


Malware Concepts


To understand the various types of malware and their impact on network and system resources, we will begin with a discussion of the basic concepts of malware. This section describes malware and highlights the common techniques used by attackers to distribute malware on the web.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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 malicious activities such as theft or fraud. Malware includes viruses, worms, Trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, etc. These may delete files, slow down computers, steal personal information, send spam, or commit fraud. Malware can perform various malicious activities ranging from simple email advertising to complex identity theft and password stealing.

Malware programmers develop and use malware to:

- Attack browsers and track websites visited
- Slow down systems and degrade system performance
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data loss
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Different Ways for Malware to Enter a System



1 Instant Messenger applications	7 Downloading files from the Internet
2 Portable hardware media/removable devices	8 Email attachments
3 Browser and email software bugs	9 Network propagation
4 Insecure patch management	10 File sharing services (NetBIOS, FTP, SMB)
5 Rogue/decoy applications	11 Installation by other malware
6 Untrusted sites and freeware web applications/ software	12 Bluetooth and wireless networks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Different Ways for Malware to Enter a System

- **Instant Messenger Applications**

Infection can occur via instant messenger applications such as Facebook Messenger, WhatsApp Messenger, LinkedIn Messenger, Google Hangouts, or ICQ. Users are at high risk while receiving files via instant messengers. Regardless of who sends the file or from where it is sent, there is always a risk of infection by a Trojan. The user can never be 100% sure of who is at the other end of the connection at any particular moment. For example, if you receive a file through an instant messenger application from a known person such as Bob, you will try to open and view the file. This could be a trick whereby an attacker who has hacked Bob's messenger ID and password wants to spread Trojans across Bob's contacts list to trap more victims.

- **Portable Hardware Media/Removable Devices**

- Portable hardware media such as flash drives, CDs/ DVDs, and external hard drives can also inject malware into a system. A simple way of injecting malware into the target system is through physical access. For example, if Bob can access Alice's system in her absence, then he can install a Trojan by copying the Trojan software from his flash drive onto her hard drive.
- Another means of portable media malware infection is through the Autorun function. Autorun, also referred to as Autoplay or Autostart, is a Windows feature that, if enabled, runs an executable program when a user inserts a CD/DVD in the DVD-ROM tray or connects a USB device. Attackers can exploit this feature to run malware along with genuine programs. They place an Autorun.inf file with the malware in a CD/DVD or USB device and trick people into inserting or plugging it into

their systems. Because many people are not aware of the risks involved, their machines are vulnerable to Autorun malware. The following is the content of an Autorun.inf file:

```
[autorun]
open=setup.exe
icon=setup.exe
```

To mitigate such infection, turn off the Autostart functionality. Follow the instructions below to turn off Autoplay in Windows 10:

1. Click **Start**. Type **gpedit.msc** in the **Start Search** box, and then press **ENTER**.
 2. If you are prompted for an administrator password or confirmation, type the password, or click **Allow**.
 3. Under **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Autoplay Policies**.
 4. In the **Details** pane, double-click **Turn off Autoplay**.
 5. Click **Enabled**, and then select **All drives** in the **Turn off Autoplay** box to disable Autorun on all drives.
 6. **Restart** the computer.
- **Browser and Email Software Bugs**

Outdated web browsers often contain vulnerabilities that can pose a major risk to the user's computer. A visit to a malicious site from such browsers can automatically infect the machine without downloading or executing any program. The same scenario occurs while checking e-mail with Outlook Express or some other software with well-known problems. Again, it may infect the user's system without even downloading an attachment. To reduce such risks, always use the latest version of the browser and e-mail software.
 - **Insecure Patch management**

Unpatched software poses a high risk. Users and IT administrators do not update their application software as often as they should, and many attackers take advantage of this well-known fact. Attackers can exploit insecure patch management by injecting the software with malware that can damage the data stored on the company's systems. This process can lead to extensive security breaches, such as stealing of confidential files and company credentials. Some applications that were found to be vulnerable and were patched recently include Microsoft Office (CVE-2019-1084), .NET Framework (CVE-2019-1083), Microsoft Exchange Server (CVE-2019-1136), Microsoft Graphics Component (CVE-2019-1118), Docker flaw in Azure (CVE-2018-15664), Microsoft SQL Server RCE (CVE-2019-1068), and RDP RCE (CVE-2019-0887). Patch management must be effective in mitigating threats, and it is vital to apply patches and regularly update software programs.

