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

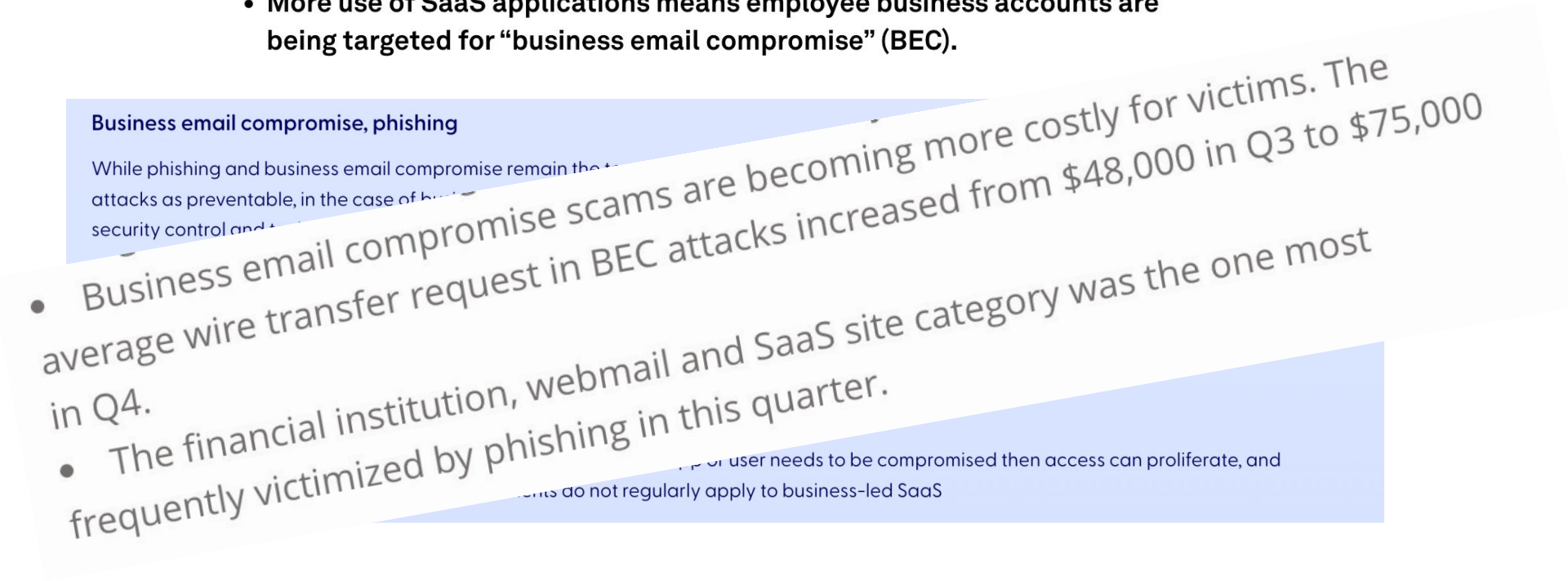
While phishing and business email compromise remain the top tactic for threat actors, and it has become commonplace to refer to these attacks as preventable, in the case of business-led SaaS and apps outside the direct control of security teams. Often, apps that live outside of security control and technologies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



