I-MEDITA

Training | Development | Placement

Palo Alto

THREATS

INTERVIEW QUESTIONS GUIDE

One Step Closer Towards Your Dream Job...

Q1. MALWARE v/s EXPLOTS

Malware

Short for malicious software, malware refers to a file, program or string of code used for malicious activity, such as damaging devices, demanding ransom and stealing sensitive data. Malware is typically delivered over a network, though it can also be delivered via physical media, and it is classified by the payload or malicious action it performs. The classifications of malware include worms, Trojans, botnets, spyware and viruses. Although each malware strain behaves uniquely, automated spreading behavior is most commonly associated with worms. Most malware today is delivered over email by way of a link or file attachment, but more and more adversaries are beginning to leverage non-email communication platforms, such as social media and instant messaging, for malware delivery.Today, there are millions of variants of malware that are constantly being tweaked ever so slightly to evade signature-based protection. Some malware types are easier to detect, such as ransomware, which makes itself known immediately upon encrypting your files. Other malware types, like spyware, may remain on a target system silently to allow an adversary to maintain access to the system. Regardless of the malware type, its detectability or the person deploying it, the intent of malware use is always malicious.

Q1. MALWARE v/s EXPLOITS (Continued...)

Exploits

An exploit is a piece of code or a program that takes advantage of a weakness (aka vulnerability) in an application or system. Exploits are typically divided into the resulting behavior after the vulnerability is exploited, such as arbitrary code execution, privilege escalation, denial of service, or data exposure. In addition, exploits may be categorized into known and unknown (i.e., zero-day) exploits. Zero-day exploits generally present a significant threat to an organization as they take advantage of unreported vulnerabilities for which no software patch is available. At times, adversaries may attempt to exploit vulnerabilities via collections or kits hidden on invisible landing pages or hosted on advertisement networks. If a victim lands on one of these sites, the exploit kit will automatically scan the victim's computer to find out the operating system the computer is using, which programs are running, and if there are any vulnerabilities associated with those software packages. Once it identifies a vulnerability, the exploit kit will use the appropriate exploit code and attempt to install and execute malware.Unlike malware, exploits are not inherently malicious, but they are still likely to be used for nefarious purposes. The key takeaway here is that exploit code may be used to deliver malware, but the code is not the malware itself. Although malware and exploits are used in combination for multiple types of malicious objectives, they present distinct issues that should be examined individually to provide well-rounded security.

Q2. WHAT ARE FILELESS MALWARE ATTACKS AND "LIVING OFF THE LAND"? UNIT 24 EXPLAINS

Fileless malware and “living off the land” have been around for a while, but they have seen a resurgence in recent months. What’s behind this growing popularity? Jen Miller Osborn, deputy director of Threat Intelligence for Unit 42, explains what fileless malware attacks are and why “living off the land” is so attractive for malicious actors.

Fileless malware attacks are something where attackers are using things that aren't written to disk. So, things that are staying in volatile memory, such as PowerShell and WMI. And they're doing that because they are much harder to both detect and to find later, because a lot of times, they aren't kept in logs.

So, you'll see attackers doing things where they're automating a lot of their initial attacks, where they'll use something such as PowerShell or WMI to figure out both where they've landed in the system and do some basic network reconnaissance to decide whether or not they are in a place where they want to be. And those things are very hard to detect via traditional AV vendors, and even without some behavior analytics, they're harder to find.

And then, along with that, to also avoid detection, we're seeing attackers more and more moving toward a thing that's called "living off the land," which is where they're repurposing things that are typically legitimate admin tools, whether Windows or Macintosh or Linux or whatever. And they're tools that admins will use to monitor their environment, to dump credentials, to kind of figure out what's going on. But now, you have attackers using those same tools, which, in a lot of cases, are whitelisted because these are legitimate tools that system admins use.

Q2. WHAT ARE FILELESS MALWARE ATTACKS AND "LIVING OFF THE LAND"? UNIT 24 EXPLAINS. (Continued...)

But, you're seeing attackers repurposing them now, where they're using them to basically accomplish the same things that a lot of sysadmins do – to determine where they are, to do some network administration, to do some account administration, and checking on hashes. But they're using them maliciously, which is much harder to detect because, as a basic network posture, those things are going to be whitelisted.

So, those are two ways that attackers now are moving into spaces that are, A, hard to detect, and B, require a lot more behavioral analytics. Because there are a lot of things that you'll typically see legitimate system admins use but you're seeing attackers use. Because instead of using malware or using something such as Mimikatz, which is a known tool, which a lot of people will flag, now they're using tools where they’re going to be whitelisted.

And they’re probably – if they're not already present on a network for legitimate purposes, you'll see, a lot of times, attackers will bring them down because they're aware that these are legitimate tools and that they’re probably whitelisted. You aren't going to detect them maliciously unless you're running additional behavioral analytics that will show you them being used in a way that the sysadmin would not be using them.

Q3. WHAT IS DNS TUNNELING AND HOW DOES IT WORK?

Domain name system, or DNS, is the protocol that translates human-friendly URLs, such as paloaltonetworks.com, into machine-friendly IP addresses, such as 199.167.52.137. Cyber-criminals know that DNS is widely used and trusted. Furthermore, because DNS is not intended for data transfer, many organizations don't monitor their DNS traffic for malicious activity. As a result, a number of types of DNS-based attacks can be effective if launched against company networks. DNS tunneling is one such attack.

How DNS Tunneling Works?

DNS tunneling exploits the DNS protocol to tunnel malware and other data through a client-server model.

1. The attacker registers a domain, such as badsite.com. The domain's name server points to the attacker's server, where a tunneling malware program is installed.
2. The attacker infects a computer, which often sits behind a company's firewall, with malware. Because DNS requests are always allowed to move in and out of the firewall, the infected computer is allowed to send a query to the DNS resolver. The DNS resolver is a server that relays requests for IP addresses to root and top-level domain servers.
3. The DNS resolver routes the query to the attacker's command-and-control server, where the tunneling program is installed. A connection is now established between the victim and the attacker through the DNS resolver. This tunnel can be used to ex-filtrate data or for other malicious purposes. Because there is no direct connection between the attacker and victim, it is more difficult to trace the attacker's computer.

Q4. WHAT IS COMMAND-AND-CONTROL?

Command-and-control attacks can compromise an entire network. Find out what they are and how they work.

Malicious network attacks have been on the rise in the last decade. One of the most damaging attacks, often executed over DNS, is accomplished through command and control, also called C2 or C&C.

The attacker starts by infecting a computer, which may sit behind a firewall.

This can be done in a variety of ways as below:

- Via a phishing email that tricks the user into following a link to a malicious website or opening an attachment that executes malicious code.
- Through security holes in browser plugins.
- Via other infected software.

Once communication is established, the infected machine sends a signal to the attacker's server looking for its next instruction. The infected computer will carry out the commands from the attacker's C2 server and may install additional software. The attacker now has complete control of the victim's computer and can execute any code. The malicious code will typically spread to more computers, creating a botnet – a network of infected machines. In this way, an attacker who is not authorized to access a company's network can obtain full control of that network.

Q5. WHAT CAN HACKERS ACCOMPLISH THROUGH COMMAND-AND-CONTROL?

1) Data Theft
Sensitive company data, such as financial documents, can be copied or transferred to an attacker's server.

2) Shutdown
An attacker can shut down one or several machines, or even bring down a company's network.

3) Reboot
Infected computers may suddenly and repeatedly shutdown and reboot, which can disrupt normal business operations.

