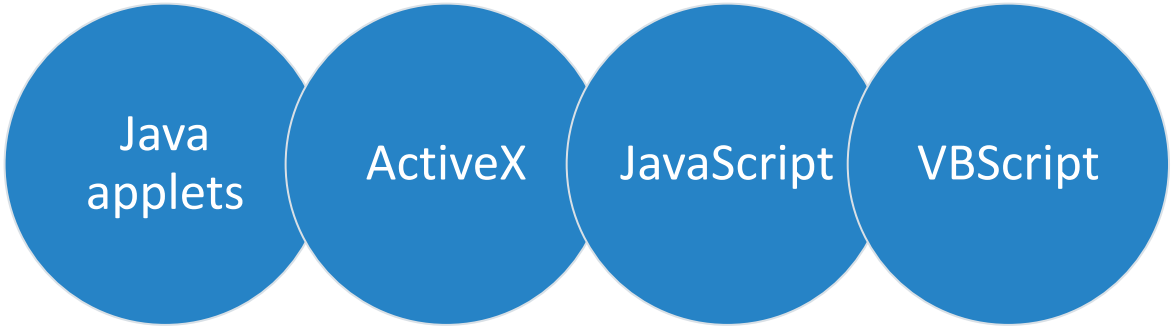


Mobile code

- Refers to programs that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics
- Transmitted from a remote system to a local system and then executed on the local system without the user's explicit instruction
- Often acts as a mechanism for a virus, worm, or Trojan horse to be transmitted to the user's workstation

Mobile code

- Popular vehicles for mobile code include



- Malicious ways of using mobile code on local systems
  - Cross-site scripting
  - Interactive and dynamic Web sites
  - E-mail attachments
  - Downloads from untrusted sites or of untrusted software

Drive-by downloads

- Exploits browser vulnerabilities so that when the user views a Web page controlled by the attacker, it contains code that exploits the browser bug to download and install malware on the system without the user's knowledge or consent
- Does not actively propagate as a worm does, but rather waits for unsuspecting users to visit the malicious Web page in order to spread to their systems

Spam

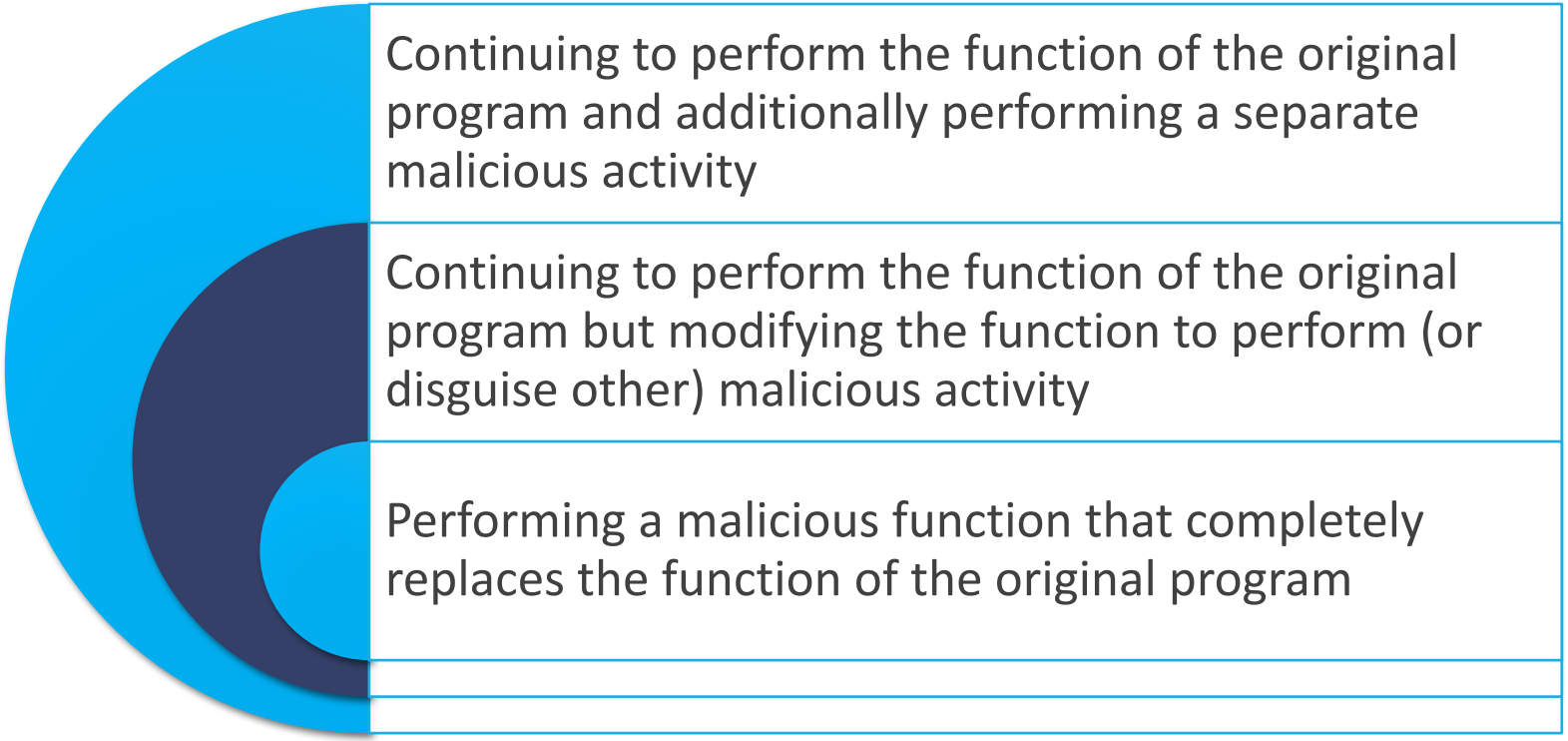
- Significant costs on the network infrastructure for relaying traffic and on users for filtering their legitimate e-mails
  - Toady, most spam is sent by botnets
  - It is a significant carrier of malware
  - It can also be used in a phishing attack
- In many cases it requires the user's active choice in order for the compromise to occur
  - By viewing the e-mail and any attached document
  - By permitting the installation of some program

