1.What is your definition of APT Security?

Advanced persistent threat (APT) works to access computer networks and systems without being detected or noticed. These threats, sometimes enacted by a nation state or state-sponsored group, can steal private information, damage IT systems and disrupt the function of vital systems. Defending against Advanced Persistent Threats is a difficult task as they act stealthily, and their intrusions can be hard to recognize.

2.Could their solution detect more than the existing security system?

You wouldn't want to buy APT Security solution which doesn't add value to the existing security ecosystem. As, APT security has become a marketing term and many perceive APT Security as traditional signature based antivirus. Therefore, you need to know whether the APT security solution you are going to buy has much capable in detecting malware. You should have a list of possible APT's variants in handy and ask whether they protect from it. Some of the variants of APT can be Insider Threats, Initial attack vectors, Spear- Phishing, Drive-by-download, Online Social Networking, Search engine poisoning and many more

3. Does your APT security solution covers all the channel by which threat might penetrate into the enterprise system?

APT Security solution must provides comprehensive coverage in various channels which are as follows:-

• End Point: These are typically deployed as agents on End Point Devices but there are also some solutions which are agentless

• Network: These are typically deployed as appliances within their network infrastructure & separate solution may be required for detection, response and forensics

• Email: Spear Phishing email is one of the main cause for Advanced Targeted Attacks

4. What is your false positive rate and how do you measure it?

There has been a times when a system falsely gives "Malware Attacks" and then organization allocate resources to investigate the issue and if it is a false positive, then people tends to ignore the real alarm as well and doesn't take it seriously.

5. Which type of technologies does your APT solution leverage?

As APT Security, multiple solutions/technologies may be required and hence you need to understand the techniques vendor APT Security solution leverages. It can leverage Sandboxing, Security Analytics, Application Containerization, Embedded URL Analysis, IOC Detection, Static Code Analysis etc.

6. What is your solution capabilities in terms of Prevention, Detection, Response and Prediction?

The multiple APT Security solution should be capable in terms of Prevention, Detection, Response and Prediction. You need to evaluate and understand how much you are going to achieve in terms of these 4 key capabilities.

7. What is the difference between APT and malware?

An APT takes a more strategic and stealthy approach than most malware. By using traditional malware such as Trojans and phishing, attackers gain access to networks, but they then move around secretly and install their attack software throughout.

8. What are APTs what are they used for?

When an APT achieves multiple points of entry into the targeted network, the attacker can retain access even if a cybersecurity defender discovers the malicious activity. This will enable defenders to close one breach.

9. What is the goal of an APT attack?

Usually, APT attacks target monitoring, stealing data, or embedding themselves deeply in an organization to make them tougher to detect and prevent in the future. APT attacks can hide and lurk in their victims' network for weeks, months, or even years.

10. How do most advanced persistent threats begin?

It is a type of attack that stealthily gains unauthorized access to network data with advanced persistent threats. An ATP breach is a sophisticated attack that can remain undetected for a considerable period of time once it passes security barriers.

11: What is an Advanced Persistent Threat (APT)?

A: An Advanced Persistent Threat (APT) refers to a sophisticated and targeted cyber attack carried out by a well-funded and highly skilled group or organization. APT attacks are characterized by their stealthy and prolonged nature, as the attackers focus on gaining persistent access to a targeted network or system for an extended period, often remaining undetected. APTs typically involve a combination of multiple attack vectors, including social engineering, zero-day exploits, malware, and advanced techniques to bypass security measures.

12: What are the objectives of an APT?

A: The objectives of an APT attack can vary depending on the motives of the threat actor behind it. Some common objectives include:

Intellectual Property Theft: APTs may target organizations to steal valuable intellectual property, such as trade secrets, proprietary technology, or research and development data.

Espionage: APT attacks can be motivated by political or military interests, aiming to gather classified or sensitive information from government agencies or organizations involved in critical infrastructure.

Financial Gain: Some APT groups target financial institutions or organizations to steal financial data, login credentials, or conduct fraudulent activities like unauthorized fund transfers.

Disruption and Sabotage: APTs may seek to disrupt or sabotage the operations of targeted organizations or critical infrastructure, causing economic damage or undermining public trust.

