

The SaaS and the Furious



A deep dive in SaaS compromises

Ryan Wisniewski



- **Head of Threat Operations @ Obsidian**
- **Fighter of APTs since 2011**
- **Collector of SANS Certifications**
- **User of AI Generated Headshots**

Are adversaries
targeting SaaS?

● Are adversaries targeting SaaS?

- **More use of SaaS applications means employee business accounts are being targeted for “business email compromise” (BEC).**
-

● Are adversaries targeting SaaS?

- **More use of SaaS applications means employee business accounts are being targeted for “business email compromise” (BEC).**

Business email compromise, phishing

While phishing and business email compromise remain the top tactic for threat actors, and it has become commonplace to refer to these attacks as preventable, in the case of business-led SaaS and apps outside the direct control of security teams. Often, apps that live outside of security control and technologies like [CASB](#).

Many times, business-led SaaS (formerly known as [Shadow SaaS](#)) has few instances, special users, and is typically newer SaaS technology. This prevents the typical rules, policies and enforcement from being effective against credential theft through phishing—there is no rule, tripwire, or trigger to flag anyone, the SaaS is wholly operated by the business team.

Business-led SaaS is particularly vulnerable to business email compromise because:

- a) it is the primary means of connection and communication for the user and the app,
- b) duplicate passwords (109 per user on average) means only one app or user needs to be compromised then access can proliferate, and
- c) security teams, policies, controls, and enforcements do not regularly apply to business-led SaaS

Are adversaries targeting SaaS?

- **More use of SaaS applications means employee business accounts are being targeted for “business email compromise” (BEC).**

Business email compromise, phishing

While phishing and business email compromise remain the most common types of attacks as preventable, in the case of business email compromise, security control and

- Business email compromise scams are becoming more costly for victims. The average wire transfer request in BEC attacks increased from \$48,000 in Q3 to \$75,000 in Q4.
- The financial institution, webmail and SaaS site category was the one most frequently victimized by phishing in this quarter.

... of user needs to be compromised then access can proliferate, and ... do not regularly apply to business-led SaaS

- Are adversaries targeting SaaS?

SAAS COMPROMISE = BEC

THANKS!



Contact Info:
rwisniewski@obsidiansecurity.com

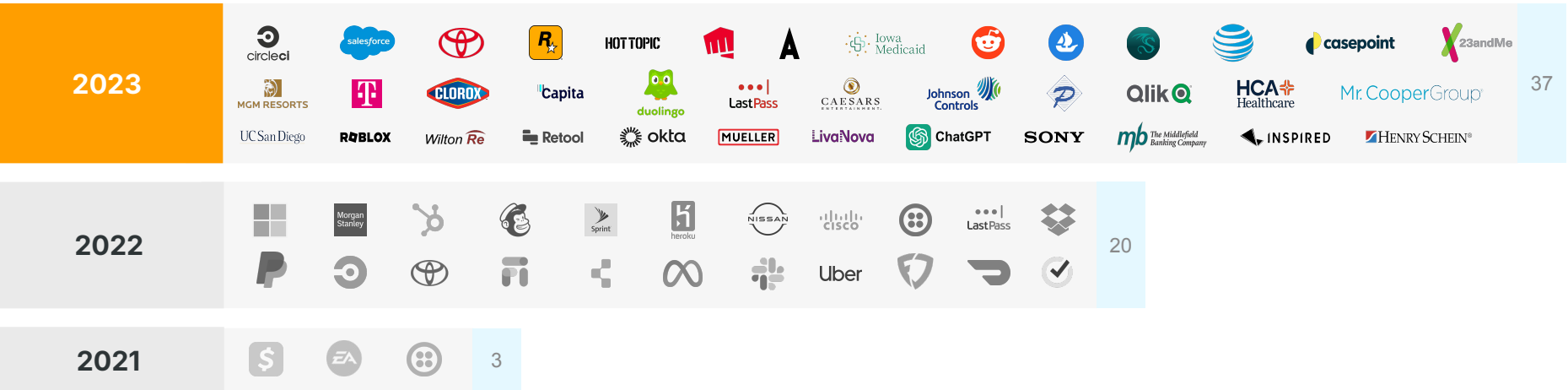


When a BEC is no longer a BEC



A deep dive in SaaS compromises

SaaS Breaches Are on the Rise



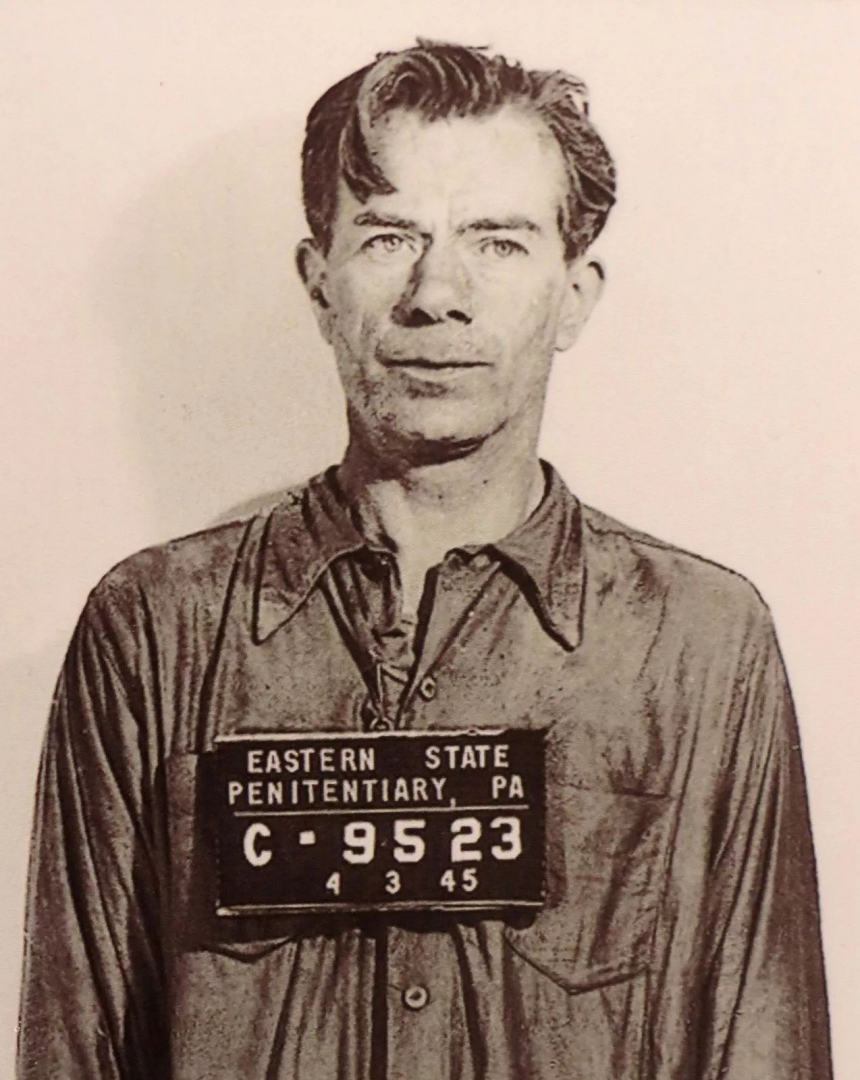
Data from [publicly disclosed](#) SaaS breaches from January 2021 through December 2023.