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

2023		37
2022		20
2021		3

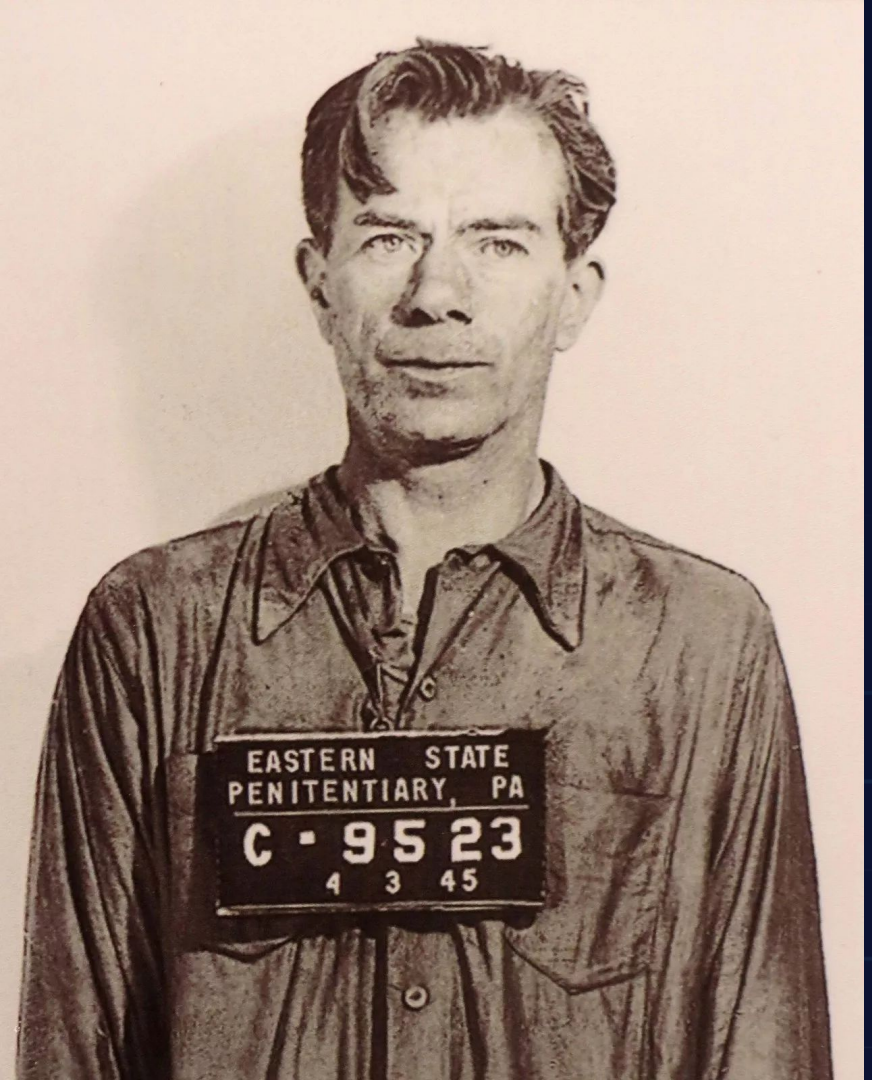
Data from publicly disclosed SaaS breaches from January 2021 through December 2023.

SaaS Breaches Are on the Rise

2024	**Can’t fit all of the logos - Need new design :(**	100+
2023		37
2022		20
2021		3

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

Mitre ATT&CK v15 Updates for SaaS

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 → **Platforms** → **Impact**

Identity Compromise

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

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

- **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

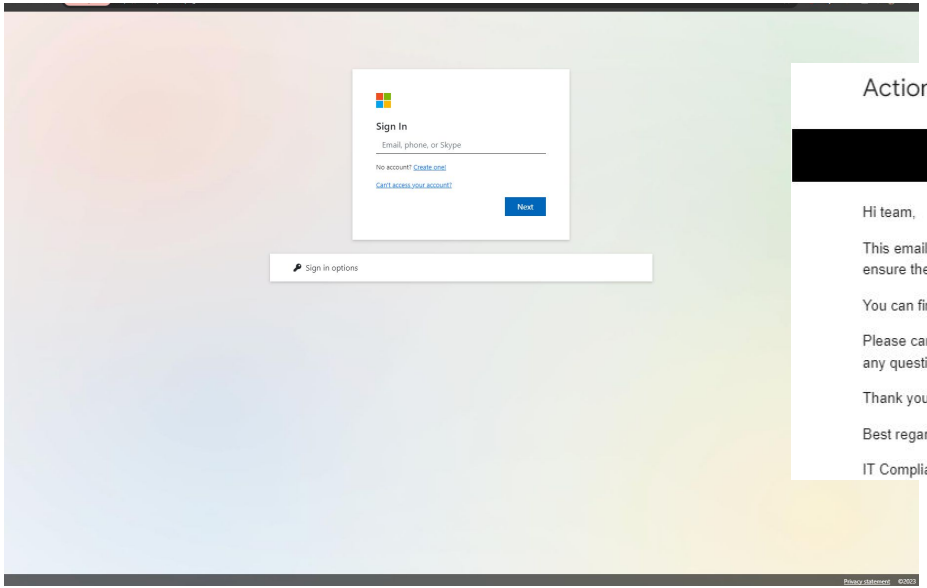
Initial Access
Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

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



AitM ⇒ Financial Fraud

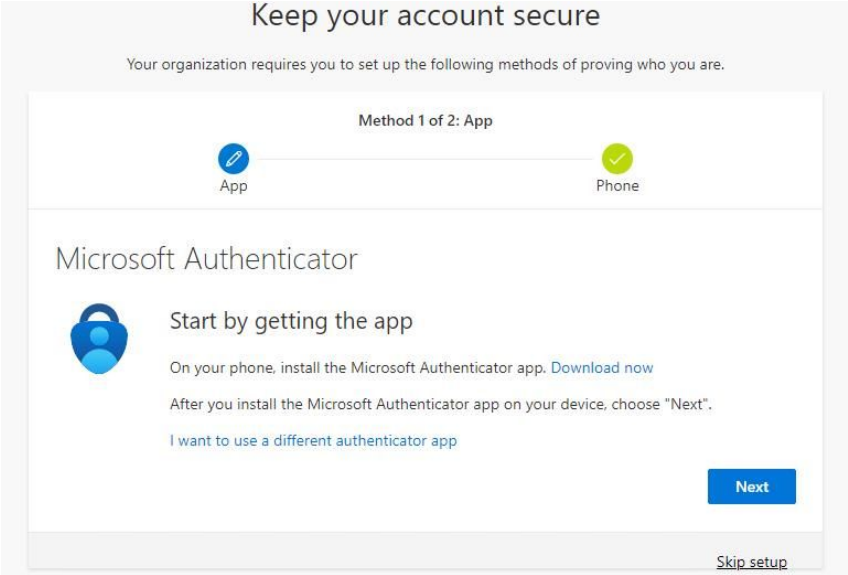
Initial Access
Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

