Hive Pro

Threat Level

Red

CISA: AA22-264A

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

Void Manticore: Iran's Evolving Cyber Warfare Model

Date of Publication	Last Updated Date	Admiralty Code	TA Number
March 11, 2026	March 20, 2026	A1	TA2026066

Summary

First Seen: July 2022
Targeted Countries: Israel, United States, Albania, Jordan, Gulf States
Targeted Platform: Windows and Linux
Targeted Industries: Government agencies and services, Critical infrastructure, Oil & Gas, Energy, Telecommunications, Defense, NGOs, Media, Think Tanks, IT and Service Providers, Education, Transportation, Airlines, Maritime and Healthcare
Threat Actor: Void Manticore (aka HomeLand Justice, Karma, Storm-0842, Banished Kitten, Handala Hack)
Malware: BiBi Wiper, Cl Wiper, No-Justice Wiper, Handala Wiper, Handala PowerShell Wiper, Rhadamanthys, Hatef Wiper, Hamsa Wiper

Timeline

July 2022
First attacks under **"Homeland Justice"** attacks Albanian e-government systems

September 2022
Second wave hits Albania; CISA/FBI attributes to Iran

Late 2023
Adopts "Handala" persona; expands cognitive warfare

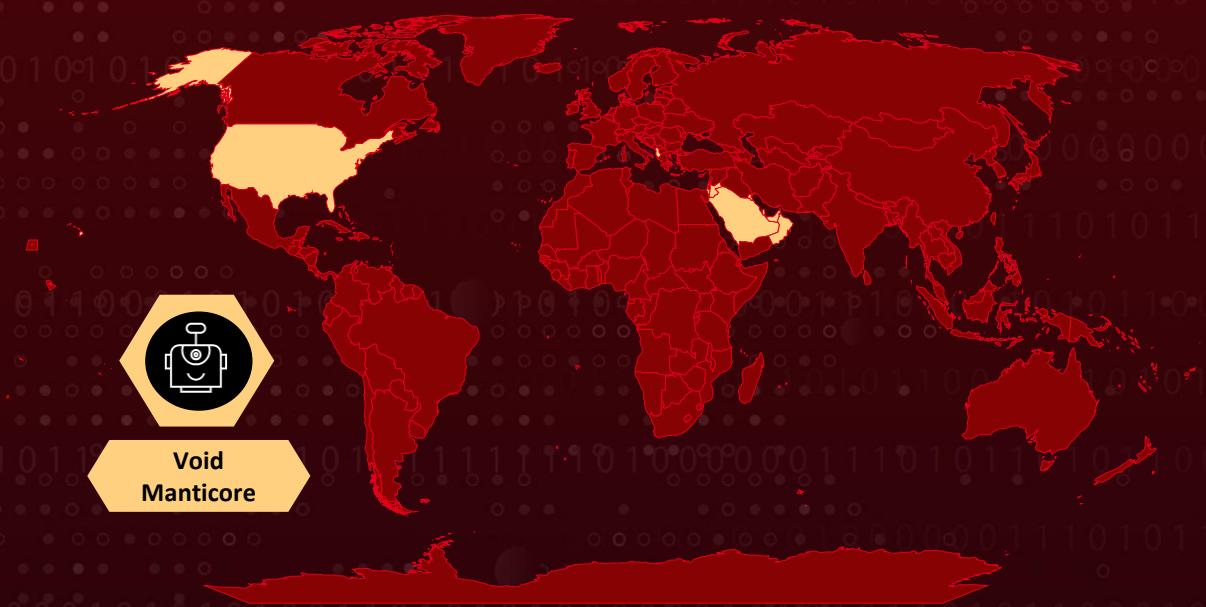
May 2024
Scarred Manticore-to-Void Manticore handoff documented

2024 - 2025
Targets NGOs, think tanks; **refines hybrid attack model**

January 2026
Uses smuggled **Starlink** terminals during Iran blackout

Late February 2026
Active **post-Epic Fury**; operations largely opportunistic

Actor Map



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2019-0604	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✓	✓

