ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks: Does remote work?

Vulnerabilities at home

threat-talks.com

Allowing remote access, whether it is for remote workers or partners, is required for almost all enterprises. But enabling remote access doesn't just bring flexibility, it comes with a number of security concerns.

Cybercriminals have honed in on the vulnerabilities of widely used remote work technologies. What are those technologies and what are those vulnerabilities? Below you'll find infographics on remote work in general, as well as three recent threats associated with working from home.

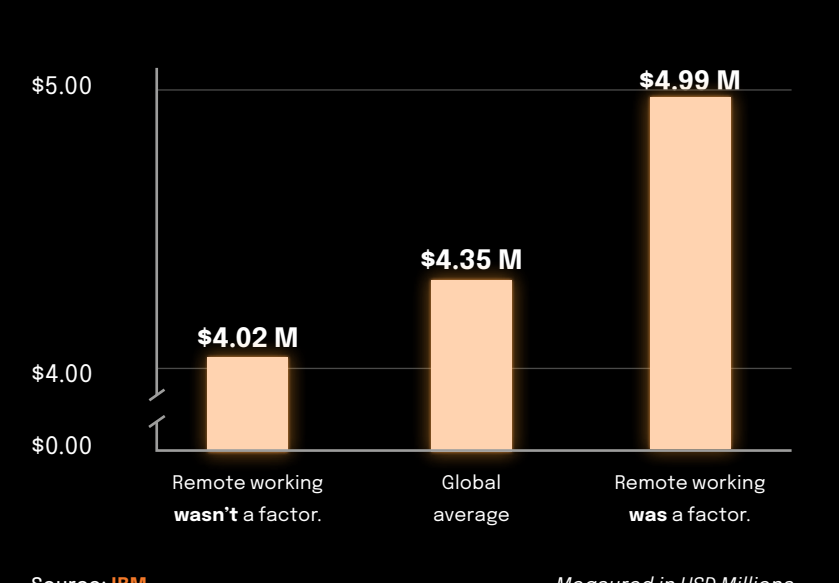
Want to know more? For instance: the FBI and NSA talk about rebooting your home router at least every week. Should we do this? Do companies still have an option to not allow remote access? What if your datacenter is (partly) in the cloud, does that count as remote work? To get answers, tune in for this Threat Talk: Does remote work?

In this Threat Talk we will discuss the following threats:

1. Citrix Netscaler ADC
2. TunnelCrack
3. Fortinet / FortiGate

What's the risk?

Average cost of a data breach where remote working was a factor in causing the breach

