

Alerta ID:	128
Fecha del reporte:	31/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Campaña ShinyHunters contra salud y tecnología médica
Herramienta de detección	N/A
Activo involucrado:	Sistema de autenticación de la organización
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre el incremento de ataques asociados a la campaña denominada ShinyHunters, orientada al compromiso de identidades digitales y al acceso no autorizado a servicios en la nube y plataformas de software como servicio, mediante técnicas de ingeniería social, llamadas fraudulentas, suplantación de personal de soporte técnico y manipulación de mesas de ayuda.

El propósito de esta alerta es que las entidades del sector salud validen sus procedimientos de verificación de identidad, restablecimiento de contraseñas y factores de autenticación, así como la configuración de sus sistemas de inicio de sesión único, aplicaciones conectadas, permisos OAuth y servicios en la nube. Estas acciones buscan prevenir el compromiso de cuentas corporativas y privilegiadas, la extracción de información sensible, la extorsión y posibles afectaciones a la continuidad de los servicios clínicos, tecnológicos y administrativos.



Descripción:

Se ha identificado un incremento de ataques asociados a operaciones de extorsión que utilizan la marca ShinyHunters y que afectan a organizaciones del sector salud y de tecnología médica. La campaña se caracteriza principalmente por el uso de llamadas fraudulentas o vishing, mediante las cuales los atacantes se hacen pasar por personal de tecnología, soporte técnico o mesa de ayuda de la organización.

Durante la llamada, los atacantes informan a la víctima sobre una supuesta actualización obligatoria de autenticación multifactor, migración a passkeys o modificación de la cuenta corporativa. Posteriormente, la dirigen a un portal falso diseñado para imitar la página de inicio de sesión de la organización, donde capturan en tiempo real el usuario, la contraseña y los códigos o aprobaciones de autenticación multifactor. En algunos incidentes también se ha observado el registro de dispositivos controlados por el atacante como nuevos factores de autenticación, con el propósito de mantener el acceso a la cuenta comprometida.

Una vez obtenido el acceso, los actores utilizan las credenciales y sesiones legítimas para ingresar a plataformas de identidad y servicios SaaS conectados, como Microsoft Entra, Okta, Microsoft 365, SharePoint, OneDrive, Salesforce y otras aplicaciones empresariales. Desde estas plataformas realizan búsquedas, descargan información sensible y extraen comunicaciones o documentos internos que posteriormente pueden ser utilizados para extorsionar a la organización.

Esta actividad no se origina principalmente en una vulnerabilidad de los productos tecnológicos ni requiere necesariamente la instalación de malware. Su efectividad depende del engaño a los usuarios, del abuso de procedimientos de soporte y restablecimiento de cuentas, y del uso de credenciales, sesiones y factores de autenticación legítimos, lo que puede dificultar su detección mediante controles tradicionales basados exclusivamente en archivos maliciosos o firmas de malware.



Consecuencias de la explotación



La materialización exitosa de una campaña asociada a ShinyHunters puede generar un impacto significativo en las organizaciones del sector salud, debido a que los actores utilizan ingeniería social, credenciales válidas, sesiones autenticadas y aplicaciones autorizadas para acceder a servicios corporativos. Este comportamiento puede dificultar la detección, dado que las actividades maliciosas pueden confundirse con acciones legítimas realizadas por usuarios o integraciones autorizadas.

1. Compromiso de cuentas corporativas y sistemas de identidad

El principal riesgo es la toma de control de cuentas de inicio de sesión único, como Microsoft Entra, Okta o Google, mediante la captura de credenciales, códigos MFA, restablecimiento fraudulento de factores de autenticación o registro de dispositivos controlados por el atacante.

Esto puede permitir acceso a:

- Microsoft 365, SharePoint y OneDrive.
- Correo y documentos institucionales.
- Plataformas CRM y servicios SaaS.
- Aplicaciones conectadas mediante SSO.
- Portales administrativos y servicios remotos accesibles por la cuenta.

Impacto clave: el atacante puede operar utilizando una identidad válida y los mismos permisos asignados al usuario comprometido.

2. Suplantación de usuarios y abuso de privilegios



Una vez comprometida la identidad, el atacante puede hacerse pasar por personal médico, administrativo, técnico o directivo, consultar información, descargar archivos y realizar acciones dentro de las plataformas a las que tenga acceso la cuenta.

También puede:

- Utilizar sesiones activas.
- Registrar nuevos factores MFA.
- Autorizar aplicaciones conectadas.
- Aprovechar permisos OAuth concedidos por el usuario.
- Ejecutar consultas mediante API en nombre de la víctima.

Impacto clave: se pierde la confiabilidad de la identidad digital como mecanismo para determinar quién realizó una acción dentro del sistema.

3. Persistencia mediante sesiones, dispositivos y aplicaciones autorizadas

Los actores pueden mantener el acceso mediante sesiones autenticadas, tokens OAuth, dispositivos registrados como factores MFA o aplicaciones conectadas con permisos permanentes.

El simple cambio de contraseña puede ser insuficiente cuando no se revocan simultáneamente:

- Las sesiones activas.
- Los tokens de acceso.
- Las autorizaciones OAuth.
- Los dispositivos MFA no reconocidos.
- Las aplicaciones conectadas maliciosas.

Impacto clave: el atacante puede conservar acceso después de que la organización considere recuperada la cuenta.