Actor Details

#1 Void Manticore (aka Storm-0842, BANISHED KITTEN) is an Iranian advanced persistent threat group operating under the direction of Iran's Ministry of Intelligence and Security (MOIS), supervised by Seyed Yahya Hosseini Panjaki, a MOIS deputy minister who was reportedly killed during Israeli strikes on Iran in early March 2026. The group first surfaced in July 2022 with a destructive cyberattack against Albania's e-government systems under the persona "Homeland Justice," strategically timed to disrupt a conference of the Iranian opposition group MEK.

#2 Iranian actors had maintained access to Albanian networks for approximately 14 months before striking, deploying custom wipers including Cl Wiper and No-Justice to cripple government infrastructure. A second wave targeted Albanian border systems in September 2022 following Albania's severing of diplomatic ties with Iran, with stolen data publicly leaked on Telegram.

#3 The group operates under multiple regional personas, "Homeland Justice" for Albania and "Karma" for Israel, with "Handala" having fully replaced Karma as the sole operational front since late 2023. Combining technical destruction with psychological warfare as a hallmark operational approach. A critical element of Void Manticore's operational model is its structured collaboration with Scarred Manticore, another MOIS-linked espionage group.

#4 This "handoff" workflow sees Scarred Manticore first breach targets to establish persistent access and conduct quiet data exfiltration, sometimes for over a year, before transferring control to Void Manticore when a decision is made to shift from intelligence collection to destruction. This partnership allows Iran to maintain espionage access while reserving the option to weaponize it during geopolitical escalations, a procedure observed against both Albania (2022) and Israel (2023-2026). In recent intrusions, initial access was established months before the destructive phase, with hundreds of brute-force attempts against VPN infrastructure observed from commercial VPN nodes and, since January 2026, from Starlink IP ranges following Iran's internet shutdown.

#5

Following the October 2023 Israel-Hamas conflict, Void Manticore pivoted aggressively toward Israeli organizations under the persona "Karma," claiming attacks against more than 40 entities, though the verified impact of many claims remains unclear. The group deployed its signature BiBi Wiper, named after Israeli Prime Minister Benjamin Netanyahu, in Windows and Linux variants to corrupt files while appending the ".BiBi" extension. Newer variants evolved to target disk partition tables directly, complicating data restoration. These destructive operations were consistently paired with public data leaks on Telegram to amplify psychological impact.

#6

In late 2023, the group adopted its most sophisticated persona yet: Handala, a name borrowed from a Palestinian refugee cartoon symbol to create moral legitimacy while complicating Iranian attribution. Under this branding, Void Manticore expanded into cognitive warfare, targeting personal devices of aides and family members to indirectly access senior Israeli decision-makers. Their "RedWanted" (aka “Saturday Files") campaign doxed personal details of Israelis in defense and media sectors while offering financial rewards for information.

#7

The group demonstrated evolving adaptability, using commercial infostealers notably Rhadamanthys disguised as software updates impersonating F5 and Israel's National Cyber Directorate, Telegram account takeover via session hijacking and SIM swapping, and wipers masked as security tools under filenames CrowdStrike.exe (July 2024) and CrowdStrike.bin (March 2026), exploiting trust in legitimate vendors. Between 2024–2026, targeting broadened to NGOs, Western think tanks, and US enterprises, most notably Stryker, where the group weaponized Microsoft Intune to remotely wipe devices globally. Leak publication evolved into a deliberately planned phase of the attack lifecycle.

#8

Since mid-January 2026, the group has exploited Starlink terminals smuggled into Iran via black markets to maintain operations during government-imposed internet blackouts. Recent operations introduced new TTPs, NetBird for internal tunneling and lateral movement (replacing earlier reliance on reGeorg), and up to four simultaneous wiping methods, a custom Handala Wiper with MBR corruption, an AI-assisted PowerShell wiper that deletes user directories and fills drives with propaganda images, weaponized VeraCrypt disk encryption, and manual file/VM deletion via RDP. These wipers are now distributed enterprise-wide using Group Policy logon scripts and scheduled tasks.