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

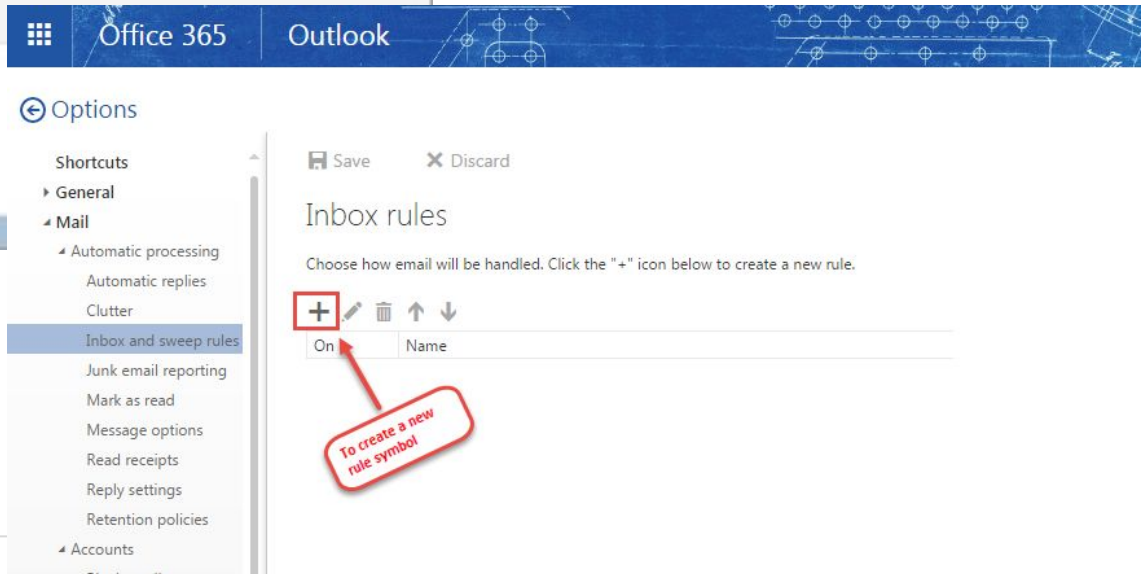
Initial Access
Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

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



AitM ⇒ Financial Fraud

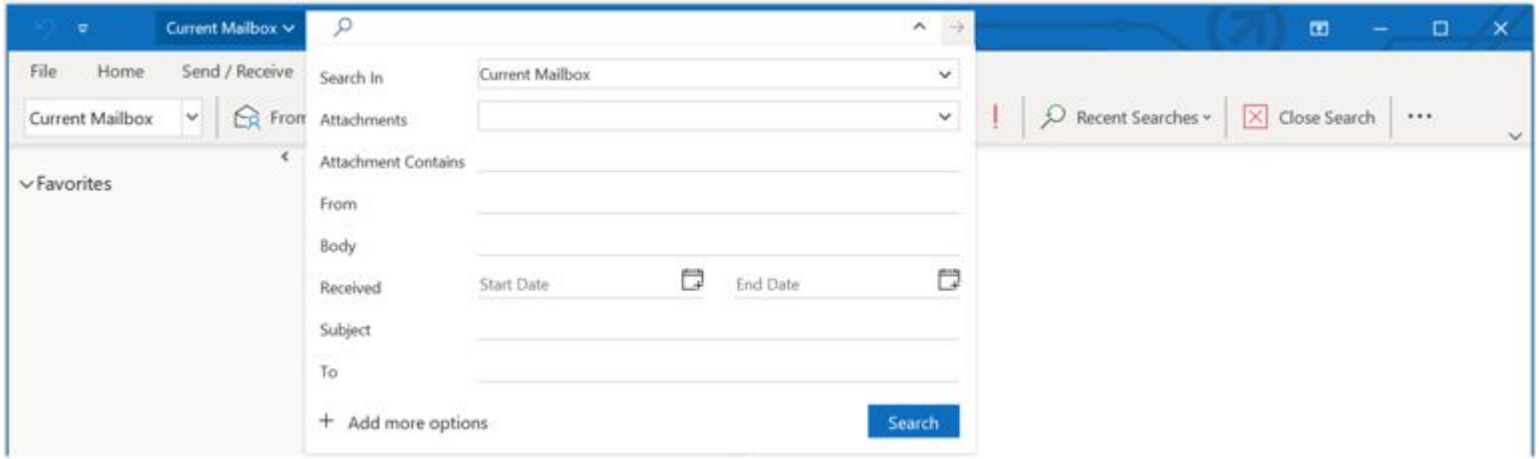
Initial Access
Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