4. Acceso a información sensible del sector salud

Si la cuenta comprometida tiene permisos sobre repositorios que contienen información clínica, administrativa o personal, el atacante podría acceder a datos de pacientes, empleados, proveedores y terceros.

La información potencialmente expuesta puede incluir:

- Documentos almacenados en SharePoint o OneDrive.
- Comunicaciones internas y correos institucionales.
- Información personal identificable.
- Registros administrativos y financieros.
- Información clínica almacenada o compartida mediante servicios SaaS.
- Credenciales, configuraciones o documentos relacionados con VPN y sistemas internos.

No existe evidencia pública suficiente para afirmar que la campaña haya comprometido de manera generalizada historias clínicas electrónicas o plataformas de diagnóstico. Ese riesgo dependerá de las aplicaciones conectadas y de los permisos de la identidad afectada.

Impacto clave: posible violación de la confidencialidad de datos personales y sensibles, incluidos datos relacionados con la salud.

5. Expansión hacia otras plataformas SaaS

Una cuenta SSO comprometida puede permitir que el atacante acceda a varias aplicaciones conectadas sin tener que vulnerar cada plataforma de forma independiente.

La expansión puede incluir:

- Microsoft 365.
- SharePoint y OneDrive.
- Salesforce.



- Slack.
- Sistemas de gestión empresarial.
- Aplicaciones integradas mediante OAuth o SSO.

Microsoft y Google han documentado que el acceso posterior puede estar determinado de forma oportunista por los permisos y las aplicaciones disponibles en la sesión comprometida.

Impacto clave: una sola identidad puede convertirse en un punto de acceso a múltiples repositorios y servicios empresariales.

6. Evasión de controles tradicionales de detección

La campaña no depende principalmente de malware ni de la explotación de una vulnerabilidad del proveedor. Los atacantes utilizan cuentas, aplicaciones y flujos de autenticación legítimos.

Esto puede permitirles:

- Evitar alertas basadas únicamente en archivos maliciosos.
- Realizar acciones mediante aplicaciones aprobadas.
- Ejecutar consultas y descargas mediante API.
- Confundirse con la actividad habitual del usuario.
- Operar sin generar anomalías tradicionales de inicio de sesión.

Impacto clave: las soluciones enfocadas exclusivamente en antivirus, firmas o detección de malware pueden no identificar oportunamente la actividad.

7. Exfiltración de información y extorsión

Después de obtener acceso, los actores buscan y descargan información sensible y comunicaciones internas para utilizarlas como mecanismo de presión económica.

Se han observado actividades como:



- Descarga de archivos desde SharePoint y OneDrive.
- Consultas masivas en plataformas CRM.
- Búsqueda de documentos confidenciales.
- Extracción de información personal identificable.
- Envío de muestras de los datos robados.
- Amenazas de publicación y exigencias de pago.

También se han reportado acciones de presión adicionales, como mensajes dirigidos a empleados, hostigamiento y ataques de denegación de servicio contra sitios de las víctimas.

Impacto clave: la organización puede enfrentar extorsión y divulgación pública de la información, incluso sin que sus archivos hayan sido cifrados mediante ransomware.

8. Afectación de la continuidad operativa

Aunque la campaña se centra en el robo de datos, la respuesta al incidente puede obligar a la organización a restringir cuentas, suspender accesos remotos, revocar sesiones, deshabilitar aplicaciones conectadas o limitar temporalmente plataformas SaaS.

En una entidad de salud esto puede provocar:

- Interrupciones en el correo institucional.
- Indisponibilidad temporal de documentos compartidos.
- Restricción de accesos de personal remoto.
- Retrasos en procesos administrativos y asistenciales.
- Afectación de integraciones entre plataformas.
- Sobrecarga de las áreas de tecnología y seguridad.

Impacto clave: la contención del incidente puede afectar temporalmente servicios que dependen de las identidades o plataformas comprometidas.



9. Consecuencias regulatorias, legales y reputacionales

En Colombia, los datos relativos a la salud son considerados datos sensibles. La Ley 1581 de 2012 exige que los responsables y encargados implementen medidas técnicas, humanas y administrativas para prevenir su pérdida, consulta, uso o acceso no autorizado o fraudulento.

La materialización de un incidente puede generar:

- Obligación de evaluar y reportar el incidente de seguridad ante la Superintendencia de Industria y Comercio, cuando corresponda.
- Investigaciones administrativas.
- Requerimientos de información y auditorías.
- Órdenes para implementar medidas correctivas.
- Posibles sanciones por incumplimiento del régimen de protección de datos.
- Pérdida de confianza de pacientes, usuarios, proveedores y aliados.

La SIC ha señalado que los incidentes deben reportarse dentro de los quince días hábiles siguientes a su detección y conocimiento por el área encargada, conforme a las condiciones aplicables al responsable o encargado del tratamiento.

Modo de explotación del ataque

La campaña asociada a ShinyHunters utiliza una cadena progresiva de ingeniería social, compromiso de identidades digitales y abuso de servicios legítimos en la nube. Su objetivo principal es obtener acceso a cuentas corporativas, mantener persistencia mediante factores de autenticación o aplicaciones autorizadas, localizar información sensible y extraerla para posteriormente extorsionar a la organización.

