Cómo protege Proofpoint contra la usurpación de cuentas cloud

Prevenga y mitigue las usurpaciones de cuentas cloud, que tienen efectos devastadores

Productos

- Proofpoint Cloud App Security Broker
- Proofpoint Zero Trust Nework Access
- Proofpoint Browser Isolation
- Proofpoint Email Isolation
- Plataforma Proofpoint Threat Protection
- Proofpoint Targeted Attack Protection

Ventajas principales

- Previene la usurpación de cuentas inicial, bloqueando los ataques de phishing diseñados para robar credenciales o activar malware.
- Detecta y soluciona todos los casos de usurpaciones de cuentas.
- Levanta una sólida barrera alrededor de sus recursos más valiosos para protegerlos de las amenazas.
- Evita que sus empleados puedan introducir involuntariamente amenazas en el entorno.
- Consiga una inteligencia inestimable que le ayudará a prepararse para posibles amenazas emergentes.

Los ciberdelincuentes van tras las empresas a la nube. Cada vez más compañías adoptan el correo electrónico alojado y el correo web, así como las apps cloud de productividad, como Microsoft 365 y Google Workspace, y los entornos cloud de desarrollo, como AWS y Azure, y los ciberdelincuentes no han tardado en comprender que las credenciales de una cuenta de empresa son una fuente potencial de ingresos y de posibilidades. Por eso está aumentando el número de campañas de amenazas cuyo objetivo es conseguir estas credenciales. Y la persistencia en esta iniciativa es precisamente el preámbulo que confirma su determinación de cometer fraudes mediante transferencias bancarias, espionaje industrial o robo de datos de identidad, entre otros ataques.

Una usurpación o secuestro de una cuenta cloud comienza cuando los atacantes se apoderan de las credenciales de los usuarios y consiguen acceder a sus sistemas. Estos ataques suelen comenzar a partir de mensajes de correo electrónico con malware o contenido diseñado para engañar a los usuarios y conseguir que entreguen sus credenciales. Una vez que se usurpa una cuenta, los ciberdelincuentes pueden hacerse pasar por personas legítimas o de confianza pertenecientes a la organización del usuario. Los infiltrados pueden moverse lateralmente y causar estragos en la empresa. Pueden robar o cifrar datos importantes o bien cargar malware para utilizar funciones de sincronización y uso compartido entre sus endpoints, Microsoft 365 y otros repositorios cloud. A continuación, se pueden distribuir rápidamente por la empresa o bien descargar archivos confidenciales que utilizarán para extorsionarle.

Además, dado el creciente uso de sistemas de inicio de sesión único, basta con comprometer las credenciales de un sistema para obtener acceso a muchos otros en la empresa.

Una de las modalidades de usurpación de cuentas cloud más peligrosas y con peores consecuencias es el ransomware. Este tipo de ciberataque provoca el cierre de empresas, obliga a hospitales a rechazar a pacientes y paraliza gobiernos enteros. Solo el año pasado, en Estados Unidos se sufrieron más de 65 000 ataques de ransomware. Según Unit 42 de Palo Alto Networks, el 75 % de estos ataques se originaron en el correo electrónico.[1] Por eso esta es una de las principales preocupaciones de los CISO y se ha convertido incluso en un problema de seguridad nacional.

Soluciones de Proofpoint

Los ciberdelincuentes emplean varias estrategias y vectores de amenazas para conseguir infiltrarse en su red. Con frecuencia usan una combinación de métodos para abordarle y obtener la información que necesitan. Y su arsenal incluye ataques por fuerza bruta, tácticas de ingeniería social y uso de malware. Para protegerse frente a estas estrategias necesita una defensa integral y multicapa. Proofpoint ofrece algunos productos y servicios que pueden ayudarle.

Juntas, las soluciones de Proofpoint le permiten defenderse de la usurpación de cuentas cloud mediante:

- La prevención de la usurpación de cuentas inicial
- La detección y solución de los ataques de usurpación de cuentas
- La implantación de barreras alrededor de sus recursos más valiosos —tanto personas como sistemas— para impedir el ataque de amenazas externas.
- Métodos para evitar que sus empleados puedan introducir involuntariamente amenazas en el entorno.
- Consiga una inteligencia inestimable que le ayudará a prepararse para posibles amenazas emergentes.

