Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

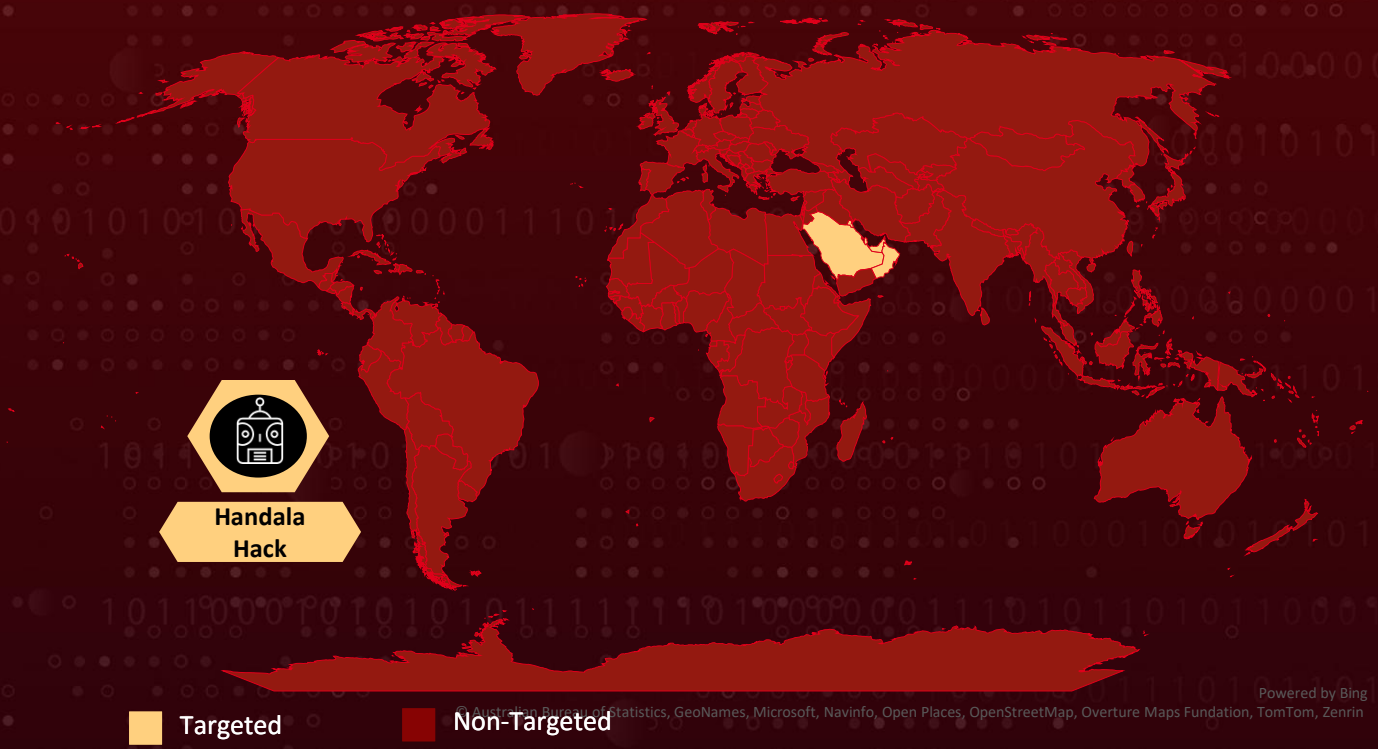
Handala Claims Destructive Wiper Attack on GCC Nation's Critical Infrastructure

Date of Publication	Admiralty Code	TA Number
April 14, 2026	A1	TA2026099

Summary

First Seen: April 12, 2026
Targeted Regions: Gulf Cooperation Council (GCC)
Targeted Platforms: Windows
Targeted Industries: Government, Real Estate, Legal, Transportation, and Critical Infrastructure
Threat Actor: Handala Hack (aka Void Manticore, HomeLand Justice, Karma, Storm-0842, Banished Kitten)
Malware: Wiper malware (specific variant undisclosed, assessed as Handala Wiper based on group's known arsenal)
Attack: The Iran-affiliated threat group Handala Hack Team, a state-directed persona operated by Iran's Ministry of Intelligence and Security (MOIS), claimed responsibility on April 12, 2026 for a destructive cyberattack allegedly targeting critical government infrastructure in a major GCC financial hub, specifically entities overseeing the country's legal, economic, and transportation sectors. The group claims to have destroyed 6 petabytes of data using wiper malware and exfiltrated 149 terabytes of classified documents, framing the operation as retaliation against the targeted nation's perceived alignment against the Iranian-led resistance axis during the ongoing 2026 conflict. The claimed attack aligns with Handala's established playbook of combining destructive wiping with hack-and-leak operations for maximum impact, consistent with techniques observed in a prior 2026 operation against a major US-based corporation. While none of the allegedly targeted entities or the host government have publicly confirmed the attack and independent verification remains pending, the group has demonstrated credible destructive capability throughout 2026, and we recommend treating Handala Hack group as a high-severity, actionable threat.

