THREAT LANDSCAPE REPORT

S21SEC

Cyber Solutions by Thales

INTRODUCCIÓN

Este segundo semestre de 2022 se ha caracterizado principalmente por la presencia de amenazas ya conocidas anteriormente, tanto en 2022 como en años anteriores, lo que ha supuesto un riesgo para entidades públicas y privadas, con casi 1500 ataques registrados públicamente por los actores de amenazas.

Como en el semestre anterior, destaca la explotación de vulnerabilidades como Follina o Spring4shell, que involucran a proveedores como Apple, Cisco, Google o Microsoft Exchange. El mayor peligro de estas amenazas es que muchas de ellas se han explotado en ataques zero-day que no disponen de parches o correcciones y que se están convirtiendo en uno de los recursos más empleados por los actores.

Según datos de la Base de Datos Nacional de Vulnerabilidades, se han divulgado 13 243 vulnerabilidades clasificadas con el estándar del Sistema de Puntuación de Vulnerabilidad Común v3.X. Por otro lado, este semestre se han identificado 44 familias de ransomware que han afectado a una amplia gama de sectores de la industria de todo el mundo, destacando al sector industrial y el sanitario.

Destaca también la aparición de nuevas operaciones con respecto al semestre anterior, en el que se observaron tan solo 10 grupos, en comparación con los 15 nuevos del último semestre de 2022.

Una vez más, los dispositivos móviles siguen siendo uno de los objetivos principales de los cibercriminales, que siguen encontrando formas de introducir sus malware en los mercados oficiales de Google y Apple.

Este semestre también resalta por la gran actividad de grupos de amenazas persistentes avanzadas de origen coreano, ruso y chino.

CONTENIDOS

01 Vulnerabilidades
02 Ransomware
03 Conflicto Ucrania
04 Sector financiero
05 Malware móvil
06 Sector energético
07 Sector defensa
08 Sector sanitario
09 Sector industrial
10 Hacktivismo
11 APTs
12 Telco
13 Sector aseguradoras
14 Ataques relevantes

VULNERABILIDADES

Las vulnerabilidades cibernéticas son debilidades en el software que pueden explotarse para comprometer los sistemas en ataques cibernéticos.

El panorama de amenazas en materia de vulnerabilidades durante el segundo semestre de 2022 se basa en el análisis de las divulgaciones de las más importantes durante este período, que se ha caracterizado por la explotación de vulnerabilidades que involucran a proveedores como Microsoft Exchange, Cisco, Google, Apple y F5, entre otros.

01

A pesar de que durante los últimos seis meses se ha observado la explotación de vulnerabilidades conocidas en la primera mitad de 2022, tales como Follina (CVE-2022-30190), la vulnerabilidad CVE-2022-26134 de Atlassian Confluence, Dog Walk (CVE-2022-34713) o Sprin4shell (CVE-2022–22965), otras vulnerabilidades siguen ocupando un lugar destacado por su explotación continuada a pesar de haber sido divulgadas en años anteriores, tales como Log4Shell (CVE-2021-44228) o ProxyLogon (CVE-2021-26855).

Destacan muchas de las vulnerabilidades explotadas en ataques zero-day antes de su divulgación o en ataques en los que se ha dado a conocer la vulnerabilidad, pero que aún no disponen de parches o correcciones, debido a su uso por parte de actores de amenazas que apuntan a sistemas vulnerables en ataques activos.

En este sentido, se aprecia una rápida capitalización de las debilidades explotadas en los sistemas, siendo los exploits zero-day uno de los recursos más empleados en ataques activos durante el segundo semestre.