Trojan horses

- Is a useful, or apparently useful, program or utility containing hidden code that, when invoked, performs some unwanted or harmful function
- Can be used to accomplish functions indirectly that the attacker could not accomplish directly

Trojan horses

- Fit into one of three models:



Συνήθεις πόρτες trojans

Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP
20	Senna Spy	1600	Shivka-Burka
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender
22	Shaft	1981	Shockrave
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow
31	Hackers Paradise	2023	Ripper
80	Executor	2115	Bugs
421	TCP Wrappers trojan	2140	The Invasor
456	Hackers Paradise	2155	Illusion Mailer, Nirvana
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise
666	Satanz Backdoor	3150	The Invasor
1001	Silencer, WebEx	4092	WinCrash
1011	Doly Trojan	4567	File Nail 1
1095-98	RAT	4590	ICQTrojan
1170	Psyber Stream Server, Voice	5000	Bubbel
1234	Ultors Trojan	5001	Sockets de Troie
1243	SubSeven 1.0 – 1.8	5321	Firehotcker
1245	VooDoo Doll	5400-02	Blade Runner

Συνήθεις πόρτες trojans

Port	Trojan	Port	Trojan
5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
6670-71	DeepThroat	22222	Prosiak
6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
7000	Remote Grab	26274	Delta
7300-08	NetMonitor	30100-02	NetSphere 1.27a
7789	ICKiller	31337-38	Back Orifice, DeepBO
8787	BackOfrice 2000	31339	NetSpy DK
9872-9875	Portal of Doom	31666	BOWhack
9989	iNi-Killer	33333	Prosiak
10607	Coma 1.0.9	34324	BigGluck, TN
11000	Senna Spy	40412	The Spy
11223	Progenic trojan	40421-26	Masters Paradise
		47262	Delta
12223	Hack´99 KeyLogger	50505	Sockets de Troie
12345-46	GabanBus, NetBus	50766	Fore
12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
16969	Priority	54321	SchoolBus .69-1.11
20001	Millennium	61466	Telecommando
20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

Ανίχνευση Trojan μέσω...

