ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks
The Evolution of Cyber Warfare

Advanced Threat Intelligence helps you know your enemy

In this episode of Threat Talks we will discuss the following threats:

- China Nexus Barracuda Hack
- Russia GRU Viasat Hack
- APT Sand Eagle – Operation Triangulation

In recent months, IT departments worldwide have been in the eye of the storm.

As countries prepare for significant elections, a wave of cyberattacks has swept across the political landscape. Lawmakers find their private communications exposed by phone hacks, while data breaches on an unprecedented scale threaten the personal information of thousands.

This surge in cyber assaults underscores a broader narrative: we are entrenched in a digital battleground.

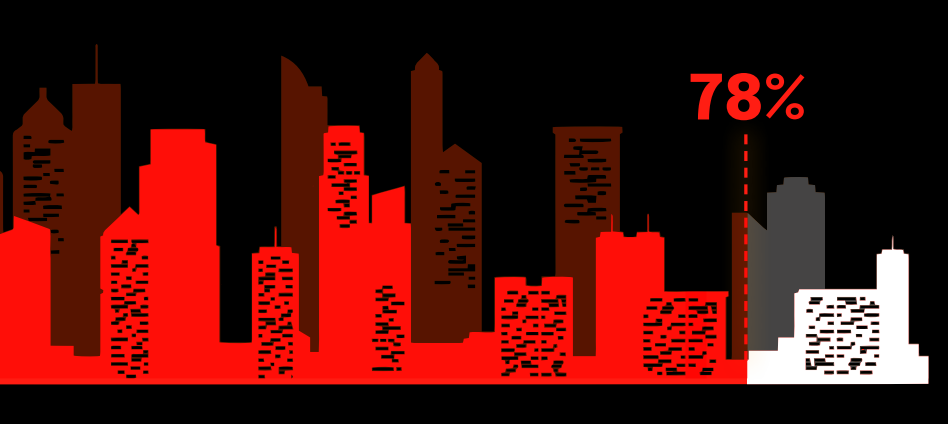
Today, possessing advanced threat intelligence isn't just beneficial; it's imperative for detecting, understanding, and countering the sophisticated threats that loom over us. In this volatile cyberspace, the call for robust norms and legislation has never been more pressing, aiming to fortify our digital defenses and secure a safer tomorrow.

In this **'Evolution of Cyber Warfare'** episode of Threat Talks, we explore whether or not we stand a chance in this continuous arms race in cyber technologies, what Advanced Persistent Threats (APTs) are, and how these modern threats can affect literally everyone.

The proportion of cyber-attacks perpetrated by nation states targeting critical infrastructure jumped from

20% to 40%

Source: 2022 Microsoft Digital Defense Report



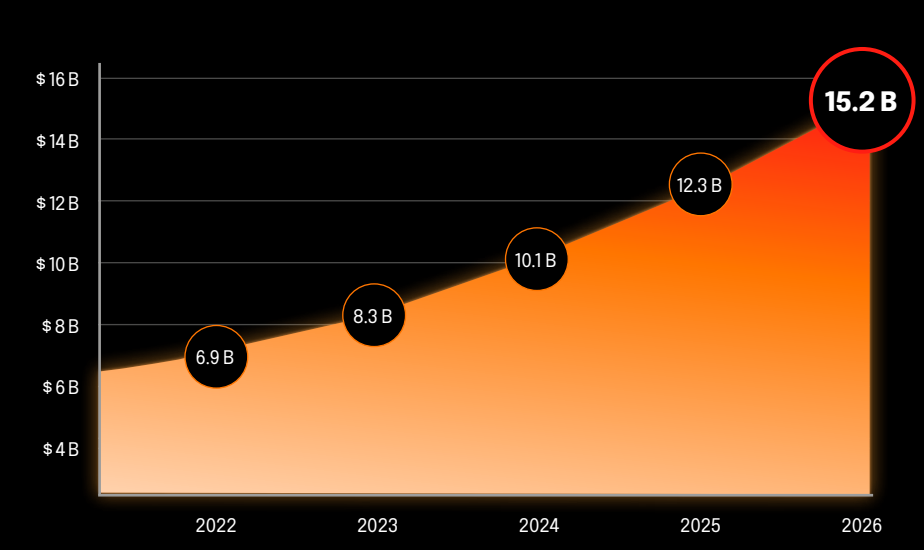
Approximately

78% of businesses

have faced downtime due to Advanced Persistent Threat (APT) attacks, often evading conventional security measures.

