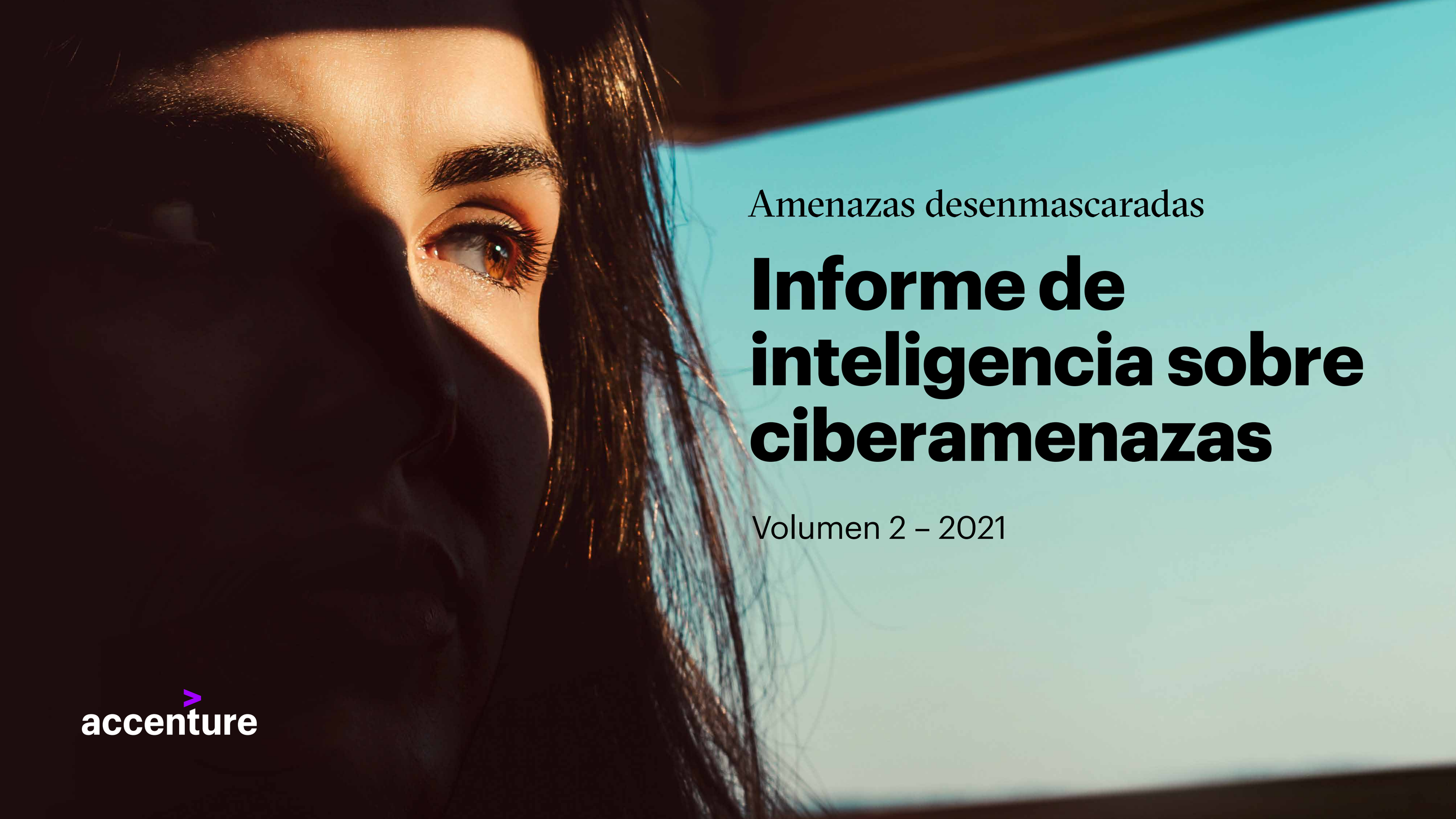


Amenazas desenmascaradas

Informe de inteligencia sobre ciberamenazas

Volumen 2 – 2021

accenture

Accenture lleva más de 20 años creando inteligencia sobre amenazas relevante, oportuna y procesable. Nuestros equipos de inteligencia sobre ciberamenazas y de respuesta a incidentes están investigando continuamente numerosos casos de ataques con motivación financiera y sospechas de ciberespionaje.

Durante estas investigaciones, nuestros analistas de inteligencia sobre amenazas y respuesta a incidentes han podido elucidar de primera mano las tácticas, técnicas y procedimientos (TTP) que emplean algunos de los ciberadversarios más sofisticados. Este informe refleja el análisis durante el segundo semestre del año natural 2021 (H2 2021).

Tendencias clave

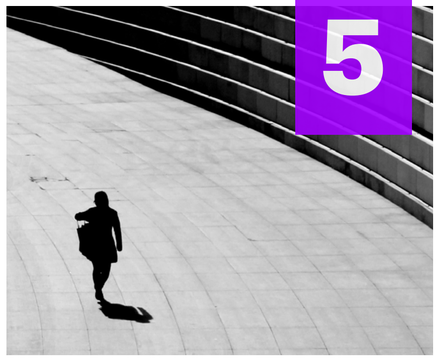
Tras el análisis realizado en el segundo semestre de 2021, Accenture identificó cinco tendencias que afectan al entorno de la ciberseguridad:

Los ataques de ransomware siguen siendo rentables

Las cadenas de suministro ofrecen un punto de ataque

Los ladrones de información impulsan el mercado del malware

La centralidad de la nube genera nuevos vectores de ataque



Los exploits de vulnerabilidad atraen un gran volumen de compras y ventas

Los ataques de ransomware siguen siendo rentables

A pesar de que la tecnología permite que los perpetradores de amenazas se vuelvan más sofisticados, todavía existen riesgos activos y en evolución derivados de las técnicas probadas de ransomware. Y hay una coherencia en la clasificación de las industrias más atacadas a lo largo del tercer trimestre del año natural 2021: los perpetradores de amenazas de ransomware han tenido más éxito contra la industria manufacturera, seguida por los servicios financieros, la atención de la salud, la tecnología y la construcción.

Los ataques de ransomware siguieron siendo **rentables**; entre los grupos de ransomware más activos en 2021 se encontraban LockBit y Conti, pero el seguimiento de los grupos individuales aún es difícil por las continuas "retiradas" y por la reinvención en nuevos grupos debido a la presión de los organismos de seguridad o a la dinámica interna del grupo.

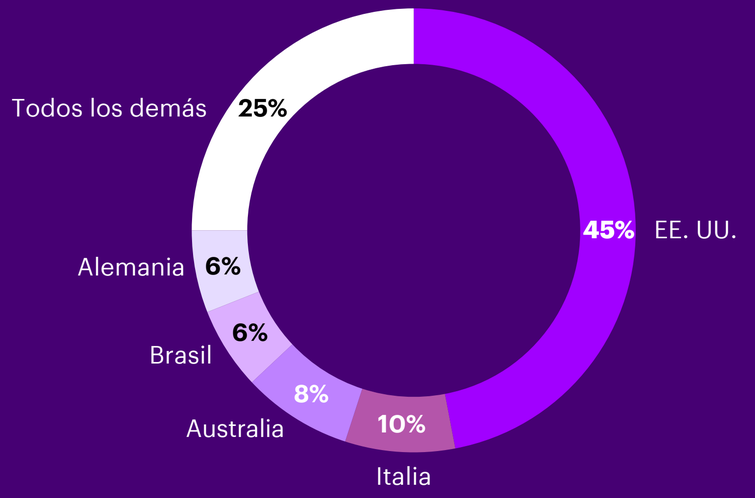
Los **conflictos** entre los **afiliados** de ransomware y sus operadores dieron lugar a fugas de información. Las discusiones entre las partes implicadas son un ejemplo de las consecuencias imprevistas de los planes de pago de **rescates a los afiliados**. A pesar de estos problemas, las operaciones de ransomware siguen siendo muy **rentables**.

Es más, los operadores de ransomware abusaron de manera creciente de la infraestructura de la nube e introdujeron nuevas técnicas de encriptación para evadir mejor la detección y aumentar el impacto.