- **Rogue/Decoy Applications**

Attackers can easily lure a victim into downloading free applications/programs. If a free program claims to be loaded with features such as an address book, access to several POP3 accounts, and other functions, many users will be tempted to try it. POP3 (Post Office Protocol version 3) is an email transfer protocol.

- If a victim downloads free programs and labels them as TRUSTED, protection software such as antivirus software will fail to indicate the use of new software. In this situation, an attacker receives an email, POP3 account passwords, cached passwords, and keystrokes through email without being noticed.
- Attackers thrive on creativity. Consider an example in which an attacker creates a fake website (say, Audio galaxy) for downloading MP3s. He or she could generate such a site using 15 GB of space for the MP3s and installing any other systems needed to create the illusion of a website. This can fool users into thinking that they are merely downloading from other network users. However, the software could act as a backdoor and infect thousands of naive users.
- Some websites even link to anti-Trojan software, thereby fooling users into trusting them and downloading infected freeware. Included in the setup is a readme.txt file that can deceive almost any user. Therefore, any freeware site requires proper attention before any software is downloaded from it.
- Webmasters of well-known security portals, who have access to vast archives containing various hacking programs, should act responsibly with regard to the files they provide and scan them often with antivirus and anti-Trojan software to guarantee that their site is free of Trojans and viruses. Suppose that an attacker submits a program infected with a Trojan (e.g., a UDP flooder) to an archive's webmaster. If the webmaster is not alert, the attacker may use this opportunity to infect the files on the site with the Trojan. Users who deal with any software or web application should scan their systems daily. If they detect any new file, it is essential to examine it. If any suspicion arises regarding the file, it is also important to forward it to software detection labs for further analysis.
- It is easy to infect machines using freeware; thus, extra precautions are necessary.

- **Untrusted Sites and Free Web Applications/Software**

A website could be suspicious if it is located at a free website provider or one offering programs for illegal activities.

- It is highly risky to download programs or tools located on "underground" sites, e.g., NeuroticKat software, because they can serve as a conduit for a Trojan attack on target computers. Users must assess the high risk of visiting such sites before browsing them.
- Many malicious websites have a professional look, massive archives, feedback forums, and links to other popular sites. Users should scan the files using antivirus

software before downloading them. Just because a website looks professional does not mean that it is safe.

- Always download popular software from its original (or officially dedicated mirror) site, and not from third-party sites with links to the (supposedly) same software.

- **Downloading Files from the Internet**

Trojans enter a system when users download Internet-driven applications such as music players, files, movies, games, greeting cards, and screensavers from malicious websites, thinking that they are legitimate. Microsoft Word and Excel macros are also used effectively to transfer malware, and downloaded malicious MS Word/Excel files can infect systems. Malware can also be embedded in audio/video files as well as in video subtitle files.

- **Email Attachments**

An attachment to an e-mail is the most common medium to transmit malware. The attachment can be in any form, and the attacker uses innovative ideas to trick the victim into clicking and downloading the attachment. The attachment may be a document, audio file, video file, brochure, invoice, lottery offer letter, job offer letter, loan approval letter, admission form, contract approval, etc.

Example 1: A user's friend is conducting some research, and the user would like to know more about the friend's research topic. The user sends an e-mail to the friend to inquire about the topic and waits for a reply. An attacker targeting the user also knows the friend's e-mail address. The attacker will merely code a program to falsely populate the e-mail "From:" field and attach a Trojan in the email. The user will check the email and think that the friend has answered the query in an attachment, download the attachment, and run it without thinking it might be a Trojan, resulting in an infection.

Some email clients, such as Outlook Express, have bugs that automatically execute attached files. To avoid such attacks, use secure email services, investigate the headers of emails with attachments, confirm the sender's email address, and download the attachment only if the sender is legitimate.

