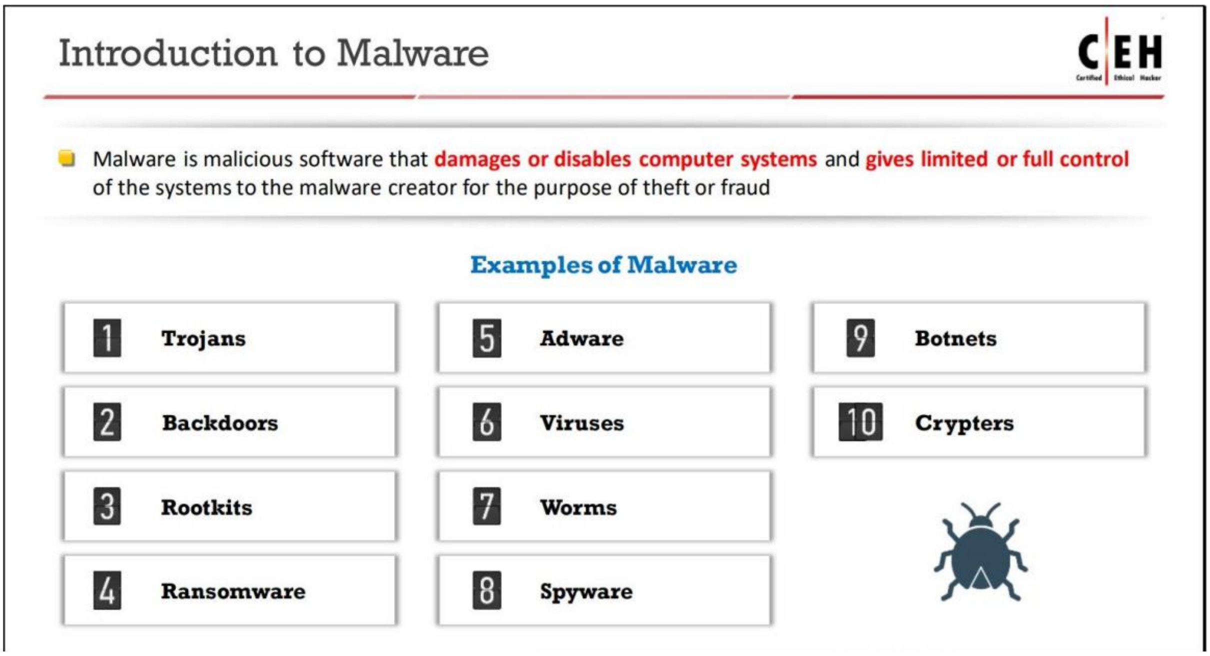
Malware Threats



Introduction to Malware

- Malware is 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

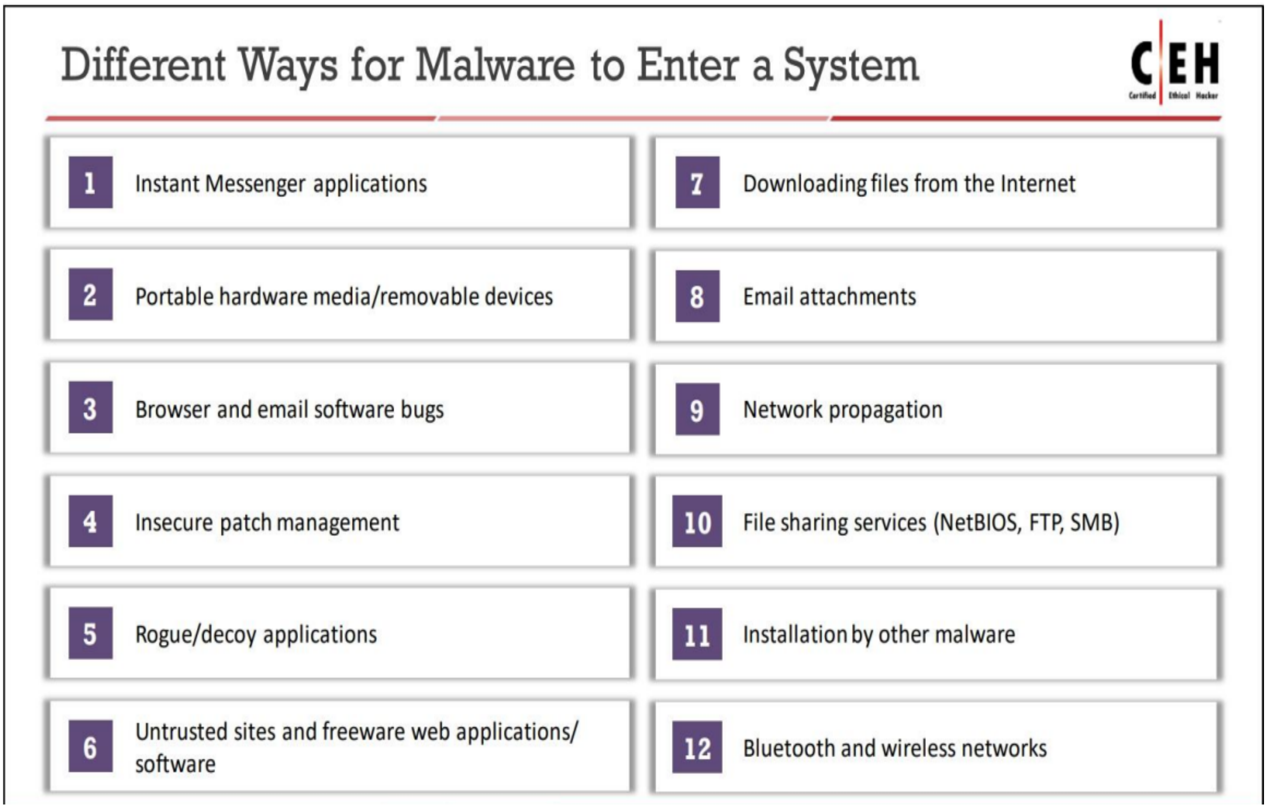
Examples of Malware

1. Trojans
2. Backdoors
3. Rootkits
4. Ransomware
5. Adware
6. Viruses
7. Worms
8. Spyware
9. Botnets
10. Crypters

Malware is a software that gets into the system without user consent with an intention to steal private and confidential data of the user that includes bank details and password. They also generate annoying pop-up ads and makes changes in system settings.

They get into the system through various means:

1) Along with free downloads.
2) Clicking on suspicious link.
3) Opening mails from malicious source.
4) Visiting malicious websites.
5) Not installing an updated version of antivirus in the system.



Different Ways for Malware to Enter a System

1 Instant Messenger applications

2 Portable hardware media/removable devices

3 Browser and email software bugs

4 Insecure patch management

5 Rogue/decoy applications

6 Untrusted sites and freeware web applications/ software

7 Downloading files from the Internet

8 Email attachments

9 Network propagation

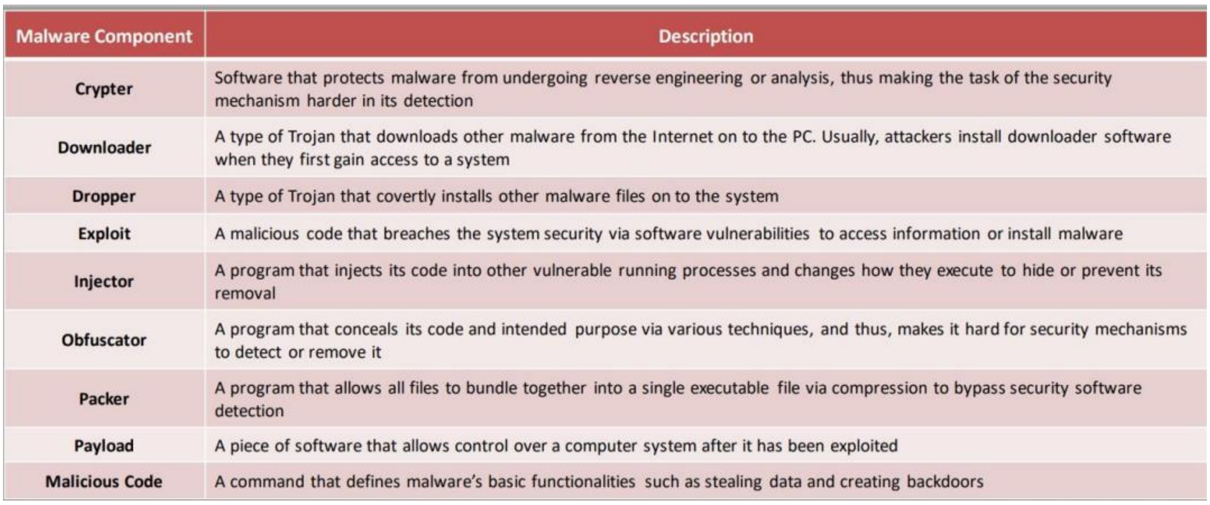
10 File sharing services (NetBIOS, FTP, SMB)

