Why Are You Texting Me? UNC3944 Leverages SMS Phishing Campaigns for SIM Swapping, Ransomware, Extortion, and Notoriety

By Mandiant

Published: 2023-09-14 · Archived: 2026-04-05 14:01:49 UTC

Written by: Mandiant Intelligence

UNC3944 is a financially motivated threat cluster that has persistently used phone-based social engineering and SMS phishing campaigns (smishing) to obtain credentials to gain and escalate access to victim organizations. At least some UNC3944 threat actors appear to operate in underground communities, such as Telegram and underground forums, which they may leverage to acquire tools, services, and/or other support to augment their operations. This activity overlaps with activity that has been reported in open sources as "0ktapus," "Scatter Swine," and "Scattered Spider." Since 2022 and through early 2023, UNC3944 appeared to focus on accessing credentials or systems used to enable SIM swapping attacks, likely in support of secondary criminal operations occurring outside of victim environments. However, in mid-2023, UNC3944 began to shift to deploying ransomware in victim environments, signaling an expansion in the group's monetization strategies. These changes in their end goals signal that the industries targeted by UNC3944 will continue to expand; Mandiant has already directly observed their targeting broaden beyond telecommunication and business process outsourcer (BPO) companies to a wide range of industries including hospitality, retail, media and entertainment, and financial services.

UNC3944 has demonstrated a stronger focus on stealing large amounts of sensitive data for extortion purposes and they appear to understand Western business practices, possibly due to the geographical composition of the group. UNC3944 has also consistently relied on publicly available tools and legitimate software in combination with malware available for purchase on underground forums. The following examples represent some of the more notable tactics, techniques, and procedures (TTPs) that have been observed during UNC3944 operations.

- UNC3944 relies heavily on social engineering to obtain initial access to its victims. They frequently use SMS phishing campaigns and calls to victim help desks to attempt to obtain password resets or multifactor bypass codes.
- The threat actors used commercial residential proxy services to access their victims from the same local area to fly under the radar of security monitoring tools.
- The threat actors consistently use legitimate software, including a variety of remote access tools the actors have downloaded from the vendor websites.
- The threat actors operate with an extremely high operational tempo, accessing critical systems and exfiltrating large volumes of data over a course of a few days. The tempo and volume of systems UNC3944 accesses can overwhelm security response teams.

- Once obtaining a foothold, UNC3944 often spends significant time searching through internal documentation, resources, and internal chat logs to surface information that could help facilitate escalating privileges and maintaining presence within victim environments.
- UNC3944 often achieves privilege escalation by targeting password managers or privileged access management systems.
- UNC3944 often creates unmanaged virtual machines inside victims' own environments, from which it launches attacks. In some cases, they've created Internet accessible virtual machines in a victim's cloud environment.
- When deploying ransomware, the threat actors appear to specifically target business-critical virtual machines and other systems, likely in an attempt to maximize impact to the victim.
- The threat actors engage in aggressive communications with victims, such as leaving threatening notes within a text file on a system, contacting executives via text messages and emails, and infiltrating communication channels being used by victims to respond to incidents.

Tactics, Techniques, and Procedures

The following sections organize UNC3944's TTPs by the stages of the Mandiant attack lifecycle model and focus on activity observed during UNC3944 intrusions in 2023.