- **Network Propagation**

Network security is the first line of defense for protecting information systems from hacking incidents. However, various factors such as the replacement of network firewalls and mistakes of operators may sometimes allow unfiltered Internet traffic into private networks. Malware operators continuously attempt connections to addresses within the Internet address range owned by targets to seek an opportunity for unfettered access. Some malware propagates through technological networks. For example, the Blaster starts from a local machine's IP address or a completely random address and attempts to infect sequential IP addresses. Although network propagation attacks that take advantage of vulnerabilities in common network protocols (e.g., SQL Slammer) have not been prevalent recently, the potential for such attacks still exists.

- **File Sharing**

If NetBIOS (Port 139), FTP (Port 21), SMB (Port 145), etc., on a system are open for file sharing or remote execution, they can be used by others to access the system. This can allow attackers to install malware and modify system files.


Attackers can also use a DoS attack to shut down the system and force a reboot so that the Trojan can restart itself immediately. To prevent such attacks, ensure that the file sharing property is disabled. To disable the file sharing option, click **Start** and type **Control Panel**. Then, in the results, click on the **Control Panel** option and navigate to **Network and Internet** → **Network and Sharing Center** → **Change Advanced Sharing Settings**. Select a network profile and under **File and Printer Sharing** section, select **Turn off file and printer sharing**. This will prevent file sharing abuse.

- **Installation by other Malware**

A piece of malware that can command and control will often be able to re-connect to the malware operator's site using common browsing protocols. This functionality allows malware on the internal network to receive both software and commands from the outside. In such cases, the malware installed on one system drives the installation of other malware on the network, thereby causing damage to the network.

- **Bluetooth and Wireless Networks**

Attackers use open Bluetooth and Wi-Fi networks to attract users to connect to them. These open networks have software and hardware devices installed at the router level to capture the network traffic and data packets as well as to find the account details of the users, including usernames and passwords.

Common Techniques Attackers Use to Distribute Malware on the Web		
Black hat Search Engine Optimization (SEO)	Ranking malware pages highly in search results	
Social Engineered Click-jacking	Tricking users into clicking on innocent-looking webpages	
Spear-phishing Sites	Mimicking legitimate institutions in an attempt to steal login credentials	
Malvertising	Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites	
Compromised Legitimate Websites	Hosting embedded malware that spreads to unsuspecting visitors	
Drive-by Downloads	Exploiting flaws in browser software to install malware just by visiting a web page	
Spam Emails	Attaching the malware to emails and tricking victims to click the attachment	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Techniques Attackers Use to Distribute Malware on the Web

Source: *Security Threat Report* (<http://www.sophos.com>)

Some standard techniques used to distribute malware on the web are as follows:

- **Black hat Search Engine Optimization (SEO):** Black hat SEO (also referred to as unethical SEO) uses aggressive SEO tactics such as keyword stuffing, inserting doorway pages, page swapping, and adding unrelated keywords to get higher search engine rankings for malware pages.
- **Social Engineered Click-jacking:** Attackers inject malware into websites that appear legitimate to trick users into clicking them. When clicked, the malware embedded in the link executes without the knowledge or consent of the user.
- **Spear-phishing Sites:** This technique is used for mimicking legitimate institutions, such as banks, to steal passwords, credit card and bank account data, and other sensitive information.
- **Malvertising:** This technique involves embedding malware-laden advertisements in legitimate online advertising channels to spread malware on systems of unsuspecting users.
- **Compromised Legitimate Websites:** Often, attackers use compromised websites to infect systems with malware. When an unsuspecting user visits the compromised website, he/she unknowingly installs the malware on his/her system, after which the malware performs malicious activities.

- **Drive-by Downloads:** This refers to the unintentional downloading of software via the Internet. Here, an attacker exploits flaws in browser software to install malware by merely visiting a website.
- **Spam Emails:** The attacker attaches a malicious file to an email and sends the email to multiple target addresses. The victim is tricked into clicking the attachment and thus executes the malware, thereby compromising his/her machine. This technique is the most common method currently in use by attackers. In addition to email attachments, an attacker may also use the email body to embed the malware.

