proofpoint.

INFORME
SOBRE AMENAZAS

# Compromiso y usurpación de cuentas cloud

## Datos básicos

### DESCRIPCIÓN

El compromiso de cuentas cloud consiste en hacerse con el control de la cuenta cloud de un servicio de correo web o de colaboración legítimo con el fin de acceder a una amplia variedad de datos, contactos, eventos de calendario mensajes de correo electrónico y otras herramientas del sistema. Más allá de los datos del usuario, el ciberdelincuente puede utilizar la cuenta para suplantar la identidad del usuario en ataques de ingeniería social, como las estafas Business Email Compromise (BEC), tanto dentro como fuera de la organización. Los ciberdelincuentes pueden acceder a datos sensibles, persuadir a los usuarios o a partners comerciales a transferir dinero o dañar la reputación y la economía de una empresa. También pueden instalar puertas traseras para conservar el acceso para futuros ataques.

### HERRAMIENTAS EN EL MERCADO

- Ataques de phishing, incluido el phishing de tokens OAuth.
- Ataques por fuerza bruta que automatizan el descubrimiento de credenciales, como Aircrack-ng y Jack the Ripper.
- Reciclado de credenciales, o *stuffing*, que emplea combinaciones de nombres de usuario y contraseñas procedentes de robos anteriores.
- Malware, incluidos registradores de pulsaciones y ladrones de credenciales, como PunkeyPOS y Spyrix.

### TIPOS

- Robo de credenciales: los ciberdelincuentes aprovechan contraseñas débiles, sistemas de seguridad insuficiente y la reutilización de contraseñas de otros sitios para piratear los sistemas.
- Aplicaciones OAuth maliciosas: los ciberdelincuentes recurren al phishing de tokens OAuth y a la suplantación de aplicaciones para incitar a los propietarios de las cuentas a delegar permisos para acceder a los recursos del sistema.
- Amenazas internas: un comportamiento negligente o intenciones maliciosas pueden generar una pérdida de credenciales.
- Malware: el software malicioso instalado en los sistemas puede eludir la detección durante largos períodos. Este malware puede robar credenciales y comunicarse con los ciberdelincuentes.

### FACTORES DE RIESGO

- Uso de servicios y aplicaciones cloud no autorizados (Shadow IT) sin la aprobación del departamento de TI.
- Herramientas de supervisión poco eficaces.
- Uso compartido de credenciales entre empleados o con partners externos.
- Bajo nivel de concienciación de los usuarios sobre las buenas prácticas de seguridad y de las técnicas de phishing actuales.

La mayoría de las empresas han migrado sus recursos a la nube, y los ciberdelincuentes no han tardado en hacer lo propio. Empezando por el correo electrónico alojado y el correo web, las apps de productividad cloud, como Microsoft 365 y Google Workspace, y los entornos cloud de desarrollo, como AWS y Azure, los ciberdelincuentes se han dado cuenta del inestimable valor de las credenciales y las han convertido en objetivo de innumerables campañas de phishing. Y dado que el inicio de sesión único ofrece acceso lateral a muchos sistemas distintos dentro de una organización, una sola cuenta comprometida puede provocar importantes daños.

## El compromiso de cuentas cloud en los medios de comunicación

### Capital One sancionada con 80 millones de dólares por el pirateo de 100 millones de solicitudes de tarjetas de crédito en 2019

El Departamento de Justicia de EE. UU. detuvo a Paige Thompson, antigua ingeniera de software de Amazon, por fraude informático y uso inapropiado por acceder a datos de Capital One. Mediante un ataque de falsificación del lado servidor (SSRF, Server-Side Request Forgery), consiguió las credenciales de una persona con acceso a información confidencial almacenados en el servicio de almacenamiento de archivos Amazon S3. Según la acusación, Paige Thompson se habría jactado de sus exploits en su canal de Slack y habría publicado en GitHub instrucciones que permitían reproducir el ataque[1].

### La NSA y el FBI acusan a Rusia de los ataques masivos por fuerza bruta contra Microsoft 365

En un informe conjunto publicado por los servicios de inteligencia británicos, la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) y el Departamento de Seguridad Nacional de EE. UU. identificaron al grupo ciberdelictivo ruso "Fancy Bear" como responsable de una campaña a largo plazo destinada a comprometer cuentas de Microsoft 365. El ataque se produjo mediante la "difusión de contraseñas", en la que algunos ordenadores intentan acceder a una cuenta varias veces utilizando diferentes combinaciones de contraseñas[2].

