

# Introduction to Computer Security Lecture Slides

© 2024 by [Mihai Chiroiu](#) & [Florin Stancu](#)

is licensed under [Attribution-NonCommercial-ShareAlike 4.0  
International](#)

# Malicious Software

# Objectives

- Definition & classification
- Malware internals
- Malware detection & analysis
- Anti-malware & defense



# Malware

- “Little monsters eating your PC’s resources”
- Software intentionally designed to cause damage to systems / information.
- Buggy software? NOT really malware :(
  - CRWD: “hold my beer”
- Potentially unwanted applications (grey zone):
  - Adware & spyware
  - potentially unwanted software: Windows Recall



# Malware attributes

- Infection / propagation mechanism
- Purpose / functionality
  - Affected properties: confidentiality / integrity / availability / non-repudiation?
- Stealth & evasion ability
- Persistence
- Command-ability / automatic triggers
- Polymorphism (self-modifying code)

# Classification

- By primary distribution method:
  - Viruses
  - Worms
  - Trojan Horses
  - Backdoors
- By function: rootkit, adware, RATs, ransomware, miners etc.



# Virus

- Requires explicit execution / open by user
- Infects & hides inside user's files
  - Executable code modification / injection
  - File format vectors (macros / scripting / local buffer overflows etc.)
- Spreading media: email attachments, removable drives (e.g., floppy / USB drives), network file sharing etc.

CFF Explorer VIII - [shipment airway bill\_PDF.exe]

File Settings ?

shipment airway bill\_PDF.exe

Member	Offset	Size	Value	Meaning
AddressOfEntryPoint	000000A8	Dword	000B06B6	.text
BaseOfCode	000000AC	Dword	00002000	
BaseOfData	000000B0	Dword	000B2000	
ImageBase	000000B4	Dword	00400000	
SectionAlignment	000000B8	Dword	00002000	
FileAlignment	000000BC	Dword	00000200	
MajorOperatingSystemVers...	000000C0	Word	0004	
MinorOperatingSystemVers...	000000C2	Word	0000	
MajorImageVersion	000000C4	Word	0000	
MinorImageVersion	000000C6	Word	0000	
MajorSubsystemVersion	000000C8	Word	0004	
MinorSubsystemVersion	000000CA	Word	0000	
Win32VersionValue	000000CC	Dword	00000000	
SizeOfImage	000000D0	Dword	000B6000	
SizeOfHeaders	000000D4	Dword	00000200	
Checksum	000000D8	Dword	00000000	
Subsystem	000000DC	Word	0002	Windows GUI
DllCharacteristics	000000DE	Word	8540	Click here
SizeOfStackReserve	000000E0	Dword	00100000	
SizeOfStackCommit	000000E4	Dword	00001000	
SizeOfHeapReserve	000000E8	Dword	00100000	

# Virus Pseudocode

```
infected program entrypoint:  
    start_spreading_thread()  
    call original program entrypoint()
```

```
resident thread:  
    for (file in scan_disks()):  
        if !check_infection(file):  
            infect(file)
```



# Worm

- Automatically spreads remotely via network / application vulnerabilities (mainly, Remote Code Execution)
- Distributed scanning for vulnerable devices:
  - early hit lists to bootstrap infection
  - local/global IPv4 address generation
  - address books for email spreading



# Early popular viruses

- Creeper / Reaper (1971), PDP-11 fork-bomb
- Boot sector viruses (Floppy period):
  - Brain (1986) – anti-piracy “solution”;
  - Stoned (1987) – fun / hacktivism: “legalize marijuana”!
  - Michelangelo (1991) – destroyed MBR of HDDs, dormant until global effect
  - CIH (1998) – highly destructive, erased BIOS flash chips => hardware unusable!
- Simile (2001) – metamorphic, rebuilds itself [2]
- Windows shortcut viruses

