ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks

APTs in war time

When the SOC becomes a combatant

threat-talks.com

In this Threat Talks infographic we discuss:

- Operation Olalampo

Why every defender of critical infrastructure is now on the front line.

Your SOC is now a combatant. You didn't sign up for that, but neither did the engineers at Ukraine's power utilities, the telecom operators in Viasat's footprint, or the sysadmins watching wipers detonate hours before the tanks rolled.

When nations go to war, APTs stop gathering intelligence and start disrupting. Wiping government systems on the eve of invasion. Taking down power grids to amplify kinetic strikes. Pre-positioning inside the critical infrastructure of every country that supports the opposing side.

Energy, transport, telecom, defense supply chains, public institutions; all legitimate military targets. And the people defending them are the new front line.

Fact 1

According to Microsoft Threat Intelligence, there are 600+ nation-state threat groups tracked globally.

Source: Microsoft

Fact 2

In 2025, over 70% of cyberattacks involved critical infrastructure.

Source: IBM

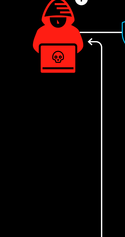
Fact 3

Russian cyberattacks on Ukraine surged nearly 70% in 2024; 4,315 incidents, primarily aimed at energy, government, and defense.

Source: CERT-UA

The Origins of Today's Most Active War Time APTs

- **Sandworm (APT44):** Russia GRU. Power grid attacks, NotPetya, Ukraine wipers.
- **Volt Typhoon:** China MSS. Pre-positioning in US critical infrastructure.
- **Lazarus Group:** North Korea. Financial theft funding the regime.
- **Charming Kitten:** Iran IRGC. Diplomatic and journalist targeting.
- **Ghostwriter:** Belarus/Russia-aligned. Disinformation and credential theft against NATO states.



Operation Olalampo

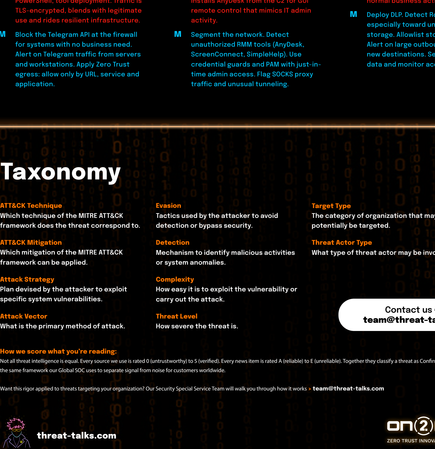
Iran weaponized Telegram, Rust, and an LLM. Then it hit 100 targets.

On January 26, 2026, MuddyWater launched Operation Olalampo: a spear-phishing campaign hitting 100+ government and critical infrastructure targets across the Middle East and North Africa. The campaign introduced four new malware families, including CHAR; a Rust-based backdoor with debug strings suggesting AI-assisted development, controlled through a Telegram bot. Attribution: Iran's Ministry of Intelligence and Security (MOIS).

Aliases	**Boggy Serpens, Mango Sandstorm, Seedworm**
mSOC confidence score	**Confirmed**
Threat category	**Cyber Attacks, APT Attacks / Cyber Espionage**
Severity	**Critical (Active campaign, nation-state actor)**

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1566.001 - Spear-phishing attachment	Hijacked internal email accounts to deliver malicious Office documents	In-memory payload execution, Rust-based tooling, Telegram C2, AI-assisted development	High	Government, Diplomats, Energy, Maritime, Telecom, Finance
T1204.002 - User Execution: Malicious File	Social engineering via blurred document lure	Sandbox evasion via nested wait loops in VBA macros	Medium	MENA region, Israel, Europe, US
T1059.001 - PowerShell	VBA macros decode and drop loaders; PowerShell for post-exploitation	Obfuscated scripts, decimal-encoded payloads hidden in UI elements	High	100+ organizations across multiple sectors