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

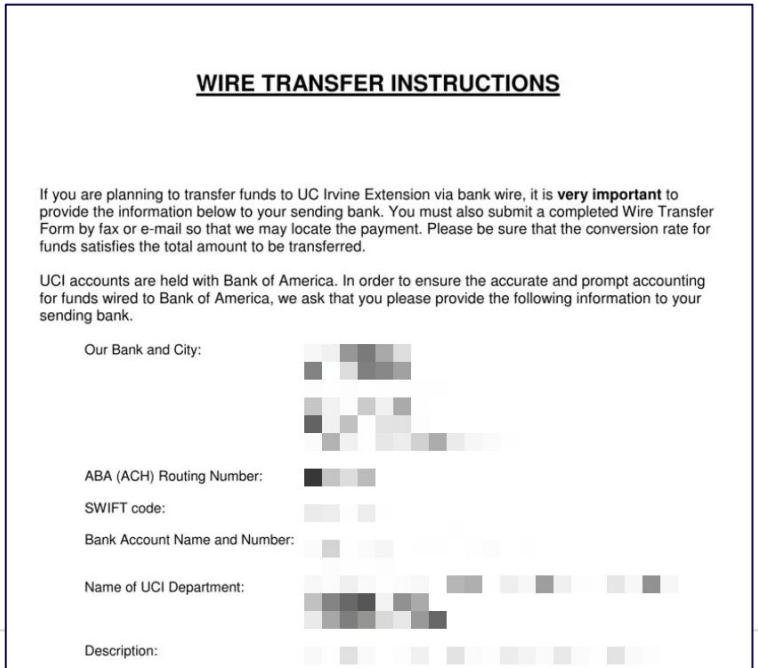
Initial Access
Threat actor phishes the user to get them to an AitM proxy (Evilginx, Tycoon, etc) and steal the session cookie

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

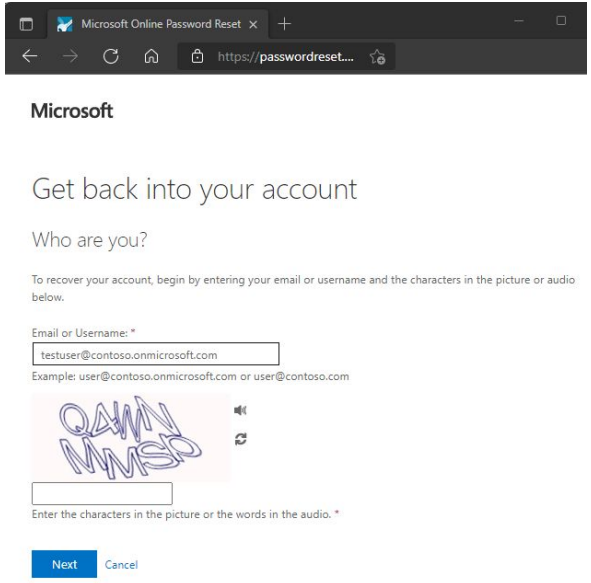
Initial Access
Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

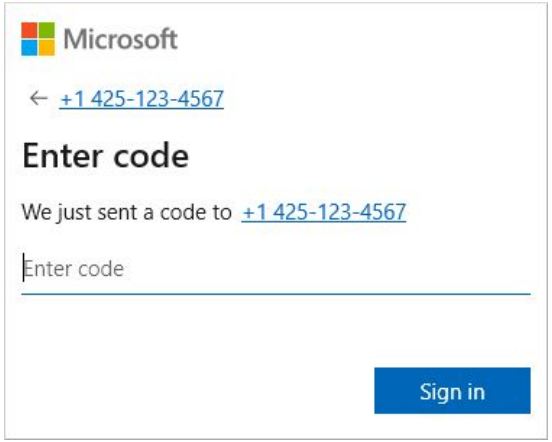
Persistence
Threat actor registers their own MFA device, typically SMS or Authenticator App

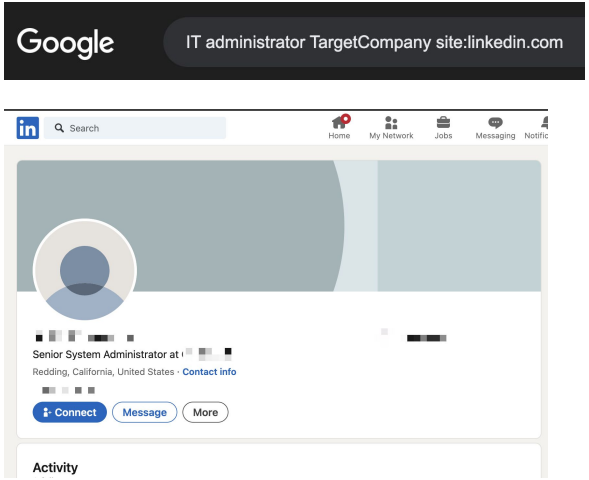
Discovery
Threat actor opens all applications in the SSO platform to see what they have access to

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.