Displacement	Hex codes	ASCII value
0000(0000)	FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20	-0J04↑●Π0
0016(0010)	20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F	Welcome to
0032(0020)	20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20	the Dungeon
0048(0030)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0064(0040)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0080(0050)	20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20	(c) 1986 Basit
0096(0060)	26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74	& Anjad (put) Lt
0112(0070)	64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20	d.
0128(0080)	20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20	BRAIN COMPUTER
0144(0090)	53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49	SERVICES.. 730 NI
0160(00A0)	5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41	ZAM BLOCK ALLAMA
0176(00B0)	20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20	.IQBAL TOWN
0192(00C0)	20 20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52	LAHDR
0208(00D0)	45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E	E-PAKISTAN..PHJN
0224(00E0)	45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 3B	E :430791,443248
0240(00F0)	2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20	,280530.

# Email-spreading worms

- Macro viruses: Concept, Melissa (1999)
  - attachments with macros: “sexxy.jpg” / “naked wife”
- ILOVEYOU (2000) – love letter with .vbs attachment
- Sobig (2003), MyDoom (2004)
  - DDoS trigger -> SCO Group & Microsoft
  - creators never caught, still active today (:
- Storm Worm (2007)
  - “230 dead as storm batters Europe” – spread via clickbaiting
- Koobface (2009 - 2013) – via social networks
- Win32.Antiman.A (2005) :(

# Popular worms (1)

- Morris (1988) – 1st wild worm
  - used sendmail vulnerability
- Code Red (2001) – MS IIS vulnerability
  - defaced websites, minor
- Blaster / Lovesan (2003)
  - DCOM RPC vulnerability stack overflow (:
- SQL Slammer (2003)
  - affected Bank of America ATMs
- Daprosy (2009) – autorun worm

Welcome to <http://www.worm.com> !

Hacked By Chinese!

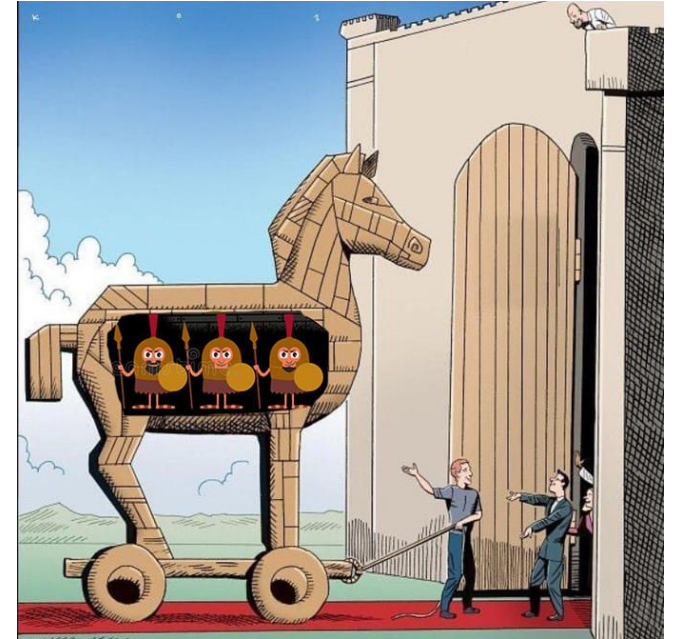
```
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 2C 39 C2 .....9T
00 31 00 00 00 00 00 00 A.....1.....
00 49 20 6A 75 73 74 20 .....I just
73 61 79 20 4C 4F 56 45 want to say LOVE
21 21 00 00 00 00 00 00 YOU SAN!!.....
61 74 65 73 20 77 68 79 .billy gates why
6D 61 6B 65 20 74 68 69 do you make thi
6C 65 20 3F 20 53 74 6F s possible ? Sto
20 6D 6F 6E 65 79 20 61 p making money a
6F 75 72 20 73 6F 66 74 nd fix your soft
00 00 00 00 00 00 00 00 ware!!.....
```

