ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks
Advanced Persistent Threats

threat-talks.com

The silent threats behind major breaches

What if a cyberattack could stay hidden in your systems for months without a trace? What if it wasn't just about stealing data, but gaining long-term access and control? These are the questions that define Advanced Persistent Threats, or APTs.

APTs are not your average cyber threats. They're highly targeted, stealthy, and often backed by nation-states. Instead of quick attacks, APTs are designed for long-term infiltration. Threat actors behind these campaigns use a mix of social engineering, zero-day exploits, and built-in system tools to breach defenses and quietly maintain access.

These groups typically aim at high-value targets–government bodies, energy infrastructure, defense contractors, and major enterprises–seeking sensitive data or positioning themselves for future disruptions. APTs are also a key tool in cyber-espionage and geopolitical conflict.

In this Threat Talks infographic we will discuss the following threats:

- Seashell Blizzard
- Volt Typhoon
- APT Handala

71% of APT attacks target **the public sector and critical infrastructure**
Source: IBM X-Force Threat Intelligence Index 2024

211 the average dwell time for an APT attack is **211 days**
Source: Mandiant M-Trends 2023 Report

43% of APTs use **stolen credentials** as their initial access vector
Source: Verizon Data Breach Investigations Report 2023

150 at least **150 distinct APT groups** are being tracked globally by threat intelligence analysts
Source: MITRE ATT&CK