- suspicious OPEN PORTS
- suspicious RUNNING PROCESSES
- suspicious REGISTRY ENTRIES
- suspicious DEVICE DRIVERS installed on the computer
- suspicious WINDOWS SERVICES
- suspicious STARTUP PROGRAMS
- suspicious FILES and FOLDERS
- suspicious NETWORK ACTIVITIES
- suspicious modification to OPERATING SYSTEM FILES
- dedicated Trojan SCANNER

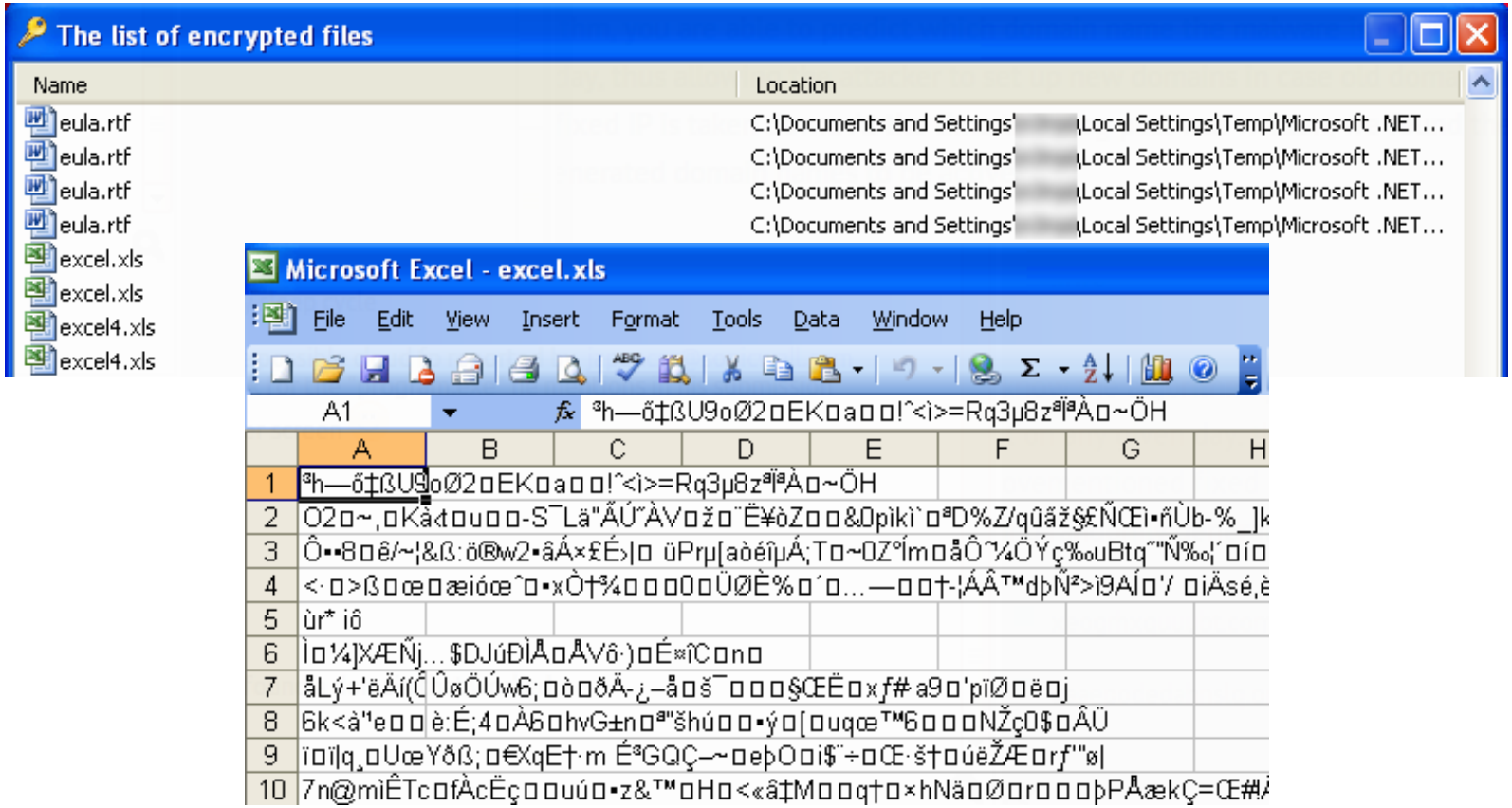
Payload: system corruption

- Once malware is active on the target system, the next concern is what actions it will take on this system
- Examples include
  - Data destruction when certain trigger conditions were met
  - Display unwanted messages or content when triggered
  - Encrypt the user's data and demand payment in order to access the key needed to recover this information (ransomware)