13: How do APT attacks differ from regular cyber attacks?

A: APT attacks differ from regular cyber attacks in several ways:

Sophistication: APT attacks are highly sophisticated, leveraging advanced techniques, tools, and expertise. They often involve custom-built malware and exploit multiple vulnerabilities in a targeted network or system.

Persistence: APT attacks are characterized by their long duration. Attackers remain hidden within the targeted infrastructure for extended periods, continuously exfiltrating data or maintaining control to achieve their objectives.

Targeted Approach: APT attacks are highly targeted, focusing on specific organizations, industries, or individuals of interest. Attackers conduct extensive reconnaissance to gather intelligence and tailor their attack techniques accordingly.

Coordinated Campaigns: APT attacks are typically part of a larger, coordinated campaign. Multiple attack vectors, such as phishing emails, compromised websites, or supply chain attacks, are employed to increase the chances of success.

Resourceful Threat Actors: APT attackers are well-funded and have access to substantial resources, including skilled personnel, advanced tools, and financial backing. They are often associated with nation-states, organized crime groups, or well-established hacking collectives.

14: How do organizations defend against APT attacks?

A: Defending against APT attacks requires a multi-layered and proactive approach to security. Some key measures organizations can take include:

Risk Assessment: Conduct regular risk assessments to identify potential vulnerabilities and prioritize security measures accordingly.

Employee Education: Train employees to recognize social engineering tactics, phishing attempts, and other common attack vectors. Promote a culture of security awareness and best practices.

Robust Access Controls: Implement strong access controls, including multi-factor authentication (MFA), privileged account management, and regular access reviews.

Network Segmentation: Segment the network to limit lateral movement for attackers. This helps contain the impact if one part of the network is compromised.

Patch Management: Keep software, operating systems, and applications up to date with the latest security patches to address known vulnerabilities.

Intrusion Detection and Prevention: Deploy advanced intrusion detection and prevention systems (IDS/IPS) to monitor network traffic, detect suspicious activities, and block or mitigate threats in real-time.

Endpoint Protection: Utilize next-generation antivirus (NGAV) solutions, host-based intrusion detection systems (HIDS), and endpoint detection and response (EDR).

15.What is Advanced Persistent Threat (APT) in Cyber Security?

The advanced persistent threat (APT) has been the bane of cybersecurity for years now. This has become a major issue as cybercriminals and nation-states have started taking advantage of this new and emerging threat vector. The primary function of APT cyber security is to penetrate the perimeter security systems of your organization so that they can access internal resources.

Main Goals of APT Attacks and their Category:

Unauthorized access to classified information such as credit cards, bank accounts, passport details, etc.

Sabotage the entire system, including the cloud, by deleting the complete database.

Taking over the critical website and making major changes such as the stock market or hospital.

Accessing essential systems with the credentials of the people.

Access to sensitive or incriminating information through communication.

16.How Does Advanced Persistent Threats Work?

APTs generally take place over time and involve the following steps:

Hackers infiltrate networks. The malware is usually planted into the network via phishing emails, malicious attachments, or application vulnerabilities.

An external command-and-control server may be used to provide additional instructions or code to the malicious software.

As a result, malware will often create other points of compromise to ensure that an attack can continue. Although a specific entry point or vulnerability has been closed or strengthened.

After successfully gaining access to a network, a cybercriminal begins working. It might involve stealing confidential information, deleting data, or stealing account names.

A staging server is used by the malware to collect data. This data is exfiltrated using an external server controlled by the hacker. As soon as the hacker breaches the network in this way, he will attempt to cover his tracks, erase all evidence, and repeat the process indefinitely.

17.Key Characteristics of an APT Attack?

Several characteristics distinguish advanced persistent threat cyber security attacks from others.

1. They are advanced

Costs for customizing APTs can range from thousands to millions of dollars. A team of highly skilled and intelligent cyber criminals created them. In the hacker’s view, APTs are the most resource-intensive form of crime because they require many months of development and launch.