A diferencia de una intrusión tradicional basada en malware, esta actividad aprovecha credenciales, sesiones, dispositivos y aplicaciones que los sistemas reconocen como legítimos.



Por esta razón, las acciones del atacante pueden confundirse con la actividad normal del usuario comprometido.

FASE 1. PREPARACIÓN DE LA INFRAESTRUCTURA DE ENGAÑO

Los actores preparan sitios de captura de credenciales personalizados para imitar la identidad visual y los portales de autenticación de la organización objetivo.

Google Threat Intelligence observó dominios contruidos con patrones similares a:

- nombreorganizaciónssso[.]com
- nombreorganizacióninternal[.]com
- portales que imitan servicios de identidad corporativa
- páginas falsas relacionadas con actualizaciones de MFA o acceso interno

Estos dominios son utilizados para aumentar la credibilidad del engaño y capturar información de autenticación en tiempo real.

MITRE ATT&CK:

- T1583.001: Acquire Infrastructure, Domains.

FASE 2. SUPLANTACIÓN DEL PERSONAL DE SOPORTE MEDIANTE VISHING

El atacante realiza llamadas telefónicas a empleados o integrantes de la mesa de ayuda y se presenta como miembro del área de tecnología, soporte técnico o gestión de identidades.

Durante la llamada puede informar sobre:

- una supuesta actualización de MFA
- una migración de la cuenta corporativa
- la activación de una passkey
- un problema de acceso que requiere validación inmediata
- la necesidad de registrar nuevamente el dispositivo
- una supuesta actualización de una aplicación empresarial

El objetivo es generar confianza y lograr que el usuario siga instrucciones relacionadas con su cuenta corporativa.

MITRE ATT&CK:



- T1598.004: Phishing for Information, Spearphishing Voice.

FASE 3. CAPTURA DE CREDENCIALES, CÓDIGOS MFA O AUTORIZACIÓN OAUTH

La campaña presenta dos rutas principales de compromiso.

Ruta A. Captura de credenciales y MFA

El atacante dirige al usuario hacia un portal falso personalizado, donde solicita:

- nombre de usuario
- contraseña corporativa
- código de autenticación multifactor
- aprobación de una notificación MFA
- información para el registro de un nuevo dispositivo

Los datos son capturados mientras la víctima permanece en la llamada, lo que permite al atacante utilizarlos inmediatamente antes de que los códigos temporales expiren.

Ruta B. Abuso del consentimiento OAuth

En otros incidentes, el atacante guía al usuario para que autorice una aplicación conectada controlada por el adversario. Microsoft observó aplicaciones maliciosas presentadas como herramientas legítimas, entre ellas aplicaciones que simulaban ser Salesforce Data Loader.

Al aceptar la autorización, la aplicación obtiene permisos heredados de la cuenta del usuario y puede ejecutar consultas mediante API sin conocer necesariamente su contraseña.

MITRE ATT&CK:

- T1598.003: Phishing for Information, Spearphishing Link.
- T1056.003: Input Capture, Web Portal Capture.
- T1528: Steal Application Access Token.

FASE 4. COMPROMISO DE LA CUENTA Y PERSISTENCIA EN EL SISTEMA DE IDENTIDAD

Después de capturar las credenciales y los códigos MFA, el atacante accede a la cuenta corporativa mediante el proveedor de identidad utilizado por la organización, como Microsoft Entra, Okta o Google.



En algunos incidentes, los actores registraron dispositivos propios como nuevos factores de autenticación. Esto les permitió mantener el acceso y superar futuros controles MFA.

También pueden conservar acceso mediante:

- sesiones autenticadas
- tokens de acceso o actualización
- aplicaciones OAuth autorizadas
- dispositivos registrados
- integraciones SaaS comprometidas

El cambio aislado de contraseña podría no eliminar estos mecanismos de persistencia.

MITRE ATT&CK:

- T1078.004: Valid Accounts, Cloud Accounts.
- T1098.005: Account Manipulation, Device Registration.
- T1528: Steal Application Access Token.

FASE 5. DESCUBRIMIENTO Y ENUMERACIÓN DE SERVICIOS SaaS

Una vez dentro de la cuenta SSO o de una aplicación conectada, el atacante identifica los servicios, permisos, repositorios y fuentes de información disponibles para la identidad comprometida.

Las actividades observadas incluyen:

- enumeración de instancias de Salesforce
- consulta de registros CRM
- identificación de aplicaciones conectadas
- revisión de servicios accesibles mediante SSO
- exploración de Microsoft 365, SharePoint y OneDrive
- identificación de información almacenada en Slack y otros servicios SaaS
- análisis de los permisos asociados a la sesión comprometida

El acceso posterior es en gran medida oportunista y depende de los permisos que tenga la cuenta afectada.



MITRE ATT&CK:

- T1526: Cloud Service Discovery.
- T1087.004: Account Discovery, Cloud Account.

FASE 6. BÚSQUEDA Y RECOLECCIÓN DE INFORMACIÓN SENSIBLE

Los atacantes realizan consultas y búsquedas dirigidas para identificar información útil para la extorsión.

Google observó búsquedas de documentos que contenían expresiones como:

- confidential
- internal
- proposal
- salesforce
- VPN
- POC

También se identificó interés en información personal, registros CRM, comunicaciones internas, archivos de SharePoint y posibles datos almacenados en aplicaciones de mensajería empresarial.