Según los datos recogidos por Accenture de los compromisos de respuesta a incidentes, las operaciones de ransomware y extorsión representaron casi 35 % del volumen de intrusiones en 2021, con un aumento interanual del 107 % con respecto a 2020.

Además, Estados Unidos fue nuevamente la principal región afectada por las amenazas de ransomware y extorsión y representó aproximadamente el 45 % del volumen de intrusiones en 2021 (Figura 1).

Figura 1. Ransomware por geografía (respuesta a incidentes)

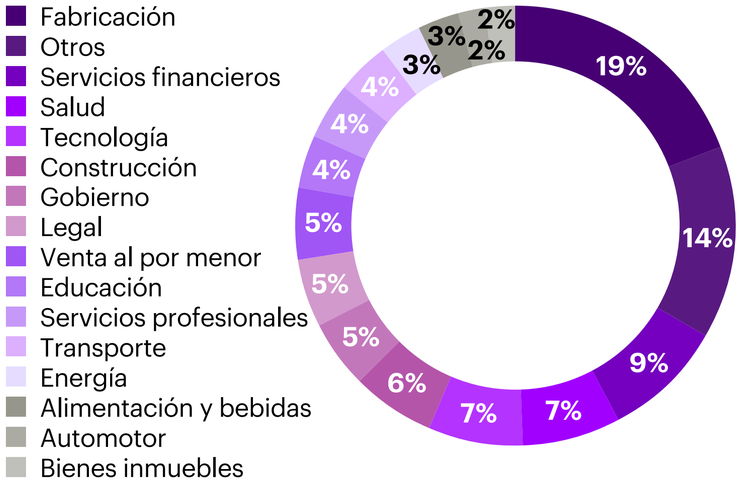


¿Qué está ocurriendo?

Los cuatro objetivos principales de la industria siguen siendo los mismos

El número de ataques de ransomware disminuyó ligeramente en el tercer trimestre en comparación con el segundo del año natural 2021, y la industria manufacturera, los servicios financieros, la atención médica y la tecnología siguen siendo los sectores más atacados. Los ataques contra el sector de la construcción aumentaron, convirtiéndolo en el quinto sector más atacado durante el tercer trimestre (ver la Figura 2).

Figura 2. 15 sectores más atacados por el ransomware en el tercer trimestre de 2021



El nuevo foro de RAMP causa revuelo

Tras la disolución del grupo DarkSide después del ataque a Colonial Pipeline,[1] en septiembre de 2021 surgió el colectivo de ransomware Groove, que creó el foro RAMP, el cual conecta a los afiliados huérfanos con los operadores de ransomware como servicio (RaaS).

La aparición de este foro podría significar un crecimiento continuo para la actividad de RaaS y supone una amenaza significativa y continua para las empresas.

La información en los medios de comunicación aumenta el impacto

La información activa de los medios de comunicación refleja una cultura de "primicia y escándalo" en la comunidad de la ciberseguridad y aumenta involuntariamente la influencia de los perpetradores de las ciberamenazas. Los ciberdelincuentes utilizaron esta publicidad en el tercer trimestre del año natural 2021 para criticar a sus rivales y aumentar la presión sobre las víctimas.

Las disputas entre afiliados van en aumento

Hay un número creciente de disputas entre los afiliados al ransomware y los operadores de grupos de ransomware. Los antiguos afiliados de los grupos de ransomware divulgaron información sensible, lo que llevó a la proliferación de potentes herramientas y técnicas de ransomware.

No todo se reduce al cuaderno de estrategias de los ataques

El grupo de amenazas de ransomware Conti sugiere que los afiliados a Conti tienden a utilizar opciones como las redes de bots de ciberdelincuencia bien establecidas, el spam malicioso y el phishing de objetivo definido.

La nube juega a favor del ransomware

Los entornos en la nube eran y siguen siendo objetivos atractivos, quizás debido a los niveles de supervisión más bajos que los entornos locales. De este modo, en 2021, el malware relacionado con la nube ha evolucionado más rápido que el malware

más tradicional, basándose en el análisis de la tasa de cambios de código entre los criptomineros (uno de los principales programas maliciosos desplegados en entornos de nube comprometidos) en comparación con los cambios de código en las redes de bots y el ransomware. Esta comparación de la tasa de cambio de código pone de manifiesto la importante inversión de los perpetradores de amenazas en herramientas centradas en la nube, especialmente en la modificación de herramientas preexistentes.[2]

En muchos de los compromisos asumidos para dar respuesta a incidentes en 2021, Accenture observó que los operadores de ransomware y extorsión apuntaban a la infraestructura de la nube y a las copias de seguridad alojadas en sus intentos de aumentar el impacto operativo. Esto incluía la explotación de la federación de identidades SAML (Security Assertion Markup Language 2.0) en uso para acceder a Amazon Web Services (AWS) a través de Microsoft Azure Active Directory (Azure AD), mediante el uso de credenciales previamente comprometidas para permitir el acceso no autorizado de la consola a a varios recursos de AWS y respaldar otros objetivos.[3] Al menos un grupo de ransomware utilizó un conjunto de herramientas ofensivas en la nube que los investigadores de Vx- underground filtraron del grupo de amenazas TeamTNT en octubre de 2021; este conjunto de herramientas se especializa en operaciones de criptominado malicioso. Este uso indica una tendencia en el desarrollo de herramientas personalizadas por parte de los grupos de ransomware para atacar cada vez más la infraestructura de la nube.[4]

Los miembros de foros clandestinos están comerciando con los accesos a los endpoints

Los foros clandestinos muestran un mayor interés por acceder a redes privadas virtuales (VPN) comprometidas, a través de credenciales robadas y el uso de exploits públicos y de día cero.

Por ejemplo, el análisis de Accenture de los datos de los vendedores de acceso a la red de septiembre a noviembre de 2021 muestra que los actores maliciosos que venden accesos a la red de las víctimas en foros clandestinos obtuvieron casi todos esos accesos a través de VPNs cuyas credenciales fueron comprometidas y utilizadas por los perpetradores de la amenaza para autenticarse.[5]

La extorsión de datos aumenta sin el despliegue del ransomware

En la segunda mitad de 2021, Accenture observó que **nuevos grupos de amenazas** establecieron una infraestructura e intensificaron los ataques centrados exclusivamente en la exfiltración de datos y la extorsión, en lugar de los despliegues de ransomware más destructivos. Esperamos que esta tendencia siga aumentando en el primer trimestre de CY2022, ya que este enfoque simplificado permite la ejecución de ataques y posteriores intentos de extorsión con mayor rapidez y a escala.

Los actores infieren que hay personas con información privilegiada

Además de afirmar infundadamente que accedían a información privilegiada de Accenture, los actores que utilizan LockBit insinuaron en noviembre de 2021 que tenían información privilegiada de otra gran empresa.[6] Los programas robustos de amenazas internas pueden ayudar a confirmar o refutar rápidamente las afirmaciones de los perpetradores de amenazas que pueden tener la intención de engañar a los responsables de dar respuesta. Esto puede ser contraproducente para los perpetradores de la amenaza, ya que puede disminuir su credibilidad y, por lo tanto, sus posibilidades de obtener pagos de rescate.

¿Qué será lo próximo?

Las siguientes son algunas formas de defenderse de los ataques de ransomware:

- Incorporar los principios de confianza cero a la estrategia de seguridad de la organización para proteger los datos de los clientes y de la empresa.

- Establecer y poner en práctica un plan de continuidad de las operaciones (COOP) que incorpore la capacidad de recuperación en la respuesta corporativa e incluya mensajes públicos y comunicaciones internas, además de aplicar una política de copias de seguridad externas sólidas.

- Implementar un programa medible de formación y concienciación en materia de seguridad que se centre en educar a los usuarios para que piensen dos veces antes de hacer clic en los enlaces y para que identifiquen y denuncien con seguridad los correos electrónicos que puedan formar parte de una campaña de phishing.

- Establecer un programa de gestión de activos que incluya un inventario de soluciones de protocolo de escritorio remoto (RDP) y la implementación de soluciones VDI seguras y supervisadas. Limitar el uso de RDP, cerrar los puertos RDP no utilizados, aplicar la autenticación de dos factores y registrar los intentos de inicio de sesión en RDP.

- Gestionar los activos de la nube supervisando los endpoints y garantizando la visibilidad de los procesos.