11 Installation by other malware

12 Bluetooth and wireless networks

Purpose of Malware

1. To steal passwords
2. To steal personal data
3. Banking info
4. Revenge
5. Spy
6. To delete sensitive data
7. To hijacking into computer



Malware Component	Description
Crypter	Software that protects malware from undergoing reverse engineering or analysis, thus making the task of the security mechanism harder in its detection
Downloader	A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system
Dropper	A type of Trojan that covertly installs other malware files on to the system
Exploit	A malicious code that breaches the system security via software vulnerabilities to access information or install malware
Injector	A program that injects its code into other vulnerable running processes and changes how they execute to hide or prevent its removal
Obfuscator	A program that conceals its code and intended purpose via various techniques, and thus, makes it hard for security mechanisms to detect or remove it
Packer	A program that allows all files to bundle together into a single executable file via compression to bypass security software detection
Payload	A piece of software that allows control over a computer system after it has been exploited
Malicious Code	A command that defines malware's basic functionalities such as stealing data and creating backdoors

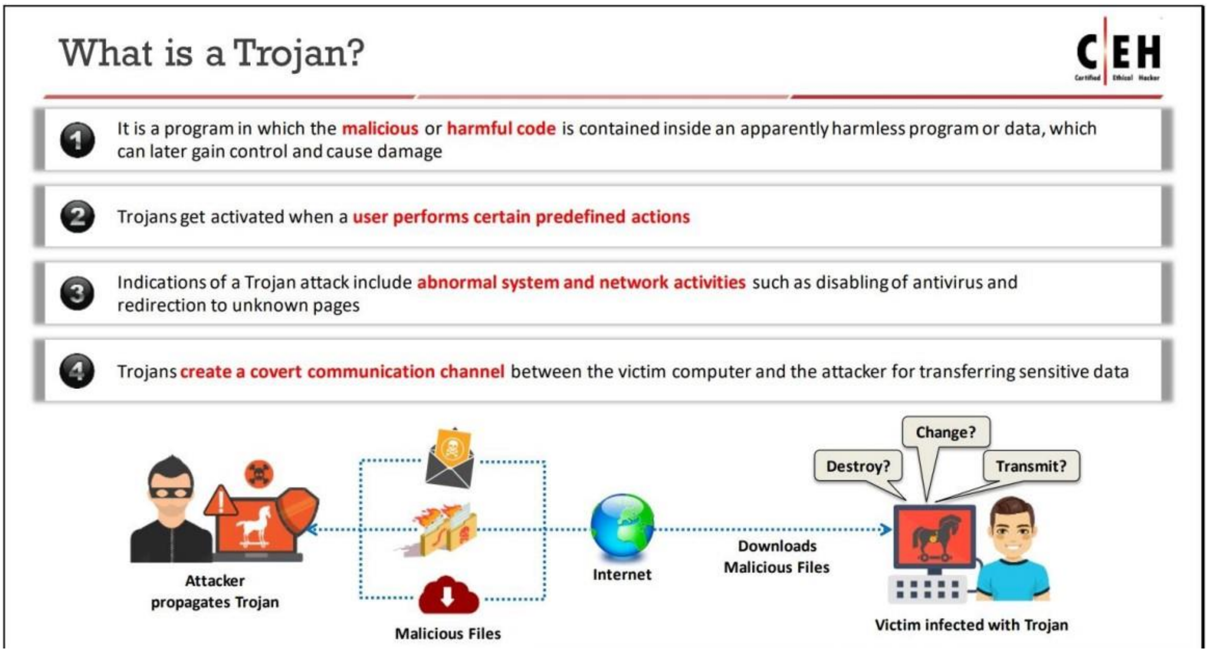
Types of Malwares

1. Computer virus **-** Computer virus refers to a program which damages computer systems and/or destroys or erases data files. A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, steal user sensitive data. Hackers design computer viruses with malicious intent and spray on online users by tricking them.

