Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

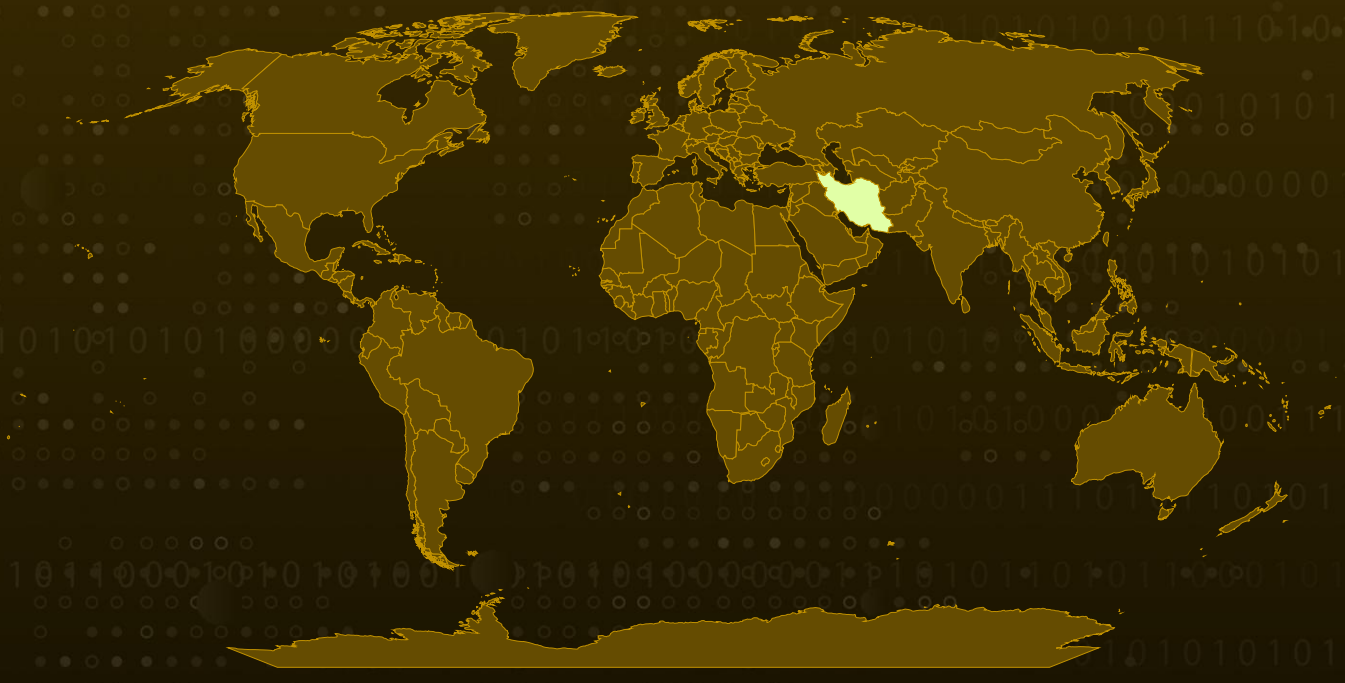
CRESCENTHARVEST an Espionage Campaign Disguised as Solidarity

Date of Publication	Admiralty Code	TA Number
February 20, 2026	A1	TA2026051

Summary

First Seen: January 9, 2026
Targeted Region: Iran
Targeted Products: Google Chrome, Microsoft Edge, Mozilla Firefox, Telegram Desktop
Targeted Industries: Civil Society Organizations, Activist Groups, Journalism, Non-Governmental Organizations (NGOs)
Campaign: CRESCENTHARVEST
Attack: CRESCENTHARVEST is a targeted espionage campaign aimed at supporters of Iran's protests, using calculated social engineering to disguise surveillance as solidarity. The operation reflects a sustained, covert intelligence effort with consequences that can extend beyond digital compromise into real-world intimidation.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

A campaign identified as CRESCENTHARVEST appears to target supporters of Iran's ongoing protests, with the objective of sustained surveillance and data theft. The operation depends on deliberate social engineering, frequently initiated through spear-phishing. Attackers invest time in establishing credibility, presenting themselves as allies of the protest movement. Targets receive a RAR archive framed as frontline documentation, containing authentic protest images and videos alongside a Farsi-language report describing the "rebellious cities of Iran." The material is structured to resonate with Farsi-speaking individuals sympathetic to the unrest.