En una organización de salud, el alcance potencial dependerá de los permisos de la cuenta y de la información almacenada en las plataformas comprometidas. No debe afirmarse que existió acceso a historias clínicas, laboratorios o imágenes diagnósticas sin evidencia específica del incidente.

MITRE ATT&CK:

- T1213.002: Data from Information Repositories, SharePoint.
- T1213.004: Data from Information Repositories, Customer Relationship Management Software.
- T1213.005: Data from Information Repositories, Messaging Applications.
- T1530: Data from Cloud Storage.

FASE 7. EXFILTRACIÓN DE INFORMACIÓN MEDIANTE SERVICIOS LEGÍTIMOS

Los actores descargan o consultan información utilizando las funciones normales de las plataformas SaaS comprometidas.

Las acciones pueden incluir:

- descargas masivas de archivos
- consultas de grandes volúmenes de registros CRM
- acceso automatizado mediante API
- exportación de información desde aplicaciones autorizadas
- descarga de documentos desde SharePoint o OneDrive
- consulta de comunicaciones internas

Microsoft indicó que estas actividades pueden no generar anomalías tradicionales de inicio de sesión, debido a que se ejecutan mediante identidades, tokens y aplicaciones autorizadas.

MITRE ATT&CK:

- T1567: Exfiltration Over Web Service.

FASE 8. EXTORSIÓN Y PRESIÓN SOBRE LA ORGANIZACIÓN

Después de extraer la información, los responsables pueden contactar a la organización, presentar muestras de los datos obtenidos y exigir un pago para evitar su publicación.

En algunos incidentes asociados a operaciones con la marca ShinyHunters también se han reportado:

- amenazas de divulgación en sitios de filtración
- contacto directo con empleados
- hostigamiento a personal de la organización
- presión reputacional
- divulgación parcial de información robada
- exigencias económicas

El modelo observado se basa principalmente en robo de información y extorsión. No requiere necesariamente cifrar archivos ni desplegar ransomware dentro de la infraestructura de la víctima.



MITRE ATT&CK:

- T1657: Financial Theft, aplicable al objetivo económico de extorsión.

Consideración técnica

Las fuentes públicas analizadas no permiten afirmar que esta campaña incluya de forma generalizada:

- movimiento lateral mediante SMB, RDP o WinRM
- compromiso de Active Directory
- escalamiento a Domain Admin
- abuso de tickets Kerberos
- instalación de malware infostealer
- despliegue de ransomware
- eliminación de copias de seguridad
- compromiso directo de servidores clínicos

Vulnerabilidades asociadas

La campaña asociada a ShinyHunters no se basa principalmente en la explotación de vulnerabilidades de software identificadas mediante códigos CVE. Su efectividad depende del abuso de la confianza de los usuarios, procedimientos débiles de verificación de identidad, configuraciones inseguras de autenticación, permisos excesivos y visibilidad limitada sobre aplicaciones SaaS, sesiones y relaciones OAuth.

Google Threat Intelligence y Microsoft han indicado expresamente que los incidentes observados no fueron consecuencia de vulnerabilidades inherentes en las plataformas afectadas, sino del abuso de procesos y funcionalidades legítimas.



1. Ingeniería social mediante llamadas fraudulentas

MITRE ATT&CK: T1598.004, Phishing for Information: Spearphishing Voice

Descripción

Los atacantes realizan llamadas de vishing y se hacen pasar por integrantes del área de tecnología, soporte técnico o mesa de ayuda. Durante la comunicación pueden informar sobre una supuesta actualización de MFA, migración de la cuenta, activación de una passkey o problema urgente de acceso.

El objetivo es convencer al usuario para que revele información, visite un portal de autenticación falso o autorice una acción controlada por el atacante. MITRE clasifica esta conducta como spearphishing de voz.

Debilidades asociadas

- Ausencia de procedimientos de devolución de llamada a números institucionales previamente registrados.
- Restablecimiento de contraseñas o MFA durante la misma llamada recibida.
- Verificación de identidad basada únicamente en información personal conocida.
- Falta de capacitación frente a llamadas de soporte no solicitadas.
- Exposición pública de nombres, cargos, teléfonos y estructura organizacional.
- Falta de canales sencillos para reportar llamadas sospechosas.

2. Captura de credenciales y códigos de autenticación

MITRE ATT&CK: T1056.003, Input Capture: Web Portal Capture

Descripción

Los atacantes utilizan portales falsos que imitan la identidad visual y la página de autenticación de la organización. La víctima es inducida a ingresar su usuario, contraseña y código MFA mientras permanece en comunicación con el supuesto técnico.



Los datos pueden utilizarse inmediatamente para iniciar sesión en el proveedor de identidad antes de que expire el código temporal. Google documentó dominios personalizados y páginas de captura diseñadas para obtener credenciales SSO y códigos MFA.

Debilidades asociadas

- Uso de MFA mediante SMS, códigos temporales o aprobaciones simples susceptibles a ingeniería social.
- Ausencia de autenticación resistente al phishing, como FIDO2 o passkeys.
- Falta de controles para detectar dominios similares al institucional.
- Ausencia de políticas que exijan dispositivos corporativos administrados.
- Falta de alertas ante autenticaciones desde dispositivos o ubicaciones nuevas.
- Capacitación insuficiente sobre portales falsos de autenticación.