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 TRUȚĂ
March 18, 2024

KrebsonSecurity
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

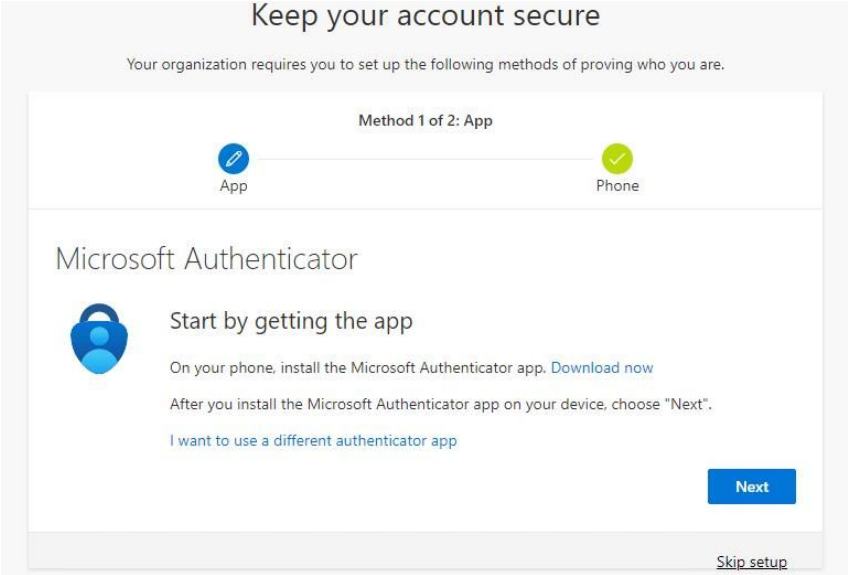
Initial Access
Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

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

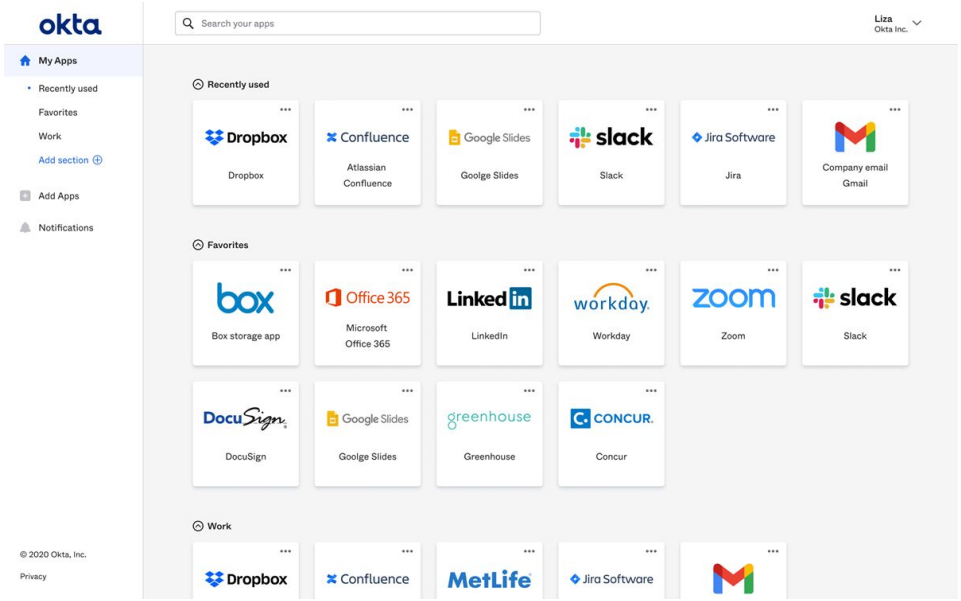
Initial Access
Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