Source: Allied MR

The worldwide revenue for APT Protection solutions is expected to grow from $6.9 billion in 2022, to nearly $15.2 billion by 2026



Source: The Radicati Group, INC. 2022

MITRE currently recognizes 152 APT 'groups'

Source: MITRE

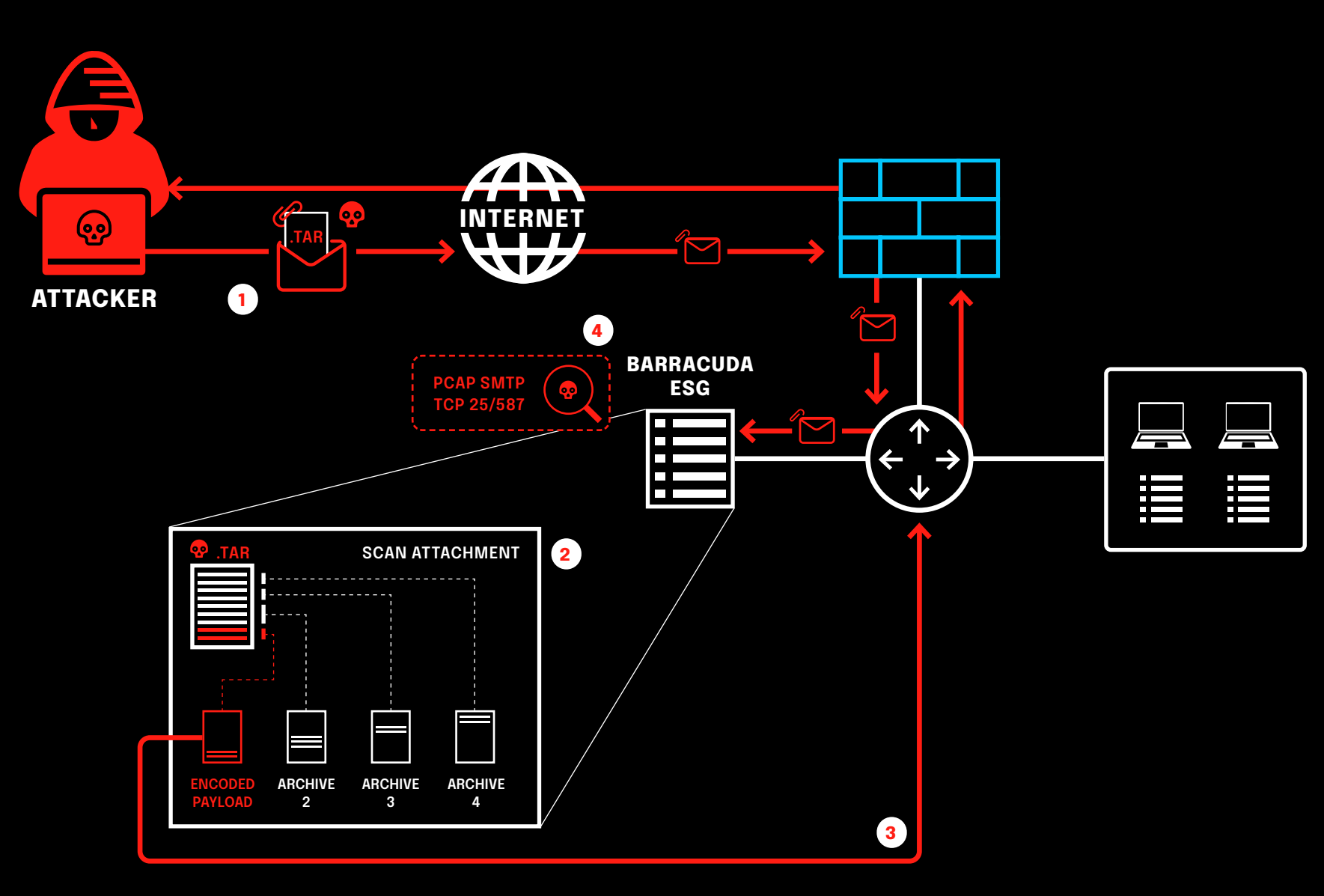
Barracuda ESG Zero-Day Vulnerability
CVE-2023-2868