1 Devling Barrett *(The Washington Post)*. “Capital One Fined $80 Million for 2019 Hack of 100 Million Credit Card Applications" (Capital One sancionada con 80 millones de dólares por el pirateo de 100 millones de solicitudes de tarjetas de crédito en 2019), agosto de 2020.
2 Thomas Brewster *(Forbes)*. "NSA and FBI Blame Russia for Massive ‘Brute Force’ Attacks On Microsoft 365" (La NSA y el FBI acusan a Rusia de los ataques masivos por fuerza bruta contra Microsoft 365), julio de 2021.

# Anatomía de una usurpación de cuentas cloud

A continuación detallamos el desarrollo de la mayoría de las usurpaciones de cuentas.

1. **Robo de credenciales.** El ciberdelincuente consigue las credenciales del usuario a través de phishing de credenciales, ataques de contraseñas mediante fuerza bruta, reciclado de credenciales o *stuffing*, aplicaciones OAuth maliciosas o malware de robo de credenciales (véase **"Herramientas en el mercado"** en la página 1).
2. **Infiltración.** Una vez conectado a la cuenta del usuario, el ciberdelincuente puede acceder a los mensajes de correo, a los contactos, al calendario y a los archivos de la víctima. Entonces puede robar directamente esos datos o utilizarlos para suplantar la identidad del usuario de una manera convincente.
3. **Persistencia y propagación.** Algunos estafadores responden a hilos de discusión existentes o envían mensajes de correo electrónico que contienen malware o URL peligrosas a compañeros y a partner comerciales externos. Haciéndose pasar por el usuario comprometido, el ciberdelincuente puede entonces engañar a otras personas dentro o fuera de la empresa enviándoles facturas falsas o instrucciones de desvío de pagos. También puede cargar malware en recursos compartidos de archivos de la empresa o sabotear la empresa de otras maneras. A menudo, el ciberdelincuente define reglas de reenvío automático que le permiten acceder a los mensajes del usuario incluso si el usuario cambia su contraseña. Al ser capaz de acceder a todos los mensajes de correo electrónico e invitaciones de calendario del usuario, el ciberdelincuente obtiene información esencial para futuros ataques.
4. **Monetización.** Si el ataque no se detecta a tiempo, puede dar lugar al robo de dinero o de datos valiosos (registros financieros o propiedad intelectual).

## Los ataques provocan fugas de datos, fraude bancario y abuso de los sistemas

| | |
|---|---|
| **1** | **RECONOCIMIENTO** |
| | **Phishing de credenciales** |
| | **Fuga o volcado** |
| | **Registradores de pulsaciones o malware** |
| | **Amenaza interna maliciosa** |
| | **Ingeniería social** |
| **2** | **INFILTRACIÓN** |
| | **Búsqueda sistemática de credenciales** |
| | **Inicio de sesión directo** |
| | **Malware para la nube (apps de terceros)** |
| **3** | **PROPAGACIÓN, PERSISTENCIA Y APRENDIZAJE** |
| | **Conservación del acceso**<br>• Creación de reglas de reenvío de mensajes<br>• Cambio de permisos<br>• Creación de cuentas de administrador<br>• Desactivación de la autenticación multifactor<br>• Establecimiento de un acceso de terceros |
| | **Uso de cuentas de confianza para lanzar ataques**<br>• Envío de mensajes de phishing internos y externos<br>• Carga y uso compartido de malware |
| | **Descubrimiento del potencial**<br>• Consulta de mensajes y archivos<br>• Exploración de la estructura organizativa<br>• Estudio de los proceso empresariales |
| **4** | **MONETIZACIÓN** |
| | **Estafas BEC/correo electrónico**<br>• Fraude de transferencia bancaria<br>• Fraude de salarios<br>• Timos de las tarjetas regalo<br>• Fraude de la cadena de suministro |
| | **Filtración de datos**<br>• Correo electrónico<br>• Descarga<br>• Uso compartido |
| | **Sabotaje**<br>• Ransomware para la nube<br>• Destrucción |
| | **Abuso de sistemas**<br>• Spam<br>• Fraude como servicio<br>• Minería de criptomonedas |

Factores de riesgo y consecuencias asociadas a la usurpación de cuentas cloud.