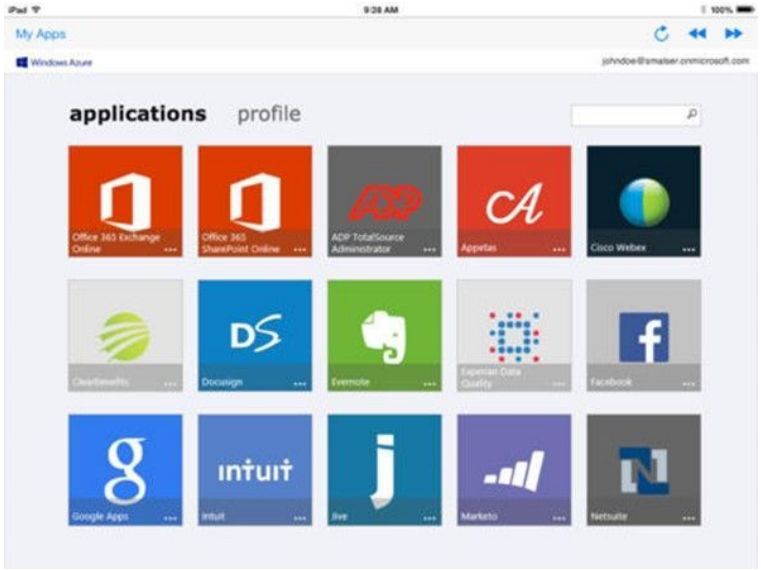
Persistence
Threat actor registers their own MFA device, typically SMS or Authenticator App

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

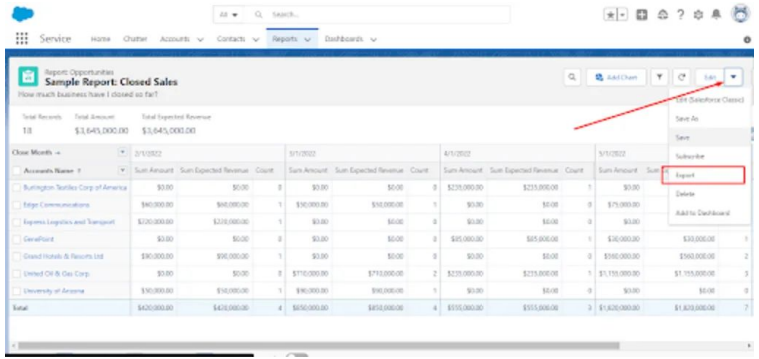
Initial Access
Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

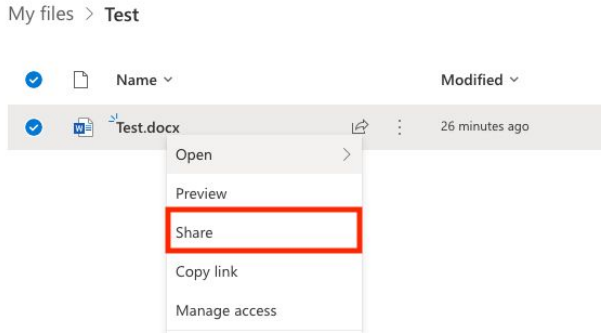
Persistence
Threat actor registers their own MFA device, typically SMS or Authenticator App

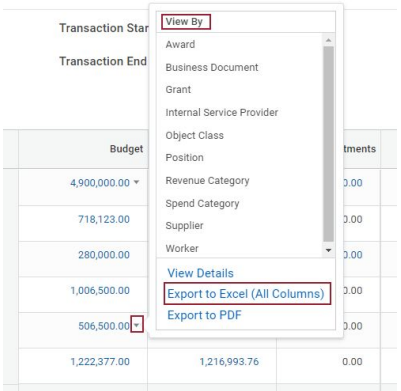
Discovery
Threat actor opens all applications in the SSO platform to see what they have access to

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.







SSPR ⇒ Data Exfil

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

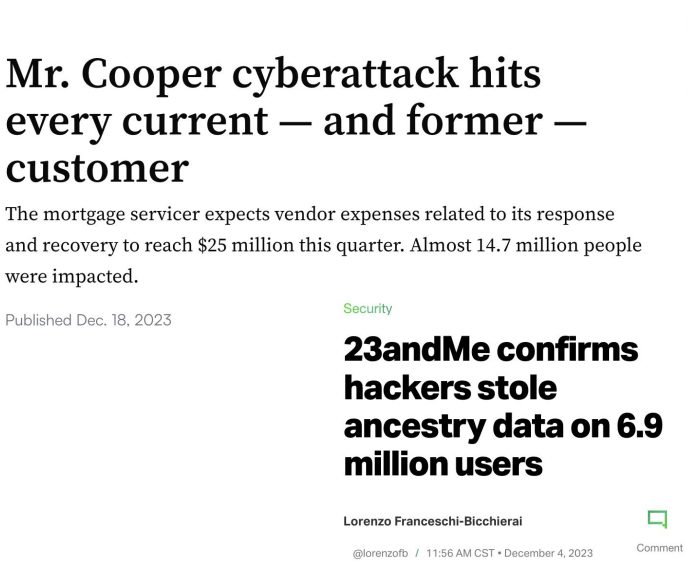
Initial Access
Threat actor performs SIM Swap and Self-Service Password to gain access to the target account