- Parchear periódicamente los sistemas operativos, el software y el firmware.

- Incorporar planes de respuesta a los ataques de malware o de wiper en el plan COOP de la organización.

- Incorporar la inteligencia a la estrategia de ciberdefensa de la organización para supervisar la dinámica de los grupos de amenazas, los foros clandestinos y la evolución de las TTP a fin de actualizar las contramedidas de detección y respuesta.

- Rechazar las solicitudes de rescate: el gobierno de Estados Unidos alienta a las víctimas de ransomware a rechazar las solicitudes de rescate, ya que el pago de rescates solo anima a los perpetradores de la amenaza a atacar de nuevo.

Las organizaciones que decidan pagar un rescate deben:

- Informar inmediatamente del incidente a las fuerzas de seguridad y a la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA).

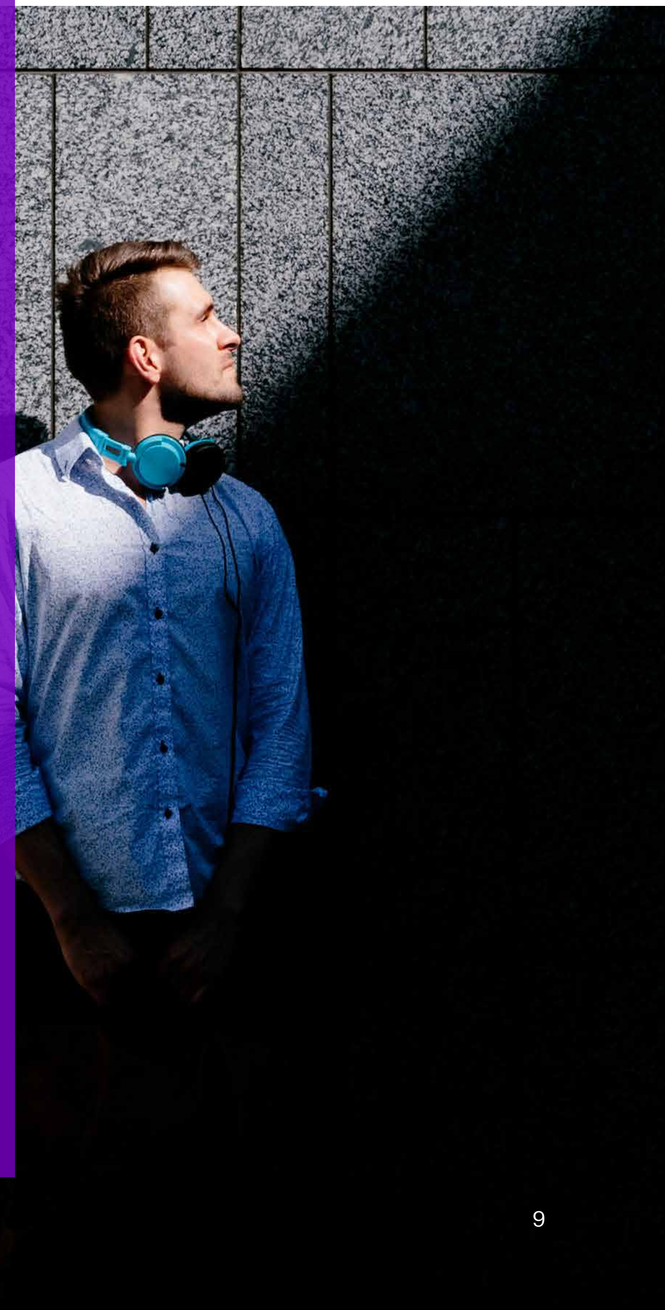
- Cooperar con las fuerzas del orden durante todo el proceso de recuperación del incidente.

- Implementar un programa de cumplimiento de sanciones para evaluar adecuadamente los riesgos. Si el grupo que pide el rescate es una entidad sancionada, ponerse en contacto con la Oficina de Control de Activos Extranjeros (OFAC) inmediatamente.

- Comprender que el pago de un rescate no garantiza la recuperación del acceso a las máquinas o a los datos bloqueados.

Las cadenas de suministro ofrecen un punto de ataque

Desde la revelación de la campaña de la cadena de suministro de SolarWinds en diciembre de 2020[7], cada vez más, los operadores maliciosos se han dado cuenta del potencial de los ataques a la cadena de suministro. Además de las complejidades de la gestión de activos y proveedores y de la visibilidad de la lista de materiales del software, el paso a la nube ha supuesto para muchas organizaciones un aumento del riesgo y de las consecuencias de las inseguridades en la cadena de suministro. Dichas vulnerabilidades pueden ser el resultado de posibles incidentes en la cadena de suministro en entornos completos, tanto locales como en la nube, que den servicio a una o varias entidades de negocio.



¿Qué está ocurriendo?

Se reportó un gran aumento de las amenazas

Durante los meses de octubre y noviembre de 2021, numerosas publicaciones sobre ciberseguridad mencionaron campañas de ataques a la cadena de suministro que hacían referencia a compromisos de bibliotecas de desarrolladores y plataformas de software.

Las amenazas de puerta trasera son más frecuentes

En el mismo periodo de tiempo, Accenture observó referencias a al menos nueve gestores de paquetes de nodos (NPM) maliciosos que se hacían pasar por paquetes legítimos. También había dos paquetes NPM legítimos con puertas traseras incorporadas que permitían a los perpetradores de amenazas eludir los canales normales de autenticación y emitir comandos de forma interactiva a un sistema.[8] NPM es un centro de intercambio de código JavaScript utilizado ampliamente por los desarrolladores de software.

Algunos paquetes de código NPM se descargan millones de veces por semana. Un paquete con una puerta trasera y una cadencia de descarga tan alta podría proporcionar puntos de apoyo iniciales al atacante en miles de redes víctimas o inquilinos de la nube. Los actores maliciosos pueden utilizar estos puntos de apoyo para una amplia variedad de propósitos, incluso para el criptominado malicioso[9] , el espionaje[10], el despliegue de ransomware y los ataques destructivos de wiper[11].

Según datos de intrusión tomados por Accenture de las iniciativas de respuesta a incidentes, el 30 % de las amenazas de malware que se observaron en 2021 fueron amenazas de puerta trasera, lo que las convierte en el segundo tipo de malware más prevalente, detrás del ransomware (33 %).

¿Qué será lo próximo?

Las siguientes son algunas formas de defenderse de los ataques a la cadena de suministro:

- **Integrar las auditorías:**
  Los administradores deben integrar las auditorías en los ciclos de DevOps. La necesidad de integrar la seguridad tanto en DevOps como en la incorporación de aplicaciones ha catalizado la integración de plataformas para el escaneo automatizado de código. Entre ellas se encuentran las plataformas inteligentes e integradas que ayudan a las organizaciones a desarrollar código más rápidamente con menores costos de reparación, mayor seguridad y menos personal. Por ejemplo, la plataforma **Intelligent Application Security Platform** de Accenture permite a los desarrolladores y a los líderes de equipo incorporar la seguridad a todos los ciclos de vida de las aplicaciones, desde el desarrollo hasta las pruebas y el despliegue, así como remediar automáticamente las vulnerabilidades de la base de código.[12]

- **Actualizar los marcos de seguridad:**
  Los administradores deben adoptar normas y utilizar herramientas de supervisión para satisfacer las exigencias de cumplimiento o inscribirse en ofertas de seguridad de aplicaciones como servicio para bloquear el acceso directo de los actores maliciosos a los entornos y repositorios sensibles, como las máquinas de los desarrolladores y los repositorios de código fuente. En el ataque a la cadena de suministro de SolarWinds, los actores maliciosos utilizaron una posición en las máquinas de los desarrolladores para inyectar código malicioso en la plataforma Orion de SolarWinds antes de que los desarrolladores de Orion compilaran y firmaran digitalmente el software de Orion.[13] Este tipo de incidentes pone de manifiesto la importancia de la seguridad de las aplicaciones y las graves consecuencias de su falla.

- **Proveedores de modelos de amenazas:** Los administradores y el personal de seguridad deben mirar más allá del software y examinar las dependencias de terceros más generales de sus organizaciones.