SaaS Breaches Are on the Rise



Are adversaries
targeting SaaS?

Why are adversaries
targeting SaaS?



**“Why do I rob
banks?...
Because that’s
where the money is”**

- William Sutton

How are they
doing it?

MATRICES

- Enterprise ▾
- PRE
- Windows
- macOS
- Linux
- Cloud ▾
- Network
- Containers
- Mobile ▾
- ICS

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

[View on the ATT&CK® Navigator](#)

[Version Permalink](#)

layout: side ▾ show sub-techniques hide sub-techniques help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (3)	Abuse Elevation Control Mechanism (3)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (3)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (8)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (3)	Account Manipulation (6)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution (14)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Boot or Logon Initialization Scripts (3)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (4)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Process (4)	Deploy Container	Input Capture (2)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)	Stage Capabilities (4)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Domain Policy Modification (2)	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Debugger Evasion	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Web Service (4)	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (15)	Escape to Host	Domain Policy Modification (2)	Multi-Factor Authentication Process (8)	Device Driver Discovery	Device Driver Discovery	Data from Information Repositories (3)	Ingress Tool Transfer	Exfiltration Over Web Service (4)	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (16)	Event Triggered Execution (16)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	File and Directory Permissions Modification (2)	Data from Local System	Multi-Stage Channels	Exfiltration Over Web Service (4)	Inhibit System Recovery
			System Services (2)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	File and Directory Discovery	Group Policy Discovery	Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Hide Artifacts (11)	Network Sniffing	Log Enumeration	Log Enumeration	Network Service Discovery	Non-Standard Port	System Shutdown/Reboot	Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Process Injection (13)	Hijack Execution Flow (12)	OS Credential Dumping (4)	Network Share Discovery	Network Sniffing	Network Share Discovery	Protocol Tunneling	System Stop	Service Stop
			Modify Authentication Process (8)	Modify Authentication Process (8)	Scheduled Task/Job (5)	Impersonation	Steal Application Access Token	Network Sniffing	Password Policy Discovery	Input Capture (4)	Traffic Signaling (2)		
			Office Application Startup (4)	Office Application Startup (4)	Valid Accounts (4)	Indicator Removal (3)	Steal or Forge Authentication Certificates	Peripheral Device Discovery	Peripheral Device Discovery	Screen Capture	Web Service (3)		
			Power Settings	Power Settings	Valid Accounts (4)	Masquerading (9)	Steal or Forge Kerberos Tickets (4)	Permission Groups Discovery (3)	Process Discovery	Video Capture			
			Pre-OS Boot (5)	Pre-OS Boot (5)	Valid Accounts (4)	Modify Authentication Process (8)	Steal Web Session Cookie	Process Discovery	Query Registry				
			Scheduled Task/Job (3)	Scheduled Task/Job (3)	Valid Accounts (4)	Modify Cloud Compute Infrastructure (3)	Unsecured Credentials (8)	Remote System Discovery	Remote System Discovery				
			Server Software Component (3)	Server Software Component (3)	Valid Accounts (4)	Modify Registry	Network Boundary Bridging (1)	Software Discovery (1)	Software Discovery (1)				
			Traffic Signaling (2)	Traffic Signaling (2)	Valid Accounts (4)	Modify System Image (2)	Obfuscated Files or Information (12)	System Information Discovery	System Information Discovery				
						Network Boundary Bridging (1)	Plist File Modification	System Location Discovery (1)	System Location Discovery (1)				
						Obfuscated Files or Information (12)	Pre-OS Boot (5)	System Network Configuration Discovery (2)	System Network Configuration Discovery (2)				
						Plist File Modification	Process Injection (12)	System Network Connections Discovery	System Network Connections Discovery				
						Pre-OS Boot (5)	Reflective Code Loading	System Owner/User Discovery	System Owner/User Discovery				
						Process Injection (12)	Rogue Domain Controller	System Service Discovery	System Service Discovery				
						Reflective Code Loading	Rootkit						
						Rogue Domain Controller	Subvert Trust Controls (4)						
						Rootkit	System Binary Proxy						
						Subvert Trust Controls (4)							
						System Binary Proxy							

Mitre ATT&CK v15 Updates for SaaS

Recon

Identify target via LinkedIn or other public information

Initial Access

Takeover target account via credential or session compromise

Persistence

Establish persistence in target account with new device registrations and defense evasion

Discovery

Build understanding of the environment and identify critical assets and additional attack paths

Privilege Escalation

Gain further access into the SaaS application landscape via additional application access and accounts

Impact

Action on objective to steal data, make fraudulent financial transactions, or disrupt operations

[T1589: Gather Victim Identity Information](#)

