

HANDALA

Destructive persona presenting as a pro-Palestinian hacktivist collective since December 2023, widely assessed to be operated by Iran's Ministry of Intelligence and Security. Hijacks cloud identity admin accounts to remotely wipe corporate devices at scale, prioritising disruption and publicity over profit.

Void Manticore (Check Point)

Homeland Justice (related persona)

MOIS-linked (Iran)

RISK RATING

Critical

ACTIVE SINCE

2022

MOTIVATION

Political disruption, not profit

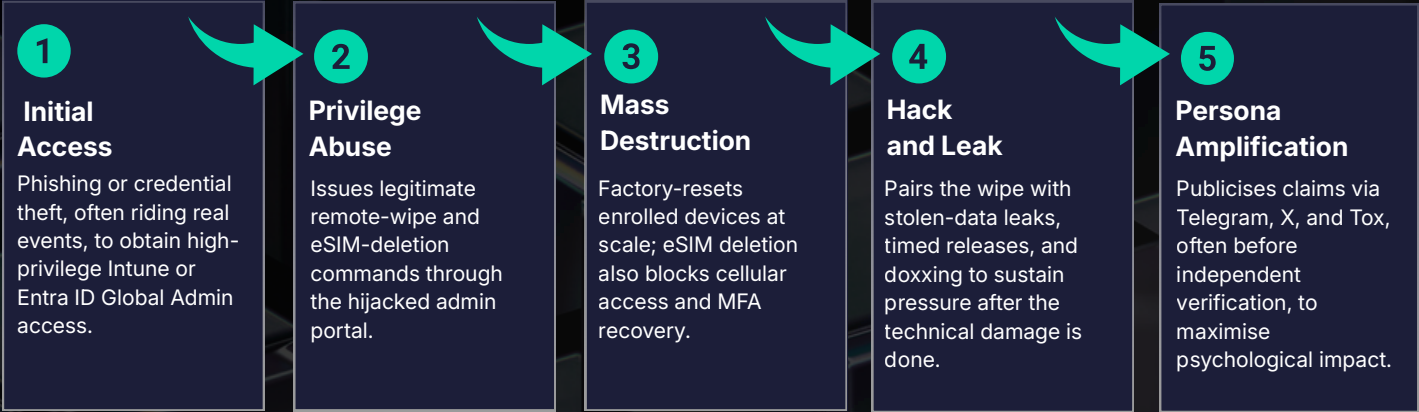
PRIMARY VECTOR

Hijacked Intune/Entra ID admin accounts

RANSOMWARE TIES

Iran MOIS (assessed, high confidence)

ATTACK CHAIN



MITRE ATT&CK MAPPING

ID	TECHNIQUE
T1566	Phishing (fake remediation tools, update lures)
T1078.004	Valid cloud accounts (hijacked Intune/Entra ID admin)
T1531	Account access removal (remote wipe via legitimate MDM commands)
T1485	Data destruction (wiper malware, mass factory reset)
T1491	Defacement (website defacement, leak-site claims)
T1102	Web service (Telegram Bot API for C2 and amplification)

SECTOR BY SECTOR Summary



Healthcare & MedTech

Struck its highest-impact target here, wiping tens of thousands of devices at a global medical device maker via hijacked cloud identity.



Government

A recurring target since the group's earliest attacks, headlined by the 2024 Synnovis breach that disrupted NHS pathology services.



Financial Services

Chosen for the client access these firms hold, extending impact well beyond the firm itself.

ORIGIN & EVOLUTION

Formed in December 2023 and tracked by Check Point as Void Manticore, widely assessed to be operated by Iran's Ministry of Intelligence and Security behind a pro-Palestinian hacktivist front. Sits inside a wider MOIS persona cluster alongside Homeland Justice and links to Scarred Manticore and MuddyWater, and reportedly lost its handler in the opening strikes of the 2026 Iran-Israel-US conflict.

THREAT LANDSCAPE CONTEXT

Sits inside a wider Iranian MOIS persona cluster alongside Homeland Justice, with links to Scarred Manticore and MuddyWater. The front persona (pro-Palestinian hacktivism) exists to obscure state attribution, not to represent the group's actual chain of command.

SIGNATURE TRADecraft

Phishes or steals credentials to reach Intune or Entra ID Global Admin access, then issues legitimate remote-wipe and eSIM-deletion commands through the hijacked portal rather than deploying custom malware. The eSIM deletion step is deliberate, blocking cellular access and MFA recovery simultaneously, and the group pairs technical damage with Telegram, X, and Tox amplification before independent verification.

ANALYST OUTLOOK

Handala's credibility problem, several major claims remain unverified or denied, may matter less than its demonstrated capability at Stryker. Expect continued targeting of cloud identity admin accounts as the group's most reliable path to large-scale disruption, regardless of how loudly it amplifies unrelated claims.

NOTABLE INCIDENTS

Stryker Corporation

March 2026

"Operation Epic Fury" wiped tens of thousands of enrolled devices at the medical device maker via hijacked Intune/Entra ID admin access, its highest-impact attack to date.

Kibbutz Ma'agan Michael

Claimed a ransomware-style attack stealing roughly 22GB of data and sent 5,000 fake SMS warnings to residents, pairing technical theft with a psychological disruption campaign.

Verifone

Claimed a breach of the payment terminal maker, which Verifone denied, illustrating the group's pattern of amplifying claims regardless of independent verification.