

# NUBES DE TORMENTA

CAOS EN EL HORIZONTE DIGITAL



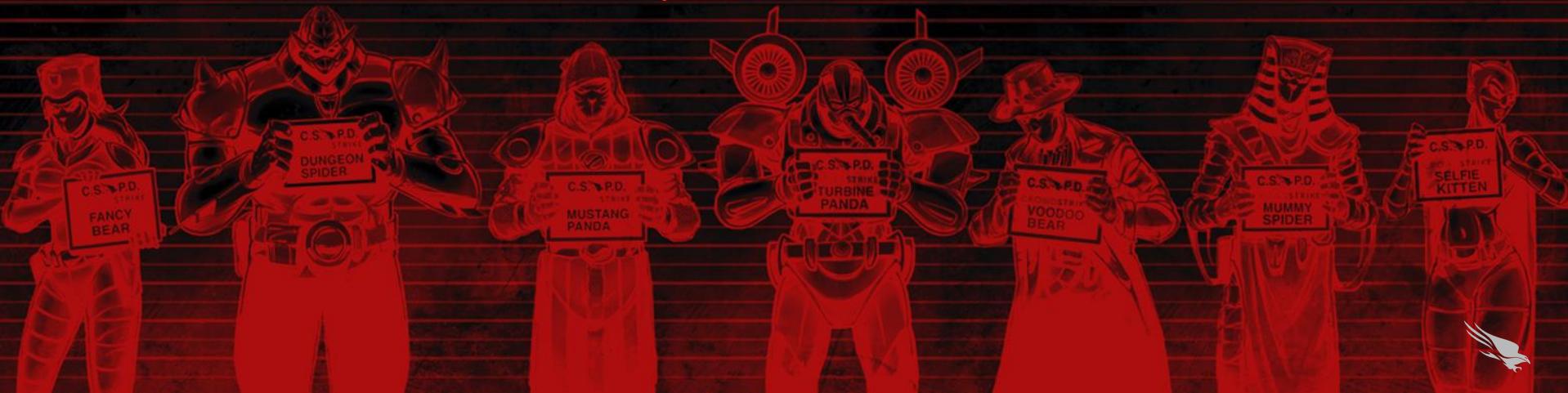
MIGUEL ANGEL DE CASTRO SIMÓN  
CROWDSTRIKE INTELLIGENCE



EMILIO RICO RUIZ  
TRC CYBERSECURITY ADVISOR

# AGENDA

- ECOSISTEMA CLOUD
- PANORAMA DE RIESGOS EN LA NUBE
- ADVERSARIO “CONSCIENTE DE LA NUBE”
- CONTRAMEDIDAS
- RECURSOS PARA ASISTENTES



# ECOSISTEMA CLOUD





## TIPOS NUBES:

- Pública, privada o híbrida



## TIPOS DE SERVICIOS

- IaaS, PaaS, SaaS y Serverless



## AMENAZAS

- Vulnerabilidades en diseño o implementación

ATAQUE  
CONFIGURACIÓN

ATAQUE  
SERVICIO



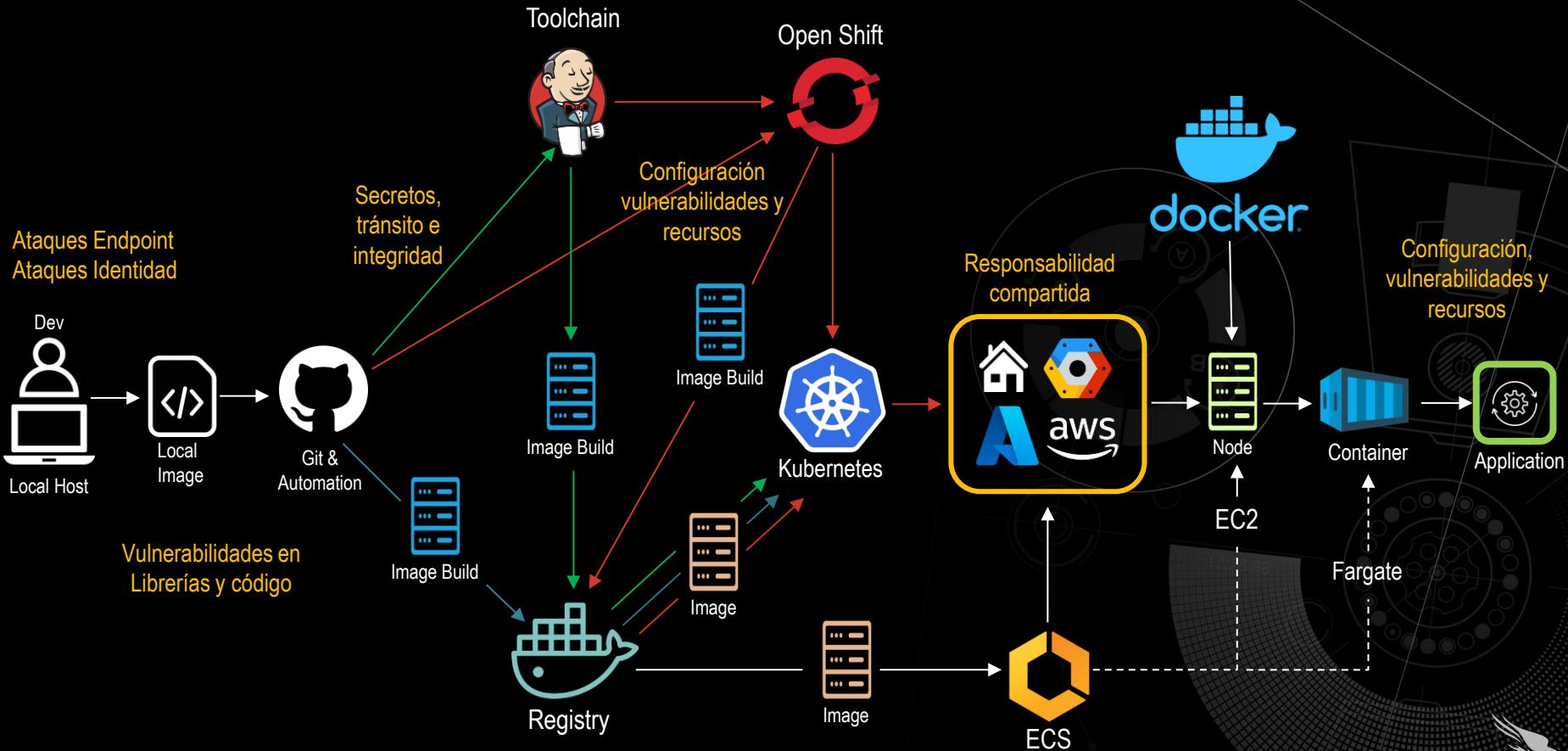


# ADOPCIÓN Y CRECIMIENTO CLOUD

- AGILIDAD, ESCALABILIDAD Y FLEXIBILIDAD
- SEGURIDAD
- COLABORACIÓN
- COSTES
- ADOPCIÓN DE LOS DEVOPS (CI/CD)