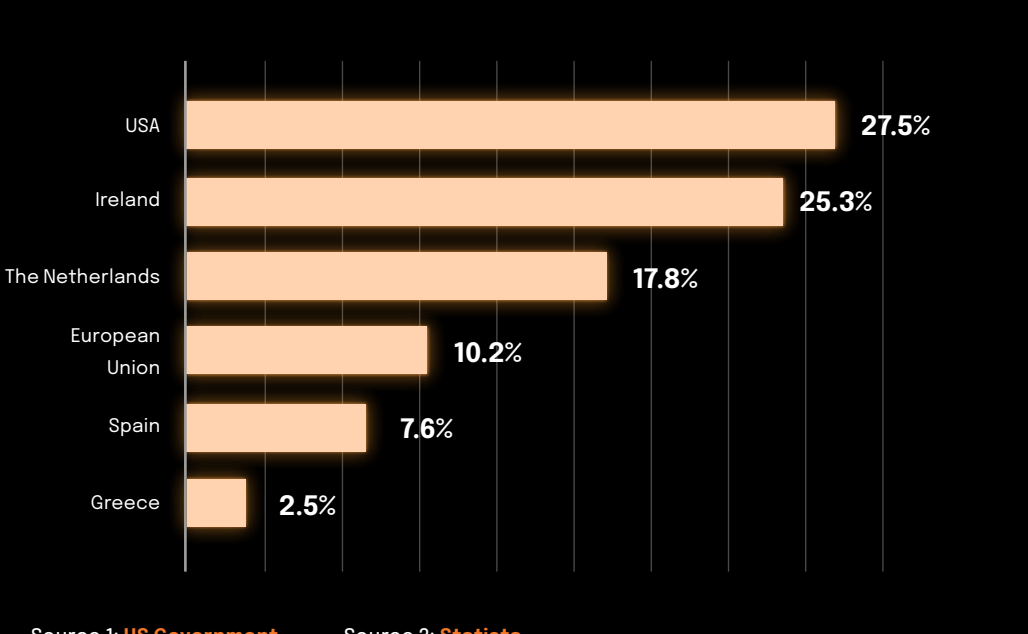


Source: IBM

Measured in USD Millions

Remote work

percentages



Source 1: US Government   Source 2: Statista

Multi-factor authentication

50%

50% of businesses allow remote workers to access their organizations' IT network without multi-factor authentication.

Source: ZipDo

Personal e-mail

48%

48% of employees working from home use personal email accounts for official communication

Source: ZipDo

Citrix NetScaler ADC and Citrix Gateway 0-Day

On July 18th 2023, Citrix released an urgent security bulletin regarding a severe vulnerability (CVE 2023-3519) identified in their NetScaler ADC and NetScaler Gateway products.

The affected appliance must be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or authentication, authorization, and auditing (AAA) virtual server for exploitation.

Evidence suggests that this vulnerability had already been exploited in the wild before its disclosure.

mSOC confidence score	Confirmed
Threat category	Vulnerability disclosure - 0-Day
Severity	Critical (CVSS score9.8)

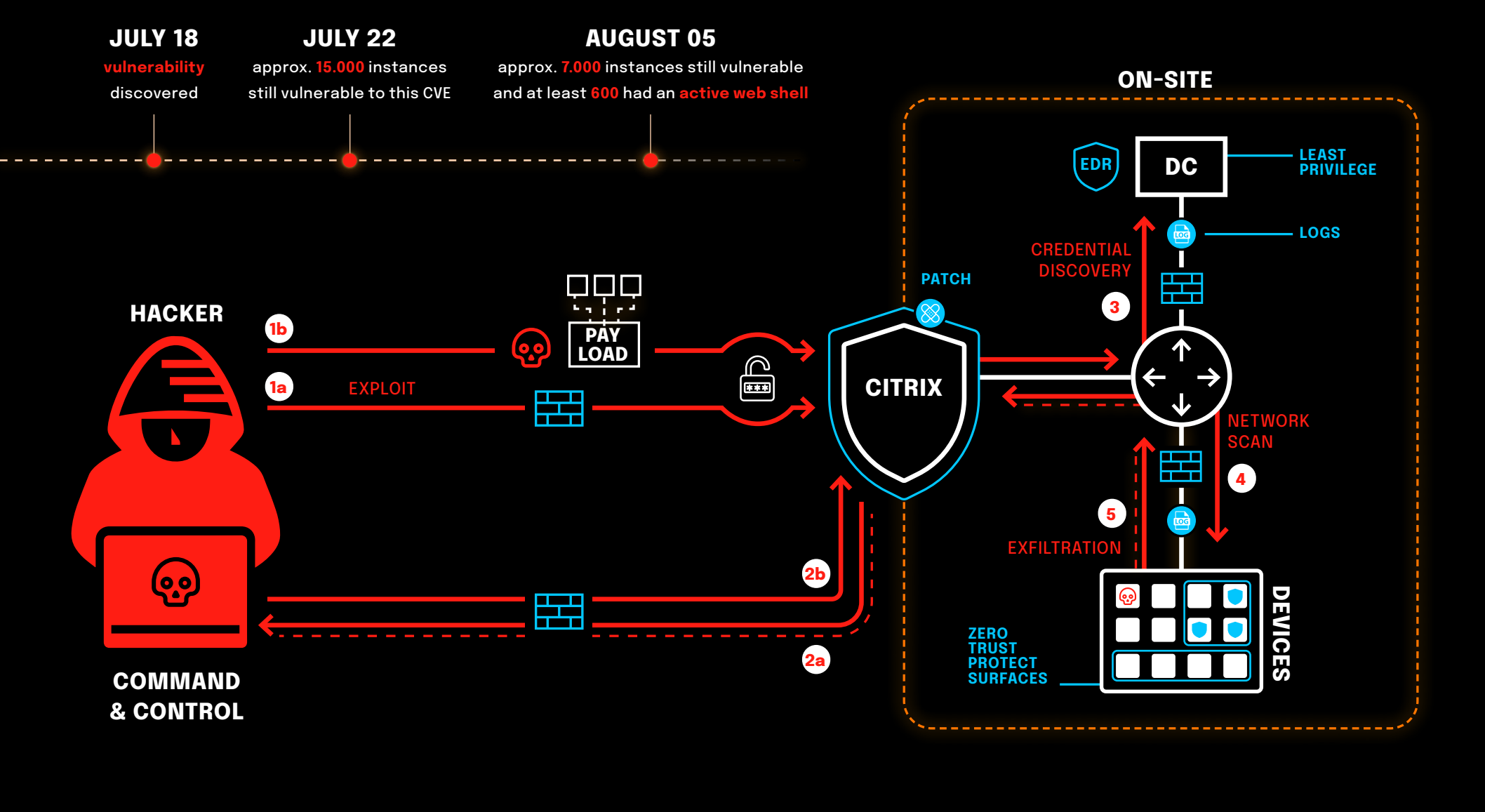
ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1190 - Exploit Public-Facing Application	Scan for public facing vulnerable appliances	Logs clearing, Traffic obfuscation	Low	Any