[T1557: Adversary-in-the-Middle](#)
[T1539: Steal Web Session](#)

[Cookie](#)
[T1566.004: Phishing - Spearphishing Voice](#)

[T1556.006: Modify Authentication Process - Multi-Factor Authentication](#)

[T1621: Multi-Factor Authentication Request Generation](#)

[T1098.005: Account Manipulation - Device Registration](#)
[T1564.008: Hide Artifacts: Email Hiding Rules](#)

[T1070.008: Indicator Removal: Clear Mailbox Data](#)

[T1556.009: Modify Authentication Process: Conditional Access Policies](#)

[T1538: Cloud Service Dashboard](#)
[T1526: Cloud Service Discovery](#)
[T1201: Password Policy Discovery](#)
[T1082: System Information Discovery](#)
[T1482: Domain Trust Discovery](#)

[T1021.007: Remote Services - Cloud Service](#)
[T1484.002: Domain or Tenant Policy Modification - Trust Modification](#)
[T1534: Internal Spearphishing](#)

[T1567: Exfiltration Over Web Service](#)
[T1021: Remote Services](#)
[T1486: Data Encrypted for Impact](#)
[T1657: Financial Theft](#)

SaaS Kill Chain

Adversaries utilize **legitimate access** and **built-in features** of SaaS applications to progress and complete their attacks

Identity



Identity Compromise

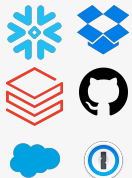
- Spear Phishing/AitM
- SSPR + SIM Swap
- Help Desk Social Engineering
- Integration Abuse
- 3rd Party Compromise

Platforms



Collaboration Spaces

- Employee Impersonation
- Sensitive Data Access
- Tracking Incident Response
- Alert Deletion/Hiding



Data Repositories

- Export Customer Reports
- Download R&D Data
- Share Private Data to Public
- Steal Credentials



Network/Compute

- Steal Credentials
- Deploy Virtual Machines
- Pivot to Internal Systems
- Expose Private Instances

Impact



- **Extortion**
 - Ransomware
 - Data Theft
- **Financial Fraud (BEC)**
- **Intellectual Theft**

Example Kill Chains



● AitM ⇒ Financial Fraud

Initial Access

Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Defense Evasion

Threat actor creates new inbox rules to hide incoming mail and deletes any security notifications in victim's inbox

Discovery

Threat actor looks through email threads to identify open invoices to modify

Impact

Threat actor sends falsified documents to recipient to perform the financial fraud



AitM ⇒ Financial Fraud

Initial Access

Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Defense Evasion

Threat actor creates new inbox rules to hide incoming mail and deletes any security notifications in victim's inbox

Discovery

Threat actor looks through email threads to identify open invoices to modify

Impact

Threat actor sends falsified documents to recipient to perform the financial fraud

The diagram illustrates the AitM attack process through five stages: Initial Access, Persistence, Defense Evasion, Discovery, and Impact. Below the timeline is a screenshot of a user's email interface. On the left, a Microsoft sign-in window is visible, indicating the user is attempting to log in. On the right, an email from the IT Compliance Team is shown, titled 'Action Required: Quarterly Compliance Report Attestation'. The email body contains a request for a 'Quarterly Compliance Report' attestation for 2024Q2, with a deadline of April 22, 2024. The email also includes a link to a 'compliance repository' and a request for confirmation by replying 'Confirmed'.

AitM ⇒ Financial Fraud

Initial Access

Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Defense Evasion

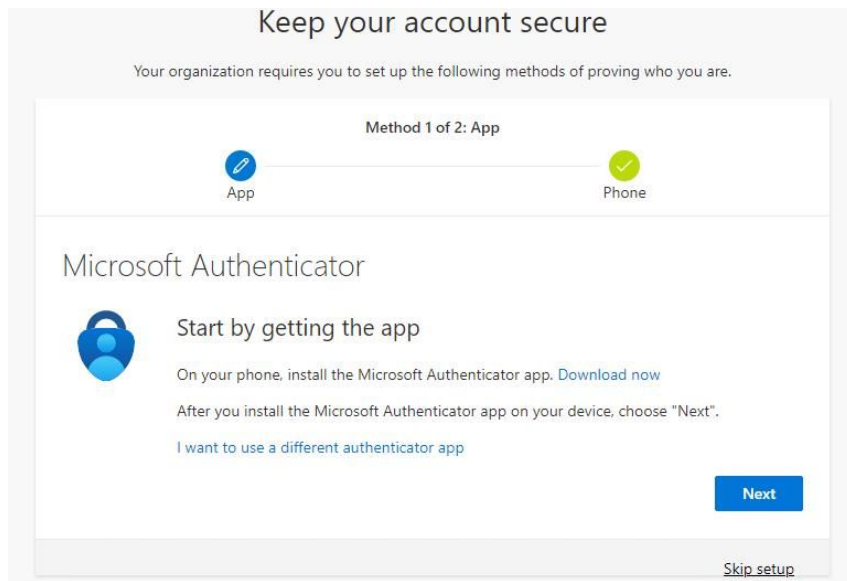
Threat actor creates new inbox rules to hide incoming mail and deletes any security notifications in victim's inbox

Discovery

Threat actor looks through email threads to identify open invoices to modify

Impact

Threat actor sends falsified documents to recipient to perform the financial fraud



● AitM ⇒ Financial Fraud

Initial Access

Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Defense Evasion

Threat actor creates new inbox rules to hide incoming mail and deletes any security notifications in victim's inbox

Discovery

Threat actor looks through email threads to identify open invoices to modify

Impact

Threat actor sends falsified documents to recipient to perform the financial fraud

The screenshot shows the Outlook interface. The 'Inbox' folder is selected in the left-hand pane. The 'Options' pane is open, showing the 'Inbox and sweep rules' section. A red callout box with the text 'To create a new rule symbol' points to the '+' icon in the 'Inbox rules' section.