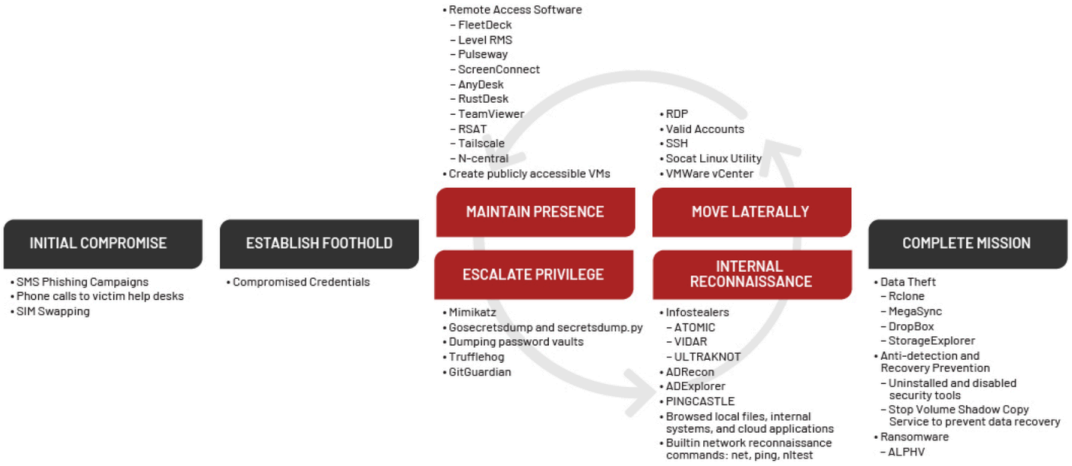


Figure 1: UNC3944 attack lifecycle

Smishing for Creds

A hallmark of UNC3944 incidents is the use of smishing messages sent to employees of targeted organizations for stealing valid credentials. In the majority of cases where we identified the initial access vector, UNC3944 obtained access to the victim environment after a successful smishing attack. After obtaining credentials, the threat actors have also impersonated employees on calls to victim organizations' service desks in an attempt to obtain multi factor authentication (MFA) codes and/or password resets. During these calls, the threat actor provided verification information requested by the help desk employees, including usernames, employee IDs, and other types of personally identifiable information (PII) associated with employees. Notably, the threat actors often asked the service desk support to repeat the question and paused for significant lengths before answering, likely due to the threat actor looking through notes or attempting to search for the answer to the question posed. In one incident,

UNC3944 social engineered the IT help desk to get the MFA token reset for account credentials that may have been exposed on a laptop used by an IT outsourcing company contracted by the victim organization. Mandiant determined that RECORDSTEALER credential theft malware was installed on this laptop through a fake software download only a few weeks prior. UNC3944 typically uses stolen credentials to then establish a foothold on victim environments.

UNC3944 phishing pages are designed to appear as if they belong to the targeted organization and frequently use single sign on (SSO) or service desk lures. The registered domains typically include both the victim organization name in combination with "-sso" or "-servicenow" in the domain. Based on analysis of suspected UNC3944 phishing domains, it is plausible that the threat actors have, in some cases, used access to victim environments to obtain information about internal systems and leveraged that information to facilitate more tailored phishing campaigns. For example, in some cases the threat actors appeared to create new phishing domains that included the names of internal systems.

Phishing Kits Associated with UNC3944 Activity

Mandiant has identified at least three phishing kits that have been used to facilitate UNC3944 campaigns.

1. Between late 2021 and mid-2022, UNC3944 campaigns involved the use of a phishing kit we have dubbed EIGHTBAIT (Figure 2). This phishing kit is designed to send captured credentials to an actor-controlled Telegram channel. Additionally, EIGHTBAIT can deploy AnyDesk to a victim's system, indicating this kit was developed with the intent of targeting non-mobile systems and not expressly designed for smishing campaigns.