Seashell Blizzard

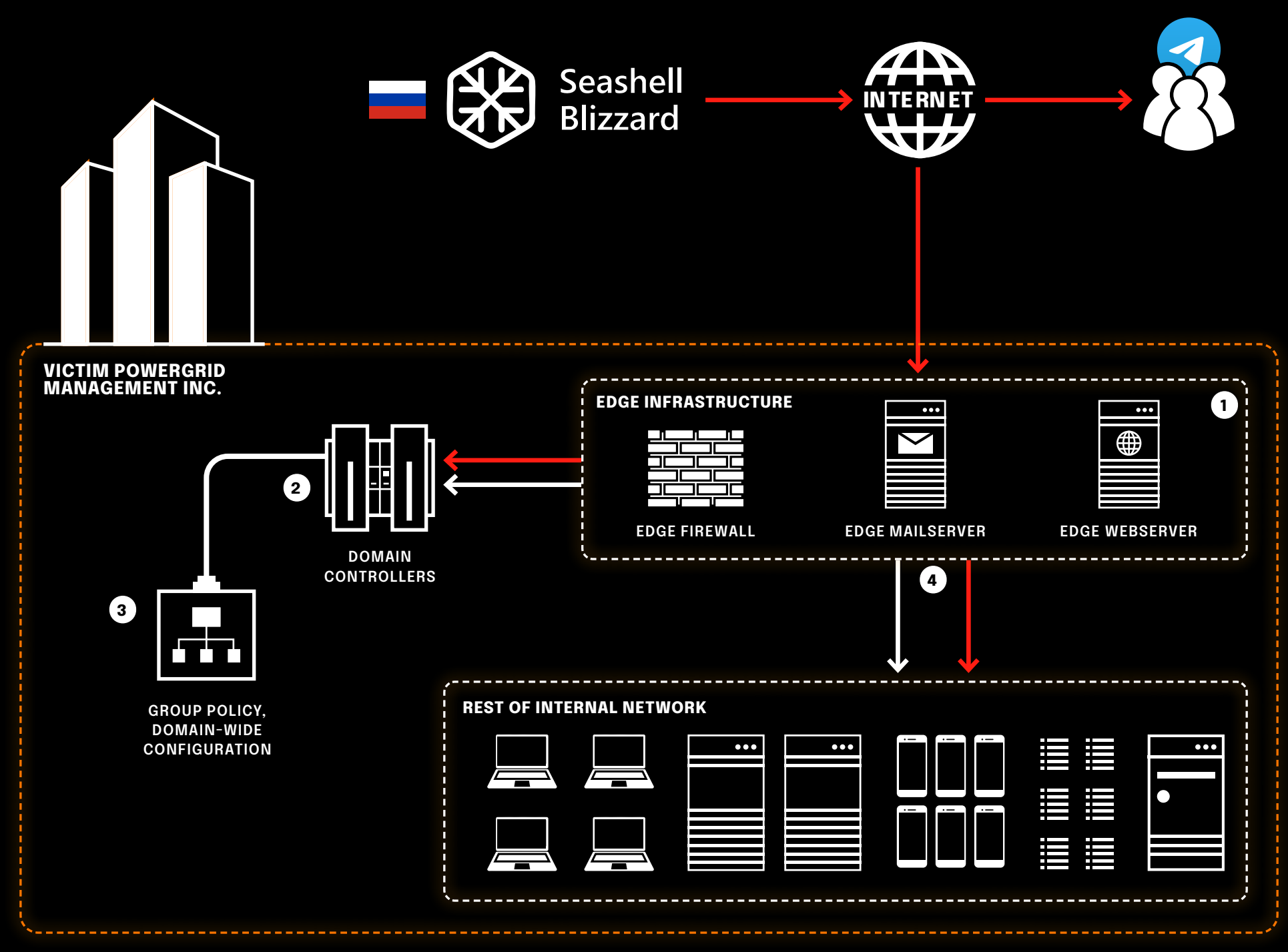
Russian espionage goes cloud-native

Seashell Blizzard is a Russian state-sponsored APT group linked to the country's Foreign Intelligence Service (SVR). Active since at least 2008, it's best known for stealthy espionage campaigns. This group was behind the infamous SolarWinds attack in 2020, which compromised multiple U.S. federal agencies and major companies. Seashell Blizzard is highly sophisticated, known for using custom malware and living-off-the-land techniques to stay under the radar for extended periods.

mSOC condidence score	Confirmed
Threat category	APTs Profiling
Severity	Nation-State

Attack Strategy	Evasion	Complexity	Target Type
Exploiting hard to detect edge infrastructure, staying stealthy throughout entire engagement until ready to act on objectives	Living off the land for lateral movement and priviledge escalation	High	Government, Critical Infrastructure, Electrical Grid Infrastructure

Attack vector	Detection	Threat level	Threat Actor Type
Exploitation of edge device vulnerabilities, followed by stealthy lateral movement	Behavioral analytics, network traffic monitoring, EDR, threat hunting, anomaly detection in OT/IT segmentation	Critical	Nation-State Actors



Initial Access and Foothold

1. Russian Seashell targets vulnerable edge devices (e.g., web/mail servers) to stay stealthy. They gain access using known or zero-day exploits, then drop basic webshells for persistence and use built-in tools (Living off the Land) to avoid detection.

M. Strong patch management helps, but zero-days that specifically work around this make EDR on edge infrastructure critical to catch both deployed backdoors and improper usage of regular system binaries for malicious purposes.

Lateral Movement & Priviledge Escalation

2. Once inside, they move laterally using only found binaries and tools to avoid further detection while in the network. The aim is to compromise Active Directory and gain Domain Admin access.

M. EDR with behavioral analysis is key here. Applying the principle of least priviledge to all accounts (user and service) is the best way to mitigate privilegde. Make sure all accounts aren't unnecessarily vulnerable to attacks like kerbroasting.

Deployment Strategy for Malware

3. The attackers often use the gained highly privileged accounts to prepare the deployment of their malware through group policy. Group policy configuration within Active Directory allows one to deploy software packages and configurational changes to all domain-joined endpoints. A modified PowerShell script (TANKTRAP) helps automate creation and spread of malicious GPOs (Group Policy Objects), which will deploy their disruptive/destructive payloads on domain-joined endpoints.

M. The monitoring of audit logs in Active Directory is absolutely imperative to detect the implementation of inappropriate GPOs. It's also important to lock down the permissions of user accounts capabale of making domain-wide GPOs.

Acting on Objectives

4. Malware is deployed en masse via GPOs, with the main intention of causing as much destruction of infrastructure and disruption of services. Seashell Blizzard is known for using "pure" distruptive tools that aren't designed for recovery, nor do they implement any modular or multi-stage designs. The primary (and usually only) design of their payloads is a simple, pre-packaged executable, exclusively with the purpose of wiping the target machine.

M. EDR is first line of defense. If that fails, clean, off-site backups are critical for recovery.

Telegraphic Success

5. Unlike typical APTs, Seashell announces attacks loudly, even mid-operation, to amplify fear and push political narratives.

