TIR-20260311 Iranian Threat Actor Banished Kitten

3/11/2026

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)

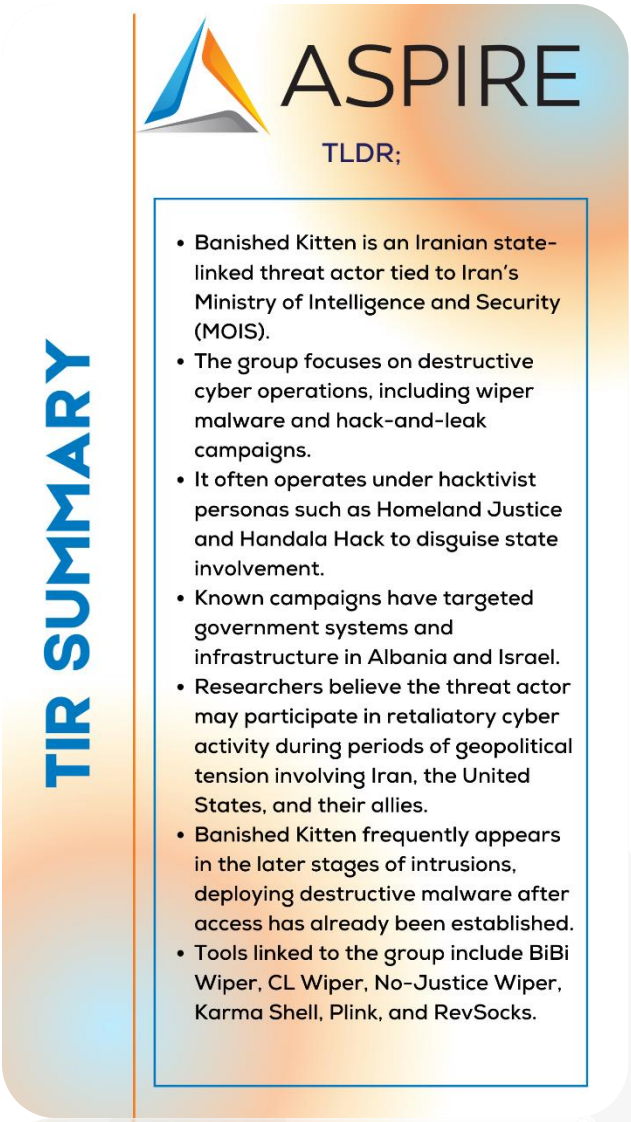
Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary

Rising geopolitical tensions between Iran, the United States, and Israel have increased the likelihood of cyber retaliation from Iranian state-linked threat actors. Iran has turned to cyber operations as a way to confront rivals like the United States and Israel without escalating into direct conflict. Through these operations, Iranian intelligence and military organizations conduct espionage and disruptive campaigns designed to pressure adversaries.

Researchers have linked Banished Kitten to destructive cyberattacks against government networks and critical infrastructure, along with hack-and-leak campaigns intended to shape political narratives. Unlike financially motivated cybercriminal groups, Banished Kitten appears to attack based on geopolitical objectives, frequently targeting countries and organizations viewed as hostile to the Iranian government.



According to intelligence reporting, Banished Kitten could be involved in Iranian cyber retaliation during periods of heightened geopolitical tension. The threat actor has drawn increasing attention from security researchers as relations between Iran, the United States, and their allies remain strained. Security researchers have highlighted Banished Kitten for using destructive malware alongside psychological and influence campaigns. The combination allows the threat actor to extend the impact of its cyber operations beyond technical disruption.

BANISHED KITTEN

Banished Kitten is an Iranian state-linked cyber threat actor believed to operate on behalf of Iran's Ministry of Intelligence and Security (MOIS). The group is tracked under several aliases including Void Manticore, Storm-0842, Red Sandstorm, Homeland Justice, and Handala Hack. Banished Kitten was first spotted in 2022 following destructive cyberattacks targeting Albanian government infrastructure.

The threat actor is typically classified as an advanced persistent threat actor (APT) rather than a financially motivated cybercriminal group. Banished Kitten's operations focus on disruption and psychological impact rather than financial gain. The threat actor has deployed destructive wiper malware and carried out hack-and-leak campaigns that expose stolen data to embarrass or pressure victims.

Banished Kitten's targeting historically aligns with Iranian geopolitical interests. Victims have included government institutions, media organizations, defense-related personnel, and critical infrastructure operators. Known campaigns have targeted organizations in Albania and Israel, though analysts believe the group may expand operations to Western nations aligned with those countries.

The threat actor often operates under hacktivist personas that frame its activity as ideological cyber activism. These personas include Homeland Justice and the Handala Hack Team. Security researchers believe the identities are used to make the attacks appear independent while masking the threat actor's ties to the Iranian government.