- **Programas maduros de la cadena de suministro de software:**
  Para reducir los riesgos asociados a las cadenas de suministro de software, debemos considerar la siguiente orientación:

  - **Consultar el documento "Best Practices in Cyber Supply Chain Risk Management"** ("Mejores prácticas en la gestión de riesgos en la cadena de suministro") del Instituto Nacional de Estándares y Tecnología, para obtener información sobre el mapeo de las cadenas de suministro, la identificación de proveedores críticos y la revisión de las prácticas de ciberseguridad del personal de los proveedores.

  - Revisar los niveles de privilegio y de acceso del software desarrollado externamente a nivel organizacional. Aunque la verificación de todo el software no sea un objetivo realista, las mejoras básicas pueden fortalecer drásticamente la postura de seguridad de una organización.

  - Revisar los acuerdos de nivel de servicio con los proveedores de software para localizar y corregir activamente el software vulnerable antes de su despliegue.

Los infostealers impulsan el mercado del malware

La creciente popularidad de los mercados clandestinos de endpoints que venden paquetes de datos de acceso comprometidos sigue siendo una amenaza sustancial para las organizaciones de todos los sectores y zonas geográficas. Los mercados de endpoints ofrecen una gran cantidad de puertas de entrada baratas a las redes corporativas.

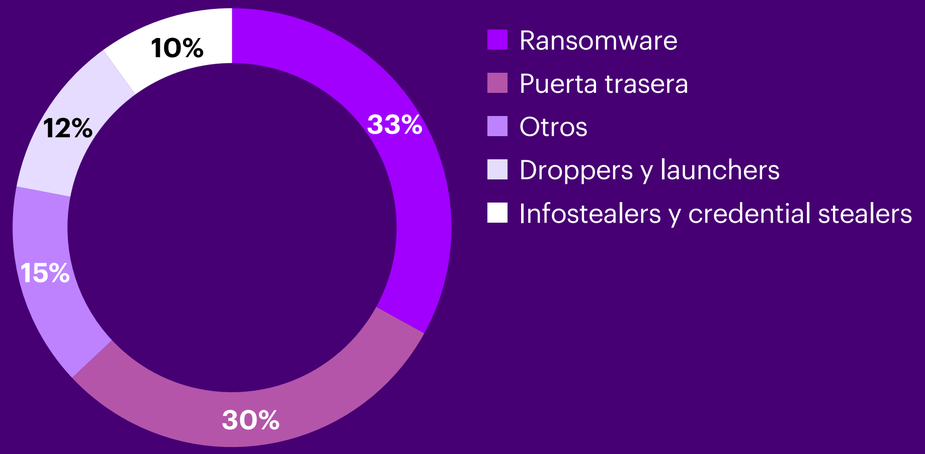
Los endpoints comprometidos – que los actores clandestinos han agrupado y vendido como los llamados “bots”–, contienen credenciales de acceso, información sensible del sistema y sesiones de cookies. Los actores extraen esta información de las máquinas de las víctimas utilizando malware de robo de credenciales y la venden en los mercados de la Dark Web por un precio ínfimo que oscila entre los 10 y los 200 dólares.

La investigación de Accenture muestra que los mercados de acceso a endpoints amenazan a la mayoría de las empresas medianas y grandes de todos los sectores y regiones geográficas, que se enfrentan a una exposición directa a través de las propias redes de la empresa o a través de compromisos de terceros.

Los ladrones de información (software malicioso conocido como infostealers) suelen estar diseñados para obtener (es decir, acceder o copiar) credenciales con una funcionalidad que va más allá del keylogging básico. Esto podría incluir nombres de usuario, contraseñas, claves, tokens, sesiones de cookies, etc.

Según datos de intrusión tomados por Accenture de los compromisos asumidos para dar respuesta a incidentes, la categoría combinada de infostealers y credential stealers (ladrones de información y de credenciales) constituyó aproximadamente el 10 % del malware observado durante las intrusiones en 2021 (Figura 3).

Figura 3. Malware por categoría (respuesta a incidentes)

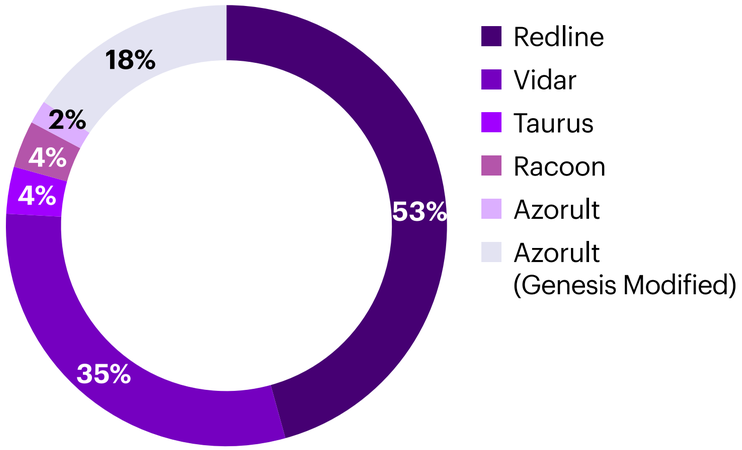


¿Qué está ocurriendo?

Los infostealers son muy activos

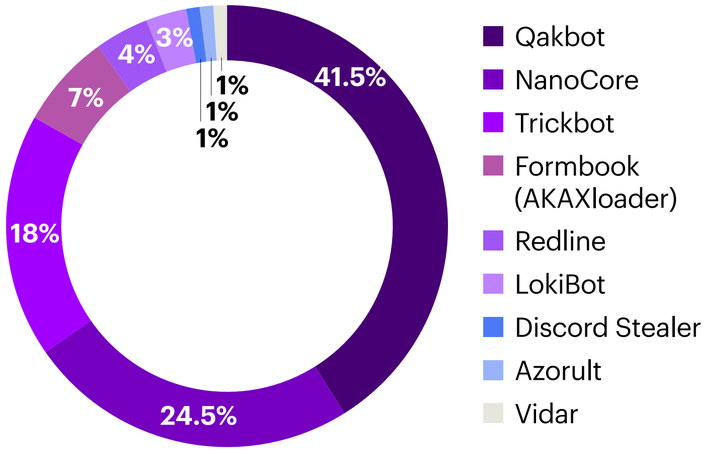
Según los datos disponibles, a noviembre de 2021, los infostealers más utilizados que proveen inventarios a los mercados clandestinos son Redline (53 %), Vidar (35 %), Taurus (4 %), Racoon (4 %) y Azorult (2 %) (ver la Figura 4).

Figura 4. Los infostealers alimentan los datos de los mercados de endpoints



Sin embargo, Accenture también encontró campañas de robo de información activas entre junio y noviembre de 2021 que utilizaban Qakbot y NanoCore con mayor frecuencia (ver Figura 5).

Figura 5. Robo de información utilizado por los actores maliciosos en las campañas de amenazas



La popularidad de los infostealers es variable

Los sesgos en la recopilación de datos explican en parte la discrepancia entre los infostealers utilizados en las campañas oportunamente activas y los que se utilizaron para volcar los inventarios en los mercados clandestinos. Sin embargo, esta incoherencia también pone de manifiesto la confianza de los mercados clandestinos en los nuevos infostealers, mientras que los grupos establecidos confían en infostealers de probada eficacia.

