ultraviolet

THREAT ADVISORY SPECIAL REPORT

Iranian Threat Actor Group Update

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
March 1, 2026
TLP:GREEN

Executive Snapshot

Iranian state backed cyber operations have evolved into a disciplined, repeatable capability that prioritizes identity compromise, social engineering, and abuse of trusted enterprise services over technically complex exploitation. Groups such as APT33, APT35, and APT42 consistently demonstrate that effective access can be achieved at scale through password spraying, phishing, and humanocentric tradecraft, followed by persistence in cloud and SaaS control planes. These operations are designed to blend into normal administrative activity, enabling long term intelligence collection and providing Iran with the option to escalate from espionage to disruption during periods of geopolitical tension.

For security leadership, the strategic risk is not confined to malware or perimeter defenses, but to the integrity of identity systems, email platforms, and the human layer that surrounds them. Iranian threat actors routinely exploit gaps in authentication hygiene, monitoring, and response readiness, particularly in environments where MFA protections are weak or cloud activity lacks sufficient visibility. Reducing exposure to these threat actors requires a shift toward identity-first security, rigorous monitoring of cloud control planes, and proactive defenses against social engineering campaigns that target both organizational and personal accounts.

UltraViolet Cyber Threat Intelligence and Detection Engineering (TIDE) Team suggests the following defensive actions:

- Review and confirm incident response plans are updated with response team roles and contact information is up to date. Additional review of recoverability capabilities should be assessed and any identified gaps addressed.
- Enforce phishing-resistant MFA and strong identity governance across all privileged and high-risk accounts, with rapid detection and containment of anomalous MFA changes or token issuance.
- Detect and disrupt credential access at scale by monitoring for password spraying, impossible travel, and abnormal authentication patterns across VPN, cloud, and SaaS services.
- Harden cloud and email control planes by auditing administrative privileges, monitoring mailbox rules and forwarding, and tightly controlling the use of remote management and admin tools.
- Expand security awareness and coverage beyond the perimeter, accounting for personal email accounts, external collaboration platforms, and social engineering risks targeting executives, administrators, and other high-value technical personnel.
- Raise awareness within Tier 1 support staff and help desks to positively identify anyone asking for a password change or MFA change. Ensure your user community knows to positively ID anyone posing as support staff or help desk; Instruct users to call back to a known support staff or help desk number before taking any actions.

TIDE Team Analysis

Iran's offensive cyber capability has matured into a durable instrument of state power used to support intelligence collection, regional influence, and strategic signaling during periods of geopolitical tension. Rather than prioritizing zero-day exploitation or highly novel malware at scale, Iranian operators tend to focus on repeatable access techniques such as credential theft, password spraying, and social engineering, followed by persistence through widely deployed enterprise services. This approach lowers operational cost, increases technical persistence, and allows campaigns to scale quietly across thousands of targets before defenders recognize an attack is underway.

A defining feature of Iran's current cyber doctrine is its emphasis on identity and cloud control planes as the primary attack surface. Iranian actors routinely target email, identity providers, and SaaS platforms, exploiting weak authentication hygiene, MFA fatigue, and permissive administrative controls. Once credentials are obtained, operators frequently modify MFA registrations, abuse trusted tokens, and rely on legitimate administrative tooling to blend into normal enterprise activity. This makes detection difficult and often delays response until sensitive data has already been accessed or exfiltrated.

APT33 exemplifies Iran's shift toward large-scale access operations paired with selective, high-impact follow-on actions. Recent campaigns attributed to APT33 demonstrate extensive password spraying against thousands of organizations, with targeting concentrated in aerospace, defense, satellite communications, pharmaceuticals, and energy. In successful intrusions, APT33 has leveraged commercial remote management tools and cloud-native techniques rather than custom malware, allowing the group to operate under the guise of normal IT administration while conducting internal reconnaissance and data collection. APT33's tradecraft also highlights Iran's continued ability to escalate from espionage to disruption when strategic conditions warrant it. Historically, the group has been linked to destructive tooling and wiper-style capabilities, and its past campaigns show that access initially gained for intelligence purposes can be repurposed rapidly. For critical infrastructure and defense-adjacent organizations, this reinforces the risk that even low-noise intrusions may represent latent destructive potential during periods of heightened geopolitical conflict.