One of the most distinctive characteristics of Banished Kitten is its focus on psychological warfare. The group frequently publishes stolen or allegedly stolen information online in order to amplify the political impact of its attacks. In some cases, attackers release both legitimate and fabricated data to increase confusion and generate media attention around their operations.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

Banished Kitten operations often combine destructive cyberattacks with influence campaigns. The threat actor has deployed wiper malware designed to erase systems and disrupt networks. In several campaigns, the threat actor released stolen or alleged data online after the attack. The tactic is used to increase the political impact of the intrusion.

Researchers have also observed Banished Kitten gaining access to networks through phishing campaigns and the exploitation of vulnerable internet-facing systems. In some cases, attackers compromised enterprise servers and deployed web shells to maintain access. These web shells allowed the threat actor to run commands on compromised systems and stage additional tools used during the intrusion.

Once inside a network, the attackers prepare systems for destructive activity. The final stage of these campaigns typically involves deploying wiper malware that permanently deletes files and renders affected machines unusable. This approach allows the threat actor to cause operational disruption while reinforcing the broader messaging surrounding the attack.

Known Tools and Malware

- BiBi Wiper
- CL Wiper
- No-Justice Wiper (LowEraser)
- Karma Shell web shell
- Mimikatz credential harvesting tool
- Native Windows command utilities used for file deletion and system manipulation

Known Vulnerabilities Exploited

- CVE-2019-0604 – Microsoft SharePoint Remote Code Execution vulnerability used to gain initial access to enterprise environments

The Final Stage - Banished Kitten's Operational Role

Security researchers have observed Banished Kitten appearing in the later stages of some Iranian cyber attacks. In these cases, another Iranian threat actor gains access to the network first and conducts espionage or reconnaissance. Banished Kitten then moves in after that access is established.

The threat actor focuses on disruption rather than intelligence collection. Investigations have linked this pattern to coordination within Iran's Ministry of Intelligence and Security (MOIS). Researchers believe the approach allows Iranian operations to shift from intelligence gathering to destructive activity once strategic objectives change.

Banished Kitten does not appear to depend on complex software exploits to get inside victim networks. Most investigations show the threat actor entering through phishing or stolen credentials. In some cases, attackers also take advantage of poorly secured internet-facing systems. Once inside, the focus shifts to maintaining access and moving through the environment until systems are positioned for destructive malware deployment. The group's objective is disruption and public impact rather than long-term espionage.

Recent Attacks

July 2022 – Albanian Government Infrastructure

In July 2022, Iranian threat actors operating under the Homeland Justice persona launched a destructive cyberattack against Albanian government networks. The attack disrupted multiple government services and destroyed data across national infrastructure systems. Investigations later attributed the operation to Iranian state-linked actors associated with Banished Kitten.

September 2022 – Albanian Border Control Systems

In September 2022, the same threat actor conducted another cyberattack targeting Albania's border control infrastructure. The attack disrupted border management

systems and government services. The campaign was widely interpreted as retaliation for Albania hosting members of the Iranian opposition group Mujahedin-e Khalq (MEK).

October 2023 – Wiper Attacks on Israeli Organizations

Following the escalation of conflict in the Middle East in October 2023, Banished Kitten conducted destructive cyber operations against Israeli organizations. These attacks utilized BiBi Wiper malware targeting both Windows and Linux systems. The malware was designed to destroy files and disrupt operations within the victim networks.

December 2025 – Political Influence Operation Targeting Israeli Officials

In late 2025, the Handala Hack persona linked to Banished Kitten claimed responsibility for compromising the mobile device of a senior Israeli government official. Attackers released phone numbers and alleged internal documents online in an effort to generate political controversy and undermine public trust in Israeli leadership.

Why Banished Kitten is a Threat

Banished Kitten is widely believed to operate on behalf of Iran's Ministry of Intelligence and Security (MOIS), one of the country's primary intelligence agencies responsible for cyber operations abroad. Researchers note that the group's targeting patterns closely align with Iranian geopolitical objectives, including retaliation against countries perceived as threats to the Iranian government.

Banished Kitten presents itself as a hacktivist group, but researchers do not see it that way. Investigators point to the threat actor's infrastructure, resources, and consistent targeting patterns. Those indicators line up more closely with a state-backed operation than with cyber activism. Researchers have also found operational overlap between Banished Kitten and other Iranian threat clusters (APT34, Void Manticore, and Scarred Manticore). Researchers say the activity points to coordination with other Iranian threat actors.

Security researchers view Banished Kitten as dangerous because of its focus on destructive attacks. The threat actor has used wiper malware in several operations. That type of malware is designed to permanently erase data and cripple systems. In periods of geopolitical tension, analysts warn that these capabilities could be directed at government networks or critical infrastructure.