In October 2022, the Chinese cyber threat group UNC4841 began exploiting a zero-day vulnerability (CVE-2023-2868) in Barracuda's Email Security Gateway (ESG). This vulnerability allowed the attackers to execute arbitrary commands, leading to the deployment of various malware families. Despite remediation efforts by Barracuda, the attackers adapted and maintained persistence on compromised systems, targeting a wide range of sectors globally.

mSOC confidence score	Confirmed
Threat category	Cyber Attacks - APT Attacks
Severity	Critical (CVSS score 9.8)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1203 - Exploitation for Client Execution	Exploiting zero-day vulnerability	Living Off the Land, Code Obfuscation	High	Government, Military, Enterprises

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1048 - Application Isolation and Sandboxing M1050 - Exploit Protection	Email Attachments with Malicious TAR files	Network Traffic Analysis, Application logs	Critical	Nation-State Actors (UNC4841)



Malicious Attachment

1. The attacker sent a maliciously crafted email with a .tar attachment. The emails are poorly crafted with generic subjects, grammar mistakes, and placeholder values in order to have Barracuda appliances flag them as SPAM.

CVE Exploit

2. The malicious attachment contains several archived files. Only the first file has a payload embedded in its name. The attacker exploits CVE-2023-2868, where a command injection vulnerability exists in the parsing logic for processing TAR files. Perl's qx{} function stores the names of the files within a TAR archive in the $f variable. This variable is inserted directly into a system command, and due to a lack of input validation, it allows command injection using escape characters.

M Modern firewalls can perform content inspection and, once the mechanism is known, block this kind of content. A more drastic approach would be to simply block file attachments.

C2 Communication

3. The payload embedded in the filename is encoded in base64 and, once decoded, it establishes a connection back to the attacker's C2 server by using OpenSSL to create a client and connect to the malicious server.

M Only allow very specific outgoing connections. Also, have known IOCs loaded into the firewall to block and alert on this traffic, indicating that something requires attention.

Additional Backdoors

4. At this point the attacker can retrieve additional backdoors such as SEASPY, SALTWATER and SEASIDE to gain persistence and establish a PCAP[1] filter on port TCP 25 and TCP 587[2]. The attacker is now able to upload, download files and execute commands on the device.

M Scan the traffic for malicious payloads and only allow very specific outgoing connections, i.e., specify destination, URL, service, and application.

[1] PCAP (Packet Capture) refers to the process of capturing network traffic. A PCAP file contains detailed information about each network packet. This data can be used to analyze network behavior, diagnose issues, and, in some cases, retrieve files and read information transmitted in clear text.

[2] TCP port 25 is primarily used for the Simple Mail Transfer Protocol (SMTP) to send emails between mail servers. TCP port 587 is used for submitting emails to a mail server with SMTP.