Prevención, detección y solución

La plataforma Proofpoint Threat Protection es una solución integrada y multicapa que reduce el riesgo de usurpación de cuentas cloud. Incluye detección de amenazas líder de la industria que evita que los usuarios reciban malware, phishing de credenciales y otros tipos de ataques basados en el correo electrónico. Además, organiza la seguridad para corregir las cuentas comprometidas. De esta forma se reduce el tiempo de respuesta a incidentes y la sobrecarga de trabajo del equipo de TI. Los usuarios víctimas de ataques y amenazas de robo de credenciales reales pueden recibir breves sesiones de formación para concienciar en materia de seguridad. Y la plataforma puede emplear banners HTML informativas y personalizables para recordar a los usuarios que deben ser cautos con los mensajes que parezcan peligrosos. Además, puede autenticar mensajes entrantes y salientes a través de DMARC, y puede identificar cuentas de proveedores comprometidas. Este enfoque por capas justifica que más del 60 % de las empresas del Fortune 1000 confíen en la protección frente a amenazas que ofrece Proofpoint para reducir el riesgo de usurpación de cuentas cloud.

1 Unit 42, Palo Alto Networks *(https://unit42.paloaltonetworks.com/ransomware-families/)*. "Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report" (Familias de ransomware: datos de 2021 para complementar el informe de amenazas de ransomware de Unit 42), julio de 2021.

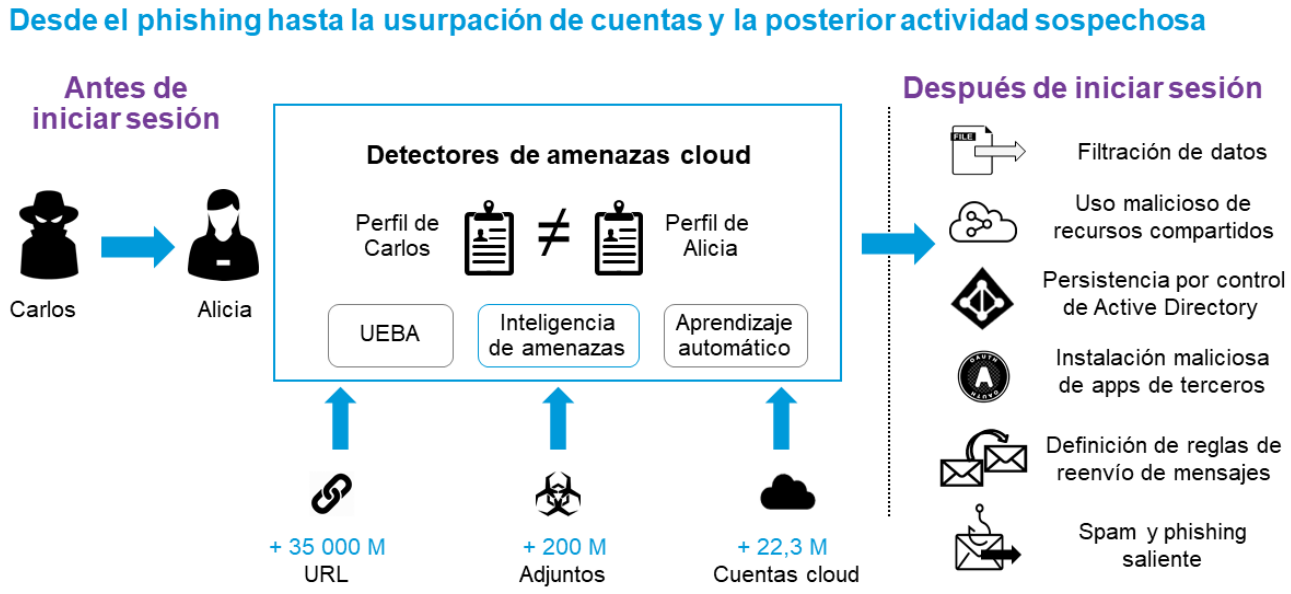

Figura 1: Detección de cuentas comprometidas con CASB.

