Module 9

Malwares

Ansh Bhawnani

Malware Concepts

Module 9

1. Introduction to Malwares

Module 9

Introduction to Malwares

- Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud.
- **Examples of Malware**:
  - Trojan Horse
  - Backdoor
  - Rootkit
  - Ransomware
  - Adware
  - Virus
  - Worms
  - Spyware
  - Botnet
  - Crypter

Introduction to Malwares

Different Ways a Malware can Get into a System

- Instant Messenger applications, or IRC
- Removable devices
- Attachments
- Legitimate "shrink-wrapped" software packaged by a disgruntled employee
- Browser and email software bugs
- NetBIOS (FileSharing)
- Fake programs
- Untrusted sites and freeware software
- Downloading files, games, and screensavers from Internet sites

Introduction to Malwares

Common Techniques Attackers Use to Distribute Malware on the Web

- **Blackhat Search Engine Optimization (SEO)**: Ranking malware pages highly in search results.
- **Malvertising**: Embedding malware in ad-networks
- **Compromised Legitimate Websites**: Hosting embedded malware that spreads to unsuspecting visitors.
- **Social Engineered Click-jacking**: Tricking users into clicking on innocent-looking webpages.
- **Spearphishing Sites**: Mimicking legitimate institutions
- **Drive-by Downloads**: Exploiting flaws in browser software

Virus Concepts

Module 9

1. Introduction to Viruses

Module 9

Introduction to Viruses

- A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program., computer boot sector or document.
- Viruses are generally transmitted through file downloads, infected disk/flash drives and as email attachments.
- **Virus Characteristics**:
  - Infects other program
  - Transforms itself
  - Encrypts itself
  - Alters data
  - Corrupts files and programs
  - Propagates

2. Stages of a Virus Lifetime

Module 9

Stages of a Virus Lifetime

- **Design**: Developing virus code using programming languages or construction kits.
- **Replication**: Virus replicates for a period of time within the target system and then spreads itself.
- **Launch**: It gets activated with the user performing certain actions such as running an infected program.
- **Detection**: A virus is identified as threat infecting target systems.
- **Incorporation**: Antivirus software developers assimilate defenses against the virus.
- **Elimination**: Users install antivirus updates and eliminate the virus threats.

3. Phases of a Virus

Module 9

Phases of a Virus

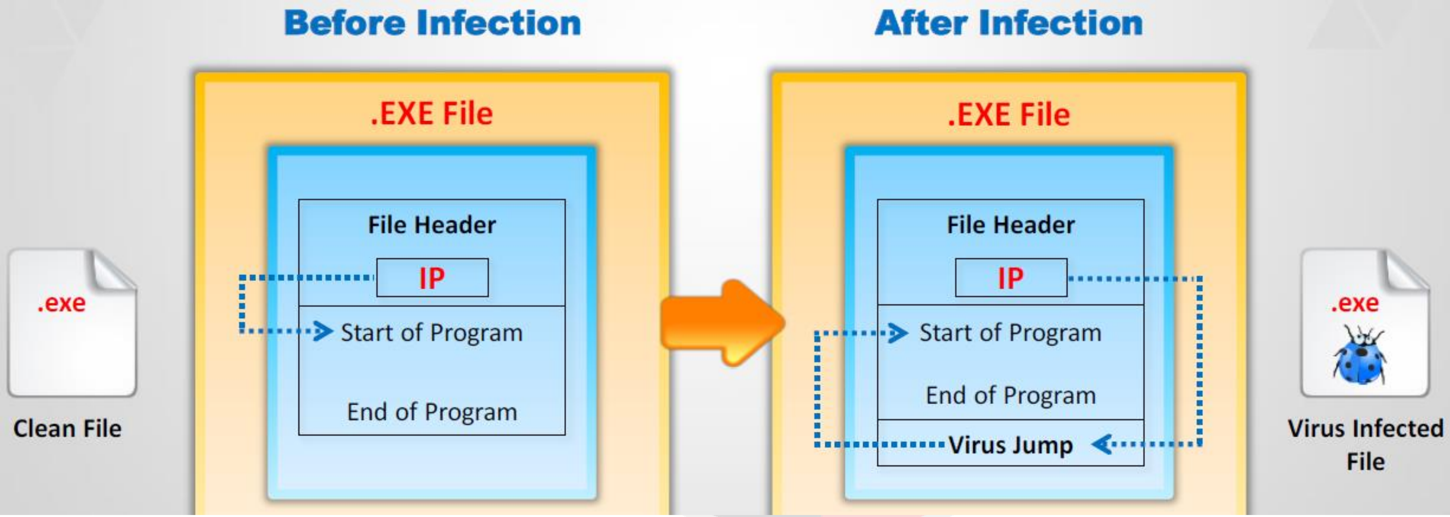
- **Dormant phase:** The virus program is into the system but idle, eventually be activated by the "trigger" which states which event will execute the virus.
- **Propagation phase:** The virus starts propagating, that is multiplying and replicating itself. The virus places a copy of itself into other programs or into certain system areas on the disk.
- **Triggering phase:** A dormant virus moves into this phase when it is activated, and will now perform the function for which it was intended.
- **Execution phase:** This is the actual work of the virus, where the "payload" will be released. It can be destructive such as deleting files on disk, crashing the system, or corrupting files or relatively harmless such as popping up humorous or political messages on screen.

4. Working of a Virus

Module 9

Working of a Virus

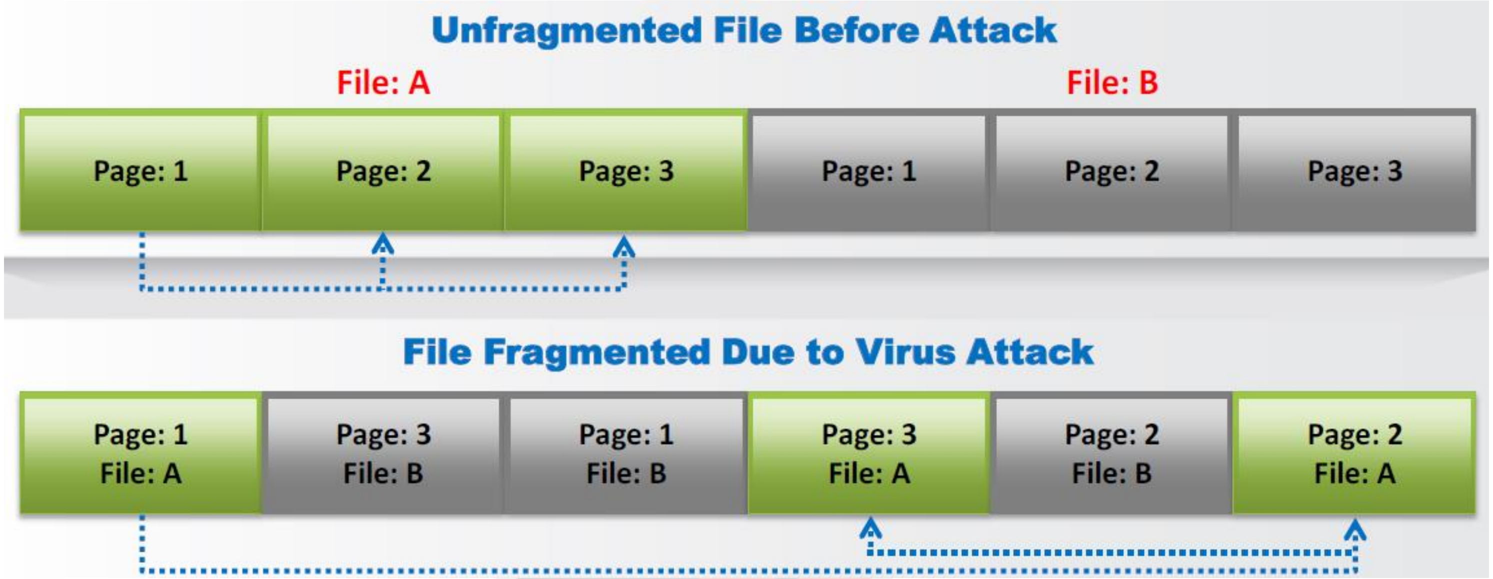
- **Infection Phase**: In the infection phase, the virus replicates itself and attaches to an .exe file in the system.



Working of a Virus

- **Attack Phase**:
  - Viruses are programmed with trigger events to activate and corrupt systems.
  - Some viruses infect each time they are run and others infect only when a certain predefined condition is met such as user's specific task, a day, time, or a particular event.

