Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

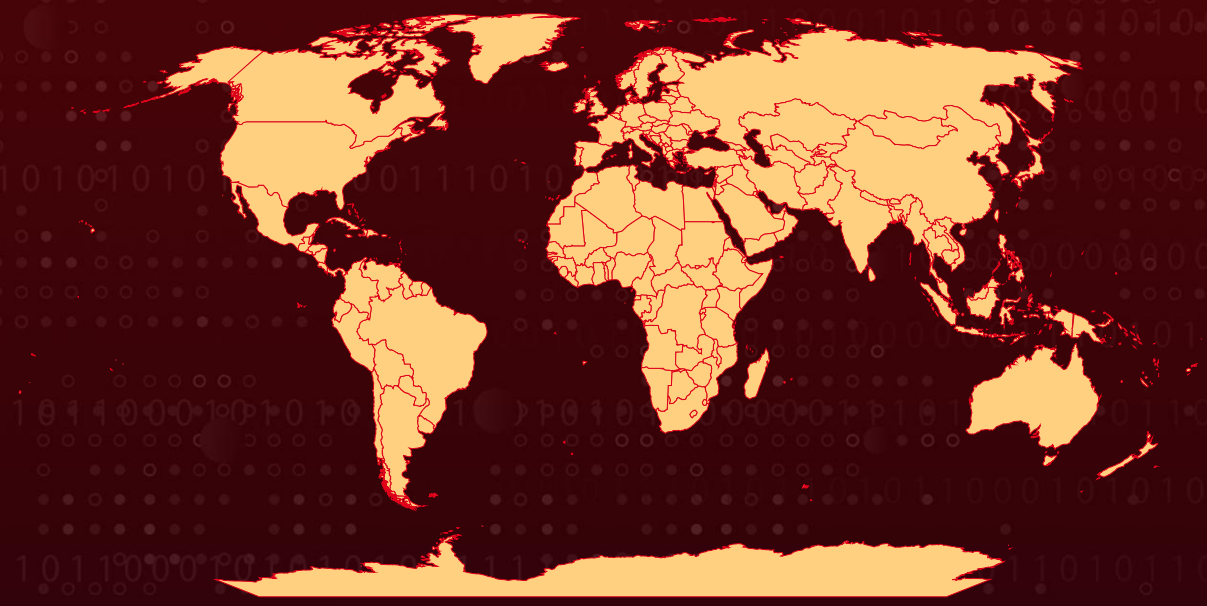
Iranian MOIS Leverages Telegram-Based C2 in Espionage Campaign Targeting Dissidents

Date of Publication	Admiralty Code	TA Number
March 26, 2026	A1	TA2026083

Summary

First Seen: Late 2023
Targeted Regions: Global (primarily Middle East-focused victims)
Targeted Platform: Windows
Campaign Name: MOIS Telegram C2 Malware Campaign
Targeted Sectors: Government, NGOs, Human Rights Organizations, Media/Journalism, Energy, Marine Services, Telecommunications, Critical Infrastructure
Targeted Individuals: Dissidents, Journalists, Political Opposition, Academics
Threat Actor: **Handala Hack** (aka HomeLand Justice, Karma, Storm-0842, Banished Kitten, Void Manticore), **MuddyWater** (aka Earth Vetala, Mango Sandstorm, MUDDYCOAST, Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, BoggySerpens, Yellow Nix), **Prince of Persia** (aka Infy, Operation Mermaid, APT-C-07)
Attack: An ongoing malware campaign conducted by Iran's Ministry of Intelligence and Security (MOIS), active since Fall 2023, in which cyber actors use Telegram as command-and-control infrastructure to deliver multi-stage malware targeting Iranian dissidents, journalists, and opposition groups worldwide. The attackers use social engineering to deliver malware disguised as legitimate applications, which then establishes persistent access for screen and audio recording, data theft, and exfiltration. This activity is attributed to the MOIS-linked entities "Handala Hack" and "Homeland Justice," known for hack-and-leak operations, phishing, extortion, and destructive wiper attacks. The campaign blends technical compromise with information operations, leveraging stolen data for public exposure to inflict reputational and political damage in support of Iran's geopolitical objectives.

Attack Regions



Attack Details

#1

An ongoing malware campaign linked to Iran's Ministry of Intelligence and Security (MOIS), the attackers use Telegram as a command-and-control (C2) platform to target Iranian dissidents, journalists, opposition groups, and others seen as threats to the government. The campaign has been active since at least Fall 2023 and is used to collect intelligence, steal data, and sometimes leak that data publicly to damage victims. The FBI has connected this activity to a group called "Handala Hack," which claimed responsibility for a July 2025 hack-and-leak operation targeting individuals voicing concerns about current events in Iran, known for phishing, data theft, extortion, and destructive attacks.

#2

The attack uses multiple stages and mainly targets Windows systems. It starts with social engineering, where attackers pretend to be trusted contacts or support staff on messaging apps. They trick victims into downloading malware disguised as legitimate software, such as Telegram or WhatsApp-related files, KeePass, or other tools. These files are often customized for each victim, which shows the attackers study their targets in advance. Once the victim runs the file, it installs another hidden malware component that connects to attacker-controlled Telegram bots.