2. Worm – A worm is a destructive program that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped**.** Types of Worms - Email worm, Internet worm and Payloads.

3. Logic Bomb - A logical bomb is a destructive program that performs an activity when a certain action has occurred. These are hidden in programming code. Executes only when a specific condition is met, e.g. Jerusalem.

4. Trojan - Trojan is a destructive program. It usually pretends as computer games or application software. If executed, the computer system will be damaged. Trojan Horse usually comes with monitoring tools and key loggers. These are active only when specific events are alive. These are hidden with packers, crypters and wrappers.



What is a Trojan?

CEH

1. It is a program in which the **malicious** or **harmful code** is contained inside an apparently harmless program or data, which can later gain control and cause damage
2. Trojans get activated when a **user performs certain predefined actions**
3. Indications of a Trojan attack include **abnormal system and network activities** such as disabling of antivirus and redirection to unknown pages
4. Trojans **create a covert communication channel** between the victim computer and the attacker for transferring sensitive data

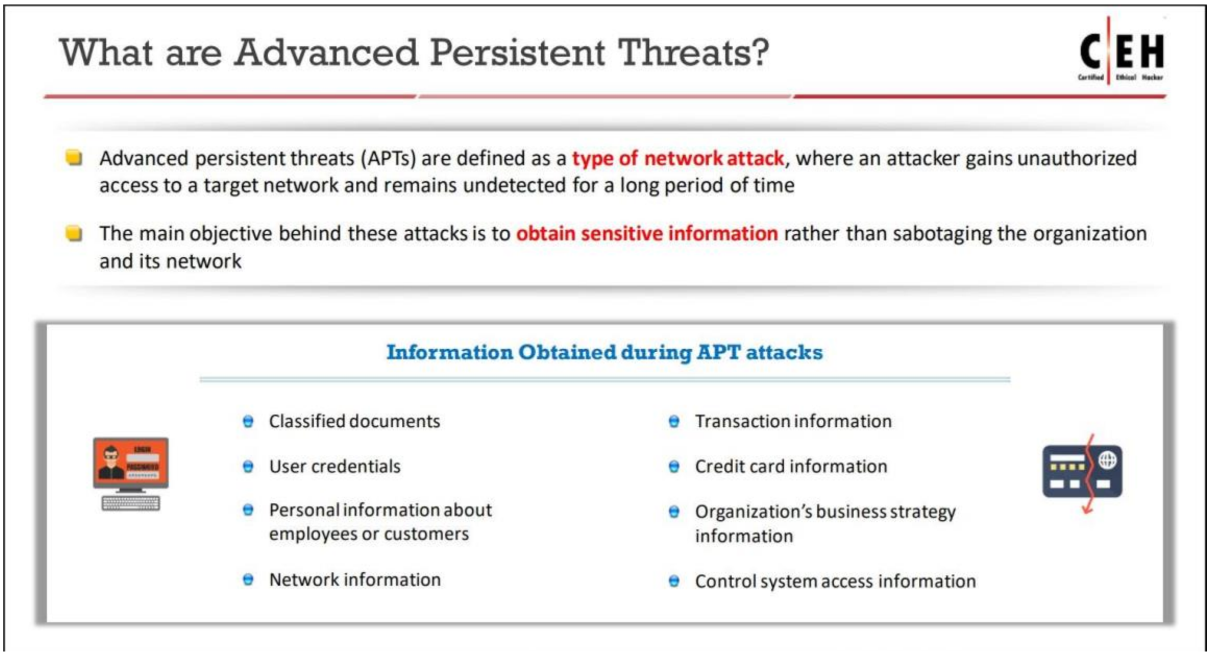
Attacker propagates Trojan
Malicious Files
Internet
Downloads Malicious Files
Change?
Destroy?
Transmit?
Victim infected with Trojan

5. Rootkit - Collection of tools that allow an attacker to take control of a system.

- Can be used to hide evidence of an attacker’s presence and give them backdoor access.
- Can contain log cleaners to remove traces of attacker.

