THREAT LANDSCAPE REPORT

El departamento de Threat Intelligence de S21sec ofrece un informe del segundo semestre de 2021 explicando aquellas amenazas existentes que pueden poner en riesgo la seguridad de las empresas y particulares, dando a conocer al lector las más relevantes que a día de hoy existen, como vulnerabilidades, malware, APT, etc., y que pueden suponer un riesgo a corto y medio plazo.

S21SEC

Segundo semestre 2021

El segundo semestre de 2021 se ha visto marcado por varios eventos de alta relevancia, como el descubrimiento y la explotación por parte de actores maliciosos de varias vulnerabilidades, que han supuesto un quebradero de cabeza para los departamentos de TI en las organizaciones.

Estas vulnerabilidades de alto impacto son Printnightmare, Log4j, CVE-2021-40444 y las conocidas como ProxyShell.

En este semestre se destaca el aumento del uso de *infostealers* para obtener información personal, credenciales de acceso o datos bancarios.

Entre los *infostealers* con mayor actividad, de acuerdo con la telemetría de S21sec, destacan Agent Tesla, Vidar y Redline.

En el segundo semestre de 2021 también se ha observado un aumento considerable de los ataques a instituciones educativas e infraestructuras críticas.

S21SEC

ÍNDICE

01. Vulnerabilidades

02. Ransomware

03. Malware bancario

04. Malware Android

05. SIM *swapping*

06. Sector sanitario

07. Sector educativo

08. Infraestructuras críticas

09. TELCO & IT

10. APT

11. Brechas de seguridad

12. Conclusiones

Threat Landscape Report

Segundo semestre 2021

VULNERABILIDADES

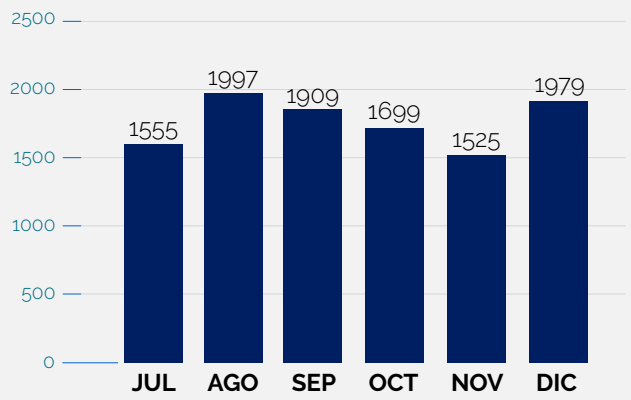
Las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas.

NIVEL DE CRITICIDAD

En total, en el segundo semestre de 2021, se han publicado 10 641 vulnerabilidades, de las cuales se registró el mayor número en agosto.

Vulnerabilidades publicadas

Durante el segundo semestre de 2021



Nivel de gravedad

Basado en CVSS versión 3

- **Crítico:** 1447
- **Alto:** 4442
- **Medio:** 4549
- **Bajo:** 226
- **Nulo:** 0

Durante el último semestre de 2021, se han publicado varias vulnerabilidades de criticidad alta que los ciberdelincuentes han explotado activamente para la realización de distintos tipos de ataques.

De hecho, cabe destacar que, en la gran mayoría de ataques que han tenido lugar a lo largo del año 2021, uno de los principales vectores de entrada observados ha sido la explotación de vulnerabilidades existentes en la infraestructura de destino.

Por este motivo, es importante que las empresas tengan en consideración este tipo de amenazas y que pongan el foco en el mantenimiento y la actualización de sus infraestructuras.

PRINTNIGHTMARE

El día 8 de junio, Microsoft publicó la CVE-2021-1675, una vulnerabilidad de ejecución de código remoto en Windows Print Spooler y, en el mes de julio, publicó la vulnerabilidad CVE-2021-34527 (denominada Printnightmare).

Esta vulnerabilidad explotaba la cola de impresión para ejecutar código remoto y conseguir permisos del sistema.

Esta amenaza tiene tres características fundamentales y es capaz de ejecutar código remoto, escalar privilegios, además de tener un vector de ataque local.

Concretamente, se puede ejecutar código alojado en otra máquina (ejecución de código remoto) con permisos de sistema (escalado de privilegios), pero es necesario tener acceso a la máquina (vector de ataque local) para poder explotarlo, ya que es necesario ejecutar el programa spoolsv.exe (cola de impresión).

PrintNightmare aprovecha el hecho de que cualquier usuario autenticado sin privilegios puede llamar a RpcAddPrinterDriverEx () y especificar un *driver/dll* con código arbitrario, que se ejecutará con privilegios de sistema.

Este *driver/dll* puede residir tanto en la propia máquina como en un servidor remoto. Esto da como resultado que el servicio de cola de impresión spoolsv.exe ejecute código en un archivo DLL arbitrario con privilegios de sistema.

CVE-2021-40444

El 7 de septiembre se encontró una nueva vulnerabilidad, la CVE-2021-40444, que afecta a las herramientas de Office donde el atacante es capaz de ejecutar código arbitrario alojado en una máquina remota.

La CVE-2021-40444 se encontró en el motor de renderizado MSHTML del navegador Internet Explorer, que es utilizado por los documentos de Microsoft Office.

MSHTML lleva a cabo las funciones de operatividad básica del navegador, en concreto el filtrado y el renderizado de los documentos web, HTML y hojas de estilo en cascada entre otras funcionalidades.

Asimismo, permite integración con otras aplicaciones para Microsoft Windows mediante la exposición de una API de documento activo. Se implementa mediante mshtml.dll.

Para explotar la vulnerabilidad, un atacante podría crear un control ActiveX malicioso para incorporarlo en un documento de Microsoft Office que aloja el motor de renderizado del navegador y convencer a la víctima para que abra el documento malicioso.

ActiveX es un entorno para definir componentes de software reusables de forma independiente del lenguaje de programación utilizado por Office como Internet Explorer, pero no Edge.

APACHE LOG4J

A principios del mes de diciembre, se divulgó una vulnerabilidad crítica conocida como Log4Shell o LogJam, de ejecución de código remoto en el componente de Apache log4j, una biblioteca de registro escrita en Java.

La vulnerabilidad crítica rastreada como CVE-2021-44228 en Apache Log4j permite que un actor remoto envíe un paquete HTTP elaborado a servidores Apache que ejecuten el software anterior a Log4j 2.15.0. El software vulnerable almacenará la solicitud HTTP como un registro legítimo, que luego ejecuta el *payload* incrustado en dicho registro.

La explotación exitosa de la vulnerabilidad permitiría a un atacante iniciar el tráfico LDAP a un nodo controlado por el atacante desde el Java Naming and Directory Interface (JNDI). El nodo controlado por el atacante responderá con un archivo de clase Java malicioso que luego comenzará a ejecutarse en el servidor víctima.

El 14 de diciembre se publicó una segunda vulnerabilidad rastreada como CVE-2021–45046, que involucra a Apache Log4j.

Se debe a que la corrección para abordar la vulnerabilidad CVE-2021-44228 estaba incompleta en ciertas configuraciones no predeterminadas, recomendando actualizar a la última versión de Log4j 2.16.0 para evitar búsquedas JNDI controladas por atacantes. La vulnerabilidad afecta a todas las versiones desde 2.0-beta9 hasta 2.12.1 y 2.13.0 hasta 2.15.0.

El 16 de diciembre de 2021, surgió una tercera vulnerabilidad en Apache Log4j 2: CVE- 2021-45105, una vulnerabilidad de denegación de servicio (DoS) en un *WebSocket* de JavaScript para activar la ejecución remota de código (RCE) en aplicaciones Log4j 2 internas y localmente expuestas sin parchear.

El 18 de diciembre de 2021, Apache Foundation lanzó actualizaciones adicionales Log4j 2.17.0, reemplazando a la versión 2.16.0, la cual es vulnerable, y 2.12.3, para corregir el fallo de seguridad.

Dado que Log4j es una librería de registro de Java de código abierto usada a nivel mundial en una gran variedad de aplicaciones y servicios de software en el ámbito empresarial Java, a los pocos días de su publicación, numerosos grupos de amenazas (APT35, Hafnium y Conti), además de actores individuales, explotaron esta vulnerabilidad.

Los objetivos de estos actores eran variados, desde la instalación de criptomineros o distintos tipos de malware.

PROXYSHELL

Durante este semestre, actores maliciosos han explorado y explotado varias vulnerabilidades de Microsoft Exchange, que reciben el nombre de ProxyShell y permiten a un actor saltarse la autenticación y ejecutar código como usuario con privilegios.

