TIR-20260408 Iranian Threat Actor – Handala

4/8/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

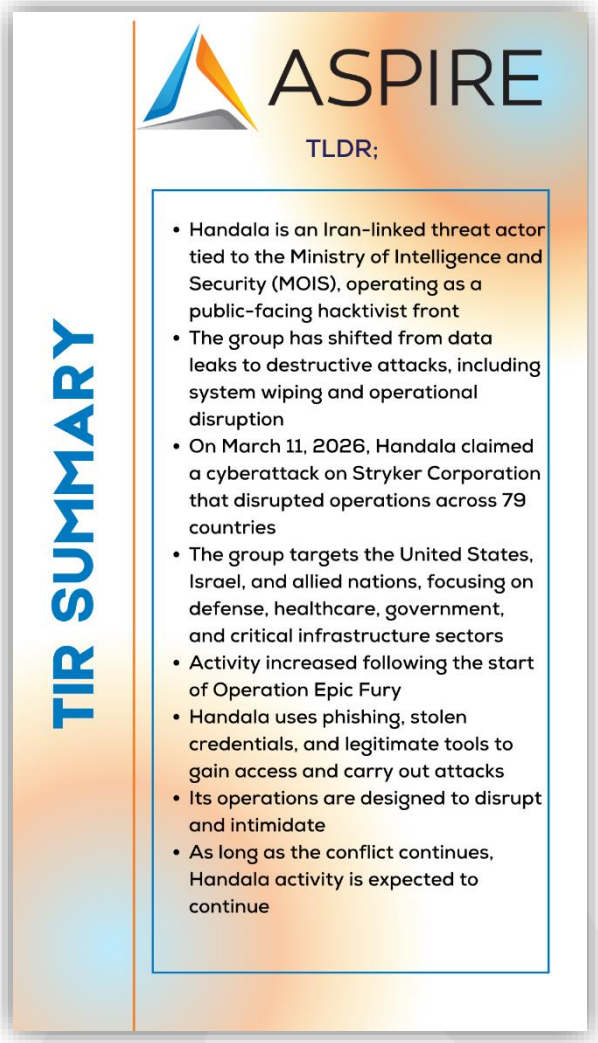
This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary



Handala is an Iranian threat actor that claims to be a hacktivist group, but that doesn't match what it actually does. The group has been linked to Iran's Ministry of Intelligence and Security (MOIS), and its operations line up with that. Handala appeared in late 2023 and didn't stay small for long. What started as data leaks has turned into destructive attacks. Activity has picked up since the conflict between the U.S. and Iran began.

In March 2026, the threat actor claimed responsibility for a destructive cyberattack against U.S.-based medical technology company Stryker. The incident caused widespread disruption across global operations and involved the wiping of thousands of systems within 79 countries. Earlier activity leaned more on data theft and leaks. Now they are wiping systems and disrupting operations. Around the same time, they expanded their targeting to include other U.S. organizations, Israeli defense, and sectors tied to government operations.

Handala's operations now combine cyberattacks with psychological pressure. The group combines phishing, credential theft, malware, and public data leaks with messaging meant to intensify impact. Some claims are exaggerated, but the real incidents are concerning. As the conflict continues, Handala has become one of the more active and visible Iranian threat actors.

Handala

As previously stated, Handala first appeared in December 2023, shortly after the October 7, 2023 Hamas attacks in Israel, where militants crossed into Israeli territory.

The group's early activity focused on Israeli targets, including data leaks and public exposure tied to the conflict.

They branded themselves as a pro-Palestinian hacktivist collective, using imagery tied to resistance movements to gain attention. That branding helped it grow quickly online, but investigations have since linked the group to Iran's Ministry of Intelligence and Security (MOIS). Handala is also tracked under names such as Handala Hack, Void Manticore and BANISHED KITTEN, placing it within a wider Iranian threat ecosystem.