#9

Following Operation Epic Fury (U.S.) and Operation Roaring Lion (Israel) in late February 2026, Handala remains active, claiming attacks on Israeli energy and Jordanian fuel infrastructure. With Iran's connectivity below 4%, operations are largely opportunistic. Operators have been observed connecting directly from Iranian IPs due to failed VPN connections, indicating significant OPSEC degradation. The group's evolution from Homeland Justice through Karma to Handala represents a mature hybrid warfare model integrating destruction with information operations for geopolitical impact. On March 19, 2026, the FBI seized Handala's clearnet domains (handala-hack[.]to and handala-redwanted[.]to) under a seizure warrant issued by the U.S. District Court for the District of Maryland.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Void Manticore	Iran **MOTIVE** Espionage, Sabotage, Geopolitical disruption, Politically and ideologically motivated	Israel, United States, Albania, Jordan, Gulf States	Government agencies and services, Critical infrastructure, Oil & Gas, Energy, Telecommunications, Defense, NGOs, Media, Think Tanks, IT and Service Providers, Education, Transportation, Airlines, Maritime and Healthcare

Recommendations

Patch Internet-Facing Systems Immediately: Prioritize patching known exploited vulnerabilities, especially CVE-2019-0604 in Microsoft SharePoint, which Void Manticore uses for initial access. Regularly update all internet-facing applications, VPN gateways, and remote access solutions to eliminate entry points that enable destructive attacks.

Deploy EDR with Wiper-Specific Detection Rules: Void Manticore's post-access TTPs are relatively unsophisticated and detectable by modern endpoint security. Configure EDR to detect known wiper behaviors including mass file corruption, partition table manipulation, ".BiBi" file extension changes, ElRawDisk driver abuse, and suspicious Mimikatz or batch file execution.

Maintain Offline, Immutable Backups: Wiper malware, including BiBi, Cl Wiper, No Justice Wiper, and Handala Wiper, are specifically designed to render data irrecoverable by corrupting files and disk partition tables. Maintain air-gapped, immutable backups of all critical data and systems, and regularly test restoration procedures through tabletop exercises. Particular attention should be given to protecting boot records and partition layouts, as the group's wipers target disk structures to make data inaccessible even when underlying data remains intact.

Prepare for Combined Destruction and Influence Operations: Void Manticore's attack lifecycle deliberately integrates data leaks and narrative amplification alongside technical destruction, leak publication is a planned phase, not a byproduct. Develop cross-functional response plans covering IT, legal, and communications teams for combined wiper-and-leak scenarios, and monitor Telegram channels and social media for the group's active personas (Homeland Justice, Karma, Handala). The handoff from Scarred Manticore to Void Manticore leaves an extremely short window before destruction begins, so pre-authorized containment playbooks should be ready for immediate execution.

Harden MDM and Identity Infrastructure: The Stryker attack demonstrated that Microsoft Intune and similar MDM platforms can be weaponized as destructive tools when administrative accounts are compromised. Enforce phishing-resistant MFA (FIDO2/hardware keys) on all Entra ID Global Administrator and Intune admin accounts. Implement Just-in-Time (JIT) administrative access using Microsoft Entra Privileged Identity Management (PIM) to ensure admin roles are only active when needed and require multi-party approval. Monitor for anomalous Intune actions including mass RemoteWipe, FactoryReset, or RetireDevice commands, first-time admin logins from unfamiliar geolocations or Starlink IP ranges, and new Global Administrator account creation. Restrict BYOD enrollment policies to limit the blast radius of a compromised MDM console.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	
	T1566: Phishing	
	T1133: External Remote Services	
	T1199: Trusted Relationship	
Execution	T1059: Command and Scripting Interpreter	
	T1204: User Execution	T1204.002: Malicious File
	T1047: Windows Management Instrumentation	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
	T1037: Boot or Logon Initialization Scripts	T1037.003: Network Logon Script
Privilege Escalation	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1068: Exploitation for Privilege Escalation	

