



Brief

Iranian APT Groups Increasing Cyber Espionage Activity

B-2023-10-25a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Military, Government, Crisis, Geopolitical,
Threat Actor Targeting

October 25, 2023

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 18:00 PM (EDT) on October 18, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Iranian APT Groups Increasing Cyber Espionage Activity

Executive Summary

Iranian state-affiliated advanced persistent threat (APT) groups APT33 and APT34 have conducted an increasing number of targeted cyberattacks in recent months. These APTs will likely continue to play a key role in the Israel-Hamas war to support Iran and Hamas' mis- and disinformation campaigns and other cyber espionage and intelligence operations. The groups have a standing mandate to conduct cyber espionage on behalf of the Iran regime, and it is very likely these groups will mirror or exceed Iran's operational pace vis-à-vis the conflicts in which Iran finds itself with its near-peer and regional geopolitical rivals.

Iranian APT Landscape

The Islamic Republic of Iran (Iran) employs many competent APT groups or clusters that often overlap in personnel, tools, techniques, and targets; however, APT33 (aka Refined Kitten) and APT34 (aka OilRig, Helix Kitten) have reportedly been responsible for several recent cyber espionage attacks. Iran's national security and intelligence are handled primarily by two organizations: the Ministry of Intelligence and Security (MOIS), which has an external and internal security mandate, and the Iranian Revolutionary Guards Corps (IRGC), which has an overlap in responsibilities but with the added duty of exporting the

Iranian revolution.¹ The difference may appear arbitrary, but the two organizations have separate chains of command and operational and targeting priorities that can vary. ZeroFox assesses APT34 to be primarily a MOIS asset, whereas APT33 is assessed to be an intelligence arm of the IRGC. Although ZeroFox lacks direct insight into the nuances of which group is responsible for any given attack, we have medium confidence that the two groups can be distinguished based on their tooling preferences and targeting priorities.

Recent Attacks

APT33 and APT34 have been conducting cyber espionage against priority targets of the Iranian regime since at least 2012. The two groups have demonstrated the capacity and motivation to conduct attacks worldwide in line with Iran's strategic priorities. However, in the course of examining a recent uptick in attacks, ZeroFox noted APT33 and APT 34 most frequently target the United States, Israel, the United Arab Emirates (UAE), and the Kingdom of Saudi Arabia (KSA), as each state is of high interest to the Iranian regime. Below are several examples of recent, high-profile activity by APT33 and APT34:

- In **September 2023**, a sophisticated phishing campaign impersonating marketing services company Ganjavi Global Marketing Services (GGMS) was attributed to APT34.² The APT group targeted organizations using a variant of its newly developed SideTwist trojan to obtain long-term control over victim hosts. The SideTwist trojan variant collects victim host information to generate a unique ID before communicating with a command and control (C2) server. Notably, the IP address for the C2 server in this APT34 campaign belonged to the U.S. Department of Defense (DoD) Network Information Center (NIC) in Columbus, Ohio. This IP choice suggests that APT34 may have utilized this operation for testing before activating a different, unidentified C2 address in subsequent operations. While the full scope and goals of the campaign are unknown, it is possible the C2 server's placement in the DoD NIC was an indicator of plans to conduct attacks or collection against the DoD.

¹ [hXXps://iranprimer.usip\[.\]org/blog/2023/feb/17/explainer-how-iran%E2%80%99s-intelligence-agencies-work](https://iranprimer.usip.gov/blog/2023/feb/17/explainer-how-iran%E2%80%99s-intelligence-agencies-work)

² [hXXps://gbhackers\[.\]com/hacker-group-disguised-as-marketing/](https://gbhackers[.]com/hacker-group-disguised-as-marketing/)

- Also in **September 2023**, APT34 conducted a phishing campaign that deployed cyber espionage software on victims' systems in the Middle East.³ The customized malware, named "Menorah," verifies the targeted computer, reads and uploads files from the victim's computer, and enables persistent access for further malware placement and exploitation. The phishing lure contained pricing information in Saudi riyals, indicating the victim was based in KSA. Menorah and the SideTwist backdoor have many similarities, implying that APT34 is constantly refining its tactics, techniques, and procedures (TTPs) based on the target and the operational environment. The TTPs in this attack are indicative of APT34 (and APT33 by extension) tailoring operations for cyber espionage to maintain limited visibility and persistence and to obscure its involvement. The group's use of common TTPs is not a sign of simplicity; rather, it should be viewed as a means to maintain a low profile and operational security.
- In **May 2023**, APT34-linked attacks employed a new PowerShell-based malware designated as "PowerExchange" to steal user credentials and install backdoors on Microsoft Exchange servers of a UAE government organization.⁴ The backdoor allowed its operators to execute commands that deliver additional malicious payloads on infected servers and exfiltrate files. The similarities between PowerExchange and the TriFive malware used to backdoor Kuwaiti government organizations' systems led to attributing these attacks to APT34. The group also used phishing emails as an initial infection vector in its attacks and reportedly breached other Emirati organizations.
- Beginning in **February 2023** and continuing throughout the year, APT33 conducted a sweeping campaign in the United States and worldwide that included the targeting and extraction of sensitive information from a small number of victims in the U.S. defense, satellite, and pharmaceutical industries.⁵ The campaign

³ [hXXps://www.trendmicro\[.\]com/en_us/research/23/i/apt34-deploys-phishing-attack-with-new-malware.html](https://www.trendmicro.com/en_us/research/23/i/apt34-deploys-phishing-attack-with-new-malware.html)

⁴

[hXXps://www.bleepingcomputer\[.\]com/news/security/new-powerexchange-malware-backdoors-microsoft-exchange-servers/](https://www.bleepingcomputer.com/news/security/new-powerexchange-malware-backdoors-microsoft-exchange-servers/)