M. These public declarations can act as last-resort detection cues while the attack is still in progress.

Volt Typhoon

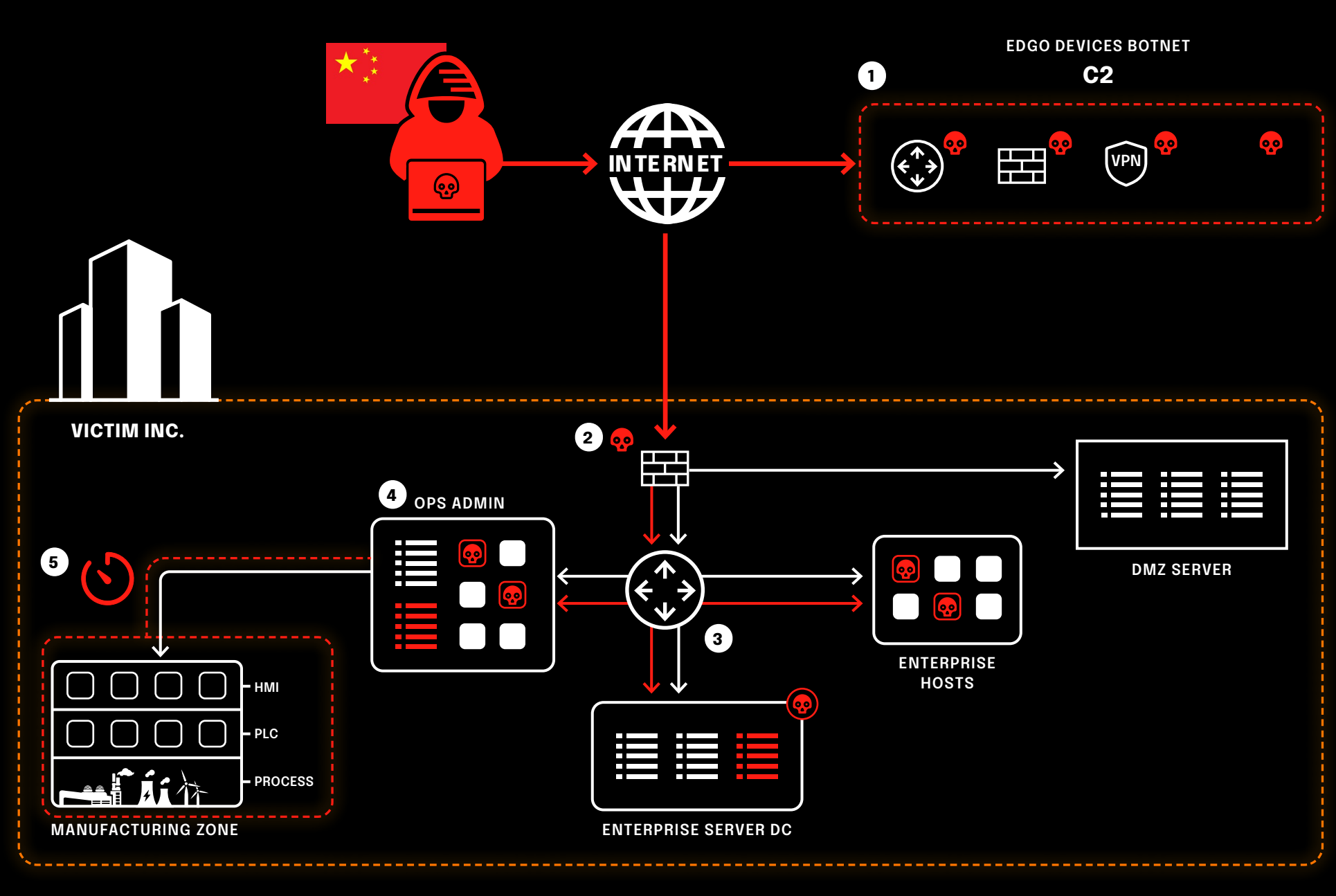
China's silent siege on US infrastructure

Volt Typhoon is a China-based APT group targeting critical infrastructure sectors in the U.S., including communications, transportation, and energy. What makes this group notable is its focus on stealth and persistence. It uses living-off-the-land techniques, which rely on built-in system tools to avoid detection, rather than deploying malware. Discovered in 2023, Volt Typhoon's intent seems to center on espionage and pre-positioning for possible disruptive actions.

mSOC condidence score	Confirmed
Threat category	APTs Profiling
Severity	Nation-State

Attack Strategy	Evasion	Complexity	Target Type
Exploiting zero-day vulnerabilities in edge devices and remaining stealthy in critical infrastructure	Living off the land, use of native tools, KV botnet proxy relays	High	Government, Critical Infrastructure, Military, Enterprises

Attack vector	Detection	Threat level	Threat Actor Type
Exploitation of edge device vulnerabilities / leaked credentials, followed by stealthy lateral movement	Behavioral analytics, network traffic monitoring, EDR, threat hunting, anomaly detection in OT/IT segmentation	Critical	Nation-State Actors



C2 Infrastructure

1. Volt Typhoon avoids traditional C2 servers. Instead, they use the KV botnet, which is made up of hijacked SOHO routers, VPN appliances, and other edge devices. These act as proxies, creating a layered relay network.