4)Distributed Denial of Service.
DDoS attacks overwhelm server or networks by flooding them with internet traffic. Once a botnet is established, an attacker can instruct each bot to send a request to the targeted IP address, creating a jam of requests for the targeted server. The result is like traffic clogging a highway – legitimate traffic to the attacked IP address is denied access. This type of attack can be used take a website down.

Q6. WHAT IS A DISTRIBUTED DENIAL OF SERVICE ATTACK (DDoS)?

A Distributed Denial of Service (DDoS) attack is a variant of a DoS attack that employs very large numbers of attacking computers to overwhelm the target with bogus traffic. To achieve the necessary scale, DDoS are often performed by botnets which can co-opt millions of infected machines to unwittingly participate in the attack, even though they are not the target of the attack itself. Instead, the attacker leverages the massive number infected machines to flood the remote target with traffic and cause a DoS.

Though the DDoS attack is a type of DoS attack, it is significantly more popular in its use due to the features that differentiate and strengthen it from other types of DoS attacks:

- The attacking party can execute an attack of disruptive scale as a result of the large network of infected computers—effectively a zombie army—under their command.
- The (often worldwide) distribution of attacking systems makes it very difficult to detect where the actual attacking party is located.
- It is difficult for the target server to recognize the traffic as illegitimate and reject it an entry because of the seemingly random distribution of attacking systems
- DDoS attacks are much more difficult to shut down than other DoS attacks due to the number of machines that must be shut down, as opposed to just one.

DDoS attacks often target specific organizations (enterprise or public) for personal or political reasons, or to extort payment from the target in return for stopping the DDoS attack. The damages of a DDoS attack are typically in time and money lost from the resulting downtime and lost productivity.

Q6. WHAT IS A DISTRIBUTED DENIAL OF SERVICE ATTACK (DDoS)? (Continued...)

Examples of DDoS attacks are abundant. In January 2012, hacktivist cybergroup Anonymous conducted an attack multiple major supporters of the Stop Online Piracy Act (SOPA). In dissent of SOPA, Anonymous executed DDoS attacks that disabled the websites of the US Justice Department, the Federal Bureau of Investigations (FBI), the White House, the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), Universal Music Group, and Broadcast Music, Inc (BMI). To facilitate the attack, Anonymous built its botnet using an unconventional model that allowed users wishing to support the organization to offer their computers as a bot for the attacks. Users who wanted to volunteer support could join the Anonymous botnet by clicking links that the organization posted in various locations online, such as Twitter.

The DDoS attack is also leveraged as a weapon of cyber warfare. For example, in 2008 during the South Ossetia war, Georgian government websites were crippled by what is expected to be Russian criminal gangs under the auspices of the Russian security services. The attack was made just prior to Russia's initial attacks on Georgian soil.

There are a number of DDoS mitigation techniques that organizations can implement to minimize the possibility of an attack. Network security infrastructure should include DDoS detection tools that can identify and block both exploits and tools that attackers use to launch an attack. Additionally, network administrators can create profiles to observe and control specific floods of traffic (i.e. SYN floods, UDP, and ICMP floods). Through looking at all traffic in aggregate, thresholds can be set to monitor and cut behaviors that indicate a possible DDoS attack.


I-MEDITA
Training | Development | Placement
INDIA'S MOST TRUSTED
NETWORKING TRAINING COMPANY
CCNA

Q7. WHAT IS A MALWARE?

Malware (short for “malicious software”) is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. Though varied in type and capabilities, malware usually has one of the following objectives:

- Provide remote control for an attacker to use an infected machine.
- Send spam from the infected machine to unsuspecting targets.
- Investigate the infected user’s local network.
- Steal sensitive data.

Malware is an inclusive term for all types of malicious software, such as:

Viruses – Programs that copy themselves throughout a computer or network. Viruses piggyback on existing programs and can only be activated when a user opens the program. At their worst, viruses can corrupt or delete data, use the user’s email to spread, or erase everything on a hard disk.

Worms – Self-replicating viruses that exploit security vulnerabilities to automatically spread themselves across computers and networks. Unlike many viruses, worms do not attach to existing programs or alter files. They typically go unnoticed until replication reaches a scale that consumes significant system resources or network bandwidth.

Trojans – Malware disguised in what appears to be legitimate software. Once activated, Trojans will conduct whatever action they have been programmed to carry out. Unlike viruses and worms, Trojans do not replicate or reproduce through infection. “Trojan” alludes to the mythological story of Greek soldiers hidden inside a wooden horse that was given to the enemy city of Troy.

Q7. WHAT IS A MALWARE? (Continued...)

Rootkits – Programs that provide privileged (root-level) access to a computer. Rootkits vary and hide themselves in the operating system.

Remote Administration Tools (RATs) – Software that allows a remote operator to control a system. These tools were originally built for legitimate use, but are now used by threat actors. RATs enable administrative control, allowing an attacker to do almost anything on an infected computer. They are difficult to detect, as they don't typically show up in lists of running programs or tasks, and their actions are often mistaken for the actions of legitimate programs.

Botnets – Short for "robot network," these are networks of infected computers under the control of single attacking parties using command-and-control servers. Botnets are highly versatile and adaptable, able to maintain resilience through redundant servers and by using infected computers to relay traffic. Botnets are often the armies behind today's distributed denial-of-service (DDoS) attacks.

Spyware – Malware that collects information about the usage of the infected computer and communicates it back to the attacker. The term includes botnets, adware, backdoor behavior, keyloggers, data theft and net-worms.

Polymorphic Malware – Any of the above types of malware with the capacity to "morph" regularly, altering the appearance of the code while retaining the algorithm within. The alteration of the surface appearance of the software subverts detection via traditional virus signatures.

Q8. WHAT IS DENIAL OF SERVICE ATTACK (DoS)?

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- **Buffer Overflow Attacks –** the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks.
- **ICMP Flood –** leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- **SYN Flood –** sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

Q8. WHAT IS DENIAL OF SERVICE ATTACK (DoS)? (Continued...)

Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system, so that it can't be accessed or used.

An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once. The distribution of hosts that defines a DDoS provide the attacker multiple advantages:

- He can leverage the greater volume of machine to execute a seriously disruptive attack
- The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide)
- It is more difficult to shut down multiple machines than one
- The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems

Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still regarded as an elevated threat and is of higher concern to organizations that fear being targeted by such an attack.

Q9. STATE THE MOST COMMON ATTACKS METHODS FOR RANSOMEWARE ATTACKS.

The three most common attack methods for ransomware attacks are: silent infections from exploit kits, malicious email attachments, and malicious links in emails.

Exploit Kits:
Exploit kits are sophisticated toolkits that exploit vulnerabilities. Most often, exploit kits are executed when a victim visits a compromised website. Malicious code hidden on the site, often in an advertisement (malvertisement), redirects you to the exploit kit landing page unnoticed. If vulnerable, a drive-by download of a malicious payload will be executed, the system will become infected, and the files will be held for ransom.

Malicious Email Attachments:
With malicious email attachments, the attacker crafts an email, likely from a believable source, such as Human Resources or IT, and attaches a malicious file, such as a portable executable (PE) file, a Word document, or a .JS file. The recipient opens the attachment thinking the email has been sent from a trusted source. Once the file is opened, the ransomware payload is unknowingly downloaded, the system is infected, and the files are held for ransom.