ProxyShell comprende tres vulnerabilidades separadas que se utilizan como parte de una única cadena de ataque:

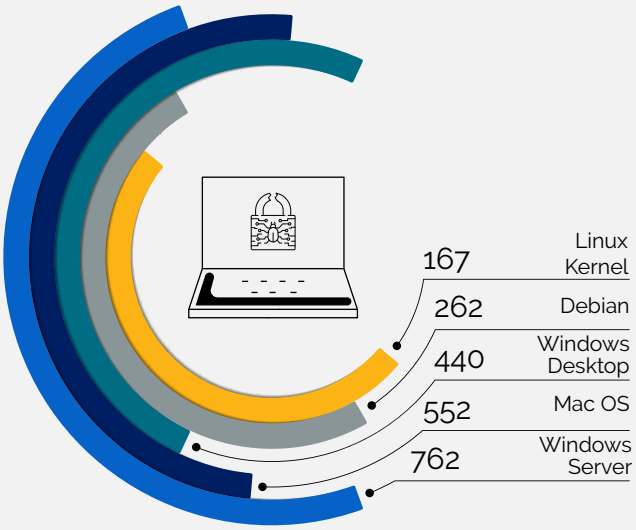
CVE-2021-34473: vulnerabilidad de ejecución remota de código con una puntuación CVSSv3 de 9,1.

CVE-2021-34523: vulnerabilidad de elevación de privilegios en el *backend* de Exchange PowerShell.

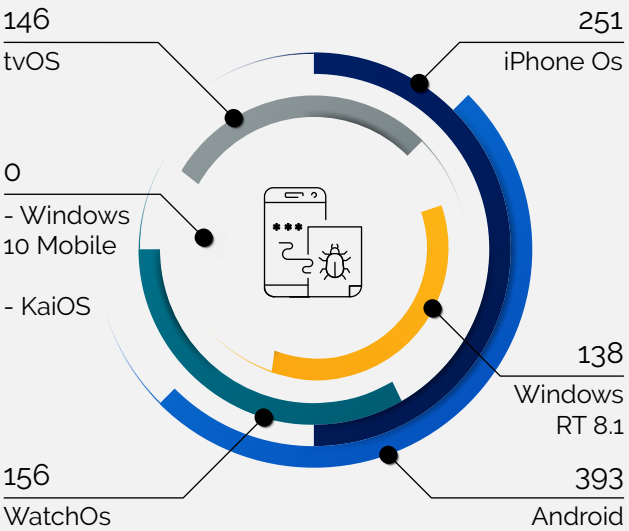
CVE-2021-31207: ejecución remota de código después de la autenticación a través de la escritura de archivos arbitrarios.

Cabe destacar que las vulnerabilidades de ProxyShell se han utilizado para desplegar malware, como el ransomware LockFile.

VULNERABILIDADES EN SISTEMAS OPERATIVOS



VULNERABILIDADES SO DISPOSITIVOS INTELIGENTES



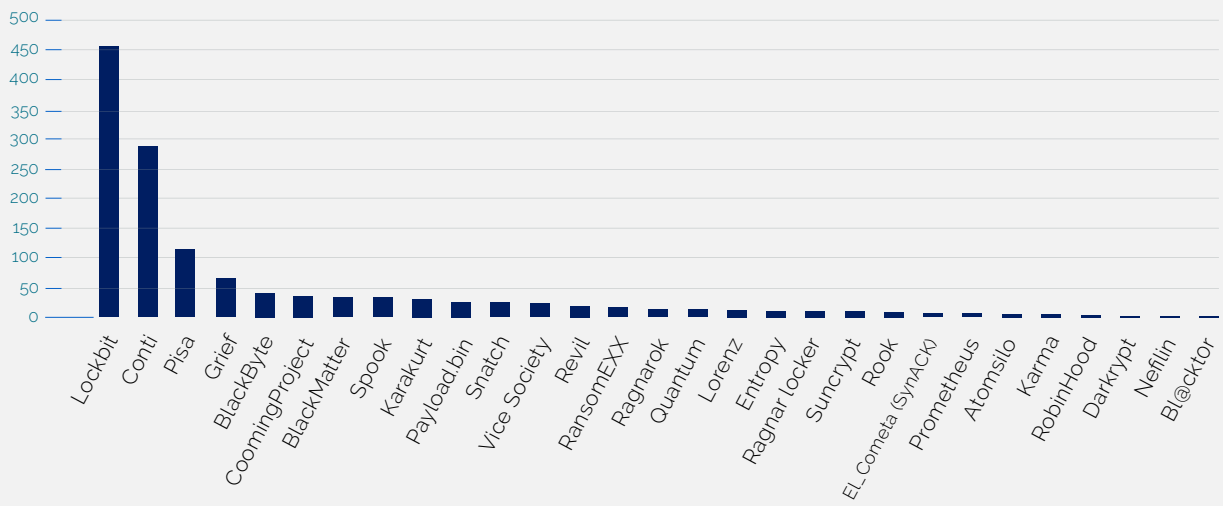
RANSOMWARE

El ransomware se ha convertido durante los últimos años en uno de los tipos de malware más utilizados por parte de actores maliciosos con motivaciones económicas.

ESTADÍSTICAS RANSOMWARE

En el segundo semestre de 2021, el equipo de Threat Intelligence de S21sec rastreó un total de 1694 víctimas de ransomware, amenazadas en los sitios *web* Tor, administrados por los operadores de distintos ransomware.

Familias de ransomware relevantes en el segundo semestre de 2021



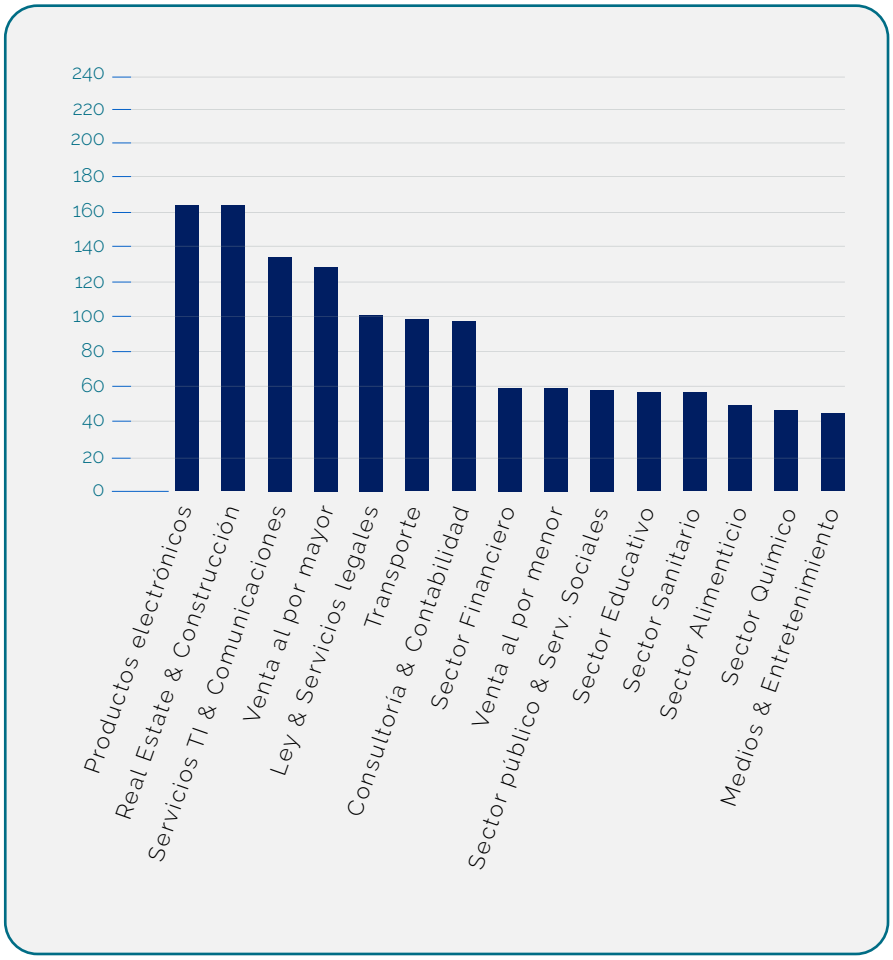
Como viene siendo habitual desde los últimos dos años, la mayor parte de ransomware funcionan bajo un esquema del llamado *ransom-as-a-service* (RaaS), en el que existe un grupo principal de desarrolladores (operadores) que venden o alquilan plazas para poder tener acceso a los paneles de control y a las herramientas.

Estas plazas son limitadas en su mayoría y los puestos generalmente los ocupan usuarios (los llamados afiliados) que hayan mostrado previamente a los operadores que tienen los conocimientos técnicos suficientes para conseguir un ataque exitoso.