The group operates in public, using Telegram and leak sites to claim attacks and share data. The Telegram channel also publishes information tied to geopolitical events. Unlike financially motivated groups, Handala focuses on disruption and visibility. Its campaigns often involve wiping systems, leaking data, or threatening targets in ways that draw attention.

Handala does not operate alone. Its activity aligns with other Iranian threat actors linked to MOIS. Groups such as MuddyWater and APT34 are often associated with gaining initial access through phishing or exploitation of known vulnerabilities. That access is then used or handed off to groups like Handala to carry out disruptive or destructive actions. One group gets access, then Handala uses it to carry out the attack.

One detail that stands out is how Handala blends real intrusions with exaggeration. Some claims overstate the level of access or impact. Others are backed by confirmed disruption. This creates uncertainty and draws attention to their operations. At the same time, the group has shown it can carry out real damage when given the opportunity.

Tactics, Techniques, and Procedures (TTPs)

Initial Access – How They Get In

Handala's operations often begin with phishing. Messages are tailored to the target and made to look legitimate. In some cases, attackers pretend to be support teams or trusted services. Victims are pushed to download files or click links that either drop malware or capture credentials. In other cases, access comes from already

compromised accounts. Once they're in, the focus shifts to holding that access. They use web shells, scheduled tasks, or valid accounts to stay in the environment without drawing attention.

Execution and Lateral Movement – What Happens After Access

After that, things move pretty quickly. The group uses scripting tools and built-in system processes to run commands and move through the network. They don't always rely on heavy malware. Earlier activity used multi-stage payloads with obfuscated scripts, AutoIT loaders, and even process injection before deploying a wiper. More recent activity shows a different approach. Instead of relying on malware, they use compromised administrative access to carry out actions directly. The Stryker attack is a good example. Once they had access, they were able to push destructive actions across the environment without needing a traditional payload.

Discovery, Credential Access, and Lateral Movement - How They Move and Prepare

Handala also takes time to understand the environment before doing anything. Activity has shown use of tools like ADRecon to map networks and identify high-value systems. Credential dumping and registry access have also been observed. This allows them to move through the environment and build control before triggering the final stage.

Known tools

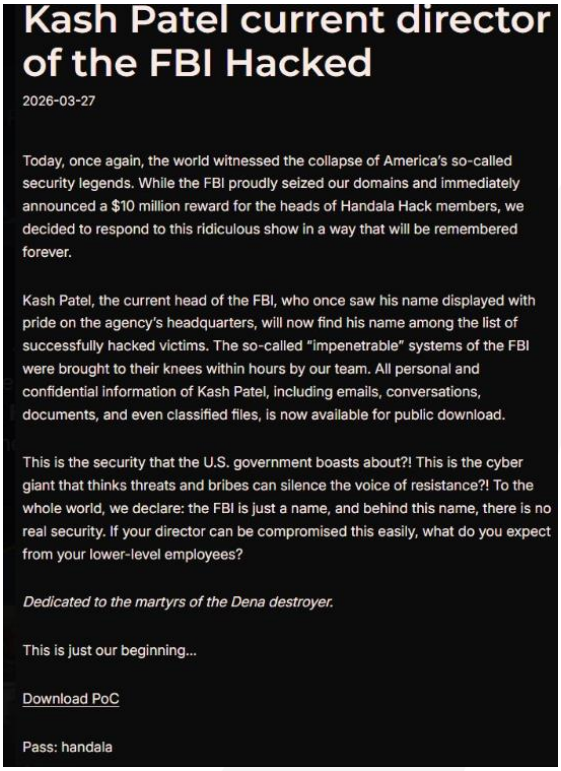
- Custom wiper malware (**BiBi Wiper, CI Wiper, Handala Wiper**)
- PowerShell and Windows command shell scripts
- AutoIT loaders and NSIS installers
- Telegram-based command-and-control
- Web shells for persistence
- ADRecon and credential harvesting tools
- Commercial tools such as infostealers in some campaigns

RECENT ATTACKS

Handala activity picked up in late February 2026 after Operation Epic Fury began. Their targets aligned with the conflict. They went after organizations tied to the United States, Israel, and allied countries.