6. Advanced Persistent Threat – An advanced persistent threat (APT) is a covert cyber-attack on a computer network where

the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period. During the time between infection and remediation the hacker will often monitor, intercept, and relay information and sensitive data.



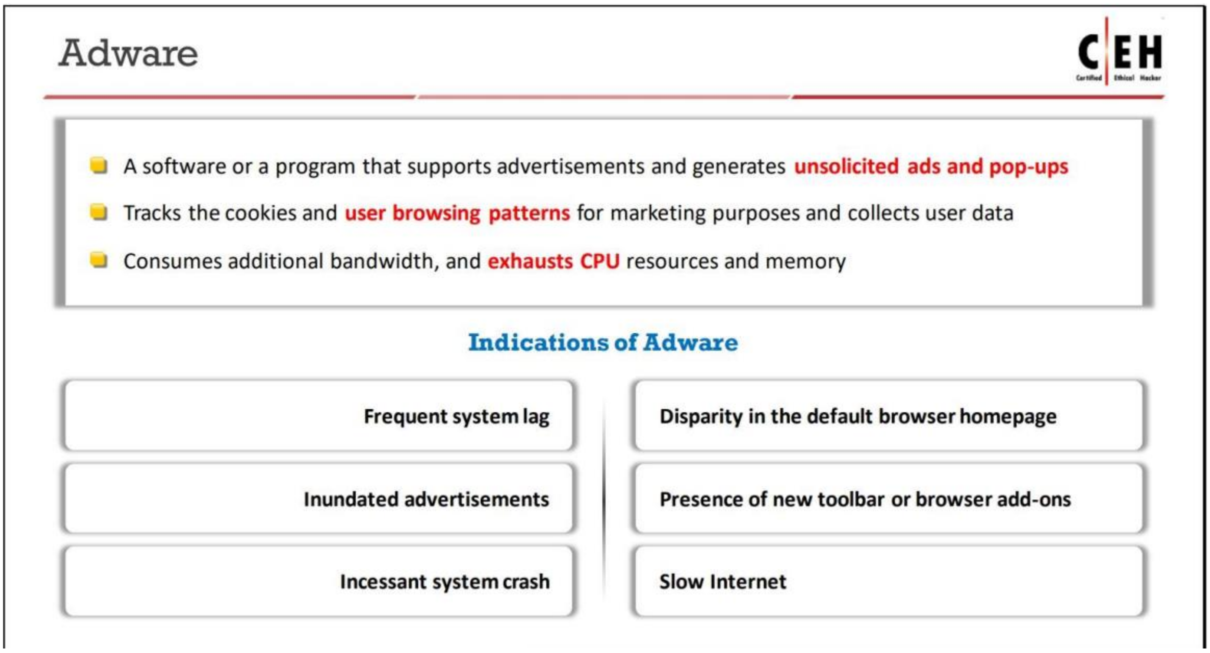
What are Advanced Persistent Threats?

- Advanced persistent threats (APTs) are defined as a **type of network attack**, where an attacker gains unauthorized access to a target network and remains undetected for a long period of time
- The main objective behind these attacks is to **obtain sensitive information** rather than sabotaging the organization and its network

Information Obtained during APT attacks

- Classified documents
- User credentials
- Personal information about employees or customers
- Network information
- Transaction information
- Credit card information
- Organization's business strategy information
- Control system access information

7. Adware – Adware, a contraction of 'advertising-supported software', displays unwanted and sometimes malicious advertising on a computer screen or mobile device, redirects search results to advertising websites, and captures user data that can be sold to advertisers without the user's consent.