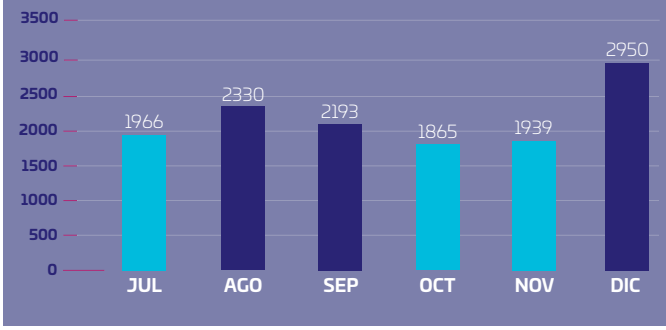
*La ingeniería social es el **principal vector** de acceso inicial*

DogWalk, Follina y muchas otras vulnerabilidades muestran una alta explotación a través de campañas de phishing y malspam por parte de actores de amenazas durante el segundo semestre de 2022.

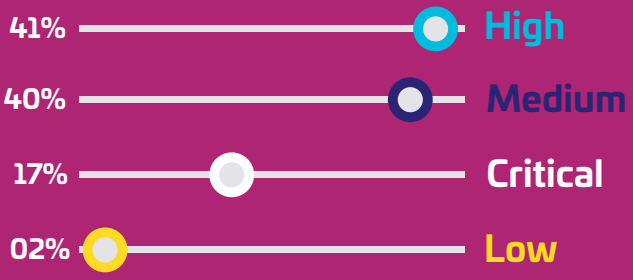
***13 243 vulnerabilidades** han sido divulgadas*

Según los datos obtenidos del NIST (National Vulnerability Database), se han divulgado un total de 13 243 vulnerabilidades clasificadas con el estándar del Sistema de puntuación de vulnerabilidad común (CVSS) v3.X.

***Agosto**, **septiembre** y **diciembre** son los meses de mayor actividad*



***Nivel de gravedad** basado en CVSS versión 3*



En cuanto a la actividad de explotación de vulnerabilidades por parte de actores de amenazas, en julio se observaron campañas de phishing que explotaban la vulnerabilidad rastreada como CVE-2022-30190, mejor conocida como Follina.

Disribuían la backdoor Rozena en sistemas Windows vulnerables mediante el envío de correos electrónicos con documentos Office maliciosos. La backdoor inyectaba una conexión de Shell remota a la máquina del atacante, pudiendo así tomar el control total del sistema.
Asimismo, los actores de amenazas explotaron la vulnerabilidad CVE-2022-2207 de elevación de privilegios, que permitiría la ejecución de código como usuario sin privilegios, que está siendo explotada por actores maliciosos y afecta a Windows 11 y Windows Server.

En agosto continuó la explotación de Follina en ataques de al menos un año dirigidos contra organizaciones rusas, para la distribución del troyano de acceso remoto (RAT) conocido como Woddy RAT.
Durante este mes, también se informó de que la explotación de vulnerabilidades zero-day y exploits de prueba de concepto (POC) recientemente publicados fueron factores que contribuyeron a una gran cantidad de vulnerabilidades de alto riesgo en productos de Apple, Google y Microsoft. Otros proveedores afectados fueron DrayTek, Moodle, Palo Alto Networks, Realtek y VMWare.
Por otro lado, en agosto de 2022 la vulnerabilidad CVE-2022-34713, conocida como DogWalk, supuso una nueva tendencia de delincuentes que explotan una falla en el Microsoft Support Diagnostic Tool (MSDT) para explotar a través de un documento malicioso, que no requiere que una víctima habilite las macros.

A finales de septiembre se compartió un análisis sobre una vulnerabilidad de ejecución remota de código zero-day utilizada en ataques in the wild por actores de amenazas. El zero-day afecta a Microsoft Exchange en las plataformas de correo corporativo.
Según el aviso publicado el 30 de septiembre para la vulnerabilidad de ejecución remota de código de Microsoft Exchange Server rastreada como CVE-2022-41040 y CVE-2022-41082, Microsoft indica estar al corriente de los ataques dirigidos y que estos serían limitados, confirmando que los sistemas están siendo atacados utilizando la vulnerabilidad zero-day con el objetivo de instalar backdoors para obtener acceso remoto a los sistemas y realizar otros ataques más específicos y de mayor impacto.