On March 1, 2026, the threat actor began sending threatening messages to individuals in the United States and Canada, including journalists and members of the Israeli community. The messages referenced personal data and were meant to intimidate. Within days, the group began releasing information tied to individuals connected to the Israel Defense Forces (IDF), including names, contact details, and identification data. The leaks were shared through Telegram and public channels alongside direct threats.

Image 1: Handala Breaches Director of FBI Email



Stryker and The FBI

On March 11, 2026, Handala claimed responsibility for a destructive cyberattack against Stryker Corporation, a U.S.-based medical technology firm with operations in more than

60 countries and over 56,000 employees. The attack disrupted core business functions, including manufacturing lines, order processing systems, and internal logistics platforms. Employees across multiple regions lost access to corporate systems at the same time, and some departments reported that a large portion of endpoints were wiped. In certain environments, company-managed laptops, mobile devices, and remote systems running Windows were impacted. The group also claimed to have exfiltrated up to 50 terabytes of data, although the full scope of data loss has not been publicly confirmed. There was no ransom demand.

Israel's Mossad Intelligence Agency

Later in March, Handala claimed it had breached the email account of Tamir Pardo, the former Director of Israel's Mossad intelligence agency. The group released what it said were emails and personal files tied to the account. At the time of reporting, the claim could not be independently verified, and no official confirmation was provided by Israeli authorities. The incident followed a pattern seen in other Handala operations, where verified activity is mixed with claims that are difficult to validate.

Image 2: Alleged Breach of Former Israeli Intelligence Chief's Email

Source: X.com/DailyDarkWeb

The U.S. Department of Justice

In the days that followed, the Federal Bureau of Investigation (FBI) and the U.S. Department of Justice (DOJ) seized at least four domains associated with Handala that were used to publish claims and host leaked data. The takedown had limited impact, because, within 24 hours, the group restored its presence using new infrastructure and resumed posting. Later in March, Handala claimed it had accessed the personal Gmail account of Kash Patel, the Director of the FBI. They released a small set of files and images. The material appeared to be limited and, in some cases, outdated, but the claim gained attention due to the target and timing.

By early April 2026, the group shifted its focus back to Israeli defense-related targets. On April 2, Handala claimed it breached PSK Wind Technologies, a company tied to defense command systems. The group stated that it exfiltrated sensitive data and passed it to allied forces. Around the same time, it issued threats tied to major holidays, reinforcing the psychological element of its operations.

Connection to Operation Epic Fury

Handala acts as a visible cyber component of the conflict. Its activity aligns with strategic targets and timing tied to military actions. The group targets sectors that support government operations, defense, and critical infrastructure.

Its role is to:

- Disrupt operations tied to opposing governments
- Apply pressure through public exposure and threats
- Amplify messaging linked to the conflict
- Support broader Iranian cyber activity

Handala's operations also fit into a larger model. Other groups gain access. Handala follows with disruption. This structure allows Iran to combine intelligence gathering, cyberattack, and messaging into a coordinated effort.

Conclusion

Handala is not just a hacktivist group. It is a state-aligned cyber actor used to disrupt systems and influence perception during a time of conflict. The group has moved into destructive attacks and is using legitimate tools to do it. That makes it harder to catch and stop. As long as the conflict continues, its activity is expected to continue and expand.

Aspire's Recommendations

Handala's activity shows a clear pattern of going after access, then moving quickly to cause damage. In some cases, they don't even need malware. They use valid accounts and built-in tools to do the work. That makes detection more difficult. Organizations should assume that if access is gained, disruption will follow. The focus should be on limiting access and watching for misuse of legitimate tools.

