13 March 2026

TLP: WHITE

INTEL471

EMERGING THREATS

Handala Threat Group

The Handala threat group has recently emerged as a disruptive Iranian-aligned cyber operation that has conducted destructive and espionage-oriented campaigns against organizations across multiple regions. Recent reporting highlights activity targeting entities in Israel and Western countries, including a high-profile attack against a medtech company, where systems were reportedly disrupted as part of a destructive cyber campaign. The threat group has also been linked to operations impacting institutions such as schools and infrastructure targets, demonstrating an evolution from traditional hacktivist messaging into more operationally damaging attacks. Over the past several months, Handala has been observed demonstrating an increased ability to coordinate attacks that combine data theft, destructive malware, and public messaging campaigns, allowing them to cause disruption while amplifying political narratives tied to regional tensions.

THREAT SUMMARY

The Handala threat group has recently emerged as a disruptive Iranian-aligned cyber operation that has conducted destructive and espionage-oriented campaigns against organizations across multiple regions. Recent reporting highlights activity targeting entities in Israel and Western countries, including a high-profile attack against a medtech company, where systems were reportedly disrupted as part of a destructive cyber campaign. The threat group has also been linked to operations impacting institutions such as schools and infrastructure targets, demonstrating an evolution from traditional hacktivist messaging into more operationally damaging attacks. Over the past several months, Handala has been observed demonstrating an increased ability to coordinate attacks that combine data theft, destructive malware, and public messaging campaigns, allowing them to cause disruption while amplifying political narratives tied to regional tensions.

THREAT SYNOPSIS

At the outset, Handala intrusion activity has been observed leveraging compromised credentials and exploiting exposed services to gain initial access into victim environments. Researchers note that once access is obtained, the attackers conduct reconnaissance within the network to identify high value systems and administrative infrastructure that can be leveraged to expand their access. In reported campaigns and attacks, the group moved quickly from initial foothold to disruptive actions that impaired operational systems. This activity indicates a campaign structure focused on rapid operational impact rather than prolonged stealth access, which differs from many traditional espionage-focused intrusions.

The group's operations have included the use of destructive malware designed to wipe systems rather than encrypt them, which allows the attackers to permanently damage systems and disrupt recovery efforts. These wiper attacks (observed to utilize custom wipers like BiBi Wiper and Hatef Wiper for example) remove or overwrite critical files and system components, rendering machines inoperable and requiring full system restoration or rebuilding. By combining credential access, internal reconnaissance, and destructive malware deployment, Handala is able to compromise enterprise environments and trigger widespread outages across targeted infrastructure. This approach allows the attackers to disrupt healthcare technology platforms, educational systems, and other high availability environments, which significantly amplifies the operational impact of their campaigns.

HANDALA THREAT GROUP HUNT COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('6de05211-fe94-400f-8fce-fc19686e8557'),touched:!t)

RELATED HUNT PACKAGES

File Writes with Single Character File Names and Execution Extension - Potential Malware Staging

https://hunter.cyborgsecurity.io/research/hunt-package/f20c5f61-c68a-446d-95c4-e227d3ac1078

WMIC Windows Internal Discovery and Enumeration

https://hunter.cyborgsecurity.io/research/hunt-package/bc0fd59c-4217-46a7-a167-764727118567

Timeout Delayed Execution

https://hunter.cyborgsecurity.io/research/hunt-package/350e41b2-b2b7-410b-85cc-74a3536a5950

MSI File Installation from Suspicious Location

https://hunter.cyborgsecurity.io/research/hunt-package/61b3d776-20c3-4804-9543-0c806c00d868

Potential Use of Findstr or Find with Tasklist

https://hunter.cyborgsecurity.io/research/hunt-package/ee9bb6c4-378e-498e-ad04-fe469da49046

Suspicious bcdedit Activity - Potential Ransomware

https://hunter.cyborgsecurity.io/research/hunt-package/8a4f0a60-2b55-4dfd-8788-8691e11e1ca1

Ping Count Activity

https://hunter.cyborgsecurity.io/research/hunt-package/9600b6f0-8f7e-4b96-a5d3-9938624c80d2

Microsoft Defender Antivirus Disabled via Registry Key Manipulation

https://hunter.cyborgsecurity.io/research/hunt-package/81d218e6-0c53-42c4-9275-4aac0eef5bc6

Shadow Copies Deletion Using Operating Systems Utilities

https://hunter.cyborgsecurity.io/research/hunt-package/2e3e9910-70c1-4822-804a-ee9919b0c419

Logical Disk Enumeration - WMIC

https://hunter.cyborgsecurity.io/research/hunt-package/38804d75-006e-47a3-bb79-84de142f6e05

MITRE CONTEXT

- MITRE Technique IDs:
    - T1074.001
    - T1016.001
    - T1059
    - T1105
    - T1497.003
    - T1562.001
    - T1047
    - T1490
    - T1218.005
    - T1016
    - T1518.001
    - T1083
- MITRE Technique Names:
    - System Network Configuration Discovery
    - Inhibit System Recovery
    - Ingress Tool Transfer
    - Command and Scripting Interpreter
    - Security Software Discovery
    - Disable or Modify Tools
    - Mshta
    - Windows Management Instrumentation
    - Time Based Evasion
    - Internet Connection Discovery
    - Local Data Staging
    - File and Directory Discover
- MITRE Tactic Names:
    - Defense Evasion
    - Discovery
    - Execution
    - Impact
    - Collection
    - Command and Control

REFERENCES

1. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
2. https://www.securityweek.com/medtech-giant-stryker-crippled-by-iran-linked-hacker-attack/
3. https://www.infosecurity-magazine.com/news/iran-massive-wiper-attack-medtech/
4. https://www.theguardian.com/world/2026/mar/12/iran-group-hack-medical-company-minab-school
5. https://blog.checkpoint.com/research/what-defenders-need-to-know-about-irans-cyber-capabilities/