Components of Malware



- The components of a malware software **depend on the requirements of the malware author** who designs it for a specific target to perform intended tasks

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

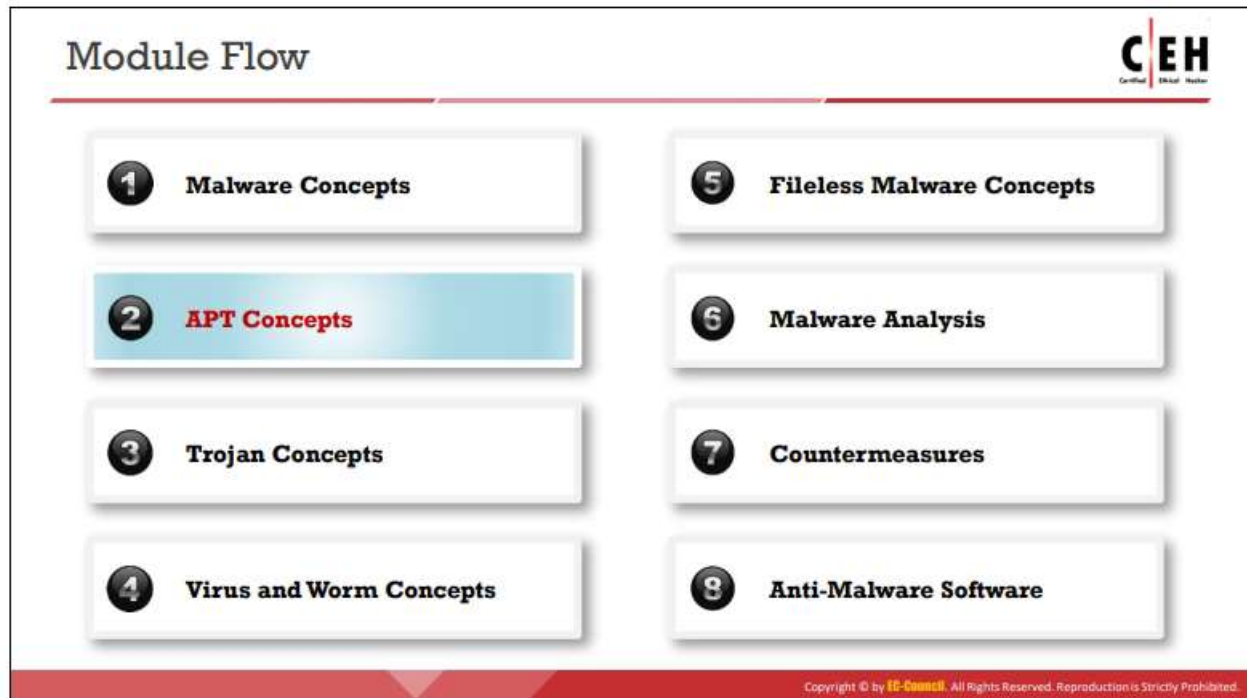
Components of Malware

Malware authors and attackers create malware using components that can help them achieve their goals. They can use malware to steal information, delete data, change system settings, provide access, or merely multiply and occupy space. Malware is capable of propagating and functioning secretly.

Some essential components of most malware programs are as follows:

- **Crypter:** It is a software program that can conceal the existence of malware. Attackers use this software to elude antivirus detection. It protects malware from reverse engineering or analysis, thus making it difficult to detect by security mechanisms.
- **Downloader:** It is a type of Trojan that downloads other malware (or) malicious code and files from the Internet to a PC or device. Usually, attackers install a downloader when they first gain access to a system.
- **Dropper:** It is a covert carrier of malware. Attackers embed notorious malware files inside droppers, which can perform the installation task covertly. Attackers need to first install the malware program or code on the system to execute the dropper. The dropper can transport malware code and execute malware on a target system without being detected by antivirus scanners.
- **Exploit:** It is the part the malware that contains code or a sequence of commands that can take advantage of a bug or vulnerability in a digital system or device. Attackers use such code to breach the system's security through software vulnerabilities to spy on information or to install malware. Based on the type of vulnerabilities abused, exploits are categorized into local exploits and remote exploits.