Y aunque Redline solo representa el 4 % de la cuota de mercado, el uso de este infostealer está creciendo a un ritmo más rápido que los demás. Redline ha ganado popularidad tras su participación en la filtración de datos de las entradas de los Juegos Olímpicos de Tokio de julio de 2021.[14] Redline infecta los sistemas a través de un cargador instalado por documentos maliciosos de Microsoft Word o Excel en correos electrónicos de phishing o mensajes de redes sociales.[15]

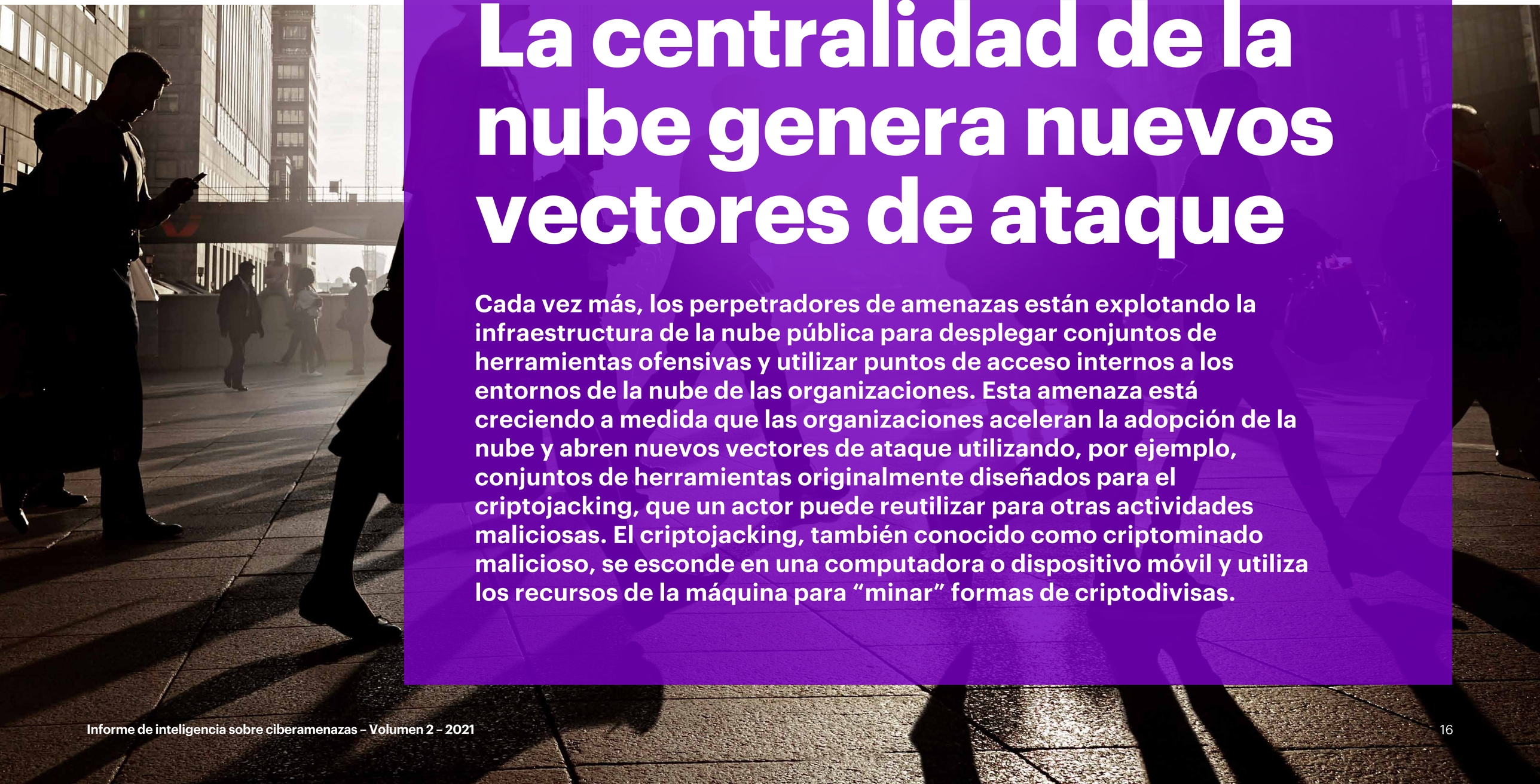
¿Qué será lo próximo?

Las siguientes son algunas formas en las que una organización puede posicionarse para hacer frente al software malicioso:

- **Proteger los entornos corporativos:**
  La investigación de Accenture muestra que, aunque los infostealers del mercado han infectado tanto las máquinas corporativas como las privadas, estas últimas crean una mayor exposición para ambas si son capaces de sincronizarse con la infraestructura corporativa. Esta sincronización permite a los infostealers evitar cada vez más las medidas de seguridad que ofrecen los entornos corporativos estrictos y les permite permanecer en los sistemas de las víctimas durante más tiempo, actualizando la información recabada a medida que cambia con el tiempo.

- **Tomar conciencia del creciente negocio de los "bots":**
  El número de los llamados "bots" (herramientas que incorporan la funcionalidad de credenciales de inicio de sesión, sesiones de cookies y "plugs" que permiten utilizar fácilmente los datos robados a través de un complemento del navegador) en venta en mercados clandestinos ha aumentado constantemente desde 2017: de aproximadamente 76.000 "bots" en venta entre diciembre de 2017 y diciembre de 2019 a más de 11 millones de "bots" en venta entre diciembre de 2019 y noviembre de 2021. Accenture atribuye este rápido aumento al entorno de trabajo remoto, acelerado por la pandemia de COVID-19 y al mayor uso de la autenticación multifactor (MFA), que ha aumentado la utilidad y el valor de estos "bots".

  Según la postura de seguridad de una corporación, estos "bots" pueden conceder acceso directo a los sistemas afectados o proporcionar a los actores hábiles una forma más fácil de entrar en las redes. El robo de una sesión de cookies activa hace que los "bots" sean significativamente más eficaces que el uso exclusivo de credenciales de acceso comprometidas. Como resultado, los grupos de ransomware, las redes de compromiso del correo electrónico empresarial y los extorsionistas de datos suelen utilizar los mercados de endpoints, y Accenture y otras organizaciones de ciberseguridad atribuyen múltiples ataques recientes al mercado de endpoints.[16]



La centralidad de la nube genera nuevos vectores de ataque

Cada vez más, los perpetradores de amenazas están explotando la infraestructura de la nube pública para desplegar conjuntos de herramientas ofensivas y utilizar puntos de acceso internos a los entornos de la nube de las organizaciones. Esta amenaza está creciendo a medida que las organizaciones aceleran la adopción de la nube y abren nuevos vectores de ataque utilizando, por ejemplo, conjuntos de herramientas originalmente diseñados para el criptojacking, que un actor puede reutilizar para otras actividades maliciosas. El criptojacking, también conocido como criptominado malicioso, se esconde en una computadora o dispositivo móvil y utiliza los recursos de la máquina para “minar” formas de criptodivisas.

What's happening?

El rápido crecimiento de la nube facilita las oportunidades de ataque
La pandemia de COVID-19 ha acelerado la tendencia ya existente de adopción de la nube para permitir el trabajo a distancia, la educación en línea, la resiliencia empresarial y la sostenibilidad medioambiental, abriendo nuevas superficies de ataque y aumentando el valor de los ataques a la infraestructura de la nube para los actores maliciosos.[17] "Las previsiones del gasto mundial de los usuarios finales en servicios de nube pública indican que alcanzará los 482.000 millones de dólares en 2022, lo que supone un aumento del 21,7 % respecto a los 396.000 millones de dólares previstos para 2021.[18]"

La ampliación de la infraestructura abre la puerta a nuevas vulnerabilidades
Algunas organizaciones no supervisan las plataformas en la nube tan minuciosamente como sus propios servidores locales, y esto puede agravar las deficiencias existentes en la gestión de los activos y de la configuración de la nube.

En lugar de ello, están depositando su confianza en un proveedor de la nube de terceros. Como resultado, los actores de las amenazas están secuestrando los servicios en la nube para explotar las ventajas de la infraestructura en la nube, recopilar datos sensibles y desplegar ransomware.

La expansión de la infraestructura en la nube también crea una infraestructura de mando y control muy escalable y fiable, además de redes de robots (botnets). Además, los entornos de nube públicos sirven como vectores de entrada iniciales a través de los cuales los perpetradores de amenazas pueden acceder a los dispositivos individuales de los endpoints.

Las amenazas de las herramientas centradas en la nube están aumentando
Accenture ha observado un conjunto de herramientas centradas en la nube muy evolucionado y activo por parte de TeamTNT, un grupo de amenazas prolífico en la minería de criptomonedas a través de la explotación de recursos en la nube, también conocido como cryptojacking.

El 29 de octubre de 2021, los investigadores de seguridad filtraron el conjunto de herramientas de TeamTNT para atacar plataformas en la nube de uso público.[19]
Accenture analizó los scripts filtrados de TeamTNT y evaluó que el grupo probablemente desplegó este conjunto de herramientas como parte de numerosas operaciones de criptojacking centradas en la nube.[20] Estas operaciones de criptojacking incluyen la campaña "Quimera", que TeamTNT supuestamente supervisó al menos desde julio de 2021 y que causó miles de infecciones en todo el mundo.[21]

Además de las actividades de criptojacking, el conjunto de herramientas de TeamTNT instaló un bot llamado "Tsunami" en los sistemas comprometidos. El código base de este bot es similar al del infame malware Mirai y puede abusar de la infraestructura orientada al público para ejecutar ataques de fuerza bruta, ejecutar escaneos globales de IP y lanzar ataques distribuidos de denegación de servicio.

