Unit 3: Advance Persistent Threat And Cyber Kill Chain

3

Unit Structure

3.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand how the Advanced Persistent Threat(APT) can be handled in a way that traditional threats are handled.
- Understand cyber kill chain

3.2 UNDERSTANDING THE PROBLEM

In today's world organizations are facing critical issues from different types of advanced threats including to the traditional ones. However, they are still finding issues that how the Advanced Persistent Threat which is known as APT can be handled in a way those traditional threats are handled. Well, APT is much complex in nature that they cannot be handled with any single approach. It is not possible to secure any organization to handle entire security and APT in a single way.

Organizations are dealing with the APT's they are completely different in nature until the organization understands where the real issue lies and how to solve them.

To understand how to handle Advanced Persistent Threats first executives of the organization has to understand the motive behind the attack. As still management of many organizations still thinks that they have paid or invested enough to handle every kind of cyber attack. Because spending the money will not solve the issue of complete security from Advanced Threats.

In the current situations or in simple terms the traditional method which is followed is to install basic security mechanisms. Then they get compromised, they will get notifications from the law enforcement and then they start the forensic investigation.

APT's are well funded, organized group of hackers who in a systematical manner to compromise the target which is mostly government organization's, private company's. They are mainly focused on gathering critical data by exploiting the vulnerability in a stealthy manner. They are very smart in hiding their tracks. They bypass highly secure infrastructure to establish the foot-hold in the target organization and to remain there until and unless the motive is not completed.

If we look deep into the APT, attacker needs one vulnerability to compromise the security and make way to get into the organization. But for the organization, they need to find out all vulnerability and to patch them. Many organization does not still understand that what are all the point of entry points or attack vectors from where the attacker can exploit it and make their way inside. The success ratio of APT is good, as they keep on trying until they find a way to exploit the system of the target.

For APT we have to learn them first before we try to stop them. Instead of looking in the future we can start learning the APT now and we can try to build the defense based on the learning from the past attacks. Though we cannot be sure that there will be no new approach.

But there are chances that same cybercriminal groups tend to use similar tactics and techniques on similar organizations. The key objective should assume the worst attack ever and hope for the best. It will help to understand the security level of your organization and will learn something new, while indirectly help to improve the security posture of the organization. Instead of assuming the best security measures are applied and doing nothing.

The final goal should be, an organization should not lose the business due to the lack of cybersecurity measures and practice. Most of the organization so spend large amount behind the cybersecurity and defend them. But the fundamental point is to understand is to identify the priority and risk and returns from the investment. The reason behind failure to defend from APT is to identify what resources which are at high risk needs more protection. There are multiple protection mechanisms which are already in place where the APT attack has been seen such as:

- Firewall
- Application Filtering
- End-Point Detection
- Anti-Virus Solutions
- Intrusion Detection

Investing a large amount of money to defend an organization from APT doesn't guarantee the protection from the APT. But the organization should focus on high-risk vulnerabilities and resources which can cause a big impact. It is better to fix 2

high-risk vulnerabilities which can cause a big impact instead of fixing low risk 20 vulnerabilities which cause not threats.

Let us now start to learn more about the APT, what does it mean and how it works.

3.3ADVANCE PERSISTENT THREAT

The term APT sounds very simple but is often taken as for granted or been misunderstood. The term **Advance** is related to the systematically crafting an attack vector in terms of its advanced and very targeted code used which is very effective.

The way attacker crafts the attack is very advanced while the methods to deliver the same are very standard methods and most important that it will work. Most of the APT will take advantage of the available advanced technology and techniques to customize the attack.

In every APT there will be a single method which will be used to bypass the security devices, which is known as Encryption. It was created to stop attackers from accessing critical information. Most security devices are unable to read the encrypted code of payload or encrypted packets in the network. The attacker sets up the encrypted outbound tunnel to attacker system. So data is encrypted and it goes undetected on the network.

The next is **persistent**. The attacker will not stop after failing once or twice. They will keep trying until they are successful in their objective. There need to be continuous defensive measured should be established.