# CICLO DE VIDA DESARROLLO CLOUD





# RESPONSABILIDAD COMPARTIDA

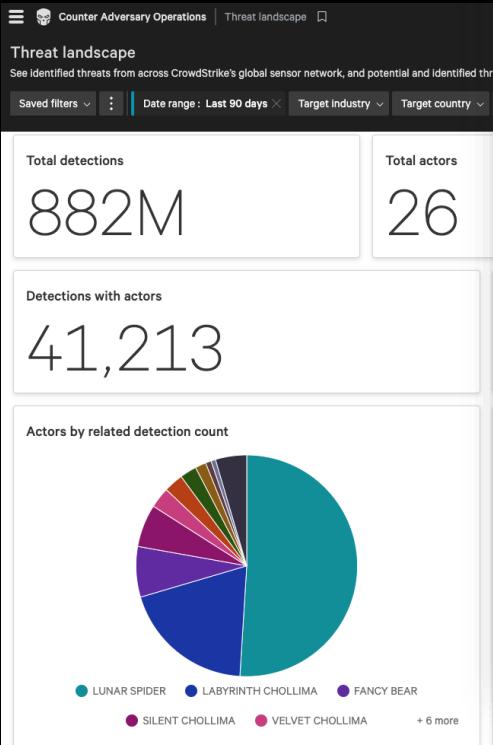


## Responsabilidades:

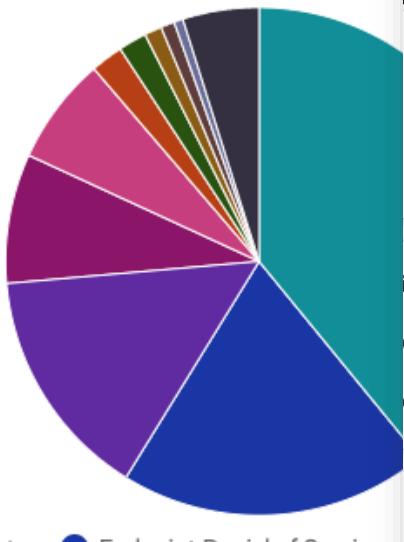
- CSP:** Parcheo e infraestructura
- Cliente:** Información, datos e identidades

# PANORAMA DE RIESGOS EN LA NUBE

# PANORAMA DE RIESGOS EN LA NUBE



## MITRE techniques by related detection count



Actor: SILENT CHOLLIMA | Malware family: XORDDoS | MITRE technique: Escape to Host

Actor	Malware family	MITRE technique	Count
SILENT CHOLLIMA	XORDDoS	Escape to Host	1,267
LUNAR SPIDER	XORDDoS	Escape to Host	529
LABYRINTH CHOLLIMA	XORDDoS	Escape to Host	190
VELVET CHOLLIMA	XORDDoS	Escape to Host	180
FANCY BEAR	XORDDoS	Escape to Host	173
WICKED PANDA	XORDDoS	Escape to Host	92
SCATTERED SPIDER	XORDDoS	Escape to Host	82
ODYSSEY SPIDER	XORDDoS	Escape to Host	43
GRACEFUL SPIDER	XORDDoS	Escape to Host	37
BITWISE SPIDER	XORDDoS	Escape to Host	36
SOLAR SPIDER	XORDDoS	Escape to Host	28

**Clear** **Apply**

# RIESGOS GLOBALES



DATOS



IDENTIDAD



APLICACIONES



CONTROLES DE RED



MIDDLEWARE

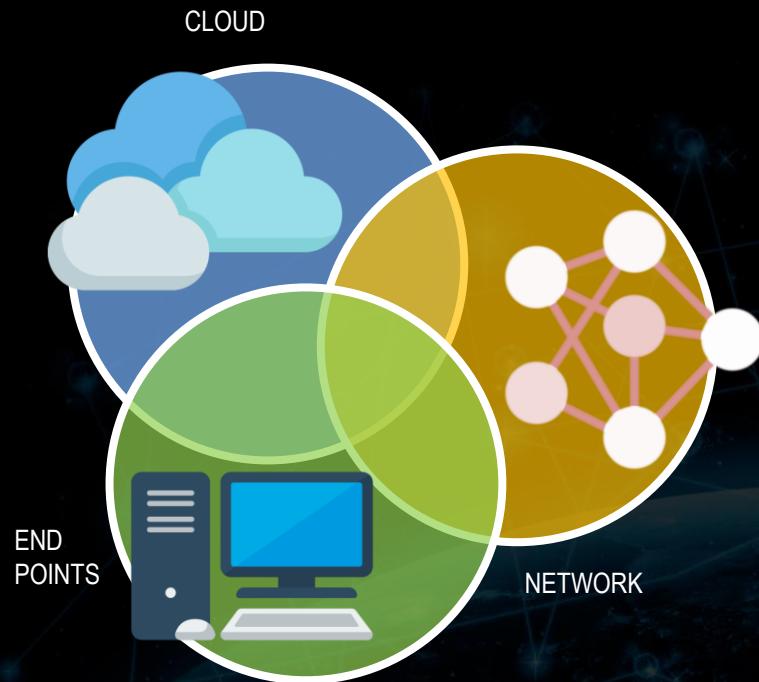


IaaS

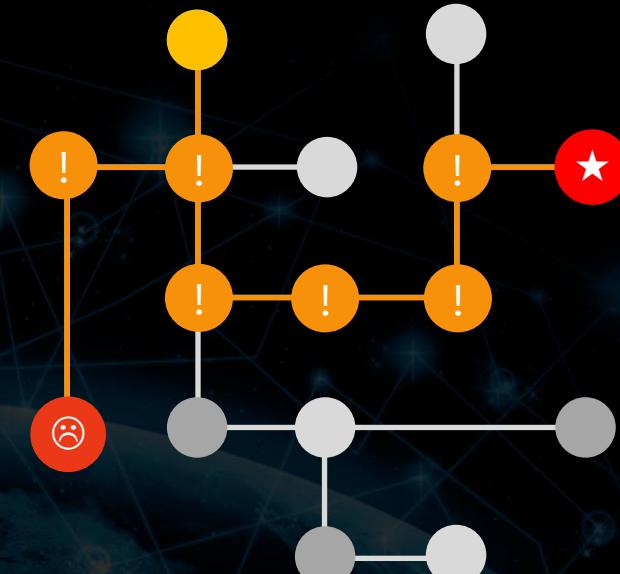


PaaS - Serverless

# PROBLEMAS AÑADIDOS



Entornos heterogéneos



Rutas de Ataque

# LA REALIDAD DE LO QUE HAY



El **65% de los repositorios** de código contenían vulnerabilidades de código fuente.  
Las vulnerabilidades permanecen **58 días**.



Las organizaciones tienen de media **351 rutas de ataque** explotables que los actores pueden aprovechar.  
Entre todas las organizaciones suman 6,3M de activos críticos.



MicroSoft descubrió **209M de identidades** en la nube de sus clientes.  
El 50% se consideraron de alto riesgo.