Proofpoint Cloud App Security Broker (CASB) es la piedra angular de nuestra defensa contra el secuestro de cuentas cloud. Para proteger a los usuarios de las amenazas cloud y garantizar la seguridad de sus datos confidenciales, se requiere un enfoque centrado en las personas. Esta defensa empieza por contar con visibilidad y controles de acceso, ya que hasta que no sepa qué es lo que desconoce no puede poner en práctica una defensa eficaz contra la usurpación de cuentas cloud. Proofpoint CASB le ayuda a desplegar medidas de prevención para la seguridad, como los controles de acceso adaptables, incluida una autenticación más estricta. Nosotros detectamos todos los intentos de usurpación y le informamos de qué hacen los ciberdelincuentes una vez que consiguen acceder a una cuenta. La solución Proofpoint CASB suspende las cuentas comprometidas y neutraliza todas las amenazas posteriores a la usurpación. Esto implica que, incluso en el caso de que un atacante haya conseguido acceso a una de sus cuentas, la solución Proofpoint CASB puede frustrar los intentos de usarla para el reenvío o la delegación de correo electrónico, la fuga de datos y el envío de mensajes de phishing y spam.

Alternativa Zero Trust a VPN

Las plantillas de teletrabajadores y empleados móviles crecen en todo el mundo. Con este crecimiento, el perímetro de la red está desapareciendo, ya que cada vez hay más aplicaciones que migran a la nube. Muchas empresas están empezando justo ahora a afrontar los nuevos retos de seguridad que implica este nuevo paradigma. Acaban de descubrir que sus sistemas de seguridad tradicionales, basados en la conectividad in situ y las pilas de seguridad, no sirven para proteger contra las amenazas cloud, que son cada vez más innovadoras.

Proofpoint Zero Trust Network Access (ZTNA) puede ayudarle a conectar a sus usuarios con las apps con seguridad, tanto en el data center como en la nube. Esta alternativa a las VPN, centrada en las personas, microsegmenta los permisos, lo que reduce drásticamente la superficie de ataque de la red. Así, proporciona un perímetro definido por software que ofrece acceso a la red de confianza cero (Zero Trust).

Proofpoint Email Isolation y Proofpoint Browser Isolation

Los equipos de TI y de seguridad deben garantizar un entorno operativo seguro para sus usuarios. Sin embargo, también deben permitirles investigar y colaborar con los miembros de su equipo de manera eficaz. Esto puede resultar difícil, ya que los dos principales vectores de usurpación de cuentas cloud son precisamente las herramientas que se emplean para la investigación y la comunicación: la Web y el correo electrónico. Proofpoint ofrece dos soluciones que permiten a sus equipos cumplir ambos objetivos, sin renunciar a nada. Ofrecen una experiencia fluida de navegación y comunicación y, al mismo tiempo, protegen a los usuarios frente a compromisos de cuentas cloud.

Proofpoint Browser Isolation protege frente a la usurpación de cuentas cloud y permite a los usuarios navegar por la Web, mientras que les protege para evitar que hagan clic de forma desapercibida en enlaces de phishing y descarguen archivos maliciosos en los dispositivos de la empresa.

Proofpoint Email Isolation amplía las funciones de Proofpoint Targeted Attack Protection (TAP). Para ello, aísla los clics en direcciones URL en función del riesgo, dentro del correo electrónico corporativo. Además, podemos identificar a las personas que reciben más ataques y determinar cuáles son las direcciones URL más peligrosas que llegan a las bandejas de entrada de sus usuarios.

Inteligencia actualizada

Un conocimiento amplio y profundo del panorama de amenazas le permite prepararse para la próxima gran amenaza. El gráfico de amenazas Nexus de Proofpoint ofrece la inteligencia global sobre amenazas que necesita para adelantarse a las mayores amenazas actuales. Combina billones de puntos de datos en tiempo real de múltiples vectores de amenazas de todo el mundo, tecnologías avanzadas de inteligencia artificial y aprendizaje automático, así como un equipo internacional de expertos en investigación de seguridad.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

proofpoint.

0205-005-01-01 11/21