chapter - 7

Malware Threats

Malware

- Trojans
- Backdoors
- Rootkits
- Ransomware
- Adware
- Worms
- Spyware
- Botnets
- Crypters
- Viruses

Distribution (Malware)

Blackhat SEO (rank malware page highly)

Social Engineered clickjacking

Spear phishing (mimick legitimate company)

Malvertising (embed malware — ad networks)

Compromised legitimate websites

Drive by downloads

Spam emails

Components (Malware)

Crypter (protects Malware from detection)

Downloader (download other malware)

Dropper (installs other malware)

Exploit (Malicious code)

Injector (Program injects to vulnerable process)

obfuscator (conceals code from detection)

Packer (Bundle all files)

Payload (Software — controls after exploit)

Malicious Code (actual intention with code)

APT Concepts

Advanced Persistent Threat

- remain undetected for long time.

objective (sensitive info)

Timeliness (time taken to gain access)

Resource (knowledge, tool, skill needed)

Risk Tolerance (undetection for ∞ time)

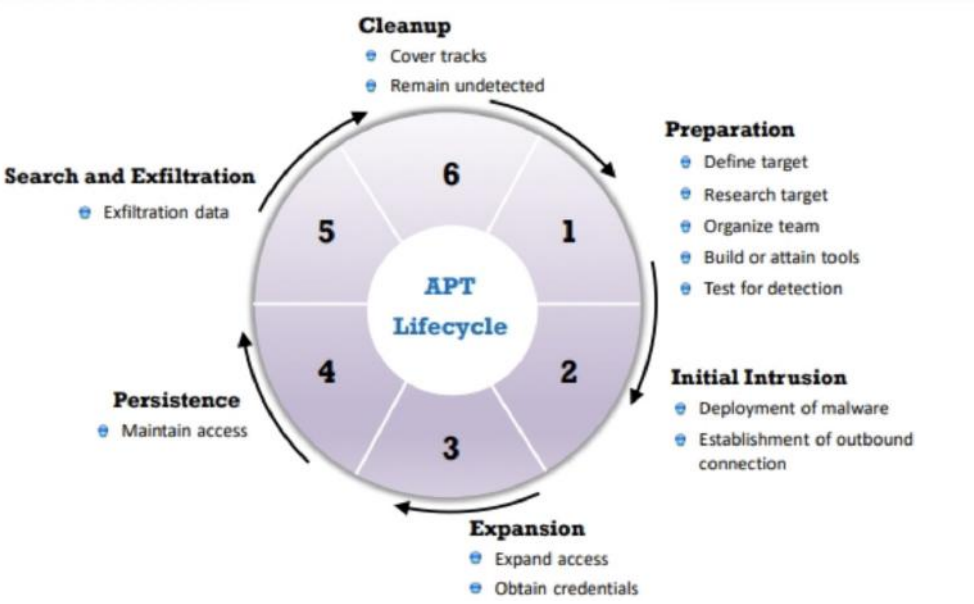
skills of Methods (methods, tools used)

Actions (technical action list)

Attack Origination Point (numerous attempts)

Multiple Points of Entry. (multiple point - maintain)

Lifecycle


Cleanup
Cover tracks
Remain undetected
Preparation
Define target
Research target
Organize team
Build or attain tools
Test for detection
Initial Intrusion
Deployment of malware
Establishment of outbound connection
Expansion
Expand access
Obtain credentials
Persistence
Maintain access
Search and Exfiltration
Exfiltration data
6
1
2
3
4
5
APT
Lifecycle

Trojan

- delete / replace OS files
- disable firewall, antivirus
- create backdoors
- encrypt data & lockout
- create DoS attacks

Port	Trojan	Port	Trojan	Port	Trojan
20/22/80/443	Emotet	1807	SpySender	8080	Zeus, Shamoon
21	Blade Runner, DarkFTP	1863	XtremeRAT	8787 / 54321	BackOfrice 2000
22	SSH RAT, Linux Rabbit	2140/3150/6670-71	Deep Throat	10048	Delf
23	EliteWrap	5000	SpyGate RAT, Punisher RAT	10100	Gift
68	Mspy	5400-02	Blade Runner	11000	Senna Spy
80	Ismdoor, Poison Ivy, POWERSTATS	6666	KilerRat, Houdini RAT	11223	Progenic Trojan
443	Cardinal RAT, ghOst RAT, TrickBot	6667/12349	Bionet, Magic Hound	12223	Hack'99 KeyLogger
445	WannaCry, Petya	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
1177	njRAT	7000	Remote Grab	31337-38	Back Orifice/ Back Orifice 1.20/ Deep BO
1604	DarkComet RAT, Pandora RAT	7789	ICKiller	65000	Devil

Types:

- RAT (complete control over victim) nJRAT
- Backdoor (bypass standard authentication) Poison Ivy

