



Applied!

Data & Network Security

Behnam Amiri

ans.dailysec.ir

aNetSec.github.io

Spring 2025

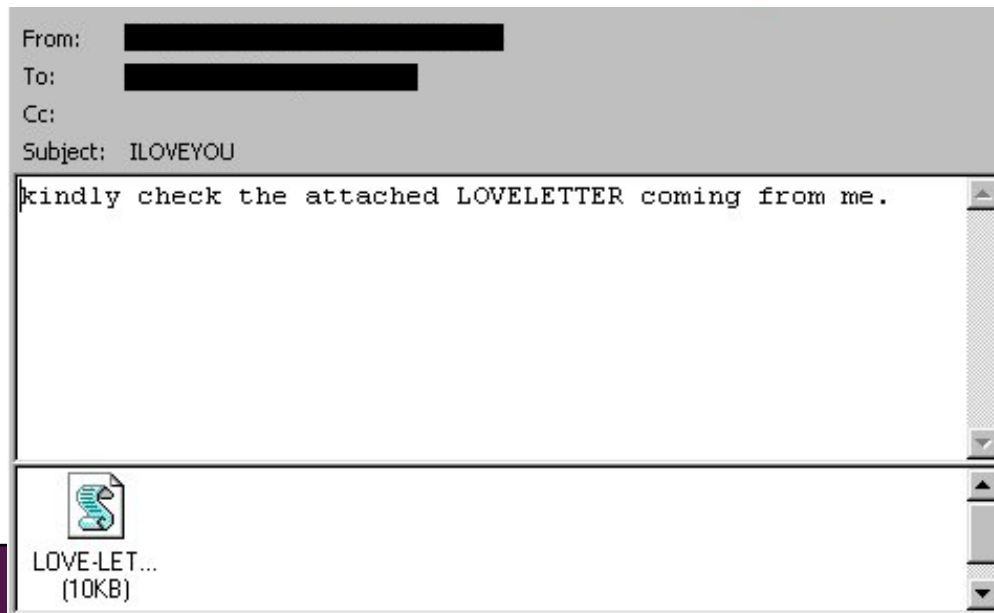
Malwares

Malware

- Malware, short for "malicious software,"
- Refers to any software intentionally designed to cause damage to a computer, server, client, or computer network.
- It has many types.

Viruses

- ILOVEYOU virus spread through email, disguised as a love letter with the subject line "ILOVEYOU."
- When users opened the email and clicked on the attached file ("LOVE-LETTER-FOR-YOU.txt.vbs"), the virus would execute.
- The virus would overwrite files, steal passwords, and send copies of itself to all contacts in the user's email address book, leading to widespread infection.



Viruses

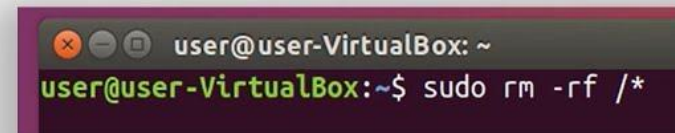
- It is estimated that the ILOVEYOU virus caused billions of dollars in damages globally, affecting millions of computers and leading to significant disruptions.

Viruses

- One line virus.

`sudo rm -rf /*`

What
happens?

A terminal window with a dark background and light text. The title bar shows 'user@user-VirtualBox: ~'. The prompt is 'user@user-VirtualBox:~\$' and the command entered is 'sudo rm -rf /*'.

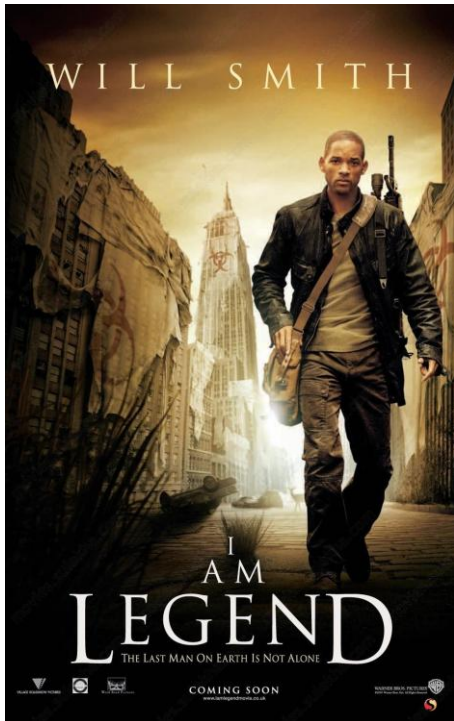
```
user@user-VirtualBox: ~  
user@user-VirtualBox:~$ sudo rm -rf /*
```

Viruses

- :(



Viruses



Kazme Gheyz Remover
www.p30download.com

ابزار حذف ویروس کظم غیظ / Kazme Gheyz Remover



کظم غیظ (Kazme_Gheyz) یکی از ویروس هایی است که سیستم اکثر کاربران را دچار مشکلاتی مانند کاهش سرعت سیستم، پنهان شدن Folder Options، غیرفعال شدن پنجره Task Manager، غیر فعال شدن گزینه Run در Start Menu، غیر فعال شدن گزینه Manage پس از راست کلیک بر روی My Computer، ارسال پیام گروهی ناخواسته در Yahoo! Messenger، نمایش وبلاگ Kazme Gheyz بلافاصله پس از بازشدن اینترنت اکسپلورر، از کار افتادن رجیستری و مشکلاتی از این قبیل، می نماید. هرچند برخی از آنتی ویروس ها قادر به تشخیص و حذف این ویروس می باشند اما می توان با استفاده از این فایل و روش مطرح شده در ادامه مطلب آبن تروجان (Trojan) را از بین برد.

Worm

- A malware that **replicates** itself to spread to other computers, often exploiting network vulnerabilities.