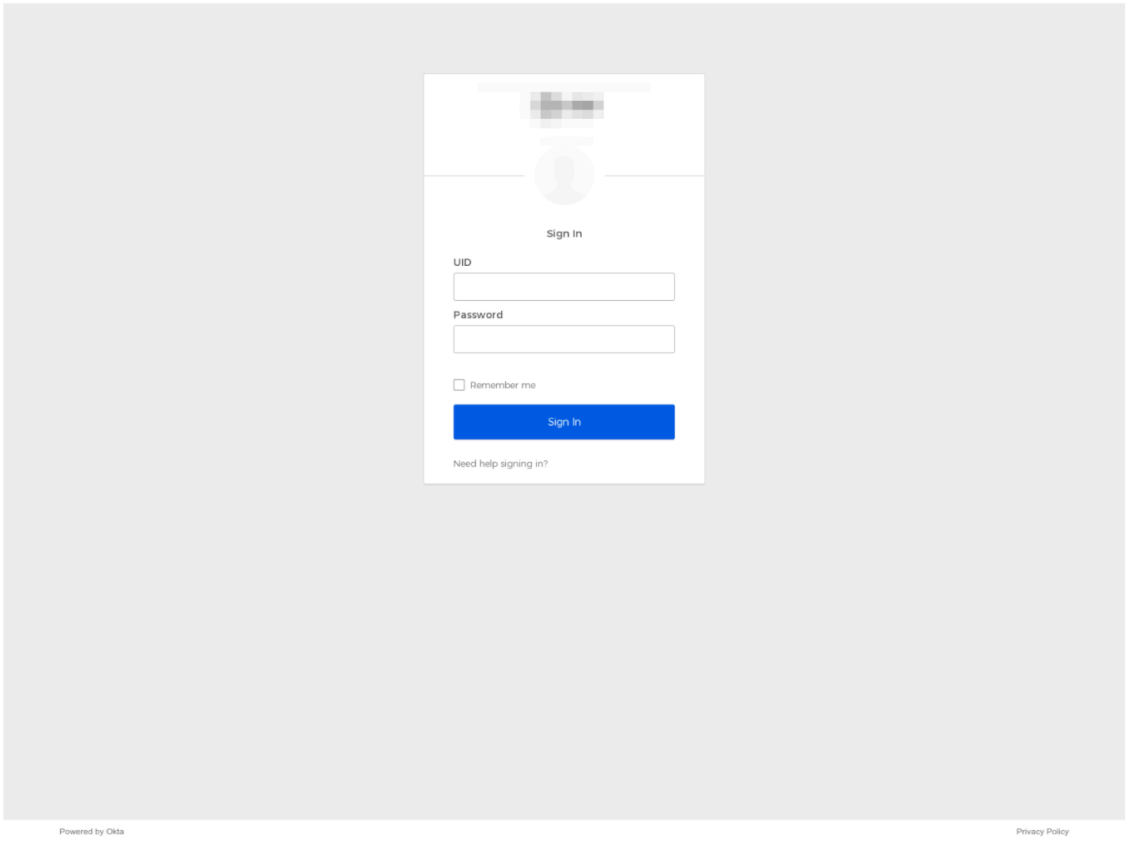


Figure 2: Sample EIGHTBAIT phishing page

2. Starting in Q3 2022, we observed UNC3944 credential phishing campaigns that leveraged a new phishing kit that appears to have been built using a webpage copied from a targeted organization (Figure 3). This kit uses a generic authentication theme and is built using a scraped copy of a target organization's authentication page. Notably, this kit has been used in some of the recent intrusions that led to extortion attempts.

Figure 3: Sample phishing page from kit 2

3. In mid-2023 we identified a third phishing kit that has been used in parallel with the second phishing kit (Figure 4). This kit has significant visual and structural similarities to the second phishing kit, and the websites they present are nearly identical. Despite these similarities, minor changes to the kit's code suggest that the theme used by the second kit was probably retrofitted into a new tool.

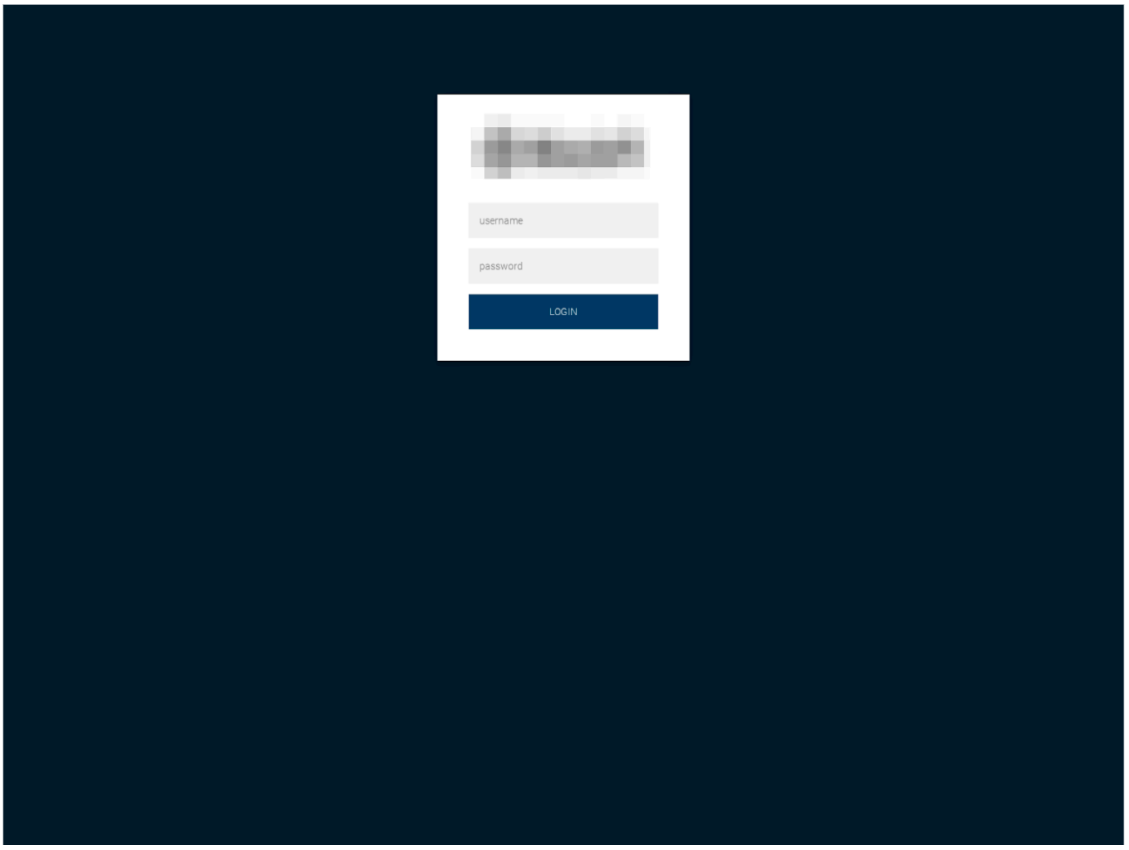


Figure 4: Sample phishing page from kit 3

When There's Nowhere to Go but Up

UNC3944 doesn't rely exclusively on smishing and social engineering to obtain the privileged access required to meet their objectives. Mandiant has observed UNC3944 use publicly available credential theft tools and expend significant effort searching through internal systems to identify ways to obtain privileged credentials. In one incident UNC3944 was able to export the data from the victim's HashiCorp Vault by using a copy of the Vault client, which the threat actors downloaded from the official HashiCorp site. They successfully exported the credentials from the HashiCorp Vault and authenticated to a file server with a domain admin account. In another incident UNC3944 installed a PowerShell module for the CyberArk API, enabling them to dump credentials from the vault server. UNC3944 has attempted to identify credentials stored in internal GitHub repositories using publicly available tools such as Trufflehog and GitGuardian. On one occasion, UNC3944 executed the open-source tool MicroBurst against a victim Azure tenant using privileged credentials. The primary function of MicroBurst is to identify Azure credentials and secrets.