#2

Among the legitimate files are two malicious shortcut (.LNK) files disguised with double extensions to resemble standard media. When executed, a concealed script initiates a sequence of system processes. Command Prompt is launched, followed by PowerShell, which extracts an embedded ZIP archive. The archive includes a legitimately signed Google binary, two malicious DLLs, several benign support files, and a decoy media file. Persistence is achieved through a scheduled task configured to trigger on Windows NetworkProfile events, ensuring execution whenever network connectivity is established, including after a reboot.

#3

The intrusion relies on DLL sideloading. The signed Google binary is leveraged to load malicious libraries without strict path controls, enabling unauthorized code to run under the appearance of a trusted application. The first module, developed in C++, extracts and decrypts Chrome's application-bound encryption keys through Component Object Model interfaces. The second module incorporates anti-analysis measures using Windows Job Objects and conducts comprehensive data collection. It extracts credentials, cookies, and browsing history from Chrome, Edge, and Firefox, captures Telegram session data, and deploys a low-level keyboard hook to record keystrokes in a hidden file.

#4

Once the keystroke log reaches approximately 2,000 bytes, it is transmitted to a command-and-control server. Additional stolen data is stored in concealed directories, compressed, and exfiltrated through encrypted HTTPS multipart uploads. CRESCENTHARVEST reflects a sustained and targeted espionage effort. Similar surveillance activity has been linked to intimidation and harassment, highlighting the broader consequences of such operations.

Recommendations

Treat Unsolicited Protest-Related Files with Extreme Skepticism: Avoid opening archives, images, videos, or documents received through unsolicited channels, especially those related to politically sensitive topics like the Iran protests, even if the content appears sympathetic to one's views.

Deploy Detection Rules for Malicious .LNK Abuse: Implement endpoint detection rules that flag .LNK files with embedded scripts, double file extensions (.jpg.lnk, .mp4.lnk), and .LNK files executing nested conhost.exe processes with headless switches, as these are hallmarks of the CRESCENTHARVEST delivery mechanism.

Monitor for DLL Sideloading via Signed Binaries: Create detection rules to alert on the execution of software_reporter_tool.exe outside of standard Chrome installation directories, and monitor for unsigned or suspicious DLLs (particularly version.dll and urtcbased140d_d.dll) being loaded alongside signed executables.

Audit Scheduled Tasks for Event-Based Persistence: Review scheduled tasks on endpoints for unusual triggers, specifically tasks bound to Windows NetworkProfile events (EventID 10000), which CRESCENTHARVEST abuses for persistence whenever the system gains network connectivity.

Adopt Hardware Security Keys for Authentication: At-risk individuals, including activists, journalists, and members of diaspora communities, should adopt FIDO2/WebAuthn hardware security keys for authentication on critical accounts, as these are resistant to credential theft even if browser data is exfiltrated.

Enable Enhanced Browser Security and App-Bound Encryption Monitoring: Monitor for unauthorized access to Chrome's Local State file and the app_bound_encrypted_key field, and alert on unexpected COM object instantiation related to browser elevation brokers, which are indicators of the CRESCENTHARVEST key decryption module.

Implement Network Segmentation and DNS Monitoring: Deploy network segmentation to limit lateral movement and monitor DNS queries for newly registered domains and connections to known suspicious ASNs. Implement DNS sinkholing for identified C2 domains.