Attack Regions



Attack Details

#1 On April 12, 2026, the Iran-affiliated threat group Handala Hack Team claimed responsibility for a destructive cyberattack allegedly targeting critical government infrastructure in a major GCC financial hub. The group claims to have compromised multiple government entities overseeing key functions within the country's legal, economic, and transportation sectors, though none of the allegedly targeted entities or the host government have publicly confirmed the attack as of this writing.

#2 According to the claims, approximately 6 petabytes of data were destroyed using wiper malware, rendering it permanently unrecoverable, while an estimated 149 terabytes of classified and sensitive documents were simultaneously exfiltrated. That said, Handala has a well-documented history of overstating the scale of its operations, the group likely achieved some level of access, but the actual impact is likely far below what is being claimed. Our analysis indicates this is part of a sustained campaign targeting GCC and regional governments viewed as hostile to Iranian interests, with the group explicitly warning of continued operations.

#3 The impact could be severe, potentially affecting judicial records, citizen data, financial information, and urban mobility infrastructure, resulting in widespread service disruptions and exposure of sensitive government and corporate data. Evidence shared alongside the claim includes storage management interfaces showing bulk volume deletions, administrative dashboards resembling email security platforms, and system-level access indicators suggesting privileged control, consistent with the group's practice of publishing proof-of-access material.

#4 The claimed attack aligns with Handala's known playbook, combining bulk data destruction via custom wiper malware with large-scale exfiltration in a hack-and-leak model engineered for maximum disruption and psychological impact. Likely initial access vectors include compromised VPN credentials, infostealer-harvested administrative accounts, and targeted phishing, techniques consistent with a prior 2026 operation where the group reportedly wiped over 200,000 devices across a major US-based corporation spanning 79 countries by weaponizing a legitimate cloud-based endpoint management platform. Handala is assessed with high confidence by the FBI and US Department of Justice to be a state-directed persona operated by Iran's Ministry of Intelligence and Security (MOIS), tracked under designations including Void Manticore, Storm-0842, and BANISHED KITTEN.

#5 While the group has a documented history of inflating operational impact, it has demonstrated credible destructive capability throughout 2026 across healthcare, government, defense, and critical infrastructure sectors. Given the current threat landscape, including ongoing kinetic and cyber escalation and retaliatory escalation following law enforcement actions against the group, we recommend treating Handala hack as a high-severity, actionable threat. Organizations across the GCC region should immediately validate their defenses against the IOCs and adversary tradecraft profiled in our Handala Hack group advisory.

Recommendations

Immediate Actions: Organizations operating in GCC government and critical infrastructure sectors should immediately audit all administrative accounts with access to endpoint management platforms such as Microsoft Intune, Entra ID, and similar MDM solutions. Enforce phishing-resistant multi-factor authentication on all privileged accounts and implement just-in-time access with zero standing permissions for global and device administrator roles. Enable multi-admin approval for sensitive bulk operations, particularly remote wipe commands, to prevent a single compromised credential from triggering enterprise-wide destruction. For detailed threat actor tradecraft, IOCs, and defensive guidance specific to this group, refer to our previously published Handala Hack group actor profile advisory.

Identity and Credential Hygiene: Given Handala's reliance on infostealer-harvested credentials and VPN brute-force for initial access, organizations should scan for credential exposure across dark web marketplaces and infostealer logs, immediately rotate any exposed credentials, and enforce conditional access policies that block authentication from anomalous geolocations, commercial VPN nodes, and Starlink IP ranges, which Handala operators have been observed using during Iran's internet blackout.

Network Defense and Monitoring: Block all known Handala-associated IOCs at the network boundary, including C2 IP 107[.]189[.]19[.]52, Telegram bot API traffic to api.telegram[.]org. Monitor for unauthorized deployment of legitimate tunneling tools such as NetBird, anomalous RDP lateral movement patterns, LSASS credential dumping via comsvcs.dll, ADRecon execution, and PowerShell-based bulk file deletion or disk encryption activity.

