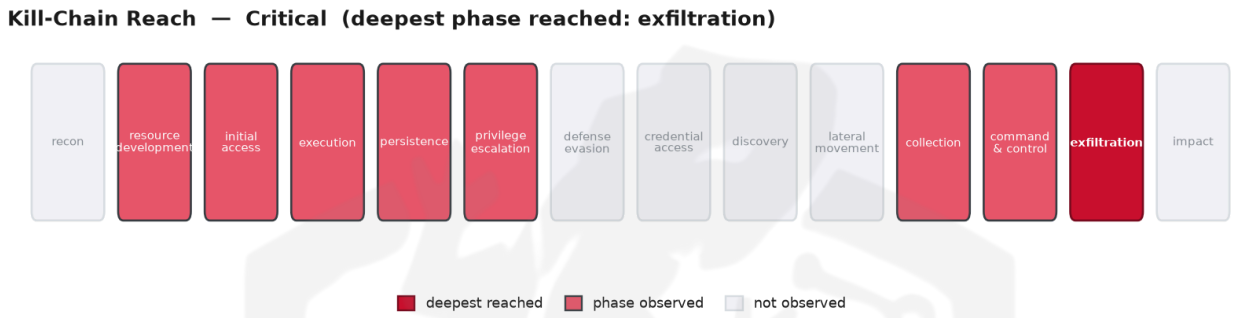
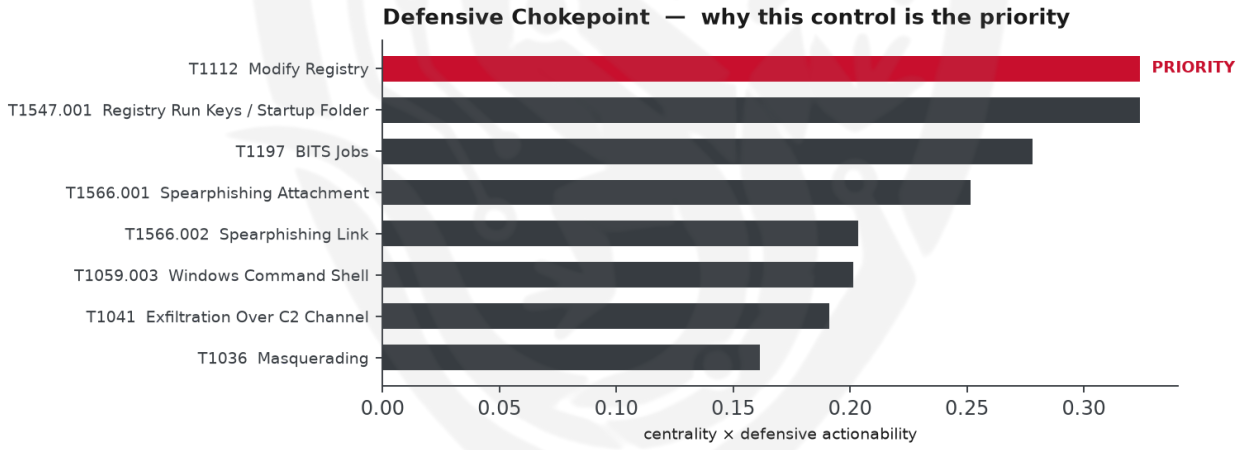
# THREAT REPORT: TAG-182 DISSEMINATES MARKIRAT SURVEILLANCE TOOL

## Visual Summary




How far down the attack chain this campaign reached; deepest phase in crimson.




The control that most disrupts the attack (priority in crimson).

## Summary

The source attributes this activity to TAG-182, who has been disseminating the MarkiRAT surveillance tool, targeting entities in the Islamic Republic of Iran. The threat actor utilizes various techniques to gain access and maintain persistence on compromised systems. Priority should be given to monitoring sensitive registry keys for modification to prevent further malicious activity. The lack of specific sector information and central CVE details highlights the need for vigilance across multiple areas.