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1030 - Network Segmentation M1026 - Privileged Account Management M1051 - Update Software	Public facing access	Log alerts, Network monitoring	Critical	Any

JULY 18 vulnerability discovered

JULY 22 approx. 15.000 instances still vulnerable to this CVE

AUGUST 05 approx. 7.000 instances still vulnerable and at least 600 had an active web shell



Exploitation and shell upload

1a The attacker exploits the vulnerability, without any authentication.

1b The attacker uploads a malicious payload, i.e. a webshell[1].

M Traffic inspection via firewall can help detect and block suspicious traffic by matching the vulnerability signature. Quickly applying software patches will prevent initial exploitation.

Command and Control

2a The exploited Netscaler initiates a connection with the command and control server[2].

2b The attacker sends commands to the compromised Netscaler.

M Traffic inspection via a firewall can assist in detecting and blocking known command and control traffic. Where possible, restricting the server's internet access only to essential destinations can help prevent command and control communications.

Active directory enumeration

3. At this point the attacker could query the Active Directory and exfiltrate user, groups and computer information. According to the privilege level of the user, the attacker could also attempt to dump password hashes or active session tokens.

M A least privilege approach[3] may help prevent dumping password hashes. Traffic inspection through a firewall, the use of an EDR (Endpoint Detection and Response)[4] or system logs monitoring will help detect and prevent stages of attacks such as account enumeration and credentials dumping.

Network scanning and lateral movement

4. After retrieving additional credentials, the attacker may start network scans in order to determine further targets for lateral movement.

M Traffic inspection via a firewall will help detect or prevent this kind of scan and lateral movement. A Zero Trust network design will limit the number of targets for the attacker significantly.

Achieving the objective

5. At this point the attacker will act on the objective. This could vary from data exfiltration to ransomware deployment etc...

M Traffic inspection via a firewall, the use of EDR solutions and system logs monitoring may help detect and prevent the attacker from achieving the goal.

Actions performed by the ON2IT SOC:

After alerting customers about the issue, urging them to apply the patch immediately, ON2IT SOC shared the scripts with them.

The SOC team assisted in interpreting the results of the scripts and, when IOCs were detected, helped in evaluating the magnitude of the breach.

[1] Secret backdoor used to establish a communication channel between the target and the attacker
[2] Server owned by the attacker, used to send orders and receive information from and to the target
[3] Assign users or services only the bare minimum permissions they need to perform their tasks
[4] Software utilized to monitor and log hosts and user behavior. EDR are also able to detect malware and prevent malicious/suspicious actions