We have observed evidence suggesting that UNC3944 may use various infostealers to support their operations. For example, the threat actors used a PowerShell script to download the ULTRAKNOT credential stealer (aka Meduza stealer) staged on the victim's AWS bucket. We have also observed the threat actors download or stage data miners such as VIDAR and ATOMIC.

The Call is Coming From Outside the House

A common hallmark of UNC3944 intrusions has been their creative, persistent, and increasingly effective targeting of victims' cloud resources. This strategy allows the threat actors to establish a foothold for their later operations, perform network and directory reconnaissance, and to access many sensitive systems and data stores while having minimal interaction with what some organizations would traditionally consider their internal corporate network.

UNC3944 is particularly adept at using privileged access to cloud environments to establish persistent access to victim environments. The persistence techniques can be difficult to monitor for and detect, especially in large multi-cloud environments. UNC3944 has added rogue federated identity providers to victims' Microsoft Entra environment (formerly Azure Active Directory), which allowed them to execute golden SAML attacks. The threat actor could then authenticate to resources protected by Entra ID as any user in the organization without knowledge of their password or possession of their MFA device. In multiple incidents the threat actors have created Azure Virtual Machines and assigned them public IP addresses. These threat actor-created Virtual Machines do not have the organization's mandated security and logging software installed on them, providing the threat actors with unmonitored access to a trusted system inside of the organization's network which they then use to progress their intrusion.

The threat actors have also used their access to victim organization cloud resources to host malicious utilities and run them across systems in the network. In one incident, the threat actors hosted malicious utilities on an Amazon Web Service (AWS) S3 bucket owned by the organization and used an Intune PowerShell orchestration to download the utilities from inside the victim environment. The scripts were configured to disable firewall rules and several Windows Defender protections, such as Microsoft Defender ATP, prior to retrieving and executing an ALPHV ransomware payload.

UNC3944 has also found use of some of the more niche features and applications within Azure to move laterally and conduct data theft. On multiple occasions UNC3944 has moved laterally within an organization's Azure environment using the Special Administration Console to connect to virtual machines via serial console. Mandiant has observed the threat actors use Azure Data Factory to modify existing pipelines to steal data that is stored in various integrated platforms such as data warehouses, storage blobs, and SQL databases. Specifically, they have created pipeline jobs that run "activities" to export data from those data sources to an attacker-controlled SFTP server. The use of data factories provided the threat actors with a stable and high-bandwidth platform to copy large volumes of data.

Outlook and Implications

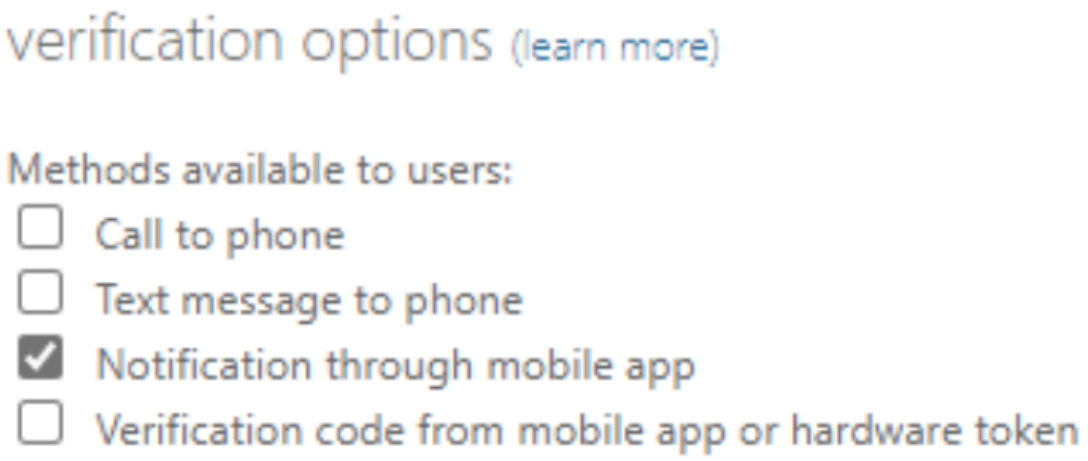
UNC3944 is an evolving threat that has continued to broaden its skills and tactics in order to successfully diversify its monetization strategies. We expect that these threat actors will continue to improve their tradecraft over time and may leverage underground communities for support to increase the efficacy of their operations. The threat actors have successfully relied on social engineering schemes to obtain initial accesses, whether in the form of SMS phishing campaigns or by calling victim organizations' help desks to reset passwords and MFA. UNC3944's initial successes likely emboldened it to expand its TTPs to more disruptive and profitable attacks, including ransomware and extortion. It is plausible that these threat actors may use other ransomware brands and/or and incorporate additional monetization strategies to maximize their profits in the future. We anticipate that

intrusions related to UNC3944 will continue to involve diverse tools, techniques, and monetization tactics as the actors identify new partners and switch between different communities.

