



Threat Level

 Red

CISA: AA22-264A

HiveForce Labs

THREAT ADVISORY



ACTOR REPORT

Void Manticore: Iran's Evolving Cyber Warfare Model

Date of Publication

March 11, 2026

Admiralty Code

A1

TA Number

TA2026066

Summary

First Seen: July 2022

Targeted Countries: Israel, United States, Albania, Jordan, Gulf States

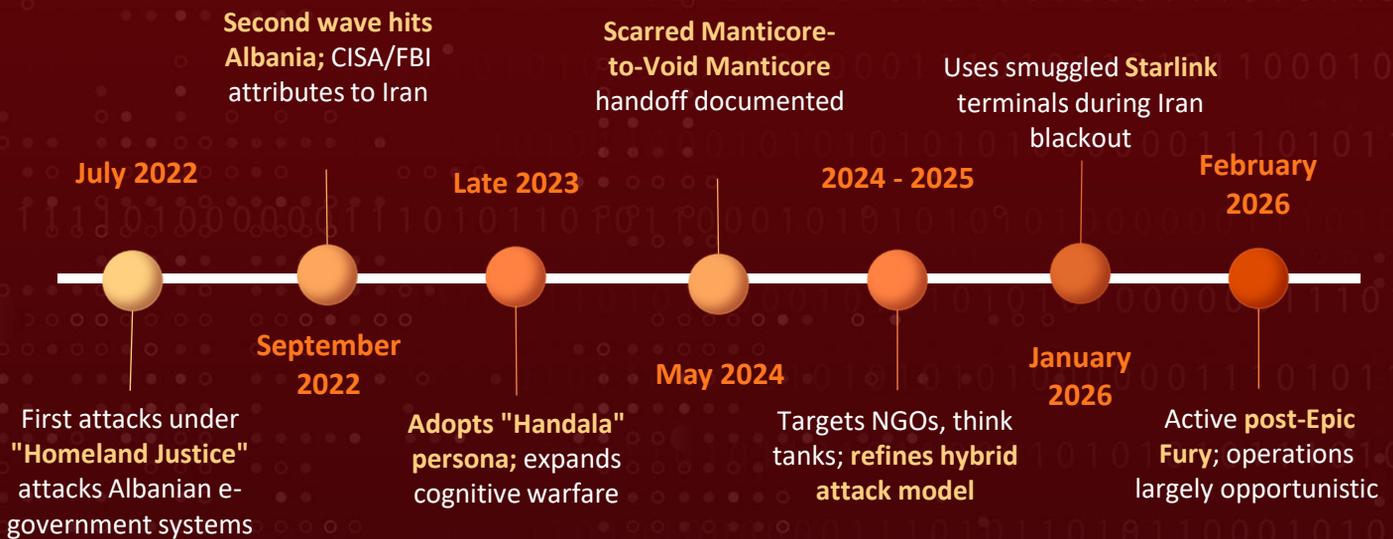
Targeted Platform: Windows and Linux

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, CI Wiper, No-Justice Wiper

Timeline



Actor Map



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 is an Iranian advanced persistent threat group operating under the direction of Iran's Ministry of Intelligence and Security (MOIS), tracked across vendors as Storm-0842, BANISHED KITTEN. 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 CI 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, 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).

#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

Technically, the group demonstrated significant adaptability: campaigns attributed to the cluster have used commercial infostealers disguised as legitimate software updates, Telegram account takeover via session hijacking and SIM swapping, and attempts to mask destructive payloads as security software updates. Between 2024 and 2026, targeting broadened to include NGOs and Western think tanks, with leak publication evolving into a deliberately planned phase of the attack lifecycle. Since mid-January 2026, the group has exploited Starlink terminals smuggled into Iran via black markets to maintain operations during government-imposed internet blackouts.