3. Uso de cuentas válidas en servicios en la nube**MITRE ATT&CK: T1078.004, Valid Accounts: Cloud Accounts****Descripción**

Después de obtener las credenciales, los atacantes acceden a servicios corporativos mediante cuentas legítimas. Esto les permite utilizar Microsoft Entra, Okta, Google, Microsoft 365, Salesforce y otras aplicaciones conectadas con los permisos asignados al usuario comprometido.

El uso de cuentas válidas puede dificultar la identificación del incidente cuando la organización no analiza el contexto de la autenticación, la ubicación, el dispositivo, el riesgo de sesión y la actividad posterior.

Debilidades asociadas

- Falta de políticas de acceso condicional.
- Ausencia de controles de geovelocidad o desplazamiento imposible.
- Permiso de acceso desde dispositivos no administrados.



- Protocolos de autenticación heredados habilitados.
- Falta de análisis de riesgo de usuario y de sesión.
- Cuentas privilegiadas utilizadas para actividades cotidianas.
- Privilegios superiores a los requeridos para la función del usuario.

4. Registro fraudulento de dispositivos MFA

MITRE ATT&CK: T1098.005, Account Manipulation: Device Registration

Descripción

En algunos incidentes, después de obtener las credenciales y superar el primer control MFA, los atacantes registraron dispositivos propios como nuevos factores de autenticación.

Este procedimiento puede proporcionar persistencia, debido a que el dispositivo del atacante queda reconocido por el sistema de identidad y puede utilizarse en futuras autenticaciones.

Debilidades asociadas

- Registro de nuevos factores MFA sin reautenticación reforzada.
- Procesos de autoservicio que permiten vincular dispositivos con controles mínimos.
- Ausencia de alertas ante inscripción o modificación de métodos MFA.
- Falta de inventario de dispositivos asociados a cada usuario.
- Falta de notificación al usuario cuando se registra un nuevo factor.
- Revocación incompleta de dispositivos después de un incidente.

5. Abuso del consentimiento y de las aplicaciones OAuth

MITRE ATT&CK:

- T1671, Cloud Application Integration.
- T1550.001, Use Alternate Authentication Material: Application Access Token.
- T1528, Steal Application Access Token.

Descripción



Microsoft observó campañas en las que los atacantes convencieron a los usuarios para autorizar aplicaciones conectadas controladas por el adversario. Algunas aplicaciones se presentaban como herramientas legítimas de carga o administración de datos.

Una vez autorizado el consentimiento OAuth, la aplicación puede realizar consultas mediante API con los permisos heredados del usuario. Esto permite acceso persistente y extracción de información sin utilizar malware ni solicitar nuevamente la contraseña en cada operación.

Debilidades asociadas

- Usuarios autorizados para aprobar libremente aplicaciones OAuth.
- Ausencia de aprobación administrativa para aplicaciones de alto riesgo.
- Permisos OAuth excesivos o sin justificación operativa.
- Falta de inventario de aplicaciones conectadas.
- Aplicaciones antiguas o no utilizadas que conservan permisos.
- Falta de revisión de tokens de acceso y actualización.
- Revocación incompleta de consentimientos después de recuperar una cuenta.
- Escasa supervisión de integraciones realizadas por terceros.

6. Enumeración de servicios y aplicaciones SaaS

MITRE ATT&CK: T1526, Cloud Service Discovery

Descripción

Una vez comprometida la identidad, el atacante puede identificar las aplicaciones, servicios, integraciones y repositorios disponibles mediante SSO o API.

La enumeración permite determinar qué plataformas contienen información de mayor valor y cuáles pueden ser consultadas con los privilegios de la cuenta comprometida. MITRE contempla esta actividad como descubrimiento de servicios en la nube.



Debilidades asociadas

- Integración de numerosas aplicaciones mediante una misma identidad SSO.
- Permisos generales para acceder a servicios que no son necesarios para la función del usuario.
- Falta de revisión periódica de aplicaciones asignadas.
- Ausencia de segregación entre cuentas clínicas, administrativas y privilegiadas.
- Falta de alertas ante enumeración anómala de aplicaciones, usuarios o recursos.
- Inventarios incompletos de servicios SaaS utilizados por la organización.

7. Acceso y recolección de información en repositorios SaaS**MITRE ATT&CK:**

T1213.002, Data from Information Repositories: SharePoint.

T1213.004, Data from Information Repositories: Customer Relationship Management Software.

T1213.005, Data from Information Repositories: Messaging Applications.

T1530, Data from Cloud Storage.

Descripción

Los atacantes buscan información sensible en SharePoint, OneDrive, plataformas CRM, mensajería corporativa y otros repositorios accesibles desde la sesión comprometida.

Google documentó búsquedas de documentos confidenciales, información personal identificable, datos internos, referencias a VPN y registros almacenados en Salesforce. El alcance depende de los permisos del usuario y de la información disponible en las plataformas conectadas.

Debilidades asociadas

- Almacenamiento de información sensible en repositorios con acceso amplio.
- Permisos de lectura heredados o asignados a grupos demasiado extensos.



- Enlaces públicos o externos sin fecha de vencimiento.
- Falta de clasificación y etiquetado de información sensible.
- Ausencia de controles de prevención de pérdida de datos.
- Falta de alertas ante búsquedas, consultas o descargas masivas.
- Conservación innecesaria de documentos antiguos o datos sensibles.

