Defending Against UNC3944: Cybercrime Hardening Guidance from the Frontlines

cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations

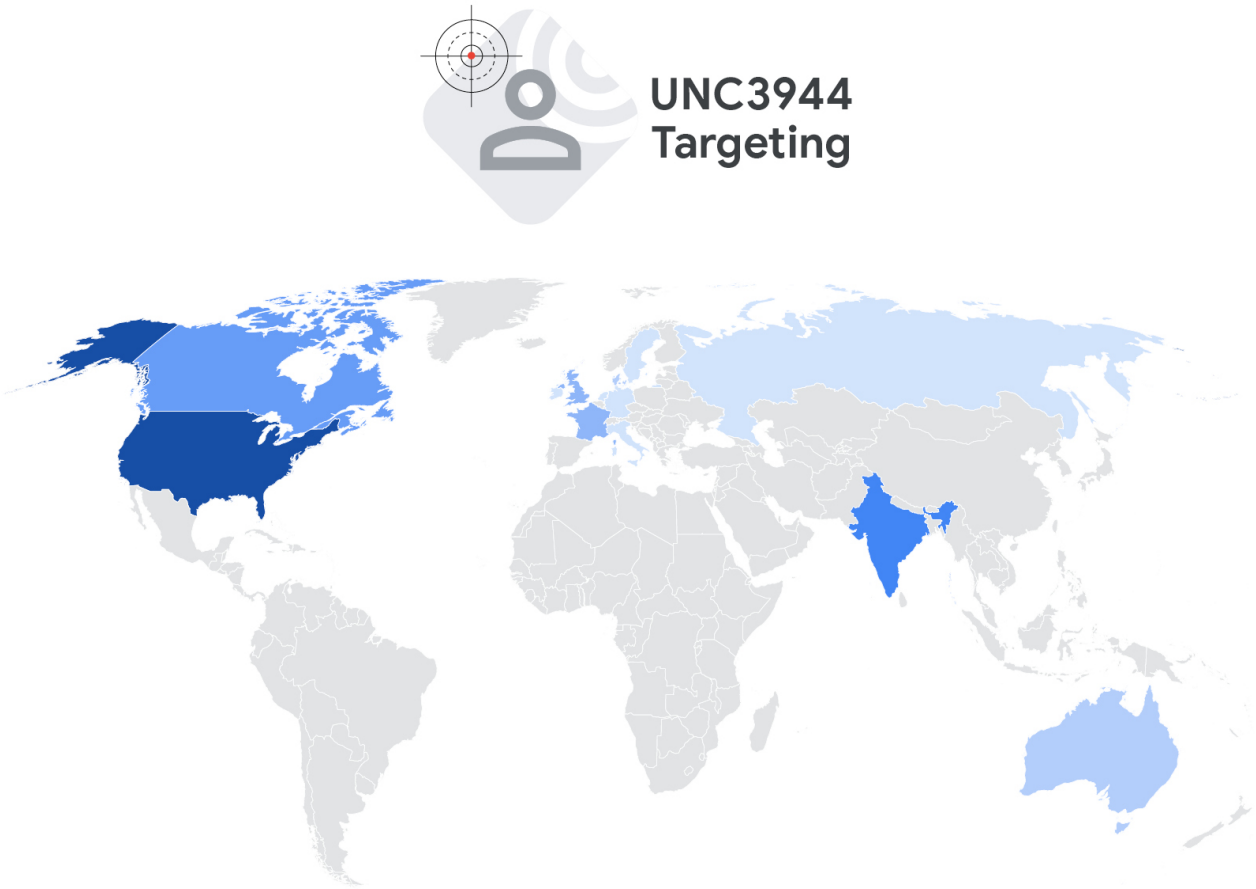
Background

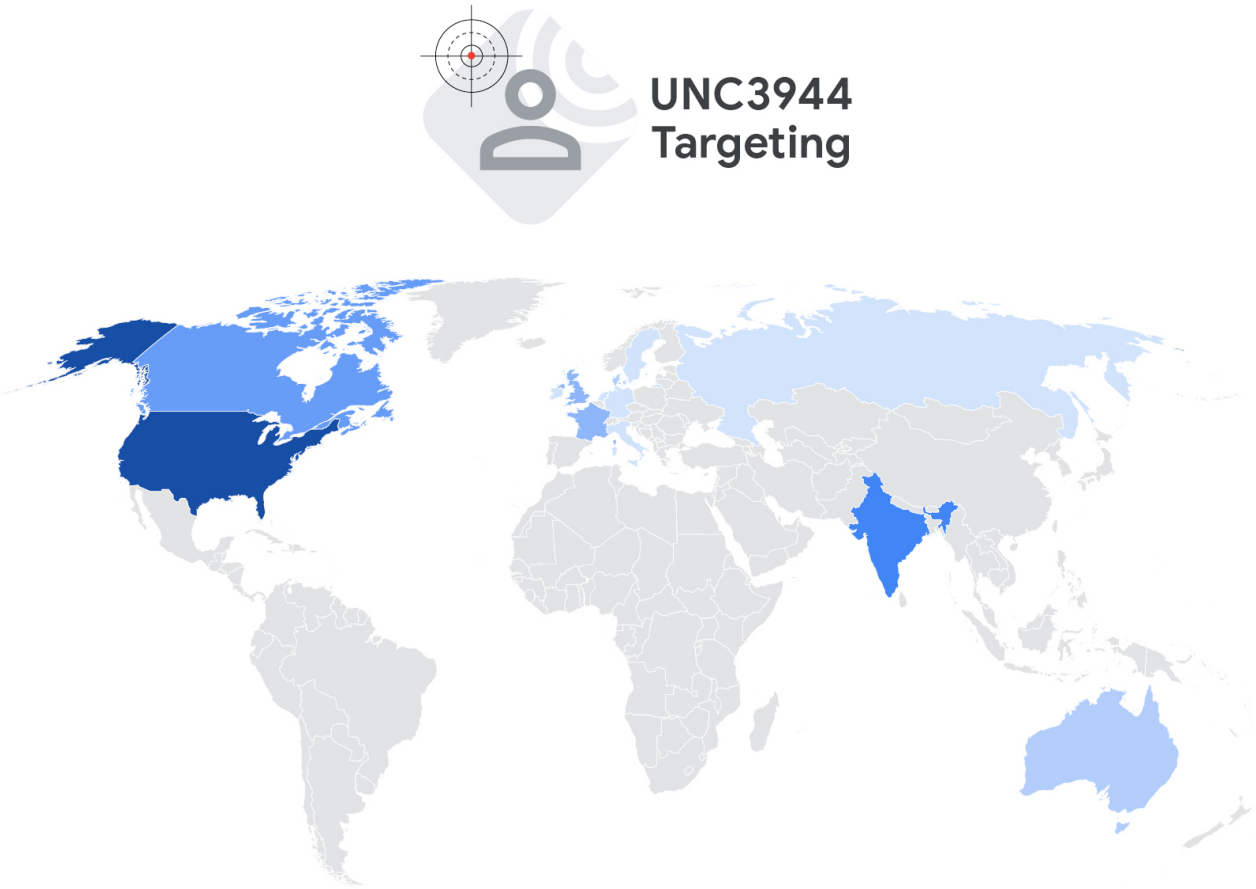
UNC3944, which overlaps with public reporting on Scattered Spider, is a financially-motivated threat actor characterized by its persistent use of social engineering and brazen communications with victims. In early operations, UNC3944 largely targeted telecommunications-related organizations to support SIM swap operations. However, after shifting to ransomware and data theft extortion in early 2023, they impacted organizations in a broader range of industries. Since then, we have regularly observed UNC3944 conduct waves of targeting against a specific sector, such as financial services organizations in late 2023 and food services in May 2024. Notably, UNC3944 has also previously targeted prominent brands, possibly in an attempt to gain prestige and increased attention by news media.

Google Threat Intelligence Group (GTIG) observed a decline in UNC3944 activity after 2024 law enforcement actions against individuals allegedly associated with the group. Threat actors will often temporarily halt or significantly curtail operations after an arrest, possibly to

reduce law enforcement attention, rebuild capabilities and/or partnerships, or shift to new tooling to evade detection. UNC3944's existing ties to a broader community of threat actors could potentially help them recover from law enforcement actions more quickly.