OCTUBRE

Destacan vulnerabilidades zero-day detectadas que afectaron a Apple, Fortinet, Google y Microsoft.
Vulnerabilidades Mark-of-the-Web (MOTW) que afectan a versiones recientes de Microsoft Windows y Windows Server aún no tienen asignados identificadores CVE, pero al parecer también han sido explotadas activamente.

NOVIEMBRE Y DICIEMBRE

En noviembre y diciembre continuó la tendencia de explotación de zero-days por parte de actores de amenazas, como el zero-day CVE-2022-41228, que estaría siendo utilizado por los operadores detrás del ransomware Magniber junto a otros grupos cibercriminales para poder ejecutar código arbitrario en el sistema infectado con privilegios de usuario, junto con la explotación en ataques ransomware de la vulnerabilidad CVE-2020-1472, que lleva activa desde 2020 y que permite la elevación de privilegios empleando el protocolo remoto de Netlogon (MS-NRPC).

RANSOMWARE

El escenario global de amenazas ransomware del segundo semestre de 2022 ha registrado un total de 1487 ataques.

Según la monitorización llevada a cabo por el equipo de Threat Intelligence de S21sec relativa a la actividad de actores de amenazas en más de 50 páginas de la Deep Web de grupos ransomware.

02

Se debe tener en cuenta que la cifra de ataques observada abarca exclusivamente la actividad pública registrada que ha sido realizada por los actores de amenazas.

Se han identificado 44 familias de ransomware dirigidas a una amplia gama de sectores y verticales de la industria a nivel mundial.

Entre los grupos más activos se encuentra LockBit, BLackCat (ALPHV) y Black Basta.

S21SEC Cyber Solutions by Thales

FAMILIAS DE RANSOMWARE

Estadísticas ransomware

A continuación mostramos el análisis de la actividad realizada por las 10 familias de ransomware más activas durante el semestre analizado. La actividad conjunta de todas ellas supone más del 70 % del total de ataques de ransomware producidos en el semestre.

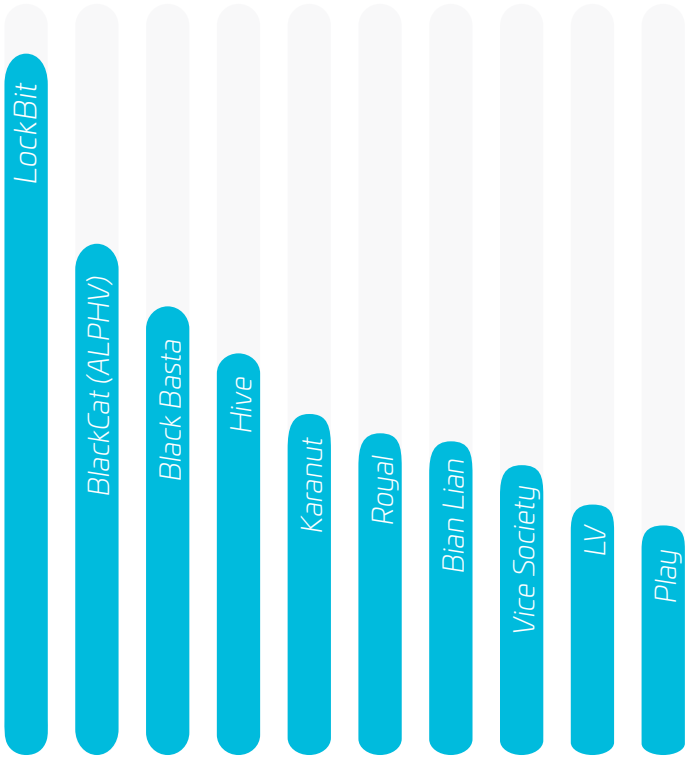
Destaca la tendencia relativa a la aparición de nuevas operaciones de ransomware, incrementándose significativamente respecto a la cantidad de grupos observados durante el semestre anterior, en el que se observaron aproximadamente 10 grupos entre enero y junio, a diferencia de la segunda mitad de 2022, en la que proliferaron más de una quincena de operaciones nuevas.