## Cómo proteger su organización

- Impida que los mensajes de phishing de credenciales lleguen a las bandejas de entrada de los usuarios.
- Transforme a los usuarios en una línea sólida de defensa a través de formación sobre las mejores prácticas del uso de contraseñas y cómo reconocer los mensajes de phishing. Preferentemente, también deben poder denunciar fácilmente los mensajes sospechosos.
- Considere la adopción de una solución CASB (Cloud Access Security Broker) para obtener una vista consolidada de los servicios cloud de su organización. Esta solución incluye los detalles de los usuarios y aplicaciones OAuth que tienen acceso a los datos de los servicios cloud desde cualquier dispositivo o ubicación.
- Adopte un enfoque Zero Trust del acceso a la red y a las aplicaciones para limitar los daños provocados por una cuenta comprometida.
- Analice los mensajes de correo electrónico internos, y no solo los mensajes entrantes, para detectar amenazas como el malware y el fraude por correo electrónico.
- Active la autenticación multifactor. Aunque no se trata de una solución milagrosa contra la usurpación de cuentas, complica enormemente la tarea a los ciberdelincuentes.
- Identifique a los usuarios que presentan mayor riesgo y supervise los incidentes.
- Configure y priorice las alertas en función de los factores de riesgo más críticos para su organización.
- Correlacione las amenazas del correo electrónico y la nube para detectar con precisión las cuentas comprometidas.
- Asegure el gobierno de las aplicaciones OAuth y revoque las aplicaciones maliciosas o peligrosas.
- Impida que los usuarios hagan clic en URL maliciosas y descarguen malware mediante el aislamiento de la navegación web.
- Investigue los incidentes de seguridad con una solución que ofrezca análisis forenses detallados e informes personalizados.
- Bloquee el acceso no autorizado a las aplicaciones y servicios cloud mediante controles de acceso adaptables, sobre todo para los dispositivos no gestionados.
- Automatice la respuesta a incidentes de seguridad con controles de políticas flexibles que generen una alerta en caso de incidente o de cambio del perfil de riesgo de un usuario. Es posible que los usuarios más atacados o que presentan un riesgo mayor por sus hábitos digitales o sus privilegios de acceso deban volver a autenticarse con regularidad.

## Información extraída de las investigaciones

Proofpoint supervisa miles de inquilinos cloud y más de 20 millones de usuarios de la nube activos. Un estudio sobre los datos de amenazas para la nube de 2020 nos permitió extraer las siguientes conclusiones:

| | |
|---|---|
| **El 95 %** | de las organizaciones sufrieron ataques |
| **El 52 %** | de las organizaciones tuvieron al menos una cuenta comprometida |
| **El 32 %** | de las organizaciones comprometidas experimentaron actividad posterior al acceso: manipulación de archivos, reenvío de mensajes de correo electrónico y actividad en aplicaciones OAuth |
| **El 10 %** | de las organizaciones tienen aplicaciones OAuth maliciosas no autorizadas |

Según el 86 % de los responsables de TI encuestados en un informe del Ponemon Institute de 2021 encargado por Proofpoint, los compromisos de cuentas costaron a las organizaciones más de 500 000 dólares al año[3]. Los encuestados también denunciaron 64 compromisos de cuentas cloud al año de media, de los que el 30 % supuso la divulgación de datos sensibles[4].

Casi el 60 % de los participantes indicaron que las cuentas de Microsoft 365 y Google Workspace son objetivos particularmente habituales de ataques de phishing y por fuerza bruta en la nube.

En general, más del 50 % de los encuestados declaró que el phishing era el método utilizado con más frecuencia por los ciberdelincuentes para conseguir credenciales cloud legítimas.

3 Ponemon Institute. "Cost of Cloud Compromise and Shadow IT" (Coste del compromiso de cuentas cloud y las shadow IT), abril de 2021.
4 Ibid.

## Más información

Para protegerse frente al compromiso de cuentas cloud, las organizaciones deben asegurarse de contar con medidas de seguridad eficaces. Las plataformas de seguridad deben permitir el cifrado de extremo a extremo y la supervisión continua de datos, así como detectar rápidamente los incidentes para que los administradores puedan limitar y corregir posibles daños.

Para obtener más información sobre cómo impedir eficazmente el compromiso de cuenta cloud, visite **www.proofpoint.com/es**.