The primary lessons from APT33 activity are operational rather than technical. Identity hardening, early detection of password spray behavior, and strict governance over remote management tools significantly reduce exposure. Organizations that lack visibility into authentication patterns, token issuance, and administrative changes remain particularly vulnerable, as APT33 consistently exploits gaps in identity monitoring rather than endpoint security weaknesses.

APT35 and APT42 represent a complementary branch of Iranian cyber capability focused on human-centric targeting and long-term intelligence collection. These groups are best known for sophisticated social engineering campaigns aimed at policymakers, academics, journalists, activists, and individuals connected to sensitive decision-making processes. Their operations often begin outside traditional corporate networks, leveraging personal email accounts, professional outreach, and trusted interpersonal channels to establish credibility before attempting credential theft or malware delivery.

These actors demonstrate a high degree of adaptability, tailoring lures and payloads to specific targets and platforms. Campaigns frequently involve prolonged engagement to build trust, followed by selective delivery of tooling designed to harvest credentials, capture communications, or maintain persistent access. In some cases, operators have demonstrated cross-platform capability, adjusting tooling based on whether a target uses Windows or macOS, underscoring the intelligence-driven nature of their operations.

APT42, in particular, illustrates Iran's willingness to operate at the intersection of cyber operations, counterintelligence, and influence. Public reporting has linked the group to sustained efforts targeting political campaigns, NGOs, and regional security personnel, as well as long-running deception operations that masquerade as legitimate businesses or recruitment firms. These campaigns emphasize patience and realism, favoring durable access and insight over rapid exploitation.

From an executive perspective, the activity of APT35 and APT42 reinforces that organizational risk increasingly extends beyond managed endpoints and corporate networks. Personal email accounts, cloud collaboration platforms, and informal professional communication channels can serve as entry points or intelligence collection vectors. Security programs that focus exclusively on perimeter defenses or malware detection will miss a substantial portion of this threat activity.

Collectively, APT33, APT35, and APT42 highlight a coherent Iranian cyber strategy centered on identity compromise, social engineering, and exploitation of trusted systems rather than technical novelty. For security leadership, the strategic takeaway is clear: identity security must be treated as a Tier-1 control. Phishing-resistant MFA, rapid containment of compromised identities, rigorous monitoring of cloud and email configurations, and well-rehearsed response procedures for identity-based intrusions are essential to countering Iran's most effective cyber offensive capabilities.

Iranian Threat Actor Groups

APT33 (aka Elfin, HOLMIUM, Peach Sandstorm)

APT33 is a long-running Iranian state-aligned cyber threat group assessed to have been active since at least 2013. The group is widely associated with Iran's strategic intelligence and military objectives and has historically demonstrated a dual mandate: long-term cyber espionage and the ability to transition to disruptive or destructive operations when required. Historical reporting has highlighted APT33's interest in reconnaissance and credential theft within industrial and defense environments, followed by the development and use of bespoke malware. Over time, the group's tradecraft has evolved away from custom implants toward identity compromise, cloud abuse, and the use of legitimate administrative tooling, reflecting a maturation toward stealth, scale, and operational resilience.

APT33's targeting has been notably consistent and strategically aligned with sectors that support national security, industrial capability, and technological advantage. Primary industry verticals include aerospace and aviation, defense contractors, energy and petrochemical firms, satellite and communications providers, pharmaceuticals, and—at times—OT/ICS-adjacent environments. Public reporting has linked APT33 activity to campaigns against U.S., European, and Middle Eastern organizations, including aerospace manufacturers, satellite operators, and energy-sector entities. Historically, the group has been associated with intrusion sets involving credential harvesting, reconnaissance of industrial environments, and in some cases the deployment or staging of destructive tooling, reinforcing concerns that access gained during espionage operations may later be repurposed for operational impact.

From a technical standpoint, APT33 is best characterized by its aggressive pursuit of initial access at scale combined with selective post-compromise activity against high-value targets. The group routinely employs password spraying and brute-force authentication attempts, leverages phishing to harvest credentials, abuses remote management tools for persistence, and targets cloud identity infrastructure to maintain durable access. Its tradecraft emphasizes living-off-the-land techniques and trusted services, allowing APT33 to blend into enterprise environments.