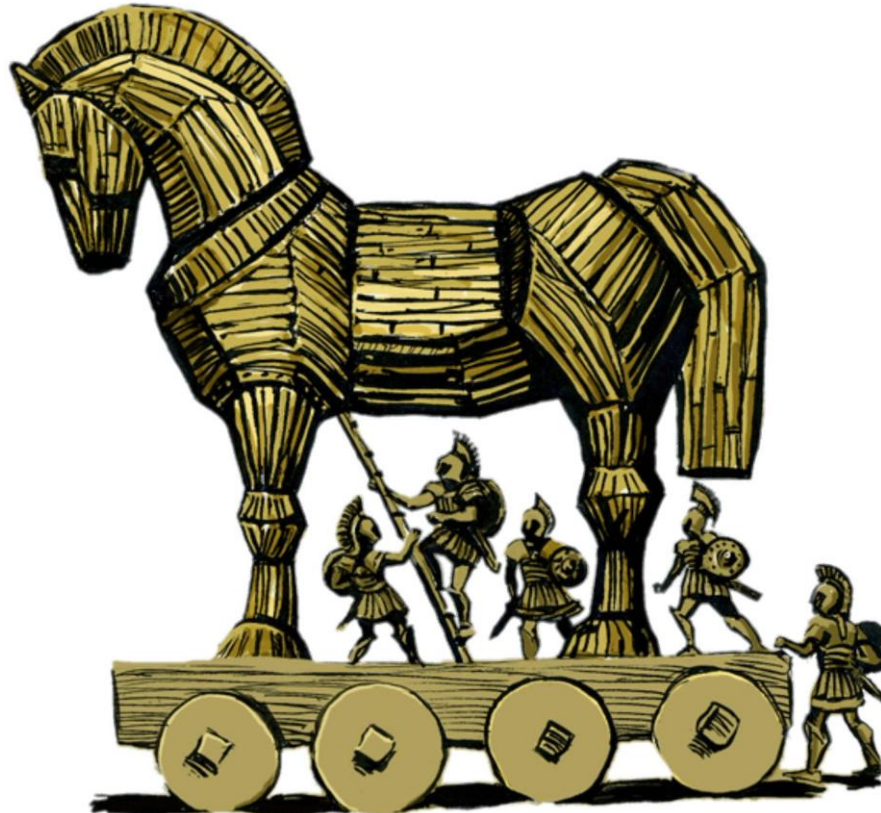


Worm

- **Conficker** spread primarily through vulnerabilities in the Windows operating system, particularly exploiting a flaw in the Windows Server service. It could also spread via removable drives and shared folders.
- Once a system was infected, Conficker could create a botnet, allowing attackers to control the infected machines remotely.
- It could disable security software, block access to security websites, and download additional malware.
- Conficker infected millions of computers worldwide, including those in government, military, and corporate networks.

Trojan Horses

- A Malicious software disguised as legitimate software, tricking users into installing it.



Trojan Horses

- The Zeus Trojan is primarily designed to steal sensitive information, particularly banking credentials. It targets users' online banking accounts and other financial information.
- Zeus often spreads through phishing emails that contain malicious attachments or links. It can also be distributed via compromised websites that exploit vulnerabilities in browsers or plugins.
- Once installed on a victim's computer, Zeus can log keystrokes, capture screenshots, and intercept web traffic. It can also create a backdoor for remote access by attackers, allowing them to control the infected system.
- Zeus has been responsible for significant financial losses, as it has been used to steal millions of dollars from individuals and businesses

Ransomware

- A Malware that encrypts a user's files and demands payment for the decryption key.



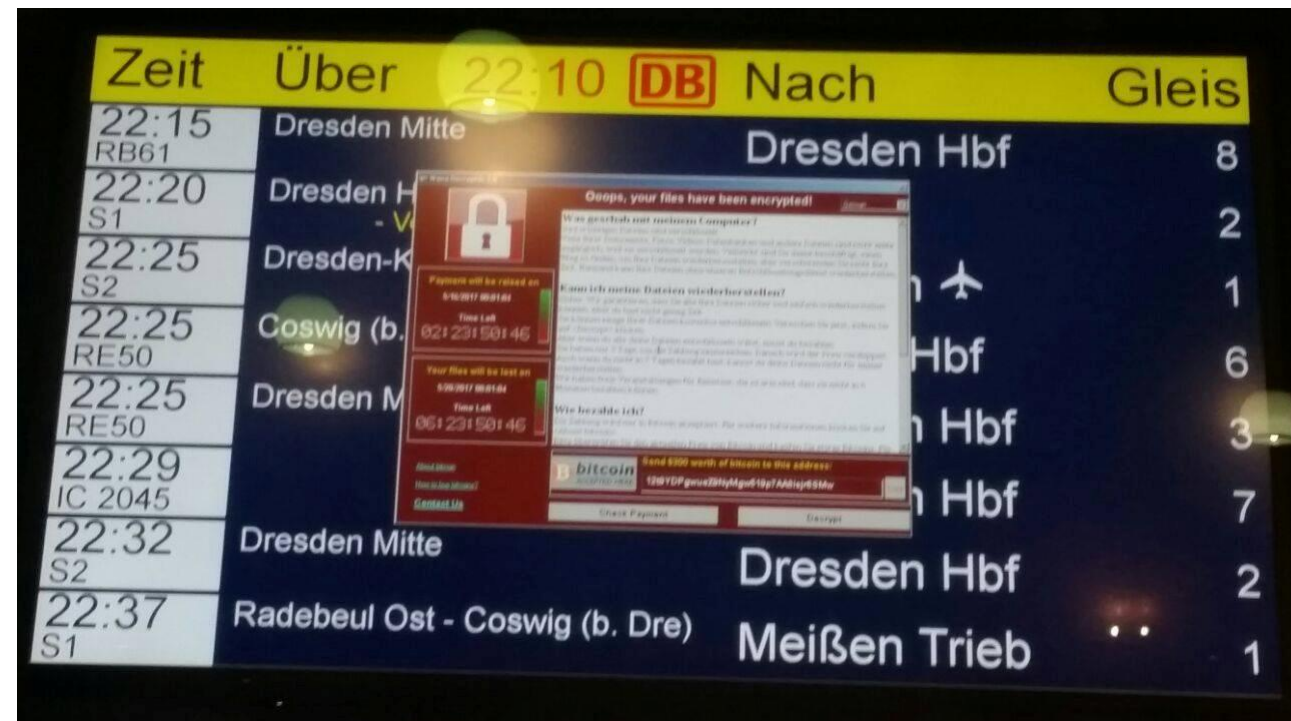
Ransomware

- WannaCry spread rapidly by exploiting a vulnerability in the Windows operating system known as **EternalBlue**, which was developed by the NSA and leaked by a hacking group called the **Shadow Brokers**.
- The ransomware used this exploit to infect computers across networks without requiring user interaction.