Malicious Email Links:
Similar to malicious email attachments, malicious email links are URLs in the body of the email. Likewise, these emails are sent from someone or some organization that you believe to be a trusted source. When clicked, these URLs download malicious files over the web, the system is infected and the files are held for ransom.

Q10. EXPLAIN THE KEYS TO PREVENT RANSOMWARE?

Legacy cybersecurity approaches have focused on detection and remediation, but this is no longer effective. To prevent a ransomware attack, a shift in practice from detection to prevention is essential. Stop attacks before they can infect organizations. Organizations must have the appropriate security architecture in place to enable this shift, which has three key elements:

1. Reduce the attack surface

In order to reduce the attack surface, you must gain full visibility into traffic on your network, across applications, threats and user behavior. It is likely that if you don't know what is happening on your network, an attacker does and will use that as a way to get in. Classifying activity allows you to make the right decisions about what should be allowed, and it highlights unknown events that require further investigation. With this visibility, you can take actions, such as blocking unknown traffic, identifying advanced attacks, or simply enabling only the applications that have a valid business purpose.

Once the traffic has been delimited, application- and user-based policies need to be enforced. There are an infinite number of permutations for these policies that limit access to certain applications for certain groups of users and for certain portions of the network. With high visibility and the right policies, a large majority of the methods attackers use to deliver malware attacks on your network can be cut off.

To further reduce the attack surface, you need to block all dangerous and potentially dangerous file types. Although not all file types are malicious, those that have a higher probability of being malicious should be blocked. After dangerous file types have been blocked, policies aligned to your risk tolerance need to be implemented. Users should be prevented from connecting non-compliant endpoints to critical network resources.

Q10. EXPLAIN THE KEYS TO PREVENT RANSOMWARE? (Continued)

2. Prevent known threats

After you have reduced your attack surface, the next step would be to prevent known threats. To do this, you need to stop known exploits, malware, and command-and-control traffic from entering your network. Once those have been stopped, the cost of executing an attack rises and, subsequently, reduces its likelihood by forcing attackers to create new malware variants and launch new exploits against lesser-known vulnerabilities.

You also need to prevent users from inadvertently downloading a malicious payload or having their credentials stolen by preventing access to known malicious and phishing URLs. Blocking these threats removes them from the equation entirely. Once these known threats have been blocked, you need to scan for known malware on your SaaS-based applications, as they are increasingly leveraged to deliver threats. Any identified malware and exploits from the scan should be blocked. The same should be done for known malware and exploits on the endpoint.

3. Identify and prevent unknown threats

Once the known threats have been blocked, it is imperative to identify and block any unknown threats, as attackers continue to deploy new zero-day exploits and develop new ransomware variants. The first step would involve detecting and analyzing unknown threats in files and URLs. As new files are submitted, it is essential to detonate, analyze and look for malicious behavior in something that has never been seen. Additionally, you need to automatically push the protections down to different parts of the security infrastructure as fast as possible in order to prevent threats from becoming successful. This should include context to understand the attacker, malware, campaign, and indicators of compromise associated with the attack. Once unknown threats or trends of suspicious behavior have been identified and blocked, block unknown malware and exploits on the endpoint to ensure that all access points are secure.

Q11. WHAT MUST YOUR SECURITY ARCHITECTURE DO TO PREVENT RANSOMWARE?

Ransomware can bring your business operations to a halt, encrypting sensitive data and forcing you to pay the attacker to regain access. Keeping your organization safe requires a fundamental shift toward prevention, and away from simple detection and remediation after infection. The right architecture can make prevention real. You can use this checklist to implement a true prevention-based platform.

Step 1: Reduce the Attack Surface

- **Gain full visibility and block unknown traffic:**

Identify all traffic on the network and block unknown, potentially high-risk traffic.

- **Enforce application- and user-based controls:**

Restrict access to SaaS-based tools for employees who have no business need for them.

- **Block all dangerous file types:**

Not all file types are malicious, but those known to present higher risk, or associated with recent attacks, can be controlled.

- **Implement an endpoint policy aligned to risk:**

Enforce policies that restrict noncompliant endpoints from connecting to critical network resources.

Q11. WHAT MUST YOUR SECURITY ARCHITECTURE DO TO PREVENT RANSOMWARE? (Continued...)

Step 2: Prevent Known Threats

- **Stop known exploits, malware, and command-and-control traffic:**

Blocking known threats raises the cost of an attack and ultimately reduces the likelihood of an attacker attempting a breach.

- **Block access to malicious and phishing URLs:**

Prevent users from downloading a payload or having their credentials stolen by blocking known malicious and phishing URLs.

- **Scan for Known Malware on SaaS-Based Applications:**

SaaS-based applications represent a new path for malware delivery and must be properly secured.

- **Block Known Malware and Exploits on the Endpoint.**

Endpoints are common targets for attacks. Ensure you are keeping them secure by blocking any known malware or exploits.

Step 3: Identify and Prevent Unknown

- **Threats Detect and analyze unknown threats in files and URLs:**

As new files are submitted, detonate, analyze and look for malicious behavior.

- **Update protections across the organization to prevent previously unknown threats:**

Automatically push protections to different parts of your organization's security infrastructure.

- **Add context to threats, and create proactive protections and mitigation:**

Developing protections requires context to better understand the attacker, malware and indicators of compromise.

- **Block unknown malware and exploits on the endpoint:**

Once unknown threats or trends of suspicious behavior have been identified and blocked, block unknown malware and exploits on the endpoint.Related Resources

Baldev Singh
CCIE SECURITY #37094

Saurabh Yadav
Triple CCIE (R&S, Sec, SP) #46962

Sudhanshu Bhat
CCIE VOICE #41212

Surendra Singh
CCIE R&S #60346

GET TRAINED BY CERTIFIED AND WORLD CLASS TRAINERS

I-MEDITA
Training | Development | Placement

Q12. WHAT IS RANSOMWARE?

Ransomware is a criminal business model that uses malicious software to hold something of value for ransom, degrading or shutting down victim's operations.

Ransomware is a criminal business model that uses malicious software to hold valuable files, data or information for ransom. Victims of a ransomware attack may have their operations severely degraded or shut down entirely.

While holding something of value for ransom is not a new concept, ransomware has become a multimillion-dollar criminal business, targeting both individuals and corporations. Due to its low barrier to entry and effectiveness in generating revenue, it has quickly displaced other cybercrime business models and become the largest threat facing organizations today.

Q13. WHAT DOES A RANSOMWARE ATTACK LOOK LIKE?

Attackers must execute five steps for a ransomware attack to be successful:

- **Compromise and take control of a system or device**

Most ransomware attacks begin by using social engineering to trick users into opening an attachment or following a malicious link in their web browser. This allows attackers to install malware onto a system and take control.

- **Prevent access to the system**

Once they have system access, attackers will either identify and encrypt certain file types or deny access to the entire system.

- **Notify the victim**

Naturally, attackers and victims often speak different languages and have varying levels of technical capabilities. Attackers must alert victims to the compromise, state their ransom demand and explain the steps for regaining access.

- **Accept ransom payment**

To receive payment while evading law enforcement, attackers demand crypto-currencies, such as bitcoin, for the transaction

- **Return full access**

Attackers must return access to the device(s). Failure to restore access to compromised data or systems undermines the scheme as few would be willing to pay a ransom if they didn’t believe their valuables would be returned.

Q14. WHAT IS A CREDENTIAL BASED ATTACK?

Credential based attacks occur when attackers steal credentials to gain access, bypass an organizations security measures, and steal critical data.