- **Injector:** This program injects exploits or malicious code available in the malware into other vulnerable running processes and changes the method of execution to hide or prevent its removal.
- **Obfuscator:** It is a program that conceals the malicious code of malware via various techniques, thus making it difficult for security mechanisms to detect or remove it.
- **Packer:** This software compresses the malware file to convert the code and data of the malware into an unreadable format. It uses compression techniques to pack the malware.
- **Payload:** It is the part of the malware that performs the desired activity when activated. It may be used for deleting or modifying files, degrading the system performance, opening ports, changing settings, etc., to compromise system security.
- **Malicious Code:** This is a piece of code that defines the basic functionality of the malware and comprises commands that result in security breaches. It can take the following forms:
 - Java Applets
 - ActiveX Controls
 - Browser Plug-ins
 - Pushed Content



APT Concepts

Advanced persistent threats are a major security concern for any organization, as they represent threats to the organization's assets, resources, financial records, and other confidential data. APT attacks can damage the reputation of an organization by revealing sensitive data. This section discusses APTs as well as their characteristics and lifecycle.

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What are Advanced Persistent Threats?

An advanced persistent threat is defined as a type of network attack whereby an attacker gains unauthorized access to a target network and remains in the network without being detected for a long time. The word “advanced” signifies the use of techniques to exploit the underlying vulnerabilities in the system. The word “persistent” signifies the external command-and-control (C&C) system that continuously extracts the data and monitors the victim’s network. The word “threat” signifies human involvement in coordination. APT attacks are highly sophisticated attacks whereby an attacker uses well-crafted malicious code along with a combination of multiple zero-day exploits to gain access to the target network. These attacks involve well-planned and coordinated techniques whereby attackers erase evidence of their malicious activities after their objectives have been fulfilled. APT attacks are usually performed on organizations possessing valuable information, such as financial, healthcare, defense and aerospace, manufacturing, and business organizations. The main objective of these attacks is to obtain sensitive information rather than sabotaging the organization and its network.

Information obtained by an attacker through APT attacks includes:

- Classified documents
- User credentials
- Employee’s or customer’s personal information
- Network information
- Transaction information
- Credit card information
- Organization’s business strategy information
- Control system access information

Characteristics of Advanced Persistent Threats		CEH <small>Certified Ethical Hacker</small>
Objectives	Obtaining sensitive information or fulfilling political or strategic goals	
Timeliness	Time taken by the attacker from assessing the target system for vulnerabilities to gaining and maintaining the access	
Resources	Amount of knowledge, tools, and techniques required to perform an attack	
Risk Tolerance	Level up to which the attack remains undetected in the target's network	
Skills and Methods	Methods and tools used by the attackers to perform a certain attack	
Actions	APT consists of a certain number of technical "actions" that causes them to differ from other cyberattacks	
Attack Origination Points	Numerous attempts to gain entry into the target's network	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Characteristics of Advanced Persistent Threats (Cont'd)		CEH <small>Certified Ethical Hacker</small>
Numbers Involved in the Attack	Number of host systems that are involved in the attack	
Knowledge Source	Gathering information through online sources about specific threats	
Multi-phased	APT attacks are multiphased which include reconnaissance, gaining access, discovery, capture, and data exfiltration	
Tailored to the Vulnerabilities	APTs target-specific vulnerabilities present in the victim's network	
Multiple Points of Entry	The adversary creates multiple points of entry through the server to maintain access to the target network	
Evading Signature-Based Detection Systems	APT attacks can easily bypass the security mechanisms such as firewall, antivirus software, IDS/IPS, and email spam filter	
Specific Warning Signs	Specific indications of an APT attack include inexplicable user account activities , presence of backdoors, unusual file transfers and file uploads, unusual database activity, etc.	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Characteristics of Advanced Persistent Threats

APTs have various characteristics based on which attackers can design and plan their activities to successfully launch an attack. According to security researchers Sean Bodmer, Dr. Max Kilger, Jade Jones, and Gregory Carpenter, some key characteristics of APTs are as follows:

- **Objectives**

The main objective of any APT attack is to repeatedly obtain sensitive information by gaining access to the organization's network for illegal earnings. Another objective of an APT may be spying for political or strategic goals.

- **Timeliness**

It refers to the time taken by an attacker from assessing the target system for vulnerabilities to exploiting them to gain and maintain access to the target system.