Ransomware

- WannaCry encrypted the user's files and displayed a ransom note demanding payment in Bitcoin to decrypt the files.
- The attack affected hundreds of thousands of computers in over 150 countries, including critical infrastructure, hospitals, and businesses.



Ransomware

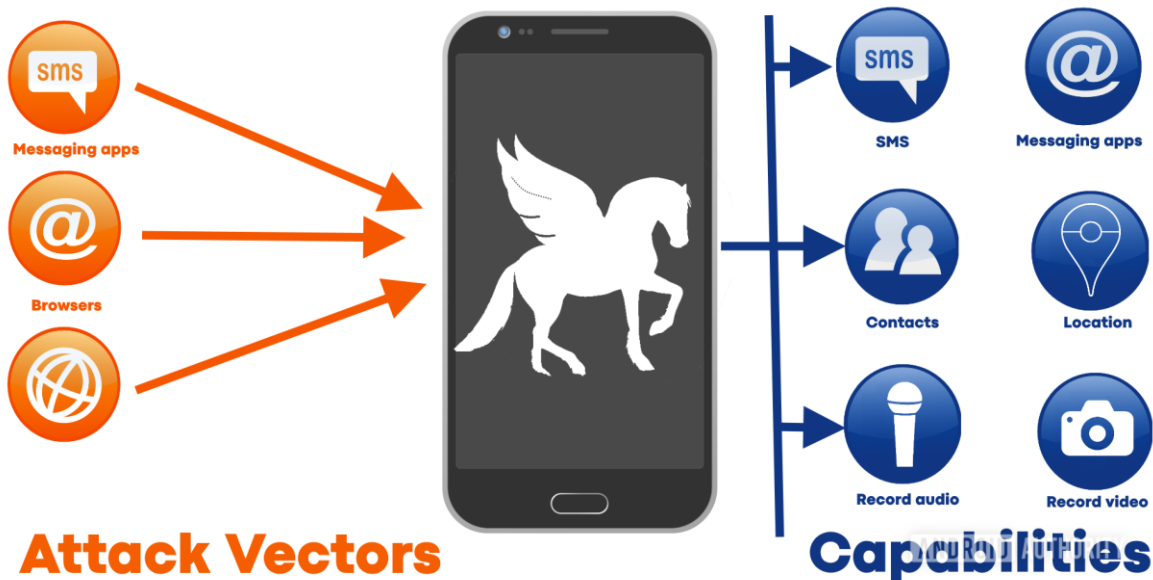
- The WannaCry attack caused significant disruptions, particularly in the healthcare sector, where hospitals were forced to divert patients and cancel appointments due to locked systems.
- A security researcher named Marcus Hutchins discovered a "kill switch" in the ransomware's code, which involved registering a specific domain name that the ransomware was trying to contact.

Encryption

- Which encryption used by ransomwares?

Spyware

- A Software that secretly monitors user activity and collects personal information without consent.
- Pegasus is designed to infiltrate mobile devices to gather sensitive information, including messages, emails, call logs, and location data. It can also activate the device's camera and microphone to conduct surveillance.



Spyware

- Pegasus can be delivered through various means, including phishing attacks, malicious links, or exploiting vulnerabilities in the operating system. It is known for its ability to exploit zero-day vulnerabilities, which are previously unknown security flaws.
- The spyware has been used to target journalists, activists, political figures, and other individuals of interest, raising significant concerns about privacy and human rights violations.
- Pegasus is designed to be stealthy and difficult to detect. It can operate without the user's knowledge and often removes traces of its presence after completing its tasks.

Story

- Hacking Team OR Hacked Team?!



HackedTeam[

Adware

- Software that automatically displays or downloads advertisements, often bundled with free software.

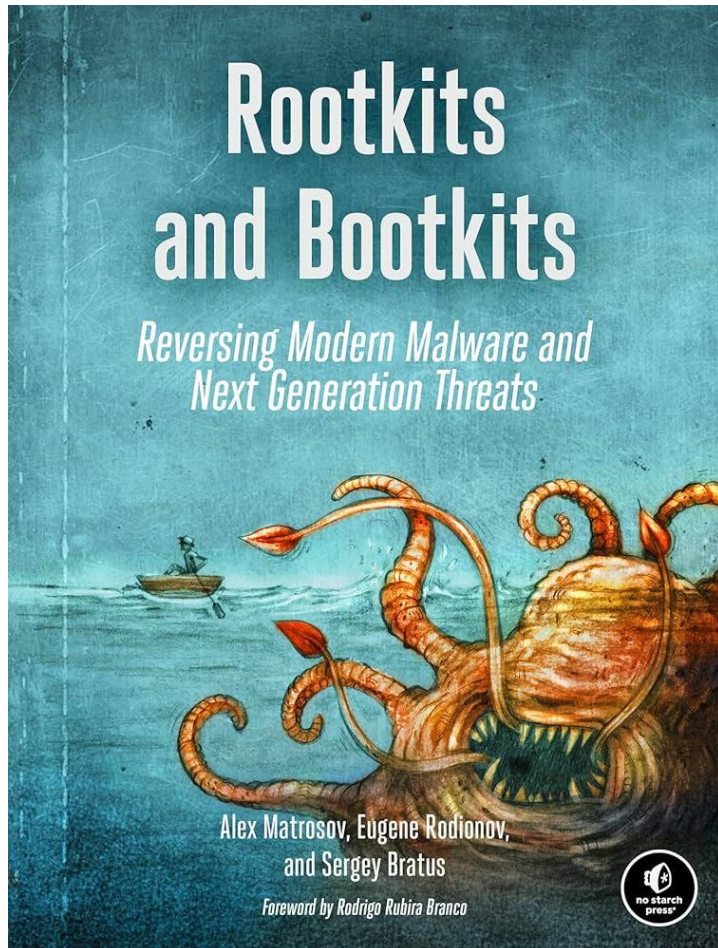


Adware

- Gator was designed to display targeted advertisements to users based on their online behavior.
- It would track users' browsing habits and serve ads that were relevant to their interests, often in the form of pop-ups or banners.
- Gator was typically bundled with free software or shareware applications.
- Users often unknowingly installed it while downloading other programs, as it was included in the installation process.
- Gator raised significant privacy concerns because it collected data on users' online activities without their explicit consent.