TunnelCrack

On August 8th 2023, a team of security researchers published a paper highlighting design flaws in various VPN clients. Their research showcased two types of attacks: LocalNet and ServerIP. The LocalNet attack involves an adversary acting as a malicious Gateway or DHCP server, tricking the victim connecting to it. This will result in possible data leakage due to the VPN's rule of sending local traffic outside its tunnel. In ServerIP attacks, the attacker spoofs the IP address of the VPN server, leading to traffic being misdirected outside the protected VPN tunnel. It's crucial to understand that for both attacks to succeed, the attacker needs either network access or the ability to deceive the victim into connecting to a rogue access point they control.

mSOC confidence score	Confirmed
Threat category	Vulnerability disclosure - CVE
Severity	Medium

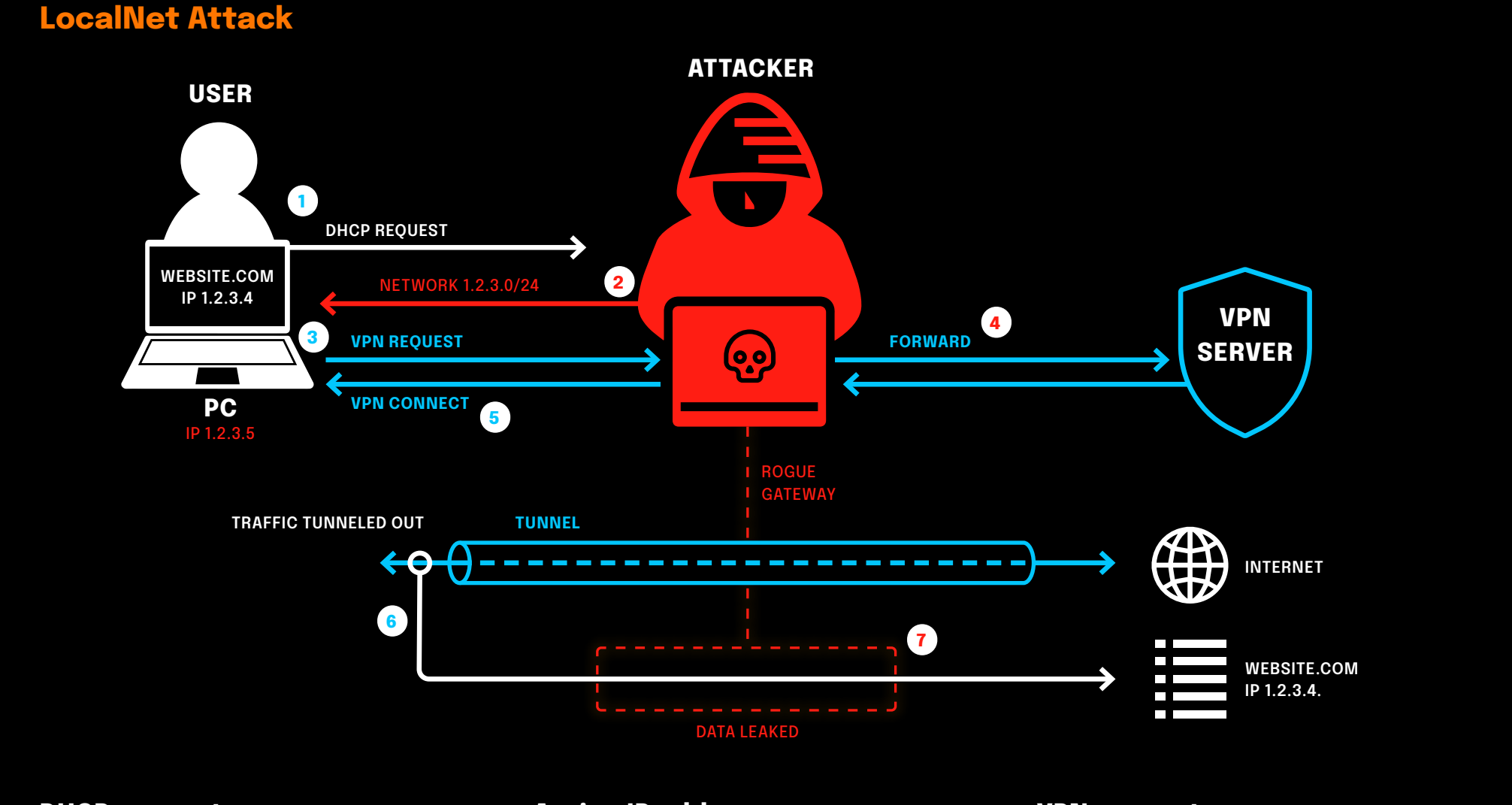
ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1557 - Adversary-in-the-Middle	Intercept VPN traffic	DNS spoofing, Traffic manipulation	Medium	Any, Enterprises, Individuals