Working of a Virus



Working of a Virus

Why Do People Create Computer Viruses

- Inflict damage to competitors
- Financial benefits
- Research projects
- Play prank
- Vandalism
- Cyber terrorism
- Distribute political messages

5. Indications of a Virus attack

Module 9

Indications of a Virus attack

- **Abnormal Activities**: If the system acts in an unprecedented manner, you can suspect a virus attack.
  - Processes take more resources and time
  - Computer beeps with no display
  - Drive label changes
  - Unable to load Operating system
  - Anti-virus alerts

Indications of a Virus attack

- Browser window "freezes"
- Hard drive is accessed often
- Files and folders are missing
- Computer freezes frequently or encounters error
- Computer slows down when programs start

False Positives: However, not all glitches can be attributed to virus attacks.

Indications of a Virus attack

How does a Computer Get Infected by Viruses

- When a user accepts files and downloads without checking properly for the source.
- Opening infected e-mail attachments.
- Installing pirated software.
- Not updating and not installing new versions of plug-ins.
- Not running the latest anti-virus application.

Indications of a Virus attack

Virus Hoaxes and Fake Antiviruses

- Hoaxes are false alarms claiming reports about a non-existing virus which may contain virus attachments.
- Warning messages propagating that a certain email message should not be viewed and doing so will damage one's system.
- Attackers disguise malwares as an antivirus and trick users to install them in their systems.
- Once installed these fake antiviruses can damage target systems similar to other malwares.

6. Types of Viruses

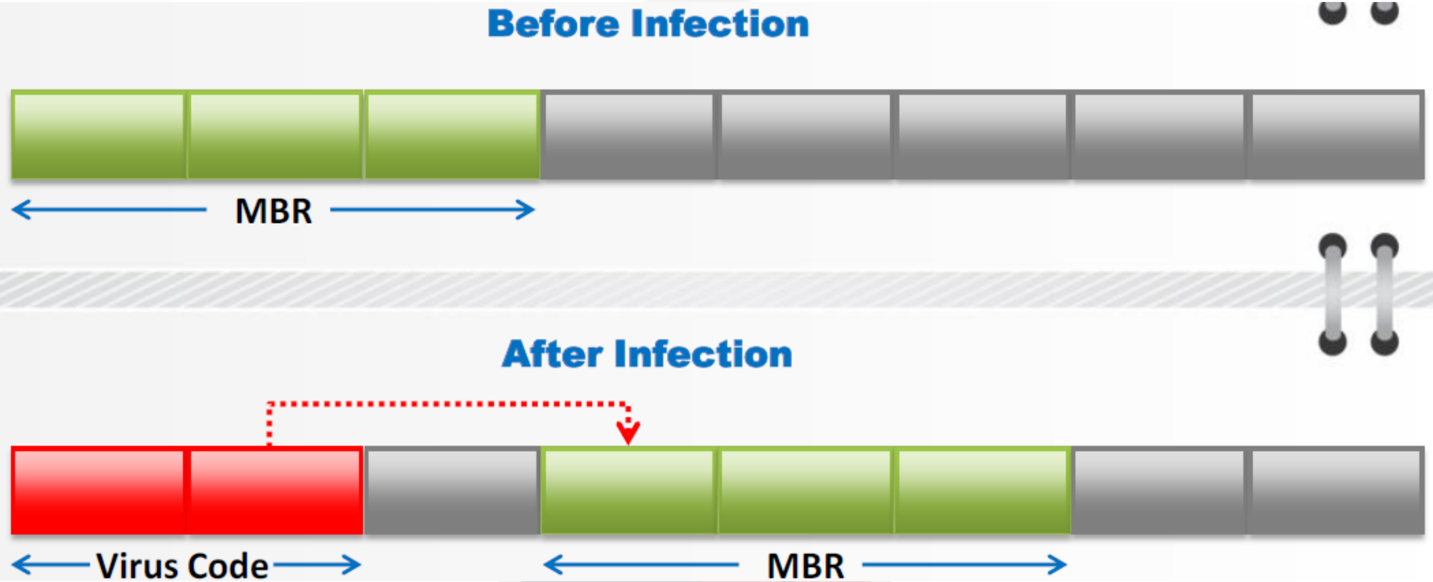
Module 9

Types of Viruses

System or Boot Sector Viruses

- Boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR.
- When system boots, virus code is executed first and then control is passed to original MBR.

Types of Viruses



Types of Viruses

File and Multipartite Viruses

- **File Viruses**:
  - File viruses infect files which are executed or interpreted in the system such as COM, EXE, SYS, OVL, OBJ, PRG, MNU and BAT files.
  - File viruses can be either direct-action (non-resident) or memory-resident.
- **Multipartite Virus**:
  - Multipartite viruses infect the system boot sector and the executable files at the same time.

Types of Viruses

Macro Viruses

- Macro viruses infect files created by Microsoft Word or Excel.
- Most macro viruses are written using macro language Visual Basic for Applications (VBA).
- Macro viruses infect templates or convert infected documents into template files, while maintaining their appearance of ordinary document files.

Types of Viruses

Cluster Viruses

- Cluster viruses modify directory table entries so that it points users or system processes to the virus code instead of the actual program.
- There is only once copy of the virus on the disk infecting all the programs in the computer system.
- It will launch itself first when any program on the computer system is started and then the control is passed to actual program.

Types of Viruses

Stealth/Tunneling Viruses

- These viruses evade the anti-virus software by intercepting its requests to the operating system.
- A virus can hide itself by intercepting the anti-virus software's request to read the file and passing the request to the virus, instead of the OS.
- The virus can then return an uninfected version of the file to the anti-virus software, so that it appears as if the file is "clean".

Types of Viruses

Encryption Viruses

- This type of virus uses simple encryption to encipher the code.
- The virus is encrypted with a different key for each infected file.
- AV scanner cannot directly detect these types of viruses using signature detection methods.

Types of Viruses

Polymorphic Code

- Polymorphic code is a code that mutates while keeping the original algorithm intact.
- To enable polymorphic code, the virus has to have a polymorphic engine (also called mutating engine or mutation engine).
- A well-written polymorphic virus therefore has no parts that stay the same on each infection.

Types of Viruses

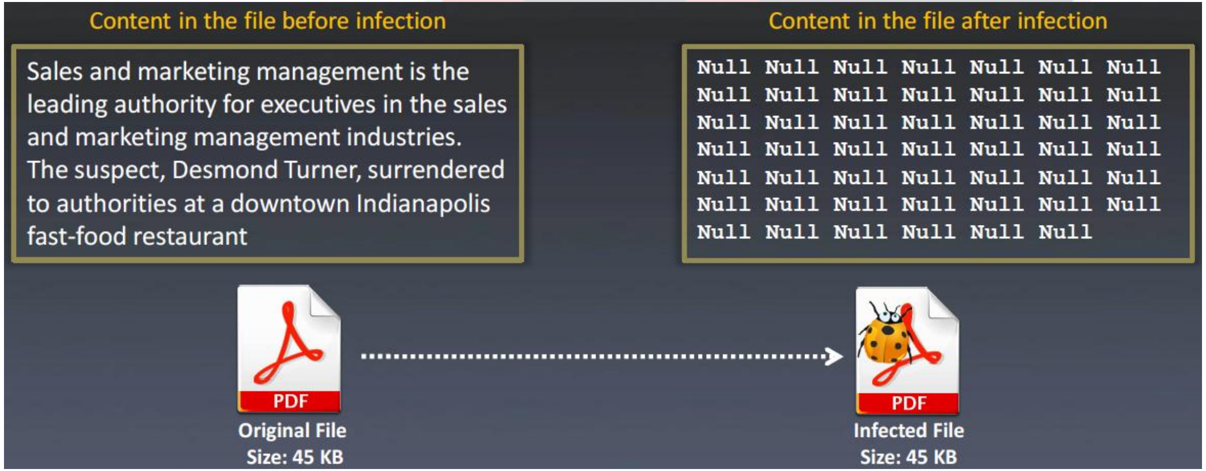
Metamorphic Viruses

- **Metamorphic Viruses**: Metamorphic viruses rewrite themselves completely each time they are to infect new executable.
- **Metamorphic Code**: Metamorphic code can reprogram itself by translating its own code into a temporary representation and then back to the normal code again.
- **Example**: For example, E32/Simile consisted of over 14000 lines of assembly code, 90% of it is part of the metamorphic engine.

Types of Viruses

File Overwriting or Cavity Viruses

- Cavity Virus overwrites a part of the host file that is with a constant (usually nulls), without increasing the length or the file and preserving its functionality.



Content in the file before infection

Sales and marketing management is the leading authority for executives in the sales and marketing management industries. The suspect, Desmond Turner, surrendered to authorities at a downtown Indianapolis fast-food restaurant

Content in the file after infection

```
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null
```

Types of Viruses

Sparse Infector Viruses

- **Sparse Infector Virus**: Sparse infector virus infects only occasionally (e.g. every tenth program executed), or only files whose lengths fall within a narrow range.
- **Difficult to Detect**: By infecting less often, such viruses try to minimize the probability of being discovered.
- **Infection Process**: For example, wake up on 15th of every month and execute code.