#8

In the current escalation following Operation Epic Fury (U.S.) and Operation Roaring Lion (Israel) in late February 2026, Handala remains active, claiming attacks on Israeli energy companies and Jordanian fuel infrastructure. However, with Iran's internet connectivity below 4%, researchers assess that near-term sophisticated operations from within Iran are likely constrained, with much observed activity being opportunistic. Void Manticore's evolution from Homeland Justice through Karma to Handala represents a mature, process-driven model of modern hybrid warfare, seamlessly integrating technical destruction with information operations, targeted intimidation, and narrative control to achieve maximum geopolitical impact.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Void Manticore	Iran	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
	MOTIVE Espionage, Sabotage, Geopolitical disruption, Politically and ideologically motivated		

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, CI Wiper, and No Justice 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.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1190</u> : Exploit Public-Facing Application	
	<u>T1078</u> : Valid Accounts	
	<u>T1566</u> : Phishing	
Execution	<u>T1059</u> : Command and Scripting Interpreter	
	<u>T1204</u> : User Execution	<u>T1204.002</u> : Malicious File
	<u>T1047</u> : Windows Management Instrumentation	
Persistence	<u>T1505</u> : Server Software Component	<u>T1505.003</u> : Web Shell
	<u>T1547</u> : Boot or Logon Autostart Execution	<u>T1547.001</u> : Registry Run Keys
	<u>T1053</u> : Scheduled Task/Job	
Privilege Escalation	<u>T1078</u> : Valid Accounts	<u>T1078.002</u> : Domain Accounts
	<u>T1068</u> : Exploitation for Privilege Escalation	

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

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

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3c9dc8ada56adf9cebfc501a2d3946680dcb0534a137e2e27a7fcb5994cd9de6, 45bf0057b3121c6e444b316afafdd802d16083282d1cbfde3cdbf2a9d0915ace, 63dd02c371e84323c4fd9a161a75e0f525423219e8a6ec1b95dd9eda182af2c9, 7ad64b64e0a4e510be42ba631868bbda8779139dc0daad9395ab048306cc83c5, bad65769c0b416bb16a82b5be11f1d4788239f8b2ba77ae57948b53a69e230a6, cad2bc224108142b5aa19d787c19df236b0d12c779273d05f9b0298a63dc1fe5, e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0, ec4cd040fd14bff86f6f6e7ba357e5bcf150c455532800edf97782836e97f6d2, f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5, D0C03D40772CD468325BBC522402F7B737F18B8F37A89BACC5C8A00C2B87BFC6, DEEAF85B2725289D5FC262B4F60DDA0C68AE42D8D46D0DC19B9253B451AEA25A, 87F0A902D6B2E2AE3647F10EA214D19DB9BD117837264AE15D622B5314FF03A5, 85FA58CC8C4560ADB955BA0AE9B9D6CAB2C381D10DBD42A0BCEB8B62A92B7636, 74D8D60E900F931526A911B7157511377C0A298AF986D42D373F51AAC4F362F6, CC77E8AB73B577DE1924E2F7A93BCFD852B3C96C6546229BC8B80BF3FD7BF24E
IPv4	64[.]176[.]169[.]22, 64[.]176[.]172[.]235, 64[.]176[.]172[.]165, 64[.]176[.]173[.]77, 64[.]176[.]172[.]101, 188[.]92[.]255[.]96, 188[.]92[.]255[.]57

TYPE	VALUE
MD5	0738242a521bdfe1f3ecc173f1726aa1, 1635e1acd72809479e21b0ac5497a79b, 18e01dee14167c1cf8a58b6a648ee049, 58d51c1152817ca3dec77f2eee52cbef, 59a85e8ec23ef5b5c215cd5c8e5bc2ab, 5b2ce9270beea5915ec9adbcd0dbb070, 60afb1e62ac61424a542b8c7b4d2cf01, 74a6ef9e7b49c71341e439022f643c8e, 78562ba0069d4235f28efd01e3f32a82, 7b71764236f244ae971742ee1bc6b098, 81e123351eb80e605ad73268a5653ff3, 8f6e7653807ebb57ecc549cef991d505, 8f766dea3afd410ebcd5df5994a3c571, a9fa6cfdba41c57d8094545e9b56db36, bbe983dba3bf319621b447618548b740, dae02f32a21e03ce65412f6e56942daa, e233f2cdc91faafe1467d9e52f166213, e9b6ecbf0783fa9d6981bba76d949c94
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,

TYPE	VALUE
File Names	bb.bat, disable_defender.exe, rwdsk.sys, App_Web_bckwsht.dll

Patch Link

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604>

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/_CPRResearch_/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/>

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

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com