Credential theft, the first stage of a credential-based attack, is the process of stealing credentials. Attackers commonly use phishing for credential theft, as it is a fairly cheap and extremely efficient tactic. The effectiveness of credential phishing relies on human interaction in an attempt to deceive employees, unlike malware and exploits, which rely on weaknesses in security defenses.

Corporate credential theft is usually a targeted effort. Attackers scour social media sites such as LinkedIn, searching for specific users whose credentials will grant access to critical data and information. The phishing emails and websites utilized in corporate credential theft are much more sophisticated than those used for consumer credential theft. Attackers put a great deal of effort into making these emails and websites look nearly identical to legitimate corporate applications and communications.

It is in this phase of credential-based attacks that security awareness training plays a role as the first line of defense. Unfortunately, there is no guarantee that employees will identify a phishing attempt 100 percent of the time. To minimize credential theft, corporate credentials should be limited to approved applications, and usage should be blocked from unlikely or unknown applications and sites. Security products be capable of blocking corporate credentials from ever leaving the organization’s network, and prevented from being submitted to malicious sites.

Q15. WHAT IS CREDENTIAL ABUSE?

Credential abuse is the actual use of compromised passwords to authenticate applications and steal data.

Once an attacker gets a hold of user credentials and passwords, they can sell the credentials in the cyber-crime underground or use them to compromise an organization's network, bypassing all security measures to keep an adversary out, move laterally within the network and steal data.In an unsegmented environment, an attacker can move freely across an organization's network. If the environment is segregated and provides visibility across users and applications, security measures can be put in place to prevent an attacker from moving laterally and gaining access to critical data.

Once an attacker has the credentials to operate like a valid user, there is very little that can be done to identify an intruder and validate if that user is really the person their credentials claim them to be. Organizations commonly implement multi-factor authentication within applications to require users to validate their identity more than once. However, doing this for every individual application used within the organization is not scalable. Implementing policy-based, multi-factor authentication at the network layer, meaning in the firewall, will provide the needed scale and end-user ease of use.

The Palo Alto Networks Next-Generation Security Platform stops the credential-based attack lifecycle in multiple places, from the theft of credentials to the abuse of stolen credentials. The combined prevention capabilities of the Next-Generation Firewall, Threat Prevention, WildFire and URL Filtering stops known and unknown attacks used for the theft and abuse of credentials, while GlobalProtect extends protections from the platform to mobile workforces and provides additional measures to identify users and devices that are accessing applications.

Q16. STATE DIFFERENT TYPES OF UNKNOWN CYBER THREATS?

Most traditional security products are built to act based on known threats. The moment they see something that is known to be malicious, they block it. To get past security products that successfully block known threats, attackers are forced to create something that has never been seen before, increasing the cost to execute an attack. How do they do it, and what can we do to prevent both known and unknown threats?

Let’s look at a few scenarios:

- Recycled Threats
- Modified Existing Code
- Newly Created Threats

All the above are explained below.

Q17. WHAT ARE RECYCLED THREATS?

Recycled Threats

Recycled threats are considered to be the most cost-effective attack method, which is why attackers often recycle existing threats using previously proven techniques. All security products have limited memory, and security teams choose the most up-to-date threats to protect against, hoping they will block the majority of incoming attacks. If an older threat, not tracked by the security product, attempts to enter the network, it could bypass the security product because it is not categorized as something seen before.

To protect against these “unknown” recycled threats, it is critical to have access to a threat intelligence memory keeper, often placed in an elastic cloud infrastructure capable of scaling to address the volume of threat data. In the event that a security product doesn’t have a particular threat identified and stored, access to the larger knowledge base of threat intelligence could help determine if something is malicious and enable the security product to block it.

Q18. WHAT IS A MODIFIED EXISTING CODE?

Modified Existing Code

Attackers take an existing threat and make slight modifications to the code, either manually or automatically, as the threat actively transitions in the network. This results in polymorphic malware or a polymorphic URL. Like a virus, the malware continuously and automatically morphs and changes rapidly. If a security product identifies the original threat as known and creates a protection for it based on only one variation, any slight change to the code will turn that threat into an unknown.

Some security products match threats using hashing technology, which generates an entirely unique number based on a string of text in such a way that it becomes impossible to get two identical hashes. Here, the hash value only matches one variation of the threat, so any new variation of the threat will be considered new and unknown.

To better protect against these threats security products need to use polymorphic signatures. Polymorphic signatures are created based on the content and patterns of traffic and files, rather than on a hash, and can identify and protect against multiple variations of a known threat. The focus on the behavior, rather than the appearance of fixed encoding, allows for the detection of patterns in modified malware.

Q19. WHAT ARE NEWLY CREATED THREATS?

Attackers who are more determined and willing to invest the money will create an entirely new threat with purely new code. All aspects of the cyber attack life-cycle have to be new for an attack to truly be considered a previously unknown threat.

- **Focus on Business Behavior**

Protecting against these new threats requires focus on your unique business behavior and data flows. This information can then be implemented into cybersecurity best practices. As an example, leveraging segmentation with user ID and application ID can help prevent new threats from spreading throughout your organization and block downloads from new, unknown and unclassified websites.

- **Utilize Collective Intelligence**

No single organization will ever experience all new threats, which is why it is so important to be able to benefit from collective threat intelligence. Targeted attacks with unknown, never-before-seen threats can quickly become known with global information sharing. When a new threat is analyzed and detected in one organization, the newly identified threat information can be distributed across the community, with mitigations deployed ahead of time to limit the spread and effectiveness of attacks.

Turning unknown threats into known threats and actively preventing against them happens in a combined environment. First, you need to predict the next attack step and location. Second, you need to be able to develop and deliver protection quickly to the enforcement point in order to stop it.

Rasika Joshi
COMPUCOM

Nakul Sonare
ZENSAR TECHNOLOGIES

Minal Ghubde
ZENSAR TECHNOLOGIES

Ketan Panpate
COMPUCOM

Mayank Chauhan
COMPUCOM

Prakash Datta
TRIOS

Vaibhav Bindu
TATA COMMUNICATIONS LIMITED

Mangesh Dhongade
COMPUCOM

Amol Sankpal
SECURVIEW

Piysuh Shrungare
ZENSAR TECHNOLOGIES

Khyati Sawant
SOPHOS

Abhijeet Kamble
COMPUCOM

Pankaj Sakore
NETSCOUT

Akshita Mankad
COMPUCOM

Amey Malotkar
AGC NETWORKS LIMITED

Arpit Kansal
CRYSTALVOXX

Pravin Valkunde
SECURVIEW

Rohit Naidu
TATA COMMUNICATIONS LIMITED

Hussain Sagwadiya
ZENSAR TECHNOLOGIES

Pravin Kawale
SECURVIEW

I-MEDITA
Training | Development | Placement

SHAPING CAREER

EMPOWERING FUTURE

Q20. HOW TO AUTOMATE PROTECTION?

When a truly new threat enters your organization, the first line of defense is having cybersecurity best practices that are specific to the organization. At the same time, you should be sending unknown files and URLs for analysis. The effectiveness of sandbox analysis depends on the time it takes to provide an accurate verdict on an unknown threat and to create and implement protections across the organization, as well as how your sandbox environment handles evasive threats. Your security posture needs to be changed fast enough to block the threat before it has the ability to progress – in other words, as soon as possible. And to ensure that this threat does not further traverse the network, preventions need to be created and implemented automatically across all security products faster than the threat can spread.