Key Threat Factors

- State-sponsored backing from Iran's Ministry of Intelligence and Security
- History of destructive cyberattacks using wiper malware
- Ability to combine cyberattacks with influence operations
- Use of hacktivist personas to obscure attribution
- Targeting of government infrastructure and politically sensitive organizations

Conclusion

Banished Kitten is a threat actor researchers continue to watch as tensions rise between Iran and Western countries. The group has shown it is willing to damage systems rather than quietly collect intelligence, which can make its operations far more disruptive. Researchers at CrowdStrike and Check Point have linked similar Iranian operations to state-backed cyber activity carried out under hacktivist groups. If tensions between Iran and the United States continue to escalate, groups like Banished Kitten could be used to target government networks or critical infrastructure.

Aspire's Recommendations

Organizations operating in sectors frequently targeted by Iranian cyber actors should implement defensive measures tailored to Banished Kitten's known tradecraft and attack patterns. The following recommendations focus on mitigating the specific tactics and tools observed in campaigns attributed to the group.

- Harden SharePoint environments and ensure patches addressing vulnerabilities such as CVE-2019-0604 are applied, as Iranian actors have exploited SharePoint servers for initial access in destructive campaigns.
- Monitor for web shell activity, particularly indicators associated with the Karma Shell web shell, which has been used by Iranian operators to maintain persistence on compromised servers.
- Deploy behavioral detection for wiper malware activity, including mass file deletion, abnormal disk writes, and scripts attempting to overwrite system files, common behaviors associated with BiBi Wiper, CL Wiper, and No-Justice Wiper.
- Restrict administrative access and monitor RDP usage across critical systems, as Iranian operators frequently move laterally using legitimate administrative protocols after initial compromise.
- Implement strict email filtering and user awareness training focused on phishing campaigns impersonating technology vendors or government organizations, a technique repeatedly used in Iranian influence and destructive operations.
- Monitor credential dumping activity, particularly suspicious execution of tools such as Mimikatz, which attackers use to escalate privileges and move laterally within compromised environments.

MITRE MAP

Initial Access	T1566.001 – Phishing: Spear-phishing Attachment T1190 – Exploit Public Facing Application
Credential Access	T1003.001 – OS Credential Dumping: LSASS Memory
Persistence	T1505.003 – Server Software Component: Web Shell
Lateral Movement	T1021.001 – Remote Services: Remote Desktop Protocol
Impact	T1485 – Data Destruction T1561 – Disk Structure Wipe

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)

Malware Families

These destructive malware families have been directly attributed to Banished Kitten / Void Manticore campaigns.

- BiBi Wiper – destructive wiper malware used against Israeli targets
- CL Wiper – destructive malware designed to erase system data
- No-Justice Wiper (LowEraser) – destructive malware used in Homeland Justice operations against Albania

Web Shell

- Karma Shell – web shell used in Iranian intrusion campaigns associated with this threat cluster

Tools Observed in Campaigns

The following tools have been observed in operations attributed to the threat actor or referenced in technical analyses of the campaigns.

- Plink – SSH tunneling tool used for remote command execution
- RevSocks – reverse SOCKS proxy tool used for tunneling traffic
- Windows 2000 Resource Kit utilities – administrative utilities used during post-compromise activity

SUPPORTING DOCUMENTATION

Iran-linked hacker group doxes journalists and amplifies leaked information through AI chatbots

Iran's Cyber Retaliation Clock Is Ticking: What CISOs Need to Know Right Now

Operation Epic Fury and Iranian Cyber Counterattacks | Tenable®

Iranian Hackers Target Israel to Sway Public Opinion in Hamas Conflict - Infosecurity Magazine

Iranian APTs Dress Up as Hacktivists for Disruption, Influence Ops

Iran-Linked UNC1549 Hackers Target Middle East Aerospace & Defense Sectors

Void Manticore Combines Data Theft And Wiper Malware

FalconFeeds.io Blog | Latest Cyber Threat Intelligence & Security Insights

A Threat Actor Landscape Assessment of ICS/OT Targeting in the 2026 Iran-US Conflict AND THE SCALE OF THE RISK | CloudSEK

Iran's Cyber Retaliation Clock Is Ticking: What CISOs Need to Know Right Now

The Iranian Cyber Capability

Iran-linked hackers claim attack on Albania's Institute of Statistics | The Record from Recorded Future News

HomeLand Justice - Threat Group Cards: A Threat Actor Encyclopedia

Bad Karma, No Justice: Void Manticore Destructive Activities in Israel - Check Point Research

Banished Kitten Adversary Profile | CrowdStrike

Iranian Threat Actors: What Defenders Need to Know

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.