Ransomware: cryptolocker

Ransomware: cryptolocker

Ransomware: cryptolocker



Payload: system corruption

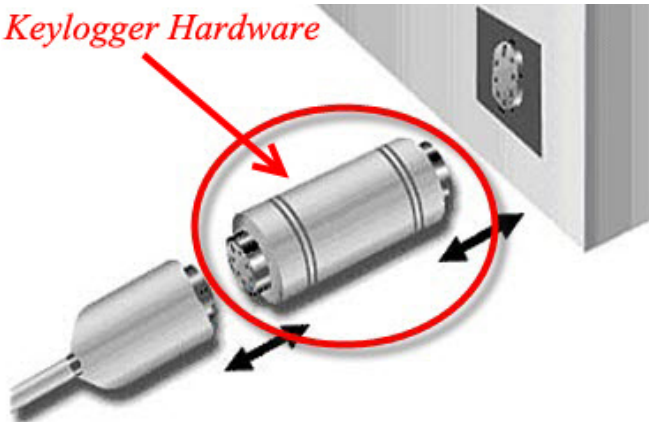
- Once malware is active on the target system, the next concern is what actions it will take on this system
- Examples include
  - Inflict real-world damage on the system
    - Attempt to rewrite the BIOS code used to initially boot the computer
    - Target specific industrial control system software
  - Logic bomb
    - The code embedded in malware that is set to explode when certain conditions are met

Payload: attack agent

- Malware subverts the computational and network resources of the infected system for use by the attacker
  - Bot (robot), zombie, drone
  - Secretly takes over another Internet-attached computer
    - uses that computer to launch or manage attacks that are difficult to trace to the bot's creator
- A *botnet* is a collection of bots often capable of acting in a coordinated manner

Common uses of bots

- Distributed denial-of-service (DDoS) attacks
- Spamming
- Sniffing traffic
- Keylogging
- Spreading new malware



- Installing ads/add-ons and browser helper objects
- Attacking Internet Relay Chat (IRC) networks
- Manipulating online polls/games