Recent public reporting has suggested that threat actors used tactics consistent with Scattered Spider to target a UK retail organization and deploy DragonForce ransomware. Subsequent reporting by BBC News indicates that actors associated with DragonForce claimed responsibility for attempted attacks at multiple UK retailers. Notably, the operators of DragonForce ransomware recently claimed control of RansomHub, a ransomware-as-a-service (RaaS) that seemingly ceased operations in March of this year. UNC3944 was a RansomHub affiliate in 2024, after the ALPHV (aka Blackcat) RaaS shut down. While GTIG has not independently confirmed the involvement of UNC3944 or the DragonForce RaaS, over the past few years, retail organizations have been increasingly posted on tracked data leak sites (DLS) used by extortion actors to pressure victims and/or leak stolen victim data. Retail organizations accounted for 11 percent of DLS victims in 2025 thus far, up from about 8.5 percent in 2024 and 6 percent in 2022 and 2023. It is plausible that threat actors including UNC3944 view retail organizations as attractive targets, given that they typically possess large quantities of personally identifiable information (PII) and financial data. Further, these companies may be more likely to pay a ransom demand if a ransomware attack impacts their ability to process financial transactions.


UNC3944
Targeting

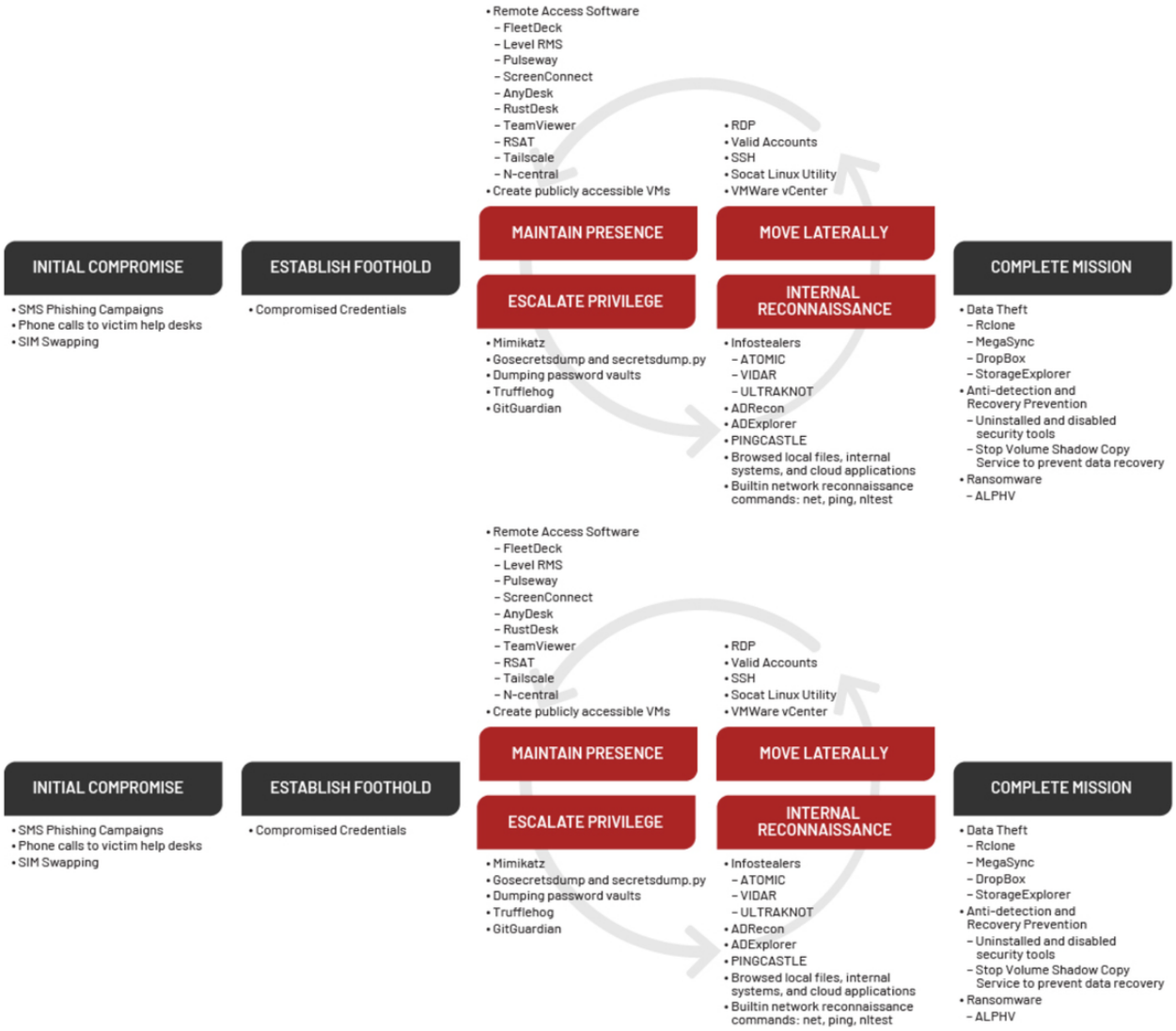

UNC3944
Targeting

UNC3944 global targeting map

We have observed the following patterns in UNC3944 victimology:

- **Targeted Sectors:** The group targets a wide range of sectors, with a notable focus on Technology, Telecommunications, Financial Services, Business Process Outsourcing (BPO), Gaming, Hospitality, Retail, and Media & Entertainment organizations.
- **Geographical Focus:** Targets are primarily located in English-speaking countries, including the United States, Canada, the United Kingdom, and Australia. More recent campaigns have also included targets in Singapore and India.
- **Victim Organization Size:** UNC3944 often targets large enterprise organizations, likely due to the potential for higher impact and ransom demands. They specifically target organizations with large help desk and outsourced IT functions which are susceptible to their social engineering tactics.

A high-level overview of UNC3944 tactics, techniques and procedures (TTPs) are noted in the following figure.



UNC3944 attack lifecycle

Proactive Hardening Recommendations

The following provides prioritized recommendations to protect against tactics utilized by UNC3944, organized within the pillars of:

- Identity
- Endpoints
- Applications and Resources
- Network Infrastructure
- Monitoring / Detections