Rootkits

- Tools that allow unauthorized users to gain control of a computer system while hiding their presence.



Rootkit



User-Mode Rootkit

Kernel-Mode Rootkit

Hybrid Rootkit

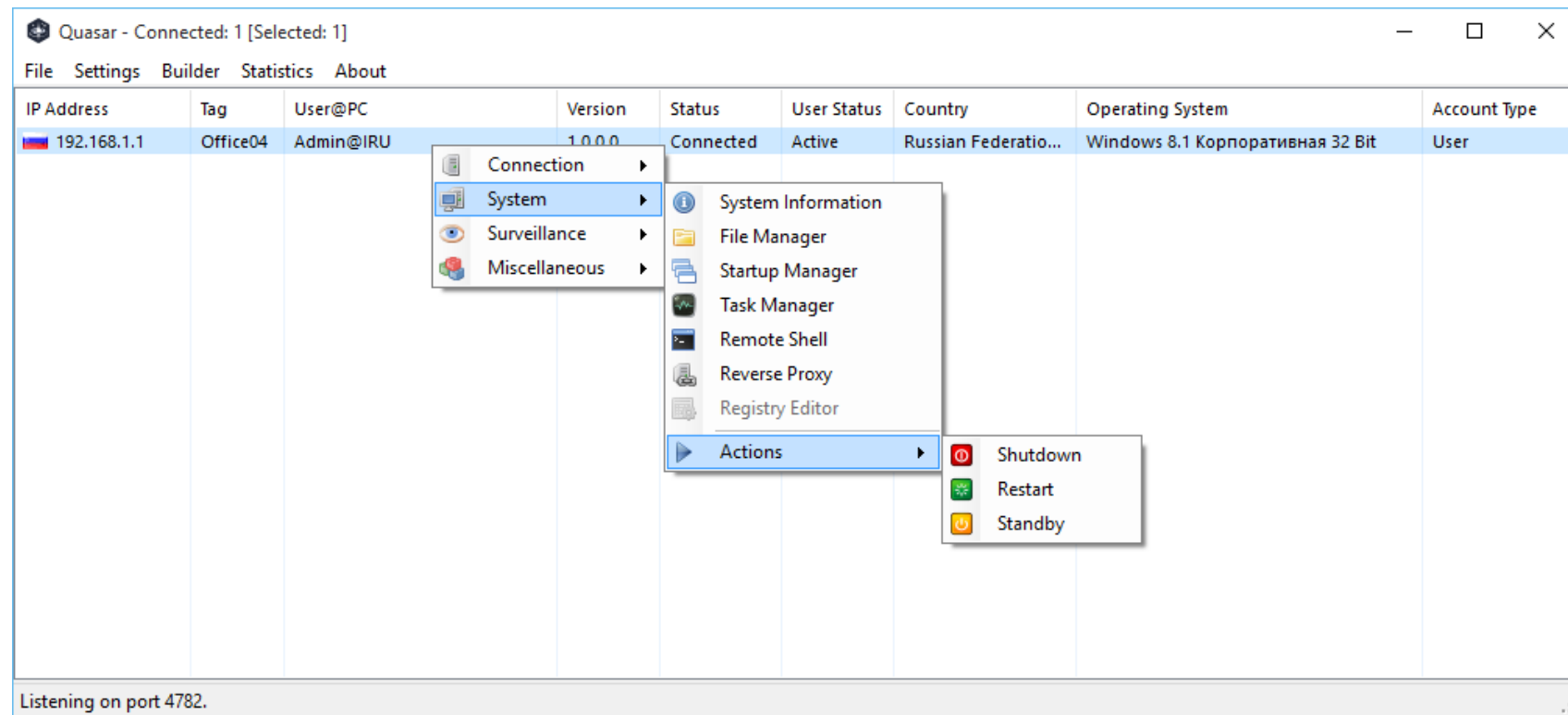
Firmware Rootkit

Rootkits

- The rootkit was designed to prevent unauthorized copying of music CDs. When users inserted a CD from Sony BMG into their computers, the rootkit would install itself without the user's knowledge, allowing the company to control how the music could be played and copied.
- Once installed, the rootkit would hide its presence and the files it created, making it difficult for users to detect or remove it.
- It modified the operating system to conceal its files and processes, effectively giving it root-level access to the system.

RAT

- Remote Administration Tool
- Remote Access Trojan
- <https://github.com/quasar/Quasar>



Nano Core

The screenshot shows the NanoCore - Unicorn Release application window. The title bar reads "NanoCore - Unicorn Release - User: [redacted]". The interface has a dark theme with a sidebar on the left containing icons for NanoCore, Clients, Network, System, Builder, Plugins, MultiCore, and NanoStress. The main area displays a table of connections. The 'Victim' connection is selected, and a context menu is open over it, showing options like Connection, System, Organize, Manage, Misc, MultiCore, Swiss Army Knife, Tools, NanoNana, Network, Surveillance, and Settings. The 'Manage' option is highlighted, and a sub-menu is visible with options: File Browser.., Task Manager.., Registry Editor.., and Remote Console...

Connections

- 0 Recent
- 1 Current
- 1 Peak
- 1 Session

NanoCore

Identity Country Ping CPU RAM Idle Time Active Window Up Time Note IP Address Port OS Name OS Bits R...

Identity	Country	Ping	CPU	RAM	Idle Time	Active Window	Up Time	Note	IP Address	Port	OS Name	OS Bits	R...
Default													
Victim	United Ki...	0ms	13%	51%	Not idle	[NanoCore] NanoCor...	00:00:30		127.0.0.1	54984	Windows 10 Pro	64-bit	Us

Context Menu for 'Victim':

- Connection
- System
- Organize
- Manage
 - File Browser..
 - Task Manager..
 - Registry Editor..
 - Remote Console..
- Misc
- MultiCore
- Swiss Army Knife
- Tools
- NanoNana
- Network
- Surveillance
- Settings

weivesecurity

Total: 1 Selected: 1

Covenant



- <https://github.com/cobbr/Covenant>

C-OVENANT Welcome, cobbr! Logout

Dashboard

Grunts

Name	CommType	Hostname	UserName	Status	LastCheckIn	Integrity	OperatingSystem	Process
176a56f1c8	SMB	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:21:46 PM	High	Microsoft Windows NT 10.0.17134.0	powershell
31f991ef6c	HTTP	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:49:18 PM	High	Microsoft Windows NT 10.0.17134.0	powershell
514c08cc97	SMB	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:16:21 PM	High	Microsoft Windows NT 10.0.17134.0	powershell
b564dcaa12	HTTP	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:49:15 PM	High	Microsoft Windows NT 10.0.17134.0	powershell