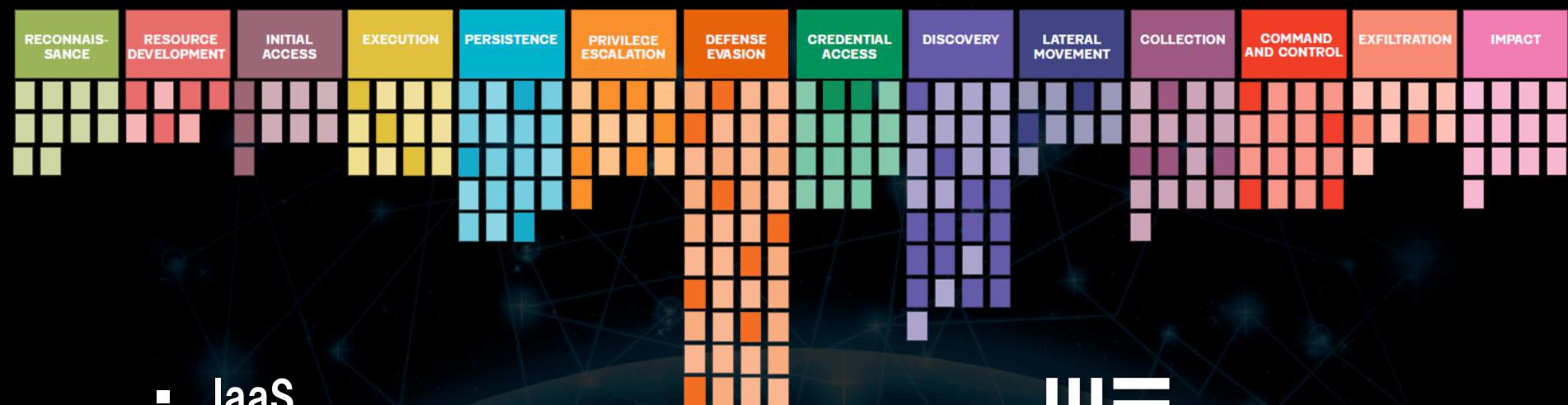
A medida que los entornos multinube crecen en escala, también lo hacen los datos y la exposición.  
En el **74%** de las ocasiones, los datos comerciales quedaron expuestos.



**59 incidentes/año** es el promedio que afrontan las empresas.  
El 25% de las vulnerabilidades de alto riesgo se explotan el mismo día de su publicación [k](#)

# CONFERENCE

# Mapping THREATS with ATT&CK®



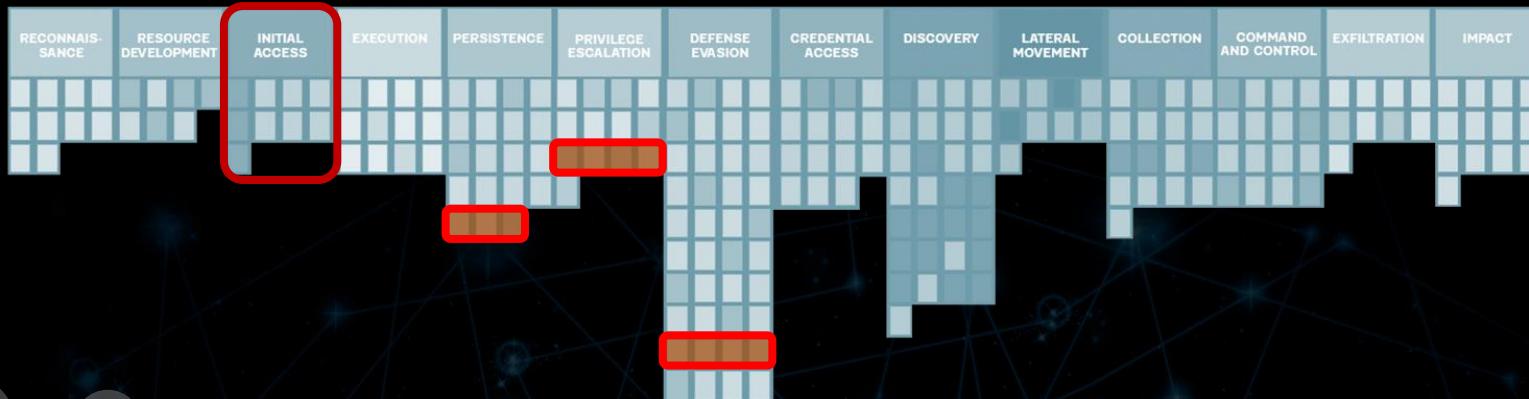
- IaaS
  - SaaS
  - Google, Amazon, MicroSoft
  - Containers



**MITRE**  
**ENGENUITY**™

# Cloud Analytic Development Blueprint

# Mapping THREATS with ATT&CK®

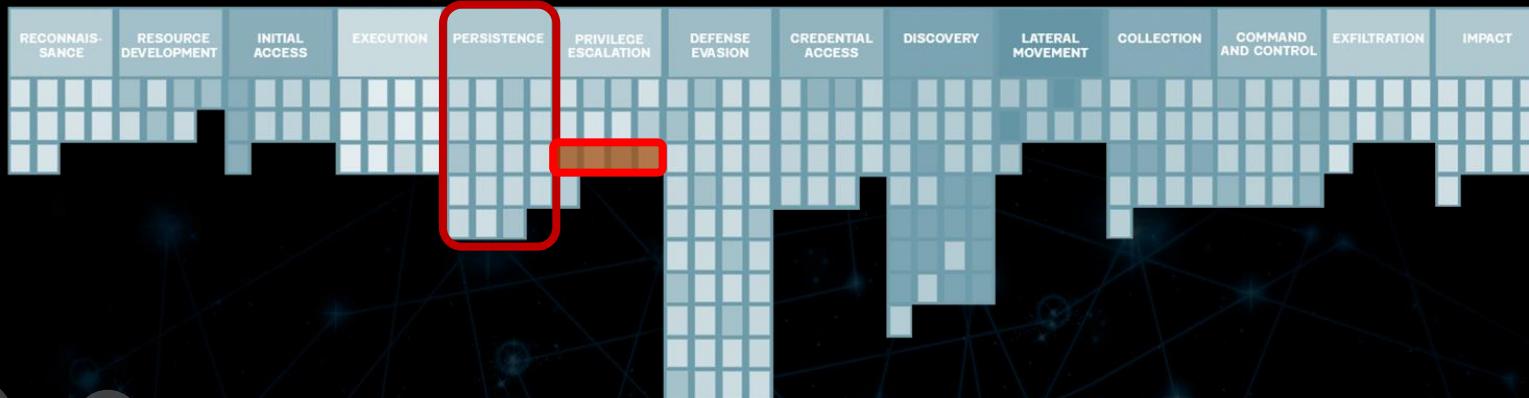


## Acceso Inicial

- CREDENCIALES VÁLIDAS (T1078): RDP, VPN, OWA, ...
  - Guest user has privileges escalated to Global Administrator
- ↳ Acceso inicial → Evasión de defensas → Persistencia → Elevación de privilegios
- (Ojo! → ¡cuentas inactivas!)