AFECTACIÓN DE RANSOMWARE POR SECTORES

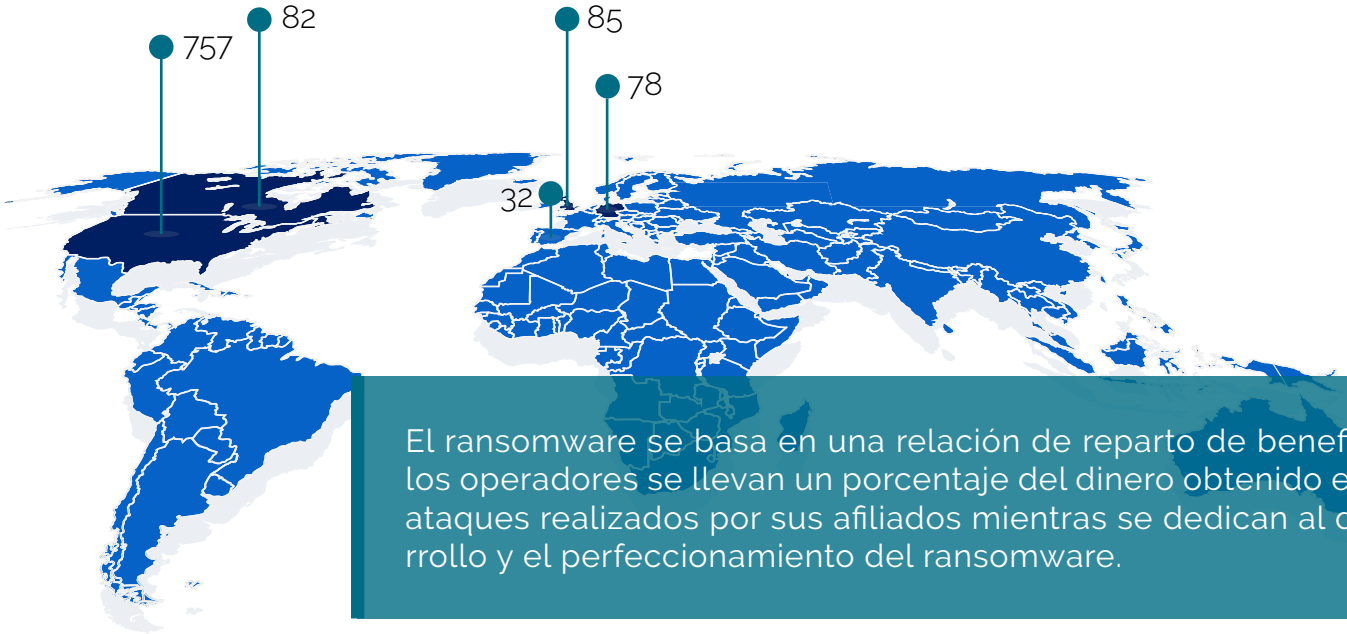
De más a menos afectados, los principales sectores que han sufrido ataques de ransomware son:

- Productos electrónicos
- Real Estate & Construcción
- Servicios TI & Comunicaciones
- Venta al por mayor
- Ley & Servicios legales
- Transportes
- Consultoría & Contabilidad
- Sector Financiero
- Venta al por menor
- Sector Público & Serv. Sociales
- Sector Educativo
- Sector Sanitario
- Sector Alimenticio
- Sector Químico
- Medios & Entretenimiento



AFECTACIÓN DE RANSOMWARE POR PAÍSES

Los atacantes se han dirigido mayoritariamente a objetivos localizados en Estados Unidos, seguido de Reino Unido, Canadá y Alemania, y con España en séptimo lugar.

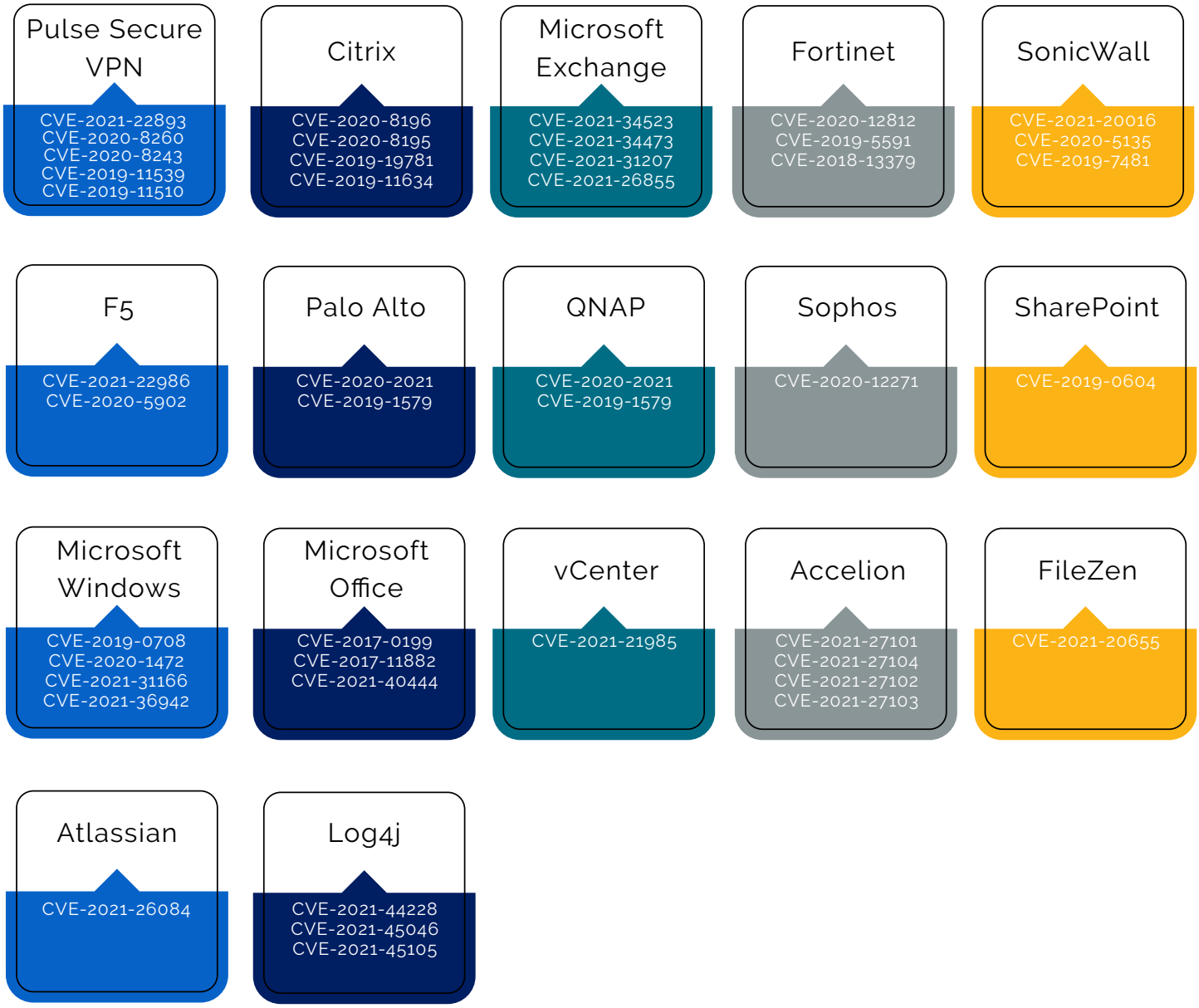


El ransomware se basa en una relación de reparto de beneficios, los operadores se llevan un porcentaje del dinero obtenido en los ataques realizados por sus afiliados mientras se dedican al desarrollo y el perfeccionamiento del ransomware.

CVE UTILIZADAS

El ransomware utiliza como vectores principales de entrada el correo electrónico (a través de mensajes con adjuntos maliciosos) y la explotación de vulnerabilidades.

En los últimos años se ha observado que las siguientes vulnerabilidades son las más comúnmente utilizadas por los actores detrás de los ransomware.



Otra tendencia que ha seguido estable en cuanto al ransomware durante este año ha sido la técnica de la doble extorsión: primero cifran los equipos, dejándolos inutilizables e incluso llegando a afectar a la productividad de las empresas, y después amenazan con la publicación de los archivos obtenidos durante el ataque.

SUNCRYPT

SunCrypt es un ransomware que se dirige a organizaciones y usuarios de todo el mundo.

Los operadores del ransomware actúan siguiendo un modelo de doble extorsión: además de cifrar sus archivos, amenazan con divulgar la información sensible obtenida si las víctimas no contactan con ellos en un periodo menor a 72 horas.

Además, prometen proporcionar un análisis de seguridad que muestre las debilidades de seguridad utilizadas para el ataque. El ransomware utiliza vulnerabilidades de la red para obtener acceso a los servidores corporativos y bloquear los archivos almacenados en ellos.

Después del cifrado, el ransomware muestra una nota de rescate con nombre "YOUR_FILES_ARE_ENCRYPTED.HTML", disponible en varios idiomas como inglés, francés, alemán o japonés, lo que sugiere el interés de los operadores en Norte América, Europa o Japón.

PYSA

El ransomware conocido actualmente como PYSA, cuyas siglas proceden del término "Protect Your System Amigo", es una variante del ransomware Mespinoza, que apareció en el mes de octubre de 2019 y al cual se le atribuyen varios ataques que llevaron a la infección de las redes de grandes corporaciones.

De acuerdo con el CERT francés, se han encontrado evidencias de la existencia de este ransomware desde el año 2018, relacionándolo también con el ataque a instituciones de ese mismo país.

Cabe destacar que, en marzo de 2021, el FBI también emitió un comunicado informando del aumento de actividad de PYSA contra organizaciones educativas en Estados Unidos y Reino Unido.

El grupo cibercriminal que está detrás de este ransomware ha enfocado sus ataques desde marzo de 2020 en centros de educación, escuelas K-12, seminarios, entidades gubernamentales de todo el mundo, en el sector de la salud y en empresas privadas.

Actualmente, los países más atacados por PYSA son Estados Unidos, Reino Unido, Brasil, España y Canadá.