Primary MITRE ATT&CK techniques associated with APT33:
T1078 – Valid Accounts
T1110.003 – Password Spraying
T1566 – Phishing
T1059 – Command and Scripting Interpreter
T1021 – Remote Services
T1105 – Ingress Tool Transfer
T1087 – Account Discovery
T1046 – Network Service Discovery
T1098 – Account Manipulation
T1550.003 – Use of Web Session Cookie (Token Abuse / Cloud Access)

APT33 Historical victims and Targeting

Historical reporting from FireEye (2017) described sustained intrusions against U.S., Saudi Arabian, and South Korean organizations, particularly those tied to aviation and energy supply chains. While FireEye did not publicly name victims, the reporting emphasized long-term access and reconnaissance consistent with strategic intelligence collection rather than opportunistic compromise.

In 2019, Symantec documented APT33 exploitation attempts against a Saudi Arabian chemical-sector organization,

including the use of a malicious WinRAR exploit. The victim organization was not publicly named, but Symantec confirmed the sector and geography. Around the same period, additional reporting described APT33-linked phishing campaigns using fake job postings targeting U.S.-based government and private-sector personnel, again without naming specific organizations due to disclosure constraints.

In 2023, Microsoft publicly attributed large-scale password spraying and follow-on intrusions to APT33, impacting organizations in the defense, satellite, and pharmaceutical sectors. Microsoft confirmed that at least one victim organization's Active Directory Federation Services (AD FS) infrastructure was compromised, enabling forged SAML authentication into Microsoft 365. As with earlier reporting, Microsoft did not disclose victim names, but the confirmation of cloud identity compromise marked a significant evolution in APT33's operational maturity.

Across all major public reporting, specific company names are rarely disclosed, but the victimology consistently centers on organizations whose compromise would yield industrial insight, defense intelligence, or strategic access, rather than direct financial gain. APT33 has historically combined custom malware, commodity remote access tools, and legitimate enterprise software, adjusting its tooling based on operational requirements and detection pressure. Below are known malware families leveraged by APT33:

DROPSHOT (observed publicly by 2017): a custom dropper used to install secondary payloads on compromised systems. DROPSHOT's primary role was reliable delivery and execution of follow-on implants.

TURNEDUP (2017): a custom backdoor delivered by DROPSHOT that enabled remote command execution, file operations, and system control, supporting long-term espionage.

POWERTON (first observed ~2018): a PowerShell-based backdoor designed for in-memory execution, persistence, and command-and-control using native Windows scripting, reducing reliance on disk-based malware.

StoneDrill / SHAPESHIFT lineage (discussed 2017–2019): tooling associated with destructive or wiper-capable behavior; while not deployed in every intrusion, its linkage to APT33 established the group's capacity for escalation beyond espionage.

APT33 has also made extensive use of commodity remote access trojans, particularly in the 2018–2019 timeframe, including Remcos, NanoCore, DarkComet, QuasarRAT, and Pupy. These tools provide standard RAT functionality—remote command execution, keystroke logging, screen capture, and file transfer—and are widely available, allowing APT33 to blend into generic malware activity and complicate attribution.

For credential access and privilege escalation, APT33 has used well-known post-exploitation utilities such as Mimikatz and LaZagne, which extract plaintext credentials, hashes, and stored secrets from compromised systems. These tools enable lateral movement and expansion of access without requiring custom exploit development.

In more recent campaigns (2023), APT33 demonstrated a marked shift toward living-off-the-land and identity abuse. Microsoft confirmed the use of AnyDesk, a legitimate commercial remote desktop and management tool, to maintain persistent access while appearing consistent with normal IT administration. Most significantly, APT33 executed a Golden SAML–style attack, stealing or abusing AD FS token-signing keys to forge trusted authentication tokens. This technique allows attackers to impersonate any user in a federated environment, bypass MFA, and access cloud services such as Microsoft 365 without deploying malware on endpoints.

APT35 (aka Charming Kitten, Phosphorus, TA453)

APT35 is a prominent Iranian state-aligned cyber threat group that has been active since at least 2014 and is best known for its intensive use of social engineering and identity-focused tradecraft. Unlike groups that emphasize broad infrastructure compromise, APT35's historical mission centers on intelligence collection against individuals and organizations tied to policy, security, and strategic influence. The group has demonstrated a high tolerance for long-duration operations, often engaging targets over weeks or months to establish credibility before attempting credential theft or selective malware deployment. Over time, APT35 has refined its approach to reduce operational noise, relying less on bespoke malware and more on cloud account compromise, impersonation, and living-off-the-land techniques.