A recent SANS survey reported that 40 percent of attacks have previously unknown elements. The ability to detect unknown threats and prevent successful attacks defines the effectiveness of your security deployment. A true next-generation security platform is agile, quickly turning unknown threats into known protection and prevention on a global level. Automatically sharing new threat data while extending new protections throughout the organization to stop the spread of an attack.

Q21. EXPLAIN CYBERCRIME PRODUCTS.

The products of the cybercrime economy, similar to any other product in any other industry, benefit both the seller and the buyers. The sellers benefit from quick and discrete payout and the buyers benefit from “out of the box” malicious operations that can be implemented immediately. These products can be broken down into two main categories: information and resources.

Information includes commodities such as:

- **Stolen Personally Identifiable Information (PII):**
  This includes everything from mass email lists used by spammers to full identity theft packages to commit financial fraud.

- **Exfiltrated Organizational Information**:
  This includes intellectual capital/property, nonpublic internal data and internal operational details.

- **Harvested Authentication Credentials:**
  Stolen username and password combinations continue to present a significant risk these days, especially when the same credentials are re-used across multiple sites.

- **Pilfered Financial Data**:
  Unauthorized withdrawals from accounts or charges against credit lines continue to plague account holders.

Q21. EXPLAIN CYBERCRIME PRODUCTS. (Continued...)

Resources include such element as:

- **Access to feature-rich malware:**
  Malware across varying capabilities (e.g., information stealers, remote administration tools – RATs, ransomware, purpose-built utilities) that demonstrate consistent results and avoid source code leakage can generate significant revenue for associated authors and distributors.

- **Purchase of system or software exploits:**
  While many white hats elect to support bug bounty initiatives by vendors, there remains a lucrative underground market for reliable, unpatched exploits.

- **Transfer of control for previously compromised machines:**
  It usually applies to always-on servers that can then be used as attack platforms or sold for the information they store.

- **Malicious actor training:**
  Training is offered through guidebooks or tutorials on effective tool usage and specific tactics, techniques and procedures (TTPs).

Q22. EXPLAIN CYBERCRIME SERVICES.

The services offered within the cybercrime economy utilizes a leasing structure, in which access to a product is promised at a set rate for a fixed period of time. The sellers benefit from a guaranteed source of recurrent revenue throughout an extended period of time, and buyers benefit from the continued availability and performance of malicious tools. The services include:

- **Distributed denial of service (DDoS):**
  These are botnet powered attacks that affect the availability of targeted servers and capabilities.

- **Exploit kits (EKs):**
  As part of the service offering, exploit kits are typically leased with a monthly rate for access to the exploit toolkit, allowing for customized end payloads.

- **Infrastructure rental:**
  These include hosting services for attack platforms, malware updates, configuration, command and control (C2), and other attack lifecycle functions.

- **Money laundering:**
  This is known as the transfer (“money muling”) of illegally obtained funds through accounts and mechanisms in money haven countries remains a key service.

Q23. WHAT ARE THE CHALLENGES FACED WHILE IDENTIFYING EVASIVE THREATS?

Organizations struggle to identify these highly evasive threats and often fail to prevent them. Here are three key challenges businesses and security tools face when combating evasive threats:

1. There is a Marketplace for Evasive Threats:

Security professionals have developed defenses to detect cyberthreats, such as virtual malware analysis environments, while threat actors have simultaneously incorporated automation and commodity hardware into well-defined “playbooks” that are available in the cybercrime underground. This has removed barriers for ease of implementation by a variety of threat actors ranging from less sophisticated novices to advanced attackers and organized nation-states. As a result, there has been an increase in the number of sophisticated attacks and the likelihood of successful data breaches.

2. Traditional Defenses are No Longer Enough:

Evasive malware uses malicious code that hides its identity and intentions from detection by traditional malware analysis environments. The attacker searches for indicators that the malware is in a virtual environment. They look to see if the file is detonated and observed; lack of valid user activity such as clicking on a keyboard, moving a mouse or plugging in a USB stick, etc.

3. Open Source Software Hurts More Than Helps:

Open source has provided a revolutionary way to develop software but when it comes to threat analysis, open source has become more of a detriment. The majority of malware analysis environments utilize open source, and attackers have leveraged known vulnerabilities to their advantage. Malware authors design threats with the ability to spot and evade detection techniques.

Q24. HOW DOES PALO ALTO HELP PROTECT AGAINST EVASIVE THREATS?

Palo Alto Networks Next-Generation Security Platform approaches evasive threat detection and prevention with these three things in mind. An integral part of the platform is **WildFire** threat analysis service – incorporating static analysis; dynamic analysis in a custom-built virtual analysis environment; machine learning; and a bare metal analysis environment for full hardware execution.

Also part of the Next-Generation Security Platform is **AutoFocus Contextual Threat Intelligence Service**, which provides the information necessary to understand why, where and how an attack will impact a network. It answers questions like “Who is attacking?” “What tools are they using?” and “How is this going to impact the network?” and automatically prioritizes targeted attacks. The result is faster analysis, easier correlation and rapid incident response.

Palo Alto Networks® Next-Generation Security Platform spans the network, cloud and endpoint, automatically preventing even the most evasive known and unknown malware and zero-day threats with high efficacy and near-zero false positives.

Q25. STATE 3 WAYS TO PREVENT EVASIVE THREATS?

1. Use Purpose-Built Virtual Analysis

To detect highly evasive malware, use a purpose-built virtual analysis environment that incorporates a unique hypervisor and emulator that doesn't rely on open source or proprietary software. This environment should not show characteristics that would divulge to the attacker that they have been spotted or the malware's behavior is being observed.

2. Employ Bare Metal Analysis

The use of a virtual environment for malware analysis is unavoidable. However, samples displaying evasion techniques in a virtual environment should also be detonated on real hardware systems, also known as bare metal analysis environments. To avoid raising suspicion with attackers, the suspected files should be dynamically steered to the bare metal environment without human intervention.

3. Incorporate Threat Intelligence

To combat the rise of highly evasive threats available in the underground economy, organizations should incorporate highly contextual and actionable threat intelligence into their security defenses.Threat intelligence should come from multiple sources and be correlated and validated for necessary context. Without proper context, threat intelligence merely adds to the noise with overwhelming amounts of raw indicators of compromise. The result is an increase in false positives and negatives, requiring security staff for any actionable response. Additionally, integrating threat intelligence with virtual analysis environments enables rapid, automated prevention, minimizing the need for additional specialized staff.

Q26. HOW TO BREAK THE CYBER ATTACK LIFE CYCLE?

The following are the different stages of the attack lifecycle and steps that should be taken to prevent an attack at each stage.

1. Reconnaissance:

Cyber adversaries research, identify and select targets that will allow them to meet their objectives. Attackers gather intel through publicly available sources, such as Twitter, LinkedIn and corporate websites. They will also scan for vulnerabilities that can be exploited within the target network, services, and applications, mapping out areas where they can take advantage. At this stage, attackers are looking for weaknesses based on the human and systems perspective.

2. Weaponization and Delivery:

Attackers will then determine which methods to use in order to deliver malicious payloads. Some of the methods they might utilize are automated tools, such as exploit kits, spear phishing attacks with malicious links, or attachments and malvertizing.

3. Exploitation:

In this stage, attackers deploy an exploit against a vulnerable application or system, typically using an exploit kit or weaponized document. This allows the attack to gain an initial entry point into the organization.

4. Installation:

Once they've established an initial foothold, attackers will install malware in order to conduct further operations, such as maintaining access, persistence and escalating privileges.