Types of Viruses

Companion/Camouflage Viruses

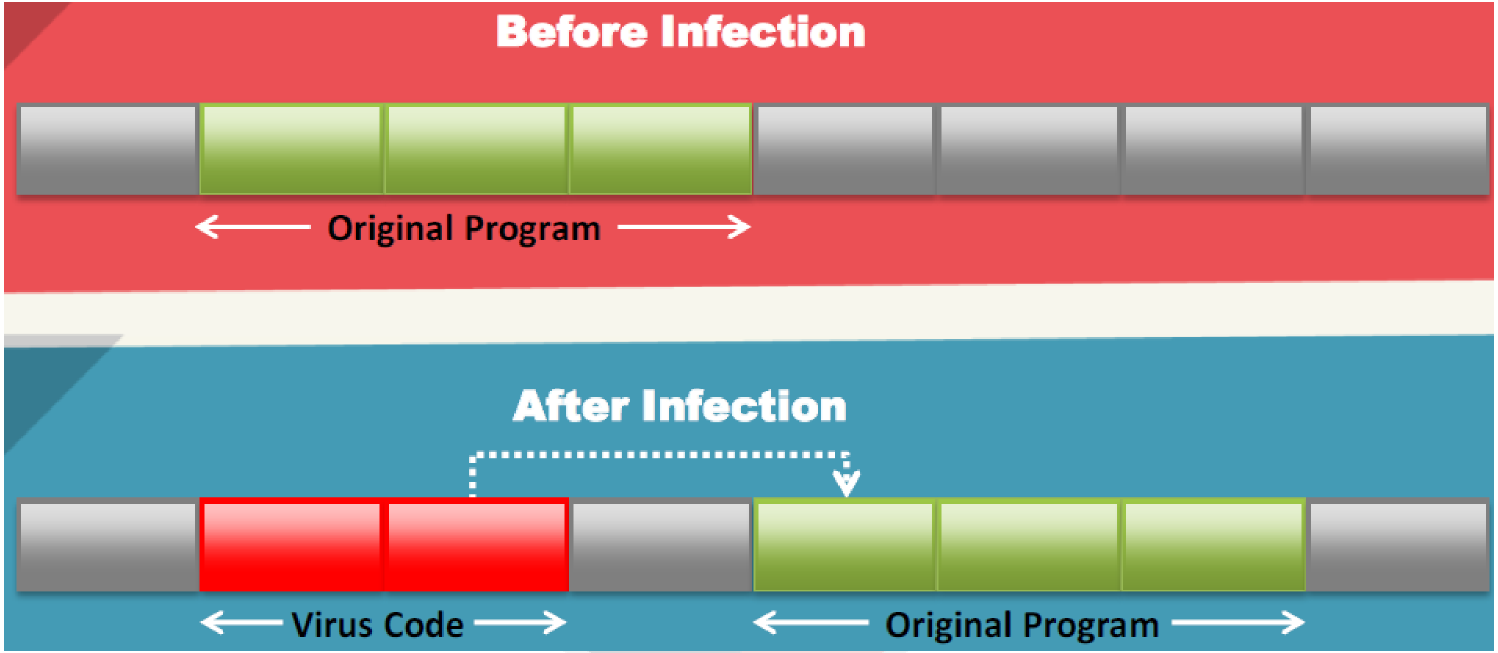
- A Companion virus creates a companion file for each executable file the virus infects.
- Therefore, a companion virus may save itself as notepad.com and every time a user executes notepad.exe (good program), the computer will load notepad.com (virus) and infect the system.

Types of Viruses

Shell Viruses

- Virus code forms a shell around the target host program's code, making itself the original program and host code as its sub-routine.
- Almost all boot program viruses are shell viruses.

Types of Viruses



Types of Viruses

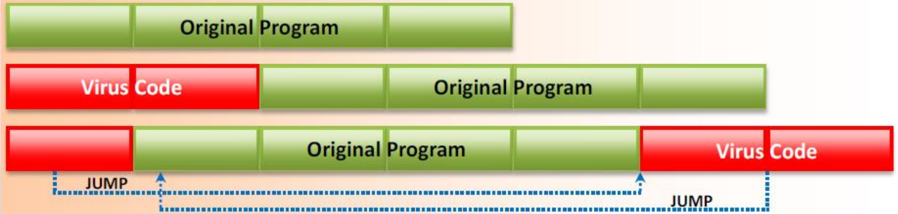
File Extension Viruses

- File extension viruses change the extensions of files.
- With extensions turned off, if someone sends you a file named BAD.TXT.VBS, you will only see BAD.TXT.
- If you have forgotten that extensions are turned off, you might think this is a text file and open it.
- This is an executable Visual Basic Script virus file and could do serious damage.
- Turn off "Hide file extensions" in Windows.

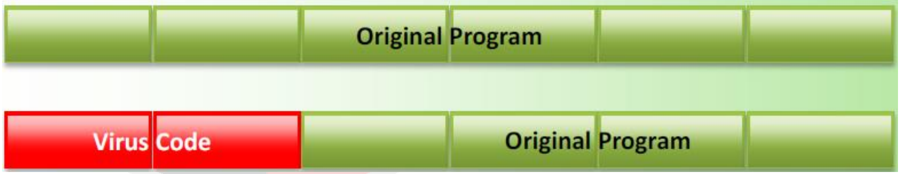
Types of Viruses

Add-on and Intrusive Viruses

- **Add-on Viruses**: Add-on viruses append their code to the host code without making any changes to the latter or relocate the host code to insert their own code at the beginning.



- **Intrusive Viruses**: Intrusive viruses overwrite the host code partly or completely with the viral code.



Types of Viruses

Transient and Terminate and Stay Resident Viruses

- **Direct Action or Transient Virus**:
  - Transfers all the controls of the host code to where it resides in the memory.
  - The virus runs when the host code is run and terminates itself or exits memory as soon as the host code execution ends.
- **Terminate and Stay Resident Virus (TSR)**:
  - Remains permanently in the memory during the entire work session even after the target host's program is executed and terminated; can be removed only by rebooting the system.

Worms

Module 9

Worms

- Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction.
- Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system.
- Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks.

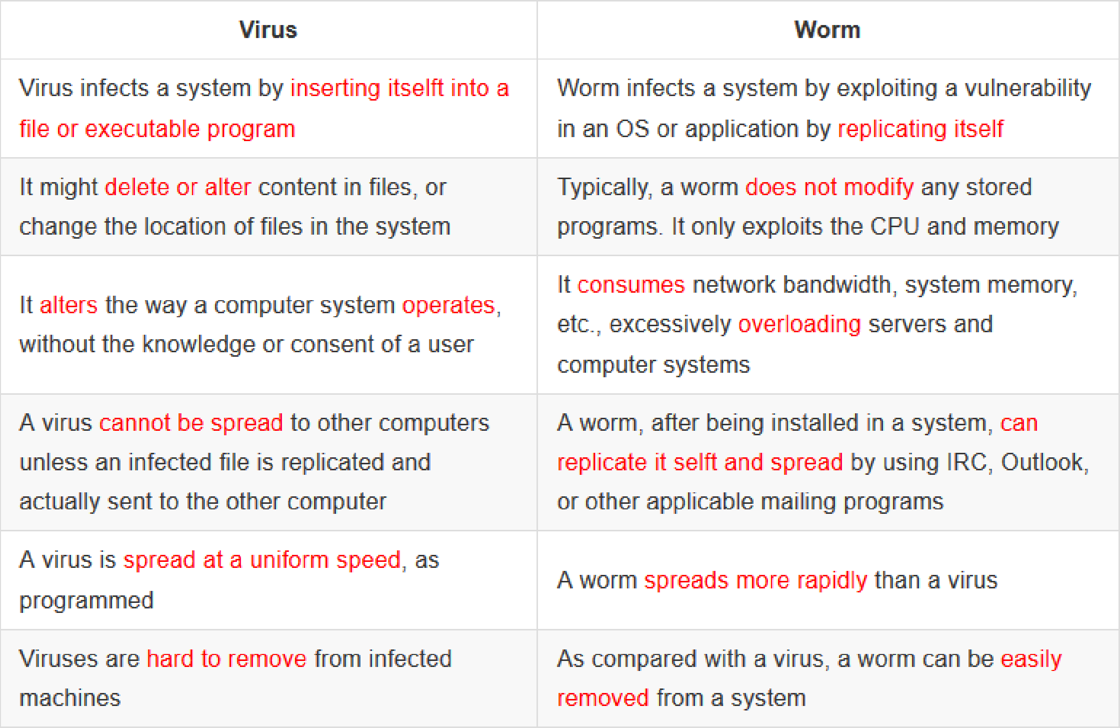
1. Worm vs. Virus

Module 9

Worm vs. Virus

- **Replicates on its own**: A worm is a special type of malware that can replicate itself and use memory, but cannot attach itself to other programs.
- **Spreads through the Infected Network**: A worm takes advantages of file or information transport features on computer systems and spread through the infected network automatically but a virus does not.