8. Exfiltración mediante servicios y API legítimas

MITRE ATT&CK: T1567, Exfiltration Over Web Service

Descripción

La información puede ser extraída utilizando funciones normales de exportación, descarga o consulta mediante API. Debido a que estas operaciones se realizan desde aplicaciones autorizadas y servicios web legítimos, pueden no ser detectadas por controles tradicionales centrados en malware o tráfico de comando y control.

Microsoft indicó que las aplicaciones OAuth comprometidas permitieron enumerar y consultar registros a gran escala mientras evitaban controles convencionales de autenticación.

Debilidades asociadas

- Falta de límites sobre consultas y exportaciones de información.
- Ausencia de líneas base sobre el volumen normal de descargas por usuario.
- Monitoreo insuficiente de llamadas API.
- SIEM sin integración con registros de Microsoft 365, Salesforce, Okta u otras plataformas SaaS.
- Falta de atribución de actividad a la aplicación conectada que realizó la consulta.
- Ausencia de alertas ante descargas realizadas en horarios, ubicaciones o dispositivos atípicos.

9. Abuso de relaciones de confianza con terceros

MITRE ATT&CK: T1199, Trusted Relationship



Descripción

Microsoft también identificó una ruta de compromiso basada en proveedores e integraciones SaaS de terceros. El acceso a credenciales, secretos de conexión o tokens utilizados por una aplicación confiable puede permitir que el atacante alcance organizaciones clientes conectadas a ese servicio.

Esta situación amplía el riesgo más allá de las cuentas internas, debido a que una integración autorizada puede conservar permisos sobre información corporativa de varias organizaciones.

Debilidades asociadas

- Falta de evaluación de seguridad de proveedores SaaS.
- Integraciones con permisos superiores a los estrictamente necesarios.
- Tokens de terceros con vigencia prolongada.
- Ausencia de rotación de secretos y credenciales de integración.
- Falta de procedimientos para revocar rápidamente accesos de proveedores.
- Inventario incompleto de relaciones OAuth y conexiones entre plataformas.
- Falta de monitoreo independiente de las acciones realizadas por aplicaciones de terceros.

Recomendaciones de detección y mitigación

Para reducir el impacto de campañas asociadas a ShinyHunters en organizaciones del sector salud, es necesario fortalecer los controles de identidad, monitoreo de servicios SaaS, autenticación multifactor y análisis de comportamiento de usuarios.

La principal superficie de ataque no corresponde a una vulnerabilidad técnica tradicional, sino al abuso de identidades legítimas, procedimientos de soporte, configuraciones de autenticación y permisos excesivos dentro de plataformas en la nube.

DETECCIÓN EN SIEM / SOC (MONITOREO AVANZADO)**Detección de accesos anómalos de identidad**

Configurar alertas para:

- Inicio de sesión desde ubicaciones geográficas inusuales.
- Accesos desde dispositivos no registrados previamente.
- Autenticaciones exitosas posteriores a múltiples intentos fallidos.
- Inicio de sesión en horarios atípicos.
- Uso de cuentas administrativas desde ubicaciones no habituales.
- Accesos simultáneos desde diferentes regiones.

MITRE ATT&CK:

- T1078.004 – Valid Accounts: Cloud Accounts.

Objetivo:

Detectar el uso de credenciales legítimas obtenidas mediante ingeniería social.

Detección de cambios en métodos MFA

Monitorear:

- Registro de nuevos dispositivos MFA.
- Cambios inesperados en factores de autenticación.
- Eliminación o modificación de métodos MFA existentes.
- Activación de passkeys o dispositivos desconocidos.
- Cambios realizados inmediatamente después de una llamada de soporte.

MITRE ATT&CK:

- T1098.005 – Account Manipulation: Device Registration.

Objetivo:

Detectar intentos de persistencia mediante dispositivos controlados por el atacante.

Detección de abuso OAuth y aplicaciones conectadas

Generar alertas sobre:

- Nuevas aplicaciones autorizadas por usuarios.
- Consentimientos OAuth de aplicaciones desconocidas.
- Aplicaciones con permisos elevados.
- Acceso mediante API desde aplicaciones no aprobadas.
- Uso de tokens desde ubicaciones o dispositivos diferentes.

MITRE ATT&CK:

- T1528 – Steal Application Access Token.
- T1550.001 – Application Access Token.

Objetivo:

Identificar aplicaciones maliciosas o accesos persistentes mediante integraciones SaaS.

Detección de extracción anómala de información

Monitorear:

- Descargas masivas desde SharePoint y OneDrive.
- Exportaciones inusuales desde plataformas CRM.
- Consultas automatizadas mediante API.
- Acceso repetitivo a grandes cantidades de documentos.
- Actividad elevada en cuentas que normalmente no realizan consultas masivas.

MITRE ATT&CK:

- T1530 – Data from Cloud Storage.
- T1567 – Exfiltration Over Web Service.

Objetivo:

Detectar actividades relacionadas con robo y extracción de información.

SEGURIDAD EN SERVICIOS DE IDENTIDAD (IAM)

Controles recomendados:

- Implementar MFA resistente al phishing mediante FIDO2 o passkeys.
- Aplicar acceso condicional basado en riesgo.
- Restringir autenticaciones desde dispositivos no administrados.
- Bloquear autenticaciones heredadas.
- Implementar revisión periódica de permisos asignados.
- Aplicar principio de mínimo privilegio.