While implementing the full suite of the recommendations in this guide will generally have some impact on IT and normal operations, Mandiant's extensive experience supporting organizations to defend against, contain, and eradicate UNC3944 has shown that an effective starting point involves prioritizing specific areas. Organizations should begin by focusing on recommendations that:

- Achieve complete visibility across all infrastructure, identity, and critical management services.
- Ensure the segregation of identities throughout the infrastructure.
- Enhance strong authentication criteria.
- Enforce rigorous identity controls for password resets and multi-factor authentication (MFA) registration.
- Educate and communicate the importance of remaining vigilant against modern-day social engineering attacks / campaigns (see Social Engineering Awareness section later in this post). UNC3944 campaigns not only target end-users, but also IT and administrative personnel within enterprise environments.

These serve as critical foundational measures upon which other recommendations in this guide can be built.

Google SecOps customers benefit from existing protections that actively detect and alert on UNC3944 activity.

Identity

Positive Identify Verification

UNC3944 has proven to be very prolific in using social engineering techniques to impersonate users when contacting the help desk. Therefore, further securing the "positive identity" process is critical.

- Train help desk personnel to positively identify employees before modifying / providing security information (including initial enrollment). At a minimum, this process should be required for any privileged accounts and should include methods such as:
    - On-Camera / In-Person verification
    - ID Verification
    - Challenge / Response questions

- If a suspected compromise is imminent or has occurred, temporarily disable or enhance validation for self-service password reset methods. Any account management activities should require a positive identity verification as the first step. Additionally, employees should be required to authenticate using strong authentication PRIOR to changing authentication methods (e.g., adding a new MFA device). Additionally, implement use of:
    - Trusted Locations
    - Notification of authentication / security changes
    - Out-of-band verification for high-risk changes. For example, require a call-back to a registered number or confirmation via a known corporate email before proceeding with any sensitive request.
- Avoid reliance on publicly available personal data for verification (e.g., DOB, last 4 SSN) as UNC3944 often possesses this information. Use internal-only knowledge or real-time presence verification when possible.
- Temporarily disable self-service MFA resets during elevated threat periods, and route all such changes through manual help desk workflows with enhanced scrutiny.

