Handala Hack: Analysis of an Iran Linked Hacktivist Group's Operational Playbook

Tracking ID#: PCS-03-1426

Date: 14-03-2026

Disclaimer: This is a shared security advisory service; hence, it can be communicated to a single dedicated point of contact. We would highly appreciate it if you assigned them to your organisation's concerned asset/technology owner. Please use it as applicable to your environment

Date: 14-03-2026

Summary:

Handala Hack is an online persona linked to **Void Manticore** (also known as **Red Sandstorm** or **Banished Kitten**), a threat actor assessed to be affiliated with Iran's **Ministry of Intelligence and Security (MOIS)**. The group has conducted multiple destructive cyber operations combined with **"hack-and-leak" campaigns**, targeting organizations in countries such as **Israel, Albania, and the United States**. In addition to Handala, the actor has operated other personas including **Karma** and **Homeland Justice**, which have been used in separate but operationally related campaigns. Activity associated with these personas demonstrates highly similar techniques, tactics, and procedures (TTPs), including manual hands-on intrusion methods, the use of compromised credentials for initial access, and collaboration with other Iranian threat groups. The attackers have frequently targeted IT service providers and leveraged compromised VPN accounts to infiltrate networks, followed by reconnaissance, credential extraction, and privilege escalation activities. During intrusions, they have been observed extracting sensitive system data, dumping credentials from processes such as LSASS, enumerating Active Directory environments using tools like ADRecon, and using Remote Desktop Protocol (RDP) for lateral movement across compromised environments. The group has also used tools such as **NetBird**, a zero-trust networking platform, to establish internal connectivity between compromised systems and maintain operational control across multiple footholds within the network.

The destructive component of the campaign relies heavily on **wiper malware**, specifically the **Handala Wiper**, which is designed to cause large-scale system destruction and data loss. This custom malware is typically distributed across compromised networks using **Group Policy logon scripts** that trigger execution of a batch file responsible for launching the wiper components. The malware overwrites file contents across systems and performs destructive operations targeting the **Master Boot Record (MBR)** and other critical disk structures, preventing affected machines from booting normally and resulting in severe data corruption. In addition to the executable wiper, attackers deploy a **PowerShell-based wiping script** that recursively enumerates and deletes files within user directories, significantly amplifying the level of destruction. This script has been observed placing a propaganda image named *handala.gif* across system drives as a marker of the attack. To further increase operational damage, the attackers also attempt to encrypt system drives using legitimate software such as **VeraCrypt**, making recovery even more difficult. In some cases, the operators manually delete files or even entire virtual machines directly from virtualization platforms after gaining access through RDP. By combining multiple wiping methods, encryption techniques, and manual destructive actions simultaneously, the attackers aim to maximize operational disruption, causing widespread system outages, permanent data loss, and significant damage to targeted environments.

Target:

Applicable to all users.

Mitigation Recommendations:

- Recommended to block all the IOCs mentioned in the attached excel sheet.
- Recommended to enforce multi-factor authentication, especially for remote access and privileged accounts.
- 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 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.

S.NO	Indicators of Compromise	Type
1	[##5986ab04dd6b3d259935249741d3eff2##]	MD5
2	[##3cb9dea916432ffb8784ac36d1f2d3cd##]	
3	[##3236facc7a30df4ba4e57fddfba41ec5##]	
4	[##3dfb151d082df7937b01e2bb6030fe4a##]	
5	[##e035c858c1969cffc1a4978b86e90a30##]	
6	82[.]25[.]35[.]25	IP
7	31[.]57[.]35[.]223	
8	107[.]189[.]19[.]52	
9	146[.]185[.]219[.]235	

References:

"Handala Hack" - Unveiling Group's Modus Operandi - Check Point Research