Durante los últimos meses se ha observado un aumento de lo que se consideraría una triple extorsión: algunos ransomware han incluido entre sus capacidades la realización de ataques de DDoS y amenazan a sus víctimas con realizar este tipo de ataque durante varios días hasta que realice el pago del rescate.

MALWARE BANCARIO

El malware bancario se mantiene como una de las amenazas de ciberseguridad más relevantes durante el segundo semestre de 2021, teniendo un alto impacto en sus víctimas.

MALWARE BANCARIO

Durante el segundo semestre de 2021, desde S21sec se han analizado varios de estos malware bancarios, entendiendo su funcionamiento, alcance e impacto. A continuación, se destacan algunos de ellos:

SQUIRREL WAFFLE

NUMANDO

GUILDMA

INFOSTEALERS

Debido al aumento de los ataques y la consecuente obtención de datos y accesos de los equipos infectados, desde S21sec se ha identificado con mayor frecuencia la venta de estos datos y accesos de equipos y redes por parte de ciberdelincuentes en markets de la *Deep* y *Dark Web*, mayormente en Genesis Market, Russian Market y 2easy Market entre otros.

Estas ventas se realizan por diversos precios y pueden incluir accesos a máquinas infectadas, credenciales y datos sensibles.

SQUIRREL WAFFLE

En el mes de septiembre se detectó una campaña de distribución del malware bancario SquirrleWaffle a través de correo electrónico, donde se pudo observar el uso de otros programas maliciosos como Cobalt Strike.

La distribución de SquirrleWaffle se lleva a cabo a través de campañas de *malspam* mediante correo electrónico, utilizando hilos de correo existentes y usando "asuntos" probablemente robados.

El modelo de funcionamiento de esta campaña es similar al observado en campañas semejantes: en una primera fase, el correo electrónico en cuestión incluye una URL que redirige a una página *web* que descarga un fichero ZIP, el cual contiene un documento ofimático malicioso, mayoritariamente en formato Word y Excel.

Una vez se descarga el archivo ZIP, se habilitan las macros embebidas de los documentos y, tras la ejecución de estos documentos, se procede a la descarga de una segunda fase del malware. En esta segunda fase, durante su instalación, el malware descarga el *payload* final donde se encuentra Cobalt Strike, aunque también se han identificado coincidencias con el malware Qakbot / Qbot.

En este caso, una vez se encuentra infectado el sistema, el malware tendría la capacidad de recopilar información del sistema afectado, cargar la configuración del malware y habilitar las infecciones para desplegar malware adicional, como Qakbot y Cobalt Strike.

NUMANDO

El malware Numando se posiciona como uno de los troyanos bancarios que más se mantiene en uso, teniendo un impacto relevante en países latinoamericanos y España.

Aunque su actividad data del año 2018, las actualizaciones en sus TTP han sido menos dinámicas que las de otros malware de la misma familia, como Mekotio por ejemplo. En las últimas campañas observadas en 2021, se han identificado nuevas técnicas de funcionamiento.

El principal vector de ataque de la campaña se basa en el envío de correos electrónicos de *malspam*. En dichos correos se adjunta un archivo ZIP con un instalador MSI (donde se oculta o descarga el malware) con un archivo en formato CAB que contiene una aplicación legítima, un inyector y una DLL cifrada con el troyano Numando.

Cuando se ejecuta el MSI, se ejecuta paralelamente la aplicación legítima y se carga lateralmente el inyector. Tras este proceso de ejecución, Numando puede realizar funciones de *backdoor*, como simular acciones del ratón y el teclado, reiniciar y apagar la máquina, mostrar ventanas superpuestas y realizar capturas de pantalla.

Entre las nuevas técnicas utilizadas se encuentra el uso de un inyector no escrito en lenguaje Delphi y el uso de plataformas públicas para almacenar su configuración remota en aplicaciones como YouTube o Pastebin.

INFOSTEALERS

El malware de robo de información (conocido como *infostealer*) también ha supuesto una amenaza muy relevante para los usuarios y entidades bancarias durante el segundo semestre de 2021.

Al igual que en el primer semestre de 2021, los *infostealers* siguen manteniendo su actividad al alza, detectándose diversas campañas dirigidas con el objetivo de obtener credenciales bancarias.

El uso de *infostealers* para obtener información personal, credenciales de acceso o datos bancarios, se sigue utilizado por parte de actores maliciosos, quienes desarrollan y mejoran las capacidades de este tipo de malware continuamente.

Entre los *infostealers* detectados en S21sec, destacan Agent Tesla, Vidar y Redline. A través de tareas de monitorización y detección se ha observado que la actividad de estos *infostealers* se centra en la infección de equipos y redes para obtener información sensible, credenciales y datos del objetivo.

Asimismo, algunos de ellos suelen distribuirse junto con otro malware o ransomware, como es el caso de Vidar, donde se ha detectado que se ha distribuido en conjunto con varias familias de ransomware.

Vidar se considera de uno de los *infostealers* más utilizados durante 2021, y con un incremento durante el último semestre de 2021 debido a su mayor compra-venta en mercados de la *Deep Web*.

En el caso de Agent Tesla, es uno de los *infostealers* que más tiempo lleva distribuyéndose entre los usuarios. Sin embargo, su afectación sigue al alza mientras que surgen variantes de Agent Tesla que contienen mejoras en sus capacidades, utilizando el *phishing* como su vector de ataque principal.

Por otro lado, el *infostealer* Redline se considera un malware reciente cuya distribución se detectó en el año 2020, pero ha notado un crecimiento notable en el último semestre de 2021. Su distribución se realiza a través de ingeniería social, incluyendo campañas de *phishing*, adjuntando archivos en diferentes formatos para proceder a la ejecución de programas maliciosos. Asimismo, se posiciona como una de las 10 amenazas emergentes en la categoría de *infostealers*.

Una de las características de los *infostealers* identificados es la facilidad con la que se compran o venden en foros de la *Deep* y *Dark Web*. Debido a sus bajos precios de compra o venta, su uso se ha extendido, aumentando los ataques con este malware.

A su vez, debido al aumento de los ataques y la consecuente obtención de datos y accesos de los equipos infectados, desde S21sec se ha identificado con mayor frecuencia la venta de estos datos y accesos de equipos y redes por parte de ciberdelincuentes en markets de la *Deep* y *Dark Web*, mayormente en Genesis Market, Russian Market y 2easy Market entre otros.

Estas ventas se realizan por diversos precios y pueden incluir accesos a máquinas infectadas, credenciales y datos sensibles.

GUILDMA

A principios del segundo semestre de 2021, desde S21sec se detectó una nueva campaña del troyano bancario Guildma que distribuía malware entre sus objetivos, mayoritariamente instituciones financieras de Latinoamérica, Portugal y España.

En este caso, en el mes de julio de 2021 se identificó nuevamente una campaña de distribución de este malware contra instituciones financieras de países latinoamericanos, Portugal y España. En dicha campaña, el troyano bancario se propaga a través de correos electrónicos donde se adjunta una URL maliciosa, la cual contiene un archivo ZIP con un falso ejecutable y desde donde se inicia el ataque.

Aunque la actividad de Guildma se remonta al año 2017, los troyanos bancarios suelen desarrollar nuevas técnicas de ataque con el objetivo de mantener activos sus ataques.

En el caso de Guildma, el archivo ZIP al que es dirigido el usuario contiene un ZIP adicional con un acceso directo de Windows desde donde se ejecuta el comando CMD, creando un acceso directo del menú de inicio de Windows para mantener la infección persistente.

MALWARE ANDROID

Los ciberdelincuentes han añadido los teléfonos y tabletas inteligentes a su lista de objetivos principales, lo que ha provocado un aumento de las amenazas, dirigidas específicamente contra este tipo de dispositivos.

VECTORES DE ENTRADA

Hoy en día, el malware para Android es mucho más frecuente, ya que este tipo de sistema operativo es el más utilizado por la mayor parte de la población.
Sin embargo, los ciberdelincuentes están comenzando a desarrollar cada vez más malware para otros sistemas operativos, como iOS.

INGENIERÍA SOCIAL

Los ciberdelincuentes utilizan mensajes (SMS) con un enlace que redirige a una URL maliciosa desde la cual se descarga una aplicación con apariencia legítima, pero que en realidad se trata de un malware.

DESCARGA DE APLICACIONES

El usuario descarga una aplicación considerada legítima, pero que realmente se encuentra troyanizada.
Este tipo de aplicaciones están disponibles en tiendas de aplicaciones oficiales (Google Play, Apple Store) o de mercados no oficiales / páginas *web* de desarrolladores.

PEGASUS

Este semestre ha tenido gran impacto otro malware móvil llamado Pegasus, que también afecta a dispositivos iOS.

Se trata de un malware comercial atribuido al grupo israelí NSO, con funcionalidades de spyware, es decir, malware espía.

Los operadores de Pegasus podían, mediante la instalación de distintos módulos, leer o hacerse con los mensajes de texto de su víctima, leer correos electrónicos, escuchar y grabar audios o llamadas mediante la activación secreta de los micrófonos, registrar las pulsaciones del teclado, acceder al historial del navegador, conocer los contactos de la agenda, etc.