Worm vs. Virus



Virus	Worm
Virus infects a system by inserting itselft into a file or executable program	Worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter content in files, or change the location of files in the system	Typically, a worm does not modify any stored programs. It only exploits the CPU and memory
It alters the way a computer system operates, without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems
A virus cannot be spread to other computers unless an infected file is replicated and actually sent to the other computer	A worm, after being installed in a system, can replicate it selft and spread by using IRC, Outlook, or other applicable mailing programs
A virus is spread at a uniform speed, as programmed	A worm spreads more rapidly than a virus
Viruses are hard to remove from infected machines	As compared with a virus, a worm can be easily removed from a system

Trojans

Module 9

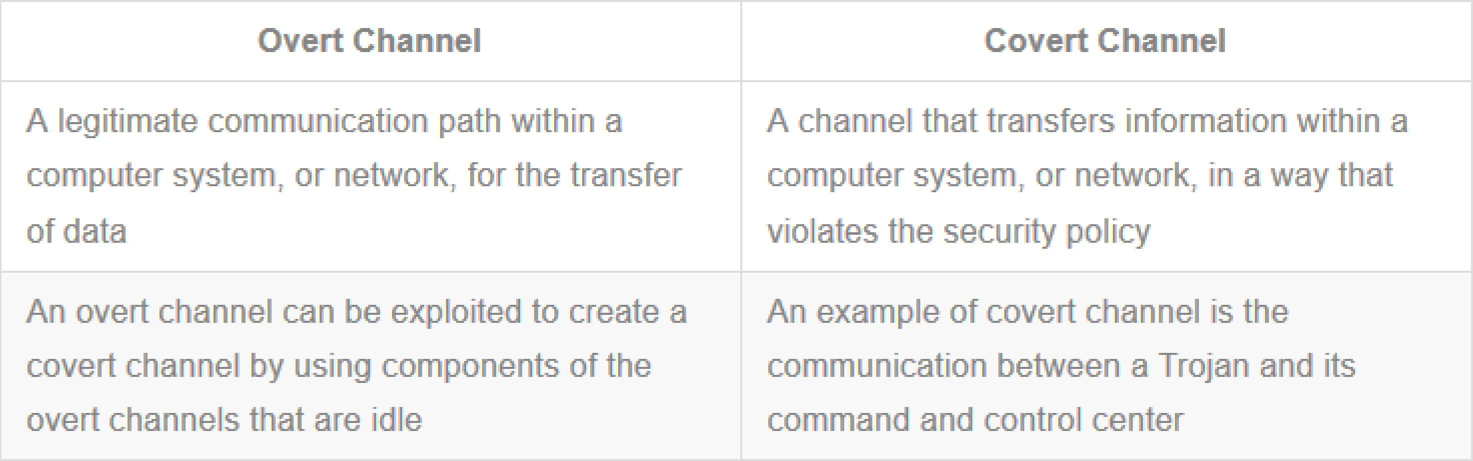
1. What is a Trojan?

Module 9

What is a Trojan?

- It is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk.
- Trojans get activated upon users' certain predefined actions.
- Indications of a Trojan attack include abnormal system and network activities such as disabling of antivirus, redirection to unknown pages, etc.
- Trojans create a covert communication channel between victim computer and attacker for transferring sensitive data.

What is a Trojan?



Overt Channel	Covert Channel
A legitimate communication path within a computer system, or network, for the transfer of data	A channel that transfers information within a computer system, or network, in a way that violates the security policy
An overt channel can be exploited to create a covert channel by using components of the overt channels that are idle	An example of covert channel is the communication between a Trojan and its command and control center

2. How Hackers use Trojans?

Module 9

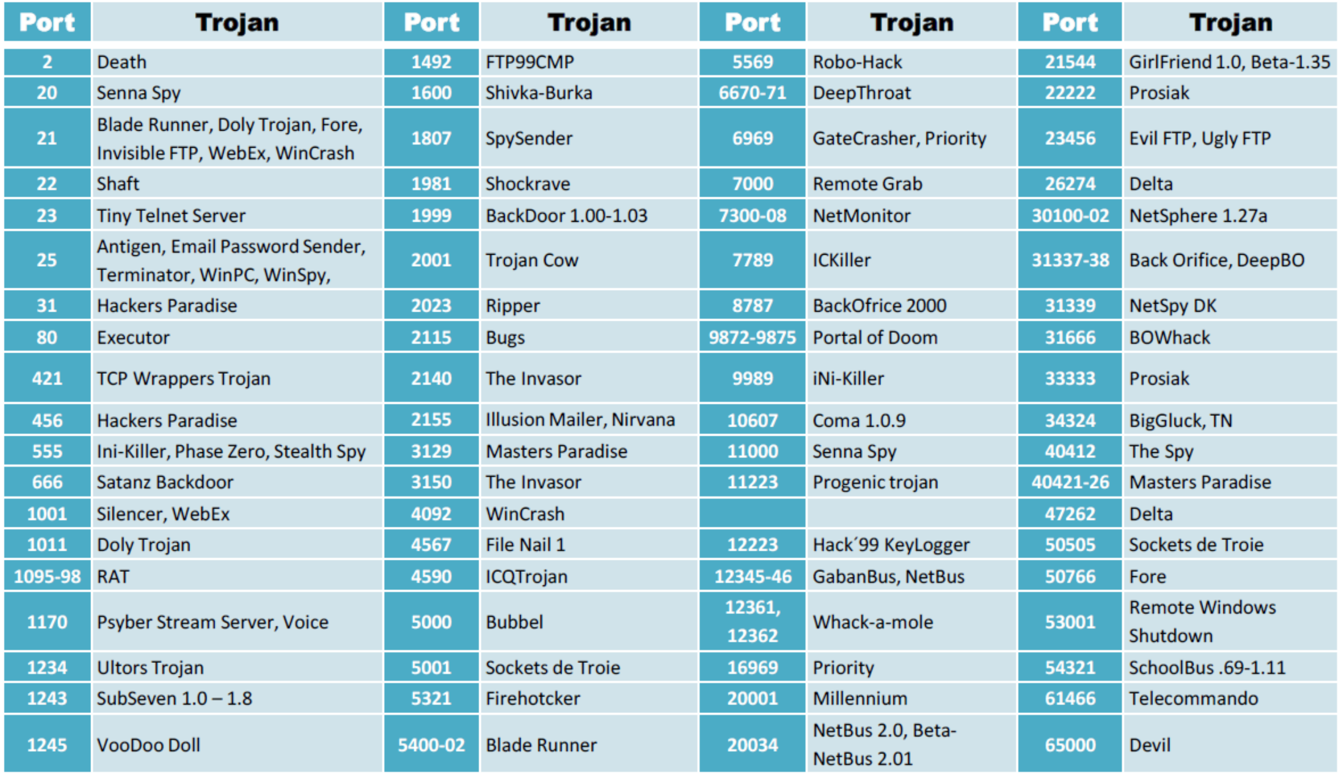
How Hackers use Trojans?

- Delete or replace operating system's critical files.
- Record screenshots, audio, and video of victim's PC.
- Use victim's PC for spamming and blasting email messages.
- Download spyware, adware, and malicious files.
- Disable firewalls and antivirus.
- Create backdoors to gain remote access.
- Infect victim's PC as a proxy server for replaying attacks.
- Use victim's PC as a botnet to perform DDoS attacks.
- Steal information such as passwords, security codes, credit card information using keyloggers.

3. Common Ports Used by Trojans

Module 9

Common Ports Used by Trojans



Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack´99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

4. How to Infect Systems Using a Trojan

Module 9

How to Infect Systems Using a Trojan

- Create a new Trojan packet using a Trojan Horse Construction Kit.
- Create a dropper, which is a part in a trojanized packet that installs the malicious code on the target system.
  - Example of a Dropper:
    - **Installation path**: c:\windows\system32\svchosts.exe
    - **Autostart**: HKLM\Software\Mic...\run\Iexplorer.exe
  - Malicious code:
    - **Client address**: client.attacker.com
    - **Dropzone**: dropzone.attacker.com

How to Infect Systems Using a Trojan

  - A genuine application:
    - **File name**: chess.exe
    - **Wrapper data**: Executable file
- Create a wrapper using wrapper tools to install Trojan on the victim's computer.
  - petite.exe, Graffiti.exe, EliteWrap
  - bind the Trojan executable to legitimate files
- Propagate the Trojan.
  - Email
- Execute the dropper.
- Execute the damage routine.