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1041 - Encrypt Sensitive Information M1042 - Disable or Remove Feature or Program M1037 - Filter Network Traffic	Protocol weakness	Network monitoring, Anomalous VPN traffic detection	Medium/high	Any, Nation-State Actors

Scenario:

A victim intends to access a specific website, "website.com," which has the IP address 1.2.3.4. To achieve this, the victim connects to an untrusted Wi-Fi network and then initiates a connection to their VPN server.

LocalNet Attack



DHCP request

1. The victim, after connecting to the untrusted network, sends a DHCP request[1] to obtain an assigned IP address.

Assign IP address

2. The attacker intercepts the request and responds to the victim's by allocating an IP address within the same subnet as the target website's IP address. In this example IP address 1.2.3.5, which is in the subnet 1.2.3.0/24, the same subnet as the target website.

VPN request

3. The victim initiates a connection to their VPN server to establish a secure VPN tunnel.

Request forward

4. The attacker forwards the victim's request to the VPN server and then relays the server's response back to the victim.

Establishing the tunnel

5. The VPN tunnel is established, normal network traffic begins to traverse through this tunnel.

Tunneled out

6. After establishing a VPN tunnel, the victim attempts to visit 'website.com', which is located at the IP address 1.2.3.4. However, since the attacker has assigned the victim an IP address within the subnet 1.2.3.0/24 (specifically, 1.2.3.5), the VPN client is misled into believing that the target website's traffic is meant for the local network. Consequently, this traffic does not get routed through the VPN tunnel but is instead sent directly over the local network.

Eavesdrop

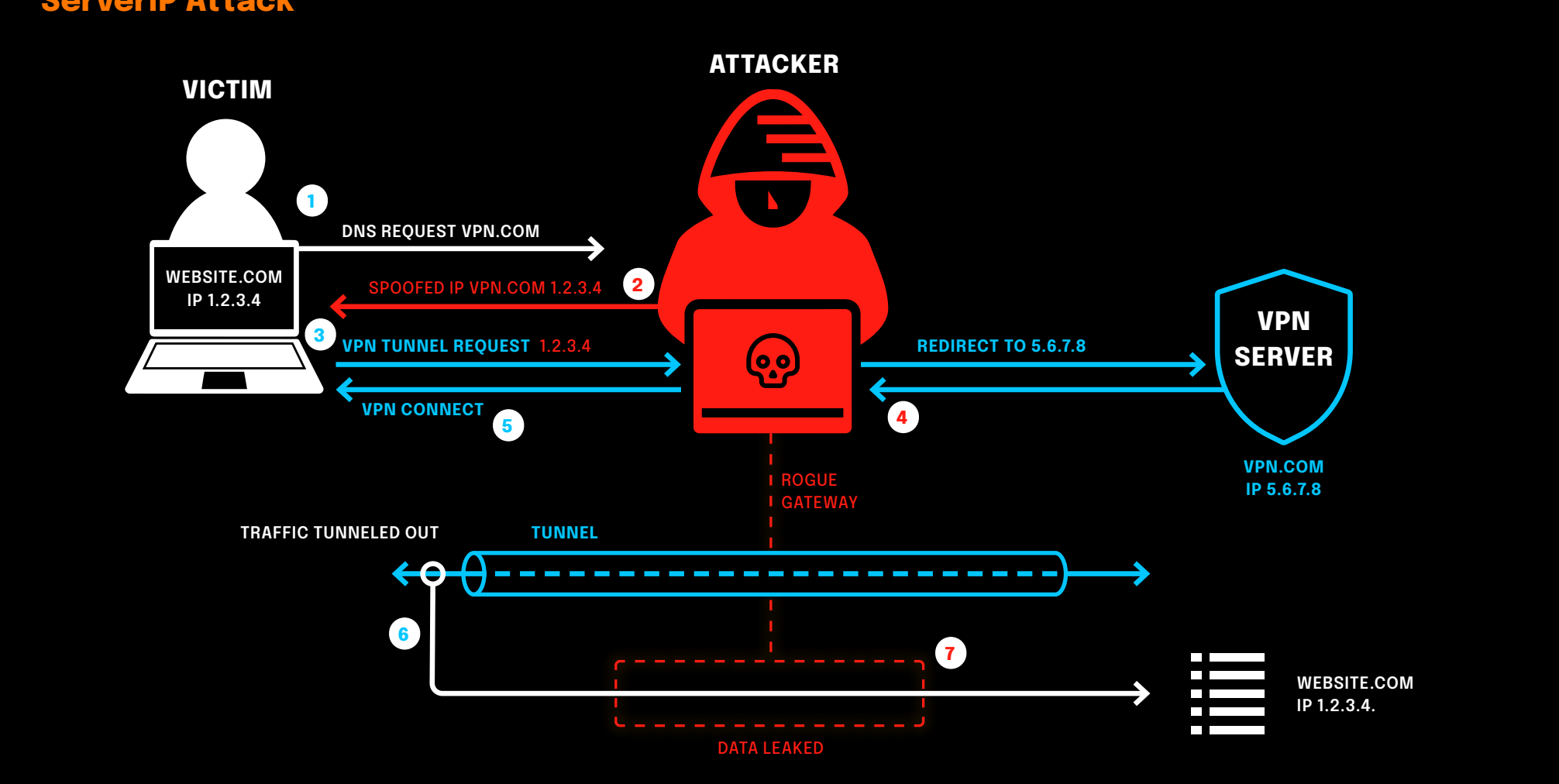
7. The attacker is now able to intercept the traffic since it is traversing outside the tunnel.