⁵

[hXXps://www.bleepingcomputer\[.\]com/news/security/iranian-hackers-breach-defense-orgs-in-password-spray-attacks/](https://www.bleepingcomputer.com/news/security/iranian-hackers-breach-defense-orgs-in-password-spray-attacks/)

initiated with password spraying, a noisy technique meant to identify initial network vectors. The attackers then conducted follow-on exploitation of the networks, targeting unpatched Confluence and ManageEngine appliances that were exposed online. Following successful attacks, APT33 used the open-source security frameworks AzureHound or Roadtools to conduct reconnaissance across the victims' Azure Active Directory and harvest data from their cloud environments. Additionally, APT33 created new Azure subscriptions in victims' active directory instances, used stolen Azure credentials, or took advantage of Azure Arc for persistence to control on-premises devices in the victims' network. APT33 also sideloaded DLLs to execute malicious payloads, deployed AnyDesk for persistence, used Golden SAML attack techniques for lateral movement, and employed a tunneling tool called EagleRelay to send malicious traffic to its C2 infrastructure. These TTPs are consistent with a cyber espionage campaign, and the cloud-based methods used in this campaign are noticeably more advanced than those previously employed by APT33.

| Analyst Commentary

Iranian state-affiliated APT groups APT33 and APT34 have conducted an increasing number of targeted cyberattacks in recent months. These groups are likely to continue to play a key role in the Israel-Hamas war to support Iran and Hamas' mis- and disinformation campaigns and other cyber espionage and intelligence operations.

- As with other APT activity, these groups often go undetected on a victim's network by design to maintain persistence commensurate with their intelligence mission.
- Judging from a recent analysis of Iranian APT activity, there has been a year-over-year increase in attacks; at least 24 attacks were detected between June 2022 and July 2023, compared to attacks in the single digits from the same reporting period the prior year.⁶
- APT33 and APT34 focus on sectors that provide access to sensitive information. This includes the telecommunications, government, defense, energy, and financial sectors historically. Both groups are adept at identifying soft targets that offer

⁶ <https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/>
Single digits prior reporting period. Tracks with activity we've reported.

vectors to sensitive targets. Sectors with direct or indirect involvement in Iranian priority areas, such as the Israel-Hamas conflict, should remain vigilant as potential targets of opportunity.

The increase in Iran's cyber espionage activity is probably linked to a number of regime priorities, including espionage aimed at near-peer and regional geopolitical rivals, preserving domestic stability, and mis- and disinformation campaigns to besmirch adversaries and shore up regional regime support. Iran relies upon APT groups to collect sensitive intelligence information; as such, these groups' activities are likely reflective of Iran's strategic intelligence requirements. For example, over the past year, Iran separately maintained high-level efforts at rapprochement with the Saudi and U.S. governments. Increased collection activity against those two countries—as well as that of the UAE, which is integral to both diplomatic engagements—would likely be a requirement to support Iran's diplomatic activities. There are indications Iran played a key role in supporting Hamas' multi-pronged attack against Israel. However, there has been no indication that the increased cyber espionage was tied to this event.

APT33 and APT34, along with other Iranian APTs, will almost certainly play a role in any conflict Iran has an interest in shaping. Iran has a strained relationship with the UAE due to maritime territorial disputes, among other issues. Iran has a long-standing conflict with KSA, which it sees as its primary regional rival despite recent diplomatic efforts to open relations. This discord has resulted in a number of proxy conflicts throughout the region and has many layers. Iran sees Israel as its mortal and primary enemy and has long backed anti-Israeli terrorist organizations such as Hamas and Hezbollah. The United States is Iran's enemy—both as the ideological counter to Iran's regime and due to it being inextricably linked with Israel from Iran's perspective. Any escalation in this web of alliances or individual hot spots will see Iranian APT activity utilized. APT 33 and APT34 focus primarily on cyber espionage. However, they have also been used as an operational arm of Iran in concert with foreign policy activity. For example, APT34 is believed to have conducted a destructive attack against Albania's digital infrastructure in July 2022.⁷ The attack was assessed to be in retaliation for Albania's support of an Iranian separatist group.

⁷ [hXXps://www.jpost\[.\]com/international/article-716572](https://www.jpost.com/international/article-716572)

ZeroFox researchers have built out a collection to assess network activity associated with Iranian APT groups, with sub-collections dedicated to APT33 and APT34. This collection contains known indicators of compromise (IOCs) associated with both groups and allows for the integration of vulnerability data. A review of this information provided a small number of IOCs with associated vulnerabilities. That information, along with a compilation of IOCs, can be requested via established contact procedures.

Recommendations

Iranian APT activity overall represents a significant threat to the United States and its allies. APT33 and APT34 are adept at gaining target access through the supply chain or vulnerable third parties. This places a broad range of organizations adjacent to government, defense, or high-priority sectors at risk. The following are recommendations for at-risk organizations:

- Implement next-generation email security and filtering.
- Conduct social engineering awareness and training for relevant stakeholders.
- Ensure vulnerabilities associated with lure file types, such as Microsoft Excel-associated CVE-2017-11882, are patched.
- Patch vulnerabilities on public, internet-facing assets.
- Assess software supply chain risks, especially with the use of third-party software and open-source software.
- Implement next-generation firewalls and configure strong policies to block known malicious or suspicious domains.
- Leverage ScoutPrime collections in conjunction with ZeroFox analysts to proactively monitor traffic associated with Iranian APT assets.

While Iranian APT groups present a threat, there is also an opportunity to identify Iran's national priorities. APT33 and APT34 are strategic assets of the Iranian regime. Monitoring their activity will offer insights into their operational directives—and Iran's operational priorities by extension.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%