Office 365 Outlook

Options

- Shortcuts
- General
- Mail
 - Automatic processing
 - Automatic replies
 - Clutter
 - Inbox and sweep rules
 - Junk email reporting
 - Mark as read
 - Message options
 - Read receipts
 - Reply settings
 - Retention policies
 - Accounts

Inbox rules

Save Discard

Choose how email will be handled. Click the "+" icon below to create a new rule.

On Name

To create a new rule symbol

● AitM ⇒ Financial Fraud

Initial Access

Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Defense Evasion

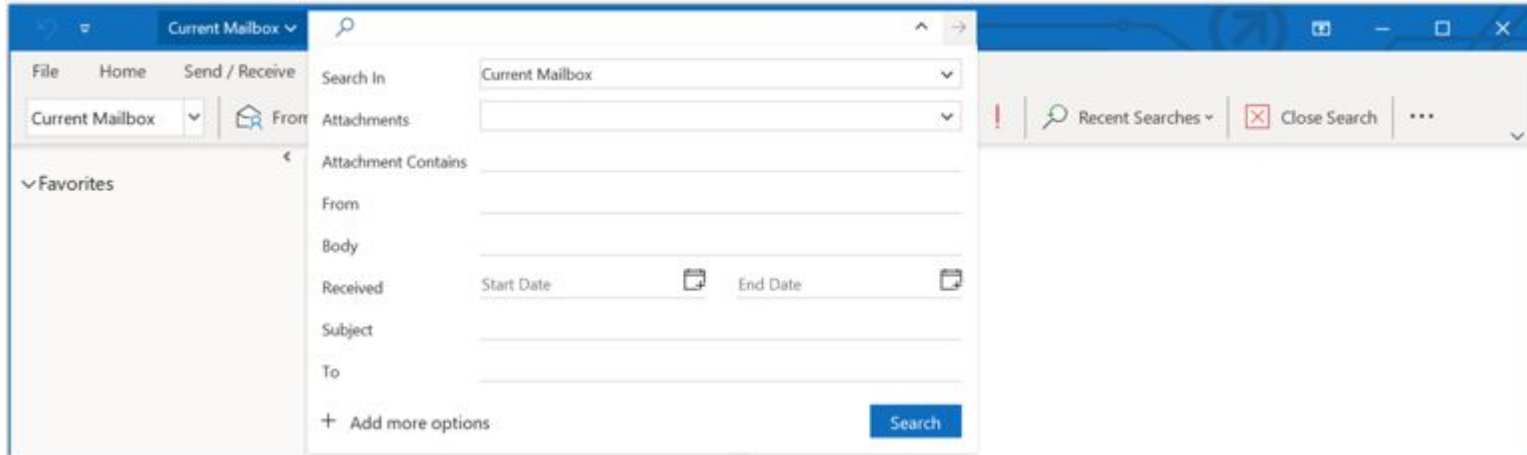
Threat actor creates new inbox rules to hide incoming mail and deletes any security notifications in victim's inbox

Discovery

Threat actor looks through email threads to identify open invoices to modify

Impact

Threat actor sends falsified documents to recipient to perform the financial fraud



AitM ⇒ Financial Fraud

Initial Access

Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Defense Evasion

Threat actor creates new inbox rules to hide incoming mail and deletes any security notifications in victim's inbox

Discovery

Threat actor looks through email threads to identify open invoices to modify

Impact

Threat actor sends falsified documents to recipient to perform the financial fraud

WIRE TRANSFER INSTRUCTIONS

If you are planning to transfer funds to UC Irvine Extension via bank wire, it is **very important** to provide the information below to your sending bank. You must also submit a completed Wire Transfer Form by fax or e-mail so that we may locate the payment. Please be sure that the conversion rate for funds satisfies the total amount to be transferred.

UCI accounts are held with Bank of America. In order to ensure the accurate and prompt accounting for funds wired to Bank of America, we ask that you please provide the following information to your sending bank.

Our Bank and City:



ABA (ACH) Routing Number:



SWIFT code:



Bank Account Name and Number:



Name of UCI Department:



Description:



SSPR ⇒ Data Exfil

Recon

Threat actor identifies target via SSPR Enumeration, LinkedIn and other public information

Initial Access

Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

Threat actor opens all applications in the SSO platform to see what they have access to

Exfiltration

Threat actor downloads, exports, or shares sensitive information outside of organization

Impact

Confidential information is sold or made public. Extortion campaigns are also common in these attacks.



SSPR ⇒ Data Exfil

Recon

Threat actor identifies target via SSPR Enumeration, LinkedIn and other public information

Initial Access

Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

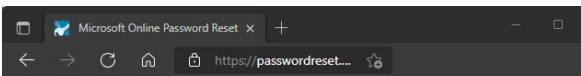
Threat actor opens all applications in the SSO platform to see what they have access to

Exfiltration

Threat actor downloads, exports, or shares sensitive information outside of organization

Impact

Confidential information is sold or made public. Extortion campaigns are also common in these attacks.



Microsoft

Get back into your account

Who are you?

To recover your account, begin by entering your email or username and the characters in the picture or audio below.

Email or Username: *

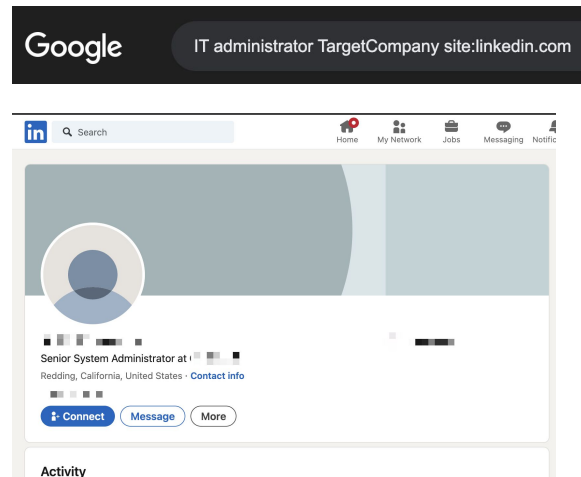
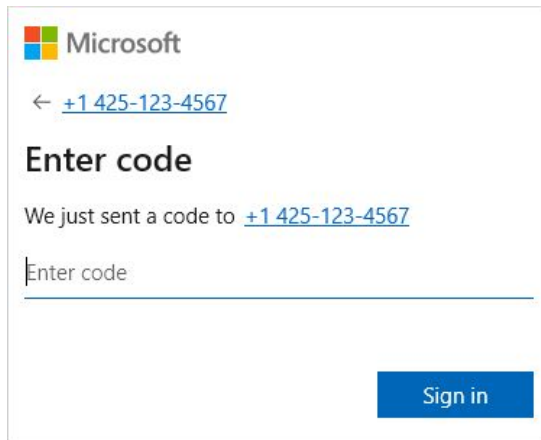
testuser@contoso.onmicrosoft.com