Así, en Julio surgen los grupos conocidos como Haron, Omega, RedAlert, Bian Llan BlOOdy y Play, todos con una intensa actividad a nivel mundial y con un enfoque amplio de objetivos. Otras operaciones como Donuts Leak, IceFire, Play o Sparta, esta última dirigida exclusivamente en objetivos españoles, cuya actividad inicia a partir del 13 de septiembre de 2022, a través del sitio de extorsiones de la Deep Web Sparta Blog, dedicado a la filtración de datos y extorsión del grupo.

Otra operación destacada es el ransomware Royal que fue en noviembre cuando el grupo hizo públicos sus ataques a través del sitio de fugas alojado en la Deep Web. Royal se dirige a las víctimas a través de ataques de phishing mediante correos de falsas renovaciones de suscripciones de productos de software o servicios de entrega de productos legítimos, indicando un número de teléfono a la víctima para que le dé acceso remoto al dispositivo y proceder así al cifrado de sus archivos a través de la extensión .royal, dejando una nota de rescate README.TXT en los sistemas infectados. El ransomware es capaz de cifrar archivos del disco virtual (VMDK).

Finalmente, el ransomware Nokoyawa, (detectada en marzo de 2022) mostró actividad en un sitio de filtraciones de la Deep Web abierto a finales de año, siendo posible que el grupo esté vinculado a la operación de ransomware Hive tras compartir similitudes en sus tácticas, técnicas y procedimientos (TTP), como la cadena de ataques y herramientas empleadas.

Top 10 de familias de ransomware más activos durante el segundo semestre de 2022.



SECTORES MÁS AFECTADOS

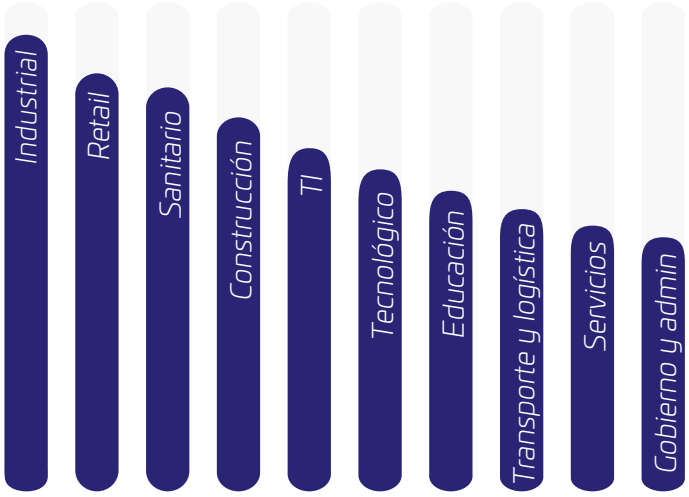
Estadísticas Ransomware

Durante el segundo semestre de 2022, la actividad se dirigió mayoritariamente a las empresas pertenecientes al sector industrial (14 %), retail (7 %) y sanitario (7 %).

En el siguiente gráfico indicamos los 10 sectores más afectados de entre la amplia gama de verticales de la industria que se han visto expuestos durante el período analizado.

En su conjunto, el impacto de las amenazas ransomware asciende a más del 65 % de los ataques monitorizados.

Top 10 víctimas de ransomware por sector durante el segundo semestre de 2022.