How to Infect Systems Using a Trojan

Wrappers

- A wrapper binds a Trojan executable with an innocent looking .EXE application such as games or office applications.
  - genuine-looking .EXE application
- The two programs are wrapped together into a single file.
- When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapping application in the foreground.
- Attackers might send a birthday greeting that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen.

How to Infect Systems Using a Trojan

Crypters

- Crypter is a software which is used by hackers to hide viruses, keyloggers or tools in any kind of file so that they do not easily get detected by antiviruses.
  - AIO UFD Crypter
  - Hidden Sight Crypter
  - Galaxy Crypter
  - Criogenic Crypter
  - Heaven Crypter
  - SwayzCryptor

5. Exploit Kits

Module 9

Exploit Kits

- An exploit kit or crimeware toolkit is a platform to deliver exploits and payloads such as Trojans, spywares, backdoors, bots, buffer overflow scripts, etc. on the target system.
- **Exploit Kits**
  - Infinity
  - Phoenix Exploit Kit
  - Blackhole Exploit Kit
  - Bleedinglife
  - Crimepack

6. Evading Antiviruses

Module 9

Evading Antiviruses

- Break the Trojan file into multiple pieces and zip them as single file.
- ALWAYS write your own Trojan, and embed it into an application.
- Change Trojan's syntax:
  - Convert an EXE to VB script
  - Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hide "known extensions", by default, so it shows up only .DOC, .PPT and .PDF)
- Change the content of the Trojan using hex editor and also change the checksum and encrypt the file.
- Never use Trojans downloaded from the web (antivirus can detect easily)

7. Types of Trojans

Module 9

Types of Trojans

Command Shell Trojans

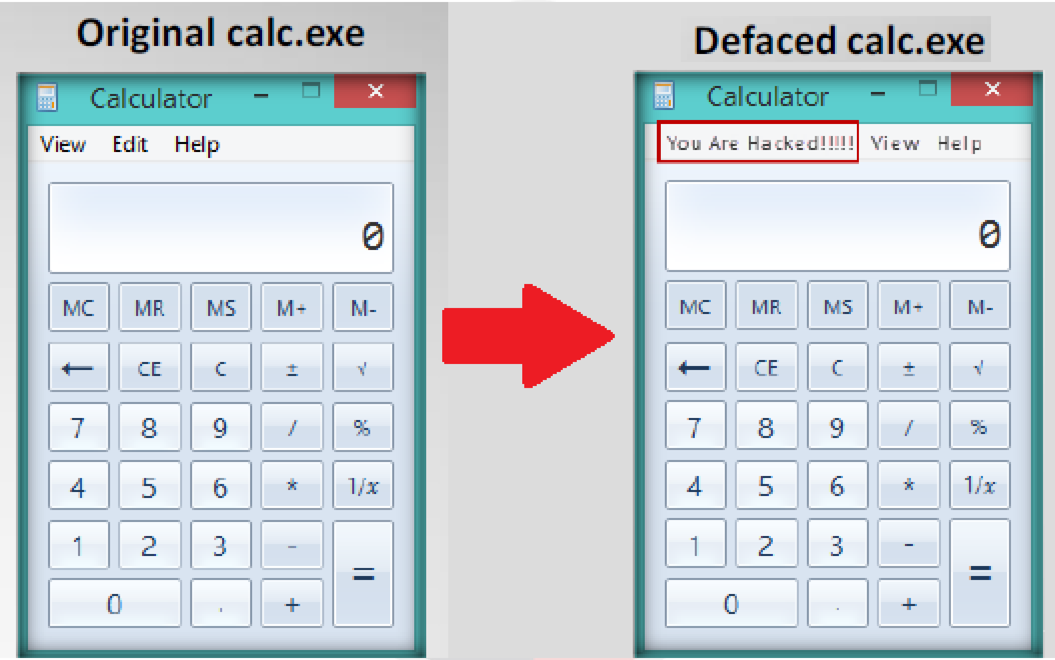
- Command shell Trojan gives remote control of a command shell on a victim's machine.
- Trojan server is installed on the victim's machine, which opens a port for attacker to connect. The client is installed on the attacker's machine, which is used to launch a command shell on the victim's machine.

Types of Trojans

Defacement Trojans

- Resource editors allow to view, edit, extract, and replace strings, bitmaps, logos and icons from any Windows program.
- It allows you to view and edit almost any aspect of a compiled Windows program, from the menus to the dialog boxes to the icons and beyond.
- They apply User-styled Custom Application (UCA) to deface Windows application.
- Example of calc.exe Defaced is shown here.

Types of Trojans



Types of Trojans

Botnet Trojans

- Botnet Trojans infect a large number of computers across a large geographical area to create a network of bots that is controlled through a Command and Control (C&C) center.
- Botnet is used to launch various attacks on a victim including denial-of-service attacks, spamming, click fraud, and the theft of financial information.

Types of Trojans

Tor-based Botnet Trojans

- Attacker uses the Tor network to provide the botnet command-and-control (C&C) servers with anonymity.
- **Skynet**: a Tor-powered trojan with DDoS, Bitcoin mining and Banking capabilities, that we observed spreading through the veins of Usenet.
- ChewBacca Trojan has stolen data on 49,000 payment cards from 45 retailers in 11 countries over a two month span.

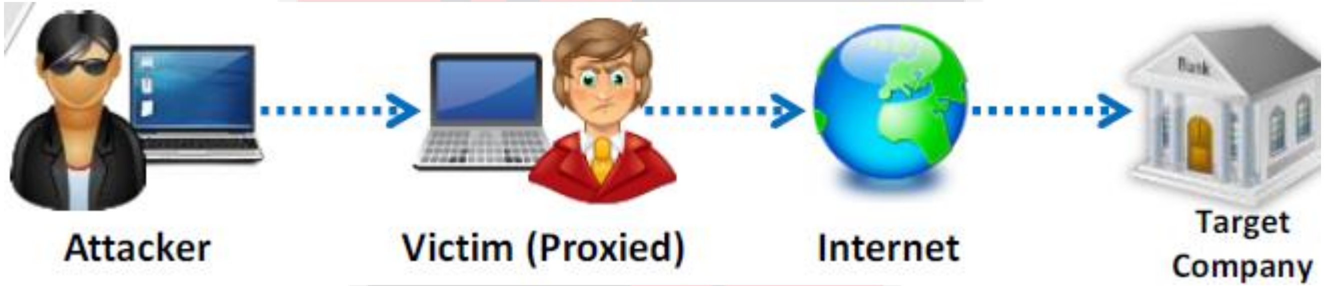
Types of Trojans

Proxy Server Trojans

- **Proxy Trojan**: Trojan Proxy is usually a standalone application that allows remote attackers to use the victim's computer as a proxy to connect to the Internet.
- **Hidden Server**: Proxy server Trojan, when infected, starts a hidden proxy server on the victim's computer.
- **Infection**: Thousands of machines on the Internet are infected with proxy servers using this technique.

Process:

Types of Trojans



Types of Trojans

FTP Trojans

- FTP Trojans install an FTP server on the victim's machine, which opens FTP ports.
- An attacker can then connect to the victim's machine using FTP port to download any files that exist on the victim's computer.

Types of Trojans

VNC Trojans

- VNC Trojans starts a VNC Server daemon in the infected system (victim).
- Attacker connects to the victim using any VNC viewer.
- Since VNC program is considered a utility, this Trojan will be difficult to detect using anti-viruses.

VNC Trojan: Hesperbot

- Hesperbot is a banking Trojan that creates a hidden VNC server to which the attacker can remotely connect.
- As VNC does not log the user off like RDP, the attacker can connect to the unsuspecting victim's computer while they are working.