Tactic	Technique	Sub-technique
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1036: Masquerading	
	T1140: Deobfuscate/Decode Files or Information	
	T1070: Indicator Removal	
	T1218 : System Binary Proxy Execution	T1218.009: Regsvcs/Regasm
Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1555: Credentials from Password Stores	
	T1110: Brute Force	
Discovery	T1087: Account Discovery	T1087.002: Domain Account
	T1082: System Information Discovery	
	T1018: Remote System Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1016: System Network Configuration Discovery	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
	T1572: Protocol Tunneling	
Collection	T1114: Email Collection	
	T1005: Data from Local System	
	T1039: Data from Network Shared Drive	

Tactic	Technique	Sub-technique
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	
	T1105: Ingress Tool Transfer	
	T1572: Protocol Tunneling	
Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	
Resource Development	T1583: Acquire Infrastructure	T1583.006: Web Services
	T1587: Develop Capabilities	T1587.001: Malware
	T1586: Compromise Accounts	
	T1585: Establish Accounts	T1585.001: Social Media Accounts
Impact	T1485: Data Destruction	
	T1561: Disk Wipe	T1561.001: Disk Content Wipe
		T1561.002: Disk Structure Wipe
	T1486: Data Encrypted for Impact	
	T1491: Defacement	T1491.002: External Defacement
	T1489: Service Stop	
	T1529: System Shutdown/Reboot	
	T1531: Account Access Removal	
Reconnaissance	T1590: Gather Victim Network Information	
	T1589: Gather Victim Identity Information	T1589.001: Credentials

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3c9dc8ada56adf9cebfc501a2d3946680dcb0534a137e2e27a7fcb5994cd9de6, 45bf0057b3121c6e444b316afafdd802d16083282d1cbfde3cdbf2a9d0915ace, 63dd02c371e84323c4fd9a161a75e0f525423219e8a6ec1b95dd9eda182af2c9, 7ad64b64e0a4e510be42ba631868bbda8779139dc0daad9395ab048306cc83c5, bad65769c0b416bb16a82b5be11f1d4788239f8b2ba77ae57948b53a69e230a6, cad2bc224108142b5aa19d787c19df236b0d12c779273d05f9b0298a63dc1fe5, e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0, ec4cd040fd14bff86f6f6e7ba357e5bcf150c455532800edf97782836e97f6d2, f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5, D0C03D40772CD468325BBC522402F7B737F18B8F37A89BACC5C8A00C2B87BFC6, DEEAF85B2725289D5FC262B4F60DDA0C68AE42D8D46D0DC19B9253B451AEA25A, 87F0A902D6B2E2AE3647F10EA214D19DB9BD117837264AE15D622B5314FF03A5, 85FA58CC8C4560ADB955BA0AE9B9D6CAB2C381D10DBD42A0BCEB8B62A92B7636, 74D8D60E900F931526A911B7157511377C0A298AF986D42D373F51AAC4F362F6, CC77E8AB73B577DE1924E2F7A93BCFD852B3C96C6546229BC8B80BF3FD7BF24E, aae017e7a36e016655c91bd01b4f3c46309bbe540733f82cce29392e72e9bd1f, 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8, fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2, ca9bf13897af109cb354f2629c10803966eb757ee4b2e468abc04e7681d0d74a, e28085e8d64bb737721b1a1d494f177e571c47aab7c9507dba38253f6183af35,