- **Lock down admin access** – remove standing Global Admin roles, use just-in-time access, and enforce strong MFA (hardware-based where possible)
- **Watch for account misuse** – flag unusual logins, new locations, and admin activity in Microsoft 365, Entra ID, and Intune
- **Tighten phishing defenses** – block malicious attachments and links, and train users to question unexpected downloads or "urgent fixes"
- **Monitor script activity** – alert on PowerShell, command line, and AutoIT running in unusual ways or from odd locations
- **Control remote access** – limit RDP use and watch for lateral movement across systems
- **Secure MDM platforms** – restrict who can issue device wipe commands and monitor for mass actions across endpoints
- **Block and watch outbound traffic –** especially to services like Telegram or unknown external infrastructure

- **Protect credentials** – monitor for credential dumping and rotate access after any suspected compromise
- **Prepare for destruction** – keep offline backups, test recovery, and alert on large-scale file deletion or wipe behavior
- **Track the actor** – monitor Handala's public channels and claims for early warning of targeting

MITRE MAP

Initial Access	T1566.001 – Spear Phishing Attachment T1078.004 – Valid Accounts: Cloud Accounts T1078.003 – Spear Phishing via Service
Execution	T1059.001 – Command and Scripting Interpreter T1059.003 – Command and Scripting Interpreter: Windows Command Shell
Persistence	T1505.003 – Server Software Component: Web Shell
Privilege Escalation	T1068 – Exploitation for Privilege Escalation
Defense Evasion	T1027 – Obfuscated Files or Information T1497.003 – Time-Based Evasion T1055.012 – Process Hollowing
Credential Access	T1003 – OS Credential Dumping T1078 – Valid Accounts
Discovery	T1082 – System Information Discovery
Lateral Movement	T1021.001 – Remote Desktop Protocol
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols
Exfiltration	T1020 – Automated Exfiltration
Impact	T1485 – Data Destruction T1561.002 – Disk Structure Wipe T1490 – Inhibit System Recovery

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Domains

- handala-redwanted[.]to
- api[.]ra-backup[.]com
- media[.]megafilehost2[.]sbs
- hyperfilevault1[.]xyz

IP Addresses

- 82[.]25[.]35[.]25
- 31[.]57[.]35[.]223
- 107[.]189[.]19[.]52
- 146[.]185[.]219[.]235

Files / Hashes

- 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8
- 19001dd441e50233d7f0addb4fcd405a70ac3d5e310ff20b331d6f1a29c634f0
- 8316065c4536384611cbe7b6ba6a5f12f10db09949e66cb608c92ae8b69e4d67

Other

- Telegram-based command-and-control infrastructure
- Phishing attachments disguised as software updates

***Note**: This is a sample of Handala's most recent IOCs. Please see a complete list of IOCs here.*

SUPPORTING DOCUMENTATION

Handala Hack Signals Rise of Destructive Cyberattacks

Dark Web Profile: Handala Hack

Handala's Wiper: Threat Analysis and Detections | Splunk

Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran (Updated March 26)

Iranian MOIS Actors & the Cyber Crime Connection - Check Point Research

Pro-Iran Handala group breached Israeli defence contractor PSK Wind Technologies

Handala Group Tied to Iranian Hack-and-Leak Operations, FBI Reveals - Infosecurity Magazine

Iranian Use of Cybercriminal Tactics in Destructive Cyber Attacks: 2026 Updates

Iranian-linked actors are engaging in disruptive attacks | Tenable®

Experts point to increasing threat intelligence in light of Handala attacks

Stryker says manufacturing mostly restored after cyberattack | Reuters

Iran-linked hackers restore website after US seizes domains | Reuters

Government of Iran Cyber Actors Deploy Telegram C2 to Push Malware to Identified Targets

Analyzing Iran-nexus TTP evolution in 2026

Top 10 Routinely Exploited Vulnerabilities | CISA

Threat Actor | FortiGuard Labs

Office of Public Affairs | Justice Department Disrupts Iranian Cyber Enabled Psychological Operations | United States Department of Justice

The Iran War: What You Need to Know

Handala Hack: What We Know About the Rising Threat Actor

FHS - Handala IOCs - LevelBlue - Open Threat Exchange

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.