M. Monitoring outbound traffic for unusual patterns can help spot this kind of activity. Threat intelligence and anomaly detection are key. Keeping firmware up to date on edge devices helps prevent them from being hijacked in the first place.

Initial Access

2. They usually get in by exploiting vulnerabilities in edge devices from vendors like Fortinet, Ivanti, Citrix, and Cisco. They use both known exploits and, when available, zero-day vulnerabilities or stolen VPN credentials.

M. Patch management and strong visibility over external facing systems is key. Apply vendor updates quickly, use intrusion prevention systems and next-gen firewalls, enforce multi-factor authentication for remote access, and monitor VPN usage for any signs of abuse.

Foothold

3. Once inside a network, Volt Typhoon typically employs malware-less attacks, relying on living-off-the-land (LOTL) techniques and hands-on-keyboard activity. They use legitimate system tools to maintain persistence and evade detection.

M. Behavior-based detection through EDR can help. Restrict or disable tools like PowerShell and WMI if not needed. Following least privilege principles and segmenting the network will limit the attacker's reach.

Lateral Movement

4. After establishing access, the group focuses on positioning themselves for lateral movement towards critical infrastructure systems and, when feasible, operational technology (OT) networks.

Act on Objective

5. Volt Typhoon's end goal is to stay hidden inside critical infrastructure for long periods, enabling them to disrupt or sabotage systems when it suits their broader strategy.

M. Detecting and disrupting long-term persistence requires proactive threat hunting and regular system audits. Blue teams should look for subtle persistence techniques, such as misused legitimate services or scheduled tasks. Run regular incident response drills, and keep up with evolving threat intelligence to know what tactics to watch for.