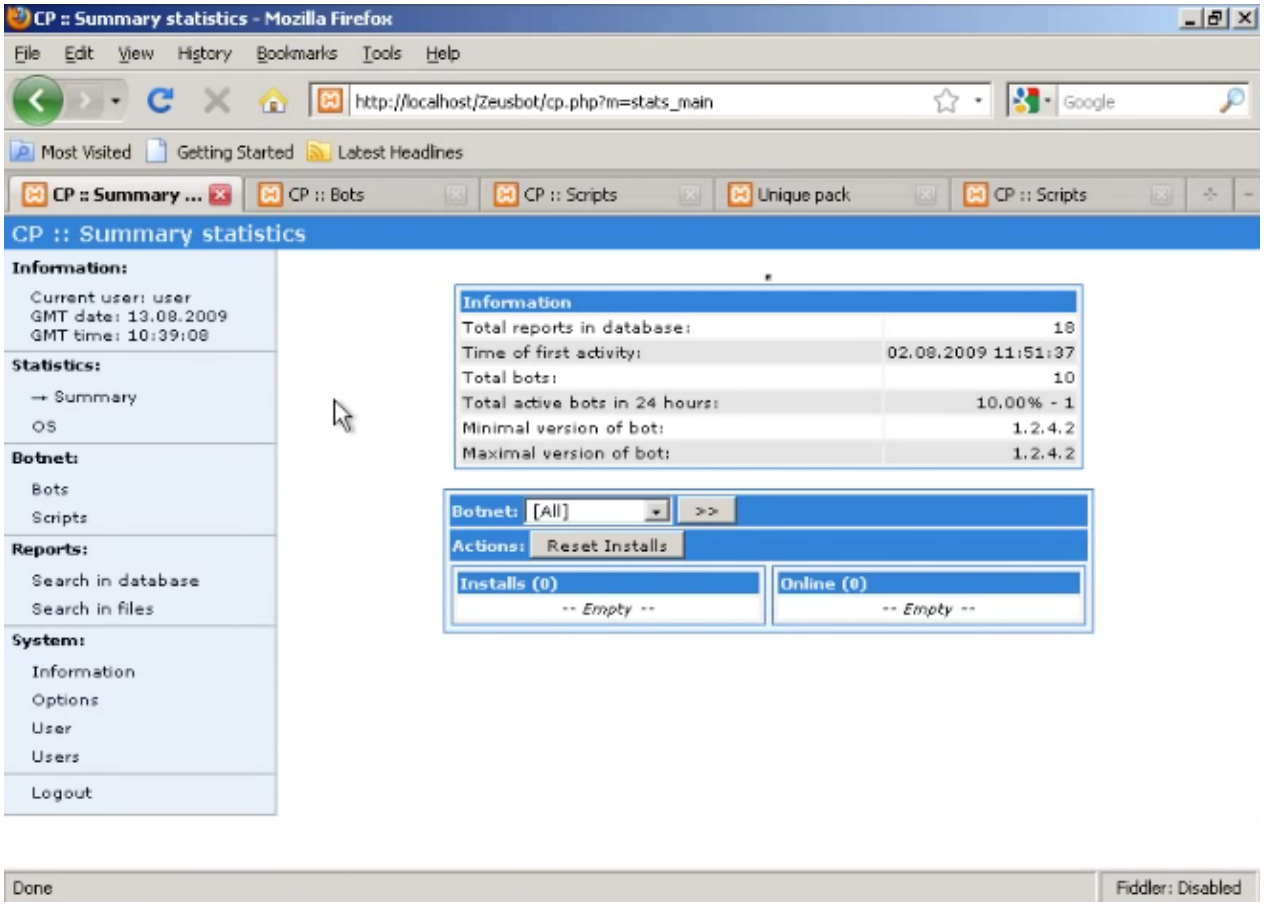
Remote control facility

- Distinguishes a bot from a worm
  - A worm propagates itself and activates itself, whereas a bot is controlled from some central facility
- Typical means of implementing is on an IRC server
- More recent botnets use covert communication channels via protocols such as HTTP

Remote control facility

- Distributed control mechanisms, using peer-to-peer protocols, are also used, to avoid a single point of failure
- Once a communications path is established between a control module and the bots, the control module can activate the bots
  - Can also issue update commands that instruct the bots to download a file from some Internet location and execute it

Zeus toolkit



Payload: information theft

Key logger

- Captures keystrokes on the infected machine to allow an attacker to monitor user login and password credentials

Spyware

- Developed in response to efforts to try and stop key logging
- Subvert the compromised machine to allow monitoring many system's activities which can result in significantly compromising the user's personal information

Phishing

- Exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source

Spear-phishing

- An e-mail claiming to be from a trusted source, however, the recipients are carefully researched by the attacker, and each e-mail is carefully crafted to suit its recipient specifically

Payload: stealthing

- Backdoor (or trapdoor)
  - Is a 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
  - Code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events
  - Usually implemented as a network service listening on some nonstandard port that the attacker can connect to and issue commands through to be run on the compromised system

Payload: stealthing

- Rootkit
  - A set of programs installed on a system to maintain covert access to that system with administrator (or root) privileges, while hiding evidence of its presence to the greatest extent possible
  - Alters the host's standard functionality in a malicious and stealthy way
  - An attacker has complete control of the system and can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand
  - Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer

Rootkits

- Can be classified using the following characteristics:

Persistent	• Activates each time the system boots
Memory based	• Has no persistent code and therefore cannot survive a reboot
User mode	• Intercepts calls to application program interfaces (APIs) and modifies returned results
Kernel mode	• Can intercept calls to native APIs in kernel mode
VM based	• Installs a lightweight virtual machine monitor and then runs the operating system in a virtual machine above it
External mode	• Malware is located outside normal operation mode of the targeted system, e.g. BIOS, where it can directly access h/w

Countermeasures

- Elements of prevention

- One of the first countermeasures that should be employed is to ensure all systems are as current as possible
  - all patches must have been applied
  - in order to reduce the number of vulnerabilities that might be exploited on the system

Countermeasures

- Elements of prevention

- The next is to set appropriate access controls on the applications and data stored on the system,
  - to reduce the number of files that any user can access
  - to reduce potentially infected files, as a result of executing some malware code