[1] DHCP (Dynamic Host Configuration Protocol), is used to request/assign a unique IP address to a device, along with other network configuration details. This process allows the device to communicate properly on the network.

Remediation

Depending on the VPN client in use, the victim may have the option to disable access to the local network while the VPN is active. This action can mitigate the attack but will also prevent access to local resources like printers or file shares. It's also important to note that the attacker may not be able to access cleartext information if protocols such as SSL are implemented. However, users should remain vigilant, especially if they encounter invalid certificates. In such case the attack can still reveal which websites a user visits and, if older insecure protocols are used, the leaked traffic might contain sensitive data.

ServerIP Attack



DNS request

1. After connecting to the untrusted network and obtaining an IP address, the victim initiates a connection to their VPN server, which is accessed through the domain 'vpn.com'. To establish this connection, the victim's sends a request to the DNS[2] server. This request is to translate the URL 'vpn.com' into the corresponding IP address, which in this case is 5.6.7.8.

IP address spoofing

2. The attacker intercepts this DNS request and, instead of providing the real IP address of the VPN server (5.6.7.8), it returns the IP address of 'website.com' (1.2.3.4).

VPN request

3. At this stage, the victim, under the impression that they are connecting to the VPN server, initiates a connection to the IP address 1.2.3.4, believing it to be the legitimate address for establishing the VPN tunnel.

Request redirection

4. Once again, the attacker intercepts the traffic from the victim. This time, however, the attacker forwards the traffic to the actual IP address of the VPN server (5.6.7.8).

Establishing the tunnel

5. The VPN tunnel is established, normal network traffic begins to traverse through this tunnel.

Tunneled out

6. After the VPN tunnel is established, the victim tries to visit 'website.com', which is located at the IP address 1.2.3.4. However, the attacker previously tricked the victim into thinking that 1.2.3.4 was the IP address of the VPN server. As a result, any traffic meant for 'website.com' is mistakenly routed outside the VPN tunnel. This happens because the VPN client is configured to exclude traffic to the IP address used for establishing the tunnel from being routed through the tunnel itself.

Eavesdrop

7. The attacker is now able to intercept the traffic since it is traversing outside the tunnel, excluding traffic to the IP address used for establishing the tunnel from being routed through the tunnel itself.

[2] DNS (Domain Name System protocol) is a protocol used to request the correct IP address corresponding to the URL that the host is attempting to visit.