Monitor for Keylogger and Data Staging Artifacts: Scan endpoints for the presence of hidden files in system directories, particularly C:\Windows\System32\spool\Drivers\color\daT.txt (keylogger output) and decrypted_appbound_key.txt in APPDATA folders, as these are direct indicators of CRESCENTHARVEST activity.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spear-Phishing Attachment
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL
	T1218: System Binary Proxy Execution	
	T1036: Masquerading	T1036.007: Double File Extension
Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1539: Steal Web Session Cookie	
Collection	T1056: Input Capture	T1056.001: Keylogging
	T1005: Data from Local System	
Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0fbc1f9cbacf076d2ced458e2d1afff0c615640a4647996bca2b651b80f90a6e, fc1319166cfb607402e9dcaf68ef13ce10f326dbb6ac406ef576e1c02e7404a9, bd8a48d4dc71552c790a44065cce77c7592f1d00e6cbe904af01f1d164d4dd78, 03315debd0c7a253b59a6b447d0673aa3de84103ca3cd4d5b6148c018d90b39b, 62c4814c88521619ec6bc42e93b88c23f6727e1413f312e53063cdf089c6bc58, e3cf12272d9103e4693333543b0f25840b18ac6bbea11d17202d752e6a49d707, dde9fec23a8db87842babb40c306ee6685a13de7a6a2d9f6dc65ed5ea5df87a3
Filename	version.dll, urtcbased140d_d.dll, VID_20260114_000556_609.mp4.lnk, IMG_20260140_000315_689.jpg.lnk, files.rar, tmp1732799711.zip, tmp205099634.zip
Domain	servicelog-information[.]com
IPv4	185[.]242[.]105[.]230

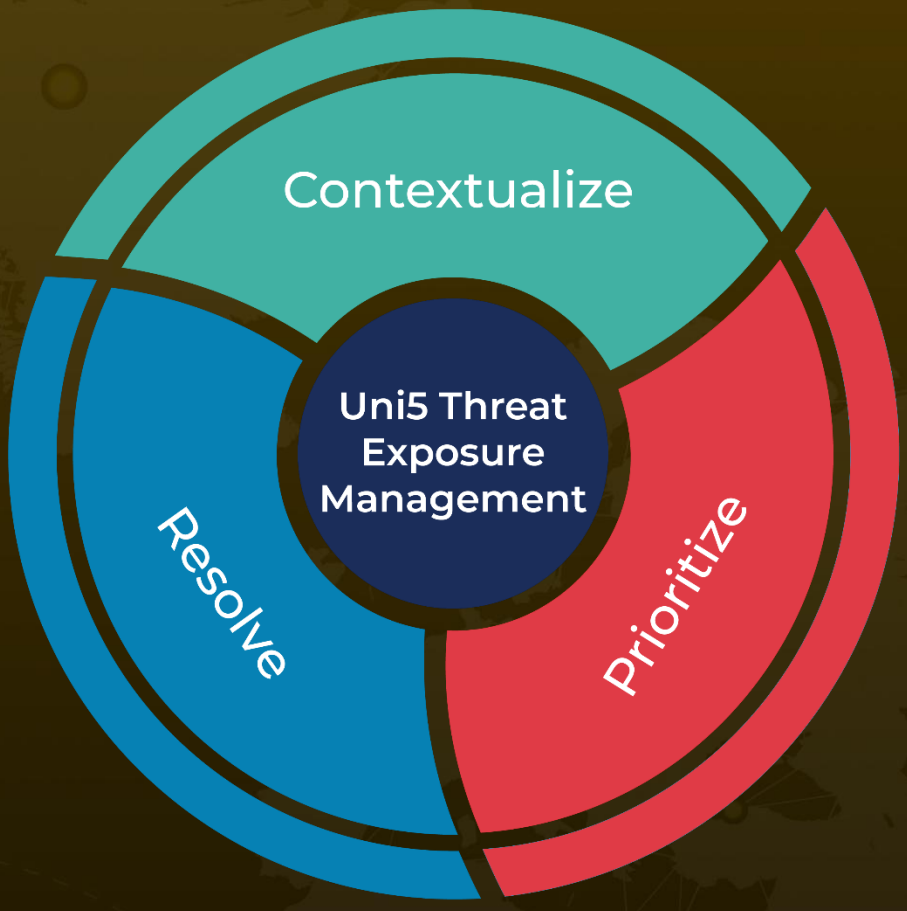
References

https://www.acronis.com/en/tru/posts/crescentharvest-iranian-protestors-and-dissidents-targeted-in-cyberespionage-campaign/

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

February 20, 2026 • 4:00 AM

More at www.hivepro.com