## Threat Overview

TAG-182, the attributed threat actor, employs the MarkiRAT malware family, among others like FurBall, DCHSpy, and BouldSpy, to target Iranian entities. The victimology indicates a focus on the Islamic

Republic of Iran, though specific sectors remain unspecified. The malware's capabilities, including screen capture and file exfiltration, pose significant risks to compromised systems.

## Attack Chain and Priority Control

The observed techniques form a complex attack chain, starting with initial access through spearphishing links or attachments, followed by the use of malicious files, and then establishing persistence through registry modifications. The priority technique identified is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To mitigate this, the recommended priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

## Infrastructure and Corroboration

The command and control infrastructure associated with this activity is hosted by providers such as GWY IT Pty Ltd and Andishe Sabz Khazar Co. P.J.S., as observed in third-party enrichment data. However, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

---

## Technical Appendix

*Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.*

### Observed Techniques (ATT&CK, expert-tagged by source)

- T1113 Screen Capture
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1583.001 Domains
- T1036 Masquerading
- T1112 Modify Registry
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1197 BITS Jobs
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1564.001 Hidden Files and Directories

### Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3412).
- Operational risk: Critical (score 0.968, reaches exfiltration).

## Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5839; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

| Historical Profile | Behavioural Overlap |
|---|---|
| LazyScripter | 0.5839 |
| Nomadic Octopus | 0.5785 |
| Windshift | 0.5658 |
| Dark Caracal | 0.538 |
| Transparent Tribe | 0.5335 |

## Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

## Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

| Type | Indicator | Context |
|---|---|---|
| IP | 46[.]30[.]191[.]123 | AbuseIPDB 0% (NL) · AS199959 GWY IT Pty Ltd |
| IP | 89[.]144[.]145[.]237 | AbuseIPDB 0% (IR) · AS39308 Andishe Sabz Khazar Co. P.J.S. |
| Domain | yemplayer[.]site | |
| Domain | min[.]comi-site[.]website | |
| Domain | microsoft[.]comi-site[.]website | |
| Domain | comesignt[.]website | |

| Type | Indicator | Context |
|---|---|---|
| Domain | min[.]come-site[.]website | |
| Domain | google[.]comisignin[.]online | |
| Domain | accountes[.]google[.]comesignt[.]website | |
| Domain | accounts[.]google[.]comisignin[.]online | |
| Domain | microsoft[.]come-site[.]website | |
| Domain | comi-site[.]website | |
| Domain | com-accounts[.]website | |
| Domain | come-signin[.]quest | |
| Domain | comisignin[.]online | |
| Domain | pis2ray[.]online | |
| Domain | admin[.]google[.]com-accounts[.]website | |
| Domain | admin[.]instagram[.]com-accounts[.]website | |
| Domain | c[.]pis2ray[.]online | |
| Domain | google[.]com-accounts[.]website | |
| Domain | google[.]com-signin[.]site | |
| Domain | host[.]comview[.]website | |

| Type | Indicator | Context |
|---|---|---|
| Domain | microsoft[.]comesite[.]website | |
| Domain | microsoft[.]comview[.]website | |
| Domain | microsoft[.]pis2ray[.]online | |
| Domain | min[.]comview[.]website | |
| Domain | min[.]pis2ray[.]online | |
| Domain | ns1[.]com-signin[.]site | |
| Domain | ns2[.]com-signin[.]site | |
| Domain | prx[.]pis2ray[.]online | |
| Domain | svpn[.]pis2ray[.]online | |
| Domain | vpn[.]pis2ray[.]online | |
| Domain | webmail[.]com-accounts[.]website | |
| Domain | webmail[.]facebook[.]com-accounts[.]website | |
| Domain | webmail[.]google[.]com-accounts[.]website | |
| Domain | webmail[.]instagram[.]com-accounts[.]website | |
| Domain | www[.]facebook[.]com-accounts[.]website | |
| Domain | www[.]google[.]com-accounts[.]website | |

| Type | Indicator | Context |
|---|---|---|
| Domain | www[.]instagram[.]com-accounts[.]website | |
| Domain | www[.]pis2ray[.]online | |

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.