Remediation

To mitigate this issue, the VPN client should be configured to route all traffic through the tunnel, with the exception of traffic originating from the VPN client itself. Similar to the previous attack, it's important to note that if protocols like SSL are in place, the attacker may not be able to access information in cleartext. However, users must remain vigilant, particularly when encountering invalid certificates. In such scenarios, the attack can still disclose the websites a user is visiting. Moreover, if outdated and less secure protocols are in use, the leaked traffic could potentially contain sensitive data.

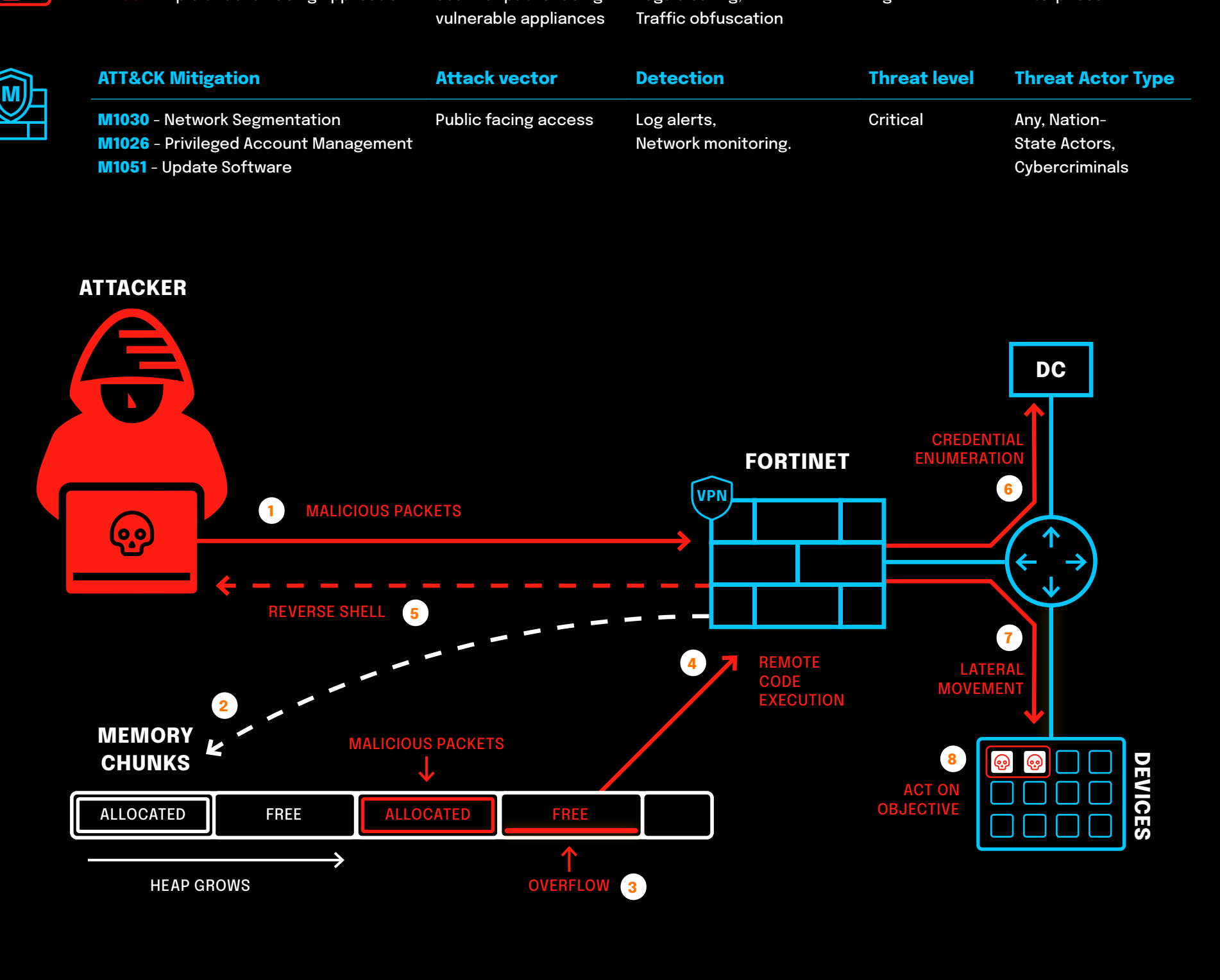
FortiOS & FortiProxy - Heap buffer overflow in sslvpn pre-authentication