Mapping THREATS with ATT&CK®

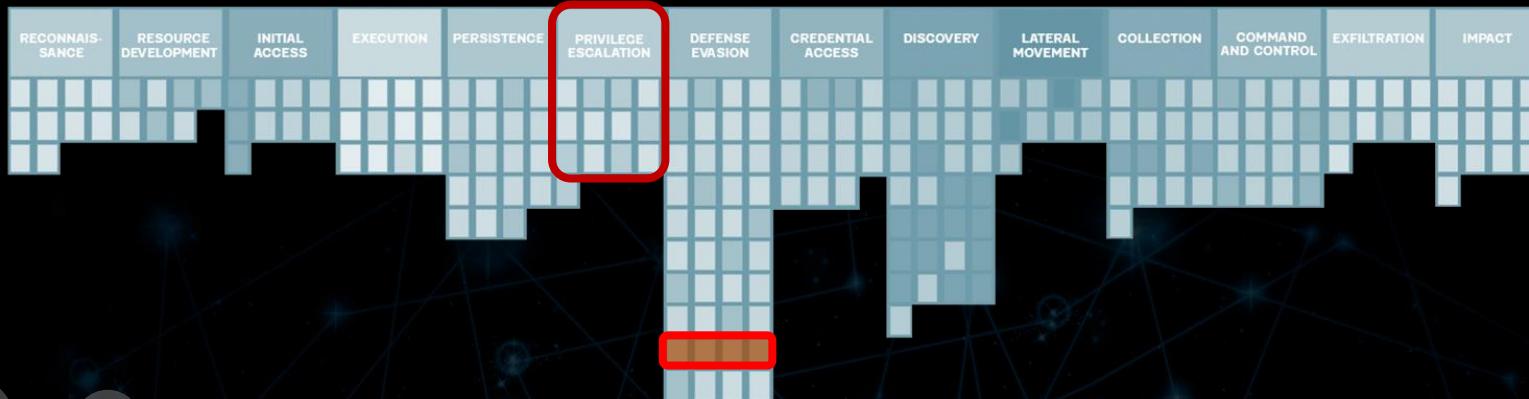


# Persistencia

- **Account Manipulation: Additional Cloud Credentials (T1098.001)**
    - Capacidad de agregar credenciales para acceso a servicios y aplicaciones (ej: SSH)
    - AWS (vía API): `CreateKeyPair`, `ImportKeyPair`, `CreateAccessKey`
    - GCP (vía comando): `gcloud iam service-accounts keys create`
  - **WEBSHELLS** para persistir.



# Mapping THREATS with ATT&CK®



## Escalada de Privilegios

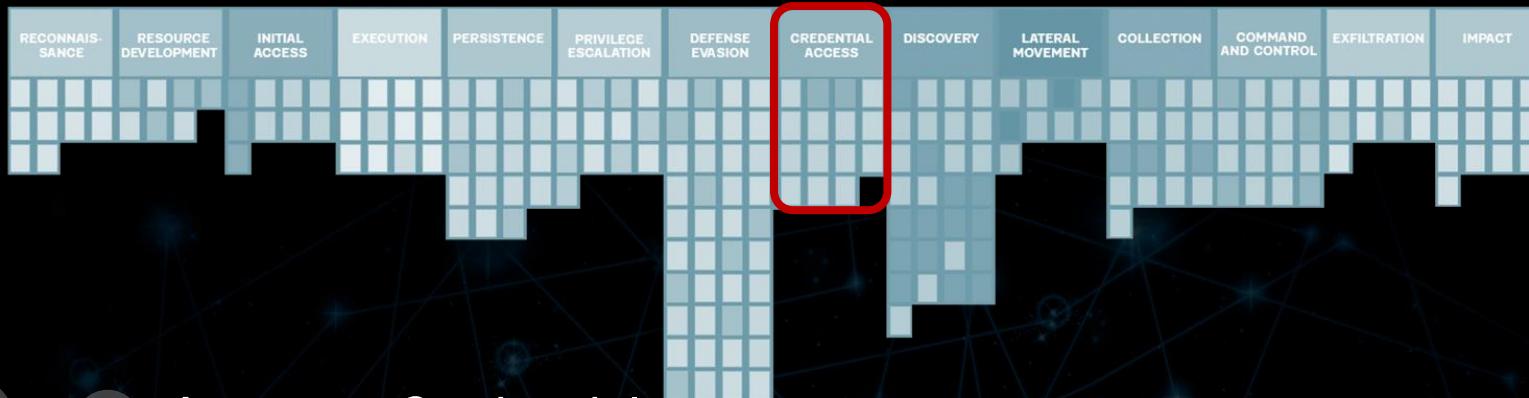
- Domain Policy Modification (T1484) & Domain Trust Modification (T1484.002)
  - Falsificación de tokens SAML sin comprometer el certificado de firma
  - Asignación de privilegios, fuera de las herramientas PIM (Privileged Identity Management)



- Escape to Host T1611



# Mapping THREATS with ATT&CK®

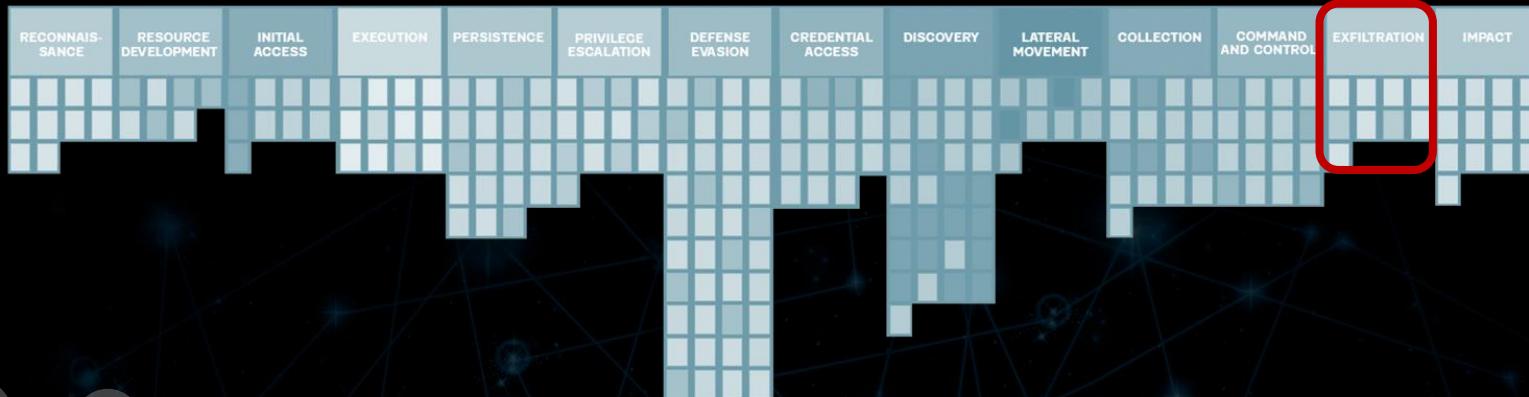


## Acceso a Credenciales

- Multi-Factor Authentication Request Generation (T1621)
  - Abuso de notificaciones push para servicios MFA → “Fatiga de FMA”
- Accesos a Almacenes de Contraseñas (Azure Key Vault)
- Posibilidad de agregar un nuevo proveedor de identidad federada (ej: Okta).