Showing 1 to 4 of 4 entries

Listeners

Name	ListenerType	Status	StartTime	BindAddress	BindPort
62eb6bd841	HTTP	Active	7/18/19 8:57:55 PM	0.0.0.0	80

Taskings

Name	Grunt	Task	Status	UserName	Command	CommandTime	CompletionTime
0903d01960	176a56f1c8	LogonPasswords	Completed	cobbr	LogonPasswords	7/18/19 9:21:11 PM	7/18/19 9:21:21 PM
2c72b6e1ce	31f991ef6c	Connect	Progressed	cobbr	connect localhost gruntsvc	7/18/19 9:08:25 PM	1/1/01 12:00:00 AM
331eedd16c	176a56f1c8	PowerShell	Completed	cobbr	powershell \$PSVersionTable	7/18/19 9:21:26 PM	7/18/19 9:21:30 PM
4f2dc6f195	514c08cc97	WhoAmI	Completed	cobbr	whoami	7/18/19 9:16:07 PM	7/18/19 9:16:10 PM

Infection Vector

Infection vector

Email Attachments:

Viruses can be attached to emails as files (e.g., .exe, .doc, .pdf) that, when opened, execute malicious code.

Malicious Websites:

Visiting compromised or malicious websites can lead to drive-by downloads, where viruses are automatically downloaded and installed without the user's knowledge.

USB Drives and External Storage:

Viruses can spread through infected USB drives, external hard drives, and other removable media. When these devices are connected to a computer, the virus can execute and infect the system.

Software Downloads:

Downloading software from untrusted sources can result in the installation of viruses. This includes pirated software, cracked versions, and even legitimate-looking but malicious applications.

Infection vector

Social Engineering:

Attackers use psychological manipulation to trick users into performing actions that compromise security, such as clicking on malicious links or downloading infected files.

Phishing:

Phishing attacks use deceptive emails or websites to trick users into providing sensitive information or downloading malware.

Instant Messaging and Chat Applications:

Viruses can be spread through infected files shared via instant messaging platforms or chat applications.

Supply Chain Attacks:

Attackers compromise software or hardware at some point in the supply chain, allowing them to distribute malware to end-users.

Phishing

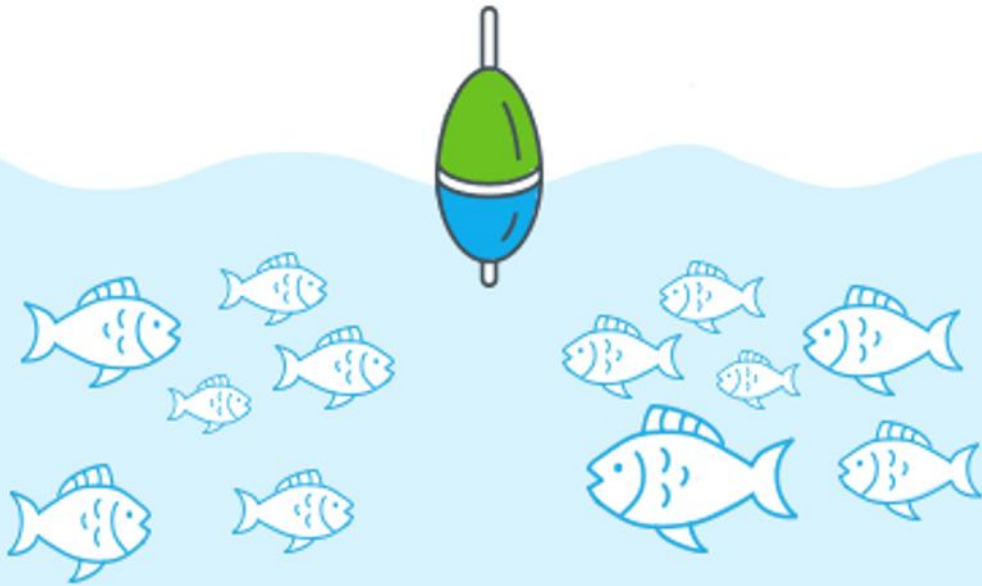
- Is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.
- Attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
- The recipient is then tricked into clicking a malicious link.



Spear phishing

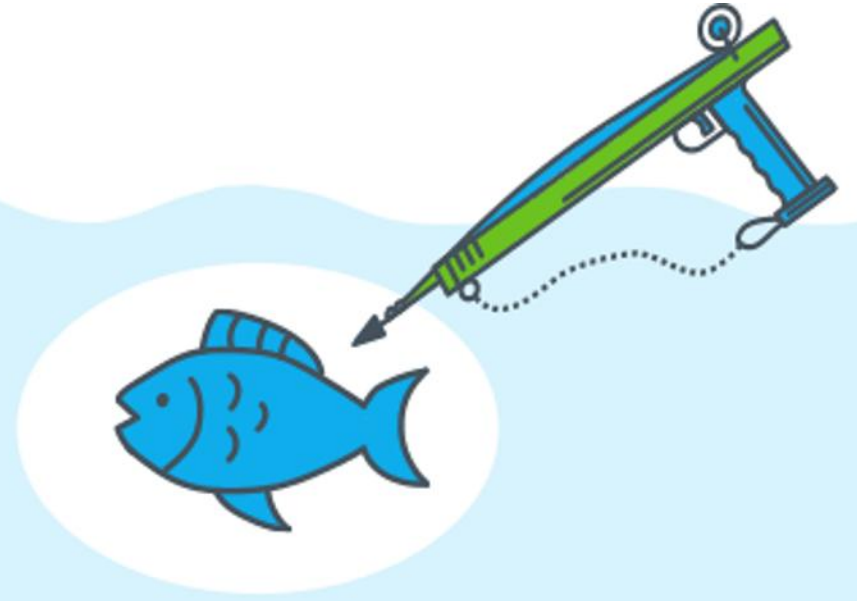
- Is a targeted and highly personalized form of phishing attack.
- Designed to trick a specific individual or organization into revealing sensitive information or performing actions that benefit the attacker.
- Unlike generic phishing attacks that cast a wide net, spear phishing is meticulously crafted to deceive a particular victim, making it more effective and dangerous.