APT Handala

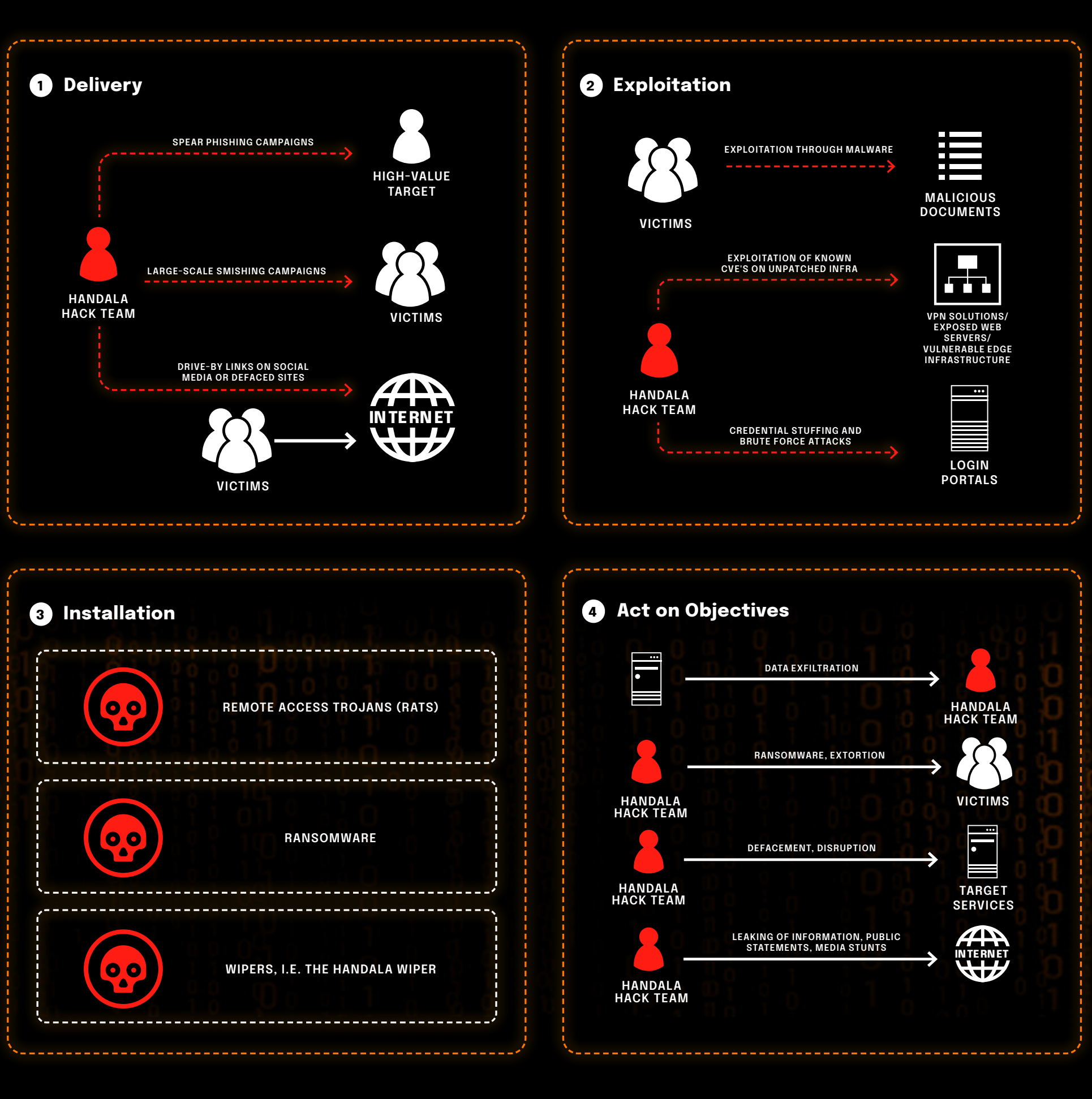
Anti-Israeli hacktivists

APT Handala, also known as the 'Handala Hack Team', is a politically motivated hacktivist group with a strong pro-Palestinian and anti-Israeli narrative. They are known for disruptive cyber operations including wiper malware attacks, data leaks, and website defacements.

mSOC condidence score	Confirmed
Threat category	APTs Profiling
Severity	Nation-State

Attack Strategy	Evasion	Complexity	Target Type
Mostly relatively simplistic attacks like high volume phishing, SMS spam and spearphishing of high-value personnel in target organizations. They've also been observed exploiting known vulnerabilities	Custom phishing message content, often written in Hebrew/Arabic. Or malicious macros embedded in documents.	Medium	Israeli-backed (government) organizations

Attack vector	Detection	Threat level	Threat Actor Type
Publicly known personnel from target organizations, determined via various OSINT techniques.	Employee phishing awareness training. URL Filtering and endpoint protection.	Low	Politically Motivated Hacktivists



Delivery

1. Handala Hack Team targets personnel with spear phishing, smishing, or drive-by links on social media/defaced sites. Their phishing often uses macro-infected documents to install backdoors or ensure persistence.

M. User awareness campaigns, anti-spam, and mail security solutions are key defenses. Disabling scripting and macros on endpoints further reduces risk. Awareness training is especially effective against phishing.

Exploitation

2. The team exploits targets through phishing-delivered malware, unpatched CVEs, or credential stuffing/brute forcing. Malware is mainly used to access personal files for potential exfiltration, while the latter two methods typically target web servers for defacement.

M. Patch management, especially for edge infrastructure, is critical. Handala Hack Team hasn't used zero-days but exploits known vulnerabilities for access. Mail security and anti-spam solutions help block phishing-delivered malware.

Installation

3. Handala Hack Team typically deploys common trojans/RATs, sometimes slightly customized. They also use ransomware or wipers, including their own "Handala Wiper." RATs help them assess access to sensitive data for possible exfiltration.

M. EDR solutions on all endpoints are crucial to defend against ransomware, wipers, and data exfiltration. Network segmentation with Zero Trust strategies further protects the network if edge servers are compromised.

Acting on Objectives

4. Handala aims to harm targets' services or reputation, commonly through data exfiltration, ransomware, web defacement, public leaks, or endpoint wiping for disruption.

M. EDR/XDR on servers and endpoints defends against ransomware, wipers, and data exfiltration. Strict network policies, limiting outbound access from sensitive sources, further protect against data leaks.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS

amsix

CONTACT US