- Botnet (infect large computers) Neeuws
- Rootkit (targets rootlos of System) EquationDrug
- E-banking (TAN, Form, Covert credentials) Dreambot
- Point of Sale (credit/debit, CVV) GlitchPOS
- Defacement
- Service Protocol (UNC, HTTP, SHTTPD, ICMP
- Mobile
- IoT
- Security Software
- Destructive
- DDoS
- Command shell

Creating Trojan

Trojan Horse Construction kits

- construct Trojan of their choice.
- eg: DarkHorse Trojan Virus Maker

Virus Types

System/boot

- Master boot record - DOS boot system

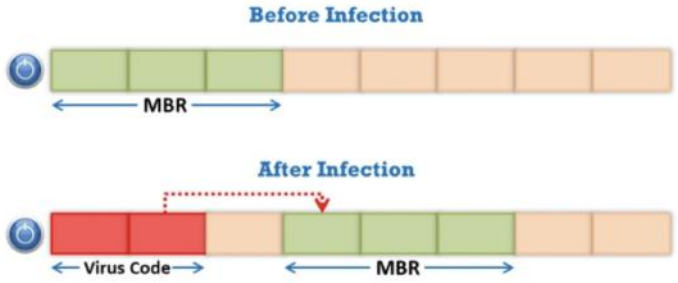


Figure 7.36: Working of system and boot sector virus

File virus

- insert code into original file.

Multipartite (hybrid)

- file infector + boot record infector.

Macro

- automatically perform actions

- less harmful

cluster

- save virus to hard drive
- overwrite pointer entry
- controls directory structure in disk

stealth / tunnel

- hide from antivirus

Encryption

- cryptolocker virus
- encrypted copy of virus, decryption module
- employ XOR on each byte with randomized key.

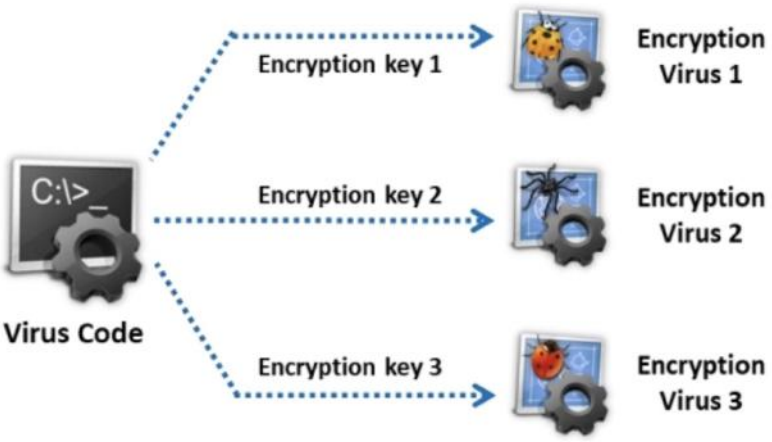


Figure 7.40: Working of encryption virus

Sparse Infector

- Minimise probability of discovery
- wake up on 15th of month date

Polymorphic

- encrypted copy of polymorphic code
- components: encrypted code, decryptor routine, mutation engine.

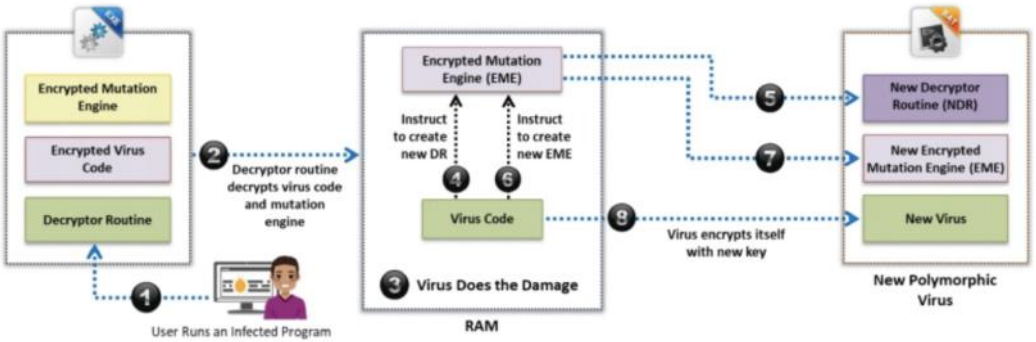


Figure 7.42: Working of polymorphic virus

Metamorphic

- rewrite themselves each time.
- avoid pattern recognition.
- techniques: disassembler, expander, Permutator, assembler.
- insert dead code, reshape expression, reorder instruction, modify variable, encrypte code, modify structure.

Overwrite file / cavity

- space fillers
- overwrite host files with nulls without increasing length

Companion/ camouflage

- same filename as target file
- runs COM or EXE file.