Q26. HOW TO BREAK THE CYBER ATTACK LIFECYCLE? (Continued..)

5. Command and Control:
With malware installed, attackers now own both sides of the connection: their malicious infrastructure and the infected machine. They can now actively control the system, instructing the next stages of attack. Attackers will establish a command channel in order to communicate and pass data back and forth between the infected devices and their own infrastructure.

6. Actions on the Objective:
Now that the adversaries have control, persistence and ongoing communication, they will act upon their motivations in order to achieve their goal. This could be data exfiltration, destruction of critical infrastructure, to deface web property, or to create fear or the means for extortion.

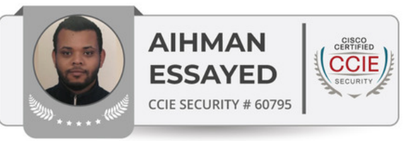
To read in detail about the above, click on the link below:
https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

RECENT CCIE FROM I-MEDITA

AMIT KHARUDE
CCIE SECURITY # 61023

KISHAN PATEL
CCIE R&S #57009

SAGAR PARIKH
CCIE R&S #57008



AIHMAN ESSAYED
CCIE SECURITY # 60795

SUNIL KUMAR
CCIE SECURITY # 60728

S. PATHAK
CCIE SECURITY # 60434

DEEPTIRANJAN
CCIE SECURITY # 60711

PRAKASH
CCIE SECURITY # 60537

MOHIT SONI
CCIE SECURITY # 60793

HASEEB MUSTAFA ALVI
CCIE R&S #59325

HAMID
CCIE R&S # 38970

SANDEEP BISHT
CCIE R&S # 60219

ALI
CCIE R&S # 41838

MALAY
CCIE R&S # 55682

HIKMAT ULLAH
CCIE R&S # 54119

ASMAT ULLAH
CCIE R&S # 55710

SAMEER KOTAK
CCIE R&S # 54932

SUMIT SINGH
CCIE SECURITY # 61271

SAQIB
CCIE SECURITY #61087

SURENDRA SINGH
CCIE R&S #60346

RAVI DHRUV
CCIE R&S # 60014

I-MEDITA
Training | Development | Placement

HELPING STUDENTS

BECOME CERTIFIED

Q27. WHAT IS SPYWARE?

Spyware is a type of malware (or “malicious software”) that collects and shares information about a computer or network without the user’s consent. It can be installed as a hidden component of genuine software packages or via traditional malware vectors such as deceptive ads, websites, email, instant messages, as well as direct file-sharing connections. Unlike other types of malware, spyware is heavily used not only by criminal organizations, but also by unscrupulous advertisers and companies who use spyware to collect market data from users without their consent. Regardless of its source, spyware runs hidden from the user and is often difficult to detect, but can lead to symptoms such as degraded system performance and a high frequency of unwanted behavior (pop-ups, rerouted browser homepage, search results, etc.).

Spyware is also notable for its networking capabilities. Using an infected system to find information is of little value if the spyware can’t deliver that information back to the attacker. As a result, spyware employs a variety of techniques to communicate back to an attacker in a way that will not cause suspicion or generate attention from network security teams.

As a tool for advertising, spyware is used to collect and sell user information to interested advertisers or other interested parties. Spyware can collect almost any type of data including web browsing habits and download activity. Perhaps the greatest concern related to spyware is that—regardless of whether it’s presence detectable or not—the user has neither any idea of what information is being captured, sent away, or used, nor any mechanism or technology for finding out.

Q27. WHAT IS SPYWARE? (Continued...)

Spyware can use keyloggers to obtain personal details such as the user's name, address, passwords, bank and credit information, and social security information. It can scan files onto the system's hard drive, snoop other applications, install additional spyware, read cookies and modify the system's internet settings and dynamically linked libraries (DLL). This can result in lowered security settings (to invite in more malware), and malfunctions on the Internet and computer varying from numerous pop-up advertisements, whether on or offline, to connectivity failures sourced deep in the Internet settings of the system. Many of these changes are difficult to reverse or recover from without reimaging the affected device.

Spywares pose to infected computers, it can also be a major consumer of system resources, often hogging up processor power, RAM, disks, and network traffic. The resulting performance degradation can lead to crashes or general system instability. Some spyware even disable or eliminate competing spyware programs, and can detect and intercept the user's attempts to remove it.

Spyware can be prevented through a combination of endpoint and network security controls. Antispyware features are often integrated into modern antivirus software products that provide protection at the endpoint. Given the need for spyware to communicate over the network, spyware is also increasingly being controlled at the network security layer, where spyware communications can be detected and blocked. Additionally, drive-by download protections can be enforced at the end-point by using the browser's pop-up blocker as well as via next-generation network controls that prevent the download of files without the user's consent. Lastly, it is important to monitor and validate which software components, plug-ins and services are allowed to run on a device as well as on the network; if the software is not recognizable or there is no specific reason to trust it, it is safer not to accept it until conducting further research.

Q28. What is a Botnet?

A botnet (short for “robot network”) is a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.” Each individual machine under the control of the bot-herder is known as a bot. From one central point, the attacking party can command every computer on its botnet to simultaneously carry out a coordinated criminal action. The scale of a botnet (many comprised of millions of bots) enable the attacker to perform large-scale actions that were previously impossible with malware. Since botnets remain under control of a remote attacker, infected machines can receive updates and change their behavior on the fly. As a result, bot-herders are often able to rent access to segments of their botnet on the black market for significant financial gain.

Common botnet actions include:

- Email spam
- DDoS attacks
- Financial breach
- Targeted intrusions

To continue reading in detail, click on the link below:
https://www.paloaltonetworks.com/cyberpedia/what-is-botnet

Q29. WHAT IS A PHISHING ATTACK?

Phishing attacks are an email-based form of social engineering. Disguised as legitimate communication, the fraudulent email tricks the recipient into responding by enticing them to click a link, open an attachment, or directly provide sensitive information.

Attack Methods:

Low: These emails are untargeted and deployed in bulk, casting a wide net in an effort to successfully victimize at least one recipient. These emails contain several “tells” that indicate an attack, such as improper grammar or plain text, or they are sent from an unknown or improbable source.

Moderate: More believable, these emails contain real branding from real websites. They have legitimate formatting and proper grammar, but remain impersonal.

Complex: These types of phishing attacks are the most difficult to identify. They are realistic and highly personal, coming from known or trusted sources. The attackers utilize specific, known details about the recipient gathered from internal and public sources to trick the recipient into taking the desired action.

The email will also contain a malicious element necessary to execute the attack and compromise the user.

- **Click only:** This is a one-step process in which the email urges the recipient to click an embedded link.
- **Data entry:** The email includes a link to a customized landing page that requires the user to enter sensitive information.
- **Attachment-based:** The email contains a legitimate attachment that could be in varying formats (Word, Excel®, PDF, etc.).
- **Double barrel:** This utilizes two emails. One is benign and doesn’t contain anything malicious nor does it require a response; the second is a follow-up that contains the malicious element in either of the above forms.

Q30. HOW TO PREVENT A PHISHING ATTACK?

As with any organization, a comprehensive security platform that addresses people, technology and process minimizes the likelihood of a successful phishing attack. In the case of people, security awareness training will educate the recipients on what to look for in a phishing email and to report suspicious emails to their security teams.

When it comes to technology, the utilization of sandboxing will analyze the unknown link or file and implement policy to prevent access if it is determined malicious; URL filtering will block known malicious websites and unknown websites to prevent attacks early on; and access to a threat intelligence cloud provides the combined knowledge of the global community, enabling protections if a similar attack has been seen before.