Una vez que el bot Tsunami infecta los sistemas, el conjunto de herramientas de TeamTNT puede enumerar la infraestructura interna y desplegar ejecutables maliciosos, explotando plataformas en la nube como Google Cloud, Amazon AWS, Kubernetes y Dockers dentro de entornos Linux/Unix y Windows.

Los investigadores afirman que los grupos de extorsión de ransomware Conti y DarkMatter están utilizando activamente el archivo filtrado de TeamTNT.

Aunque Accenture no ha observado pruebas de afiliados al ransomware que desplieguen el conjunto de herramientas de TeamTNT, Accenture evalúa con un nivel de confianza alto que los perpetradores de amenazas moderadamente hábiles pueden desplegar fácilmente los scripts del conjunto de herramientas para comprometer los puntos de entrada de la nube privada y adaptar las funcionalidades de minería del código para encriptar los datos después del compromiso. Esta adaptación marcaría una evolución natural de las campañas de ransomware a medida que crece el interés de los grupos de ransomware por la infraestructura en la nube.

¿Qué será lo próximo?

A continuación se sugieren algunas formas de mitigar el impacto de las amenazas de las plataformas en la nube:

- **Auditar y comprobar las desconfiguraciones de la nube** junto con las iniciativas de digitalización de las operaciones de la organización.
- **Adoptar un marco de gestión de identidades y accesos** para supervisar y controlar los permisos de acceso de los usuarios de la nube.
- **Establecer la MFA** en los puntos de acceso a la nube y supervisar el acceso a la infraestructura de virtualización.

Los exploits de vulnerabilidad atraen un gran volumen de compras y ventas

Accenture ha observado un enorme crecimiento del mercado clandestino de exploits de vulnerabilidad, especialmente de aquellos que permiten a los adversarios obtener un acceso no autorizado a una red corporativa. Los mercados del ransomware y el acceso no autorizado a la red afectan sin duda de forma significativa a los mercados de exploits, ya que el acceso no autorizado a la red es fundamental para el éxito de las operaciones de ransomware.

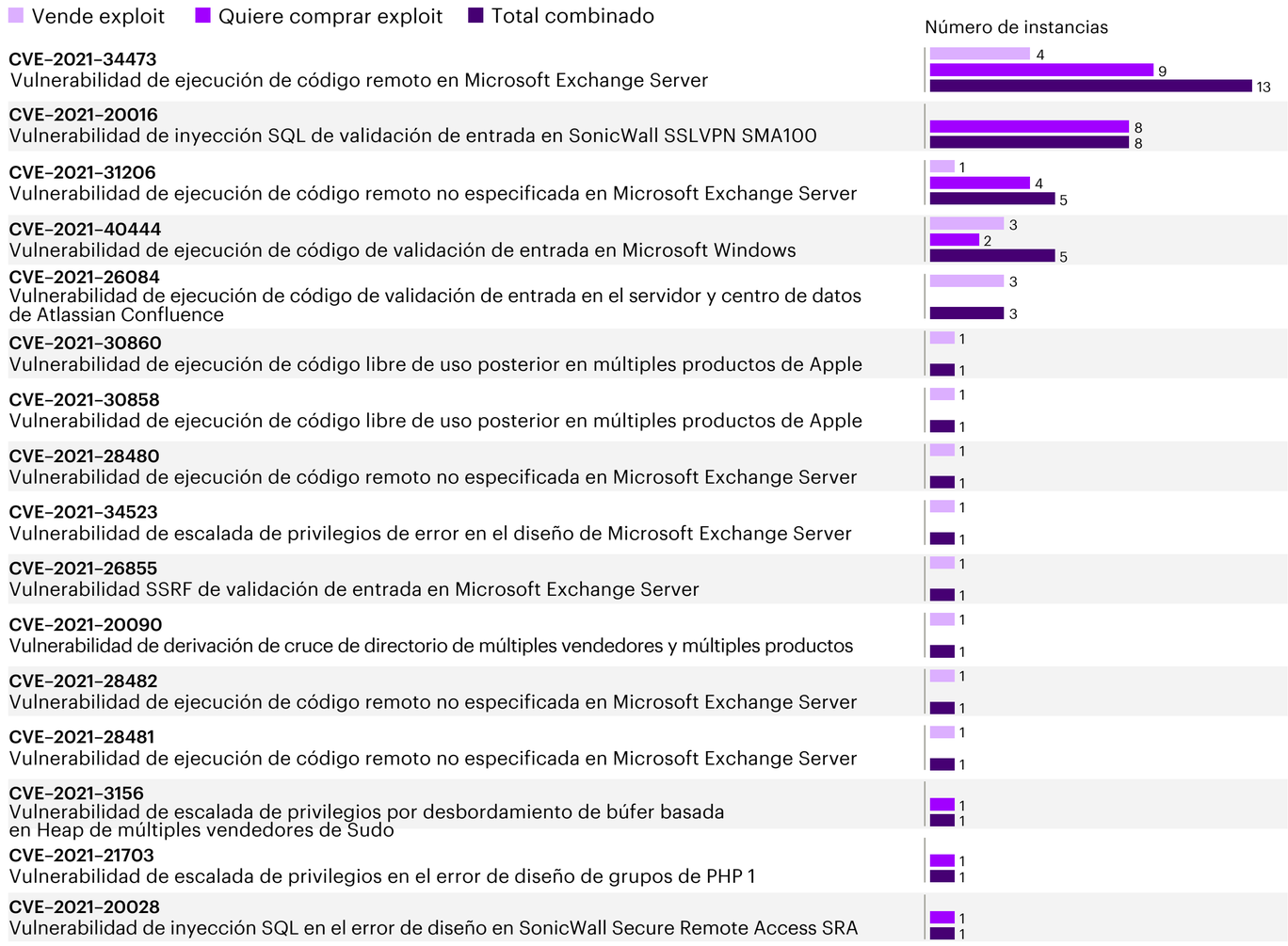
¿Qué está ocurriendo?

Los atacantes están ocupados vendiendo o comprando exploits de CVE

Accenture analizó 45 casos de usuarios clandestinos que querían vender o comprar exploits para vulnerabilidades y exposiciones comunes (CVE) entre agosto y octubre de 2021 (Figura 6). Identificamos:

- 24 actores que compraban o vendían exploits para 16 CVE en cuatro foros o mercados.
- 16 actores que querían comprar exploits para siete CVE.
- 9 actores que vendían exploits para 12 CVE.

Figura 6. Instancias de actores que compran o venden exploits para CVEs (agosto-octubre 2021)



Los atacantes tienen tres vulnerabilidades principales que compran y venden:

Durante el período de agosto a octubre de 2021, los tres exploits CVE más populares en el mercado son para CVE-2021-34473, CVE-2021-20016 y CVE-2021-31206.

Accenture analizó estas vulnerabilidades en el contexto del impacto potencial de una explotación exitosa y de las intenciones evaluadas de los actores que buscaban comprar exploits relacionados.

Accenture encontró que la explotación exitosa de cada una de las vulnerabilidades advertidas permitía a un adversario remoto el acceso no autorizado a una red de la víctima y la ejecución de código arbitrario en un host de la víctima. El análisis de las actividades pasadas de los actores que buscaban comprar exploits indica que los actores están motivados económicamente y que es probable que tengan la intención de utilizar los exploits para facilitar esquemas de acceso a la red no autorizados.

A continuación se detallan los exploits CVE más populares:

- **CVE-2021-34473:** Accenture identificó dos actores que vendían el mismo exploit y ocho actores con motivación económica que querían comprar un exploit para CVE-2021-34473 en el periodo de agosto a octubre de 2021. CVE-2021-34473 (también conocida como ProxyShell) es una vulnerabilidad de validación de entrada inadecuada (CWE-20) en Microsoft Exchange Server 2013-2019. Un actor que encadene CVE-2021- 34473 con CVE-2021-34523 y CVE-2021- 31207 podría ejecutar código arbitrario con privilegios de nivel SYSTEM en un host de la víctima.