The persistent nature of an APT is what it causes more damage to the organization. It simply means to remain stealthy for a prolonged period of time and not get caught due to its state of the art coding techniques.

They get into the system, remain there until the data is completely exfiltrated, and they leave without getting on the surface and they do not leave any trace. So it becomes very hard for an organization during the post-investigation when any third party services such as law enforcement agency inform them regarding the APT attack on your organization. It would be very difficult for an organization, as they don’t know where to start an investigation and how to decide a timeline for that.

As mainly APT attacks are not for a few days, an attacker could have a foothold in systems from many days, weeks, months or sometimes it may be years. The persistent process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "**Threat**" process indicates human involvement in orchestrating the attack.

For an APT to work successfully, it' important to hide the identity of the attackers, as APT attribution could lead to some real-world conflicts. So the attackers will want to hide their tracks. It is not uncommon to see the use of unpatched vulnerabilities (zero-days) in this kind of operations.

Figure 3.1 Avance Persistent Threat

APT will gather as much as information as possible so it will help the attacker to customize the attack to become successful.

- **APT Intentions:** For a defender, it is very important to find out the intentions behind the APT attack. That would be useful in investigating the post-incident analysis. We will look into some of the intentions of the attacker which were concluded based on the previous APT attacks.

  Data: For any organization, it is important to understand the market strategy, other competitive organization working in the similar product market.

The intentions behind such type of attack in which an attacker tries to exfiltrate data such as proprietary designs, schematics, formulas, experiment details, source code.

Information: It is very important for any organization to keep internal information in a very closed loop. Such as its financial status, future Corporate directions, its mergers, and acquisitions. This type of information is very useful to target the organization.

- **APT Threat Vectors:**

External:

Internet:

- Email Attachments
- File Sharing
- Pirated Softwares
- Mass vulnerability Exploits

Physical:

- Infection using external devices(USB, CD, External Disk Drives)
- Malicious IT Equipment
- Rogue Wifi Access points
- Stolen Mobile devices / Laptops

Internal:

Trusted Insider:

- Rogue Employee
- Third Party Contractors & Vendors

Trusted Channel:

- Stolen Credentials
- P2P tapping
- Un-Trusted devices
- Hijacked Cell communications

There are other threat vectors which are also present which are related to Softwares used inside the organizations.

Insecure Build:

- Insecure Devices.
- Unpatched software versions.
- Misconfigured Device.

Information Leakage:

- Exposure of sensitive material on online/social media.

Application Security:

- Fuzzing / Reverse Engineering.
- Buffer Overflows.

- **APT- Tools:**
  - Open Source exploit Softwares
  - Malware: Botnets, Rootkits, Ransomware, Malicious Attachments
  - Open source Available Exploit Code
  - Using Zero Days.

- **APT- Techniques:**
  - Open Source Intelligence (OSINT)
  - Social Engineering / Using SET (Social Engineering Toolkit)
    - Leverage Social media information.
    - Identify contextual and behavioral information.
  - Targeted Spear Phishing Attack
    - Requires in-depth knowledge of internal communication method.
    - Requires to build a strategy which lures the target and perform a predetermined action which.
  - Malicious Attachments
    - File format such as PDF, Office (Word/Excel/Access) is used mostly in APTs.

- Usage of exploit kits to generate the documents which contain malicious macros and craft the malicious attachments to send it the target using a properly crafted email. Such as Fallout, Angler, RIG, Nuclear, Neutrino are well-known examples of exploit kits.
- Exploits are easy to use, can be easily obtained from the dark web.
- Provides command and control infrastructure services.

- Hardware Devices
  - Hardware exploits in the internal devices used.
  - Projectors, Printers, Shared file servers, which are now usually connected with the internet, they are left open which out any security measures. An attacker tries to use such resources gain access to the internal network.

In the below image, we can clearly see and understand how the different attack vectors take part in making a successful APT attack.

