

Handala Hack Targets U.S. Troops with Doxxing Threats in Bahrain

 socradar.io/blog/handala-hack-us-doxxing-troop-bahrain

Ameer Owda

April 28, 2026



Apr 28, 2026

On Monday, U.S. service members stationed in Bahrain started getting WhatsApp messages on their personal phones telling them they were being watched and that missiles and drones were already aimed at them. The messages were signed by a group called “Handala” and included a link to the group’s website.

According to Stars and Stripes, [messages sent](#) to service members at Naval Support Activity Bahrain, which hosts U.S. Naval Forces Central Command. The messages came from what appeared to be a Bahraini phone number belonging to a local business, suggesting the number had been spoofed or compromised to send them.

“Your identities are fully known to our missile units, and every move you make is under our surveillance. Very soon, you will be targeted by our Shahed drones and Kheibar and Ghadeer missiles.” — Handala message sent to US troops, April 28, 2026

The following day, Handala posted on Telegram claiming it had [doxxed](#) personal details for 2,379 U.S. Marines stationed in the Persian Gulf.

Who Is Handala?

[Handala](#) or **Handala Hack** appeared on December 18, 2023, launching its Telegram and X accounts at the same time. The timing was not a coincidence. The group surfaced weeks after the October 7 Hamas attack, riding the wave of pro-Palestinian hacktivist activity that followed. Its name and logo borrow from the barefoot boy cartoon by Palestinian artist Naji al-Ali, a symbol of resistance that the group has plastered across everything from defaced websites to Telegram posts.

Early posts referenced Hamas directly, with the group calling itself a fighter within the movement before shifting to broader anti-Israel messaging. The branding has stayed consistent throughout, built to generate emotional resonance and credibility inside the pro-Palestinian hacktivist space.



[Handala Hack Dark Web Profile](#)

On attribution, the picture is now fairly clear. Check Point Research tracks the group as Void Manticore. Other firms use Storm-0842, BANISHED KITTEN, or Dune. Different names, same cluster. All reporting converges on **Ministry of Intelligence (MOIS)** affiliation, which separates Handala from IRGC-linked operations like CyberAv3ngers. That distinction matters operationally: MOIS runs intelligence and influence work, not purely military cyber operations.

Known aliases: Void Manticore · Storm-0842 · BANISHED KITTEN · Dune · Hanzalah Hacking Group

Why MOIS and not IRGC? The distinction matters. Iran’s Islamic Revolutionary Guard Corps (IRGC) runs its own cyber operations, like the group known as CyberAv3ngers. MOIS is Iran’s civilian intelligence ministry. Handala’s attribution to MOIS, specifically to a counter-terrorism division led by sanctioned deputy minister Yahya Hosseini Panjaki, tells analysts this is more of an intelligence and influence operation than a purely military one. The goal is psychological damage and data collection, not just technical disruption.

A Pattern of Escalation

The Bahrain messages are the latest step in a campaign that has been climbing in scale and audacity since early 2026. What started as attacks on Israeli infrastructure has moved into direct confrontation with U.S. institutions and military personnel.

In March 2026, Handala claimed a devastating attack on [Stryker Corporation](#), the medical device company that holds nearly **\$450 million in U.S. Department of Defense contracts**. The group said it **wiped more than 200,000 systems across 79 countries** by hijacking compromised Global Administrator credentials inside Microsoft Intune, then using legitimate admin tools to factory-reset everything without deploying traditional malware. Stryker filed an SEC disclosure confirming severe global disruption.

That same month, Handala breached the personal Gmail account of [FBI Director Kash Patel](#) and published a sample of more than 300 emails along with photographs. The FBI confirmed the breach but said the data was historical, mostly from 2010 to 2019, and contained no government information. The group was explicit about the motive: the U.S. had seized four Handala domains on March 19 and announced a **\$10 million reward for information about the group’s members**. The hack was retaliation.

Before targeting U.S. entities, Handala was primarily focused on Israel. It **hijacked the public address systems of more than 20 kindergartens** in January 2026 and played air raid sirens along with threatening messages in Arabic. It claimed to have exfiltrated nearly 200 gigabytes from the Soreq Nuclear Research Center, though Israel’s National Cyber Directorate assessed that as a psychological operation rather than a confirmed breach. The group also doxxed 28 Lockheed Martin engineers working on military projects in Israel and threatened their families.

How the Group Operates

Handala’s toolkit is a mix of custom malware and commercial tools, combined with social engineering that rides on real-world events. The most studied example is a phishing campaign from July 2024 that exploited the global CrowdStrike outage. The group sent emails to Israeli organizations with fake remediation tools. Victims who downloaded the archive got hit with a multi-stage chain that ended in a wiper payload erasing their files.