Data Protection and Recovery: Ensure all critical data, particularly government records, financial databases, and critical infrastructure configurations, is backed up to offline, segmented, and immutable storage. Wiper attacks render data permanently unrecoverable, making backup integrity the sole recovery path. Validate backup restoration procedures immediately and implement DLP controls to detect bulk data exfiltration patterns consistent with the 149 TB extraction claimed in this attack.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	
	T1110: Brute Force	
	T1566: Phishing	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Persistence	T1133: External Remote Services	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1484: Domain or Tenant Policy Modification	
Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
Discovery	T1087: Account Discovery	T1087.002: Domain Account
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
Command & Control	T1572: Protocol Tunneling	
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1485: Data Destruction	
	T1561: Disk Wipe	T1561.002: Disk Structure Wipe
	T1486: Data Encrypted for Impact	

Tactic	Technique	Sub-technique
Collection	T1005: Data from Local System	
	T1560: Archive Collected Data	
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.006: Web Services
	T1585: Establish Accounts	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	api.telegram[.]org, handala-hack[.]to, handala-redwanted[.]to, handala-alert[.]to, justicehomeland[.]org, karmabelow80[.]org, handala[.]to, handala-hack[.]ps, handala-hack[.]tw
IPv4	107[.]189[.]19[.]52, 82[.]25[.]35[.]25, 31[.]57[.]35[.]223, 146[.]185[.]219[.]235
Email	Admin[@]handala-alert[.]ps, Handala_Team[@]outlook[.]com
Telegram Channel	t.me/handala_hack26, t.me/handala_channel, t.me/HANDALA_INTEL
SHA256	454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567, 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8, fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2
MD5	3cb9dea916432ffb8784ac36d1f2d3cd, 5986ab04dd6b3d259935249741d3eff2
Telegram Bot Token	6428401585
Telegram Chat ID	6932028002

Note: All indicators are associated with Handala's broader 2026 campaign. No IOCs specific to the April 12 claimed attack have been publicly disclosed at the time of writing.

References

https://www.presstv.ir/Detail/2026/04/12/766723/Handala-hacking-group-cyberattack

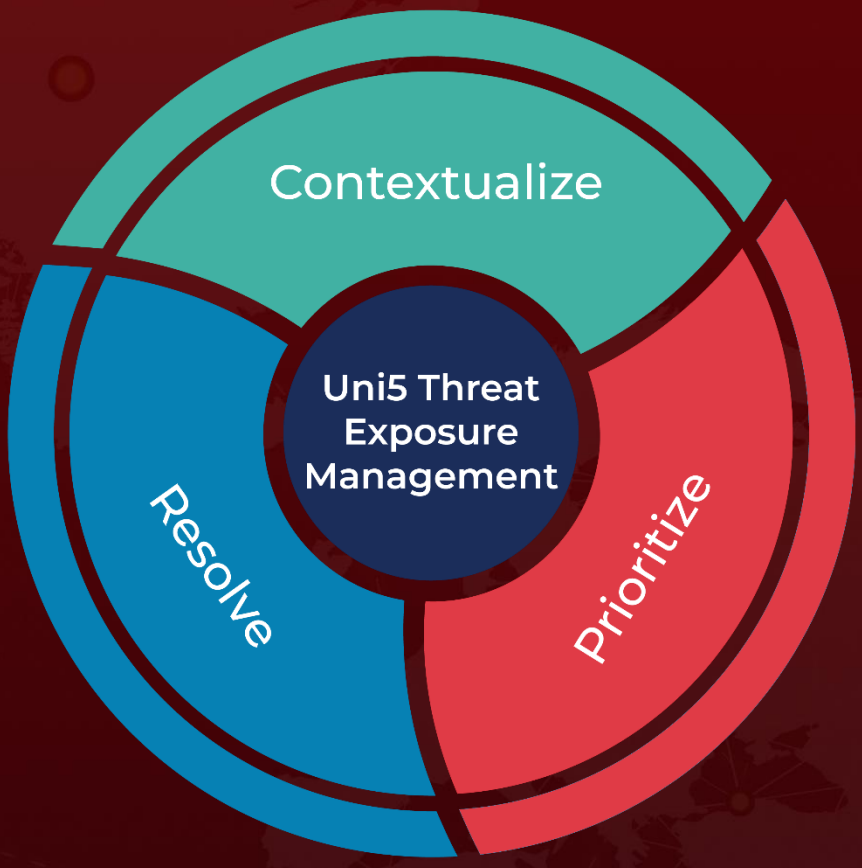
https://x.com/DailyDarkWeb/status/2043525184494182696

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

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

April 14, 2026 • 04:30 AM

More at www.hivepro.com