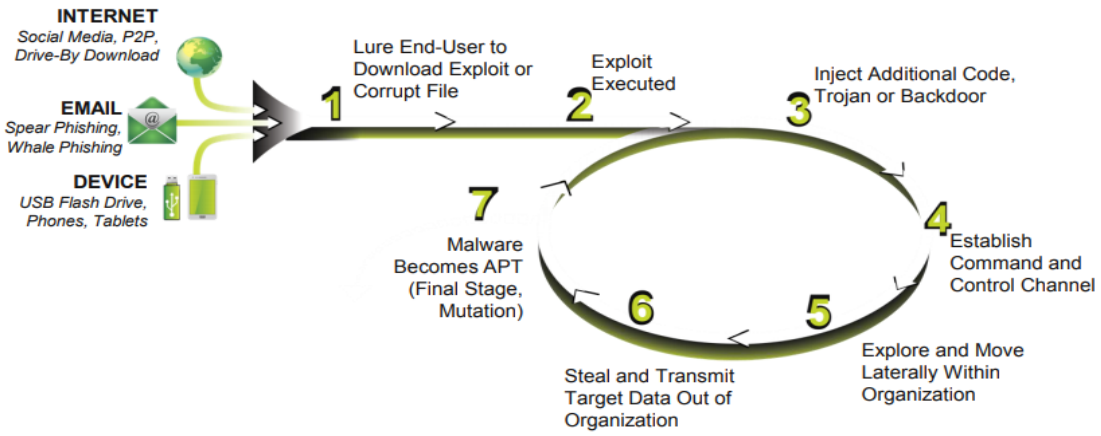

Figure 3.2 Attack Vector Cycle Source: Attack Vector chain by Brian Wrozek, Optive.com

➢ **Defending Against APT:**

We will see some of the high-level strategies that an organization must use to defend against the APT. It is always important that prevention is good but detection is a must. Mostly, the organization builds and invest in preventive measures.

But they forget that such type of APT attacks mostly comes with the legitimate traffic inside the organization and which is very difficult to identify by the installed

security measures. There are few things which an organization must do to prevent against such threats.

Raise Awareness and Control Users: Humans which are considered the end user and are targeted mostly to perform malicious actions, though they are not known what will be the consequences when clicks on such unknown links in the email. So it is better to conduct the internal phishing test and user awareness by giving basic ideas regarding phishing and how to identify them.

Reputation Scoring and Malicious Traffic Identification: Traditional security measures work on to block or access network traffic. While in APT mostly in pretends to the legitimate traffic. Once they enter into the network, they become bad or evil. So it is better to monitor the network traffic and scoring them based on their behavior in the network. That will help to identify if any malicious packets try to change its behavior from good to bad.

Monitor Outbound Traffic: Security Measures are generally built around the inbound traffic and monitor it to stop the threats from spreading. While in APTs, it is also important to monitor outbound traffic as their motive is to exfiltrate the internal data which will harm the organization. So it important to detect the anomaly in the outbound traffic also.

Understand the changing Threat Landscape: It is difficult when we don't know from what we have to defend to save ourselves. Something which is unknown or unseen. The only way to defend is to understand and learn how the offensive part works and operates. If the organization will not learn the new attack techniques and tactics they will lose the battle and not be able to tune their defensive measures.

Manage Endpoint: The ultimate goal of the attacker is to steal information which is stored on the endpoint. So even if the attacker has access inside the network, they still need to access the endpoint to get the information.

So to limit the damage, controlling the endpoint and locking down endpoint by disconnecting it from other networks and isolating it will protect the information from getting outside of the organization.

Now we will learn the complete and in-depth process and stages which the attacker performed to conduct such an APT attack. It is very important to learn each kill stage components in detail. This complete cycle is known as the Cyber Kill Chain.

It can simply be understood as a chain of multiple stages which are related to each other. The output of each stage can be considered as input for the next stage. We will see the offensive steps which are part of the cyber kill chain as well as from the defensive side, how to stop such attack.