2. They are persistent

The types of hackers involved in APT usually have a lower risk tolerance than those who engage in “script kiddies” or other types of hacking that cast a wide net to attract a single target. These attacks aim to evade detection for as long as possible by planning and designing them carefully with knowledge of the target’s vulnerabilities.

3. They are stealthy

An APT attack is not shallow when it comes to skills and methodologies. It is typical for these threats to be characterized by highly sophisticated social engineering activities, detection, and prevention, as well as persistence once they have gained access.

4. They are non-obvious

It is pertinent to note that, in addition to the tools listed above, there are an endless array of potential advanced persistent threat tools, including the deadliest Trojan virus.

5. They are tailored

Semi-technical script kiddies rarely run advanced persistent threats. Their development takes your organization’s vulnerabilities into account, and they’re highly targeted at you. Zero-day malware attacks falling within the APT category may require millions or even millions of dollars to develop.

6. They have a specific purpose

Using an APT, criminals can repeatedly gather sensitive information over time and maximize their earnings. There are also times when the objective is politically, strategically, or espionage-related. This period of time also involves repeated pursuit of APT goals.

7. They establish multiple through multiple weak points

Multiple attempts may be launched for an initial presence in a network, although first attempts are generally sufficiently well-researched to succeed. Your organization’s human gatekeepers as well as your network’s vulnerabilities, can be discovered through months of research.

8. They occur in multiple stages

An APT’s multiphase nature is one of its most defining characteristics. Social Engineering, phishing, exploit kits, etc., are among the phases in which they attempt to enter a system. The process involves:

Mapping an organization’s network.

Developing a precise approach.

Capturing data.

Repeating the exfiltration process as often as possible.

9. They have particular signs of detection

The following symptoms may be observed by organizations following a compromise, although APTs are almost universally incredibly difficult to detect:

Activity on user accounts that seems odd

A widespread method of securing access is the use of backdoor trojans

Increasing database operations suddenly, which can involve enormous amounts of data, is unusual database activity

Exfiltration may be facilitated by combining collected data into files

10. They have knowledge sources

Businesses everywhere should be aware of APT attacks. These attacks should not be ignored by small and medium enterprises, however. In order to gain access to large organizations, APT attackers increasingly use smaller companies that are part of the supply chain.

18.Types of Advanced Persistent Threats?

It's hard to imagine a situation worse than being hacked by a sophisticated APT. Malware that performs APT attacks over a prolonged period of time is referred to as APT malware. Instead of causing damage to a computer or network, APT malware repeatedly steals data over a long period of time. Although there are many types of advanced persistent threats, the following are the most common:

1. Social engineering

By exploiting social engineering techniques, systems, networks, and physical locations can be accessed by unauthorized individuals without their knowledge. Hackers conceal their identities and motives by posing as trusted individuals or sources of information. It is possible to influence, manipulate, or trick an organization into revealing sensitive information.

2. Phishing

APT phishing attack is when a website pretends to be legitimate but actually contains someone trying to steal your credit card number, bank account information, or password. Cybercriminals typically send a fake message that contains a phishing website link that appears to come from a reputable company, a friend, or an acquaintance.

3. Spear phishing

Emailing or using electronic communications to target an individual, company, or organization is called spear phishing. Malware can also be installed on a targeted user's computer by cybercriminals, even though they usually intend to steal data for malicious purposes.

4. Rootkits

Hackers can take control of a target device with malware, such as rootkits. The hardware and software on your computer can be infected by some rootkits and the operating system and software.

5. Exploit Kits

Exploits exploit software vulnerabilities. When hackers find outdated systems with critical vulnerabilities, they deploy targeted malware to exploit them. Malware payloads commonly include shellcode, a small piece of malware that downloads additional malware from attacker-controlled networks. Organizations and devices can be infiltrated and infected with shellcodes.

6. Other methods

Other APT attack examples are computer worms, bots, spyware, adware, ransomware, remote execution, spear phishing, web shell, rootkits, keylogger, and many more.

19.Five Stages of Advanced Persistent Threat Attack (APT)?

1. Initial access

Cybercriminals gather information about their targets during the initial access phase of an APT attack. The primary targets of the initial stage are the employees of the organization, their workstations, exploiting application vulnerabilities, vulnerabilities in security tools, and malicious uploads, spear phishing commonly targets employees with privileged accounts. The attackers hope to gain control over the target by infecting it with malicious software.