Spear phishing



PHISHING

IS A BROAD, AUTOMATED ATTACK
THAT IS LESS SOPHISTICATED.



SPEAR-PHISHING

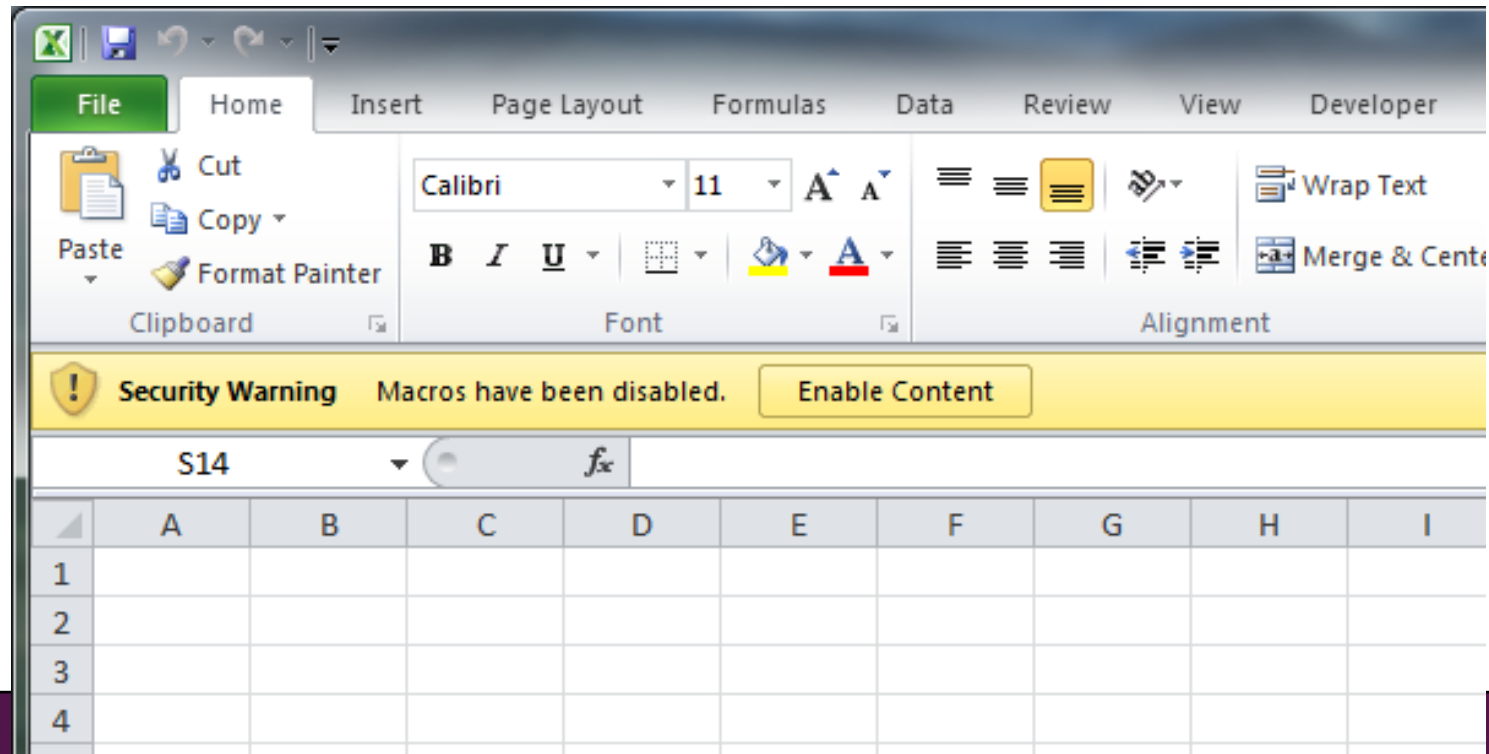
IS A CUSTOMIZED ATTACK ON A SPECIFIC
EMPLOYEE & COMPANY

Phishing test

- <https://phishingquiz.withgoogle.com>
- <https://www.phishingbox.com/phishing-test>

Office Macro

- Office macro phishing is a type of phishing attack that leverages macros in Microsoft Office applications (such as Word, Excel, and PowerPoint) to deliver malware or steal sensitive information.
- Macros are automated scripts that can perform repetitive tasks, but they can also be exploited by attackers to execute malicious code.