TYPE	VALUE
SHA256	454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567, 6f79c0e0e1aab63c3aba0b781e0e46c95b5798b2d4f7b6ecac474b5c40b840ad, ad66251d9e8792cf4963b0c97f7ab44c8b68101e36b79abc501bee1807166e8a, 64c5fd791ee369082273b685f724d5916bd4cad756750a5fe953c4005bb5428c, 336167b8c5cfc5cd330502e7aa515cc133656e12cbedb4b41ebbf847347b2767, f58d3a4b2f3f7f10815c24586fae91964eeed830369e7e0701b43895b0cefbd3, aae989743dddc84adef90622c657e45e23386488fa79d7fe7cf0863043b8acd4
IPv4	64[.]176[.]172[.]101, 188[.]92[.]255[.]96, 188[.]92[.]255[.]57, 82[.]25[.]35[.]25, 31[.]57[.]35[.]223, 107[.]189[.]19[.]52, 146[.]185[.]219[.]235, 188[.]92[.]255[.]X, 209[.]198[.]131[.]X, 149[.]88[.]26[.]X, 169[.]150[.]227[.]X, 149[.]154[.]167[.]220
IPv4:PORT	31[.]192[.]237[.]207[:]2515
MD5	0738242a521bdfe1f3ecc173f1726aa1, 1635e1acd72809479e21b0ac5497a79b, 18e01dee14167c1cf8a58b6a648ee049, 58d51c1152817ca3dec77f2eee52cbef, 59a85e8ec23ef5b5c215cd5c8e5bc2ab, 5b2ce9270beea5915ec9adbcd0dbb070, 60afb1e62ac61424a542b8c7b4d2cf01, 74a6ef9e7b49c71341e439022f643c8e, 78562ba0069d4235f28efd01e3f32a82, 7b71764236f244ae971742ee1bc6b098, 81e123351eb80e605ad73268a5653ff3, 8f6e7653807ebb57ecc549cef991d505, 8f766dea3afd410ebcd5df5994a3c571, a9fa6cfdba41c57d8094545e9b56db36, bbe983dba3bf319621b447618548b740, dae02f32a21e03ce65412f6e56942daa,

TYPE	VALUE
MD5	e233f2cdc91faafe1467d9e52f166213, E9b6ecbf0783fa9d6981bba76d949c94, 5986ab04dd6b3d259935249741d3eff2, 3cb9dea916432ffb8784ac36d1f2d3cd, 3236facc7a30df4ba4e57fddfba41ec5, 3dfb151d082df7937b01e2bb6030fe4a, E035c858c1969cffc1a4978b86e90a30, 8f69c9bb80b210466b887d2b16c68600, 8bdd1cb717aa2bd03c12c8b4c9df2d94
SHA1	14b8c155e01f25e749a9726958606b242c8624b9, 30632ea310114105969d0bda28fdce267104754f, 382c18388fb326221dfd7a77ee874f9ba60e04bf, 495847a93187cfb8c71f840cb7b41497ad95c64f, 49fd8de33aa0ea0c7432d62f1ddca832fab25325, 55d90ec44b97b64b6dd4e3aee4d1585d6b14b26f, 57534ccc33914c41f70e2cbb2103a1db18817d8b, 5d117d8ef075f3f8ed1d4edcc0771a2a0886a376, 5e061701b14faf9adec9dd0b2423ff3cfc18764b, 683eaec2b3bb5436f00b2172e287dc95e2ff2266, e03edd9114e7a0138d1309034cad6b461ab0035b, e866cc6b1507f21f688ecc2ef15a64e413743da7, f22a7ec80fbfdc4d8ed796119c76bfac01e0a908, fce0db6e66d227d3b82d4564446ede0c0fd7598c
File Names	Error4.aspx, cl.exe, GoXML.exe, Goxml.jpg, ClientBin.aspx, Pickers.aspx, evaluatesiteupgrade.cs.aspx, mellona.exe, win.bat, bb.bat, disable_defender.exe, rwdsk.sys, App_Web_bckwssht.dll, handala.exe, handala.bat, handala.gif, dra.ps1, carroll.cmd, L.a3x, CrowdStrike.bin CrowdStrike.exe