# Mapping THREATS with ATT&CK®



## Exfiltración

- Transfer Data to Cloud Account (T1537).
- Uso compartido y sincronización de datos. También creación de copias de seguridad de entornos de nube
- Mecanismos nativos para compartir datos con cuentas de adversario, con links anónimos



# Mapping THREATS with ATT&CK®



## Impacto

- Resource Hijacking (T1496)
- Minería de criptomonedas, envío de Spam, DDoS, ...
- Acciones destructivas: Eliminación de backups, datos y/o recursos.
- Robo de Información y Ransomware



# ESCAPE TO HOST

-  **ABUSO DE PRIVILEGIOS DE HOST:** APROVECHAR PERMISOS ELEVADOS EN EL CONTENEDOR PARA ACCEDER AL SISTEMA HOST SUBYACENTE.
-  **FUGAS DE INFORMACIÓN DEL HOST:** UTILIZAR ARCHIVOS O DISPOSITIVOS MONTADOS EN EL CONTENEDOR PARA EXTRAER INFORMACIÓN DEL HOST.
-  **ESCALADA DE PRIVILEGIOS:** UTILIZAR VULNERABILIDADES PARA ESCALAR PRIVILEGIOS DESDE EL CONTENEDOR AL HOST.
-  **ESCANEO Y ENUMERACIÓN DEL HOST:** REALIZAR UN ESCANEO DE LA RED Y ENUMERAR LOS SERVICIOS Y RECURSOS DISPONIBLES EN EL HOST DESDE EL CONTENEDOR.
-  **MANIPULACIÓN DE RECURSOS DEL HOST:** MODIFICAR CONFIGURACIONES O RECURSOS DEL HOST A TRAVÉS DEL CONTENEDOR.



# ESCAPE TO HOST

-  **EXPLOTACIÓN DE VULNERABILIDADES DEL KERNEL:** APROVECHAR VULNERABILIDADES EN EL KERNEL COMPARTIDO PARA ESCAPAR DEL CONTENEDOR Y ACCEDER AL HOST.
-  **ABUSO DE SOCKETS Y PIPES COMPARTIDOS:** UTILIZAR CANALES DE COMUNICACIÓN COMPARTIDOS ENTRE EL CONTENEDOR Y EL HOST PARA EJECUTAR COMANDOS O TRANSFERIR DATOS.
-  **ACCESO A ARCHIVOS SENSIBLES:** LEER O ESCRIBIR EN ARCHIVOS SENSIBLES DEL HOST QUE ESTÁN EXPUESTOS AL CONTENEDOR.
-  **INYECCIÓN DE CÓDIGO EN EL HOST:** INSERTAR CÓDIGO MALICIOSO DESDE EL CONTENEDOR PARA SER EJECUTADO EN EL HOST.
-  **EVASIÓN DE POLÍTICAS DE SEGURIDAD:** MANIPULAR POLÍTICAS DE SEGURIDAD DEL CONTENEDOR PARA GANAR ACCESO AL HOST.





ADVERSARIOS “CONSCIENTES DE LA NUBE”



# MAPPING ATTACKS

## - SCATTERED SPIDER -

# Scattered Spyder



- Adversaries
- [SCATTERED SPIDER](#)
- Last activity: Sep 2024
- Status: Active
- Origin: Unknown
- Intel reports: [204](#)
- Target industries: 22
- Target countries: 16
- Adversary type: Crime
- Motivation: [Criminal](#)
- Community identifiers:
  - Storm-0875, LUCR-3, Octo
  - Tempest, Roasted Oktapus,
  - Scatter Swine, UNC3944

# Mapping Scattered Spider with ATT&CK®

## about

## Scattered Spider

Tácticas y técnicas  
asociadas al grupo Scattered Spider

## domain

## Enterprise ATT&amp;CK v15

## platforms

Windows, Linux, macOS,  
Network, Containers, Office 365, SaaS,  
Google Workspace, IaaS, Azure AD, PRE

	Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Extrition	Account Access Removal
Gather Victim Infrastructure	Acquire	Drive-by	Command and Scripting Interpreter	BITS Job	Access Token Manipulation	Access Token Manipulation	BITS Job	Bear Trap	Application Window Discovery	Internal	Archive	Communication Through Removable Media	Data Transfer	Data Destruction
Gather Victim Accounts Application	Compromise	Container	Exploit Public-Facing Application	Administrator Command	Boot or Logon Manipulation	Account Manipulation	BITS Job	Credentials from Password Store	Browsing Information Discovery	Lateral Tool Transfer	Content Audio Capture	Exfiltration Over Alternative Protocol	Data Encrypted for Impact	
Gather Victim External Infrastructure	Compromise	External Remote Services Container	Deploy	Boot or Logon	Build	Build	Build	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over One-Click Channel	Data Manipulation
Gather Victim Device Capabilities	Device Client Execution	Exploit for Device Extenders	Exploit for Device Extenders	Boot or Logon Debugger	Image on Host	Debugger Execution	Debugger Execution	Fileless	Obfuscation Services	Browser Session Hijacking	Data Hijacking	Data Encryption	Endpoint Takeover	Other Network Medium Defacement
Privilizing Information Assets	Establish	Phishing	Inter-Process Communication	Comprehensive Host Software Binary	Create or Modify System Process	Create or Modify Credentials	Forge Web Credentials	Forge Web Credentials	Cloud Service Discovery	Propagation Through Removable Media	Clipboard Data Reception	Dynamic Physical Medium	Exfiltration Over Disk Wipe	
Search Closed Sources Capabilities	Obtain	Replication Through Removable Media	Native API	Create Account	Create or Tenant Policy Modification	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service	
Search Open Technical Databases Capabilities	Stage	Supply Chain Compromise	Scheduled Task Job	Create or Modify System Process	Escape to Host	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Scheduled Transfer	Financial Theft	
Search Open Websites Domains Capabilities	Trusted Relationship	Serviceless Execution	Event Triggered Execution	Event Triggered Execution	Domain or Tenant Policy Modification	Domain or Tenant Application Interception	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Hide Infrastructure	Transfer Data to Cloud Account	Fileware Corruption		
Search Victim-Owned Websites	Valid Accounts	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails	Execution Guardrails	Device Driver Discovery	Data from Local System	Ingress Tool Transfer	Data from Network	Multi-Stage Channels	Initiate System Recovery		
User Execution	Modify Authentication Process	Software Deployment Tools	Hijack Execution Flow	Execution Flow	Exploitation for Defense Evasion	Exploitation for Defense Evasion	OS Credential Duplication	File and Directory Discovery	Data from Shared Drive	Non-Application Removable Media	Non-Standard Port			
Windows Management Instrumentation	Instrumentation	Office Application Startup	Power Settings	Power Settings	Impersonate User	Hide Artifacts	Stale or Forge Access Tokens	Group Policy Discovery	File and Directory Discovery	Log Enumeration	Protocol Tunneling			
			PreOS Boot	Scheduled Task Job	Impersonate User	Impersonate User	Stale or Forge Kerberos Tickets	Network Service Discovery	Input Capture	Log File	Proxy			
			Server Software Component	Traffic Signaling	Indicator Removal	Indicator Removal	Stale or Forge Session Cookie	Network Share Discovery	Screen Capture	Non-Application Software	Traffic Signaling			
			Macos	Valid Accounts	Indirect Command Execution	Indirect Command Execution	Credentials	Network Sniffing	Video Capture	Non-Application Software	Web Services			
			Malicious Authentication Process		Malicious Authentication Process	Malicious Authentication Process	Password Policy Discovery	Pathshell Device Discovery		Non-Application Software				
			Malicious Cloud Compute Infrastructure		Malicious Registry	Malicious Registry	Permission Group Discovery	Process Discovery		Non-Application Software				
			Malicious System Image		Malicious System Image	Malicious System Image	Process Discovery	Query Registry		Non-Application Software				
			Network Boundary Bridging		Network Boundary Bridging	Network Boundary Bridging	Remote System Discovery			Non-Application Software				
			Obfuscation Rises or Information		Obfuscation Rises or Information	Obfuscation Rises or Information	System Information Discovery			Non-Application Software				
			Plist File Modification		Process Discovery	Process Discovery	System Location Discovery			Non-Application Software				