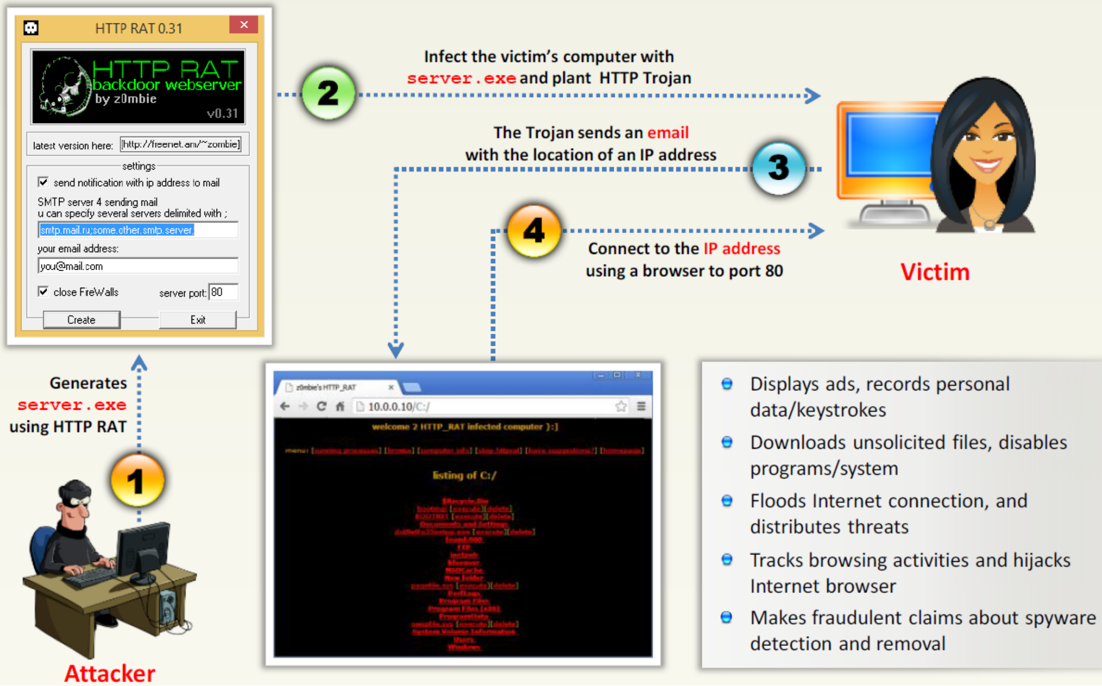
Types of Trojans

HTTP/HTTPS Trojans

- **Bypass Firewall**: HTTP Trojans can bypass any firewall and work in the reverse way of a straight HTTP tunnel.
- **Spawn a Child Program**: They are executed on the internal host and spawn a child at a predetermined time.
- **Access the Internet**: The child program appears to be a user to the firewall so it is allowed to access the Internet.

Types of Trojans

HTTP Trojan: HTTP RAT



HTTP RAT 0.31

latest version here: [http://freenet.am/~zombie]

settings

☑ send notification with ip address to mail

SMTP server 4 sending mail
u can specify several servers delimited with ;

smtp.mail.ru;some.other.smtp.server;

your email address:

you@mail.com

☑ close FreWalls

server port: 80

z0mbie's HTTP_RAT

10.0.0.10/C:/

welcome 2 HTTP_RAT infected computer }:]

menu: [running processes] [browse] [computer info] [stop httprat] [hacks suggestions!] [homepage]

listing of C:/

```
$Recycle.Bin
bootmgr [execute][delete]
BOOTNXT [execute][delete]
Documents and Settings
[illegible] [execute][delete]
found.000
FTP
[illegible]
[illegible]
MSOCache
New folder
pagefile.sys [execute][delete]
PerfLogs
Program Files
Program Files (x86)
ProgramData
swapfile.sys [execute][delete]
System Volume Information
Users
Windows
```

1 Generates **server.exe** using HTTP RAT

2 Infect the victim's computer with **server.exe** and plant HTTP Trojan

3 The Trojan sends an email with the location of an IP address

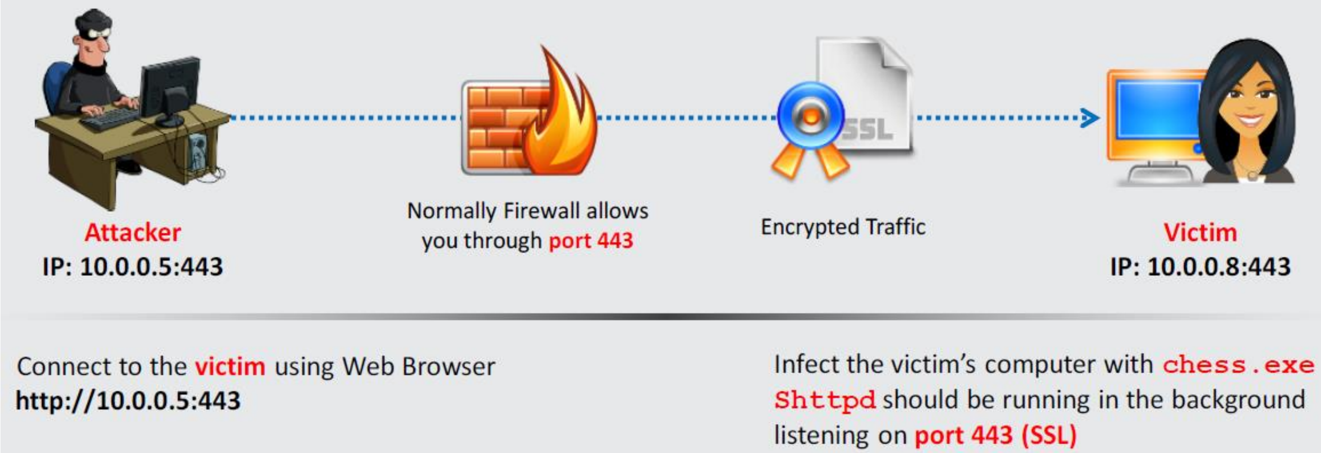
4 Connect to the IP address using a browser to port 80

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

Types of Trojans

Shttpd Trojan - HTTPS (SSL)

- SHTTPD is a small HTTP Server that can be embedded inside any program.
- It can be wrapped with a genuine program (game chess.exe), when executed it will turn a computer into an invisible web server.



Connect to the victim using Web Browser
http://10.0.0.5:443

Infect the victim's computer with `chess.exe`
`Shttpd` should be running in the background listening on port 443 (SSL)

Types of Trojans

ICMP Tunneling

- Covert channels are methods in which an attacker can hide the data in a protocol that is undetectable.
- They rely on techniques called tunneling, which allow one protocol to be carried over another protocol.
- ICMP tunneling uses ICMP echo-request and reply to carry a payload and stealthily access or control the victim's machine.

Types of Trojans

Remote Access Trojans

- This Trojan works like a remote desktop access.
- Hacker gains complete GUI access to the remote system.
- Optix Pro, MoSucker, BlackHole RAT, SSH - R.A.T., njRAT, Xtreme RAT, SpyGate - RAT, Punisher RAT, DarkComet RAT, Pandora RAT, HellSpy RAT, ProRAT, Theef, Hell Raiser, Atelier Web Remote Commander

Types of Trojans

E-banking Trojans

- e-banking Trojans intercept a victim's account information before it is encrypted and sends it to the attacker's Trojan command and control center.
- It steals victim's data such as credit card related card no., CVV2, billing details, etc. and transmits it to remote hackers using email, FTP, IRC, or other methods.
  - **TAN Grabber** (Transaction Authentication Number)
  - **HTML Injection**
  - **Form Grabber**
- ZeuS, SpyEye, Citadel Builder and Ice IX

Types of Trojans

Destructive Trojans: M4sT3r Trojan

- This Trojan formats all local and network drives.
- M4sT3r is a dangerous and destructive type of Trojan.
- The user will not be able to boot the Operating System.
- When executed, this Trojan destroys the operating system.

Types of Trojans

Notification Trojans

- Notification Trojan sends the location of the victim's IP address to the attacker.
- Whenever the victim's computer connects to the Internet, the attacker receives the notification.

Ransomware

Module 9

Ransomware

- Ransomware is a type of a malware which restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) in order to remove the restrictions.
- Form of ***malware*** that encrypts a victim's files
- Users are shown instructions for how to pay a fee to get the decryption key.
- The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.
- Ransomware kits are sold on the deep/dark web and purchased by cybercriminals

1. Types of Ransomware

Module 9

Types of Ransomware

- **Scareware:** Poses as security software or tech support. Not responding to this will not do anything except lead to more pop-ups.
- **Screenlockers**: Completely lock a user out of their computer.
- **Encrypting ransomware**: The attacker will gain access to and encrypt the victim’s data and ask for a payment to unlock the files.
- **Doxware**: Attacker may also threaten to publish your data online if the victim does not pay a ransom.
- **Mobile ransomware**: Affects mobile devices.
- The victims also get a warning that if the demanded sum is not paid by a specific date, the private key required to unlock or decrypt files will be destroyed.