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

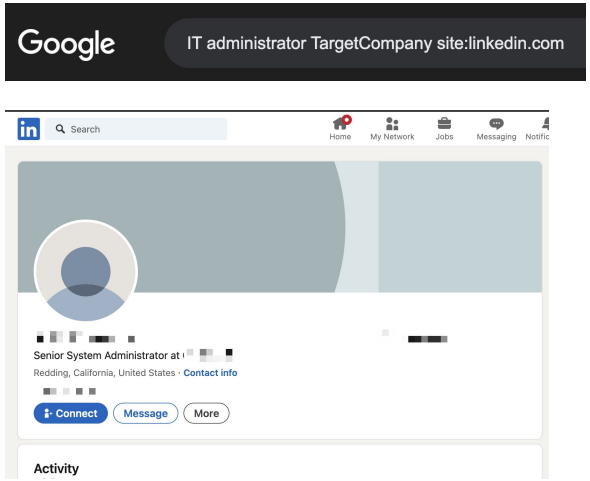
Initial Access
Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

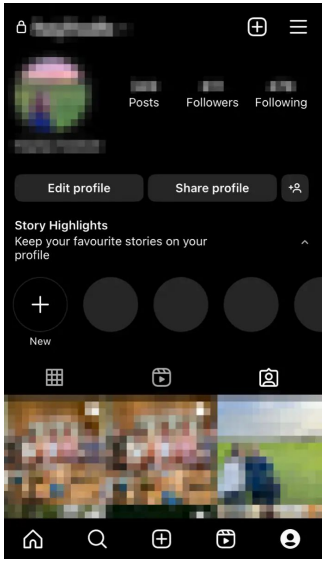
Persistence
Threat actor registers their own MFA device, typically SMS or Authenticator App

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

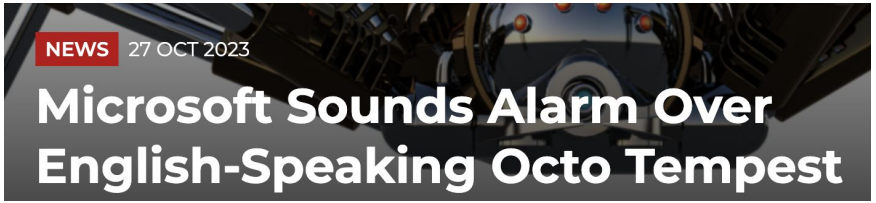
Initial Access
Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

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

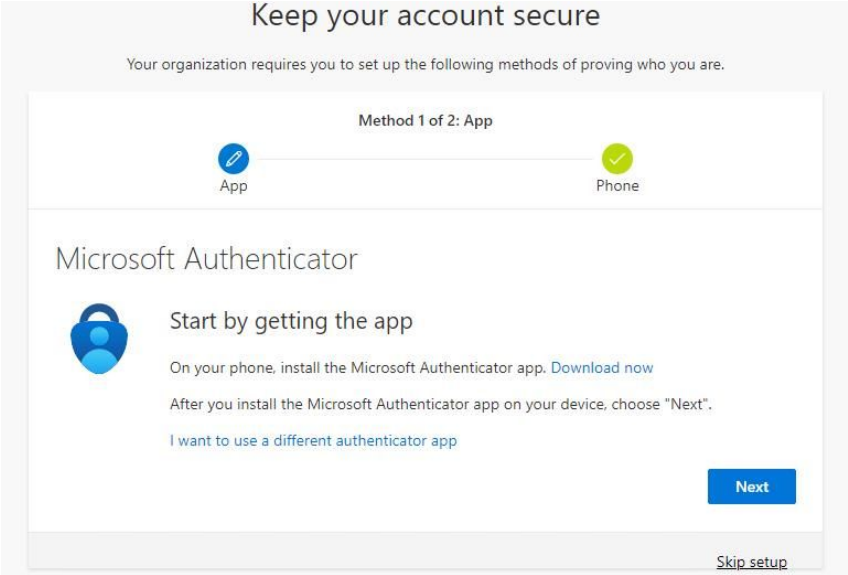
Initial Access
Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