- **CVE-2021-20016:** Accenture identificó cuatro actores con motivación económica que querían comprar un exploit CVE-2021-20016, pero no identificó a ningún actor que quisiera vender alguno. CVE-2021-34473 es una vulnerabilidad de inyección SQL (CWE-89) en SonicWall SSLVPN SMA100 que un atacante podría aprovechar para acceder y modificar la base de datos de un host de la víctima, facilitando el acceso del atacante a las credenciales de administrador, que pueden utilizarse para ejecutar remotamente código arbitrario en el host de la víctima.

- **CVE-2021-31206:** Accenture identificó un actor que vendía y cuatro actores con motivación económica que querían comprar un CVE-2021-31206. CVE-2021- 31206 es una vulnerabilidad de error de procesamiento de datos (CWE-19) en Microsoft Exchange Server 2013-2019 que un actor podría explotar para permitir la ejecución de código arbitrario en el host de la víctima.

Los atacantes comienzan a sacar provecho de la vulnerabilidad de Log4j

El 9 de diciembre de 2021, los mantenedores de Log4j informaron detalles de una vulnerabilidad de ejecución remota de código,[22] identificada como CVE-2021-44228 o como Log4Shell, que podría permitir a los atacantes ejecutar código arbitrario en un host vulnerable.

Una explotación exitosa permitiría a los atacantes ejecutar código sin autenticación. Dado que la explotación se produce mediante el registro de entrada, la superficie de ataque de esta vulnerabilidad es extremadamente amplia. La primera explotación importante que se informó se produjo en un popular videojuego en línea. También se observó otro uso de la vulnerabilidad que implicaba a un usuario que cambiaba el nombre de su teléfono y lo utilizaba para inyectar código en el servicio en la nube del fabricante del teléfono.

A fines de diciembre de 2021 se registraron los primeros informes de un gusano que aprovechaba Log4j en hábitats naturales y se observó mayor evidencia del interés de los actores de amenazas en explotar Log4j y un nuevo vector de ataque Log4j a través de WebSockets.

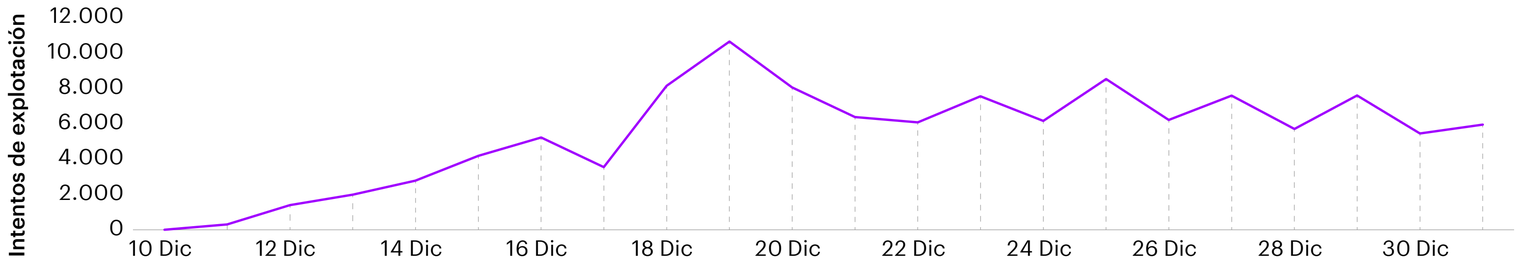
CISA estima que hay 100 millones de instancias de software y tecnología afectadas en una amplia gama de productos y proveedores tecnológicos.

En diciembre de 2021, Accenture identificó a los actores clandestinos que capitalizaban la noticia de la vulnerabilidad Log4j. Los actores de la amenaza comenzaron a identificar formas de incorporar la vulnerabilidad para atacar a las empresas vulnerables y aprovechar el acceso en las operaciones de las redes de bots.

En enero de 2022, los actores comenzaron a investigar redes y direcciones IP vulnerables a la debilidad Log4shell y empezaron a vender sus análisis a otros actores clandestinos.[23]

Figura 7. Tendencias y volumen de explotación de Log4j, diciembre de 2021

Esta línea de tiempo de los datos de telemetría sobre los intentos de explotación de la vulnerabilidad log4j revela las tendencias de los actores maliciosos por industria y región.



11.153
IP de origen del atacante único

119.514
Intentos de explotación únicos

26
Industrias objetivo
La mayoría:
Manufactura
Servicios financieros
Salud

6
Regiones objetivo
La mayoría:
América del Norte,
Asia Pacífico, Japón
Europa, Oriente Medio, África

Fuente: Datos de telemetría de incidentes de seguridad para la detección y respuesta ampliada de Accenture, 9-31 de diciembre de 2021

¿Qué será lo próximo?

Las siguientes son algunas formas de manejar los exploits de vulnerabilidad:

- **Defender sólidamente el acceso a la red:** Las vías más eficientes que puede tomar un adversario para monetizar el acceso a la empresa es vender el acceso a la red de la víctima o extorsionarla mediante ransomware, amenazas de divulgación de datos, o ambas. Las medidas para ayudar a defender la red de una organización incluyen la aplicación de los principios de confianza cero, la supervisión de la seguridad de la red, como el despliegue de firmas de detección para captar los intentos de explotación contra un entorno específico y alertar sobre los procesos que se ejecutan desde un sistema específico o un directorio de registro de aplicaciones web, controles de acceso estrictos y controles de endpoints. Asimsimo, bloquear las conexiones desde los dominios, direcciones IP y URL que hayan explorado y explotado activamente vulnerabilidades conocidas, y bloquear el DNS de salida y recursivo en los servidores. Los actores pueden intentar aprovechar los servidores web y de aplicaciones para resolver las llamadas a sitios web públicos que contienen código malicioso. También pueden reforzar las reglas del cortafuegos de salida y del WAF para bloquear este tipo de llamadas del entorno.

- **Volver a los fundamentos de la seguridad:** A menudo, las organizaciones pueden prevenir los ataques exitosos ejecutando programas de gestión de parches programados regularmente, realizando un inventario de los sistemas y el software de su entorno y probando proactivamente las tecnologías existentes para detectar debilidades. La combinación de los programas de gestión de parches con la supervisión de la inteligencia sobre ciberamenazas de los mercados de la Dark Net puede proporcionar contexto, además de informar posturas y tácticas de defensa cuando surjan nuevas vulnerabilidades como la de Log4j en diciembre de 2021.

- **Actualizar las versiones de Log4j:**
  Las versiones 2.0-beta9 a 2.14.1 de Log4j son susceptibles a esta vulnerabilidad. Para mitigar esta vulnerabilidad en esas versiones de Log4j, Accenture sugiere actualizar Log4j a la versión 2.17.0 para Java 8 (o posterior). Los usuarios deberían actualizar Log4j que funciona con Java 7 a la versión 2.12.2. Apache, Accenture y otros medios de ciberseguridad recomendaron anteriormente el uso de la versión 2.15.0 como solución a esta vulnerabilidad; sin embargo, la corrección fue incompleta. La versión 2.15.0 permitía la ejecución de código en ciertas configuraciones y ni Apache ni Accenture lo consideran todavía una corrección oficial. La vulnerabilidad causada por la corrección incompleta de la versión 2.15.0 es CVE-2021-45046. El 18 de diciembre de 2021, MITRE publicó CVE-2021-45105; esta vulnerabilidad afecta a las versiones 2.0-beta9 a 2.16.0 de Log4j.

  CVE-2021-45105 permite a los atacantes remotos causar una denegación de servicio a través de una recursión infinita cuando la aplicación encuentra entradas con búsquedas recursivas. Apache resolvió esta vulnerabilidad en la versión 2.17.0.

  Apache ha proporcionado el registro oficial de cambios del parche aquí:

  https://logging.apache.org/log4j/2.x/security.html

  Si no es posible actualizar a la versión 2.17.0, los usuarios de las versiones 2.10 de Log4j y posteriores pueden mitigar esta vulnerabilidad eliminando la clase JndiLookup de la siguiente ruta de clase:

  zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

  A largo plazo, las organizaciones deberían hacer un inventario de los sistemas y el software de su entorno. También utilizar software de mapeo de dependencias de aplicaciones para identificar cualquier dependencia de software de la biblioteca Log4j.