Example: user@contoso.onmicrosoft.com or user@contoso.com



Enter the characters in the picture or the words in the audio. *

Next Cancel



SSPR ⇒ Data Exfil

Recon

Threat actor identifies target via SSPR Enumeration, LinkedIn and other public information

Initial Access

Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

Threat actor opens all applications in the SSO platform to see what they have access to

Exfiltration

Threat actor downloads, exports, or shares sensitive information outside of organization

Impact

Confidential information is sold or made public. Extortion campaigns are also common in these attacks.

INDUSTRY NEWS • 2 min read

Telecoms Manager Admits to Taking Bribes to Help Carry Out SIM Swapping Attacks



Filip TRUŤA
March 18, 2024

Krebs on Security

In-depth security news and investigation



HOME

ABOUT THE AUTHOR

ADVERTISING/SPEAKING

Hackers Claim They Breached T-Mobile More Than 100 Times in 2022

February 28, 2023

36 Comments

The indictment states that the perpetrators in this heist stole the \$400 million in cryptocurrencies on Nov. 11, 2022 after they SIM-swapped an AT&T customer by impersonating them at a retail store using a fake ID. However, the document refers to the victim in this case only by the name "Victim 1."

SSPR ⇒ Data Exfil

Recon

Threat actor identifies target via SSPR Enumeration, LinkedIn and other public information

Initial Access

Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

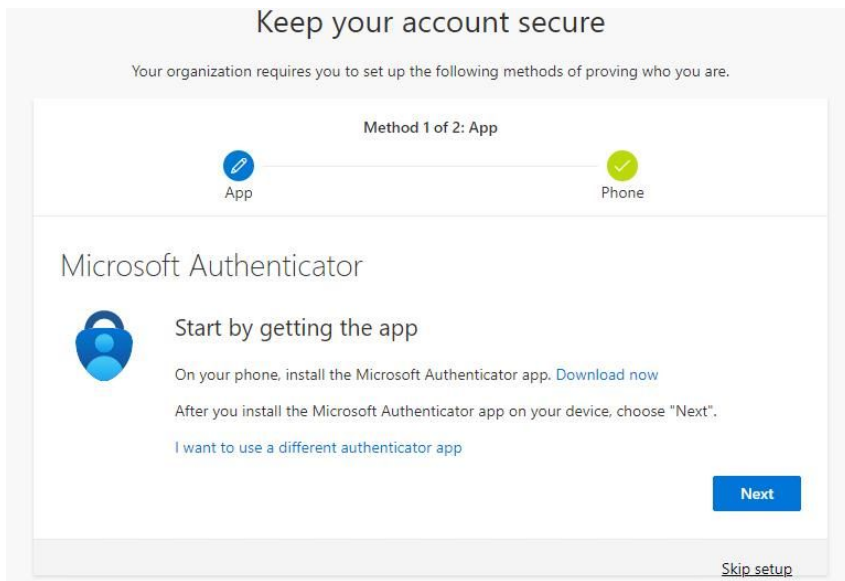
Threat actor opens all applications in the SSO platform to see what they have access to

Exfiltration

Threat actor downloads, exports, or shares sensitive information outside of organization

Impact

Confidential information is sold or made public. Extortion campaigns are also common in these attacks.



SSPR ⇒ Data Exfil

Recon

Threat actor identifies target via SSPR Enumeration, LinkedIn and other public information

Initial Access

Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

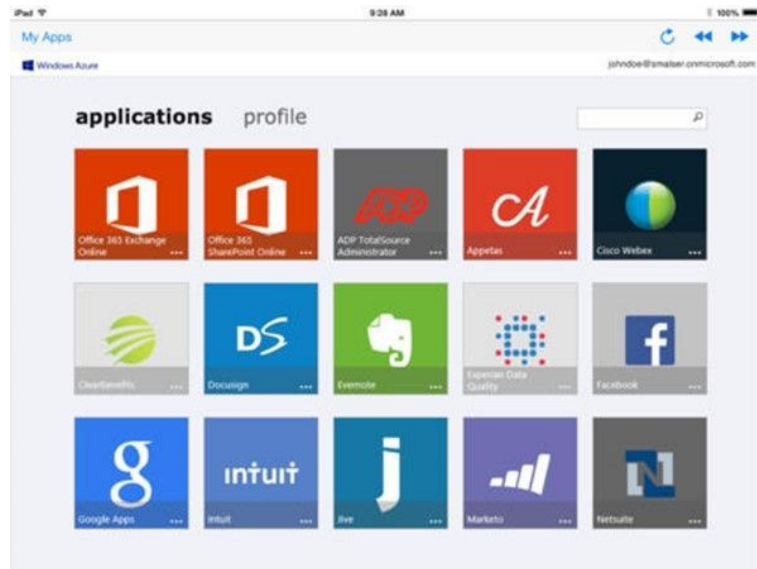
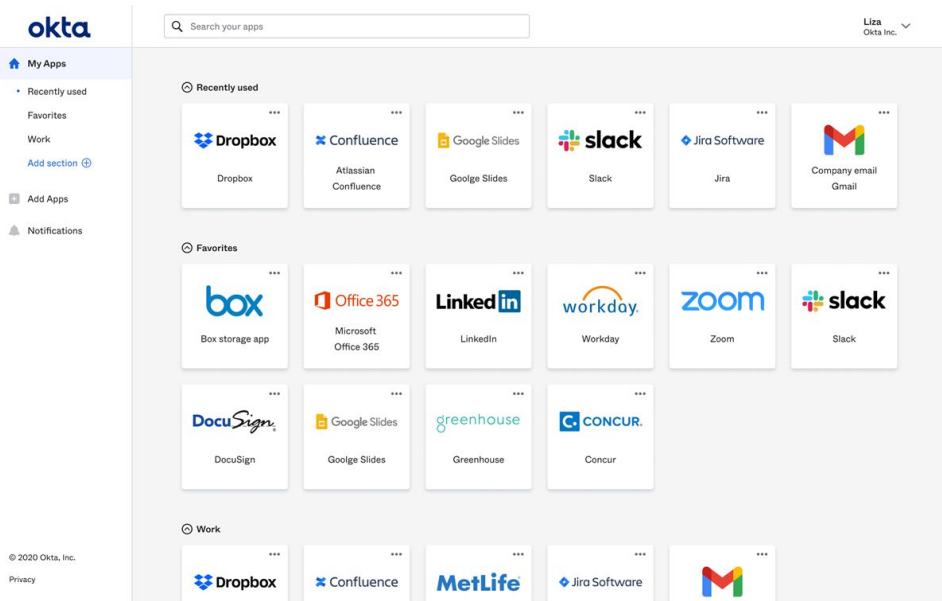
Threat actor opens all applications in the SSO platform to see what they have access to