Strong Authentication

To prevent against social engineering or other methods used to bypass authentication controls:

- Remove SMS, phone call, and/or email as authentication controls.
- Utilize an authenticator app that requires phishing resistant MFA (e.g., number matching and/or geo-verification).
- If possible, transition to passwordless authentication.
- Leverage FIDO2 security keys for authenticating identities that are assigned privileged roles.
- Ensure administrative users cannot register or use legacy MFA methods, even if those are permitted for lower-tier users.
- Enforce multi-context criteria to enrich the authentication transaction. Examples include not only validating the identity, but also specific device and location attributes as part of the authentication transaction.
    - For organizations that leverage Google Workspace, these concepts can be enforced by using context-aware access policies.

    - For organizations that leverage Microsoft Entra ID, these concepts can be enforced by using a Conditional Access Policy.

MFA Registration and Modification

To prevent compromised credentials from being leveraged for modifying and registering an attacker-controlled MFA method:

- Review authentication methods available for user registration and disallow any unnecessary or duplicative methods.
- Restrict MFA registration and modification actions to only be permissible from trusted IP locations and based upon device compliance. For organizations that leverage Microsoft Entra ID, this can be accomplished using a Conditional Access Policy.
- If a suspected compromise has occurred, MFA **re-registration** may be required. This action should only be permissible from corporate locations and/or trusted IP locations.
- Review specific IP locations that can bypass the requirement for MFA. If using Microsoft Entra ID, these can be in Named Locations and the legacy Service Settings.
- Investigate and alert when the same MFA method or phone number is registered across multiple user accounts, which may indicate attacker-controlled device registration.

Administrative Roles

To prevent against privilege escalation and further access to an environment:

- For privileged access, decouple the organization's identity store (e.g., Active Directory) from infrastructure platforms, services, and cloud admin consoles. Organizations should create local administrator accounts (e.g., local VMware VCenter Admin account). Local administrator accounts should adhere to the following principles:
    - Created with long and complex passwords
    - Passwords should not be temporarily stored within the organization’s password management or vault solution
    - Enforcement of Multi-Factor Authentication (MFA)
- Restrict administrative portals to only be accessible from trusted locations and with privileged identities.
- Leverage just-in-time controls for leveraging (“checking out”) credentials associated with privileged actions.

- Enforce access restrictions and boundaries that follow the principle of least-privilege for accessing and administering cloud resources.
    - For organizations that leverage Google Cloud, these concepts can be enforced by using IAM deny or principle access boundary policies.
    - For organizations that leverage Microsoft Entra ID, these concepts can be enforced by using Azure RBAC and Entra ID RBAC controls.
- Enforce that privileged accounts are hardened to prevent exposure or usage on non-Tier 0 or non-PAW endpoints.

Playbooks

Modern-day authentication is predicated on more than just a singular password. Therefore, organizations should ensure that processes and associated playbooks include steps to:

- Revoke tokens and access keys.
- Review MFA device registrations.
- Review changes to authentication requirements.
- Review newly enrolled devices and endpoints.

Endpoints

Device Compliance and Validation

An authentication transaction should not only include strong requirements for identity verification, but also require that the device be authenticated and validated. Organizations should consider the ability to:

- Enforce posture checks for devices remotely connecting to an environment (e.g., via a VPN). Example posture checks for devices include:
    - Validating the installation of a required host-based certificate on each endpoint.
    - Verifying that the endpoint operates on an approved Operating System (OS) and meets version requirements.
- Confirming the organization's Endpoint Detection and Response (EDR) agent is installed and actively running. Enforce EDR installation and monitoring for all managed endpoint devices.

Rogue / Unauthorized Endpoints

To prevent against threat actors leveraging rogue endpoints to access an environment, organizations should:

- Monitor for rogue bastion hosts or virtual machines that are either newly created or recently joined to a managed domain.
- Harden policies to restrict the ability to join devices to Entra or on-premises Active Directory.
- Review authentication logs for devices that contain default Windows host names.

