INTRUSIVE

THREAT ACTOR INTELLIGENCE PROFILE

Handala

MOSS Destructive Operations Unit, Void Manticore (Storm-0842)

Status Active **Last Updated** March 15, 2026 **Classification** TLP:CLEAR **Intelligence Confidence** HIGH

Intrusive Technologies

200,000+

Devices Remotely Wiped in Stryker Attack (March 11, 2026)

Iran's MOSS Destructive Operations Unit deploys Handala for maximum psychological impact and operational deniability.

Attribution & Identity

Background

Handala is the public persona of Void Manticore, an Iran-nexus MOSS-unit operated destructive operations group. Since its emergence in late 2023 with the Telegram channel and dark web leak site, Void Manticore has combined data theft, wiper deployment, and psychological operations, and staged coordinated influence campaigns through multiple personas, and supply chain compromise to maximize disruption and deniability. Void Manticore's most significant operation to date is the March 11, 2026 Stryker attack, in which Handala claimed to have remotely wiped 200,000 devices across 79 countries, affecting Stryker's Microsoft Intune environment. Attribution has been confirmed by Microsoft, Check Point Research, Palo Alto Networks, and others.

Known Aliases

Void Manticore · Handala Hatred · Storm-0842 · Banished Kitten · Red Sandstorm · Marigold Sandstorm · Pioneer Kitten · Scarlet Sandstorm · Cobalt Mirage · Cobalt Sandstorm · Emperor Dragonfly · Yellow Liderc · Yellow Maze · Yellow Garfield · Yellow Dragon · Yellow Cob · Yellow Banshee

Operational Status

Active — Confirmed operations March 2026

Motivation

Ideologically motivated (Iran-nexus). Secondary financial motivation through ransom demands. Psychological operations designed to erode trust in institutions and sow internal distrust.

Sponsor

MOSS Unit, Ministry of Intelligence and Security (MOIS), Islamic Republic of Iran

Victim Profile

Broad, opportunistic targeting across sectors. Recent focus on healthcare and manufacturing. Operations have impacted organizations in Israel, the United States, and the United Arab Emirates.

Capabilities

Data exfiltration · Wiper deployment · Supply chain compromise · Credential harvesting · Psychological operations · Influence campaigns · Persona management · Dark web leak site operations · Multi-platform messaging

Targeting Profile

Industries

Healthcare / Medical · Healthcare / Healthcare Services · Manufacturing · Government · Defense · Technology · Critical Infrastructure · Justice / Defense

Geographic Focus

Israel (primary) · Iran (secondary) · Albania · Saudi Arabia · UAE · Kuwait · Qatar · Bahrain · Thailand · Jordan · Italy · Turkey

Technologies

Microsoft Intune / MDM · Active Directory · Windows Endpoints · Linux Servers · MDM Administrative Consoles · SOC · EDR / AV

IoT / OT Systems

Access Control · Building Automation · Industrial Systems

Tactics, Techniques & Procedures

MITRE ATT&CK

T1486 · Data Encrypted for Impact · T1485 · Data Destruction · T1078 · Valid Accounts · T1566 · Phishing · T1059.001 · PowerShell · T1021.004 · SSH · T1105 · Ingress Tool Transfer · T1027 · Obfuscated Files or Information · T1036 · Masquerading · T1070.004 · File Deletion · T1082 · System Information Discovery · T1083 · File and Directory Discovery · T1018 · Remote System Discovery · T1657 · Financial Theft

Initial Access

Credential Harvesting · Phishing · Supply Chain Compromise · Exploitation of Public-Facing Applications

Persistence

Scheduled Tasks · Registry Run Keys · Valid Accounts · Web Shells

Defense Evasion

Obfuscated Files or Information · Masquerading · File Deletion · Log Tampering · Living-off-the-land Binaries

Credential Access

Credential Harvesting · Password Spraying · Brute Force · Stolen Credentials

Discovery

Network Scanning · Active Directory Enumeration · Remote System Discovery · Network Share Discovery

Lateral Movement

Remote Desktop Protocol · SMB / Admin Shares · Remote Management Tools · Stolen Credentials

Impact

Data Destruction · Data Encryption · Wiper Deployment · Ransom Demands · Service Disruption · Psychological Operations

Exfiltration

Data Staging · Encrypted Channels · Cloud Storage · Dark Web Leak Site

Operational Security

Persona Management · Dark Web Anonymity · Multi-platform Messaging · Deniability Through Proxy Actors

Tooling & Infrastructure

Malware Arsenal

Tool	Type	Description	First Seen
BitLocker Abuse	Ransomware	Custom wiper that corrupts the OS boot volume without encryption. PDF variant: CoreLocker. Linux variant: SwiftLocker. Windows variant: Chaos.	Mar 2026
Dr. Wiper	Data Wiper	Data Wiper Wiper (SHA256: 2f3f6f1b2d7c7 ...) for mass wiping. Leverages legitimate vendor tools.	Mar 2026
Lookback	Remote Access Trojan	Windows and Linux RAT. Persistence via Scheduled Task. Communicates over HTTPS.	Mar 2026
Fakeset	Backdoor Wiper	Fake Windows screen saver.	Mar 2026
Wipers	Wiper	Wiper family. Wiper Wiper Recent Wiper variant.	2024
Agrat	Wiper	Wiper family. Agrat Agrat Agrat