Countermeasures

- Elements of prevention

- The third common propagation mechanism is to use appropriate user awareness and training
  - Avoid users being targeted by a social engineering attack

Social engineering attack

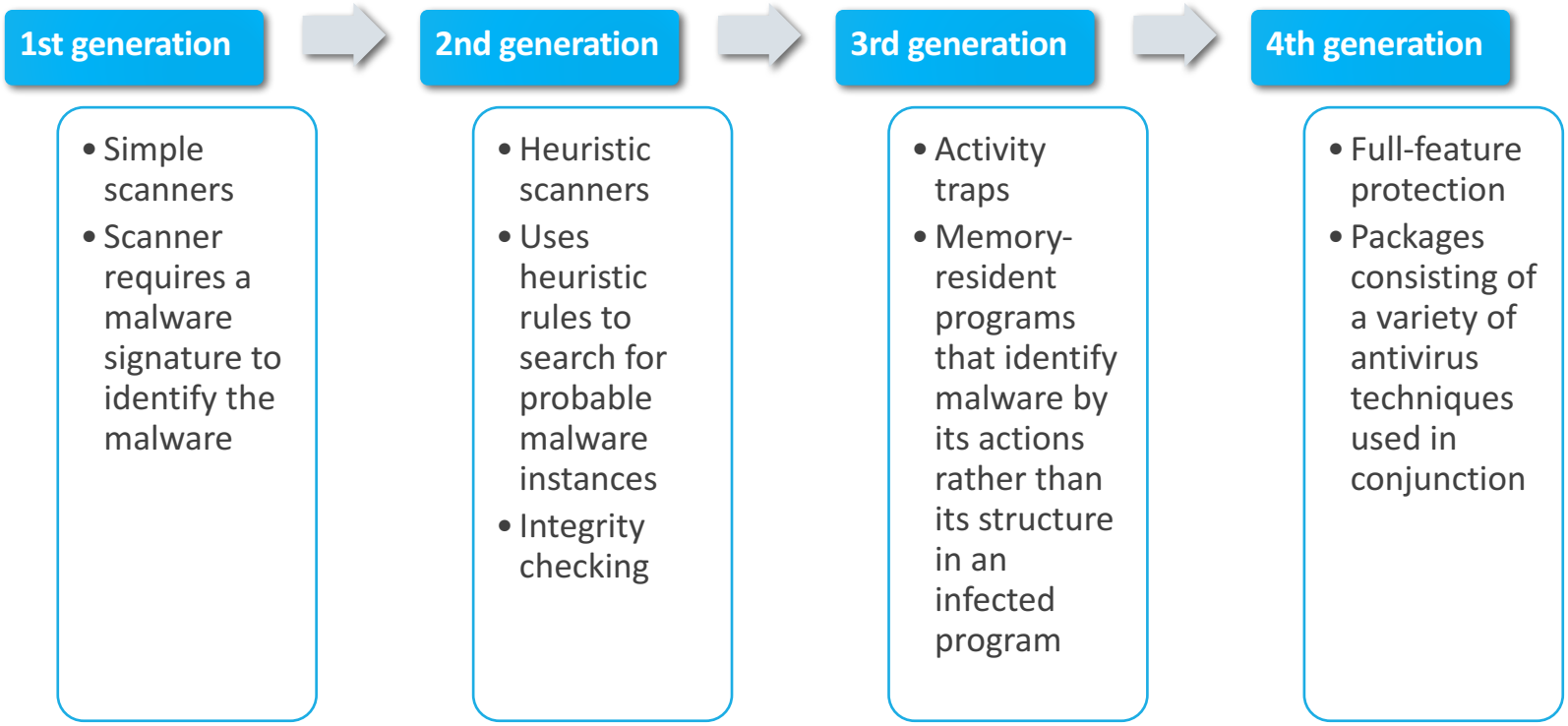
Malware countermeasures

- Technical mechanisms can be used to support the threat mitigation options
  - Detection
  - Identification
  - Removal
- if prevention fails

- Requirements for effective malware countermeasures
  - Generality
  - Timeliness
  - Resiliency
  - Minimal denial-of-service costs
  - Transparency
  - Global and local coverage