Lateral Movement Hardening

To prevent against lateral movement using compromised credentials, organizations should:

- Limit the ability for local accounts to be used for remote (network-based) authentication.
- Disable or restrict local administrative and/or hidden shares from being remotely accessible.
- Enforce local firewall rules to block inbound SMB, RDP, WinRM, PowerShell, & WMI.

GPOs: User Rights Assignment Lockdown (Active Directory)

For domain-based privileged and service accounts, where possible, organizations should restrict the ability for accounts to be leveraged for remote authentication to endpoints. This can be accomplished using a Group Policy Object (GPO) configuration for the following user rights assignments:

- Deny log on locally
- Deny log on through Remote Desktop Services
- Deny access to this computer from network
- Deny log on as a batch
- Deny log on as a service

Applications and Resources

Virtual Private Network (VPN) Access

Threat actors may attempt to change or disable VPN agents to limit network visibility by security teams. Therefore, organizations should:

- Disable the ability for end users to modify VPN agent configurations.
- Ensure appropriate logging when configuration changes are made to VPN agents.
- For managed devices, consider an “Always-On” VPN configuration to ensure continuous protection.

Privileged Access Management (PAM) Systems

To prevent against threat actors attempting to gain access to privileged access management (PAM) systems, organizations should:

- Isolate and enforce network and identity access restrictions for enterprise password managers or privileged access management (PAM) systems. This should also include leveraging dedicated and segmented servers / appliances for PAM systems, which are isolated from enterprise infrastructure and virtualization platforms.
- Reduce the scope of accounts that have access to PAM systems, in addition to requiring strong authentication (MFA).
- Enforce role-based access controls (RBAC) within PAM systems, restricting the scope of accounts that can be accessed (based upon an assigned role).
- Follow the principle of just-in-time (JIT) access for checking-out credentials stored in PAM systems.

Virtualization Infrastructure

To prevent against threat actors attempting to gain access to virtualization infrastructure, organizations should:

- Isolate and restrict access to ESXi hosts / vCenter Server Appliances.
- Ensure that backups of virtual machines are isolated, secured and immutable if possible.
- Unbind the authentication for administrative access to virtualization platforms from the centralized identity provider (IdP). This includes individual ESXi hosts and vCenter Servers.
- Proactively rotate local root / administrative passwords for privileged identities associated with virtualization platforms.
- If possible use stronger MFA and bind to local SSO for all administrative access to virtualization infrastructure.

- Enforce randomized passwords for local root / administrative identities correlating to each virtualized host that is part of an aggregate pool.
- Disable / restrict SSH (shell) access to virtualization platforms.
- Enable lockdown mode on all ESXi hosts.
- Enhance monitoring to identify potential malicious / suspicious authentication attempts and activities associated with virtualization platforms.

Backup Infrastructure

To prevent against threat actors attempting to gain access to backup infrastructure and data, organizations should:

- Leverage unique and separate (non-identity provider integrated) credentials for accessing and managing backup infrastructure, in addition to the enforcement of MFA for the accounts.
- Ensure that backup servers are isolated from the production environment and reside within a dedicated network. To further protect backups, they should be within an immutable backup solution.
- Implement access controls that restrict inbound traffic and protocols for accessing administrative interfaces associated with backup infrastructure.
- Periodically validate the protection and integrity of backups by simulating adversarial behaviors (red teaming).

Endpoint Security Management

To prevent against threat actors weaponizing endpoint security and management technologies such as EDR and patch management tools, organizations should:

- Segment administrative access to endpoint security tooling platforms.
- Reduce the scope of identities that have the ability to create, edit, or delete Group Policy Objects (GPOs) in on-premises Active Directory.
- If Intune is leveraged, enforce Intune access policies that require multi-administrator approval (MMA) to approve and enforce changes.
- Monitor and review unauthorized access to EDR and patch management technologies.
- Monitor script and application deployment on endpoints and systems using EDR and patch management technologies.