- **Resources**

It is defined as the amount of knowledge, tools, and techniques required to perform an attack. APT attacks are more sophisticated attacks performed by highly skilled cyber-criminals, and they require considerable resources.

- **Risk Tolerance**

It is defined as the level up to which the attack remains undetected in the target network. APT attacks are well planned and executed with proper knowledge of the target network, which helps them remain undetected in the network for a long time.

- **Skills and Methods**

These are the methods and tools used by attackers to perform a certain attack. The methods used for performing the attack include various social engineering techniques to gather information about the target, techniques to prevent detection by security mechanisms, and techniques to maintain access for a long time.

- **Actions**

APT attacks follow a certain number of technical "actions" that make them different from other types of cyber-attacks. The main objective of such attacks is to maintain their presence in the victim's network for a long time and extract as much data as possible.

- **Attack Origination Points**

They refer to the numerous attempts made to gain entry into the target network. Such points of entry can be used to gain access to the network and launch further attacks. To succeed in gaining initial access, the attacker needs to conduct exhaustive research to identify the vulnerabilities and gatekeeper functions in the target network.

- **Numbers Involved in the Attack**

It is defined as the number of host systems involved in the attack. APT attacks are usually performed by a crime group or crime organization.

- **Knowledge Source**

It is defined as the gathering of information through online sources about specific threats, which can be further exploited to perform certain attacks.

- **Multi-phased**

One of the important characteristics of APTs is that they follow multiple phases to execute an attack. The phases followed by an APT attack are reconnaissance, access, discovery, capture, and data exfiltration.

- **Tailored to the Vulnerabilities**

The malicious code used to execute APT attacks is designed and written such that it targets the specific vulnerabilities present in the victim's network.

- **Multiple Points of Entries**

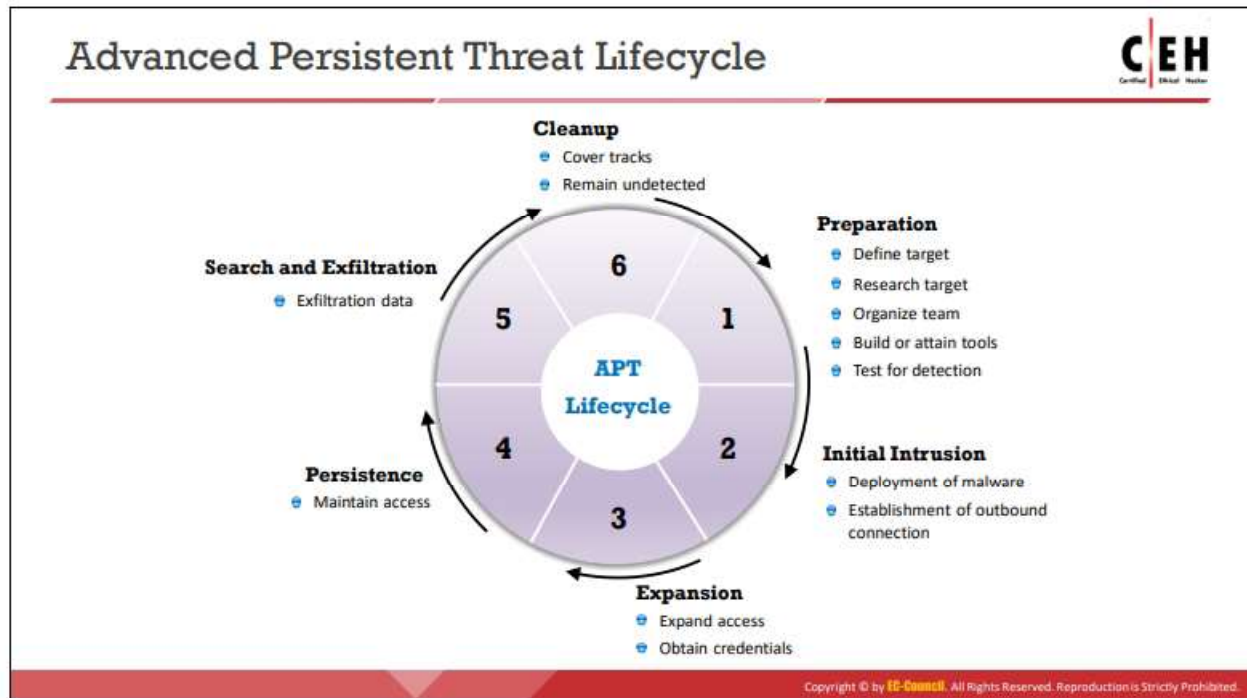
Once an adversary enters the target network, he/she establishes a connection with the server to download malicious code for further attacks. In the initial phase of an APT attack, the adversary creates multiple points of entry through the server to maintain access to the target network. If one point of entry is discovered and patched by the security analyst, then the adversary can use a different entry point.