3.4CYBER KILL CHAIN

The term kill chain was first used in the military which is related to the structuring of an attack, which includes identification of the target, getting a foothold in the organization, attack timing, and decision, destruction of the target. Though this process is not universal but is accepted by the information security community and converted into the part of the cyber kill chain to better understand it which can be useful to break the kill chain in different stages. As per the Wikipedia Traditional Military Kill Chain includes multiple stages which are listed below:

F2T2EA:

- ***Find:*** Locate the target.
- ***Fix:*** Fix their location, make it difficult for them to move.
- ***Track:*** Monitor their movement.
- ***Target:*** Select an appropriate weapon or asset to use on the target to create desired effects.
- ***Engage:*** Apply the weapon to the target.
- ***Assess:*** Evaluate the effects of the attack, including any intelligence gathered at the location.

Now we will look at the different phases of cyber kill chain part of which mention below, is majorly derived from the Lockheed Martin which was first published by them in 2011. Since then it has been adopted by many organizations. Cyber kill chain reveals different phases of a cyber attack, from the initial stage of reconnaissance to the last stage of data exfiltration.

This has been also used as a tool for the management to understand the phases of cyber attack to continuously improve their defensive measures. According to Lockheed Martin, these phases threats must pass through the model which is shown below.

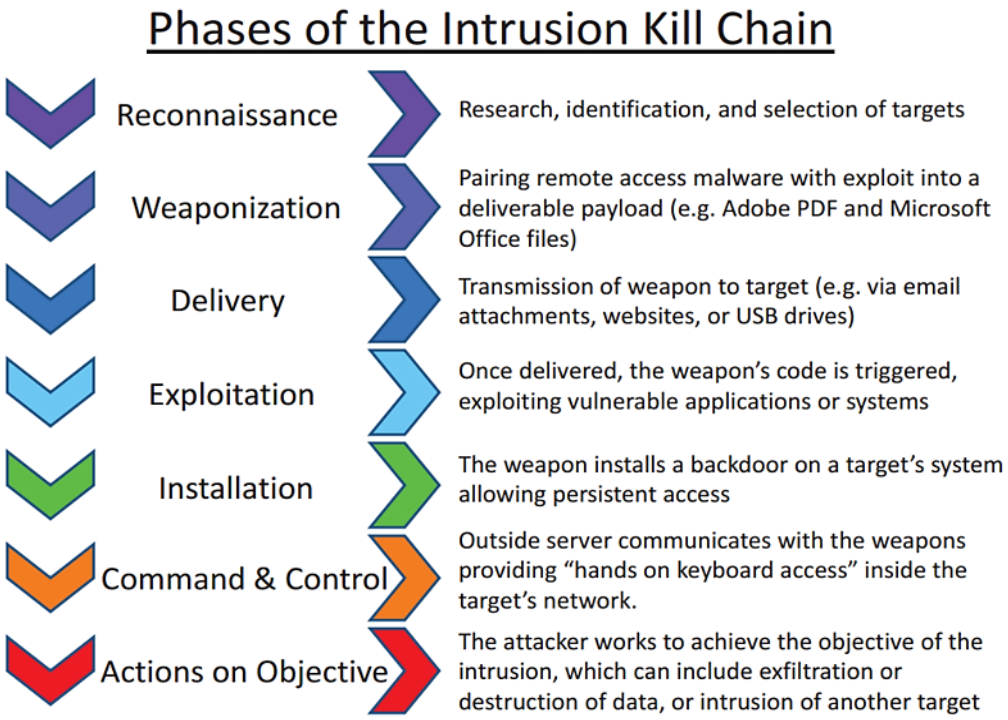

Figure 3.3 Cyber Kill Chain Source: Wikimedia.com

Check Your Progress 1

1. List out any three APT threat vectors.
2. List of any 3 exploit kit names.
3. What are software related APT threat vectors.

Let us understand all 7 technical phases in detail.

Reconnaissance: Reconnaissance means to gather information regarding the target. It can an individual or an organization. It further drills down to the identification and profiling of target. Further to extract all kinds of information from the internet such as email address, social media relationship data, blogs, sites, conferences. Information gathers from this stage will be later used in the design and delivery of payload. Reconnaissance is divided into two parts:

Active Reconnaissance: This step is to gather information regarding a target without his/her knowledge. Such as using open source intelligence tools(OSINT) for information gathering.