SOVA

A mediados de septiembre de 2021, varios medios de comunicación se hacían eco de la existencia de un nuevo troyano para Android denominado SOVA (búho en ruso).

Las muestras analizadas de este troyano por parte del equipo de Threat Intelligence de S21sec son muestras que suplantaban a actualizaciones de seguridad de aplicaciones muy extendidas, como Adobe Flash Player.

Tras la descarga de la aplicación por parte de la víctima, el malware pide al usuario que le conceda una serie de permisos que le permitirán realizar distintas acciones en el futuro, por ejemplo, los servicios de accesibilidad BIND_ACCESSIBILITY_PERMISSION.

Será precisamente mediante la utilización de estos servicios cómo SOVA realiza su ataque de *overlay*.

OSCORP

Oscorp es un malware para Android de la familia de los troyanos bancarios que surgió a principios de 2021 con campañas dirigidas principalmente a Italia.

Este malware tiene funcionalidades de troyano bancario, *keylogger*, RAT e *infostealer*.

Oscorp posee un servicio destinado a la solicitud del acceso a los servicios de accesibilidad.

Si consigue acceso a estos servicios, podrá concederse a sí mismo otra serie de permisos que le garantizarán, entre otras, la persistencia en el dispositivo.

Como troyano bancario, cuenta con técnicas para la realización de ataques de *overlay* (superposición). Oscorp posee un servicio que se encarga de detectar la aplicación en primer plano en el dispositivo en un momento dado.

Para versiones de Android inferiores a Android 5.0, hace uso del gestor de actividades del sistema para obtener el nombre de paquete de la actividad en ejecución y, a partir de Android 5.0, utiliza las estadísticas de uso del dispositivo para acceder a esta misma información.

Cuando ha detectado la aplicación que le interesa (generalmente aplicaciones bancarias), comienza el ataque de superposición (*overlay*) del troyano, consistente en cargar el contenido de un *phishing kit*, que imitará el aspecto de la aplicación legítima en una vista de tipo WebView que será superpuesta a la aplicación legítima.

SIM SWAPPING

En los últimos meses de 2021, se ha registrado un incremento de ataques telefónicos mediante el cambio de las tarjetas SIM de los dispositivos móviles.

SIM *SWAPPING* O SIM *HIJACKING*

Es una técnica que permite a los atacantes tomar el control del número de teléfono móvil de un objetivo, engañando o sobornando a los empleados de su proveedor de telefonía para que reasigne los números a las tarjetas SIM controladas por el estafador. De ser exitoso el cambio, la víctima pierde conexión con la red y no le es posible realizar o recibir llamadas ni mensajes.

Este tipo de ataque se dirige especialmente a las transacciones bancarias del usuario, pero no de forma exclusiva.

También se busca obtener acceso a las billeteras de criptomonedas, redes sociales, aplicaciones de mensajería y cuentas de correo electrónico.

Para que un atacante realice el engaño con éxito, debe realizar previamente un trabajo de obtención de datos de su víctima.

MODUS OPERANDI DEL SIM *SWAPPING*

A lo largo de 2021, se ha observado un aumento considerable en las quejas realizadas por usuarios en las que se reportan transacciones bancarias no autorizadas o pérdida repentina en el control de su número telefónico.

Algunas personas han puntualizado que, tras recibir códigos no solicitados en sus teléfonos móviles, sufren la extracción de todo o la mayor parte del dinero de sus cuentas bancarias.

El *modus operandi* identificado en el SIM *swapping* tiene tres fases:

ROBO DE CREDENCIALES DEL USUARIO CON TÉCNICAS DE INGENIERÍA SOCIAL

Páginas *web* falsas o duplicadas, mensajes de correo electrónico con *phishing*, instalación de aplicaciones con malware o suplantando aplicación de alguna entidad bancaria.

La obtención de información también se realiza a través de técnicas OSINT o de *footprinting*, o con la explotación de brechas de datos obtenidas de forma ilegal.

RECOPILADA LA INFORMACIÓN, EL ATACANTE INTENTA CLONAR LA TARJETA SIM DE LA VÍCTIMA PARA RECIBIR SUS CONTRASEÑAS DE UN SOLO USO (CÓDIGO 2FA) Y TOMAR CONTROL DE LA RED TELEFÓNICA

El estafador se presenta físicamente o contacta con la compañía de telecomunicaciones para duplicar la tarjeta. Realizado el cambio, el usuario pierde la señal en su dispositivo móvil, situación que puede interpretarse como una intermitencia del dispositivo y no de un robo efectuado.

CONFIRMADOS LOS CÓDIGOS 2FA, ESTOS LLEGAN A LA SIM DUPLICADA, OBTENIENDO EL CONTROL DE LA RED TELEFÓNICA

El siguiente movimiento lateral es el robo de cuentas de correos, suplantación de identidad o, en su caso, el retiro de dinero a su nombre.

SECTOR SANITARIO

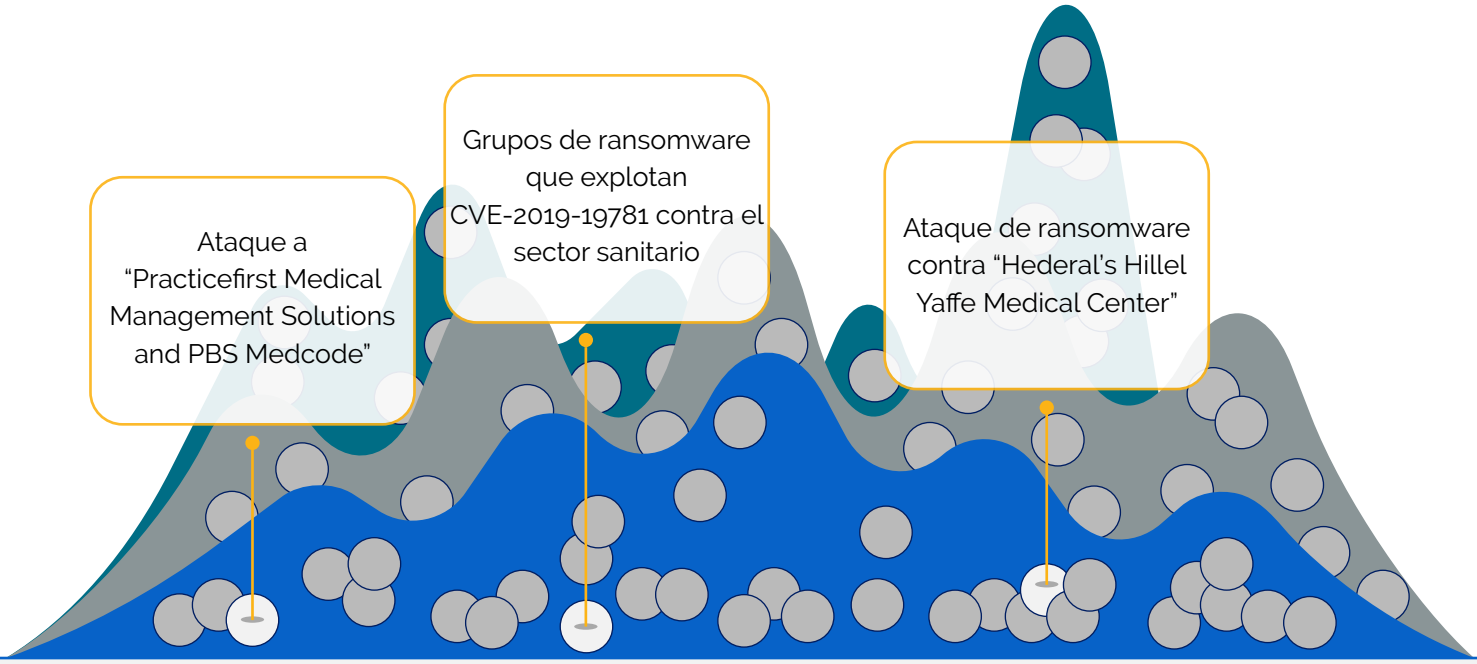
Las redes informáticas del sector sanitario se han visto afectadas en el segundo semestre de 2021 por diversos ataques cibernéticos de ransomware y con la distribución de otros tipos de malware.

SARS-CoV-2 (COVID-19)

La tendencia en cuanto a ciberataques contra el sector sanitario se sigue manteniendo al alza tras la declaración de pandemia por el SARS-CoV-2 (COVID-19).

De acuerdo con la información monitorizada y recopilada en el segundo semestre de 2021, el sector sanitario ha sufrido más de 60 ataques ransomware, incluyéndose en dicho sector hospitales, clínicas privadas, centros de salud y laboratorios.

A la hora de analizar todos los ataques cibernéticos sufridos por el sector sanitario en el último semestre de 2021, esta cifra incrementa notablemente, pudiendo distinguir entre ataques informáticos de diversa tipología (troyanos, brechas de seguridad, *infostealers*, spyware, ransomware).