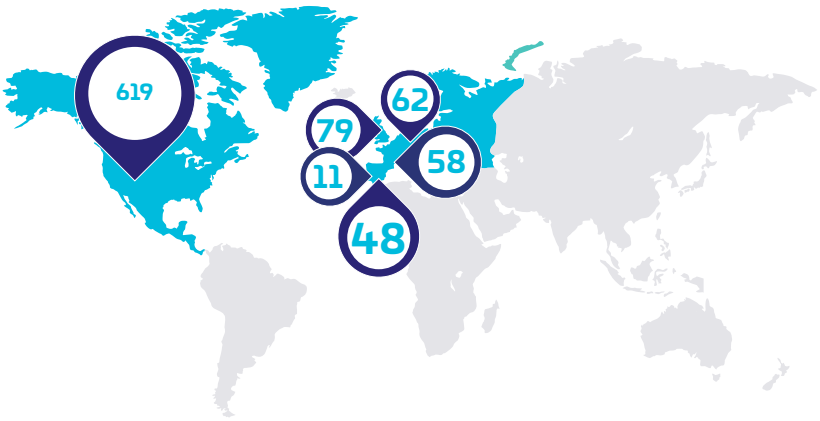
PAÍSES MÁS AFECTADOS

Estadísticas ransomware

Los grupos de ransomware se han dirigido mayoritariamente a objetivos localizados en América del Norte, con un total de 696 ataques registrados, el 42 % del total de ataques reivindicado en el segundo semestre (1487). Europa ha sufrido 421 ataques registrados, y Asia 189 incidentes cibernéticos.

España ha sufrido 48 ataques durante el segundo semestre de 2022, lo que supone un incremento del 41 % comparado con semestre anterior. Lo mismo sucede con Portugal, que registra 11 ataques, un 120 % de incremento en cuanto a incidentes de ransomware.

Víctimas de ransomware por países durante el segundo semestre de 2022.



LOCKBIT 3.0

Desde el lanzamiento de la versión 3.0 del ransomware en junio de 2022, los operadores detrás de LockBit han empleado novedosas tácticas, técnicas y procedimientos (TTP) en sus ataques desplegados durante el segundo semestre.

Una vez que LockBit cifra los archivos de las víctimas, la nueva versión 3.0 del ransomware cambia el fondo de pantalla de los equipos infectados al color negro (LockBit Black), dejando un archivo denominado [texto_aleatorio].README.txt con las instrucciones para proceder al pago del rescate.

En septiembre, LockBit fue víctima de una filtración del builder de LockBit 3.0, por parte de un presunto afiliado del grupo.

El builder filtrado consta de cuatro archivos, un generador de claves de cifrado, un builder, un archivo por lotes para construir todos los archivos y un archivo de configuración modificable que permite que cualquiera pueda personalizarlo y modificar la nota de rescate para crear una nueva infraestructura.

La filtración supone un posible aumento de actores de amenazas que puedan emplear el builder para lanzar sus propias operaciones y ataques de ransomware, como en el caso de BlOODy Ransomware Gang, a quien se le ha observado utilizando el builder para crear el cifrador de BlOOdy en un ataque dirigido a una organización ucraniana en septiembre.

BLACKCAT (ALPHV)

Durante el segundo semestre, se ha observado que el grupo de amenazas ransomware emplea en sus ataques la herramienta BruteRatel para la etapa de intrusión, junto con otras herramientas comerciales de acceso remoto como AnyDesk y TeamViewer, además de la herramienta de código abierto llamada nGrok. BlackCat (ALPHV), que se caracteriza por la explotación de firewalls y VPN sin parches en los sistemas internos, junto con el uso de vulnerabilidades ya conocidas.

BLACK BASTA

Es otro de los grupos de amenazas más activo durante la segunda mitad de 2022. Descubierto en abril de este año, se dirige a organizaciones de todo el mundo. El ransomware Black Basta está escrito en C++ y es multiplataforma, ya que se dirige a sistemas operativos Windows y Linux a través de una variante de VMware ESXi dirigida a máquinas virtuales que se ejecutan en servidores Linux.

A pesar de que Black Basta mostraba un código novedoso, compartía algunas similitudes con el ransomware Conti y, en noviembre, la operación lanzó su nueva versión Black Basta 2.0 con algunas actualizaciones en lo relativo a sus algoritmos de cifrado de archivos a través de la Biblioteca aritmética de precisión múltiple (GMP) de GNU, la biblioteca de cifrado Crypto++, la introducción de la ofuscación de cadenas basada en la pila y las extensiones de archivo por víctima.

Una vez que Black Basta 2.0 cifra los archivos de las víctimas, cambia los nombres de archivos agregándoles la extensión codificada por víctima como .agnkdbd5y, .taovhsr3u o .tcw9lnz6q, a diferencia de la versión anterior del ransomware que utilizaba .basta como extensión del archivo encriptado.