  Las herramientas SCA, como Veracode, Blackduck y Sonatype, tienen complementos para identificar este problema. Otros escáneres de vulnerabilidades, como Qualys, Tenable y Rapid7 han publicado complementos para detectar este problema y los administradores deberían actualizarlos con regularidad mientras siga desarrollándose esta situación de explotación de CVE-2021-44228.

  Tan pronto como sea posible, se debe aplicar un parche al software interno y al software orientado a Internet que utilice Log4j.[24]

Referencias

1. Accenture Cyber Threat Intelligence, "Colonial Pipeline Ransomware" ("Ransomware de Colonial Pipeline"), 9 de mayo de 2021. Informe de IntelGraph.

2. Accenture Cyber Threat Intelligence, "Ransomware Trends Q3 2021" ("Tendencias del ransomware en el tercer trimestre de 2021"), 11 de noviembre de 2021. Informe de IntelGraph; 2021 IBM Security X-Force Cloud Threat Landscape Report.

3. Estudio sobre ciberinvestigaciones y respuesta forense de Accenture.

4. Mensaje de vx-underground en Twitter, 28 de octubre de 2021.

5. Accenture Cyber Threat Intelligence, "A View from the Dark Web: Are Ransomware Gangs Shifting Their Focus towards Europe? ("Una visión desde la Dark Web: ¿están las bandas de ransomware cambiando su enfoque hacia Europa?"), 15 de noviembre de 2021. Informe de IntelGraph.

6. Cuenta de Twitter @darktracer, 17 de noviembre de 2021

7. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor" ("Un atacante altamente evasivo aprovecha la cadena de suministro de SolarWinds para comprometer a múltiples víctimas globales con la puerta trasera SUNBURST"). Mandiant. 13 de diciembre de 2020.

8. "Two NPM Packages With 22 Million Weekly Downloads Found Backdoored," ("Dos paquetes de NPM con 22 millones de descargas semanales encontrados en la puerta trasera"), The Hacker News. 7 de noviembre de 2021. "Newly Found npm Malware Mines Cryptocurrency on Windows, Linux, macOS Devices" ("Un nuevo malware npm descubierto mina criptomonedas en dispositivos Windows, Linux y macOS"), 20 de octubre de 2021. "The inside story of ransomware repeatedly masquerading as a popular JS library for Roblox gamers" ("La historia interna del ransomware que se hace pasar repetidamente por una popular biblioteca JS para los jugadores de Roblox"), 16 de noviembre de 2021.

9. ibídem.

10. "APT trends report Q3 2021" ("Informe sobre las tendencias de APT en el tercer trimestre de 2021"), Kaspersky, 26 de octubre de 2021.

11. "TeleBots are back: Supply-chain attacks against Ukraine" ("Vuelven los telebots: Ataques a la cadena de suministro contra Ucrania"), ESET. 30 de junio de 2017.

12. Accenture "Application Security"

13. "SUNSPOT: An Implant in the Build Process" ("Seguridad de las aplicaciones. SUNSPOT: Un implante en el proceso de construcción"), CrowdStrike, 11 de enero de 2021.

14. "Japanese government official says Olympic ticket data leaked," ("Funcionario del gobierno japonés menciona que se han filtrado los datos de las entradas olímpicas"), ZDNet, 21 de julio de 2021.

15. Accenture Cyber Threat Intelligence, "Technical Analysis of DoppelDridex" ("Análisis técnico de DoppelDridex"), 19 de abril de 2021. Informe de IntelGraph.

16. "Hackers leak full EA data after failed extortion attempt" ("Los hackers filtran datos completos de EA tras un intento fallido de extorsión"), The Record, 31 de julio de 2021.

17. Aggarwal, Gaurav, "How the pandemic has accelerated cloud adoption," ("Cómo la pandemia ha acelerado la adopción de la nube"), Forbes, 15 de enero de 2021.

18. Comunicado de prensa de Gartner®, Gartner says Four Trends are Shaping the Future of Public Cloud ("Gartner afirma que hay cuatro tendencias que marcan el futuro de la nube pública"), 2 de agosto de 2021.
GARTNER es una marca registrada y una marca de servicio de Gartner, Inc. o sus filiales en EE. UU. y otros países y se ha utilizado en este documento con permiso. Todos los derechos reservados.

19. Mensaje de vx-underground en Twitter, 28 de octubre de 2021.

20. Accenture Cyber Threat Intelligence, "TeamTNT Operations Show the Cloud Is the New Battleground" ("Las operaciones de TeamTNT demuestran que la nube es el nuevo campo de batalla"), 14 de enero de 2022, informe de Intelgraph.

21. "TeamTNT with new campaign aka 'Chimaera'" ("TeamTNT con nueva campaña conocida como 'Quimera'"), AT&T. 8 de septiembre de 2021.

22. Accenture Cyber Threat Intelligence, "Log4j Unauthenticated RCE Vulnerability CVE-2021-44228" ("Vulnerabilidad RCE no autenticada en Log4j CVE-2021-44228"), 4 de enero de 2022, informe de Intelgraph.

23. Accenture Cyber Threat Intelligence, "Account "leopoldo787" Advertises List of 500,000 IP Addresses Potentially Vulnerable to Log4j Exploitation" ("La cuenta "leopoldo787" anuncia una lista de 500.000 direcciones IP potencialmente vulnerables a la explotación de Log4j"), 2 de enero de 2022, informe de IntelGraph.

24. Accenture Cyber Threat Intelligence, "Log4j Unauthenticated RCE Vulnerability CVE-2021-44228" ("Vulnerabilidad RCE no autenticada en Log4j CVE-2021-44228"), 4 de enero de 2022, informe de Intelgraph.

Contactos

Joshua Ray
Managing Director
Accenture Security
joshua.a.ray@accenture.com

Howard Marshall
Managing Director
Accenture Security
howard.marshall@accenture.com

Robert Boyce
Managing Director
Accenture Security
Global Cyber Investigations,
Forensics & Response (CIFR) Lead
r.boyce@accenture.com

Christopher Foster
Senior Principal – Security Innovation
Accenture Cyber Threat Intelligence
Product Strategy Lead
c.foster@accenture.com

Valentino De Sousa
Senior Principal – Security Innovation
Europe and Latin America
Cyber Threat Intelligence Lead
valentino.de.sousa@accenture.com

Colaboradores

Omar Al-Shahery, Hassan Alsaffar, Gian Luca Giuliani, Randall R. Griffith, Paul Mansfield, Hannaire Mekaouar, Akihiro Nishumura, Nellie Ohr, Max Smith, Thomas Willkan and the Cyber Investigations, Forensics & Response (CIFR) and Managed Detection and Response (MxDR) teams.

Acerca de Accenture

Accenture es una compañía global de servicios profesionales, líder en capacidades digitales, de nube y de seguridad. Combinamos una experiencia inigualable y habilidades especializadas en más de 40 sectores económicos, prestamos servicios de Estrategia y Consultoría, Interactivos, Tecnológicos y de Operaciones, impulsados por la red de centros de tecnología avanzada y operaciones inteligentes más grande del mundo. Nuestros 674.000 empleados cumplen la promesa de la tecnología y el ingenio humano todos los días y prestan servicio a clientes en más de 120 países. Adoptamos el poder del cambio para crear valor y éxito compartido para nuestros clientes, profesionales, accionistas, socios y comunidades. Visitanos en **accenture.com**

Acerca de Accenture Security

Accenture Security es un proveedor líder de servicios integrales de ciberseguridad que incluyen ciberdefensa avanzada, soluciones de ciberseguridad aplicada y operaciones de seguridad gestionada. Ofrecemos innovación en seguridad, además de una escala global y una capacidad de entrega a nivel mundial a través de nuestra red de centros de tecnología avanzada y operaciones inteligentes. Con la colaboración de nuestro equipo de profesionales altamente capacitados, ayudamos a nuestros clientes a innovar de manera segura, desarrollar la resiliencia cibernética y crecer con confianza. Seguinos en **@AccentureSecure** en **Twitter**, **LinkedIn** o visitanos en **accenture.com/security**.

210863