To address the process, there should be a hierarchy of actions to take should a phishing attack successfully penetrate the network.

Q31. WHAT IS A EXPLOIT KIT?

Exploit kits were developed as a way to automatically and silently exploit vulnerabilities on victims' machines while browsing the web. Due to their highly automated nature, exploit kits have become one of the most popular methods of mass malware or remote access tool (RAT) distribution by criminal groups, lowering the barrier to entry for attackers. Exploit kits are also effective at generating profit for malicious actors. Creators of exploit kits offer these campaigns for rent on underground criminal markets in the form of exploit kits as a service, where the price for leading kits can reach thousands of dollars per month.

Landing Page

Exploit kits start with a website that has been compromised. The compromised page will discreetly divert web traffic to another landing page. Within the landing page is code that will profile the victim's device for any vulnerable browser-based applications. If the device is fully patched and up-to-date, the exploit kit traffic will cease. If there are any vulnerabilities, the compromised website discreetly diverts network traffic to the exploit.

Exploit

The exploit uses a vulnerable application to secretly run malware on a host. Targeted applications include Adobe® Flash® Player; Java® Runtime Environment; Microsoft® Silverlight, whose exploit is a file; and the web browser, whose exploit is sent as code within web traffic.

Q31. WHAT IS A EXPLOIT KIT? (Continued...)

If and when an exploit is successful, the exploit kit sends a payload to infect the host. The payload can be a file downloader that retrieves other malware or the intended malware itself. With more sophisticated exploit kits, the payload is sent as an encrypted binary over the network, which, once on the victim's host, is decrypted and executed. While the most common payload is ransomware, there are many others, including botnet malware, information stealers and banking Trojans.

A recent example of this is the utilization of the Neutrino exploit kit to deliver Locky ransomware in the Afraidgate campaign. Pages from the compromised site contain an injected script that redirects visitors to the Afraidgate domain. Once connected to the compromised URL, the server returns more JavaScript with an iframe, leading to a Neutrino exploit kit landing page. If the exploit of the vulnerability with JavaScript is successful, the Locky ransomware payload will be delivered, and the host system will lock out the user and give control to the attacker.

With exploit kits becoming the go-to tool for attackers of varying skill sets and objectives, it is imperative that your systems are able to protect against these attacks. This can be achieved through reducing the attack surface, blocking known malware and exploits, and quickly identifying and stopping new threats. The Palo Alto Networks Next Generation Platform proactively blocks known threats while using static and dynamic analysis techniques to identify unknown threats. Any unknown files, emails and links are analyzed in a scalable sandbox environment to determine if they are malicious or benign. If a file is determined to be malicious, protections are created automatically and delivered across all technologies within the platform for full protection, preventing exploit kits from progressing further throughout their lifecycle.

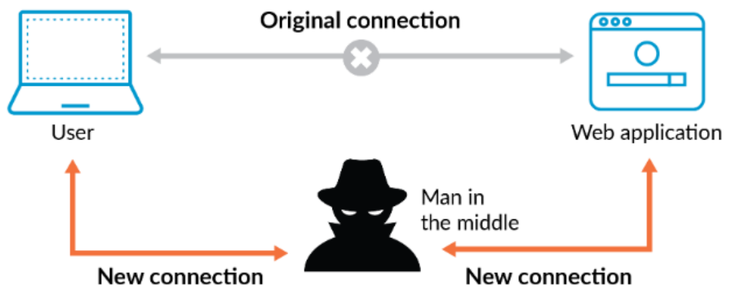
Q32. WHAT IS DNS HIJACKING?

Cybercriminals know that DNS – or Domain Name System – is a trusted, ubiquitous protocol, and many organizations don't monitor their DNS traffic for malicious activity. Because of this, DNS can serve as the medium for a variety of attacks against company networks. In fact, DNS-based attacks have been on the rise in the last decade.

DNS is the protocol that translates human-friendly URLs into machine-friendly IP addresses. Once you initiate a query by typing ww.paloaltonetworks.com into your browser, for instance, a request is sent to a DNS resolver, a computer that tracks down the IP address – in this case, 199.167.52.137. The DNS resolver does this by communicating with top-level domain and root servers, and then sending a response back to your computer.

Here are two common ways in which DNS hijacking occurs:

1. **"Man-in-the-middle" attacks**: An attacker intercepts a user's DNS requests and redirects them to the attacker's own compromised DNS server.



I-MEDITA
Training | Development | Placement

WORLD CLASS INFRASTRUCTURE

Q32. WHAT IS DNS HIJACKING? (Continued...)

2. Attacks that use malware: An attacker infects a victim's machine through email or other malicious activity. The malware changes the victim's settings and redirects DNS requests to the attacker's DNS server. As long as the user's browser displays the original URL, the user will likely believe the website is genuine. Roaming Mantis, one such piece of malware, infected Android-based tablets and smartphones around the world in 2018.

DNS hijacking can be used for phishing, to serve users statistics or advertisements, or to collect user information.

Q33. WHAT IS MALWARE PROTECTION?

Malware is designed to spread quickly, create havoc and affect as many machines as possible. To protect your organization against such threats, you need a holistic, enterprise-wide malware protection strategy. Your strategy should include includes a global threat intelligence community and covers the network, endpoint and cloud.

Threat Intelligence

A successful military operation relies on credible threat intelligence to make executive decisions. Similarly, contextual threat intelligence shared with a global community enables organizations to respond to attacks more quickly. Security analysts can subscribe to premium and free versions of global threat feed to help their teams stay ahead of attackers.

Network

Everything runs on the network. Business transactions, application deployments, access to resources, web browsing and video streaming all depend on the network running smoothly. The network is also a doorway to your most critical business assets, and it needs protection. Firewalls, intrusion prevention systems, URL filtering and sandboxing systems are typically deployed to protect the network by detecting, analyzing and preventing malicious activity.

Q33. WHAT IS MALWARE PROTECTION? (Continued...)

Endpoint

The main targets for attackers are mostly laptops, desktop computer and servers – wherever there is valuable data. Attackers look for vulnerabilities and target users with credential theft, phishing and social engineering. Organizations can deploy endpoint security products like antivirus, anti-spam and anti-malware in the form of agents that protect against advanced attacks. These agents can provide effective malware protection by employing static and dynamic malware analysis.

Cloud

More organizations are moving their critical assets to the cloud for its scalability, agility and cost savings. However, there are some security risks organizations must address. Hackers go after your data no matter where it lives, so cloud infrastructure is still open to cyber-attacks similar to those that target traditional data centers. To protect against malware, you need to gain complete visibility into your cloud infrastructure, provide strong protections for incoming and outgoing traffic, secure your containers, and run compliance audits to expose data leaks.

The key is to seamlessly integrate cloud, network and endpoint security with global threat intelligence to quickly detect and deliver automated malware protections in near-real time. Tight integration across your network, cloud and endpoint environments, coupled with global threat intelligence, simplifies security so you can secure your users, applications and data everywhere.

Q34. WHAT IS BROWSER CRYPTOCURRENCY MINING?

How It Works

Cyber-criminals will compromise a website and abuse a legitimate tool on that site to gain access to the compute resources of site visitors' systems. Using this access, attackers will essentially steal compute resources and exchange them for cryptocurrency credit. This all occurs without the users' consent or knowledge throughout the duration of their site visits.The malicious activity itself doesn't cause long-term damage to systems, and ends as soon as users leave the malicious or compromised site. Additionally, the site will still provide users with its normal, intended functionality. However, users likely experience a noticeable slowdown in system performance.