2. First penetration and malware deployment

The development phase of an APT attack is when the cybercriminals and nation-states focus on finding vulnerabilities in the networked resources of the organization. They will then attempt to exploit these vulnerabilities and gain access to internal resources they didn’t initially intend to access. An attacker installs backdoor shells and trojans disguised as legitimate software to access the network and control the compromised system. By encrypting, obfuscating, or rewriting code, advanced malware techniques the attacker can conceal an APT’s activity.

3. Expand access and move laterally

In an expanded access phase of an APT attack is the process where the cybercriminals install their malicious code onto endpoints. The installation process varies from case to case. Their goal is to gain deeper access and control over more sensitive systems by using brute force attacks or exploiting other vulnerabilities. It could be as easy as getting an employee to open an infected attachment and thus an attacker can bypass firewalls and create tunnels as well as install additional backdoors.

4. Stage the attack

This stage is where the cybercriminals attempt to remain under the radar of the network security systems. During this phase, the cybercriminals and nation-states employ techniques such as watering-down activity to lower their risk.

This stage can take time as the common practice of attackers is to encrypt and compress data to prevent it from being easily accessed. The primary goal of this stage is to let the APT attacks run while keeping a low profile.

5. Exfiltration or damage infliction

The exfiltration or damage infliction phase of an APT attack is when the cybercriminals attempt to damage or destroy as many resources as possible. The hacker can fully exploit a system's vulnerabilities from within, giving a complete control of the system.

To distract security teams, hackers frequently use a Distributed Denial of Service (DDoS) attack when transferring data outside a network perimeter.

Once hackers achieve a particular goal, they may withdraw or continue to run this process indefinitely. It is common for hackers to leave a backdoor open to regain access to the system later

20.APT Security Measures?

1. Traffic monitoring

Communication and information technologies will never cease to evolve, and data in motion will always exist. Because hackers always target the main arteries and thoroughfares of data flow, monitoring network traffic is crucial for organizations of all sizes. A network traffic monitoring system safeguards against potential problems and is also used to maintain network performance and speed.

2. Application and domain whitelisting

Whitelisting applications help protect your computer system against malware, spam, ransomware, and other threats, like email whitelisting. The application whitelist works oppositely to approve email addresses, allowing only approved applications to run. Unwhitelisted items are blocked and considered unsafe.

3. Access control

Access control is one of the most effective defenses against advanced persistent threats, such as using strong passwords, two-factor authentication, or Google Authentication, because it mitigates the threat of compromised passwords. Without approval from the second factor, a password alone won’t provide access if hacked, guessed, or even phished.

4. Keeping Security Patches Updated

Whenever software is vulnerable, security patches are issued to fix the issue. The term vulnerability refers to a weakness in software that malicious individuals can exploit.

These vulnerabilities may have a theoretical aspect, but they can have serious consequences. Someone with physical access could steal all your files if your operating system has a flaw that allows anyone to gain administrative privileges. Your private information could be exposed by a flaw in an app that leaks data.

5. Avoid Phishing Attempts

Ensure your computer is protected from malicious messages by installing anti-phishing and anti-spam software. Other types of threats are prevented by antivirus malware. Security researchers program anti-malware software to detect even the stealthiest malware, just as they do with anti-spam software.

6. Perform Regular Scans for Backdoors

Backdoors are one of the widespread problems. Security measures govern access to internet-facing services or infrastructure behind them, which are all protected by security measures. As well as supporting various parameters and configurations that enable the security mechanisms to function, they are also supported by the various security implementations.

Backdoor conditions may occur if such parameters are not configured correctly. It is possible for IT admins to accidentally or intentionally enable anonymous access for specific purposes without thinking about the security implications and then forget to disable it afterwards.

21.Advanced Persistent Threat Examples?

The first step in detecting persistent threats is to know how these attackers operate. They are usually well-educated on the organization they are targeting, which allows them to change tactics quickly and evade detection.