# Popular worms (2)

- Conficker (2008)
  - M\$ / NetBIOS exploits (Win 2000 → 7)
  - downloaded updates from pseudorandom domains
- Stuxnet (2010)
  - Advanced Persistent Threat
  - Mainly attacked Iran's SCADA systems, destroyed nuclear centrifuges
  - *“most complicated and sophisticated malware at the time”*
- Mirai (2016): routers & IoT devices
- Exploit kits: Angler (2015), BlackHole (2010), Nuclear (2016)

# Trojan Horse

- User is tricked into opening it
- Targeted: does not propagate automatically
  - may be hidden inside exe/docs (like viruses)
  - may be installed as late payload by worms!
- Functions: remote access, info stealing (keylogger), botnet zombies, ransomware, backdoor etc.
- *Script kiddies: trojan construction kits!*



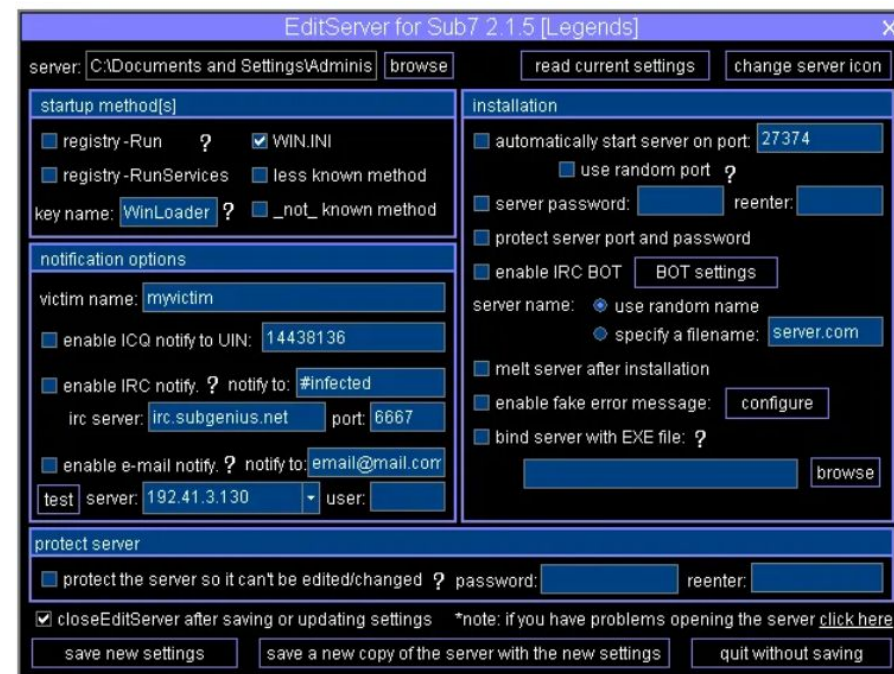
# RATs

- Remote Admin/Access ~~Tool~~ Trojan
  - may have ethical uses (e.g., remote desktop) – if owner consents!
- Usually, installed by social engineering / physical device access
  - E.g., spying on your lover(s) – **please don't!**
- Features:
  - Taking full control of the infected machine
  - Full file system access (download / upload / execution)
  - Online / offline key logging, live webcam / microphone
  - Remote shutdown and reboot, disable user input etc.
- Commercial tools / open source projects for building yourself



# Historical / popular RATs

- Antiques: Back Orifice / Beast / Sub7 [3] / Houdini
- “Grey” market: NjRat, MoSucker, ProRAT, DarkHorse, Senna Spy, Pandora etc.
- Open / leaked sources:
  - <https://github.com/sin5678/gh0st>
  - <https://github.com/hfiref0x/ZeroAccess>
  - <https://github.com/killeven/Poison-Ivy-Reload>
  - <https://github.com/PushpenderIndia/thorse> (Python3 :D)
  - <https://github.com/UpSetst/SilverRAT-FULL-Source-Code>