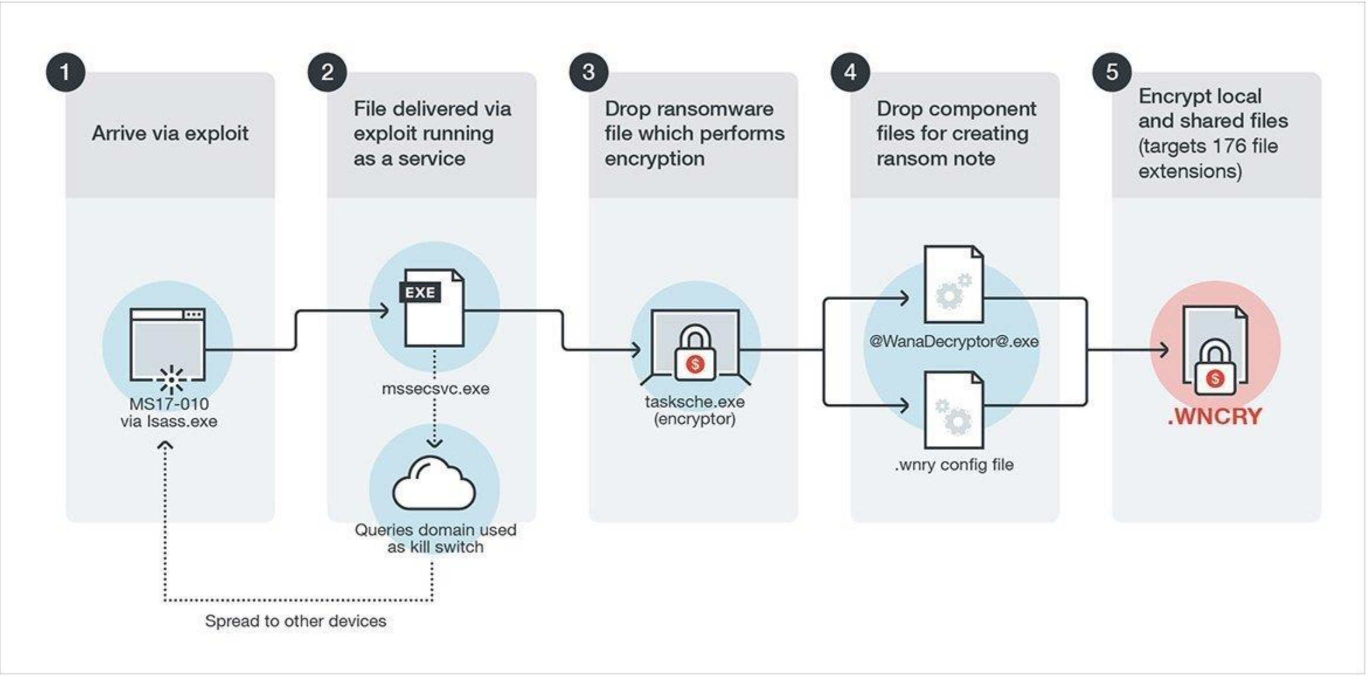
2. Case Study: WannaCry

Module 9

WannaCry Ransomware

- In May 2017, WannaCry was able to infect and encrypt more than a quarter million systems globally.
- It used asymmetric encryption. During the thick of the week in which WannaCry was most virulent, only about $100,000 in bitcoin was transferred.
- No accounts have been known to be recovered even after Payment
- The damages caused have exceeded $1 billion.
- 20% of businesses that chose to pay the ransom demanded of them didn't receive their files back.

WannaCry Ransomware


1
Arrive via exploit
2
File delivered via exploit running as a service
3
Drop ransomware file which performs encryption
4
Drop component files for creating ransom note
5
Encrypt local and shared files (targets 176 file extensions)
MS17-010 via lsass.exe
EXE
mssecsvc.exe
Queries domain used as kill switch
taskche.exe (encryptor)
$
@WanaDecryptor@.exe
.wnry config file
.WNCRY
Spread to other devices

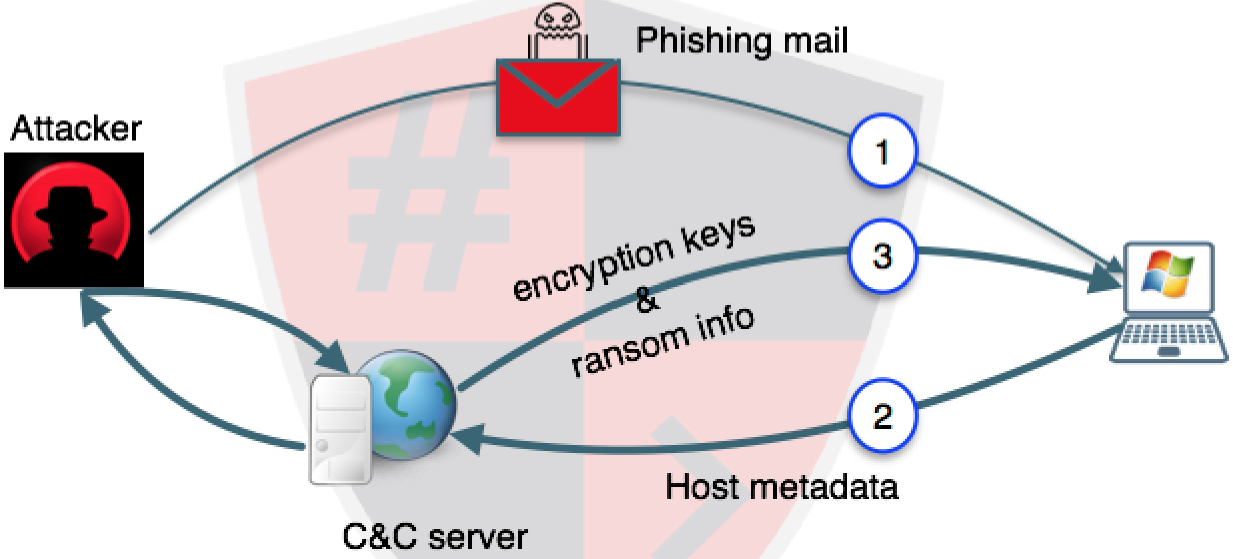
3. Case Study: Cryptolocker

Module 9

Cryptolocker Ransomware

- Perhaps the first example of a attack that used public-key encryption widely spread
- A Trojan horse that was active on the internet from September 2013 through May of the following year.
- Demanded payment in either Bitcoin or a prepaid voucher, and experts generally believed that the RSA cryptography was used
- In May 2014, however, a security firm gained access to a command-and-control server used by the attack and recovered the encryption keys used in the attacks.

Ransomware


Phishing mail
Attacker
1
3
encryption keys
&
ransom info
2
Host metadata
C&C server

4. Ransomware Families

Module 9

Ransomware Families

- Ransomware Family:
  - TeslaCrypt
  - SimpleLocker
  - WannaCry
  - NotPetya
  - Locky

Ransomware Families

- **Ransomware Family**:
  - Cryptorbit Ransomware
  - CryptoLocker Ransomware
  - CryptoDefense Ransomware
  - CryptoWall Ransomware
  - Police-themed Ransomware

5. How to remove Ransomwares

Module 9

How to remove Ransomwares

RESTORE CLEAN BACKUP

It would be your great advantage if you know how to remove ransomware virus. One way of doing so is by restoring a clean backup. If you are able to secure a clean backup to another separate disk or to the cloud and you have been attacked by the ransomware, you will be able to reformat your disk and restore your clean backup. That way, you will successfully remove the ransomware virus from your computer.

DECRYPTION TOOLS

Another way of removing ransomware is through the use of the decryption tools. If you were attacked by the ransomware and know how to remove ransomware virus, you will not be afraid. This decryption tool is developed by the computer programmers aimed to help victims recover their stolen data by the ransomware. This decryption tool will depend on which type of ransomware got into your computer. Apparently, not all ransomware are covered by this decryption utility. Some developers unable to make a decryption tool because the ransomware has more advanced encryption technique.

NEGOTIATION

If you don't know how to remove ransomware virus, this could be your last and most dangerous action. This option is very common for some small businesses who value their data so much. They are willing to pay the ransom just to retrieve their valuable data on the computer. Others try to negotiate and avoid to pay the demanded ransom fee. They pay the smaller amount, chances are high because all they want is money, it is better for them to get a small amount rather than nothing at all.

Malware Detection

Module 9

Malware Detection

How to Detect Trojans

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

Malware Detection

Scanning for Suspicious Ports

- Trojans open unused ports in victim machine to connect back to Trojan handlers.
- Look for the connection established to unknown or suspicious IP addresses.
- Type netstat -an in command prompt.

Port Monitoring Tools: TCPView and CurrPorts

- **TCPView**: TCPView show detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.
- **CurrPorts**: CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer.

Malware Detection

Scanning for Suspicious Processes

- Trojans camouflage themselves as genuine Windows services or hide their processes to avoid detection.
- Some Trojans use PEs (Portable Executable) to inject into various processes (such as explorer.exe or web browsers).
- Trojans can also use rootkit methods to hide their processes.
- Use process monitoring tools to detect hidden Trojans and backdoors.
- **Process Monitor**: Process Monitor is a monitoring tool for Windows that shows file system, registry, and process/thread activity.