New tactics and techniques are created to stay a step ahead of detection. While detecting a persistent threat and having a quick APT solution is difficult, it’s not impossible. The next step is to understand how attackers operate to identify the best ways to detect their activities. Two primary methods of detecting persistent threats are tracking and analysis.

An APT is usually sponsored by a nation or a very large organization. Examples of APTs include Iran's nuclear program and Hydraq, which Stuxnet brought to an end. Iran's ability to enrich uranium was slowed in 2010 by cyberattacks by the United States and Israel. In comparison to other viruses or worms, Stuxnet was unique. Centrifuges that enrich uranium are destroyed instead of hijacked or stolen by malware. To accomplish this, one required intricate programming. Stuxnet targeted industrial control systems and CPUs from Siemens.

As part of Operation Aurora in 2009, Hydraq was used to attack Google and other U.S. companies. The malicious Trojan horse Hydraq was installed using a zero-day exploit, reportedly from China, as part of Operation Aurora. A Google spokesperson revealed the attack in January 2010. Rackspace, Juniper Networks, and Adobe Systems were among the victims. Even though various banks, defence contractors, security vendors, oil and gas companies, technology companies, and others were attacked, they didn't publicize the incident.

22.APT Detection and Protection?

The first step in detecting persistent threats is to be aware of how these attackers operate. They are usually well-educated on the organization they are targeting, which gives them the ability to change tactics quickly and evade detection.

New tactics and techniques are created to stay a step ahead of detection. While it’s difficult to detect a persistent threat and have a quick APT solution, it’s not impossible. The next step is to understand how attackers operate to identify the best ways to detect their activities. Two primary methods of detecting persistent threats are tracking and analysis.

1. Email filtering

During email filtering, the software automatically moves unwanted emails to a separate folder after analyzing them for red flags that signal phishing. You are more likely to lose your personal sensitive information such as banking or identity number when you click on a phishing email. The sole purpose of phishing emails is to steal your personal information.

2. Endpoint protection

Data and workflows associated with individual devices on your network are protected through endpoint security. Endpoint protection platforms examine files as they enter the network. With endpoint security, you'll not only be protected from malicious software, you'll also be protected against evolving zero-day threats.

3. Access control

Providing access to and using company information and resources is a fundamental component of data security. By authenticating and authorizing users, access control policies ensure they have access to company data in accordance with their claims.

4. Monitoring of traffic, user and entity behavior

Monitoring network events generated each day by users, users, and entities is the process of gathering insight into their behavior. By collecting and analyzing this data, you can identify compromised credentials, lateral movement, and other malicious activity.

23.Most common tactics used by APTs?

In order to fully understand APTs, it is essential to understand their flexibility. In addition to launching sophisticated attacks, they also launch very basic attacks. Sometimes, a simple attack works for an adversary just as much as it does for anyone else. Here are the common advanced persistent threat list that are used by the hackers:

1. Spear phishing

Phishing is the primary attack vector of most attacks, including advanced persistent threats. APTs sometimes use phishing attacks to spread their malicious influence widely, while spear phishing is sometimes used to target specific individuals or businesses. By engaging in phishing scams, users' login credentials are commonly exposed or malware is installed on their machines.

2. Watering hole attack

Similar to phishing attacks, watering holes use legitimate websites infected with malware to deliver malicious payloads or steal credentials. Watering holes are targeted by attackers who corrupt websites that people are likely to visit.

3. Privilege escalation

As the name implies, privilege escalation is an attack where users are granted elevated rights or privileges beyond what is provided. The attacker may be an outsider or an insider. An important part of the cyberattack chain involves privilege escalation vulnerabilities, such as system bugs, misconfigurations, or inadequate access controls.

4. Credential harvesting

In Credential Harvesting (or Account Harvesting), large amounts of credentials are obtained via MITM attacks, DNS poisoning, phishing, and other methods. Assailants aggregate large quantities of credentials for sale on the dark web and in other covert channels.

5. Data exfiltration

Several different terms are used to describe data exfiltration, including data exportation and data theft. These terms refer to data transfer from a computer or other device without authorization. A person with physical access to a computer can perform data exfiltration manually, but a malicious computer program can also achieve it over the network.