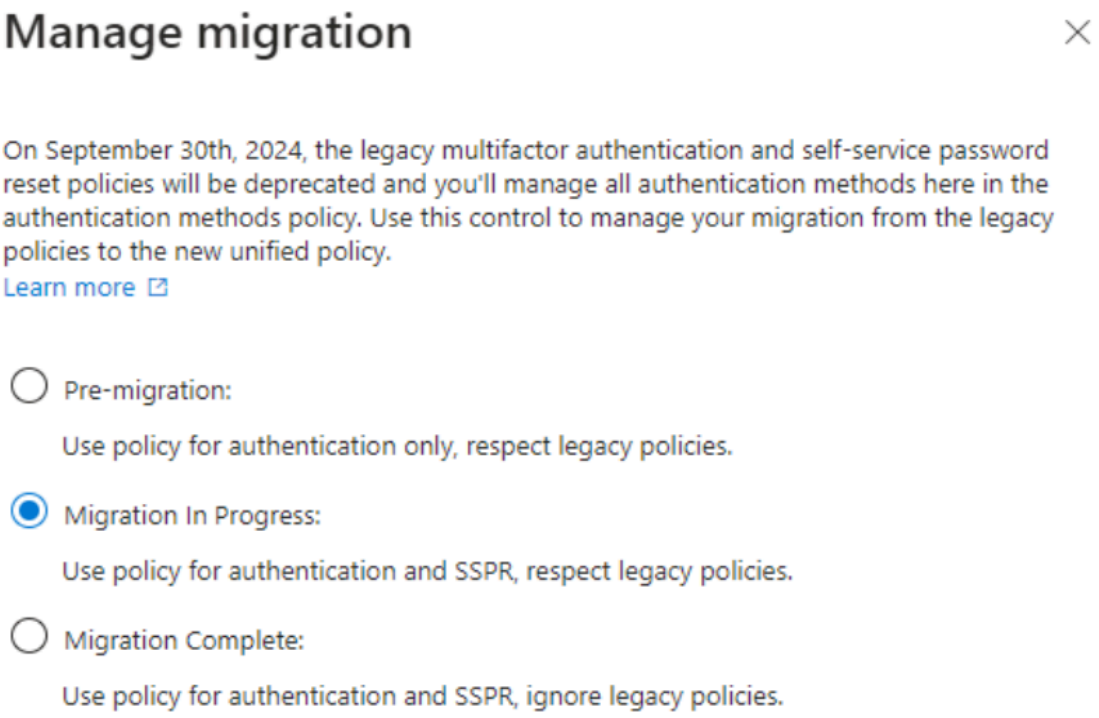
Mitigations

For organizations that are utilizing Entra ID (formerly Microsoft Azure Active Directory), the following recommendations have proven effective in mitigating against common UNC3944 TTPs such as MFA abuse and unauthorized use of privileged accounts within the Microsoft cloud environment:

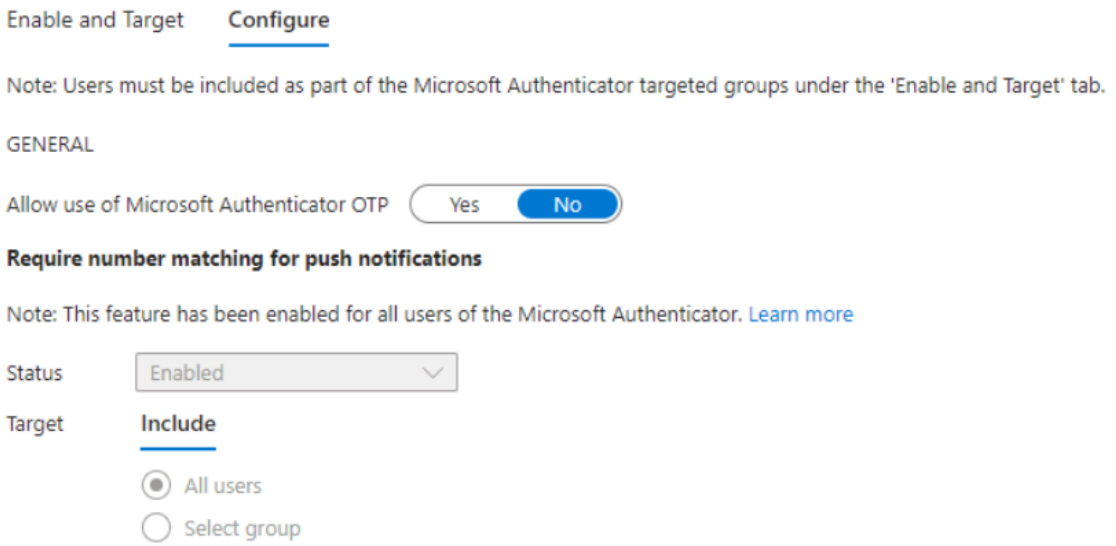
1. Enforce Microsoft Authenticator with number matching and remove SMS as an MFA verification option.
    - Remove SMS as a MFA verification option by clearing the checkbox for “Text message to phone” in the multi-factor authentication service settings dialog.