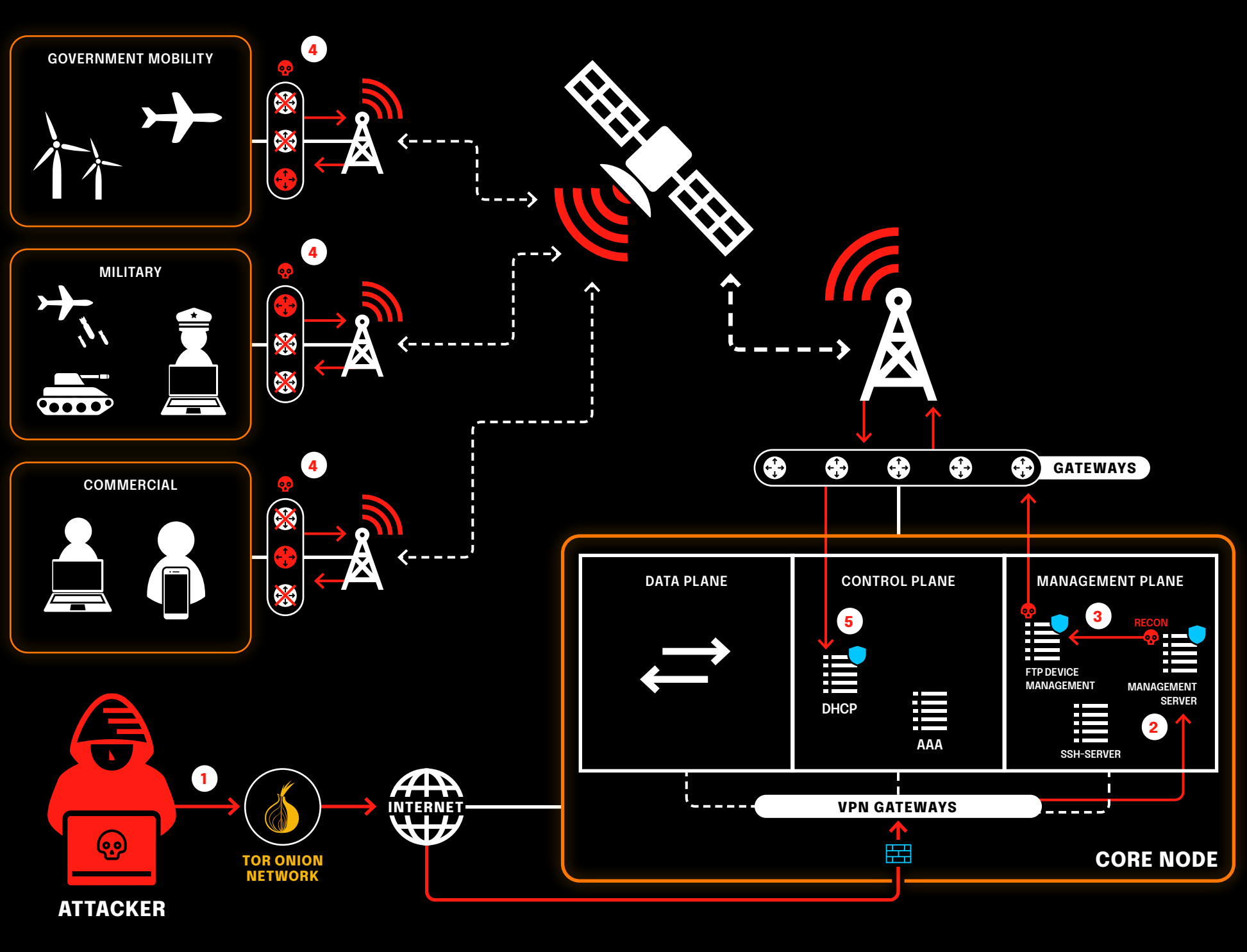
Viasat Cyber Warfare Viasat Hack (Russian GRU)

On February 24, 2022, just hours before Russia's invasion of Ukraine, a significant cyberattack targeted Viasat's KA-SAT satellite network. This attack, attributed to the Russian GRU, involved the deployment of the "AcidRain" wiper malware, which rendered thousands of Viasat modems and routers inoperable by erasing their data and rebooting them. The attack had widespread implications, disrupting both military and civilian communications.

mSOC confidence score	Confirmed
Threat category	Cyber Attacks - APT Attacks
Severity	Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1561.002 - Disk Wipe T1499.002 - Endpoint Denial of Service: Service Exhaustion Flood	Wipe devices to create downtime	Living Off the Land, Use of legitimate credentials	High	Military, Civilian, Infrastructure

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1037 - Filter Network Traffic M1053 - Data Backup	Network traffic, Sensor Health	Network Traffic Analysis, Anomaly Detection	Critical	Nation-State Actor



Initial Acces

1. The attacker gained initial access to the Viasat network using compromised credentials via a VPN gateway. The malicious sessions were established using the Tor network[1].