Exfiltration

Threat actor downloads, exports, or shares sensitive information outside of organization

Impact

Confidential information is sold or made public. Extortion campaigns are also common in these attacks.



SSPR ⇒ Data Exfil

Recon

Threat actor identifies target via SSPR Enumeration, LinkedIn and other public information

Initial Access

Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

Threat actor opens all applications in the SSO platform to see what they have access to

Exfiltration

Threat actor downloads, exports, or shares sensitive information outside of organization

Impact

Confidential information is sold or made public. Extortion campaigns are also common in these attacks.

Close Month	2/1/2022	3/1/2022	4/1/2022	5/1/2022	Subscribe
Accounts Receivable					Save
Sunington Textile Corp of America	\$0.00	\$0.00	\$0.00	\$0.00	Send As
Edge Communications	\$40,000.00	\$40,000.00	\$30,000.00	\$231,000.00	Export
Logan Logistics and Transport	\$200,000.00	\$200,000.00	\$0.00	\$0.00	Delete
Cleveland	\$0.00	\$0.00	\$0.00	\$75,000.00	Add to Dashboard
Closed Hotels & Resorts Ltd	\$90,000.00	\$90,000.00	\$0.00	\$0.00	
United Oil & Gas Corp	\$0.00	\$0.00	\$710,000.00	\$25,000.00	
University of Arizona	\$10,000.00	\$10,000.00	\$90,000.00	\$0.00	
Total	\$430,000.00	\$420,000.00	\$800,000.00	\$151,000.00	\$1,820,000.00

My files > Test

Open

Preview

Share

Copy link

Manage access

Transaction Start	Transaction End	Budget	Items
		4,900,000.00	
		718,123.00	
		280,000.00	
		1,006,500.00	
		506,500.00	
		1,222,377.00	1,216,993.76

View By

- Award
- Business Document
- Grant
- Internal Service Provider
- Object Class
- Position
- Revenue Category
- Spend Category
- Supplier
- Worker

View Details

Export to Excel (All Columns)

Export to PDF

SSPR ⇒ Data Exfil

Recon

Threat actor identifies target via SSPR Enumeration, LinkedIn and other public information

Initial Access

Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

Threat actor opens all applications in the SSO platform to see what they have access to

Exfiltration

Threat actor downloads, exports, or shares sensitive information outside of organization

Impact

Confidential information is sold or made public. Extortion campaigns are also common in these attacks.

Mr. Cooper cyberattack hits every current – and former – customer

The mortgage servicer expects vendor expenses related to its response and recovery to reach \$25 million this quarter. Almost 14.7 million people were impacted.

Published Dec. 18, 2023

Security

23andMe confirms hackers stole ancestry data on 6.9 million users

Lorenzo Franceschi-Bicchierai

@lorenzofb / 11:56 AM CST • December 4, 2023



Comment



Home > News > Security > Golf gear giant Callaway data breach exposes info of 1.1 million



Golf gear giant Callaway data breach exposes info of 1.1 million

By [Bill Toulas](#)

September 1, 2023 08:43 AM 0

Medical Device Network

News |

LivaNova gives notice of personal patient data compromised by hackers

The US subsidiary of LivaNova has warned that patient contact details as well as care records could have been accessed by the malicious cyber-attack.

Joshua Silverwood | April 26, 2024

● Help Desk SE ⇒ Ransomware

Recon

Threat actor identifies target via LinkedIn and other public information

Initial Access

Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

Threat actor searches for IT documentation related to VPN, configurations, BYOD, and infrastructure

Lateral Movement

Threat actor pivots to the internal systems via VPN or virtual desktop environments

Impact

Ransomware is launched and encrypted data and systems.