La imagen del icono de los archivos de rescate que han sido cifrados por el ransomware también ha pasado de ser un cuadro blanco a un cuadro rojo.

En cuanto a la nota de rescate Black Basta 2.0, ha modificado el nombre y contenido de su texto (anteriormente se llamaba readme.txt y ahora pasa a ser instrucciones_read_me.txt), que se abre en el Bloc de notas de Windows mediante el comando cmd.exe /c start /MAX notepad.exe.

Asimismo, Black Basta 2.0 ya no implementa el cambio del fondo de pantalla del escritorio de la víctima, ni finaliza los procesos y servicios que pueden interferir con el cifrado de archivos.

TIPS UTILIZADAS

Los grupos de ransomware han evolucionado en cuanto al empleo de nuevas tácticas, técnicas y procedimientos en sus operaciones, destacando el uso por parte de Black Basta del nuevo método de evasión de las detecciones que consiste en la técnica conocida como "cifrado intermitente", que permite el cifrado de los sistemas de manera más rápida, cifrando solo partes del contenido de los archivos y haciendo que los datos sean irrecuperables sin el uso de la clave de descifrado. La técnica también reduce las posibilidades de detección de los ataques. A principios de octubre, los investigadores hallaron evidencias de la funcionalidad de wiper añadida a una herramienta utilizada anteriormente para la exfiltración de datos empleada por los operadores de ransomware. Las evidencias apuntan a una posible versión de Exmatter, una herramienta de exfiltración de datos asociada a las intrusiones del ransomware BlackCat, que destaca en este período por el uso del troyano bancario QakBot empleado como punto de entrada inicial y payload para el movimiento lateral, además del empleo del método de persistencia basado en el secuestro de un servicio legítimo borrándolo y volviendo a crear un nuevo servicio malicioso con el mismo nombre.

CONFLICTO UCRANIA V V

2022 ha estado marcado por la invasión rusa a Ucrania, un conflicto que ha pasado del terreno físico al cibernético y que ha supuesto un aumento de los ciberataques no solo en los países contendientes, sino a nivel global.

En el primer semestre de 2022, se observaron ataques como el atribuido a la APT Sandworm contra una empresa proveedora de energía de Ucrania mediante la utilización del malware Industroyer o la utilización de distintos malware destructivos de tipo wiper contra organizaciones ucranianas.

Esta tipología de ataques se ha mantenido durante todo el 2022, observándose en total al menos siete cepas de wiper en ataques por parte de actores supuestamente vinculados con el gobierno ruso.

03

El Servicio de Seguridad de Ucrania asegura que los ciberataques dirigidos contra el país se han triplicado en 2022 con respecto a años anteriores.

Los objetivos de estos ataques son los sectores de infraestructuras críticas, como energía, comunicaciones, logística, militar y bases de datos gubernamentales, principalmente. Durante el mes de diciembre de 2022, el sector energético ha sido el más afectado por ciberataques.

Los gobiernos de los países occidentales aliados de Ucrania también se han visto afectados por una intensificación de los ciberataques.

De acuerdo con Microsoft, los servicios de inteligencia rusos han mostrado esfuerzos de intrusión en las redes de 128 objetivos de 42 países diferentes.

La mayoría de estos ataques tienen como objetivo obtener información sensible de agencias gubernamentales de los países con un rol importante en la OTAN, por lo que sus objetivos suelen ser entidades públicas.

El Consejo de la Unión Europea publicó un aviso de los riesgos de ciberataques relacionados con la guerra de Ucrania a los países europeos a manos de los actores del conflicto entre Rusia y Ucrania.

Durante este conflicto, los ciberataques más comunes buscaban destruir datos y sistemas, interrumpir el funcionamiento de infraestructuras críticas y exfiltrar un volumen significativo de datos.