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

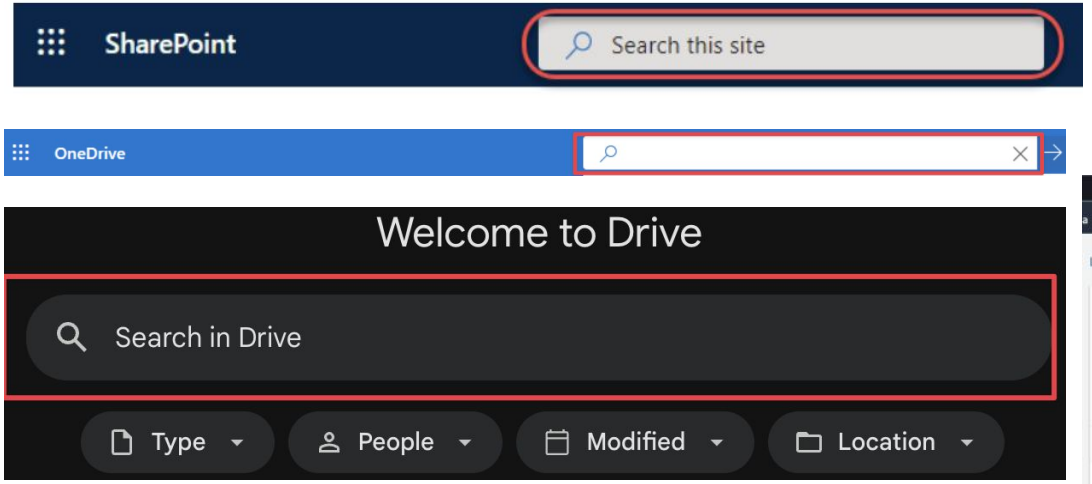
Initial Access
Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

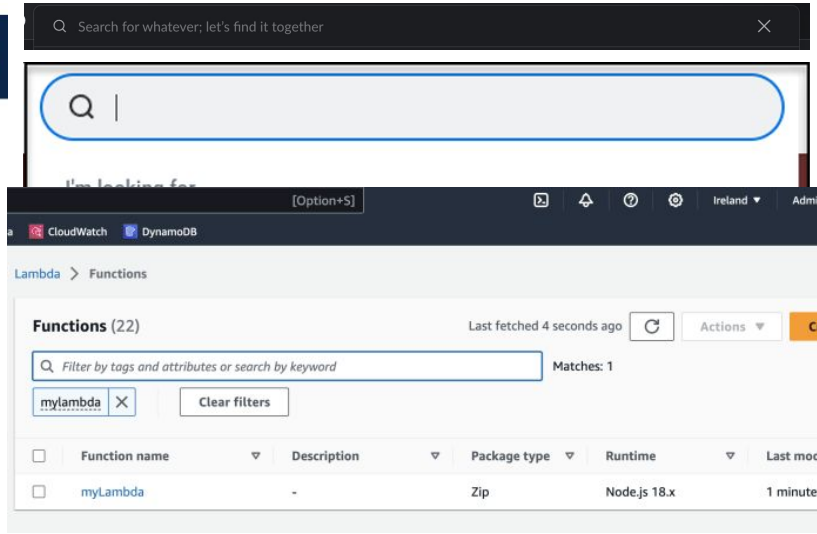
Persistence
Threat actor registers their own MFA device, typically SMS or Authenticator App

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

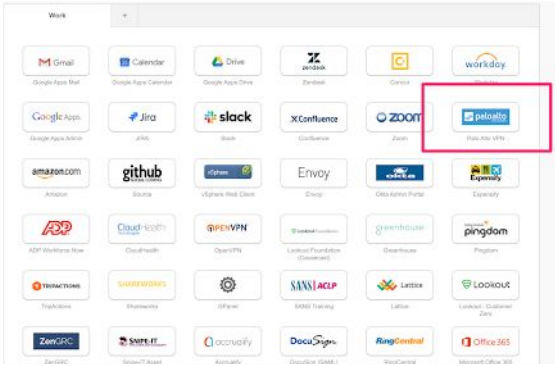
Initial Access
Threat actor calls the help desk impersonating the target requesting password reset and MFA deactivation

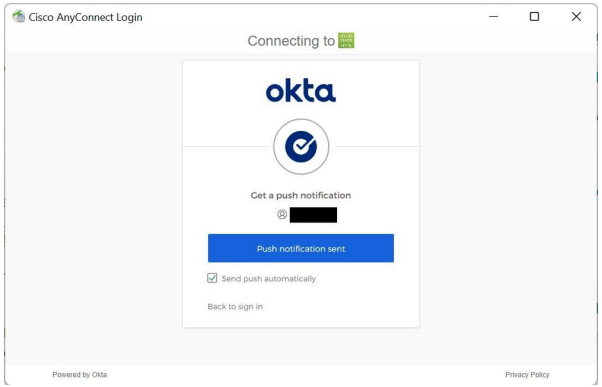
Persistence
Threat actor registers their own MFA device, typically SMS or Authenticator App

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

Citrix Virtual Apps and Desktops

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

CNBC WATCH LIVE

TECH

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

PUBLISHED THU, SEP 14 2023 1:39 PM EDT UPDATED FRI, SEP 15 2023 3:28 PM EDT

Contessa Brewer
@CONTESSABREWER

WATCH LIVE

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

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