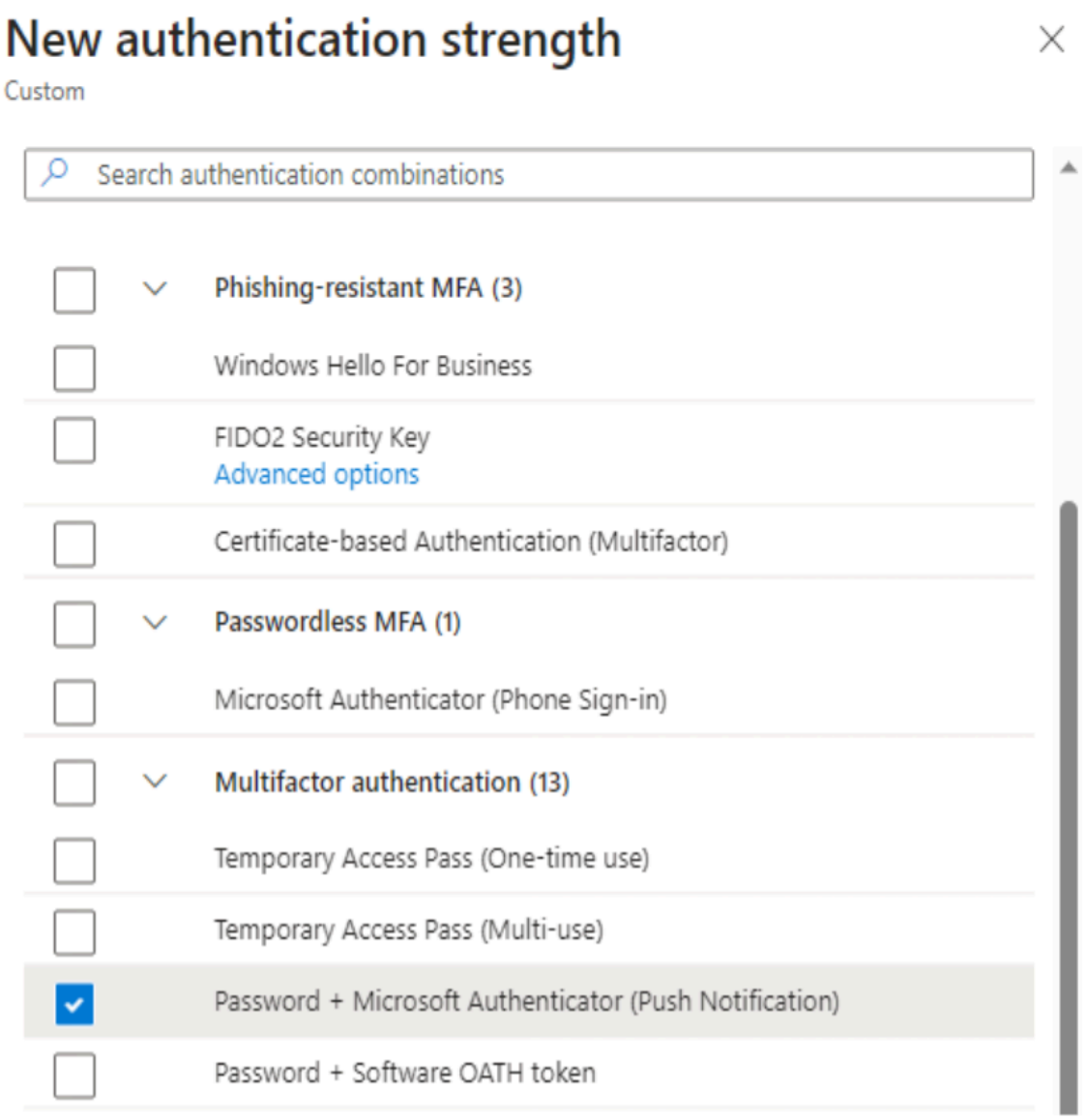
- To restrict MFA to only utilize Microsoft Authenticator with number matching, organizations will need to ensure they are at least in the “Migration In Progress” stage for leveraging authentication methods and then appropriately configure the Microsoft Authenticator authentication method.