DATOS DESTACABLES DE ATAQUES AL SECTOR SANITARIO DURANTE EL SEGUNDO SEMESTRE DE 2021

- Se han producido más de 300 incidentes de seguridad en el sector sanitario a nivel internacional.
- Se observan altos picos en los meses de julio, septiembre, octubre y principios de diciembre.
- Destacan diversos ataques informáticos que han tenido un impacto considerable en el sector sanitario, sobre todo centros hospitalarios y sus laboratorios, como el ataque a la Corporación de Salud Macquarie (MHC, por sus siglas en inglés) o diversos centros médicos en Israel.
- Este tipo de ataques suelen tener consecuencias largo plazo.
- Tras el ataque de ransomware al Servicio Ejecutivo de Salud de Irlanda que tuvo lugar en mayo de 2021, aún en el segundo semestre de 2021, los hospitales irlandeses no han vuelto a funcionar con total normalidad.
- En el mes de diciembre, el Hospital Coombe de Dublín sufría un nuevo ciberataque, y el HSE ha advertido a otro hospital de Dublín sobre un potencial ciberataque próximo.

SECTOR EDUCATIVO

Durante la segunda mitad de 2021, las entidades educativas han continuado siendo uno de los principales objetivos de ciberataques, manteniendo la tendencia observada a lo largo del último año.

CONVERSIÓN TECNOLÓGICA

Se estima que los ciberataques contra estas organizaciones han constituido un importante número de incidentes, así como un impacto significativo en el desarrollo de su actividad.

La conversión tecnológica que han afrontado las entidades educativas tras el COVID-19 ha supuesto un nuevo escenario de riesgos tecnológicos a los que han tenido que enfrentarse a lo largo del último semestre de 2021.

CAMPAÑAS DE *MALSPAM* Y *SPEARPHISHING*

ATAQUES DDoS

BRECHAS DE DATOS

INFECCIÓN POR MALWARE Y RANSOMWARE

A lo largo del segundo semestre de 2021, los actores maliciosos han aprovechado esta rápida reconversión del sector para explotar las vulnerabilidades existentes en las organizaciones y desplegar un amplio número de ataques.

En los últimos meses, se ha podido observar cómo el sector enfrenta una serie de riesgos generales que ponen en peligro la ciberseguridad de las organizaciones.

ESTE TIPO DE ORGANIZACIONES SE ENFRENTAN A UNA SERIE DE PREMISAS QUE LOS VUELVEN VULNERABLES AL ATAQUE DE ACTORES MALICIOSOS

Uso de tecnologías vulnerables, como puede ser la plataforma de videoconferencias Zoom, ampliamente utilizada para la docencia online.

Sistemas desactualizados y con sistemas de defensa débiles.

Comunidades de usuarios con falta de conocimientos sobre ciberseguridad, que convierten a las organizaciones en objetivo de ataque.

La pandemia de coronavirus ha afectado drásticamente al sector de la educación y los centros e instituciones se han visto obligados a acelerar su reconversión tecnológica para mantener su actividad.

Se estima que el sector educativo ha sido uno de los más afectados durante el último semestre del año en cuestión de ciberataques. A escala mundial, se han registrado importantes infecciones por ransomware (especialmente, por el programa PYSA) a escuelas K-12 en Estados unidos y centros educativos británicos. Pero no son las únicas organizaciones impactadas: se han registrado importantes brechas de datos en centros educativos de India y Turquía, así como campañas de *phishing* contra universidades estadounidenses.

ALGUNOS DE LOS ATAQUES MÁS SIGNIFICATIVOS EN EL ÚLTIMO SEMESTRE HAN SIDO:

Ciberataque a la Universidad Autónoma de Barcelona

Ciberataque a la Universidad de Lisboa

Ataque informático a la Pontificia Universidad Javeriana

CIBERATAQUE A LA UNIVERSIDAD AUTÓNOMA DE BARCELONA

El pasado mes de octubre, la UAB comunicó públicamente haber sido víctima de un ataque ransomware, atribuido al programa de cifrado PYSA, que habría provocado el cifrado de archivos e información confidencial, impactando en más de 650 000 archivos.

Aunque el vector de entrada del ataque es desconocido hasta el momento, la institución tomó medidas de contención del ataque que incluyeron la desconexión de las redes del campus, así como el bloqueo de accesos a sus plataformas.

De igual manera, la institución puso en marcha un entorno online completo de Microsoft para poder continuar con su actividad y trabaja para reestablecer por completo su actividad.

Aunque hasta el momento no se ha producido filtración de información, las autoridades no descartan que se publiquen datos internos o de miembros de la comunidad educativa en el blog de la Deep Web de PYSA.

CIBERATAQUE A LA UNIVERSIDAD DE LISBOA

A finales del mes de octubre, la Universidad de Lisboa fue víctima de un ataque informático contra los servidores Windows de la institución.

Según medios públicos, el incidente se produjo tras la infección por un ransomware a los sistemas universitarios, que fueron suspendidos como medida de prevención.

Aunque el centro ha hecho público que no ha habido compromiso de información personal o financiera de la comunidad académica y que se limitó a la recopilación de credenciales de acceso a cuentas e-mail, hasta seis facultades se habrían visto involucradas en el incidente, suspendiéndose el acceso a sus servidores de correo electrónico.

CIBERATAQUE A LA PONTÍFICA UNIVERSIDAD JAVERIANA

El pasado mes de noviembre, la Universidad Javeriana hizo pública la noticia de un ataque informático contra sus sistemas que habría obligado a la organización a deshabilitar algunos de sus servicios tecnológicos para proteger la operación.

Aunque se desconoce el origen o naturaleza del incidente, el centro instó a la comunidad a abstenerse de utilizar las infraestructuras o red informática para evitar la extensión del ataque.

INFRAESTRUCTURAS CRITICAS

Durante el segundo semestre del año 2021, se han visto numerosos ataques cuyos objetivos han sido las infraestructuras críticas de diferentes países, relacionadas con medios de transportes, entidades relacionadas con la energía eólica, empresas suministradoras de petróleo, gasolineras, etc.

CIBERATAQUES A INFRAESTRUCTURAS CRÍTICAS

Continúan siendo uno de los mayores riesgos a los que la sociedad se enfrenta debido al gran daño, repercusión y a las consecuencias que traen consigo, tales como la paralización o los colapsos en los servicios públicos, situaciones de desabastecimiento, etc.

TRANSPORTES

Durante este periodo se han detectado una multitud de ciberataques contra grandes empresas de transportes que forman parte de la infraestructura crítica de un país: la red ferroviaria de Irán junto al Ministerio de Transportes, aerolíneas como Mahan Air, el sistema de transporte público de Toronto, etc., aunque destacan dos incidentes debido a la magnitud y al número de afectados que tuvieron.

TRANSNET

Empresa sudafricana encargada de administrar la infraestructura ferroviaria, portuaria y de tuberías del país. Tras sufrir un ciberataque, las terminales de contenedores del puerto de Ciudad del Cabo dejaron de funcionar y el registro de movimiento de contenedores se tuvo que realizar manualmente.
El puerto de Durban también se vio afectado, produciendo que la congestión logística se viera incrementada en gran medida, repercutiendo en la economía del país.

GRUPO DE AMENAZAS DEV-0343

De acuerdo con la información difundida por el Centro de Inteligencia de Amenazas de Microsoft (MSTIC), sería el responsable de haber difundido las contraseñas de más de 250 clientes que utilizan Office 365.
Algunos de esos clientes fueron empresas de tecnología de defensa estadounidenses e israelíes, puertos de entrada del Golfo Pérsico o empresas de transporte marítimo global con presencia comercial en el Medio Oriente.

RANSOMWARE "CONTI"

Durante el segundo semestre de 2021, el ransomware Conti se ha empleado en diferentes ciberataques dirigidos a una multitud de empresas o entidades pertenecientes al sector de las infraestructuras críticas (eléctricas, petrolíferas, etc.).

En la mayoría de los ataques que han tenido éxito utilizando este ransomware, los ciberdelincuentes obtuvieron información confidencial e información personal de los trabajadores de las empresas y diferentes muestras fueron publicadas por el grupo Conti en su sitio *web* de la *Deep Web* Conti News para su posterior venta.

Entre las empresas que se vieron afectadas por el ransomware Conti durante este periodo, se encuentran una empresa de exploración y producción de petróleo y gas de Kansas, una operadora italiana de gas natural y electricidad, una empresa fotovoltaica china y un proveedor de electricidad en Australia.

RANSOMWARE LOCKBIT & LOCKBIT 2.0

En el segundo semestre del año 2021, tanto el ransomware Lockbit como el Lockbit 2.0 se utilizaron en diferentes ciberataques relacionados con infraestructuras críticas.

Entre los principales ciberataques empleando el ransomware Lockbit, se encuentran los sufridos por el primer operador de energía eólica en Italia, una prestadora de servicios de gas natural que opera en Indonesia, un fabricante de turbinas eólicas o la aerolínea Bangkok Airways.

En la mayoría de los ataques consiguieron información confidencial de la empresa o de sus clientes y la pusieron a la venta en su sitio *web* de la *Dark Web*.

Posteriormente, y con la versión 2.0 del malware, se vieron afectados un operador alemán de parques eólicos, una multinacional francesa que ofrece soluciones digitales de energía y automatización, y un grupo de energía renovable con sede en la India.