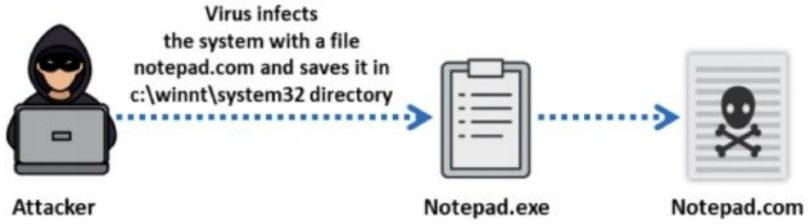


Figure 7.45: Working of companion virus/ camouflage virus

Shell virus

- all boot program virus are shell virus
- forms shell around host program code.

File extension

- changes the extension

FAT

- attacks File Allocation table

Logic bomb

- launch at specific time / date

Web Scripting

- Vulnerability - breaches web security.
- injects client side scripting.
- persistent or non persistent.

Armored

- confuse / trick to prevent from detection.
- Technique:

- Anti-disassembly (incorrect listing)
- Anti-debugging (Program not running)
- Anti-heuristics (prevent heuristic analysis)
- Anti-emulation (avoid dynamic analysis)
- Anti-goat

Add on

- append code to host code
- No alter / No relocation of code
-

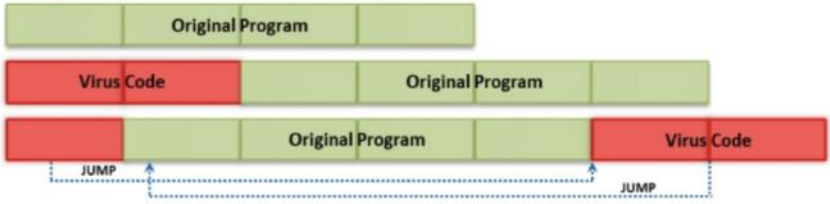


Figure 7.48: Working of add-on virus

Intrusive

- overwrite code completely / partly.

Direct action / Transient

- operates only for short duration
- life (virus file) = life (target file)
- transfer control to where it resides in memory.

Terminate and Stay Resident

- Permanent in machine's memory
- control over other process.

Malware

divergent – type of fileless malware
- depends mostly on registry
- employs key in registry to maintain Poristence

sheep dip computer
- analysis of suspect files, messages for malware;
- connects to network only under strictly controlled conditions

Antivirus Sensor System – detects, analyzes malicious code threats

Types of Malware Analysis

Static - code analysis

Dynamic - behavorial analysis

Static Analysis

- File Fingerprinting (compute hash value)
- local vs online scan
  - binary code scan locally.
  - Virustotal : scan engine.
- Perform string Search (embedded strings)
- identify packing / obfuscation (PEid)

reverse engineering

- Find portable executable (PE) information
  - use metadata of PE
- identify file dependencies.
  - kernel32.dll (import / export)
  - dependency walker : Tool.
  - check dynamic linked list
- Malware Disassembly.
  - dissassemble binary code to analyse
  - IDA : Tool to reverse code → assembly

Dynamic Analysis

- System Baselining
- Host Integrity Monitoring

} stages

System Baseline

- takes snapshot of system before start
- identify significant changes

Host Integrity Monitoring

- takes snapshot before & after
- detect changes made to entities.

Dynamic Analysis

- Port Monitoring
  - Netstat, TCPView
  - Scan suspicious ports → unknown
- Process Monitoring
  - Process Monitor tool
  - real time process / thread activity
  - identify camouflage apps
- Register Monitoring
  - check register configuration.
  - Jv16 PowerTools.
  - find registry errors & junk.

- Windows Services Monitoring
  - remote control, malicious instruction
  - rename process to avoid detection
  - Windows Service Manager (SrvMan) to trace malicious services.

- Startup programs Monitoring
  - Perform malicious activity @ startup menu when system starts.
  - c:\windows\System32\drivers.
  - boot.ini or bootmgr entries.
  - services.msc

- Event logs Monitoring
  - splunk → suspicious logs, events
  - automatically collect logs from SIEM tool.
- Installation Monitoring
  - Mirekusoft Install Monitor : Tool.
  - data left after Install / Uninstall.
- Files, Folders Monitoring
  - check integrity for files, Folders.
- Device drivers Monitoring
  - downloaded from untrusted Source
  - DriverView : Tool.

- msinfo32 (system drivers)

- Network Traffic Monitoring
  - packet sniffer to monitor traffic
  - Solarwind Netflow Traffic Analyzer

- DNS Monitoring / Resolution
  - DNS changer → change Server setting
  - Tool : DNSQuery Sniffer

- API calls Monitoring
  - analyze API → reveal suspicious apps
  - API Monitor : Tool

Emotet (Banking Trojan)

- Trojan + polymorphic Malware + downloader & dropper.

1. Initial Infection
2. Malicious .doc file download
3. relocation & creation of 1st culturesource.exe
4. Creation of second culturesource.exe
5. encryption
6. Deploy Timer function
7. Communication with C&C Server.
8. System Compromise
9. Network propogation (NetPass, Outlook, Mail, Webbrowser, Credential)