#3

After infection, the malware tries to stay hidden and avoid detection. It changes system settings to bypass security tools and uses Windows registry entries to stay active even after reboot. Additional tools such as MicDriver.exe/dll, Winappx.exe, MsCache.exe, RuntimeSSH.exe, and smqdservice.exe are used to collect and send data, including recording the screen and audio, capturing cache data, and compressing stolen files with password protection before exfiltrating them. One tool, MicDriver, is designed to record screen and audio specifically during Zoom meetings, showing that attackers are interested in capturing private virtual conversations.

#4

This campaign also shows how attackers combine hacking with information operations. Stolen data can be manipulated or selectively exposed and leaked online through aligned media channels to embarrass or pressure victims. Using Telegram helps attackers hide their activity because it is a trusted and widely used platform, making it harder for defenders to detect or block.

#5

Notably, the abuse of Telegram as C2 is not limited to this campaign alone, it reflects a broader tactical shift among multiple Iranian state-sponsored actors. MuddyWater, another MOIS-linked APT group, adopted Telegram bot-based C2 in its Operation Olalampo campaign (first observed January 2026), deploying a Rust-based backdoor called CHAR controlled via a Telegram bot to target organizations across the MENA region.

#6 The Prince of Persia (Infy) APT group, active since 2007, also shifted from its legacy FTP-based C2 to Telegram with its updated Tonnerre v50 malware, detected in September 2025, to conduct long-term surveillance of dissidents and academics. Additionally, a newly identified campaign dubbed RedKitten, first observed in early January 2026, uses Telegram for C2 alongside GitHub and Google Drive to target Iranian NGOs and human rights documenters. This convergence of multiple Iranian threat actors on Telegram as C2 infrastructure underscores a deliberate strategic trend of exploiting trusted commercial platforms to blend malicious traffic with legitimate usage, complicating detection and attribution for defenders.

#7 Overall, this is a sophisticated and long-term campaign focused on espionage, intelligence gathering, and inflicting reputational damage, while also maintaining the capability for destructive attacks through custom wiper malware. It highlights how advanced threat actors are improving their methods and abusing trusted platforms to evade detection, making strong security practices and user awareness more important than ever.

Recommendations

Verify Software Sources and Incoming Communications: Download software only from official app stores or verified vendor websites, as this campaign relies on victims downloading malware disguised as trusted applications like Telegram, WhatsApp, KeePass, and Pictory. Exercise heightened caution with communications on messaging platforms, especially from unknown individuals or contacts making unusual requests, and verify identities through a separate trusted channel before downloading any files.

Monitor for Telegram-Based C2 Traffic: Monitor network traffic for connections to api.telegram[.]org from endpoints where Telegram is not an approved application. Unexpected outbound traffic to Telegram's API infrastructure may indicate C2 activity associated with this campaign.

Harden Endpoint Defenses: Enable and regularly run antivirus or anti-malware solutions across all endpoints. Configure security tools to monitor PowerShell activity and flag unauthorized registry modifications, as this campaign uses both techniques for evasion and persistence. Keep all devices updated with the latest operating system patches.

Enforce Strong Authentication: Enforce strong, unique passwords across all accounts and implement multi-factor authentication (MFA) wherever possible. This adds an additional layer of defense even if credentials are compromised during data exfiltration.

Conduct Security Awareness Training: Educate employees and at-risk individuals about social engineering tactics, particularly the impersonation methods used in this campaign. Training should cover how attackers pose as known contacts or platform support staff to build trust before delivering malicious files, and how to recognize and report such attempts.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1589: Gather Victim Identity Information	
	T1598: Phishing for Information	
Resource Development	T1583: Acquire Infrastructure	
	T1587: Develop Capabilities	T1587.001: Malware
	T1585: Establish Accounts	T1585.001: Social Media Accounts
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Collection	T1113: Screen Capture	
	T1123: Audio Capture	
	T1005: Data from Local System	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
Exfiltration	T1567: Exfiltration Over Web Service	
	T1041: Exfiltration Over C2 Channel	
Command & Control	T1102: Web Service	
	T1071: Application Layer Protocol	T1071.001: Web Protocols