Fortinet released a security bulletin addressing a heap-based buffer overflow vulnerability (CVE-2023-27997) in the SSL-VPN feature of several versions of their product. This vulnerability, if exploited, could lead to remote code execution.

mSOC confidence score	Confirmed
Threat category	Vulnerability disclosure - 0-Day
Severity	Critical (CVSS score 9.2)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1190 - Exploit Public-Facing Application	Scan for public facing vulnerable appliances	Logs clearing, Traffic obfuscation	High	Enterprises

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1030 - Network Segmentation M1026 - Privileged Account Management M1051 - Update Software	Public facing access	Log alerts, Network monitoring.	Critical	Any, Nation-State Actors, Cybercriminals



Exploitation

1. The attacker sends a specially crafted malicious request to the vulnerable appliance.

M While it can be challenging to implement, limiting access to the device is a viable strategy to mitigate such vulnerabilities.

Memory allocation

2. The firewall allocates a predetermined amount of memory space for processing the request.

Heap-Overflow

3. The attacker's request exceeds the allocated heap buffer[1] size. Due to insufficient security checks, this causes the memory to be written outside its intended boundary.

M It is crucial to promptly apply patches to affected appliances immediately following the publication of a new vulnerability or CVE in order to prevent exploitation.

Remote code execution

4. This overflow of memory can lead to various outcomes, such as system crashes or unexpected behavior. In this scenario, it enables remote code execution.

Reverse shell

5. Consequently, the attacker gains the ability to execute arbitrary code on the device, potentially implanting a reverse shell.

M Firewall rules can be effective in identifying and obstructing suspicious command and control traffic.

Enumeration & lateral movement

6-7 Using this foothold, the attacker can start extracting credentials and scan the network for additional targets.

M Adopting a least privilege approach can aid in thwarting the extraction of password hashes. Implementing traffic inspection via firewalls, utilizing Endpoint Detection and Response (EDR) systems, and monitoring system logs are crucial measures for detecting and preventing various stages of attacks. These stages include account enumeration, credentials dumping, and lateral movements within a network.

Act on objectives

8. Finally, the attacker proceeds to exploit their primary objective based on the compromised device.

[1] The heap buffer is a segment of memory allocated for temporary storing dynamic data that is utilized by a program or process.

Actions performed by the ON2IT SOC:

The SOC informed all customers about this newly identified vulnerability through a newsletter. Following the distribution of this communication, the SOC team conducted a thorough examination of the environments of all managed customers to determine which ones were impacted by this vulnerability. Upon identification, they proactively reached out to the affected customers through the customer portal to schedule a version upgrade.

Taxonomy

ATT&CK Technique
Which technique of the MITRE ATT&CK framework does the threat correspond to.

ATT&CK Mitigation
Which mitigation of the MITRE ATT&CK framework can be applied.

Attack Strategy
Plan devised by the attacker to exploit specific system vulnerabilities.

Attack Vector
What is the primary method of attack.

Evasion
Tactics used by the attacker to avoid detection or bypass security.

Detection
Mechanism to identify malicious activities or system anomalies.

Complexity
How easy it is to exploit the vulnerability or carry out the attack.

Threat Level
How severe the threat is.

Target Type
The category of organization that may potentially be targeted.

Threat Actor Type
What type of threat actor may be involved.

CONTACT US

mSOC score explanation:
We assign scores to both our sources and the news items. Sources are scored on a numeric scale ranging from 0 (untrustworthy) to 5 (verified), while news items are scored with a letter, ranging from E (unreliable) to A (reliable). By considering the scores of both the source and the news item and the quality of the available information, we classify the overall reliability into three categories: Confirmed, Verified, and Credible. Interested in learning more about our reliability scoring system for sources and news items? Our Threat Intelligence team would be happy to walk you through our procedure, so please don't hesitate to reach out.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS   amsix