Adware

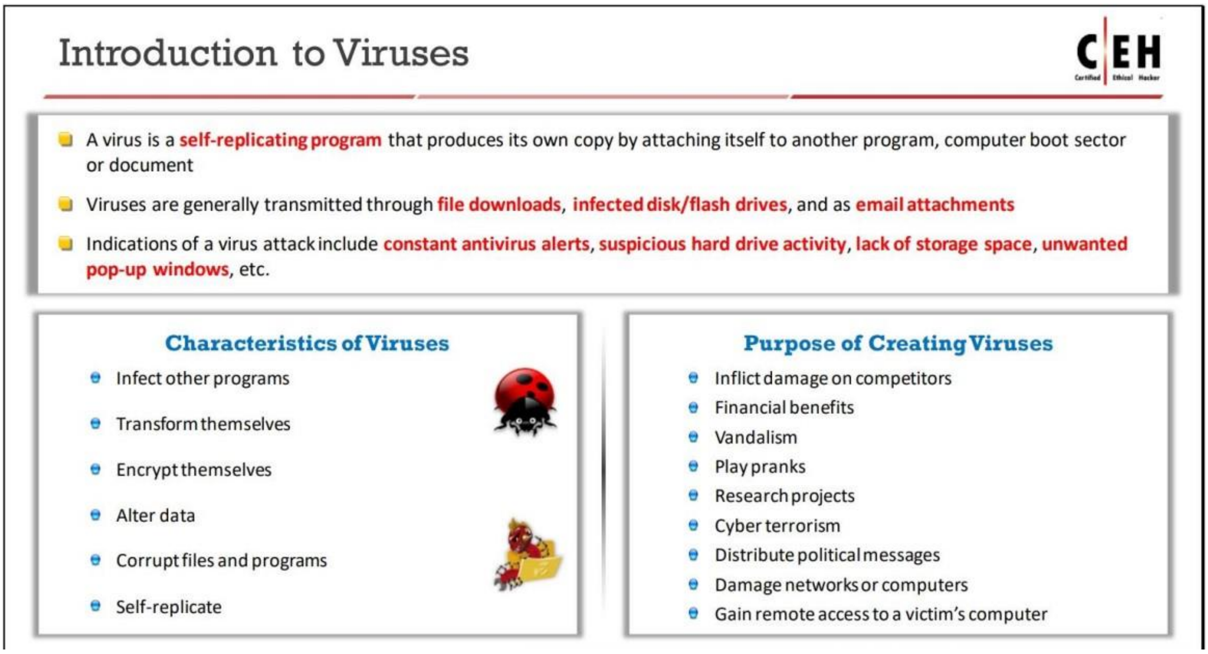
- A software or a program that supports advertisements and generates **unsolicited ads and pop-ups**
- Tracks the cookies and **user browsing patterns** for marketing purposes and collects user data
- Consumes additional bandwidth, and **exhausts CPU** resources and memory

Indications of Adware

Frequent system lag	Disparity in the default browser homepage
Inundated advertisements	Presence of new toolbar or browser add-ons
Incessant system crash	Slow Internet

8. Spyware – Spyware is a form of malware that hides on your device, monitors activity, and steals sensitive information like financial data, account information, logins, and more. Spyware can spread by exploiting software vulnerabilities or else be bundled with legitimate software or in Trojans.

Virus



Introduction to Viruses

CEH
Certified Ethical Hacker

- A virus is a **self-replicating program** that produces its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through **file downloads**, **infected disk/flash drives**, and as **email attachments**
- Indications of a virus attack include **constant antivirus alerts**, **suspicious hard drive activity**, **lack of storage space**, **unwanted pop-up windows**, etc.

Characteristics of Viruses

- Infect other programs
- Transform themselves
- Encrypt themselves
- Alter data
- Corrupt files and programs
- Self-replicate