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1031 - Network Intrusion Prevention	Spear-phishing from compromised internal mailboxes	Anomalous internal email patterns, macro execution monitoring	Critical	Nation-State Actors (MuddyWater / MOIS)
M1038 - Execution Prevention	Malicious Office macros dropping loaders	Block Office child process creation (ASR rules), VBA execution logging	Critical	APT / Initial Access Broker
M1037 - Filter Network Traffic	Telegram API for C2, HTTP status code-based tasking	Monitor for Telegram API traffic from endpoints, flag unauthorized RMM tools	Critical	Iranian MOIS (Boggy Serpens)
M1040 - Behavior Prevention on Endpoint	In-memory payload execution via process hollowing (RunPE)	Behavioral analysis for memory injection, Rust binary anomaly detection	Critical	



Compromised mailbox and spear-phishing

1 The attacker hijacks an internal mailbox (masked via NordVPN) and sends spear-phishing emails from this trusted address to colleagues or partners. Lures are tailored to region and sector: HR documents, cybersecurity guidelines, government memos, all carrying malicious Office attachments.

M Enforce DMARC, DKIM and SPF, then layer behavioral analytics on internal mail flow. Flag mailboxes suddenly contacting new departments, off-hours sends, or bursts of similar messages. These emails pass reputation checks; only behavior gives them away.

Macro execution and payload drop

2 Opening the document shows blurred content and an "Enable Content" prompt. Once macros run, a VBA Workbook_Open() event fires a nested wait loop to dodge sandboxes, then decodes a payload hidden in UserForm1.TextBox1.text, drops it as MicrosoftExcelUser.exe and executes.

M Disable macros by default via Group Policy. Apply ASR rules to block Office from spawning child processes or writing executables. Log VBA execution. Where macros are essential, allow only signed macros from trusted locations.

Loader deploys CHAR backdoor

3 The dropped loader XOR-decrypts the final payload and uses process hollowing (RunPE) to inject CHAR, a Rust-based backdoor, into a legitimate process in memory. Rust complicates reverse engineering. Debug strings with emoji's hint at AI-assisted development.

M Use EDR with behavioral detection for process hollowing and in-memory execution. Watch parent-child relationships (Office spawning unknown binaries). Application allowlisting stops the loader before it runs.

Telegram C2 communication

4 CHAR connects to a Telegram bot ("Olalampo", username stager_S1_bot) for C2. Operators issue commands through the chat. CHAR runs them locally: directory navigation, cmd.exe, PowerShell, tool deployment. Traffic is TLS-encrypted, blends with legitimate use and rides resilient infrastructure.

M Block the Telegram API at the firewall for systems with no business need. Alert on Telegram traffic from servers and workstations. Apply Zero Trust egress: allow only by URL, service and application.

Post-exploitation and lateral movement

5 Operators add a SOCKS5 reverse proxy for tunneling, the Kalim backdoor as secondary access and tools to harvest browser credentials and sessions. Parallel campaigns drop HTTP_VIP, which installs AnyDesk from the C2 for GUI remote control that mimics IT admin activity.

M Segment the network. Detect unauthorized RMM tools (AnyDesk, ScreenConnect, SimpleHelp). Use credential guards and PAM with just-in-time admin access. Flag SOCKS proxy traffic and unusual tunneling.

Data exfiltration

6 Operators collect emails, documents, credentials and strategic intel, then exfiltrate using Rclone to Wasabi cloud storage. Legitimate sync tools and cloud services make the traffic look like normal business activity.

M Deploy DLP. Detect Rclone usage, especially toward unapproved cloud storage. Allowlist storage providers. Alert on large outbound transfers to new destinations. Segment sensitive data and monitor access patterns.

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 @
team@threat-talks.com

How we score what you're reading:
Not all threat intelligence is equal. Every source we use is rated 0 (untrustworthy) to 5 (verified). Every news item is rated A (reliable) to E (unreliable). Together they classify a threat as Confirmed, Verified, or Credible; the same framework our Global SOC uses to separate signal from noise for customers worldwide.

Want this rigor applied to threats targeting your organization? Our Security Special Service Team will walk you through how it works > **team@threat-talks.com**

threat-talks.com

ON2IT ZERO TRUST INNOVATORS

amsix