M Implementing additional authentication methods (MFA) can help prevent abuse of leaked/stolen credentials. Implementing restrictive firewall policy rules and adopting dynamic blocklist rules can help prevent such attacks by blocking malicious or suspicious IPs, such as Tor exit nodes.

Lateral Movement

2. Once in the network, the attacker accessed the management server and performed reconnaissance to find further targets to compromise.

M Network segmentation (Zero Trust) and EDR solutions may help detect or prevent suspicious activities, such as reconnaissance events.

Staging

3. The attacker gained access to the FTP server used to push firmware updates to the gateways in the network. The attacker used this server to stage the malware and push it to the gateways.

M EDR solutions may help detect or prevent suspicious activities, such as staging or suspicious file downloads. Restricting network connections and making policies very specific will make it more difficult for an attacker to push the firmware.

AcidRain

4. The attacker installed the wiper "AcidRain"[2] on many routers in the network. The malware performs an in-depth wipe of the filesystem and various known storage device files. If the code runs as root, AcidRain performs a recursive overwrite and delete of non-standard files in the filesystem. The wiper iterates over all possible device file identifiers, opens them, and overwrites them. Once the wiping processes are complete, the device is rebooted, rendering it inoperable.

DDoS

5. Simultaneously, the attacker initiated a volumetric DDoS attack by sending multiple DHCP requests using legitimate modems with a valid subscription, causing network instability. The combined impact of the DDoS attack and the wiper malware resulted in significant disruptions, including:
   - Military and civilian network disruptions
   - Control and management of 5,800 Enercon wind turbines in Germany were down
   - Disruptions to commercial airlines
   - Approximately 40,000 modems were unable to connect

M There are multiple ways to limit the impact of a DDoS attack. See previous episodes around this topic.

[1] The Tor network is an anonymity network that routes internet traffic through multiple encrypted relays to conceal users' locations and usage, enhancing privacy and security.

[2] Type of malware designed to erase or overwrite the data on a target system's storage devices, rendering the system inoperable and causing significant data loss.