- **Evading Signature-Based Detection Systems**

APT attacks are closely related to zero-day exploits, which contain malware that has never been previously discovered or deployed. Thus, APT attacks can easily bypass security mechanisms such as firewalls, antivirus software, IDS/IPS, and email spam filters.

- **Specific Warning Signs**

APT attacks are usually impossible to detect. However, some indications of an attack include inexplicable user account activities, the presence of a backdoor Trojan for maintaining access to the network, unusual file transfers and file uploads, unusual database activities, etc.



Advanced Persistent Threat Lifecycle

In the current threat landscape, organizations need to pay greater attention to APTs. APTs may target an organization's IT assets, financial assets, intellectual property, and reputation. Commonly used security and defensive controls will not suffice to prevent such attacks. Attackers behind such attacks adapt their TTPs based on the vulnerabilities and security posture of the target organization. Thus, they can evade the security controls of the target organization.

To launch an APT attack, attackers follow a certain set of phases to target, penetrate, and exploit an organization's network. Attackers must follow each phase step by step to successfully compromise and gain access to the target system.

The various phases of the APT lifecycle are as follows:

1. Preparation

The first phase of the APT lifecycle is preparation, where an adversary defines the target, performs extensive research on the target, organizes a team, builds or attains tools, and performs tests for detection. APT attacks usually require a high level of preparation, as the adversary cannot risk detection by the target's network security. Additional resources and data may be necessary before carrying out the attack. An attacker needs to perform highly complex operations before executing the attack plan against the target organization.

2. Initial Intrusion

The next phase involves attempting to enter the target network. Common techniques used for an initial intrusion are sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Spear-phishing emails usually appear legitimate but they contain malicious links or attachments containing executable

malware. These malicious links can redirect the target to the website where the target's web browser and software are compromised by the attacker using various exploit techniques. Sometimes, an attacker may also use social engineering techniques to gather information from the target. After obtaining information from the target, attackers use such information to launch further attacks on the target network. In this phase, malicious code or malware is deployed into the target system to initiate an outbound connection.

3. Expansion

The primary objectives of this phase are expanding access to the target network and obtaining credentials. If the attacker's aim is to exploit and gain access to a single system, then there is no need for expansion. However, in most cases, the objective of an attacker is to access multiple systems using a single compromised system. In this scenario, the first step performed by an attacker after an initial compromise is to expand access to the target systems. The main objective of the attacker in this phase is to obtain administrative login credentials to escalate privileges and to gain further access to the systems in the network. For this purpose, the attacker tries to obtain administrative privileges for the initial target system from cached credentials and uses these credentials to gain and maintain access to other systems in the network. When attackers are unable to obtain valid credentials, they use other techniques such as social engineering, exploiting vulnerabilities, and distributing infected USB devices. After the attacker obtains the target's account credentials, it is difficult to track his/her movement in the network, as he/she uses a legitimate username and password.

This expansion phase supports other phases of the APT lifecycle. In the search and exfiltration phase, the attacker can obtain the target data by gaining access to the systems. Attackers identify systems that can be used for installing persistence mechanisms and identify appropriate systems in the network that can be leveraged to exfiltrate data.

4. Persistence

This phase involves maintaining access to the target system, starting from evading endpoint security devices such as IDS and firewalls, entering into the network, and establishing access to the system, until there is no further use of the data and assets.