MITRE ATT&CK:

- T1078 – Valid Accounts.

CONTROL DE APLICACIONES SaaS Y OAUTH

Implementar:

- Aprobación administrativa para nuevas aplicaciones empresariales.
- Inventario permanente de aplicaciones conectadas.
- Revisión de permisos OAuth otorgados.
- Eliminación de aplicaciones sin uso.
- Rotación periódica de tokens y secretos.
- Supervisión de integraciones con terceros.

Objetivo:

Evitar que aplicaciones autorizadas sean utilizadas como mecanismo de persistencia.

SEGURIDAD DEL CORREO Y COMUNICACIONES

Aunque la campaña se enfoca principalmente en vishing, se recomienda:



- Mantener filtros anti-phishing avanzados.
- Bloquear dominios sospechosos y recién registrados.
- Implementar SPF, DKIM y DMARC.
- Analizar enlaces sospechosos.
- Capacitar usuarios frente a comunicaciones falsas de soporte técnico.

GESTIÓN DEL FACTOR HUMANO

Implementar:

- Capacitación específica contra llamadas fraudulentas.
- Procedimientos para validar solicitudes del área TI.
- Prohibición de entregar códigos MFA por teléfono.
- Confirmación por canales alternos antes de modificar cuentas.
- Canal rápido de reporte de incidentes.

La mesa de ayuda debe contar con procedimientos estrictos para evitar que un atacante pueda restablecer credenciales o modificar factores MFA mediante ingeniería social.

RECOMENDACIONES DE RESPUESTA ANTE COMPROMISO

Contención inmediata

Ante sospecha de compromiso:

- Bloquear temporalmente la cuenta afectada.
- Revocar sesiones activas.
- Eliminar dispositivos MFA no reconocidos.
- Revocar tokens OAuth activos.
- Deshabilitar aplicaciones sospechosas conectadas.
- Cambiar credenciales comprometidas.

Objetivo:

Eliminar la capacidad del atacante de continuar utilizando la identidad comprometida.



Preservación de evidencia

Recolectar:

- Registros de autenticación.
- Historial de cambios MFA.
- Eventos de Microsoft Entra, Okta o proveedor de identidad utilizado.
- Aplicaciones OAuth autorizadas.
- Registros de descarga y acceso a documentos.
- Actividad realizada mediante API.

Objetivo:

Determinar el alcance real del compromiso.

Análisis del incidente

Validar:

- Usuarios afectados.
- Sistemas SaaS comprometidos.
- Información consultada o descargada.
- Aplicaciones autorizadas durante el incidente.
- Dispositivos registrados por el atacante.
- Tokens o sesiones persistentes.

MITRE ATT&CK:

- T1078 – Valid Accounts.
- T1528 – Steal Application Access Token.
- T1530 – Data from Cloud Storage.

Recuperación

Ejecutar:



- Restablecimiento seguro de cuentas.
- Reinscripción de MFA legítimo.
- Revocación completa de sesiones.
- Eliminación de aplicaciones no autorizadas.
- Revisión de permisos del usuario comprometido.
- Monitoreo reforzado posterior al incidente.

Notificación y cumplimiento

Evaluar:

- Activación del equipo CSIRT/SOC.
- Comunicación con áreas jurídicas y cumplimiento.
- Evaluación de afectación de datos personales.
- Aplicación de obligaciones derivadas de la Ley 1581 de 2012 cuando corresponda.

Lecciones aprendidas

Después del incidente:

- Ajustar reglas de detección de identidad.
- Mejorar controles de MFA.
- Revisar procedimientos de mesa de ayuda.
- Reducir permisos excesivos en SaaS.
- Fortalecer entrenamiento del personal.
- Auditar aplicaciones OAuth y accesos de terceros.

La defensa contra campañas como ShinyHunters requiere priorizar la protección de identidad digital, debido a que el atacante busca operar con accesos legítimos y aprovechar la confianza depositada en usuarios, aplicaciones y procesos internos.

Conclusiones



La presente alerta de ciberseguridad evidencia una evolución en las campañas dirigidas contra organizaciones del sector salud y tecnología médica, donde los actores maliciosos han desplazado el enfoque tradicional basado exclusivamente en explotación de vulnerabilidades técnicas hacia el compromiso de identidades digitales mediante ingeniería social, suplantación de personal de soporte, captura de credenciales, abuso de autenticación multifactor y manipulación de aplicaciones conectadas.

La campaña asociada a ShinyHunters demuestra que los atacantes pueden obtener acceso a entornos corporativos utilizando mecanismos legítimos de autenticación, lo que dificulta su detección mediante controles tradicionales enfocados únicamente en malware o vulnerabilidades conocidas. El uso de cuentas válidas, sesiones autenticadas, tokens de acceso y autorizaciones OAuth permite que las actividades maliciosas se desarrollen dentro de plataformas empresariales como servicios de identidad, correo corporativo, almacenamiento en la nube y aplicaciones SaaS.

El análisis permite concluir que el principal riesgo no se limita al robo inicial de credenciales, sino a la capacidad del atacante para mantener acceso mediante modificaciones en factores MFA, registro de dispositivos no autorizados, autorización de aplicaciones maliciosas y aprovechamiento de los permisos asignados a la identidad comprometida.