- Review and monitor “allow-listed” executables, processes, paths, and applications.
- Inventory installed applications on endpoints and review for potential unauthorized installations of remote access (RATs) and reconnaissance tools.

Cloud Resources

To prevent against threat actors leveraging access to cloud infrastructure for additional persistence and access, organizations should:

- Monitor and review cloud resource configurations to identify and investigate newly created resources, exposed services, or other unauthorized configurations.
- Monitor cloud infrastructure for newly created or modified network security group (NSG) rules, firewall rules, or publicly exposed resources that can be remotely accessed.
- Monitor for the creation of programmatic keys and credentials (e.g., access keys).

Network Infrastructure

Access Restrictions

To proactively identify exposed applications, ingress pathways, and to reduce the risk of unauthorized access, organizations should:

- Leverage vulnerability scanning to perform an external unauthenticated scan to identify publicly exposed domains, IPs, and CIDR IP ranges.
- Enforce strong authentication (e.g., phishing-resistant MFA) for accessing any applications and services that are publicly accessible.
- For sensitive data and applications, enforce connectivity to cloud environments / SaaS applications to only be permissible from specific (trusted) IP ranges.
- Block TOR exit node and VPS IP ranges.

Network Segmentation

The terminology of “Trusted Service Infrastructure” (TSI) is typically associated with management interfaces for platforms and technologies that provide core services for an organization. Examples include:

- Asset and Patch Management Tools
- Network Management Tools and Devices

- Virtualization Platforms
- Backup Technologies
- Security Tooling
- Privileged Access Management Systems

To minimize the direct access and exposure of the management plane for TSI, organizations should:

- Restrict access to TSI to only originate from internal / hardened network segments or PAWs.
- Create detections focused on monitoring network traffic patterns for directly accessing TSI, and alert on anomalies or suspicious traffic.

Egress Restrictions

To restrict the ability for command-and-control and reduce the capabilities for mass data exfiltration, organizations should:

- Restrict egress communications from all servers. Organizations should prioritize enforcing egress restrictions from servers associated with TSI, Active Directory domain controllers, and crown jewel application and data servers.
- Block outbound traffic to malicious domain names, IP addresses, and domain names/addresses associated with remote access tools (RATs).

Monitoring / Detections

Reconnaissance

Upon initial compromise, UNC3944 is known to search for documentation on topics such as: user provisioning, MFA and/or device registration, network diagrams, and shared credentials in documents or spreadsheets.

UNC3944 will also use network reconnaissance tools like ADRecon, ADExplorer, and SharpHound. Therefore, organizations should:

- Ensure any sites or portals that include these documents have access restrictions to only required accounts.
- Sweep for documents and spreadsheets that may contain shared credentials and remove them.

- Implement alerting rules on endpoints with EDR agents for possible execution of known reconnaissance tools.
- If utilizing an Identity monitoring solution, ensure detection rules are enabled and alerts are created for any reconnaissance and discovery detections.
- Implement an automated mechanism to continuously monitor domain registrations. Identify domains that mimic the organization's naming conventions, for instance: `[YourOrganizationName]-helpdesk.com` or `[YourOrganizationName]-SSO.com`.

MFA Registration

To further harden the MFA registration process, organizations should:

- Review logs to specifically identify events related to the registration or addition of new MFA devices or methods to include actions similar to:
    - MFA device registered
    - Authenticator app added
    - Phone number added for MFA
    - The same MFA device / method / phone number being associated with multiple users
- Verify the legitimacy of new registrations against expected user behavior and any onboarding or device enrollment records.
- Contact users if new registrations are detected to confirm if the activity is intentional.

Collaboration and Communication Platforms

To prevent against social engineering and/or unauthorized access or modifications to communication platforms, organizations should:

- Review organizational policies around communication tools such as Microsoft Teams.
- Allow only trusted external domains for expected vendors and partners.

    If external domains cannot be blocked, create a baseline of trusted domains and alert on new domains that attempt to contact employees.
- Provide awareness training to employees and staff to directly contact the organization’s helpdesk if they receive suspicious calls or messages.

The following is a Microsoft Defender advanced hunting query example. The query is written to detect when an external account (attempting to impersonate the help desk) attempts to contact the organization's users.