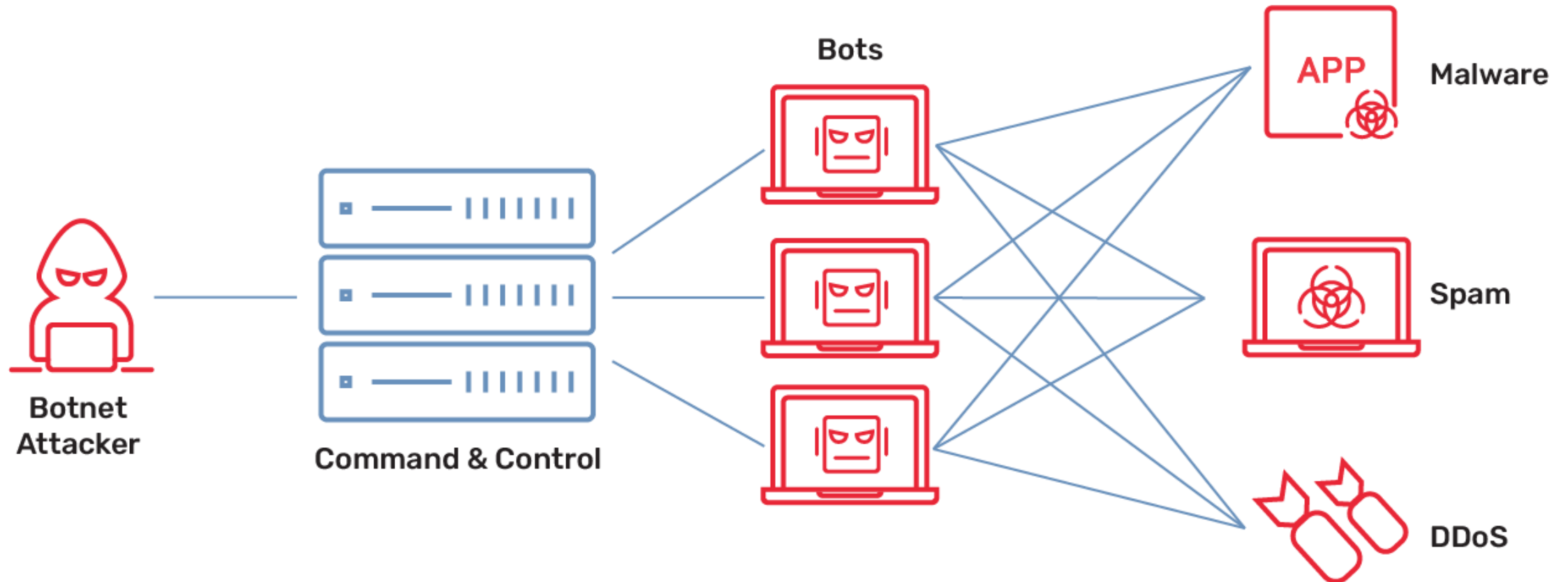


Bots and Botnets

Definition 23–15. A *bot* is malware that carries out some action in coordination with other bots. The attacker, called a *botmaster*, controls the bots from one or more systems called *command and control (C&C) servers* or *motherships*. They communicate over paths called *C&C channels*. A collection of bots is a *botnet*.

Bots and Botnets

- Command and Control (C&C) Server



Hackers

Hacker

- The term "hacker" was used to describe individuals who enjoyed exploring the details of programmable systems and stretching their capabilities.

White, gray and black hat comparison



WHITE HAT

Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws



GRAY HAT

May have good intentions, but might not disclose flaws for immediate fixes

.....
Prioritize their own perception of right versus wrong over what the law might say



BLACK HAT

Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong

.....
Exploit security flaws for personal or political gain—or for fun

Who are you?

White, gray and black hat comparison



WHITE HAT

Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws



GRAY HAT

May have good intentions, but might not disclose flaws for immediate fixes

.....

Prioritize their own perception of right versus wrong over what the law might say



BLACK HAT

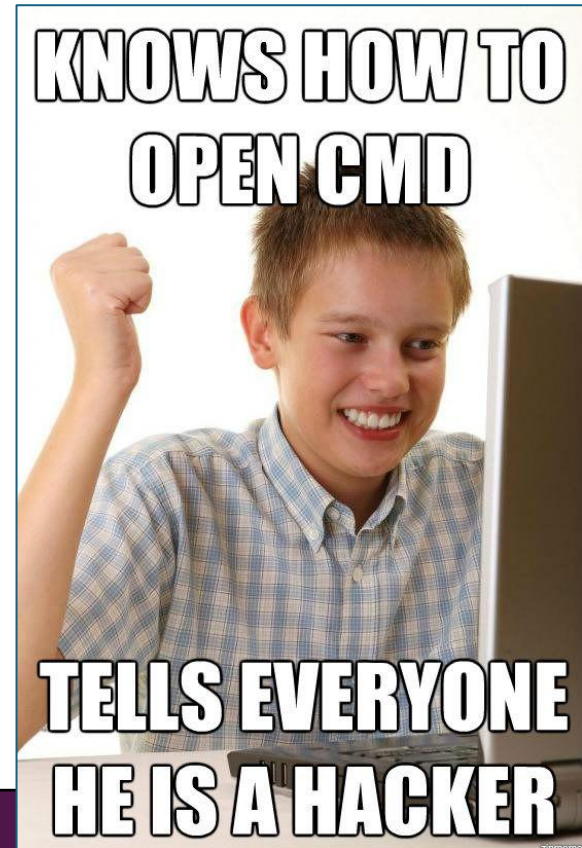
Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong

.....

Exploit security flaws for personal or political gain—or for fun

Script Kiddies

- These are individuals with limited technical skills who use pre-written scripts and tools to launch attacks. They often lack a deep understanding of how the tools work.
- To cause disruption or gain attention, often without a clear understanding of the consequences.
- Using readily available hacking tools and scripts.



Hacktivists

- Hacktivists use hacking techniques to promote political or social causes. They may deface websites, leak sensitive information, or launch DDoS attacks to draw attention to their cause.
- Political or social activism.
- Website defacement, data leaks, DDoS attacks.



APT Hacker

- **State-Sponsored Hackers**

- These hackers are backed by governments and engage in cyber espionage, sabotage, or other malicious activities to achieve national objectives.
- National security, economic advantage, or political gain.
- Advanced persistent threats (APTs), cyber espionage, and cyber warfare.



CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

Defense

Antivirus

- **Signature-Based Antivirus:** This is the most common type of antivirus software.
- It detects malware by comparing files against a database of known malware signatures.
- If a file matches a signature, it is flagged as malicious.
- **Behavioral-Based Antivirus:** this type monitors the behavior of programs in real-time.
- If a program behaves suspiciously e.g., trying to access sensitive files or making unauthorized changes, it is flagged as a potential threat.