Para las organizaciones del sector salud, el impacto potencial es elevado debido a la cantidad de información sensible gestionada en plataformas digitales. Una cuenta comprometida puede permitir el acceso a documentos institucionales, comunicaciones internas, repositorios de información y servicios conectados, dependiendo de los privilegios asignados al usuario afectado.

Asimismo, se identifica que factores como la ausencia de autenticación resistente al phishing, controles débiles en los procesos de mesa de ayuda, exceso de permisos en aplicaciones SaaS, falta de monitoreo de cambios MFA y baja visibilidad sobre aplicaciones OAuth incrementan significativamente la probabilidad de compromiso.



La mitigación efectiva de esta amenaza requiere un enfoque basado en protección de identidad, bajo principios de Zero Trust, donde cada acceso sea validado considerando el usuario, dispositivo, ubicación, comportamiento y nivel de riesgo. Las organizaciones deben fortalecer sus capacidades de monitoreo continuo, análisis de comportamiento, gestión de aplicaciones conectadas y respuesta ante incidentes relacionados con cuentas comprometidas.

Finalmente, se recomienda a las entidades del sector salud fortalecer sus controles de autenticación, implementar mecanismos resistentes al phishing como FIDO2 o passkeys cuando sea posible, establecer procedimientos estrictos para la validación de solicitudes de soporte técnico, revisar periódicamente permisos y aplicaciones autorizadas, y mantener programas permanentes de capacitación al personal.

La protección frente a campañas como ShinyHunters requiere comprender que la identidad digital se ha convertido en uno de los principales activos de seguridad institucional, por lo que su protección debe ser considerada un componente crítico para garantizar la confidencialidad de la información, la continuidad operativa y la confianza de pacientes y usuarios.

Fuentes:



- **Health-ISAC – ShinyHunters Impact to Health Sector and Recommended Mitigation Strategies**

Alerta sectorial sobre la actividad de ShinyHunters contra organizaciones del sector salud y tecnología médica. Incluye técnicas observadas, afectación al sector, mecanismos de compromiso de identidad y recomendaciones de mitigación.

o <https://health-isac.org/shiny-hunters-impact-to-health-sector-and-recommended-mitigation-strategies/>



- **Google Threat Intelligence / Mandiant – Expansion of ShinyHunters SaaS Data Theft Operations**

Análisis técnico sobre campañas asociadas a ShinyHunters, incluyendo robo de identidad, vishing, captura de credenciales, abuso de MFA, compromiso de aplicaciones SaaS, OAuth y extracción de información mediante servicios legítimos.

o <https://cloud.google.com/blog/topics/threat-intelligence/expansion-shinyhunters-saas-data-theft>

- **Microsoft Security Blog – Defending SaaS-Based Applications Against ShinyHunters OAuth Abuse**

Investigación técnica sobre abuso de aplicaciones OAuth, consentimiento fraudulento, tokens de acceso y compromiso de aplicaciones conectadas en entornos Microsoft 365.

o <https://www.microsoft.com/en-us/security/blog/>

- **MITRE ATT&CK Framework – Enterprise Techniques**

Base de conocimiento oficial utilizada para la clasificación de técnicas asociadas a la campaña, incluyendo:

- o T1078 – Valid Accounts.
- o T1098.005 – Account Manipulation: Device Registration.
- o T1528 – Steal Application Access Token.
- o T1526 – Cloud Service Discovery.
- o T1530 – Data from Cloud Storage.
- o T1567 – Exfiltration Over Web Service.
- o T1598.004 – Phishing for Information: Spearphishing Voice.

o <https://attack.mitre.org/>



- **CISA Cybersecurity Alerts & Advisories**

Publicaciones oficiales sobre amenazas activas, protección de identidades, arquitectura Zero Trust y recomendaciones para organizaciones críticas.

o <https://www.cisa.gov/news-events/cybersecurity-advisories>

- **CISA Zero Trust Maturity Model**

Modelo oficial para fortalecer arquitecturas Zero Trust con enfoque en identidad, dispositivos, aplicaciones, datos y acceso seguro.

o <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>

- **Microsoft Security Intelligence & Defender Reports**

Reportes oficiales sobre amenazas contra identidades, Microsoft Entra, Microsoft 365, abuso de OAuth, phishing y compromiso de cuentas corporativas.

o <https://www.microsoft.com/en-us/security>

- **ENISA Threat Landscape (ETL)**

Informes europeos de inteligencia sobre amenazas que afectan sectores críticos, incluyendo salud, robo de identidad, phishing, ransomware y riesgos asociados a servicios digitales.

o <https://www.enisa.europa.eu/publications>

- **ENISA Cybersecurity Guidelines for Health Sector**

Lineamientos de ciberseguridad para entidades del sector salud, orientados a protección de información, continuidad operativa, gestión de incidentes y resiliencia digital.

o <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health>

- **Verizon Data Breach Investigations Report (DBIR)**

Informe anual de análisis de incidentes de seguridad que evidencia la importancia del factor humano, el phishing y el uso de credenciales válidas como vectores frecuentes de





Alerta Vulnerabilidad
Campaña ShinyHunters contra
salud y tecnología médica

CSIRTSALUD-AL-20260731-128

TLP: CLEAR

compromiso inicial.

o <https://www.verizon.com/business/resources/reports/dbir/>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