Purpose of Creating Viruses

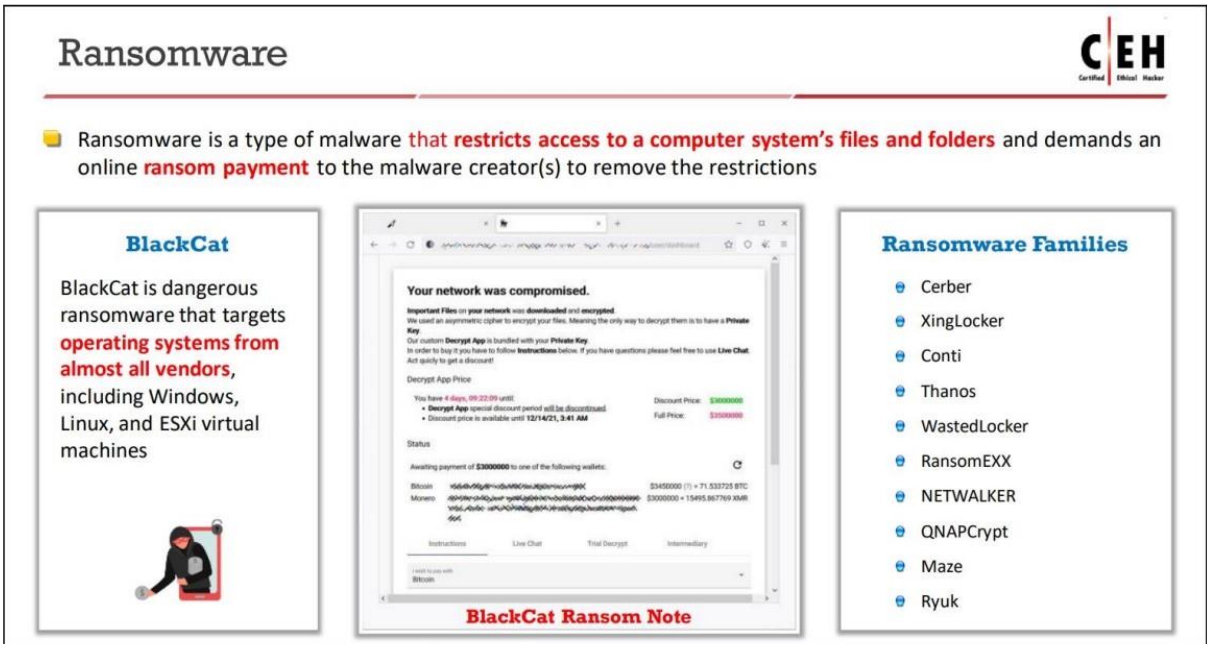
- Inflict damage on competitors
- Financial benefits
- Vandalism
- Play pranks
- Research projects
- Cyber terrorism
- Distribute political messages
- Damage networks or computers
- Gain remote access to a victim's computer

Viruses are the storage of modern computing. A computer virus is a type of malicious computer program that replicates itself and adds its own code when executed. When the replication process is complete, this code infects the other files and programs on your system. These computer viruses exist in a variety of types, and each of them can infect a device in a unique way.

Ransomware

Ransomware is a type of malware that permanently block access to the victim's personal data unless a ransom is paid.

While some simple ransomware may lock the system without damaging any files.



Ransomware

CEH Certified Ethical Hacker

- Ransomware is a type of malware **that restricts access to a computer system's files and folders** and demands an online **ransom payment** to the malware creator(s) to remove the restrictions

BlackCat

BlackCat is dangerous ransomware that targets **operating systems from almost all vendors**, including Windows, Linux, and ESXi virtual machines

[redacted]

Your network was compromised.

Important Files on **your network** was **downloaded** and **encrypted**.
We used an asymmetric cipher to encrypt your files. Meaning the only way to decrypt them is to have a **Private Key**.
Our custom **Decrypt App** is bundled with your **Private Key**.
In order to buy it you have to follow **Instructions** below. If you have questions please feel free to use **Live Chat**.
Act quicly to get a discount!

Decrypt App Price

You have 4 days, 09:22:09 until:
- **Decrypt App** special discount period will be discontinued
- Discount price is available until **12/14/21, 3:41 AM**

Discount Price: $3000000
Full Price: $3500000

Status

Awaiting payment of **$3000000** to one of the following wallets:

Bitcoin [redacted] $3450000 (?) = 71.533725 BTC
Monero [redacted] $3000000 = 15495.867769 XMR

BlackCat Ransom Note

Ransomware Families

- Cerber
- XingLocker
- Conti
- Thanos
- WastedLocker
- RansomEXX
- NETWALKER
- QNAPCrypt
- Maze
- Ryuk