How to Defend Against It

If you believe your system is being affected by this type of attack, leaving the site or closing your browser will, in most cases, end the attack. Additionally, you should practice good cybersecurity hygiene. This means avoiding unfamiliar websites, clicking on links or downloading attachments from unknown email senders, keeping products updated with the latest security patches, enabling multi-factor authentication, and using reputable security products.

Q35. WHAT IS AN ANDROID TOAST OVERLAY ATTACK?

How it Works

The vulnerability affects the Toast feature on Android devices, an Android feature that allows display messages and notifications of other applications to “pop up,” and allows an attacker to employ an overlay attack.An overlay attack happens when an attacker places a window over a legitimate application on the device. Users will interact with the window, thinking they are performing their intended function, but they are actually engaging with the attackers overlay window and executing the attacker’s desired function. You can see an example of how this would work in Figure 1.

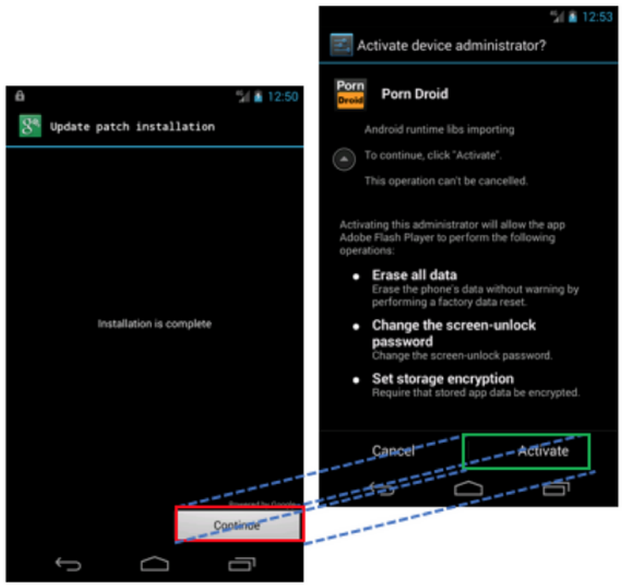


Figure 1: Bogus patch installer overlying malware requesting administrative permissions

This interaction can install malware or malicious software on the device, grant malware full administrative privileges or lock the user out and render the device unusable.

In the past successful overlay attacks were typically dependent on two conditions:

1) The malicious application must be downloaded from Google Play.
2) The malicious application must explicitly request permissions from the user to enable the “draw on top” functionality, allowing the application to display something on the window even if the application is not in the foreground.

However, with this particular vulnerability, these conditions are no longer required for a successful attack. This means that attackers can use this vulnerability in apps users get from places other than Google Play. And when they install these malicious apps, they don’t have to ask for the “draw on top” permission.

Q35. WHAT IS ANDROID TOAST OVERLAY ATTACK? (Continued...)

How to Defend Against It

Keeping devices updated is a general security best practice. The Android Toast Overlay attack specifically targets outdated devices using versions prior to 8.0. In order to defend against the Android Toast Overlay attack, update all Android devices to the latest version. Additionally, avoid downloading malicious applications by only downloading from the Google Play store is another best practice you should always follow.

Q36. WHAT IS FREEMILK CONVERSATION HIJACKING SPEAR PHISHING CAMPAIGN?

Unit 42 released details about a new spear phishing campaign called FreeMilk that uses a relatively new attack technique that can be highly effective. This is the kind of technique that is likely to be aimed at high value targets. Targets of these attacks are likely to be individuals with access to valuable or sensitive information such as members on a Board of Directors, C-level executives, military and political personnel, or those with compromising information such as journalists or activists. Individuals close to those previously mentioned could also be used as part of the attack campaign such as an executive assistant to a CEO or even friends or family.

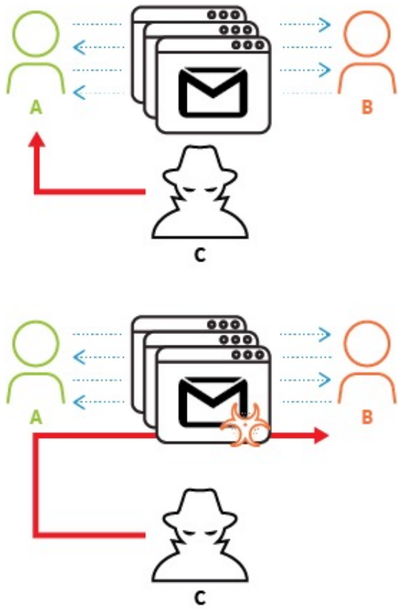
How it Works

Phishing attacks are broad, leveraging email messages crafted around common, generalized topics in order to trick recipients into opening an email message and its attachments. Attackers will cast a wide net, with no regard to who the victims are, hoping that a decent percentage of attacks are successful.

Spear phishing, like the name implies, is a more targeted form of phishing which incorporates a theme directly related to the target. Using this approach, victims are more inclined to trust the sender, and open the email message and any attachments resulting in the success of the attack.

FreeMilk is an advanced spear phishing attack campaign that, instead of using a theme to lure targets into downloading a malicious attachment, hijacks an in-progress email conversation.

Q36. WHAT IS FREEMILK CONVERSATION HIJACKING SPEAR PHISHING CAMPAIGN? (Continued...)



Simply explained:

- Alice (A) and Bob (B), are having an ongoing email conversation.
- The attacker, Charlie (C) will carry out an attack, likely using some form of credential theft, in order to gain control to Alice's email account.
- Using Alice's email account, Charlie sends an email containing a malicious attachment that appears to be relevant to the ongoing email conversation between Alice and Bob.
- Bob receives the email, and thinking it's from Alice, opens the malicious attachment and the attack is successful.

How to Defend Against It

Unit 42 observed this specific attack taking advantage of a vulnerability in Microsoft Office, which has a patch available. To protect against FreeMilk and attacks alike, ensure your systems and devices are updated with the latest operating systems and security patches.

Additionally, multiple layers of security for devices and networks create additional layers of protection to prevent against these types of attacks. For example, multi-factor authentication would prevent an attacker from abusing stolen credentials, hindering their ability to access an email account and successfully complete the FreeMilk attack campaign.

Q37. EXPANDING TARGETS FOR NEW SUNORCAL MALWARE VARIANT

While investigating Reaver we recently also discovered a new variant of the SunOrcal malware family. While the SunOrcal malware family has been confirmed to have been active since 2013, possibly even earlier, this new variant has been observed targeting regions outside of the typical target radius for this threat group, now expanding to include Vietnam and Myanmar.

How it Works

Emails were sent to targets containing malicious attachments. Targeting a Vietnamese speaking audience, one of the malicious documents mentions Donald Trump and the disputed South China Sea area. This is a classic lure technique – including something the target will find interesting or important causing them to open the file and download the malware on to the victims' system.

How to Defend Against it

These malware attacks utilize email phishing, and relies on targets opening the malicious email attachment. Security awareness is critical to avoid falling victim to such an attack.

General email best practices:

- Make sure the sender is a trusted source. If you've never received something from them before, or the email address has typos, don't open it.
- If the sender appears to be convincing, pay close attention to the body of the email. Are there a lot of typos? Does the branding/logo look different? Does it look unprofessional?
- Never click on a link within the email or download an attachment.
- Don't respond to the email with any password or personal information.