# Backdoors

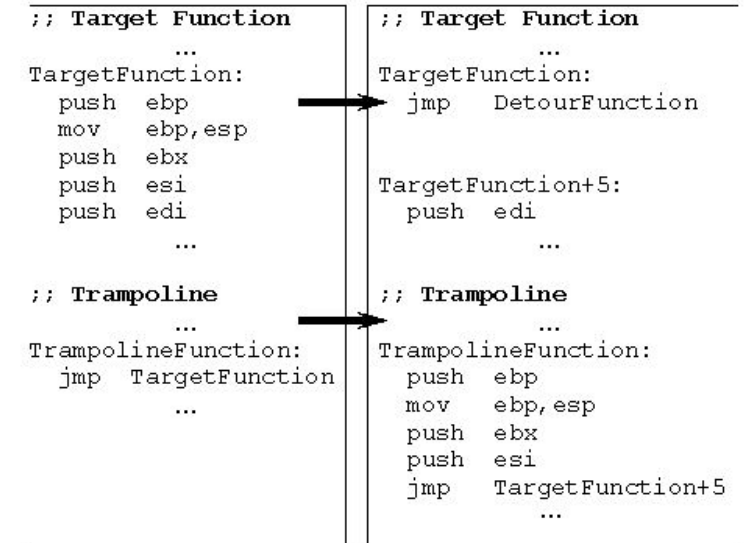
- Highly targeted:
  - Installed at manufacturing / compile time (“supply chain attacks”)
  - Inserted via vulnerabilities in a system
- They just “keep the door open” for future payload execution
- Examples:
  - libXZ compile-time auth. bypass for OpenSSH server
  - NIST Dual EC DRBG crypto RNG by NSA (speculated)
  - Master passwords in Cisco & Juniper routers/firewalls
  - Numerous NPM / Python packages, PC/Android/iOS apps (e.g., VLC) etc.

# Rootkits

- Actively prevent detection, offer privileged (root) access
  - concealment (userspace / kernel / hypervisor / firmware)
  - antivirus software manipulation
  - persistence (survive reboots)
  - stealth network communication / updates
- Usually embeds / combines with a RAT or backdoor
- Benign uses? there are some ;)
- <https://github.com/milabs/awesome-linux-rootkits>

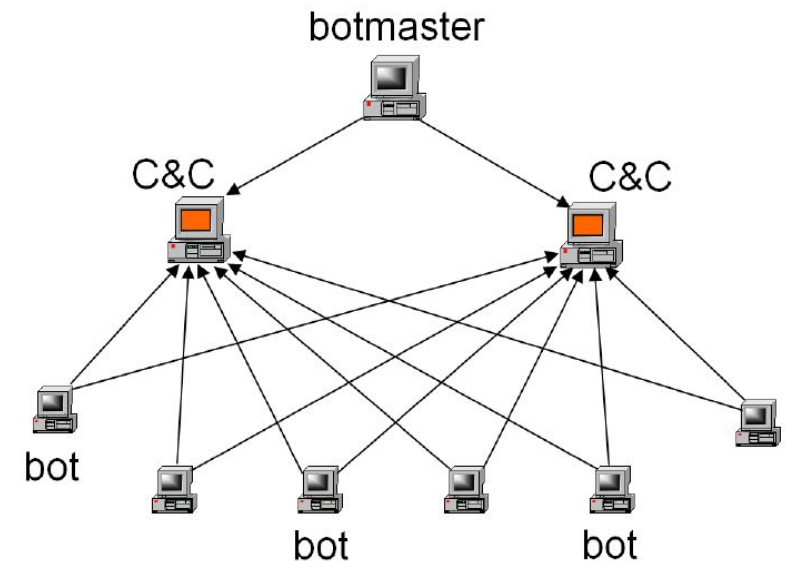
# Execution concealment

- User mode:
  - System file hiding (e.g., inside *C:\Windows\System32*)
  - Library injection (e.g., explorer.exe plugin)
  - Binary patching / detour hooks
- Kernel mode:
  - kernel modules (run with SYSTEM privileges / modprobe)
  - system call table patching
- Firmware-level (SMM rootkits)
- Code obfuscators / packers