Help Desk SE ⇒ Ransomware

Recon

Threat actor identifies target via LinkedIn and other public information

Initial Access

Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

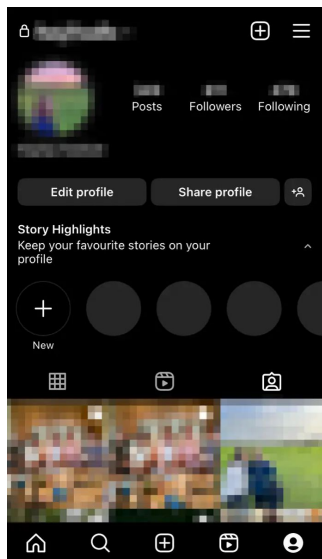
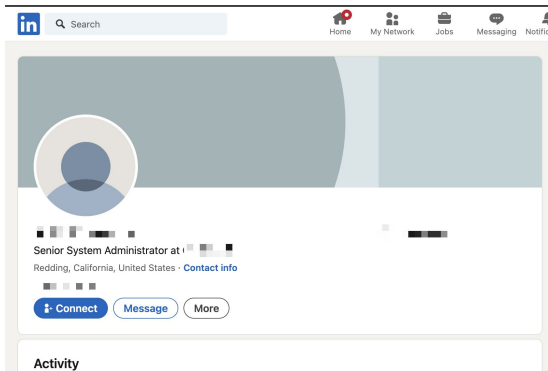
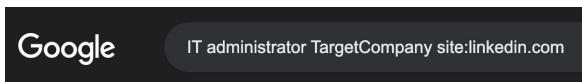
Threat actor searches for IT documentation related to VPN, configurations, BYOD, and infrastructure

Lateral Movement

Threat actor pivots to the internal systems via VPN or virtual desktop environments

Impact

Ransomware is launched and encrypted data and systems.



● Help Desk SE ⇒ Ransomware

Recon

Threat actor identifies target via LinkedIn and other public information

Initial Access

Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

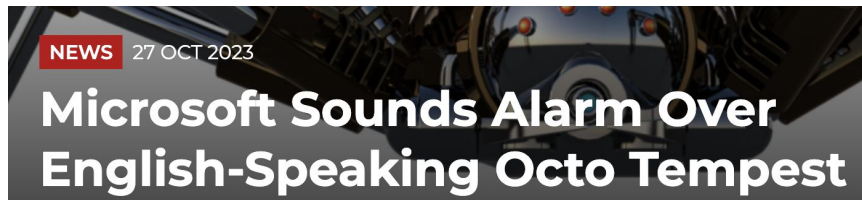
Threat actor searches for IT documentation related to VPN, configurations, BYOD, and infrastructure

Lateral Movement

Threat actor pivots to the internal systems via VPN or virtual desktop environments

Impact

Ransomware is launched and encrypted data and systems.



AI Makes Perfect Impersonations: AI Scam will hit the Help Desks

“Hey John, this is **Jerry from Systems**. I just got paged out for a **system outage** - I am **out on vacation**, but I need to get this database back up and running. I don't have any of my corporate stuff with me, but I have a laptop that I can use to access the VPN. **Can you do me a favor and reset my credentials** for me so I can resolve this storage issue before the start of business?”

● Help Desk SE ⇒ Ransomware

Recon

Threat actor identifies target via LinkedIn and other public information

Initial Access

Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

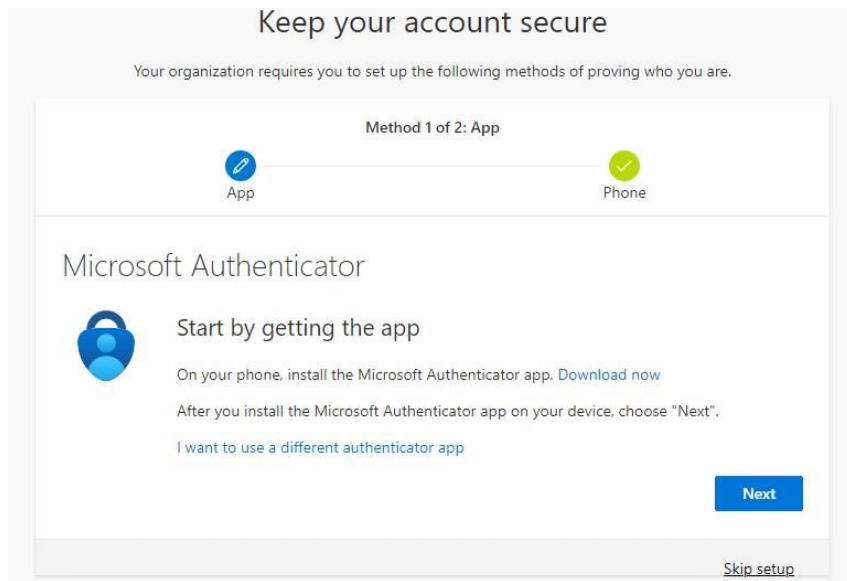
Threat actor searches for IT documentation related to VPN, configurations, BYOD, and infrastructure

Lateral Movement

Threat actor pivots to the internal systems via VPN or virtual desktop environments

Impact

Ransomware is launched and encrypted data and systems.



Help Desk SE ⇒ Ransomware

Recon

Threat actor identifies target via LinkedIn and other public information

Initial Access

Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

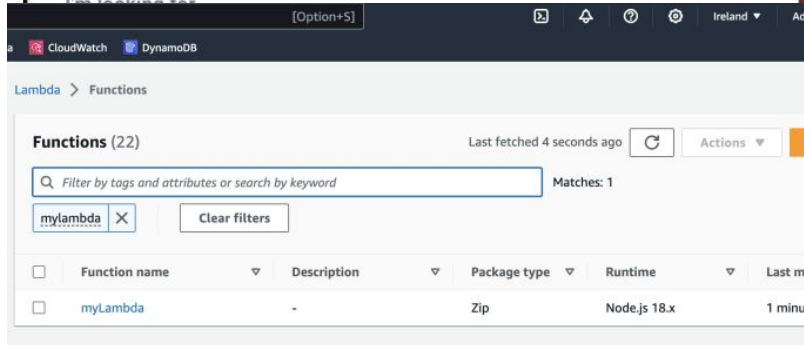
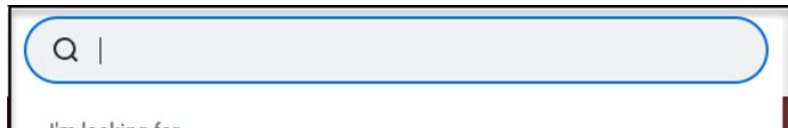
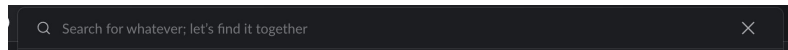
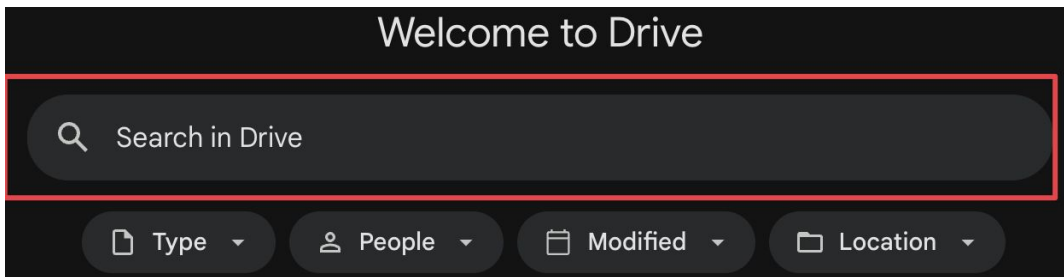
Threat actor searches for IT documentation related to VPN, configurations, BYOD, and infrastructure