To maintain access to the target system, attackers follow certain techniques or procedures, which include use of customized malware and repackaging tools. These tools are designed such that they cannot be detected by the antivirus software or security tools of the target. To maintain persistence, attackers use customized malware that includes services, executables, and drivers installed on various systems in the target network. Another way to maintain persistence is finding locations for installing the malware that are not frequently examined. These locations include routers, servers, firewalls, printers, etc.

5. Search and Exfiltration

In this phase, an attacker achieves the ultimate goal of network exploitation, which is generally to gain access to a resource that can be used for performing further attacks or using that resource for financial gain. In general, attackers target specific data or documents before launching an attack. However, in some cases, although attackers determine that crucial data are available in the target network, they are unaware of the location of the data. A common method for search and exfiltration is to steal all the data including important documents, emails, shared drives, and other types of data present on the target network. Data can also be gathered using automated tools such as network sniffers. Attackers use encryption techniques to evade data loss prevention (DLP) technologies in the target network.

6. Cleanup

This is the last phase, where an attacker performs certain actions to prevent detection and remove evidence of compromise. Techniques used by the attacker to cover his/her tracks include evading detection, eliminating evidence of intrusion, and hiding the target of the attack and attacker details. In some cases, these techniques also include manipulating the data in the target environment to mislead security analysts.

It is imperative for attackers to make the system appear as it was before they gained access to it and compromised the network. Therefore, it is essential for an attacker to cover his/her tracks and remain undetected by security analysts. Attackers can change any file attributes back to their original state. Information listed, such as file size and date, is just attribute information contained in the file.

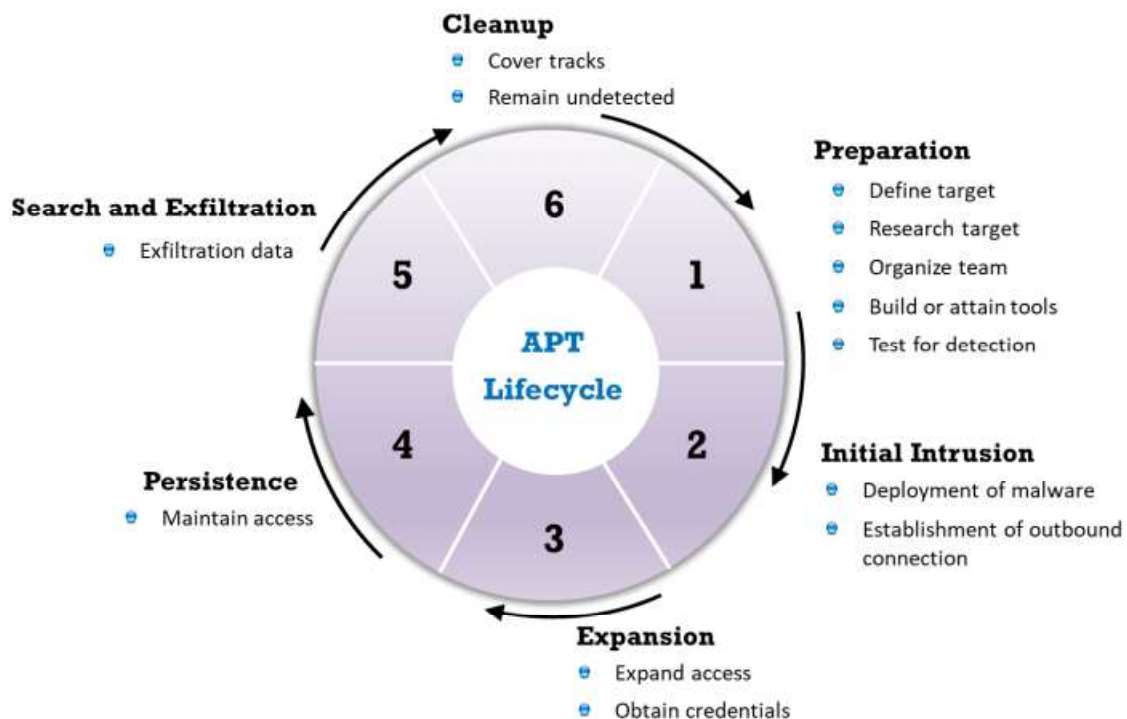


Figure 7.1: Advanced Persistent Threat Lifecycle