Note: The DisplayName field can be modified to include other relevant fields specific to the organization (such as "IT Support" or "ServiceDesk").

```
CloudAppEvents
| where Application == "Microsoft Teams"
| where ActionType == "ChatCreated"
| extend HasForeignTenantUsers =
parse_json(RawEventData)["ParticipantInfo"]["HasForeignTenantUsers"]
| extend DisplayName = parse_json(RawEventData)["Members"][0]["DisplayName"]
| where IsExternalUser == 1 or HasForeignTenantUsers == 'true'
| where DisplayName contains "help" or AccountDisplayName contains "help"
or AccountId contains "help"
```

The following is a Google SecOps search query example.

Note: The DisplayName field can be modified to include other relevant fields specific to the organization (such as "IT Support" or "ServiceDesk").

```
metadata.vendor_name = "Microsoft"
metadata.product_name = "Office 365"
metadata.product_event_type = "ChatCreated"
security_result.detection_fields["ParticipantInfo_HasForeignTenantUsers"] =
"true"
(
principal.user.userid = /help/ OR
principal.user.email_addresses = /help/ OR
about.user.user_display_name = /help/
)
```

Identity Session Risk & Visibility

Detections should include:

- Authentication from infrequent locations - including from proxy and VPN service providers.
- Attempts made to change authentication methods or criteria.
- Monitoring and hunting for authentication anomalies based upon social engineering tactics.

Bypassing Multi-Factor Authentication

UNC3944 has been known to modify requirements for the use of Multi-factor Authentication. Therefore, organizations should:

- For Entra ID, monitor for modifications to any Trusted Named Locations that may be used to bypass the requirement for MFA.
- For Entra ID, monitor for changes to Conditional Access Policies that enforce MFA, specifically focusing on exclusions of compromised user accounts and/or devices for an associated policy.
- Ensure the SOC has visibility into token replay or suspicious device logins, aligning workflows that can trigger step-up (re)authentication when suspicious activity is detected.

Abuse of Domain Federation

For organizations that are using Microsoft Entra ID, monitor for possible abuse of Entra ID Identity Federation:

- Check domain names that are registered in the Entra ID tenant, paying particular attention to domains that are marked as Federated.
- Review the Federation configuration of these domains to ensure that they are correct.
- Monitor for creation of any new domains within the tenant and for changing the authentication method to be Federated.
- Abuse of Domain Federation requires the account accomplishing the changes to have administrative permissions in Entra ID. Hardening of all administrative accounts, portals, and programmatic access is imperative.

Social Engineering Awareness

UNC3944 is extremely proficient at using multiple forms of social engineering to convince users into doing something that will allow them to gain access. Organizations should educate users to be aware of and notify internal security teams of attempts that utilize the following tactics:

- SMS phishing messages that claim to be from IT requesting users to download and install software on their machine. These may include claims that the user's machine is out-of-compliance or is failing to report to internal management systems.
- SMS messages or emails with links to sites that reference domain names that appear legitimate and reference SSO (single sign-on) and a variation of the company name. Messages may include text informing the user that they need to reset their password and/or MFA.

- Phone calls to users from IT with requests to reset a password and/or MFA - or requesting that the user provide a validated one time passcode (OTP) from their device.
- SMS messages or emails with requests to be granted access to a particular system, particularly if the organization already has an established method for provisioning access.
- MFA fatigue attacks, where attackers may repeatedly send MFA push notifications to a victim's device until the user unintentionally or out of frustration accepts one. Organizations should train users to reject unexpected MFA prompts and report such activity immediately.
- Impersonation via collaboration tools - UNC3944 has used platforms like Microsoft Teams to pose as internal IT support or service desk personnel. Organizations should train users to verify unusual chat messages and avoid sharing credentials or MFA codes over internal collaboration tools like Microsoft Teams. Limiting external domains and monitoring for impersonation attempts (e.g., usernames containing 'helpdesk' or 'support') is advised.
- In rare cases, attackers have used doxxing threats or aggressive language to scare users into compliance. Ensure employees understand this tactic and know that the organization will support them if they report these incidents.

Additional References

Posted in

Threat Intelligence