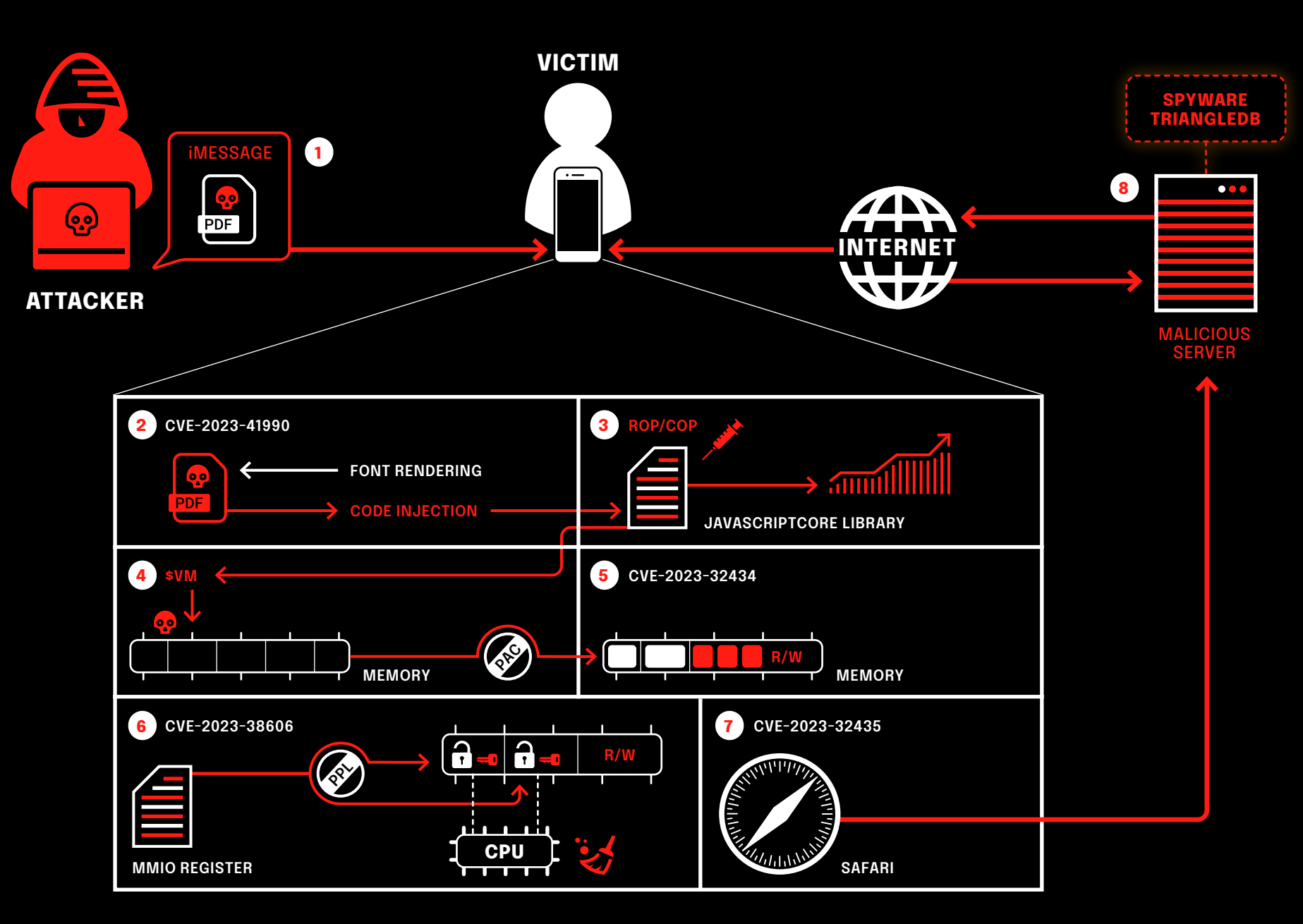
Operation Traingulation APT Sand Eagle

On March 11, 2024, Russian cybersecurity firms designated the US government as APT "Sand Eagle," alleging that American agencies had launched cyberattacks on Russian devices. The FSB reported that on June 1, 2023, thousands of iPhones, including those of Russian diplomatic missions, were infected with malware through a kernel vulnerability, leading to the campaign being dubbed "Operation Triangulation."

mSOC confidence score	Credible
Threat category	Cyber Attacks - APT Attacks
Severity	Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1055 - Process Injection T1071.001 - Application Layer Protocol: Web Protocols T1140 - Deobfuscate/Decode Files or Information	Exploit kernel vulnerability to gain admin privileges and install malware	Fileless Malware	Extreme	Government

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1058 - Antivirus/Antimalware M1010 - Deploy Compromised Device Detection Method M1001 - Security Updates	Zero-Day Exploits	Behavioral Analysis, Network Monitoring	Critical	Nation-State Actors



Malicious Attachment

1. The attacker sends a specially crafted iMessage containing a malicious PDF attachment.

1st 0-Day

2. The message is processed by the iMessage application without any user interaction. The attachment exploits CVE-2023-41990, a vulnerability in the ADJUST TrueType font instruction, a legacy feature present on Apple devices that allows manipulation of font rendering. The exploit leverages this vulnerability, allowing the attacker to execute arbitrary code on the device.

3. ROP/COP Techniques

3. ROP/COP techniques[1] are used to chain together short sequences of existing legitimate system functions in a sequence controlled by the attacker and modify the JavaScriptCore[2] library environment to enable JavaScript code execution with elevated privileges. The exploit code is heavily obfuscated to make it difficult to read and analyze.