SECTOR IT Y TELECOMUNICACIONES

El sector de las telecomunicaciones ha sido uno de los principales sectores objetivo de ciberataques durante el segundo semestre de 2021. Durante este periodo, se han descubierto varias campañas a empresas del sector en Europa, Estados Unidos y Asia, con especial mención al grupo REvil.

AUMENTAN LOS ATAQUES CON EL PASO DE LOS AÑOS

Desde que en el año 2010 se produjera un incidente en una central nuclear de Irán, causado por el malware Stutnex, cada vez son más comunes este tipo de ataques.

Desde comienzos de 2019, este sector ha sufrido un aumento de ciberataques, llevados a cabo por todo tipo de actores: desde los que buscan un beneficio económico, hasta los que desean robar información confidencial, APT, etc.

KASEYA

REVIL

GODADDY

CIBERESPIONAJE CHINO

MALKAMAK

El sector de las telecomunicaciones ha sido uno de los sectores más afectados desde el comienzo de la pandemia, desde los bulos compartidos en las redes sociales sobre las redes de 5G, hasta los *phishings* en los que empresas de telefonía son suplantadas para ofrecer "gigas gratis por el coronavirus".

KASEYA

A principios del mes de julio, la empresa multinacional de software y servicios IT Kaseya fue víctima de un ciberataque de ransomware.

El vector inicial del ataque fue una vulnerabilidad *zero-day* (CVE-2021-30116) en Kaseya VSA, lo que permitió a los atacantes ejecutar comandos de forma remota en el dispositivo VSA.

Esta solución es utilizada comúnmente por parte de estos proveedores de servicios para administrar los sistemas de sus clientes.

Se desconoce el número de empresas afectadas por dicho ataque, estimándose que el total de compañías está entre 800 y 1500 distribuídas por todo el mundo, siendo su gran mayoría proveedores y pequeñas o medianas empresas.

El grupo REvil proclamó su autoría a través de su blog oficial, requiriendo 70 millones de dólares para publicar la herramienta que permitía el descifrado de la información vulnerada.

A mediados del mes de julio, Kaseya obtuvo una clave de descifrado universal para el ataque de ransomware de un desconocido "tercero de confianza", comenzando a distribuirla a los clientes afectados.

REVIL

Uno de los operadores de telecomunicaciones más consolidados de España, anunció a principios del mes de julio haber sufrido el ciberataque de un ransomware.

El grupo REvil publicó en su blog oficial haber comprometido a dicha empresa, habiendo accedido y descargado bases de datos e información confidencial de la misma. Diversas imágenes de los archivos sustraídos se publicaron con el fin de demostrar dicho ataque.

Tras el ataque, no se publicó ninguna petición de rescate por los delincuentes, ni se informó por parte de la compañía, desconociéndose la existencia de la misma.

Desde dicho proveedor de telefonía, se informó que diversos servidores se vieron afectados por el ataque, aunque su importancia fue baja, “no habiéndose perdido ninguna información”.

GODADDY

La plataforma de hosting GoDaddy sufrió a principios del mes de septiembre una intrusión a través del uso de una contraseña comprometida, al entorno de alojamiento de WordPress.

Dicha vulneración se detectó a mediados de noviembre, implementándose medidas de seguridad y de mitigación.

La empresa comunicó que la afectación de dicho incidente supera los 1,2 millones de clientes, habiéndose filtrado datos como direcciones de correos electrónicos, contraseñas, nombres, claves privadas SSL y números de clientes.

Esta compañía de *hosting* sufrió en marzo y en mayo del año 2020 otros ciberataques con más de 28 000 cuentas de clientes afectadas.

CIBERESPIONAJE CHINO

En el mes de septiembre se detectó una campaña de ciberespionaje a empresas del sector de telecomunicaciones del Sudeste Asiático en los últimos años por parte de ATP relacionadas con el gobierno chino.

Dicha posible relación se lleva a cabo a través del uso de las técnicas, tácticas y procedimientos empleados, encontrándose sus objetivos alineados con los intereses del gobierno de China.

Se conoce que los actores explotaron vulnerabilidades en los servidores de Microsoft Exchange, pudiendo acceder a las comunicaciones sensibles llevadas a cabo en los servicios de telecomunicaciones afectados.

Entre los objetivos se encuentran corporaciones políticas y gubernamentales, agencias policiales y organizaciones disidentes para el estado chino.

MALKAMAK

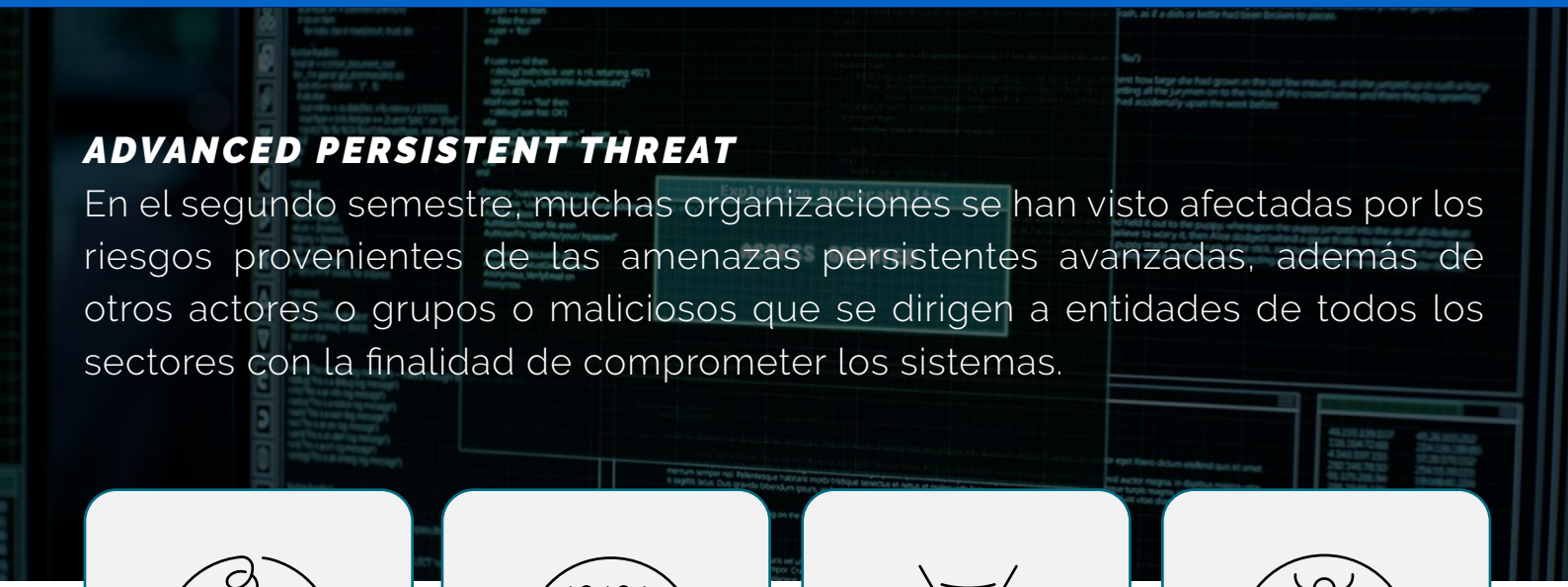
En el mes de octubre se descubrió un nuevo actor de amenazas denominado MalKamak, relacionado con una operación de ciberespionaje dirigido a empresas de telecomunicaciones y del sector aeroespacial desde el año 2018.

MalKamak opera a través de un troyano de acceso remoto denominado ShellClient, el cual es capaz de evadir los dispositivos de seguridad para lograr el comando y control.

Los principales objetivos de dicho grupo se centran en Oriente Medio, Estados Unidos, Rusia y Europa. Se han detallado distintas conexiones con APT iraníes como Chafer APT o Agrius APT.

APT

Destaca la aparición de nuevos actores de amenazas como grupos o APT, además del regreso de la botnet Emotet, que han conseguido evolucionar en cuanto a sus tácticas, técnicas y procedimientos.



ADVANCED PERSISTENT THREAT

En el segundo semestre, muchas organizaciones se han visto afectadas por los riesgos provenientes de las amenazas persistentes avanzadas, además de otros actores o grupos o maliciosos que se dirigen a entidades de todos los sectores con la finalidad de comprometer los sistemas.

NOBELIUM

CHAMELGANG

EMOTET

TRICKBOT

El término APT o *"Advanced Persistent Threats"* hace referencia a un ciberataque con un alto grado de sofisticación, así como a grupos patrocinados por estados que llevan a cabo estas campañas maliciosas.

Durante los últimos años, se han podido observar diversos incidentes de seguridad relacionados con la acción de estas APT, que han permitido contemplar el alcance global de las campañas que llevan a cabo estos actores.

NOBELIUM

El grupo de amenazas vinculado a Rusia, conocido por el ataque de la cadena de suministro contra SolarWinds, ha mostrado actividad durante el segundo semestre.