# OCEAN'S 11



# Mapping MGM RESORTS attack

- ③ Reset del MFA del usuario privilegiado.  
→ Atacante consigue acceso a Okta



- ④ Uso de acceso privilegiado permite comprometer más cuentas de administradores.



- ② Ataque de Vishing al helpdesk del Dpto IT  
(simulando ser un usuario privilegiado)  
Pide restablecer el MFA del usuario víctima



- ① Búsqueda en LinkedIn de personas con posible acceso a la infraestructura crítica



- ⑧ Numerosos archivos exfiltrados y sistemas críticos bloqueados por un ransomware

- ⑤ Establece cuentas de Domain Admin en los DC,s  
Agrega proveedor de identidad federado al tenant de la víctima  
El nuevo IdP tiene acceso completo a los sistemas de autorización de MGM

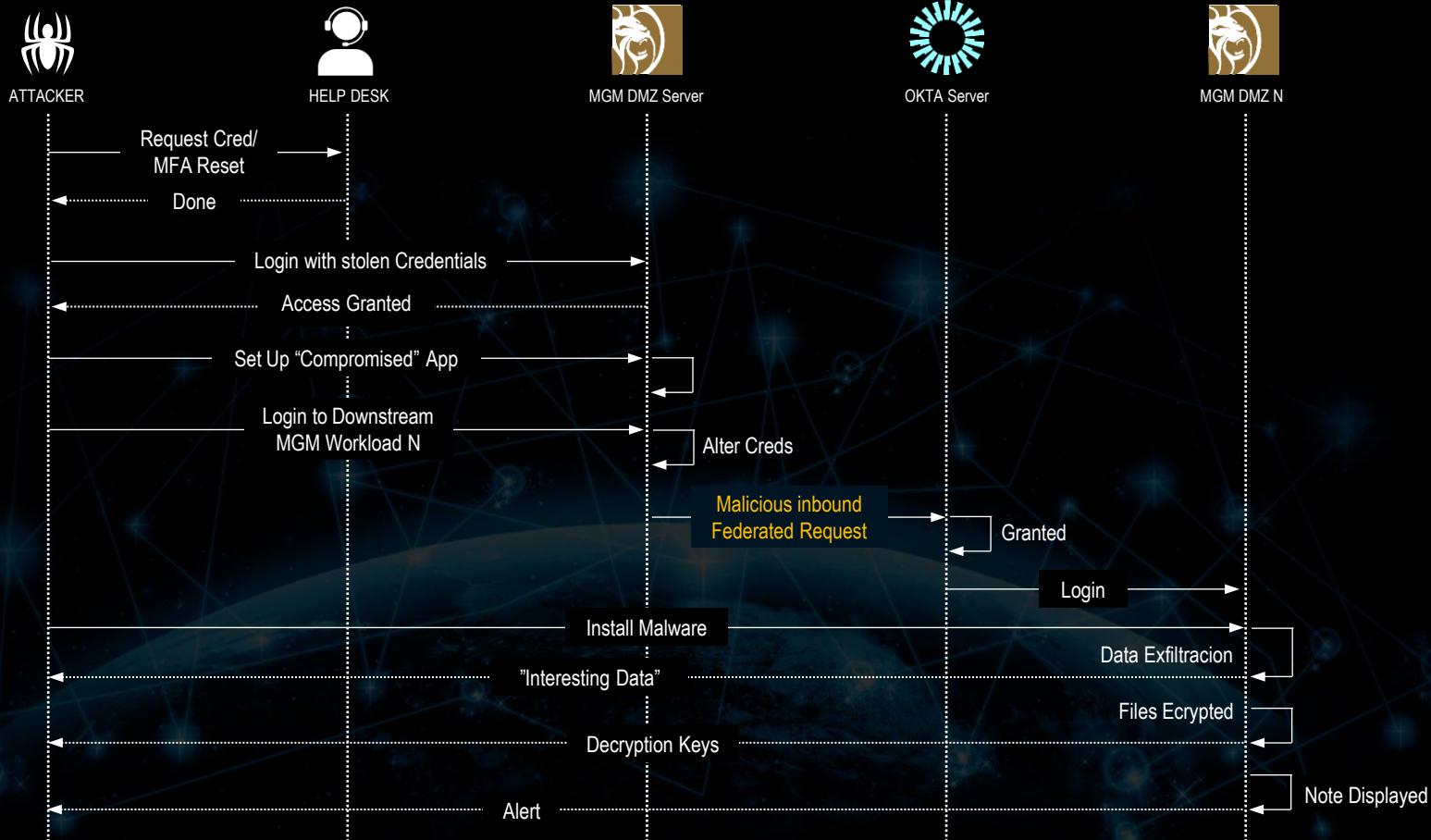


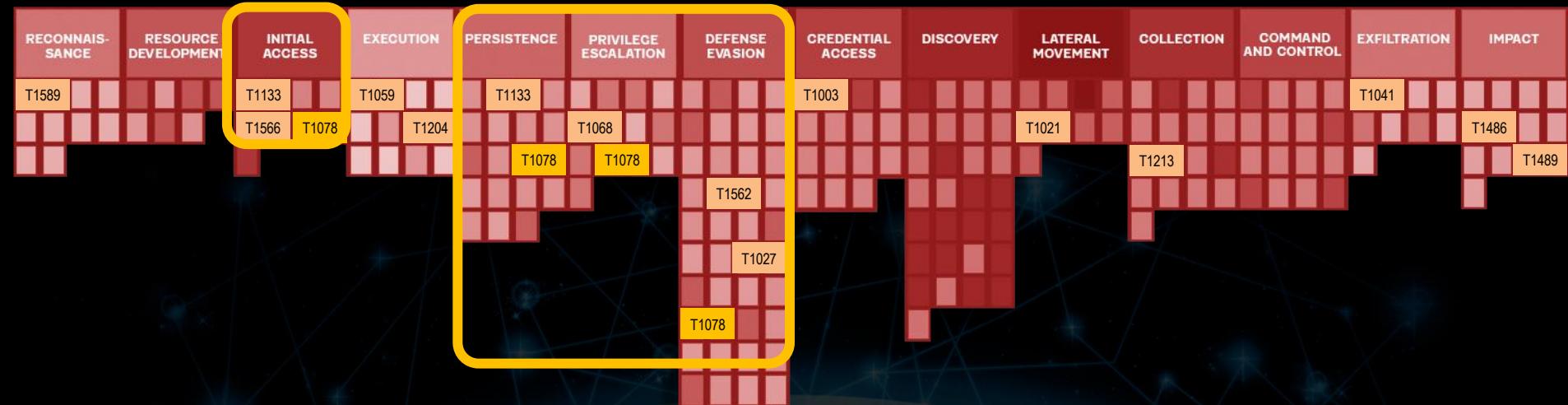
- ⑥ IdP permitió la administración global en Azure



- ⑦ Casi 100 servidores ESXi encriptados.  
→ Interrupción de aplicaciones críticas







1. Gather Victim Identity information (T1589)
2. External Remote Services: TeamViewer y AnyDesk (T1133)
3. Phishing: Vishing (T1566.003)
4. Valid Accounts (T1078)
5. Command and Scripting Interpreter: PowerShell (T1059.001)
6. User Execution: Malicious File (T1204.002)
7. Exploitation for Privilege Escalation (T1068)
8. Disable Security Tools (T1562.001)
9. Obfuscated Files or Information (T1027):
10. Credential Dumping (T1003)
11. Brute Force (T1110)
12. Remote Desktop Protocol (T1021.001)