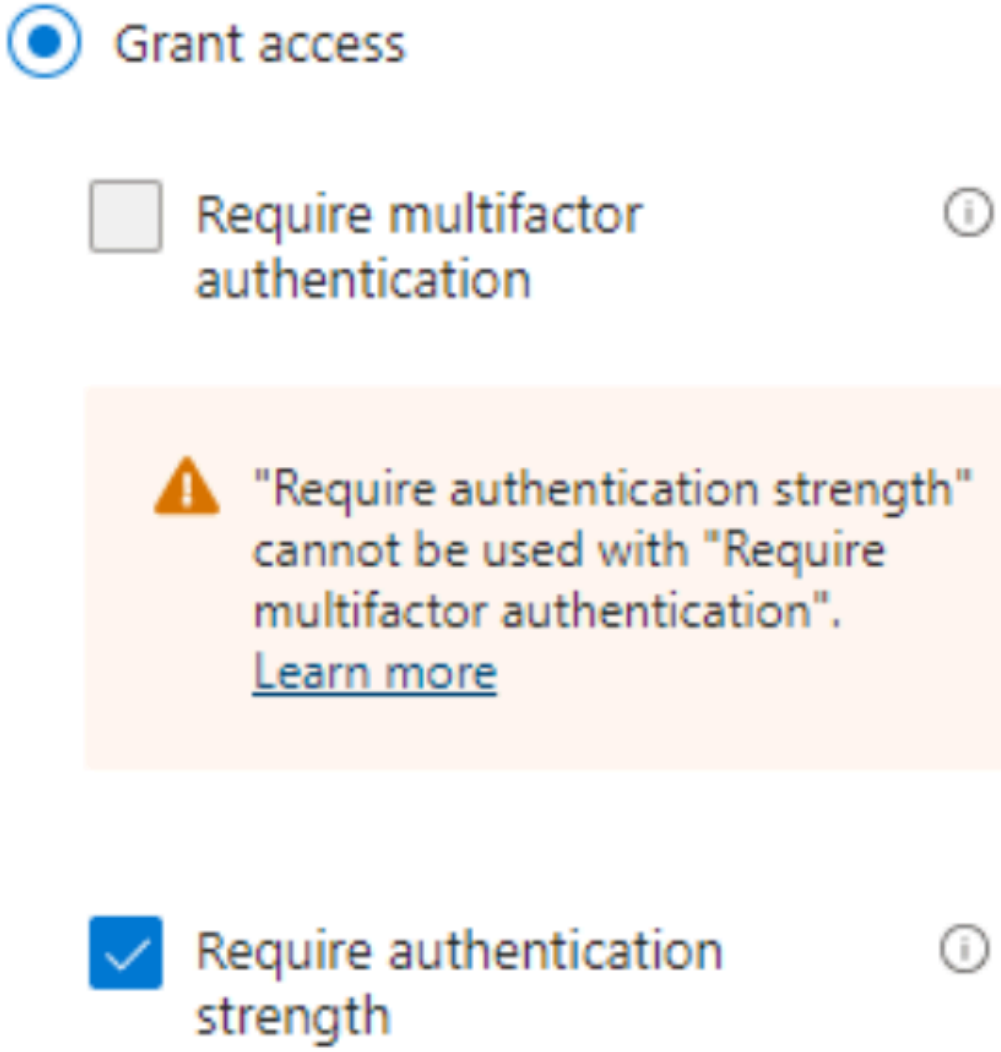
Configure Microsoft Authenticator to require number matching for push notifications.



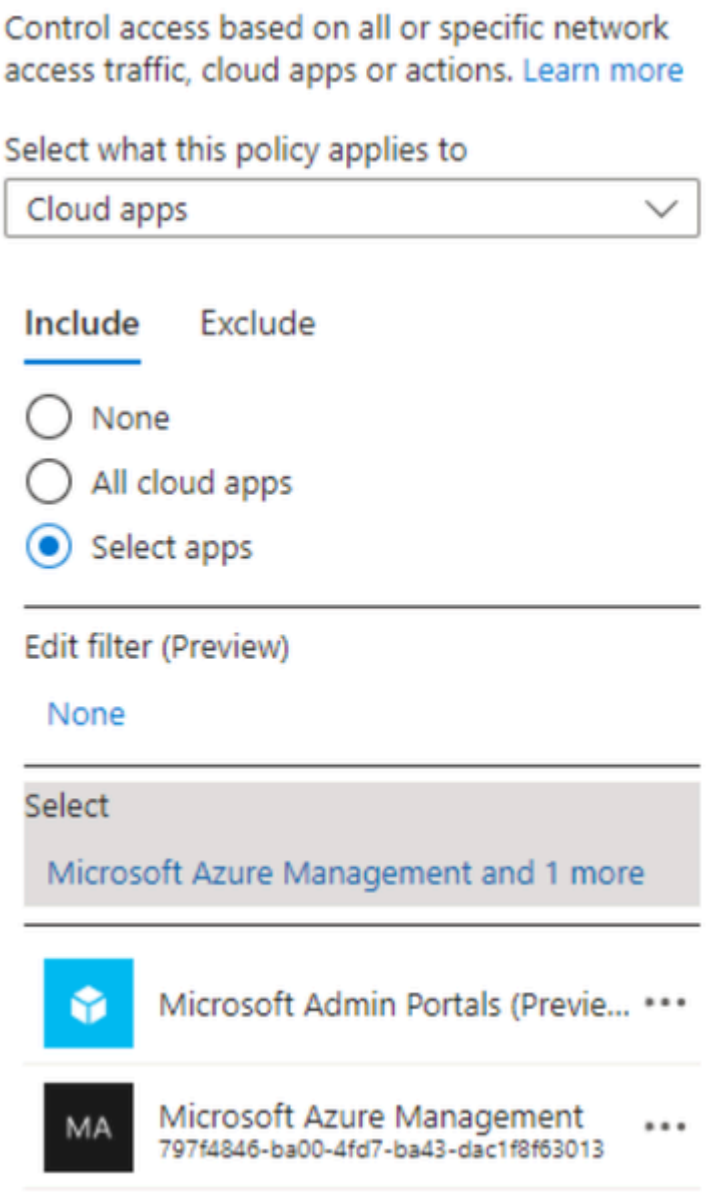
- Create a custom authentication strength that specifies **ONLY** “Password + Microsoft Authenticator (Push Notification).”