APT35's targeting profile is strongly humanocentric and aligned with intelligence priorities rather than purely economic or industrial objectives. Key industry and organizational verticals include government agencies, foreign policy and defense think tanks, academia, media organizations, journalists, activists, dissidents, and political figures. The group has also targeted technology and security professionals when they provide indirect access to higher-value information or networks. Public reporting has linked APT35 campaigns to credential harvesting operations against personal and corporate email accounts, as well as follow-on access to collaboration platforms and document repositories used by research and policy communities across the United States, Europe, and the Middle East.

Technically, APT35 excels at exploiting trust relationships rather than infrastructure weaknesses. The group frequently impersonates academics, journalists, conference organizers, or reputable institutions to initiate contact, then delivers phishing links or weaponized documents tailored to the target's interests and operating environment. Once access is achieved, APT35 focuses on email collection, credential reuse, cloud persistence, and quiet lateral movement rather than rapid exploitation. In some operations, the group has demonstrated cross-platform capability, adjusting payloads or delivery mechanisms based on whether the target uses Windows or macOS, reinforcing its intelligence-driven, operator-led tradecraft.

Primary MITRE ATT&CK techniques associated with APT35:
T1566 – Phishing
T1589 – Gather Victim Identity Information
T1598 – Phishing for Information
T1078 – Valid Accounts
T1110 – Brute Force / Credential Access
T1059 – Command and Scripting Interpreter
T1204 – User Execution
T1087 – Account Discovery
T1098 – Account Manipulation
T1114 – Email Collection

APT35 Historical victims and targeting

Public reporting consistently links APT35 activity to campaigns against government agencies, foreign policy and defense think tanks, academic institutions, journalists, activists, dissidents, and political figures, particularly those with insight into Middle Eastern security, nuclear policy, or international relations.

Between 2016 and 2019, multiple vendors documented APT35 spear-phishing campaigns targeting U.S. and European academics, journalists, and policy experts, frequently using impersonation of conference organizers, media outlets, or trusted research institutions. Victim organizations were generally not named, but reporting confirmed compromises of personal email accounts and cloud services used by individuals affiliated with major think tanks and

universities.

From 2020 through 2024, Proofpoint and others tracked APT35 conducting increasingly sophisticated social-engineering campaigns against think tanks, NGOs, religious figures, and regional security experts. In several cases, the actor engaged targets over extended periods using benign outreach (e.g., interview or podcast invitations) before attempting credential harvesting or malware delivery. These campaigns were geographically focused on the United States, Europe, and the Middle East, and while some targeted institutions were indirectly identified by role or affiliation, specific organization names were rarely disclosed publicly.

APT35 has also been linked to operations against technology and security professionals when those individuals provided indirect access to sensitive information or networks, reinforcing the group's focus on human access paths rather than enterprise perimeter compromise.

Tooling and software used by APT35

APT35's tooling reflects its human-centric and intelligence-driven mission, combining credential harvesting infrastructure, lightweight malware, and legitimate cloud services rather than heavy exploitation frameworks.

A defining feature of APT35 operations is extensive use of phishing frameworks and spoofed login portals, often designed to mimic Google, Microsoft, or other widely used email and collaboration platforms. These portals are used to harvest credentials and MFA tokens directly from victims, enabling account takeover without endpoint compromise. Once credentials are obtained, APT35 frequently relies on valid account access to read email, download documents, and monitor communications over time.

When malware is deployed, APT35 has historically favored custom or semi-custom backdoors designed for persistence and command execution rather than automated exploitation. Examples documented in public reporting include PowerShell-based backdoors that allow in-memory execution, tasking, and data exfiltration while minimizing on-disk artifacts. These implants are typically delivered after an operator confirms target value, reinforcing APT35's selective approach.

In several campaigns, APT35 has demonstrated cross-platform awareness, adjusting delivery mechanisms based on the victim's operating system. Reporting from the early 2020s describes the group experimenting with macOS-compatible malware, alongside Windows-focused tooling, to maintain access to researchers and analysts using non-Windows systems. This flexibility differentiates APT35 from groups that rely on homogeneous enterprise environments.