Host-based scanners

- Four generations of antivirus software



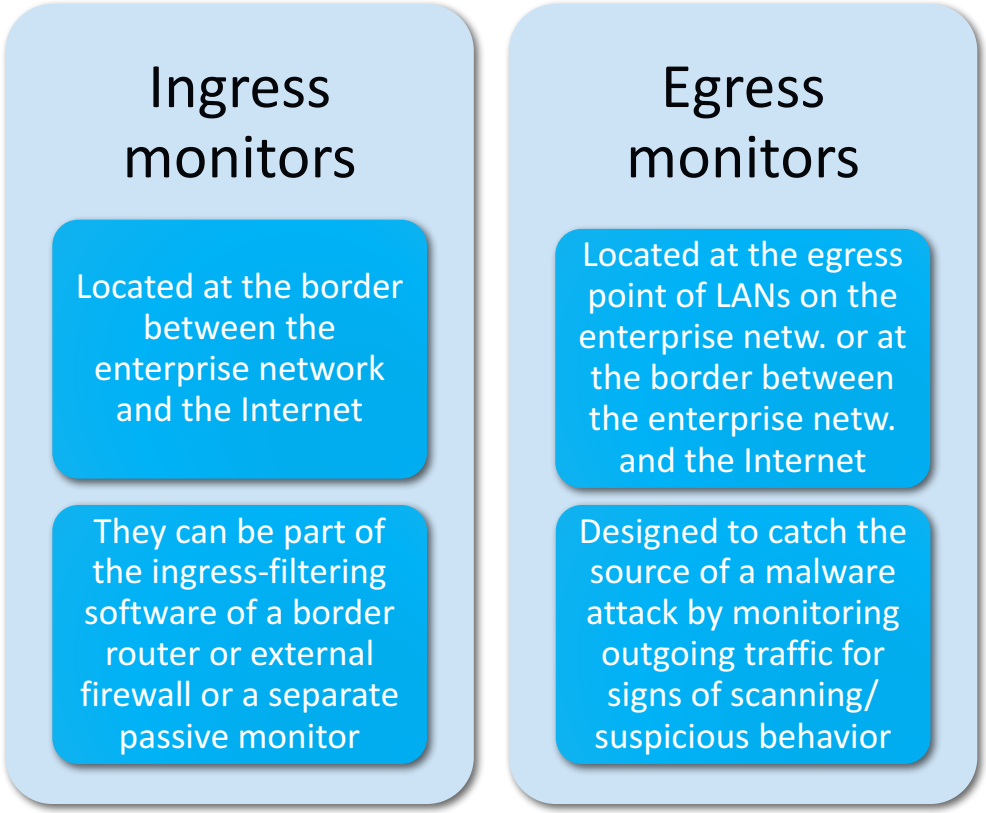
Host-based behavior blocking

- Integrates with the OS of a host PC and monitors program behavior in real time for malicious actions
  - The software then blocks potentially malicious actions before they have a chance to affect the system
- Can block suspicious software in real time
  - It has an advantage over antivirus detection techniques such as fingerprinting or heuristics
- Limitations
  - As the malicious code must run on the target machine before it is identified, it can cause harm before it has been detected/blocked

Perimeter scanning approaches

- Antivirus s/w is used on a firewall and IDS
  - Typically included in e-mail and Web proxy services running on these systems
  - May also be included in the traffic analysis component of an IDS

- Types of monitoring software



Perimeter worm c/measures

Class A: Signature-based worm scan filtering

- This type of approach generates a worm signature, which is then used to prevent worm scans from entering/leaving a network/host

Class B: Filter-based worm containment

- This approach is similar to class A but focuses on worm content rather than a scan signature

Class C: Payload-classification-based worm containment

- These network-based techniques examine packets to see if they contain a worm

Perimeter worm c/measures

Class D: Threshold random walk (TRW) scan detection

- Exploits randomness in picking designations to connect to as a way of detecting if a scanner is in operation

