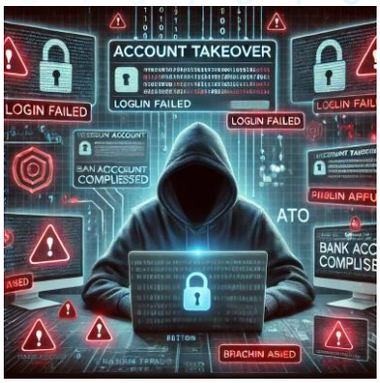
Alerta de Seguridad

COLCERT AL-20250314-064

Ataque Account Takeover: Un riesgo creciente en la ciberseguridad

TLP:CLEAR

El Account Takeover (ATO) es un tipo de ciberataque en el que un atacante obtiene acceso no autorizado a la cuenta de un usuario legítimo. Una vez dentro, cambia las credenciales de acceso y puede utilizar la cuenta para actividades maliciosas, como fraude financiero, suplantación de identidad o robo de información.



Principales riesgos y vulnerabilidades

- **Reutilización de credenciales:** Los atacantes prueban combinaciones de usuario y contraseña filtradas en múltiples plataformas (credential stuffing).
- **Ataques de phishing y smishing:** Envío de correos o mensajes falsos para engañar a los usuarios y obtener sus credenciales.
- **Fugas de datos:** Bases de datos expuestas en la web oscura facilitan el acceso a cuentas legítimas.
- **Uso de bots automatizados:** Herramientas que prueban miles de credenciales en diferentes plataformas para obtener acceso no autorizado.
- **Malware y keyloggers:** Programas que registran contraseñas y otros datos ingresados en dispositivos comprometidos.

Impacto del ataque Account Takeover

- **Pérdidas económicas:** Fraudes financieros, transacciones bancarias no autorizadas y robo de activos digitales.
- **Riesgos legales:** Suplantación de identidad y uso de cuentas legítimas para cometer delitos.
- **Daño reputacional:** Exposición de información privada y uso indebido de perfiles personales o corporativos.
- **Acceso a infraestructuras críticas:** Si el ataque compromete credenciales de acceso a sistemas gubernamentales o empresariales.

Medidas de mitigación

- **Bloqueo de cuentas comprometidas:** Implementar alertas para detectar accesos sospechosos y bloquear cuentas en riesgo.
- **Uso de inteligencia artificial:** Herramientas que analicen patrones de comportamiento y detecten anomalías en los accesos.
- **Concienciación y capacitación:** Informar a los usuarios sobre riesgos de phishing y la importancia de buenas prácticas de seguridad.
- **Monitoreo y respuesta rápida:** Implementar soluciones de detección y respuesta ante incidentes para minimizar daños.

Recomendaciones de seguridad

- **Habilitar la autenticación multifactor (MFA):** Agregar una capa de seguridad adicional para evitar accesos no autorizados.
- **Utilizar contraseñas únicas y robustas:** No reutilizar credenciales en diferentes plataformas y emplear gestores de contraseñas.
- **Monitorear actividad sospechosa:** Estar atento a intentos de acceso fallidos o cambios inesperados en la cuenta.
- **Evitar enlaces y archivos sospechosos:** No hacer clic en correos electrónicos o mensajes que soliciten credenciales.
- **Actualizar software de seguridad:** Mantener el sistema operativo y antivirus actualizados para prevenir malware.
- **Revisar filtraciones de credenciales:** Utilizar herramientas como Have I Been Pwned para verificar si una cuenta ha sido comprometida.

COLCERT

Alerta de Seguridad

Ataque Account Takeover: Un riesgo creciente en la ciberseguridad

COLCERT AL-20250314-064

TLP:CLEAR

¿Cómo se ejecuta un ataque de Account Takeover (ATO)?