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4a3b003994112b4dd24ac8b9cc4757f4a12576b57b3cc8f5028d85fbceb7c405, 0d74156089292eee308017c8e8a7550739ecb6149ff379810f7c54b1dbaabc91, 067d93741bcab16810ef15c11941245229519470dc7b24793dd1d3a7addacaae, e8b633dcad173eb41ef02686b46779a4a0e53df7f6c63039a798f2db5eb83afc, d3bb28307d11214867c570fe594f773ba90195ed22b834bad038b62bf75a4192, c40c94d787f6a35ac1cb4c5f031cf5777b77c79dc3929181badea33aaf177aa7, 59ee007fd17280470724eb8a11ab12a98e85fd2383af3065f5f09a7e1a73f88c, 90aebc9849b659515fd70dde6db717ad457ab2a90522a410d1fd531ca8640624, 96ee9d3ed80c59c4bf39ed630efbfa53591fbe51155db7919ef64535a6171044, 6d474cf5aeb58a60f2f7c4d47143cc5a11a5c7f17a6b43263723d337231c3d60, 16164c83ce4786ab85aa3fc9566a317519e866ff6cad3fbd647f3e955b8a8255, 36413af1a7c7dc9e49fdf465ebc5abc3b4bb6b33f1c5ccaa17ae5e0794b6faaa, 6e1bb2c41500ee18bd55a2de04bb3d74bd5c5e8c45eaeef030c7c6ea661cc2db, ac0e045b6f3683315ef420971f382e167385e39023d118d023fa6989e35fadf6, d58e3617d759d46248718ac4dfb46535d73febffd17fad1fd8ab47ce08da2fb4, e5c4295c5c57d80c875860b44f4c33ee921393bb8ce14c7be0f5ef47d7171265
MD5	7402F2F9263782A4C469570035843510, F8B5554808428291ACC65D1FD2EFE01C, D70EBF20E3D697897BAD5BEBF72EA271, 3E7A2FCEF1D038D05B20148C573A6499, 1E6B601F733BC40EAA58916986BFC5B9, A3394EF7FFA7E88B2E7EFAEE4617FE04, 2965817D063F1E8F9889F9126443D631, EBDD9595B79B39F53909D862499DBC94, E51FF37FB431767DCDEC0B5E6D2A786A,

TYPE	VALUE
MD5	7E23FFADB664B0E53D821478A249D84C, B9086413E7B6A0C6A11C25D14C22615F, 481C5B5E69A08C3DF206C59FD8DDC0DC
File Names	KeePass.exe, MicDriver.dll, MicDriver.exe, MsCache.exe, Pictory_premium_ver9.0.4.exe, rantom.txt, RuntimeSSH.exe, RuntimeSSH.exe, smqdservice.exe, Telegram_Authenticator.exe, winappx.exe
File Path	%LOCALAPPDATA%\WindowsMediaSync\AppVStreamingUX_Multi_User.dll

References

https://www.ic3.gov/CSA/2026/260320.pdf

https://hivepro.com/threat-advisory/void-manticore-irans-evolving-cyber-warfare-model/

https://hivepro.com/threat-advisory/operation-olalampo-muddywater-expanding-campaign-across-mena/

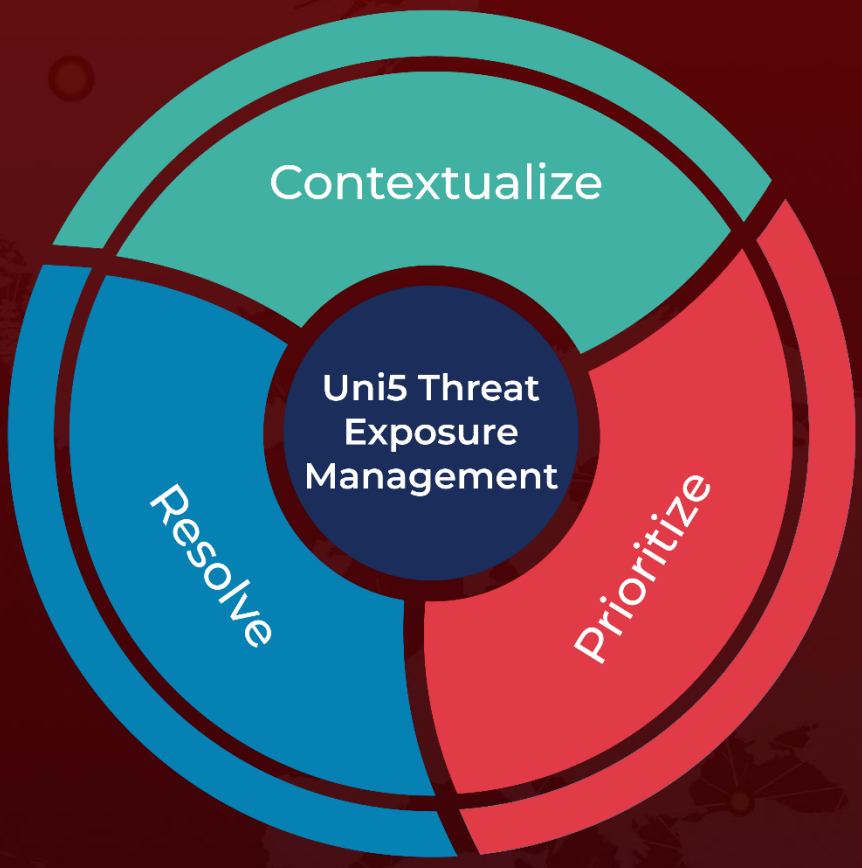
https://hivepro.com/threat-advisory/prince-of-persia-apt-campaigns-across-iran-europe-and-beyond/

https://harfanglab.io/insidethelab/redkitten-ai-accelerated-campaign-targeting-iranian-protests/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 26, 2026 • 06:30 AM

More at www.hivepro.com