MITRE ATT&CK TTPs

Tactic	ID	Technique
Initial Access	T1566.001	Spear Phishing Attachment
Initial Access	T1566.003	Spear Phishing via SMS
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.010	AutoHotKey & AutoIT Scripting
Defense Evasion	T1055.012	Process Hollowing
Defense Evasion	T1218	System Binary Proxy Execution

Lateral Movement	T1021.001	Remote Desktop Protocol
Impact	T1561.002	Disk Structure Wipe
Impact	T1485	Data Destruction

The group's wiper [malware](#) family includes variants named BiBi Wiper, Hatef, Hamsa (Linux), CoolWipe, and ChillWipe. For command and control, Handala routes telemetry through the Telegram Bot API, a common technique because Telegram traffic blends in with normal network use and is harder to flag at the perimeter.

For the Stryker attack, the group used Microsoft Intune to push a factory reset to enrolled devices. When an attacker has cloud admin credentials, they can cause destruction through authorized channels that traditional endpoint security tools will not stop.

Indicators of Compromise

The following indicators are linked to Handala infrastructure and malware campaigns documented through early 2026.

Network Infrastructure

Type	Indicator	Note
IP	82.25.35[.]25	VPS attack infrastructure
IP	31.57.35[.]223	Command infrastructure
IP	107.189.19[.]52	Staging node
IP	146.185.219[.]235	VPN exit node
URL	hxxps://link[.]storjshare[.]io/.../crowdstrikesupport/update.zip	Payload hosting, phishing campaign

Malware Hashes

Type	Hash	Description
MD5	5986ab04dd6b3d259935249741d3eff2	Handala wiper
MD5	fca0910949d92dc3dd3dfcf0fb3d0408	AutoIT loader
MD5	2a5dd680c05b43d72365e8beb7e40088	Final wiper payload
MD5	755c0350038daefb29b888b6f8739e81	CrowdStrike.exe loader
SHA256	454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567	Handala.exe

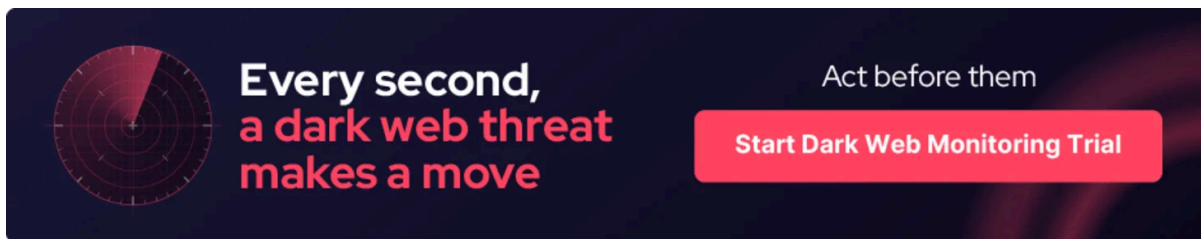
(Source: [SOCRadar Threat Actor Intelligence](#))

Bottom Line

Handala is not a group to dismiss because some of its claims turn out to be exaggerated. The personal data of thousands of U.S. military personnel being in the group's hands, real or not, is a serious enough claim to treat as credible until proven otherwise.

The group operates inside a larger Iranian intelligence structure, gets initial network access handed to it by more sophisticated actors, and has shown it can cause significant operational damage when it reaches its target. The shift toward directly threatening military personnel through personal communications channels shows it is willing to move beyond corporate or infrastructure targets and apply pressure to individuals and their families.

This kind of hybrid campaign has a clear goal: not just to compromise a network, but to make people feel unsafe in their own phones.



We value your privacy

We use cookies to improve your experience, analyze traffic, and personalize content. You can accept all or customize your preferences.

Manage your cookie preferences

Select which types of cookies you allow. You can update these at any time.

Essential Cookies

Required for the website to function properly, including security, login, and saving consent preferences

Analytics Cookies

Collect anonymous data to help us understand how visitors use the website and improve content and usability.

Functional Cookies

Enable enhanced features such as remembering preferences, interactive tools, and other functionality improvements.

Personalisation Cookies

Allow the site to tailor content and recommendations based on user interactions without collecting personal information.

Optimisation Cookies

Help us test and improve site speed, layout, and overall performance for a better user experience.

© 2026 [SOCRadar](#). All rights reserved.

Insights  4.9/5
★★★★★