Lateral Movement

Threat actor pivots to the internal systems via VPN or virtual desktop environments

Impact

Ransomware is launched and encrypted data and systems.



Help Desk SE ⇒ Ransomware

Recon

Threat actor identifies target via LinkedIn and other public information

Initial Access

Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

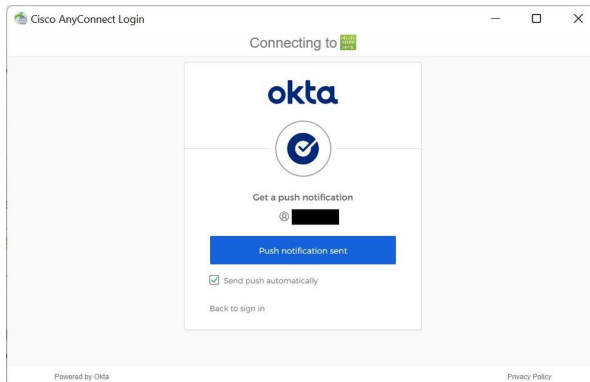
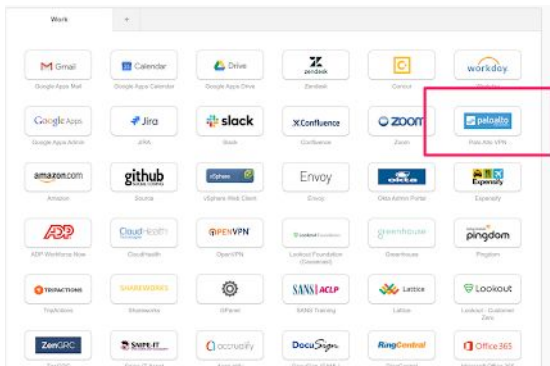
Threat actor searches for IT documentation related to VPN, configurations, BYOD, and infrastructure

Lateral Movement

Threat actor pivots to the internal systems via VPN or virtual desktop environments

Impact

Ransomware is launched and encrypted data and systems.



Microsoft
Azure Virtual Desktop



● Help Desk SE ⇒ Ransomware

Recon

Threat actor identifies target via LinkedIn and other public information

Initial Access

Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

Persistence

Threat actor registers their own MFA device, typically SMS or Authenticator App

Discovery

Threat actor searches for IT documentation related to VPN, configurations, BYOD, and infrastructure

Lateral Movement

Threat actor pivots to the internal systems via VPN or virtual desktop environments

Impact

Ransomware is launched and encrypted data and systems.

MGM Resorts ransomware attack led to \$100 million loss, data theft

By **Bill Toulas**

October 6, 2023 09:53 AM 1

VF Corp Says Data Breach Resulting From Ransomware Attack Impacts 35 Million

Apparel and footwear brands owner VF Corp shares more details on the impact of a December 2023 ransomware attack.



By **Ionut Arghire**
January 19, 2024



TECH

Caesars paid millions in ransom to cybercrime group prior to MGM hack

PUBLISHED THU, SEP 14 2023 4:29 PM EDT UPDATED FRI, SEP 15 2023 3:28 PM EDT

3C/ **Contessa Brewer**
@CONTESSABREWER

WATCH LIVE



● Key Takeaways

- **Account Takeovers** are how SaaS environments are compromised, with **AitM, SSPR+SIM Swap, and Help Desk Social Engineering** being the favorite techniques
 - Adversaries are using cloud-based identities to **gain internal access** to **both traditional data center environments and cloud/SaaS based environments**
 - Adversaries are using **residential proxies** and **personal vpn** services to **bypass conditional access policies**
 - Adversaries **almost always modify MFA devices** on the account once the account takeover is successful
 - Adversaries **hide emails and security notifications** to prevent victims from being alerted
 - Adversaries use **internal documentation** to learn about the environment and plan their attack
 - SaaS compromises are **not isolated to SaaS environments** - often they are part of a bigger kill chain
-

Recommendations to combat SaaS compromise

MFA Policy

- Require secure verification prior to allowing new MFA enrollments
- Migrate off SMS & call-based MFA methods
- Require phishing-resistant MFA methods
- Ensure MFA is required from all locations (no exceptions for on-site)
- Ensure number matching is enabled

Authentication Policy

- Reduce session lengths to limit compromise time frame
- Require the use of cloud-only accounts for privileged and break-glass accounts
- Remove inactive accounts
- Disallow service account login for accounts that do not need cloud logins

SaaS Posture and Configuration Management

- Inventory all SaaS applications in use by the organization
- Enforce a least privilege model for data access controls in SaaS applications
- Continuously monitor and manage configurations of the SaaS applications

SaaS Detection/Response Capabilities

- Monitor your SaaS identities for both posture and threat activities within SaaS compromise
 - Build response capabilities to invalidate sessions and rotate credentials within SaaS environments
-

THANKS!

Contact Info:

Ryan Wisniewski

rwisniewski@obsidiansecurity.com