APT35 also makes heavy use of legitimate cloud and email features for persistence and collection. This includes creation of email forwarding rules, abuse of OAuth tokens or application access, and long-term monitoring of inboxes and cloud-stored documents. These techniques allow the actor to maintain visibility into a target's communications without repeated re-infection or noisy network traffic.

APT42 (aka TA456, Mint Sandstorm)

APT42 is an Iranian state-aligned cyber threat group that has emerged as a distinct operational cluster over the past several years, reflecting Iran's increasing emphasis on cloud-centric and identity-focused intelligence collection. The group is assessed to be closely aligned with Iranian intelligence objectives and is best characterized by its sustained focus on credential theft, account takeover, and long-term surveillance rather than malware-heavy intrusions. APT42 operations often blur the line between traditional cyber intrusion and counterintelligence-style activity, with campaigns designed to quietly collect sensitive communications, documents, and relationship data over extended periods.

APT42's targeting profile is tightly aligned with political, security, and strategic intelligence priorities. The group has targeted government officials, political campaigns, NGOs, policy experts, regional security personnel, and individuals connected to diplomatic or military decision-making. Unlike groups that primarily pursue enterprise network access, APT42 frequently targets personal email accounts and cloud-based identities that sit outside formal corporate security controls but still provide access to sensitive information. Public reporting has also linked APT42 to long-running deception operations that masquerade as legitimate organizations or services in order to build trust and collect credentials, highlighting the group's patience and operational discipline.

From a technical perspective, APT42 is emblematic of Iran's shift toward identity as the primary attack surface. The group commonly employs phishing and credential harvesting to obtain initial access, followed by abuse of MFA workflows, session tokens, and cloud-native features to maintain persistence. Post-compromise activity typically focuses on mailbox access, email forwarding rules, data discovery, and account expansion rather than lateral movement across endpoints. APT42's tradecraft relies heavily on legitimate cloud services and administrative actions, allowing the group to evade endpoint-based defenses and operate almost entirely within SaaS and identity provider telemetry.

Primary MITRE ATT&CK techniques associated with APT42:
T1566 – Phishing
T1598 – Phishing for Information
T1078 – Valid Accounts
T1110 – Brute Force / Credential Access
T1556 – Modify Authentication Process
T1098 – Account Manipulation
T1114 – Email Collection
T1534 – Internal Spearphishing
T1087 – Account Discovery
T1550.001 – Application Access Token Abuse

APT42 Historical victims and targeting

APT42 emerged as a distinct activity cluster in the early 2020s, reflecting Iran's growing focus on identity-centric and cloud-based intelligence collection. Public reporting consistently links the group to targeting of government officials, political campaigns, NGOs, policy experts, regional security personnel, and individuals connected to diplomatic or military decision-making. Unlike infrastructure-focused groups, APT42 frequently targets personal email accounts and cloud identities that exist outside formal enterprise security controls but still contain sensitive information.

Between 2022 and 2024, multiple vendors reported APT42 activity directed at Western and Middle Eastern policy communities, including attempts to access personal email accounts associated with political campaigns and senior advisors. In 2024, public reporting confirmed disruption of APT42-linked attempts to compromise email accounts

connected to U.S. presidential campaign personnel, though specific individuals and organizations were not named. Separate investigations have also tied APT42 to long-running deception operations—posing as legitimate organizations or service providers—to collect credentials and background information from military- and security-adjacent targets, with some of these efforts assessed to have been active since 2017.

Across reporting, victim names are rarely disclosed; however, the roles and affiliations of targets are consistently described, underscoring that APT42 prioritizes access to communications and relationships over direct network control.

Tooling and software used by APT42

APT42's tooling is notably lightweight and cloud-native, optimized for credential theft, account takeover, and long-term surveillance rather than endpoint exploitation. Initial access is commonly achieved through phishing and credential harvesting, using spoofed login pages or impersonated communications that mimic trusted institutions or contacts. These mechanisms are designed to capture usernames, passwords, and in some cases MFA artifacts, enabling direct access to email and SaaS platforms without malware deployment.