# Command & Control / stealth comm.

- Botnet: command & control
  - Centralized -> “easy” to shutdown
    - except for generated DNS
  - Peer-2-peer
- Encryption, D-H, asymmetric keys...
- Stealth communication + data exfiltration:
  - Transport protocols (HTTP, SMTP, SNMP)
  - Auxiliary protocols: DNS, ICMP, ARP
  - Extreme: 1 bit at a time (:



# Ransomware

- Usually as worms, most destructive so far
- Delete / steal / encrypt user's documents
- Advanced techniques (asymmetric ciphers, timed triggers etc.)
- CryptoLocker (2013), WannaCry (2017), Petya
- Ransomware as a Service (e.g., REvil, Hive)



# White-hat time! Malware defense?



- Endpoint protection:
  - Realtime protection (AVs) / malware scanning tools
  - Cloud-based endpoint protection
  - Periodic updates & **backups!**
- Network protection:
  - Firewalling (or the extreme: air gapping)
  - Cloud-based threat intelligence
  - Honeypots
- Malware analysis
  - Reverse engineering tools
  - Sandboxes



# Malware detection

- File/memory integrity checks
- Signature-based scans
  - vs new or self-modifying (polymorphic) malware?
  - advanced patterns (e.g., regular expressions)
- Behavioral heuristics (e.g., opened files, system calls)
- Machine learning (requires training phase + resource-intensive)
- Network traffic / anomaly detection
  - Intrusion Detection / Prevention Systems

# Endpoint security tools

- Historical: Symantec Norton, McAfee,  Kaspersky, ESET Nod32
  - *“Kaspersky deletes itself, installs UltraAV antivirus without warning”*
- Microsoft: buys [RO] GeCAD (2003), Windows Defender (2005)
  - *Actually, Defender was based on prev. acquired GIANT AntiSpyware*
- Softwin (1996) -> Bitdefender (2001)
- Cloud threat intelligence: Crowdstrike, Sophos, Cisco AMP / Fortinet / Palo Alto / Check Point etc.
  - ^ ^ ^ mostly for Windows (& Mac OS X, probably )
- **Open source:** ClamAV => Linux support!
  - Linux rootkit detectors: chkrootkit, rkhunter, clamav, LMD



# Malware datasets & intelligence

- EICAR Anti-Virus Test File – simple test files (not malware)
- Many free malware databases:
  - VirusShare, Malware Bazaar, Canadian Institute of Cybersecurity, SOREL-20M, BODMAS, VirusSign etc.
- Multi-scanning: VirusTotal
- AV companies publish latest threats (responsible disclosure!)
  - for fame & profit
  - also share threat info with each other via partnerships
- Companies crowdsource unknown threats from cloud customers
  - “all for one and one for all”

# Malware analysis

- Quick response -> isolation!
  - Stealth rootkit? Put RAM into freezer :)
- Sandboxing – execute piece inside a virtual machine to study its behavior
  - must make environment undetectable!
  - sometimes: simulate entire network of devices to capture malware before production (honeypots)!
- Reverse engineering tools (+ skillz) [4] [5]
  - IDA Pro / Ghidra / Binary Ninja / gdb & pwndbg/PEDA / x64dbg etc.
  - Sysinternals (MS) / frida / radare2 / ptrace / eBPF

# Bibliography

- [1] <https://people.scs.carleton.ca/~paulv/toolsjewels/TJrev1/ch7-rev1.pdf>
- [2] Win32/Simile  
<https://docs.broadcom.com/doc/striking-similarities-metamorphic-virus-code-03-en>
- [3] <https://medium.com/phrozen/a-malware-retrospective-subseven-d86fed0c88bf>
- [4] <https://www.stationx.net/malware-analysis-tools/>
- [5] <https://github.com/onethawt/reverseengineering-reading-list>