Los atacantes utilizan diversas técnicas para obtener acceso no autorizado a una cuenta legítima y tomar control de ella. El proceso típico de ATO sigue estos pasos:

1 Recolección de credenciales

Los ciberdelincuentes obtienen nombres de usuario y contraseñas mediante diferentes métodos, como:

- **Filtraciones de datos:** Uso de bases de datos de credenciales expuestas en la dark web.
- **Phishing y smishing:**Correos y mensajes fraudulentos que engañan a las víctimas para robar credenciales.
- **Ataques de malware y keyloggers:**Software malicioso que captura lo que el usuario escribe.
- **Ingeniería social:**Manipulación psicológica para obtener información de acceso.

2 Pruebas masivas de credenciales robadas

Una vez obtenidas las credenciales, los atacantes prueban estas combinaciones en múltiples plataformas mediante técnicas como:

- **Credential stuffing:** Se utilizan bots automatizados para probar credenciales robadas en diversos servicios, aprovechando la reutilización de contraseñas.
- **Brute force attacks:** Intentos sistemáticos para descifrar contraseñas débiles.
- **Password spraying:** Intento de iniciar sesión con contraseñas comunes en muchas cuentas para evitar bloqueos por intentos fallidos.

3 Toma de control de la cuenta

Cuando los atacantes logran acceder a una cuenta, realizan cambios para bloquear el acceso de la víctima y evitar ser detectados:

- Cambio de contraseñas y correos electrónicos asociados.
- Activación de autenticación multifactor (MFA) a favor del atacante.
- Modificación de información de recuperación.

4 Explotación de la cuenta comprometida

Una vez dentro, los atacantes pueden usar la cuenta para distintos fines maliciosos:

- Fraude financiero: Transferencias no autorizadas, compras con tarjetas vinculadas.
- Extorsión y venta de acceso: Revenden cuentas en foros clandestinos o extorsionan a la víctima.
- Difusión de ataques: Envían mensajes de phishing a contactos de la víctima.
- Acceso a sistemas corporativos: Uso de credenciales comprometidas para infiltrarse en redes empresariales.

COLCERT

TIC

Alerta de Seguridad

COLCERT AL-20250314-064

Ataque Account Takeover: Un riesgo creciente en la ciberseguridad

TLP:CLEAR

Casos confirmados de Account Takeover

Incremento global de ataques ATO en 2024

- Los ataques de Account Takeover aumentaron un 250% en 2024, con picos significativos en períodos de alto tráfico.
- Más de 1,000 grandes empresas fueron atacadas, comprometiendo millones de cuentas de clientes.
  Fuente: Kasada.io

Ciberataque al grupo TENDAM

- Ciberdelincuentes tomaron el control de cuentas de clientes de Women'secret, Springfield y Cortefiel.
- Datos comprometidos: nombres, apellidos y datos de contacto de clientes de sus clubes de fidelidad.
- Aunque no se expusieron datos financieros, los atacantes podrían utilizar la información para suplantación y fraudes futuros. **Fuente: Cadena Ser**

Suplantación de identidad en plataformas de salud en Cataluña

- 150 personas fueron víctimas de suplantación de identidad digital a través de la plataforma La Meva Salut.
- Los ciberdelincuentes tomaron el control de las cuentas y solicitaron prescripciones médicas de opioides y ansiolíticos.
- Medida correctiva: Implementación de doble autenticación para evitar futuros ataques. Fuente: El País

NIVEL DE RIESGO

ALTO

"Las cuentas comprometidas no solo pueden convertirse en un punto de entrada para ataques más sofisticados, sino que también representan pérdidas económicas significativas. La seguridad de tus credenciales es la primera línea de defensa."

FUENTES:

1. **Definición del ataque Account Takeover** -
2. **Centro Cibernético Policial – COLCERT -**
3. **Riesgos y vulnerabilidades del ATO**.
4. **Recomendaciones de seguridad para prevenir** .
5. **Incremento global de ataques ATO en 2024**.
6. **Suplantación de identidad en plataformas de salud en Cataluña**.
7. **Ciberataque al grupo TENDAM**.

OWASP
CAI Virtual
FBI - Advisory on Credential Stuffing Attacks
NIST (National Institute of Standards and Technology) - Digital Identity Guidelines
Kasada.io

El País
Cadena Ser

COLCERT