Malware Detection

Scanning for Suspicious Registry Entries

- Windows automatically executes instructions in:
  - Run
  - RunServices
  - RunOnce
  - RunServicesOnce
  - HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*.
- Scanning registry values for suspicious entries may indicate the Trojan infection.
- Trojans insert instructions at these sections of registry to perform malicious activities.

Malware Detection

Scanning for Suspicious Device Drivers

- Trojans are installed along with device drivers downloaded from untrusted sources and use these drivers as a shield to avoid detection.
- Scan for suspicious device drivers and verify if they are genuine and downloaded from the publisher's original site.
- Go to **Run -> Type msinfo32 -> Software Environment -> System Drivers**

Malware Detection

Scanning for Suspicious Windows Services

- Trojans spawn Windows services allow attackers remote control to the victim machine and pass malicious instructions.
- Trojans rename their processes to look like a genuine Windows service in order to avoid detection.
- Trojans employ rootkit techniques to manipulate **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Service** registry keys to hide its processes.

Malware Detection

Scanning for Suspicious Startup Programs

- **Check startup program entries in the registry**: Details are covered in next slide.
- **Check device drivers automatically loaded**: C:\Windows\System32\drivers
- **Check boot.ini**: Check boot.ini or bcd (bootmgr) entries.
- **Check Windows services automatic started**: Go to **Run -> Type services.msc -> Sort by Startup Type.**
- **Check startup folder**:
  - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
  - C:\Users(User-Name)\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Malware Detection

Scanning for Suspicious Files and Folders

- Trojans normally modify system's files and folders. Use these tools to detect system changes.
- **SIGVERIF:**
  - It checks integrity of critical files that have been digitally signed by Microsoft.
  - To launch SIGVERIF, to to **Start -> Run**, type **sigverif** and press **Enter**.

Malware Detection

Scanning for Suspicious Files and Folders

- **FCIV (File Checksum Integrity Verifier):**
  - It is a command line utility that computes MD5 or SHA1 cryptographic hashes for files.
  - You can download FCIV at **http://download.microsoft.com**
- **TRIPWIRE:**
  - It is an enterprise class system integrity verifier that scans and reports critical system files for changes.

Malware Detection

Scanning for Suspicious Network Activities

- Trojans connect back to handlers and send confidential information to attackers.
- Use network scanners and packet sniffers to monitor network traffic going to malicious remote addresses.
- Run tools such as Capsa to monitor network traffic and look for suspicious activities sent over the web.

Malware Detection

Virus Detection Methods

- **Scanning**:
  - Once a virus has been detected, it is possible to write scanning programs that look for signature string characteristics of the virus.
- **Integrity Checking**:
  - Integrity checking products work by reading the entire disk and recording integrity data that acts as a signature for the files and system sectors.
- **Interception**:
  - The interceptor monitors the operating system requests that are written to the disk.

Malware Detection

- **Code Emulation**:
  - In code emulation techniques, the anti-virus executes the malicious code inside a virtual machine to simulate CPU and memory activities.
  - This techniques is considered very effective in dealing with encrypted and polymorphic viruses if the virtual machine mimics the real machine.
- **Heuristic Analysis**:
  - Heuristic analysis can be static or dynamic.
  - In static analysis the anti-virus analyses the file format and code structure to determine if the code is viral.
  - In dynamic analysis the anti-virus performs a code emulation of the suspicious code to determine if the code is viral.

Malware Analysis

Module 9

1. Prerequisites

Module 9

Malware Analysis

What is Sheep Dip Computer?

- Sheep dipping refers to the analysis of suspect files, incoming messages, etc. for malware.
- A sheep dip computer is installed with port monitors, file monitors, network monitors and antivirus software and connects to a network only under strictly controlled conditions.
- A computer used for sheep dipping should have, for example:
  - Run user, group permission and process monitors
  - Run port and network monitors
  - Run device driver and file monitors
  - Run registry and kernel monitors

Malware Analysis

Malware Analysis Procedure: Preparing Testbed

- Install Virtual machine (VMware, Hyper-V, etc.) on the system.
- Install guest OS into the Virtual machine.
- Isolate the system from the network by ensuring that the NIC card is in "host only" mode.
- Disable the "shared folders", and the "guest isolation".
- Copy the malware over to the guest OS.

2. Analysis Procedure

Module 9

Malware Analysis

- Perform static analysis when the malware is inactive.
- Collect information about:
  - String values found in the binary with the help of string extracting tools such as BinText.
  - The packaging and compressing techniques used with the help of compression and decompression tools such as UPX.
- Set up network connection and check that it is not giving any errors.
- Run the virus and monitor the process actions and system information with the help of process monitoring tools such as Process Monitor and Process Explorer.

Malware Analysis

- Record network traffic information using the connectivity and log packet content monitoring tools such as NetResident and TCPView.
- Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as RegShot.
- Collect the following information using debugging tools such as OllDbg and ProcDump:
  - Service requests and DNS tables information
  - Attempts for incoming and outgoing connections

3. Ransomware Analysis: CryptoLocker

Module 9

Malware Analysis

Infection and Propagation Vectors:

- The malware is being propagated via malicious links in spam e-mails which leads to pages exploiting common system vulnerabilities.
- These exploit pages will drop Ransom Cryptolocker and other malicious executable files on the affected machine.

Malware Analysis

Characteristics and Symptoms:

- The contents of the original files are encrypted using AES Algorithm with a randomly generated key.
- Once the system is infected, the malware binary first tries to connect to a hard coded command and control server with IP address 184.164.136.134
- If this attempt fails, it generates a domain name using random domain name algorithm and appends it with domain names such as .org, .net, .co.uk, .info, .com, .biz, and .ru.

Malware Analysis

Encryption Technique:

- The malware uses an AES algorithm to encrypt the files. The malware first generates a 256 bit AES key and this will be used to encrypt the files.
- In order to be able to decrypt the files, the malware author needs to know that key.
- To avoid transmitting the key in clear text, the malware will encrypt it using an asymmmetric key algorithm, namely the RSA public/private key pair.
- This encrypted key is then submitted to the C&C server.

Malware Analysis

- Once the system is compromised, the malware displays the below mentioned warning to the user and demand ransom to decrypt the files.
- It maintains the list of files which was encrypted by this malware under the following registry entry
  - HKEY_CURRENT_USER\Software\CryptoLocker\Files
- On execution, this malware binary copies itself to %AppData% location and deletes itself using a batch file
  - %AppData%\{2E376276-3A5A-0712-2BE2-FBF2CFF7ECD5}.exe

Countermeasures

Module 9

1. Malwares (Trojans, Viruses, Worms, Backdoors)

Module 9

Countermeasures

- Block all unnecessary ports at the hosts and firewall.
- Avoid accepting the programs transferred by instant messaging.
- Harden weak, default configuration settings and disable unused functionality including protocols and services.
- Monitor the internal network traffic for odd ports or encrypted traffic.
- Avoid downloading and executing applications from untrusted sources.
- Install patches and security updates for the operating systems and applications.
- Use anti-virus tools such as McAfee, Norton, etc. to detect and eliminate backdoors.

Countermeasures

- Install anti-virus software that detects and removes infections as they appear.
- Generate an anti-virus policy for safe computing and distribute it to the staff.
- Pay attention to the instructions while downloading files or any programs from the Internet.
- Update the anti-virus software regularly.
- Avoid opening the attachments received from an unknown sender as viruses spread via e-mail attachments.
- Possibility of virus infection may corrupt data, thus regularly maintain data back up.

Countermeasures

- Scan CDs and DVDs with antivirus software before using.
- Restrict permissions within the desktop environment to prevent malicious applications installation.
- Avoid typing the commands blindly and implementing pre-fabricated programs or scripts.
- Manage local workstation file integrity through checksums, auditing, and port scanning.
- Run host-based antivirus, firewall, and intrusion detection software.

Countermeasures

- Schedule regular scans for all drives after the installation of anti-virus software.
- Do not accept disks or programs without checking them first using a current version of an anti-virus program.
- Ensure the pop-up blocker is turned on and use an Internet firewall.
- Run disk clean up, registry scanner and defragmentation once a week.
- Turn on the firewall if the OS used is Windows XP.
- Run anti-spyware or adware once in a week.
- Do not open the files with more than one file type extension.

2. Ransomware

Module 9

How to prevent Ransomware Attacks

- Do not pay the ransom. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.
- Restore any impacted files from a known good backup.
- Do not provide personal information when answering an email, unsolicited phone call, text message or instant message.
- Use reputable antivirus software and a firewall. Do employ content scanning and filtering on your mail servers.
- Do make sure that all systems and software are up-to-date with relevant patches.
- Make sure you use a trustworthy Virtual Private Network (VPN) when accessing public Wi-Fi.

HACKING

Is an art, practised through a creative mind.