- Create a new or edit an existing Conditional Access Policy to grant access only for the newly created authentication strength.



- Ensure MFA and SSPR registration is secure by requiring the users to authenticate from a trusted network location and/or ensuring device compliance. Microsoft has documented how to accomplish this.
- Block external access to Microsoft Azure and Microsoft 365 administration features by creating a Conditional Access Policy that only allows access if users are authenticating from a trusted network location and/or ensuring device compliance. Read Microsoft's documentation for securing MFA and SSPR registration as a template, ***except*** specify specific cloud apps instead of the User action. Add the following cloud apps to include: Microsoft Admin Portals (Preview), and Microsoft Azure Management. This can also be leveraged to further secure other capabilities, such as restricting access to Graph Explorer and Microsoft Graph PowerShell.



Because UNC3944 has proven to be very prolific in using social engineering techniques with victim's help desk organizations, further securing the process of accomplishing password and/or MFA resets is imperative. An extremely effective technique that help desks should utilize prior to accomplishing password and/or MFA resets is to require video verification of the user via a video call. The help desk should verify the face of the user by comparing it to an internal system such as an HR or security badge system where a photo of the user is stored. Additionally, help desk personnel should ensure the user shows a form of identification on the video call, such as an identification badge, driver's license, etc. This process can be further customized to meet specific needs of the organization.

Mandiant plans to release additional resources that dive further into detection mechanisms, containment and eradication techniques, and additional hardening opportunities to further mitigate UNC3944 TTPs.

Appendix: Common Phishing Domain Structures

UNC3944 frequently hosts their phishing kit on domains with the following patterns.

- {}-sso.[com|net]
- sso-{}.[com|net]
- {}sso.com.[com|net]
- {}-help.com
- {}-helpdesk.com
- {}-servicedesk.com
- {}-servicenow.[com|net]
- servicenow-{}.com
- {}-internal.com
- {}-schedule.[ca|com]

Appendix: Common Tools/Software

UNC3944 frequently uses built-in tools/commands and downloads publicly available tools and software from vendor websites or GitHub repositories. The following table highlights tools of this nature that have been used by UNC3944.

Common Tools/Software Used by UNC3944	
Data Exfiltration Tools	• DropBox • filezilla • StorageExplorer • Winrar • 7-Zip • Rclone • MegaSync
Internal Reconnaissance Tools	• ADExplorer • ADRecon • Pingcastle • MicroBurst • Advanced Port Scanner
Lateral Movement Tools	• CitrixReceiver • CitrixWorkspaceApp • mobaxterm • ngrok • OpenSSH • proxifier • PuTTY / Plink

	• socat • Wstunnel • RDP • Impacket (wmiexec / smbexec) • Cloudflare Tunnel client • Chrome Remote Desktop • PsExec • Sshimpanzee
Maintain Access Tools	• Anydesk • DWAgent • Fleetdeck • Level Remote Management • Parsec • Pulseway • Remote Server Administration Tools (RSAT) • RemotePC • Rustdesk • ScreenConnect • Splashtop • Tailscale • TeamViewer • TightVNC • Twingate • N-Able
Other Utilities	• dbeaver • emeditor • git • mongodb • Postman • IISCrypto • ZipExec • moonwalk • covermyass
Privilege Escalation Tools	• GitGuardian • gosecretsdump • HashiCorp Vault • Jecretz

	• pacu • Trufflehog • secretsdump.py • Mimikatz
Scripting Tools	• python • Vmware-powercli
Web Browsers	• Chrome Portable • Edge • Firefox Portable • Librefox • Ungoogled Chromium Portable

Common publicly available tools used by UNC3944

Posted in

- Threat Intelligence