Once credentials are obtained, APT42 relies heavily on valid account abuse and cloud-native persistence mechanisms. This includes the creation or modification of email forwarding and mailbox rules, which automatically exfiltrate communications to attacker-controlled accounts, and the abuse of OAuth application access or session tokens to maintain access even after password changes. These techniques allow the actor to persist silently and monitor communications over long periods with minimal observable footprint on endpoints.

APT42 has also been associated with MFA abuse techniques, including exploitation of weak MFA enrollment and recovery workflows. By manipulating authentication settings or session tokens, the group can bypass MFA protections and retain durable access to cloud services. This identity-focused approach enables APT42 to operate almost entirely within email and SaaS audit logs, often avoiding traditional EDR or network-based detection.

Where malware is used, reporting suggests it is selective and secondary, typically lightweight implants or scripts designed to support credential harvesting or data collection rather than broad system control. However, many documented APT42 intrusions involve no malware at all, relying instead on legitimate cloud features and user trust.

MITRE ATT&CK Technique Heatmap

Legend:
✓ = Frequently Observed
* = Observed / Situational
— = Rare / Not Characteristic

ATT&CK Tactic	Technique (T-Code)	APT33	APT35	APT42
Initial Access	T1566 – Phishing	✓	✓	✓
	T1598 – Phishing for Information	*	✓	✓
	T1078 – Valid Accounts	✓	✓	✓
	T1110.003 – Password Spraying	✓	*	✓
Execution	T1059 – Command & Scripting Interpreter	✓	*	*
	T1204 – User Execution	*	✓	✓
Persistence	T1098 – Account Manipulation	✓	✓	✓
	T1550.003 – Web Session Cookie / Token Abuse	✓	*	✓
Privilege Escalation	T1098 – Account Manipulation	✓	✓	✓
	T1556 – Modify Authentication Process	*	*	✓
Defense Evasion	T1036 – Masquerading	✓	✓	✓
	T1070 – Indicator Removal on Host	*	—	—
Credential Access	T1110 – Brute Force	✓	*	✓
	T1556 – Modify Authentication Process	*	*	✓
Discovery	T1087 – Account Discovery	✓	✓	✓
	T1046 – Network Service Discovery	✓	—	—
	T1016 – System Network Configuration Discovery	✓	*	—
Lateral Movement	T1021 – Remote Services	✓	*	—
	T1534 – Internal Spearphishing	—	✓	✓
Collection	T1114 – Email Collection	*	✓	✓
	T1005 – Data from Local System	✓	*	—
Exfiltration	T1041 – Exfiltration Over C2 Channel	✓	*	—
	T1567 – Exfiltration Over Web Services	*	✓	✓

Why It Matters

State actor–backed threat groups matter because they operate with a level of persistence, resourcing, and strategic intent that fundamentally exceeds traditional cybercrime. These actors are not constrained by short-term financial return and can sustain long-running campaigns focused on intelligence collection, access development, and pre-positioning inside target environments. As a result, organizations may experience prolonged, low-noise compromises that evade standard detection models and quietly erode the confidentiality and integrity of sensitive systems, data, and communications.

From a technical perspective, state-backed operators consistently demonstrate an ability to adapt faster than enterprise defenses by exploiting common, trusted components of modern IT environments. Identity systems, cloud services, email platforms, and administrative tooling are routinely abused as primary attack vectors, allowing adversaries to blend into legitimate activity and bypass traditional perimeter- and malware-focused controls. This shifts the defensive challenge from blocking individual exploits to maintaining continuous visibility and control over authentication flows, privilege use, and configuration changes across complex, distributed environments.

Ultimately, the threat posed by state-aligned actors forces organizations to rethink resilience rather than prevention alone. Even well-defended environments may be compromised at some point, making rapid detection, decisive containment, and effective recovery critical security outcomes. Without mature identity governance, cloud monitoring, and incident response processes designed for stealthy, long-term intrusions, organizations risk operating under persistent adversary presence—undermining trust in systems, decision-making processes, and the reliability of core digital operations.

How to Respond

- Strictly adhere to CyberSecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Ensure user communities are aware of active social engineering threats and how they can respond individually and as teams when these threats appear.
- Perform interdepartmental tabletop exercises that cover DR/BCP processes.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a RedTeam or PurpleTeam engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Tracking state sponsored threat actor activity through open and closed source intelligence sharing partnerships.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---