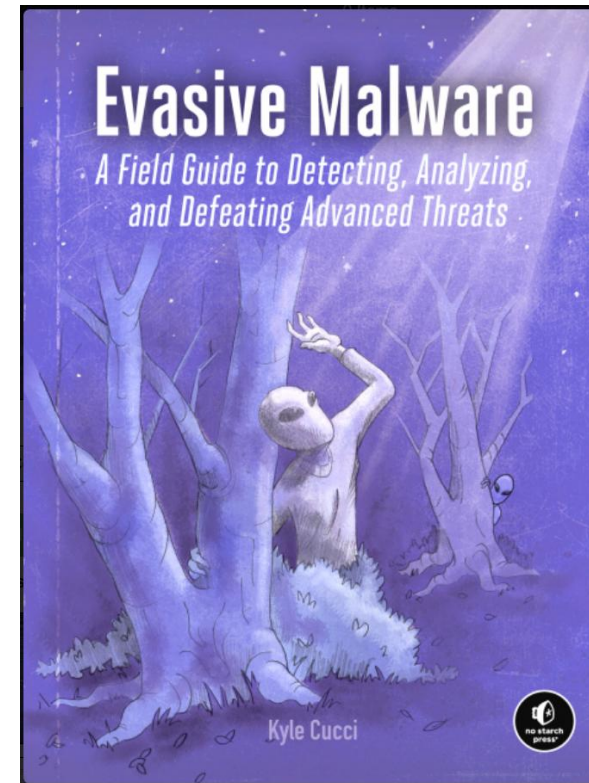
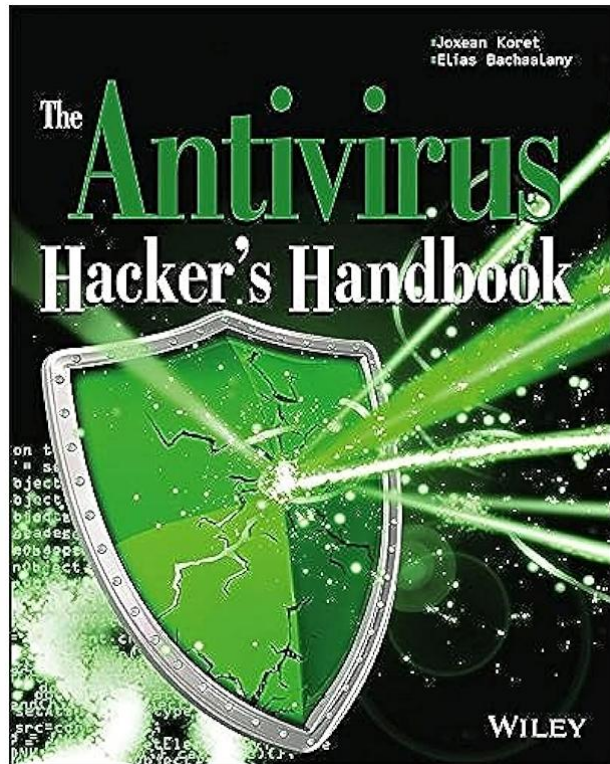
Antivirus

- **Cloud-Based Antivirus:** This type leverages cloud computing to analyze and store data. It can quickly update its database with the latest threats and offload some of the processing from the user's device to the cloud, improving performance.
- **Endpoint Protection:** This is a more comprehensive solution that not only includes antivirus capabilities but also offers additional security features like firewalls, intrusion detection systems, and data loss prevention. It is often used in corporate environments.



FUD

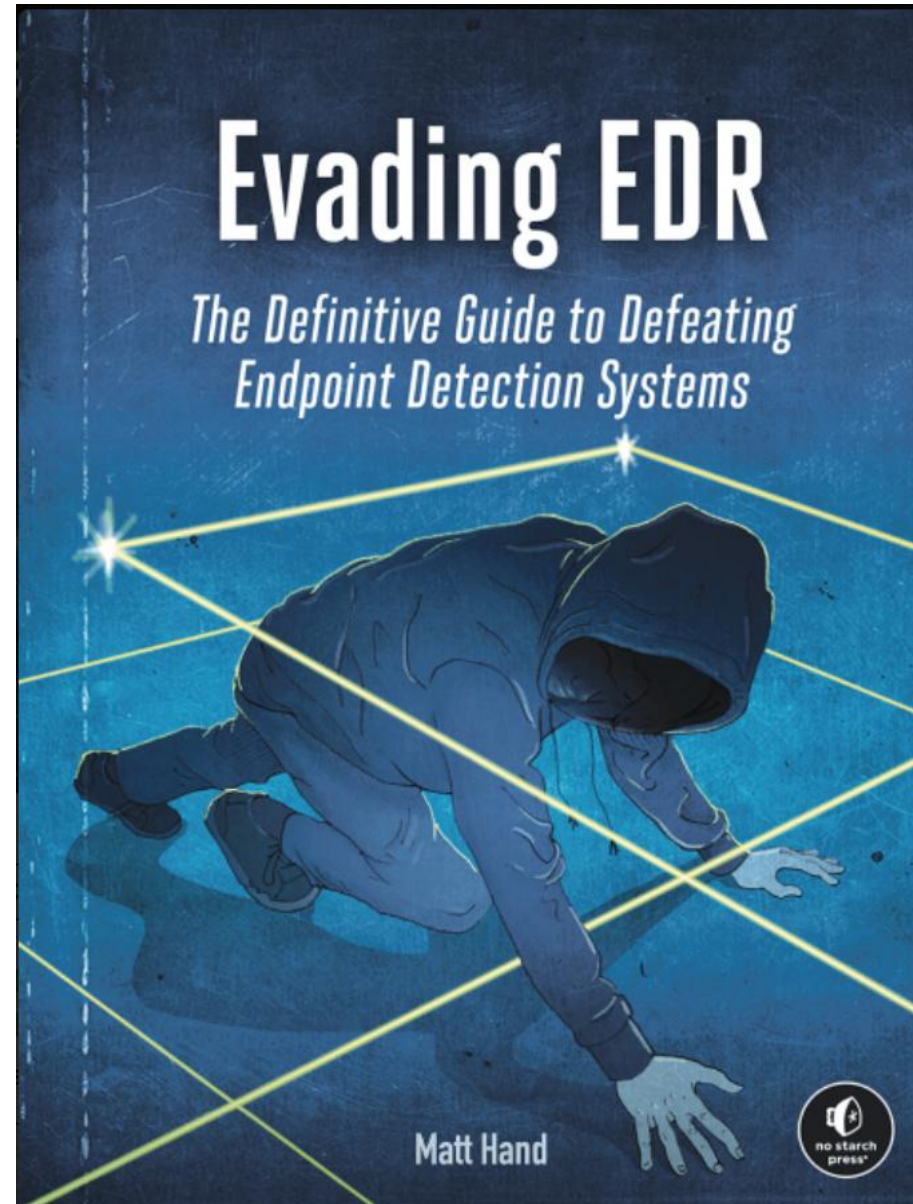
- FUD malware stands for "Fully UnDetectable" malware.
- It refers to malicious software that is designed to evade detection by antivirus programs and other security measures



Endpoint Protection

- EDR: Endpoint Detection and Response
- Is a cybersecurity technology that continuously monitors endpoints for evidence of threats and performs automatic actions to help mitigate them.
- XDR, MDR, ...

- ☹️



What we can do?



What we can do?



12 angry men - 1957