TYPE	VALUE
Host Names	WIN-P1B7V100IIS, DESKTOP-FK1NPHF, DESKTOP-R1FMLQP, WIN-DS6S0HEU0CA, DESKTOP-T3SOB36, WIN-GPPA5GI4QQJ, VULTR-GUEST, DESKTOP-HU45M79, DESKTOP-TNFP4JF, DESKTOP-14O69KQ, DESKTOP-9KG46L1, DESKTOP-G2MH4KD
Domain	api[.]telegram[.]org, Justicehomeland[.]org, Handala-Hack[.]to, Karmabelow80[.]org, Handala-Redwanted[.]to
URL	hxxp[:]//sjc1[.]vultrobjects[.]com/f5update/update[.]sh

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/

https://x.com/_CPResearch_/status/2013349461070586054

https://www.sophos.com/en-us/blog/hacktivist-campaigns-increase-as-united-states-iran-and-israel-conflict-intensifies

https://blog.checkpoint.com/research/unveiling-void-manticore-structured-collaboration-between-espionage-and-destruction-in-mois/

https://hivepro.com/threat-advisory/iranian-cyber-actors-target-critical-infrastructure/

https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/

https://research.checkpoint.com/2026/iranian-mois-actors-the-cyber-crime-connection/

https://www.dugganusa.com/post/the-handala-wiper-masquerades-as-crowdstrike-we-found-it-on-github

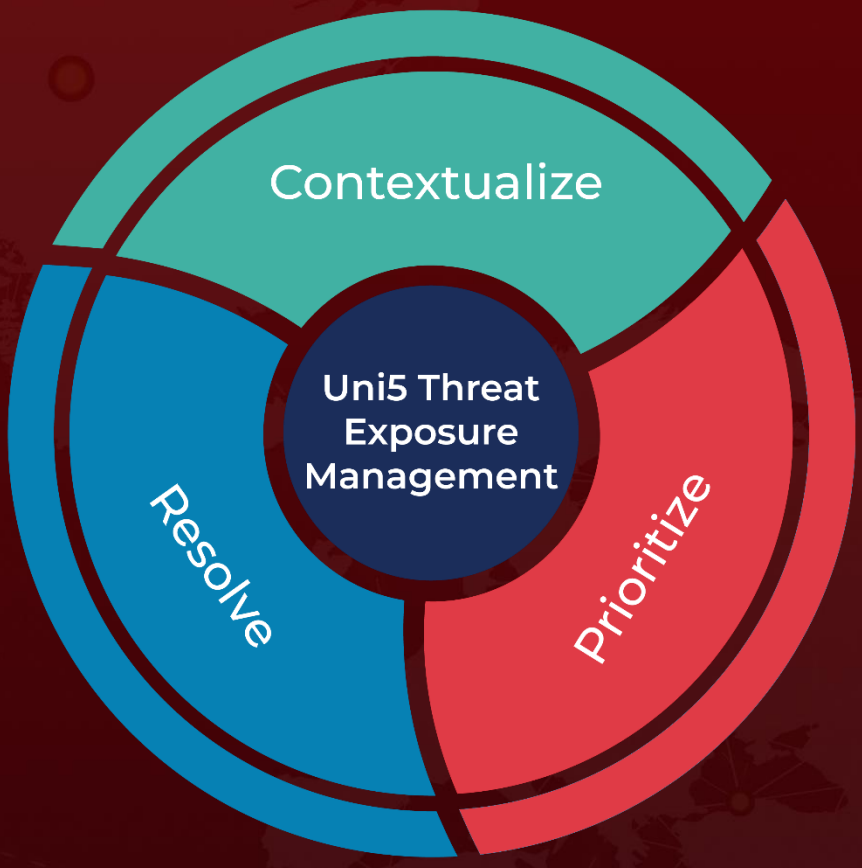
https://www.justice.gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations

https://intezer.com/blog/stealth-wiper-israeli-infrastructure/

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 11, 2026 • 9:00 AM

More at www.hivepro.com