Passive Reconnaissance: It involved deep profiling of the target which might trigger alert to the target. Such as using network scanning tools like Nmap, Nessus,

Weaponization: In these phases, the attacker uses the details gathered from the above stage to create malicious payload such as RAT(Remote Access Trojans). Also how to deliver it to the target. The attacker leverages the usage of open source offensive framework tools such as the Metasploit, Msfvenom, Veil and to write reverse shells. Then it is injected into the legitimate software or binaries and is finally obfuscated in order to prevent from detection.

Exploit: Exploit is a part of the weapon which facilitates RAT to execute in the target machine. It uses system or software vulnerabilities to drop and execute a RAT. The major objective to use exploits is to evade the detection. Exploits can be related to MS Office (doc/ppt/excel) which can be identified from its CVE(Common Vulnerabilities and Exposure) number. Such as CVE-2017-11882, CVE-2014-9165 and so on.

There are methods which do exist in which the target system can be accessed without using exploit they are very unreliable in these times as the organization has already set up multiple security layers. Embedding RAT or an exploit code inside the legitimate file will be easier to evade the detection. In some cases, multiple exploits are used to create a payload using the exploit kits. Which provides the exploit code for different software.

Operating system level exploits use kernel level exploits or exploits the device driver itself to perform remote or local code execution. Network level exploits try to exploit network devices or protocols to perform privilege escalation.

Delivery: It is a critical part of the cyber kill chain which is responsible for an efficient and effective cyber attack. In most of the cyber attack, it is mandatory to have some user interactions such as using email attachments, drive-by downloads, USB, browser-based attack.

Check Your Progress 2

1. List out any 2 methods used for reconnaissance.
2. List of any 2 offensive framework used to prepare payload.
3. List of network scanning tools for passive reconnaissance.
4. List of any 2 Network level exploits.

For which the initial target information is necessary for deciding which method will be useful, this can be varied according to the target. There are some attacks which are performed without user interaction by exploiting network devices or services such as CVE-2014-3306, CVE-2014-9583.

Delivery is a very high-risk phase, it leaves the digital footprints behind. So most of the attacks are performed in an anonymous way using paid services. Successfully targeting the user in the first attempt cannot be guaranteed.

In such cases, the attacker will gain all information due to which the first attempt was failed and will make sure that in the second attempt it successfully exploits target machine. In some cases where one delivery method is not sufficient, multiple delivery methods are used.

Exploitation: Once the successful delivery of the weapon is done. The next step is to execute or trigger the exploit on the target side. The goal here is to silently install or execute the exploit. There are certain conditions need to be matched for this to work such as User must be using software or services for which the exploit is created.

Next operating system should not be updated with the latest patches which fail the exploit to work. And last Anti Virus software should not detect the payload.

Installation: Nowadays, traditional methods of the infection will not work in which the machine Is infected with the links created in the startup folder, or creating the registry of the file to run in a startup. As of end-user protection, mechanisms has grown.

Modern malware is multi-staged and they heavily depend on the droppers and downloaders to deliver the malware.

Command and Control: After successfully triggering the malware. The important part of the remote attack is command and controls (CnC/C&C). C&C gives the instruction to the compromised machine. There are mainly three different types of communication structures, such as centralized structure, peer-to-peer and latest social network based communication structure.

C&C communication traffic analysis is a traditional approach to detect the communication pattern in the target machines. Malware authors tend to use new techniques in which it is difficult to separate it from the legitimate traffic of the network to make it more anonymous.

Actions on Objective: In the last phase the attacker tries to achieve the final goal which is to exfiltrate the data from the compromised machine by giving instruction from the command and control server.

3.5 LET US SUM UP

In this chapter, we have seen the life cycle of the APT. We have seen the different threats and attack vectors which are part of the APT. Apart from this, we have seen tools and techniques which are used in the APT attack. Also, we have seen the different phases of the cyber kill chain along with the other technical details.

3.6CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

1. Email Attachments, File sharing, Pirated software
2. Fallout, Neutrino, Angler
3. Unpatched software, Misconfigured Devices, Fuzzing

Check Your Progress 2

1. Email address harvesting and social media related data
2. Msfvenom, Veil
3. Nmap, Nessus
4. Exploiting Network devices and Protocols