13. Data from Information Repositories (T1213)
14. Exfiltration Over C2 Channel (T1041)
15. Data Encrypted for Impact (T1486)
16. Service Stop (T1489)

# MAPPING ATTACKS

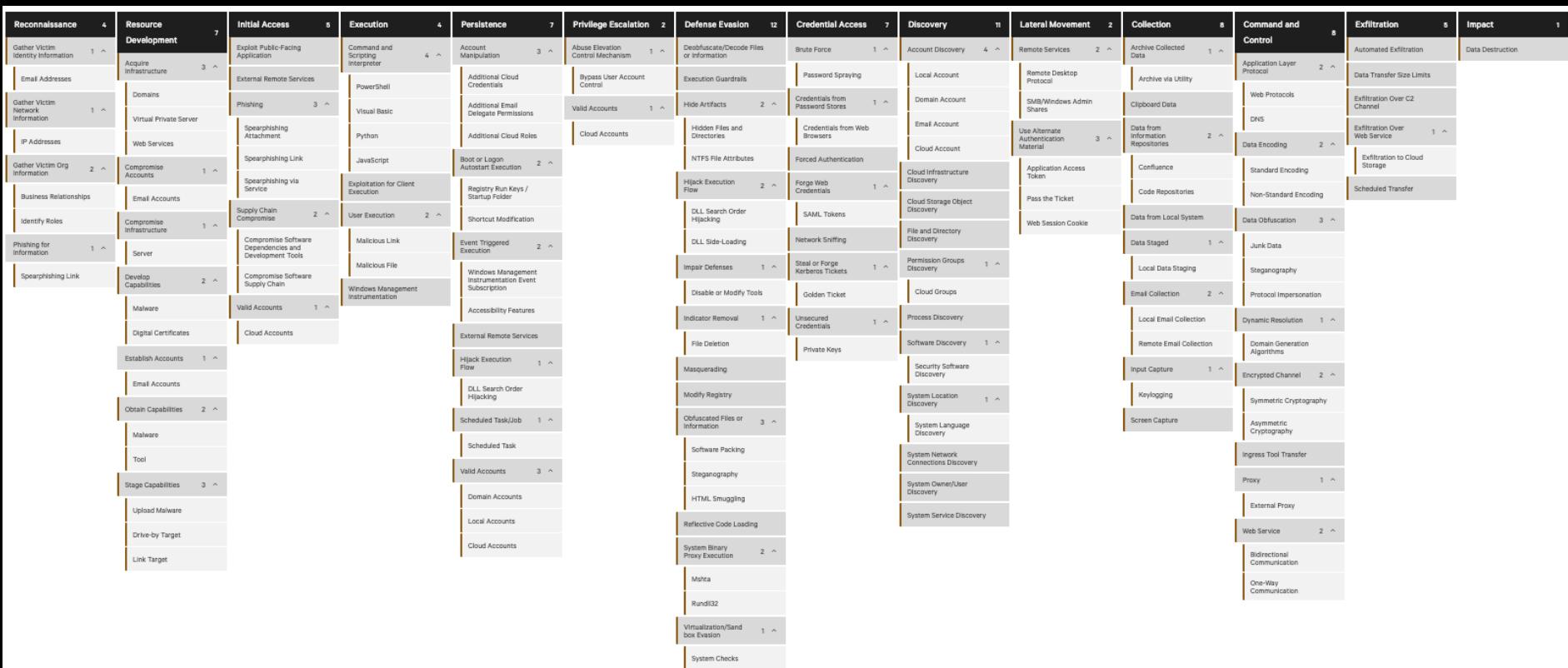
## - COZY BEAR -

# Cozy Bear



- Adversaries
- [COZY BEAR](#)
- Last activity: Jun 2024
- Status: Active
- Origin: [Russian Federation](#)
- Intel reports: [204](#)
- Target industries: 15
- Target countries: 21
- Adversary type: Targeted
- Motivation: [State-Sponsored](#)
- Community identifiers
  - NOBELIUM, The Dukes, JACKMACKEREL, CozyCar, Midnight Blizzard, “The Dukes”, IRON RITUAL, UAC-0029, APT29, YTTRIUM, IRO

# Mapping Cozy Bear with ATT&CK®



# COZY BEAR Targets Azure Environment



## Mapping



## Targets Azure Environment

- ③ El atacante identifica y modifica cuentas de interés, restablece contraseñas y agrega usuarios a grupos administrativos



- ② El tráfico del atacante es enmascarado a través de nodos Tor y proxies residenciales



- ① El atacante accede al entorno de Azure con credenciales previamente comprometidas



- ⑧ Registra una aplicación de terceros para acceder de manera persistente a datos críticos

- ④ Registra dispositivos MFA para mantener acceso persistente a cuentas comprometidas



- ⑤ Obtiene acceso a correos y archivos en OneDrive, SharePoint y Exchange



⑥

- Modifica permisos de buzones para acceder a correos de interés con privilegios completos