En octubre, Microsoft observó una campaña dirigida a más de 600 clientes, aprovechando una gama diversa de técnicas como el robo de *tokens*, la explotación de API o el *spear-phishing* para desviar credenciales asociadas a cuentas privilegiadas de proveedores de servicios, permitiendo el movimiento lateral en entornos de nube.

Durante el mes de diciembre, continuaron con ataques dirigidos a diversas organizaciones francesas.

Por otro lado, según los investigadores de seguridad, el grupo ha hecho uso de una nueva variante de malware, apodada CEELOADER e incorporada en su arsenal con el objetivo de vulnerar las redes gubernamentales y empresariales a nivel mundial.

Finalmente, se ha identificado una nueva infraestructura de servidor sospechosa, probablemente asociada con el grupo, la cual se conoce como SOLARDEFLECTION.

La infraestructura se encuentra en la fase operativa y es probable que ya se esté utilizando o que pronto se utilice para operaciones.

CHAMELGANG

Se trata de un nuevo grupo cibercriminal no asociado con ningún actor de amenazas existente que ha estado aprovechando las vulnerabilidades conocidas como ProxyShell de Microsoft Exchange Server y utilizando un malware nuevo para comprometer las redes en ataques dirigidos a empresas rusas del sector energético y de aviación.

El grupo oculta su infraestructura de red y malware bajo los servicios legítimos de empresas como Microsoft, TrendMicro, McAfee, IBM y Google a través del uso de dominios parecidos a los legítimos y también mediante el uso de certificados SSL que imitan a empresas conocidas.

Según los ataques conocidos, uno de ellos se dirigió a la red de una compañía energética a través de la cadena de suministro mediante el compromiso de una versión vulnerable de la aplicación web de una empresa subsidiaria, además de comprometer redes de otros países como Estados Unidos, Japón, Turquía, Taiwán, Vietnam, India, Afganistán, Lituania y Nepal, incluyendo servidores gubernamentales como objetivo.

EMOTET

Se ha tratado de una de las amenazas más relevantes en este periodo.

A mediados del mes de noviembre, se observaron evidencias del regreso de Emotet, una *botnet* que había sido desmantelada a principios de año, pero que ha vuelto a ser activada por los actores maliciosos, mostrando actividad de propagación a través del malware Trickbot.

Además, se ha observado que Emotet actualmente despliega una *beacon* de Cobalt Strike, lo que facilitaría la acción a los ransomware.

TRICKBOT

El troyano bancario modular Trickbot es otra de las amenazas más relevantes del panorama cibercriminal actual.

Según datos de s21sec, Trickbot ha atacado a 194 países. El 36,67 % de los ataques de Trickbot se produce sobre máquinas en suelo estadounidense. Le siguen Alemania con un 8,25 % e Italia con un 6,85 %.

España es el decimosegundo país con más *endpoints* atacados por Trickbot, con un 1,06 %. Portugal es el núemero 52 con un 0,07 % de los ataques.

BRECHAS DE SEGURIDAD

El segundo semestre de 2021 se caracterizó por incidentes de alto perfil que involucraron software de proveedores que llevaron a brechas de seguridad generalizadas de datos y ataques de malware.

BRECHAS DE DATOS

Organizaciones pertenecientes a múltiples sectores (finanzas, gobierno, educación, telecomunicaciones, salud, energía, tecnología y manufactura) han sufrido brechas de datos como resultado del compromiso de los sistemas por parte de actores de amenazas.

LINKEDIN | **ZURICH ESPAÑA** | **FORTINET** | **EPIK**

ACER | **ACCENTURE** | **TELEFÓNICA**

Las consecuencias de este tipo de incidentes de ciberseguridad incurren en daños reputacionales y financieros para la empresa afectada, así como ataques de tipo *phishing*, ransomware o suplantación de identidad en caso de víctimas afectadas por la información personal comprometida.

LINKEDIN

TomLiner, un actor del foro RaidForums, puso a la venta a finales de junio un presunto volcado de datos relativos a 700 millones de usuarios de usuarios de la red profesional de LinkedIn.

Los datos incluían nombres, género, correo electrónico, teléfono e información de la industria.

LinkedIn emitió un comunicado oficial en su sitio *web* en el que se aportaba información acerca de la investigación llevada a cabo a cerca del incidente, afirmando que se trataban de datos que se habían extraído de LinkedIn y otros sitios web que incluyen los mismos datos que ya habían sido informados previamente.

ZURICH ESPAÑA

En agosto, la división española de Zurich Seguros fue víctima del robo de las bases de datos de sus clientes, tras un ciberataque ocurrido entre el 12 y 13 de agosto en el que se extrajo información que fue puesta a la venta en un foro underground de piratería.

Con un total de 4 260 757 líneas de registro se aprecia una base de datos relativa a pólizas privadas de vehículos, con datos que van desde el DNI, domicilio, teléfono, o correo electrónico, hasta la matrícula o modelo de estos.

La información robada se puso a la venta en internet a un precio de 1000 dólares en bitcoins.

FORTINET

Un actor de amenazas con motivaciones financieras apodado Groove, activo desde agosto de 2021, filtró en el mes de septiembre aproximadamente 500 000 credenciales comprometidas de VPN de Fortinet.

Es probable que las credenciales se hayan recopilado explotando una vulnerabilidad de tipo directorio restringido (CVE-2018-13379) en Fortinet FortiOS que se ejecuta en los dispositivos Fortigate.

Las credenciales filtradas pueden permitir a actores de la amenaza comprometer redes de las organizaciones con dispositivos VPN comprometidos y realizar actividades maliciosas como desplegar ransomware o robar datos confidenciales.

De entre los países afectados mundialmente por esta brecha se encuentran Portugal, México y España.

EPIK

La empresa estadounidense Epik, especializada en registros de dominios y alojamiento *web*, fue víctima de un incidente de seguridad reivindicado por el grupo hacktivista Anonymous como parte de una operación conocida como "#OperationJane" u "Operation Epik Fail" anunciada en septiembre.

Anonymous filtró 180 GB de datos y el grupo hacktivista Distributed Denial of Secrets señaló que habrían conseguido una copia de la base de datos robada, la cual fue publicada a través de sus canales digitales.

Poco después, se filtró la segunda parte de los datos, un total de 300 GB de información entre la cual, según afirman, se exponen al menos 59 claves API y credenciales de inicio de sesión de los sistemas de Epik y sus cuentas oficiales en Twitter, Coinbase y PayPal.

ACER

Octubre se vio marcado por una filtración de datos publicada en un foro de cibercriminales de acceso público.

Un grupo llamado Desorden afirmó haber robado 60 GB de bases de datos y otros archivos de los servidores de Acer India que habían sido violados.

Los *hackers* compartieron un enlace a una muestra de los datos robados y publicaron un vídeo que muestra los archivos que supuestamente robados que incluían información de millones de clientes, credenciales de acceso utilizadas por miles de minoristas y distribuidores de Acer, así como documentos corporativos, financieros y de auditoría.

ACCENTURE

A mediados de octubre, Accenture reveló una brecha de datos tras el ataque del ransomware LockBit 2.0, ocurrido en agosto de 2021.

Cyble informó que la banda de ransomware robó bases de datos que contenían más de 6 TB de datos y exigía un rescate de 50 millones de dólares.

TELEFÓNICA

Movistar se vió afectado por un incidente de seguridad, tras el cual terceros no autorizados accedieron a una base de datos con información personal de clientes de la compañía.

Según los datos de la investigación realizada, la brecha afectó en torno al 1 % de los clientes, exponiendo información relativa a nombres, números de teléfono y productos contratados con la compañía.

CONCLUSIONES

RANSOMWARE

Ha continuado la tendencia a la alza de la utilización de este tipo de programas informáticos por parte de actores maliciosos para la obtención de beneficios económicos.

Algunos ransomware activos durante los últimos años han acabado con su actividad (por ejemplo, REvil).

Han surgido nuevos ransomware que se han convertido en amenzas para las redes corporativas.

En el informe se han mostrado las diferentes vulnerabilidades explotadas por los operadores de ransomware.

MALWARE BANCARIO

Se destaca la amenaza conocida como SquirrelWaffle, un malware que se distribuye a través de correos electrónicos con adjuntos maliciosos que descarga un payload final de Qbot o de Cobalt Strike.

MALWARE MÓVIL

Se sigue destacando Android como el principal sistema operativo al que se dirigen estos malware.

iOS también ha recibido numerosas menciones tras descubrirse el spyware Pegasus, que habilita un *jailbreak* en el dispositivo y permite leer mensajes de texto, rastrear llamadas, etc.

SIM SWAPPING

Se ha producido un aumento de este tipo de ataques, que permiten a los atacantes tomar el control del número de móvil de un objetivo, engañando o sobornando a los empleados de su proveedor de telefonía para que reasigne los números a las tarjetas SIM controladas por el estafador.

SECTOR SANITARIO

Se mantiene la tendencia al alza de los últimos dos años de ataques a centros de salud y hospitales.

Además, los actores maliciosos siguen aprovechando la situación sociosanitaria y las diferentes variantes de la COVID-19 para engañar a las víctimas.

THREAT LANDSCAPE REPORT

S21SEC

www.s21sec.com