$VM Exploit

4. At this point, the malware exploits $vm[3] debugging functionality, which allows scripts to directly manipulate memory within the JavaScriptCore environment, effectively allowing the attacker to bypass PAC[4] functionalities by manipulating hardware registers and memory in a way that neutralizes PAC protections, enabling the exploit to gain full control over the device.

2nd 0-Day

5. The malware exploits another 0-Day vulnerability, CVE-2023-32434, which leverages an integer overflow vulnerability in the XNU kernel's memory mapping syscalls (mach_make_memor_entry [5] and vm_map[6]). By exploiting the integeroverflow, the attacker can manipulate the arguments passed to these syscalls, allowing them to create memory entries that exceed normal boundaries, effectively gaining read and write access to physical memory that should be restricted.

3rd 0-Day

6. After gaining initial access and memory manipulation capabilities, the malware leverages an extra 0-day vulnerability, CVE-2023-38606. The exploit leverages MMIO[7] (Memory-Mapped I/O) registers to manipulate the memory mappings controlled by PPL[8] (Page Protection Layer). This allows the attacker to read from and write to protected memory regions, effectively neutralizing PPL's security measures, giving the attacker full control over the device's memory and processes. At this point, the malware hijacks the IMAgent[9] process, a legitimate system process, and injects a malicious payload into it designed to erase traces of the attack.

4th 0-Day

7. The malware exploits a fourth zero-day vulnerability, CVE-2023-32435, by running Safari in the background and redirecting it to a malicious web page. CVE-2023-32435 allows remote code execution through shell code by exploiting a flaw in Safari's handling of certain web content. The web page contains scripts to verify the target device, checking for specific characteristics and previous exploit markers to ensure it's the intended target.

TriangleDB

8. Once the device is verified, the shell code executes arbitrary commands leading to the download of the TriangleDB spyware. TriangleDB operates entirely in RAM, making it difficult to detect. It collects sensitive information, including personal data and credentials. It communicates with a command-and-control server to exfiltrate data and receive further instructions. If the victim reboots their device, the attackers have to reinfect it by sending an iMessage with a malicious attachment, thus launching the whole exploitation chain again. If no reboot occurs, the implant uninstalls itself after 30 days unless this period is extended by the attackers.

Defense

Sand Eagle is an extremely sophisticated attack, leveraging multiple zero-day vulnerabilities. These vulnerabilities were previously unknown, making them extremely difficult to defend against. Mobile Endpoint Detection and Response (EDR) solutions are not very common but are maturing and gradually becoming more widespread. Such EDR solutions might detect system abuse, primarily by identifying abnormal behavior. As with most attacks, there is a command and control channel used to manage the malware or extract the collected data. By controlling the device's communication through Secure Access Service Edge (SASE) or always-on VPN, you can enforce very strict policies, making it challenging to establish these control channels and/or exfiltrate data. Additionally, ensure your iOS devices are up-to-date and, if possible, use "lockdown mode".

[1] Return-Oriented Programming (ROP) and Call-Oriented Programming (COP) are exploit techniques that use sequences of existing code (gadgets) in a program's memory to execute arbitrary commands, bypassing security mechanisms without injecting new code.

[2] JavaScript engine used by the WebKit browser engine. It compiles and executes JavaScript code in web pages, providing a runtime environment for JavaScript execution.

[3] Hidden debugging feature in JavaScriptCore that allows scripts to directly manipulate memory and execute native API functions.

[4] PAC is a security feature in newer iPhone models that protects against memory corruption by verifying the integrity of pointers.

[5] Used to create a memory entry object, which represents a mapping of memory in the system.

[6] Used to establish a mapping from virtual to physical memory.

[7] Registers used by hardware to map device memory directly into the address space of the processor.

[8] Security feature designed to protect critical system memory regions from unauthorized access and modifications.

[9] IMAgent is a background process on Apple devices associated with handling iMessage and FaceTime services. It is responsible for managing message delivery and communication functions.

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