- ⑦ Usa la técnica de impersonación para acceder a buzones sin generar registros de acceso

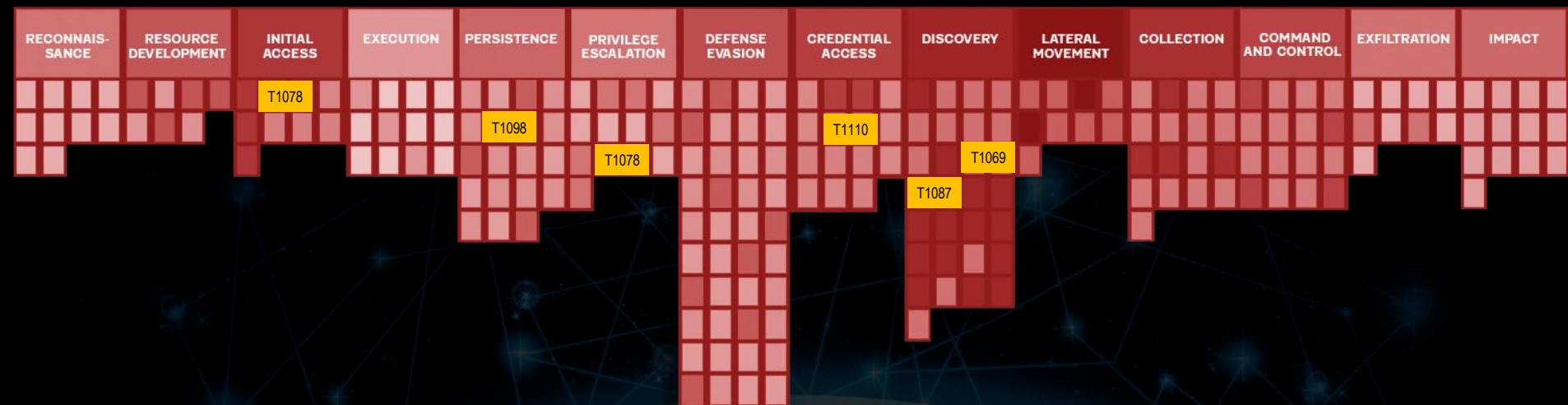
## COZY BEAR Targets Azure Environment

The screenshot shows a Microsoft 365 Outlook interface. On the left, there's a sidebar with various icons and a search bar at the top. The main area displays two separate windows for 'Permissions for the confidential\_folder folder'. The first window shows a list of users with checkboxes next to their names: cisco, aging, vp, in, ., offline\_access, People.Read, and User.Read. The second window shows the same list. Below these windows is a table titled 'Table 1. deffo3847-Assigned API permissions'.

API Permission	Description
Mail.Read	Read user mail
Mail.ReadWrite	Read and write access to user mail
offline_access	Maintain access to data
People.Read	Read users' relevant people lists
User.Read	Sign in and read user profile

*Table 1. deffo3847-Assigned API permissions*

*Figure 3. Adjusting Mailbox Folder Permissions in Microsoft 365 Outlook*



1. Valid Accounts (T1078.004)
2. Account Manipulation: Additional Cloud Credentials (T1098.001)
3. Account Manipulation: Additional Email Delegate (T1098.002)
4. Account Manipulation: Additional Cloud Roles (T1098.003)
5. Valid Accounts (T1078.004)
6. Brute Force: Password Spraying (T1110.003)
7. Permission Groups Discovery: Cloud Groups (T1069.003)
8. Account Discovery: Cloud Account (T1087.004)

# CONTRAMEDIDAS





# RECURSOS

<https://start.me/p/w9G0GA/cloud>



## MITRE - modeling the cloud

- ⌚ GCP - controles de seguridad nativos
- ⌚ AWS - Security Control Mapping navigator
- ⌚ Using Cloud Analytics with CALDERA
- ☰ Cloud Analytic MATRIX
- ⌚ SIGMA RULEs Quickstart
- ⌚ Sigma Rules Heatmap JSON

## MITRE - How to modeling

- ⌚ Cloud Analytics Development Blueprint
- ⌚ GCP Security Control Mappings to MITRE ATT&CK
- ⌚ M365 – Mappings Explorer
- ☰ Defending IaaS with ATT&CK

## Mappings

APTS JSONS CLOUD ANALYTIC +

- ⌚ IaaS Matrix
- ⌚ SaaS Matrix
- ⌚ Azure Matrix
- ⌚ Google workspace Matrix
- ⌚ Office 365 Matrix

## More Cloud Sec Tools

- ⌚ STRATUS Red Team
- ⌚ Cloud analytics - Emulation plugin for CALDERA
- ⌚ TeamTNT - Adversary\_Emulation
- ⌚ MITRE Security Stack Mapping Tools
- ⌚ SyCode7's gists

## Cloud Offensive Tools

- ⌚ Prowler
- ⌚ CloudSploit - Aqua
- ⌚ ScoutSuite - nccgroup
- ⌚ SteamPipe

## Cloud Offensive Tools: GOOGLE CLOUD

- ⌚ GCP Hound : A Swiss Army Knife Offensive Tool
- ⌚ GCP Bucket Brute

## Artículos de interés

- ⌚ 7 Ways to Escape a Container
- ⌚ Attacking AWS Cognito with Pacu (p1)
- ⌚ Attacking AWS Cognito with Pacu (p2)
- ⌚ Getting started with AWS open-source tools (1/3)
- ⌚ Open-source tools to analyze your AWS environment (2/3)
- ⌚ How open-source tools help you with your code (3/3)
- ⌚ Introducing BloodHound 4.0: The Azure Update
- ⌚ A Beginner's Guide to Gathering Azure Passwords

## Cloud Offensive Tools: AZURE

- ⌚ AADInternals
- ⌚ NetSPI MicroBurst
- ⌚ MicroBurst - wiki
- ⌚ Power Zure
- ⌚ Bloodhound
- ⌚ ROADtools
- ⌚ Stormspotter
- ⌚ AADInternals.com
- ⌚ TeamFiltration
- ⌚ Azure Goat
- ⌚ PurpleCloud

## Cloud Offensive Tools: AMAZON WEB SERVICES

- ⌚ weirdAAL
- ⌚ PACU
- ⌚ Cloud Mapper - (duo-labs)
- ⌚ Air IAM
- ⌚ Cloud Splaining - AWS IAM tool
- ⌚ Cloud Goat

## CTF específicos de Contenedores

- ⌚ Container Security CTF - DEFCON 32
- ⌚ ./KiddoCTF
- ⌚ web-ctf-container - HightechSec
- ⌚ CTF challenges: Dockerizing and Repository structure
- ⌚ Hosting CTF challenges on a Kubernetes cluster
- ⌚ ctf\_container - Caesurus

# GRACIAS



**CROWDSTRIKE**

MIGUEL ANGEL DE CASTRO SIMÓN  
CROWDSTRIKE INTELLIGENCE



**trc**

EMILIO RICO RUIZ  
TRC CYBERSECURITY ADVISOR