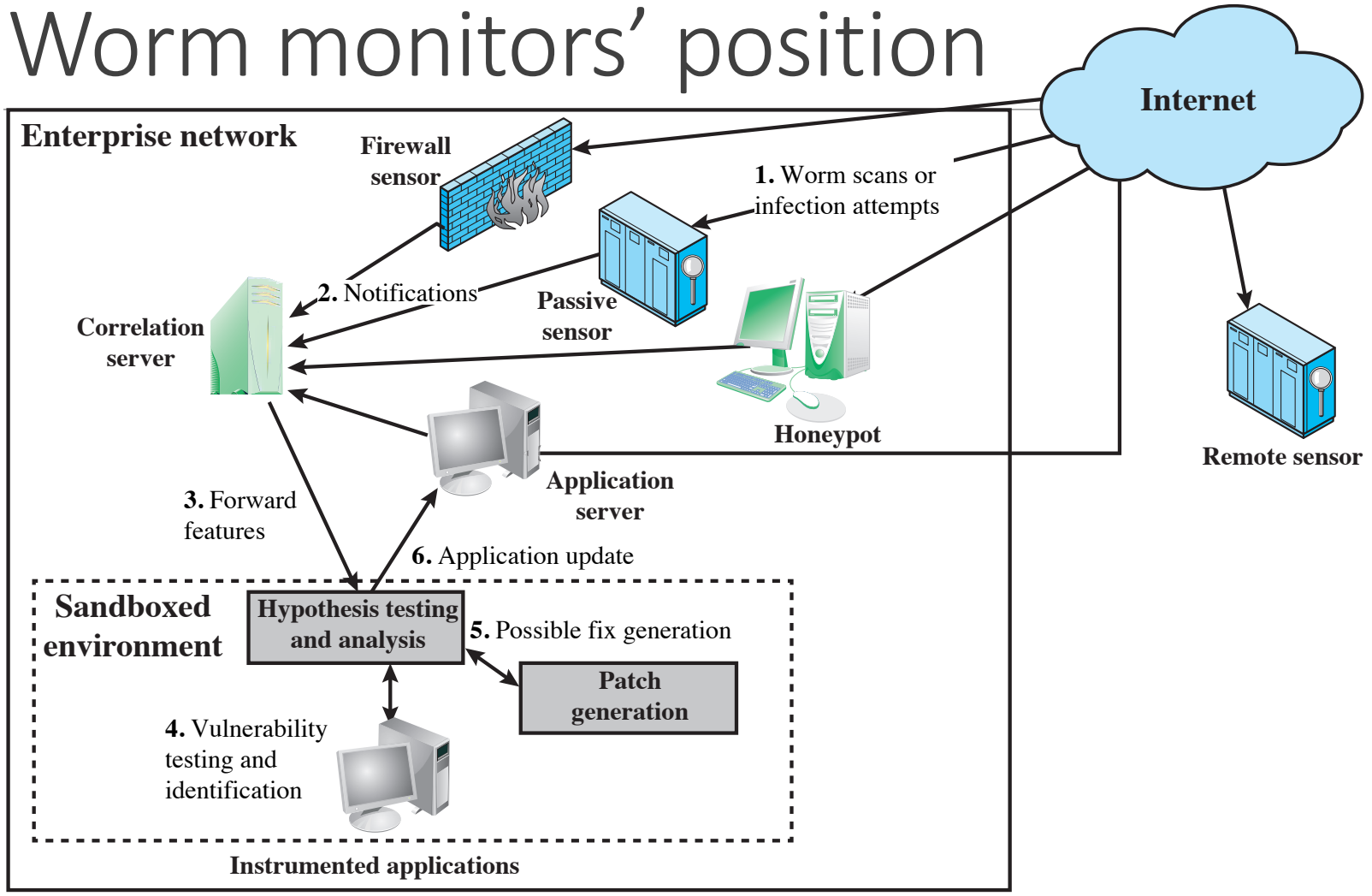
Class E: Rate limiting

- This class limits the rate of scan-like traffic from an infected host

Class F: Rate halting

- This approach immediately blocks outgoing traffic when a threshold is exceeded either in outgoing connection rate or in diversity of connection attempts

Worm monitors' position



Εργαλεία antivirus


Avast


Bitdefender

Comodo

ESET


F-Secure

Kaspersky


McAfee


Norton


Panda


Sophos


Titanium


ZoneAlarm

Προτεινόμενη βιβλιογραφία

- W. Stallings
  Cryptography and Network Security: Principles & Practice
  7th Ed., Prentice Hall, 2017
- W. Stallings and L. Brown
  Computer Security: Principles & Practice
  3rd Ed., Prentice Hall, 2015
- M. Bishop
  Computer Security: Art and Science
  Addison Wesley, 2003