HACKTIVISMO EN EL CONFLICTO UCRANIA

El panorama hacktivista se ha visto alterado desde el inicio de la guerra de Ucrania, con la participación de colectivos denominados prorrusos y proucranianos

Esta alteración ha tenido una afectación no solo en los países envueltos directamente en el conflicto militar (Rusia y Ucrania), sino que Estados pertenecientes a la OTAN también han sufrido las consecuencias de ciberataques, de diversa magnitud, contra sus organismos y entidades de Defensa.

TIPOLOGÍA DE LOS CIBERATAQUES

En su mayoría, son DDoS e intrusión para recopilar información sensible, aunque no se han detectado mayores acciones por parte de grupos hacktivistas que hayan podido causar graves daños informáticos a las redes de diferentes organizaciones.

Los grupos prorrusos más reconocidos durante los últimos 6 meses han sido NoName057(16), KillNet, Anonymous Russia, Cyber Army of Russia y XakNet Team. Grupos proucranianos también se han movilizado bajo operaciones hacktivistas, destacando IT Army of Ukraine, Studen Cyber Army, AnonGhOst, Belarusian Cyber-Partisans y NB65. Se identifican ciberataques contra entidades militares rusas y fábricas de drones, plataformas de voluntarios (Dobro), tiendas militares y armamento (Arsenal Army, Kapterka), así como empresas logísticas de transporte militar (Dostavka-Krym).

S21SEC Cyber Solutions by Thales

KILLNET

Principal grupo de hackers prorrusos. Ha llevado a cabo múltiples ciberataques tanto hacia Ucrania como a todo aquel país que se posicionase a su favor.

- Este grupo surgió a raíz de la invasión rusa a Ucrania y se cree que está patrocinado por el propio gobierno de Rusia, aunque también podrían estar motivados financieramente.
- En su mayoría se han tratado de ataques DDoS, su especialidad, contra objetivos no combatientes de todo el mundo percibidos como hostiles al gobierno ruso, para presionarlos.
- En julio de 2022, realizó un ataque de DDoS contra el dominio americano congress.gov, el cual afectó brevemente al acceso público.
- En agosto, KillNet atacó a la empresa de industria aeroespacial estadounidense Lockheed Martin, de nuevo mediante DDoS y a su vez robó datos de empleados de la empresa.
- En noviembre, la web del Parlamento Europeo fue víctima de un ciberataque llevado a cabo por KillNet, poco después de que se aprobara una resolución en la que se denominaba a Rusia "Estado patrocinador del terrorismo".

SECTOR FINANCIERO

Los procesos de digitalización han llevado a que el sector financiero se encuentre en los últimos años entre una de las industrias más atacadas por parte de los cibercriminales, especialmente por parte de aquellos cuyo interés principal se basa en conseguir un beneficio económico.

Los ataques más comunes dirigidos a empresas del sector financiero se tratan principalmente de ransomware, acceso no autorizado a los servidores y robo de datos.

04

Los infostealers más activos en los últimos seis meses a nivel mundial han sido Formbook, Agent Tesla, Raccoon Stealer, Lokibot y Vidar.

En este sentido, en el último semestre de 2022 se ha observado un aumento de los ataques a empresas del sector financiero por parte de los denominados infostealers, programas maliciosos diseñados para robar información del equipo de la víctima, como credenciales de inicio de sesión, nombres de usuario, credenciales del portapapeles y cookies, y obtener 2FA o credenciales almacenadas en los navegadores.

Una vez que obtiene esta información, la extrae a un servidor de comando y control bajo la infraestructura del ciberdelincuente, donde recibe toda esta información.

AGENT TESLA

Agent Tesla es un RAT (Remote Access Trojan) e infostealer distribuido como Malware-as-a-Service (MaaS). Desde su aparición en 2014, este RAT ha seguido adaptándose para continuar robando credenciales y datos de sus víctimas como cookies o pulsaciones del teclado.

El vector de entrada más frecuente de Agent Tesla se trata de correos de phishing que contienen un fichero malicioso adjunto. Cuando el usuario descarga y ejecuta este fichero se inicia la infección.
En los últimos seis meses se han observado campañas en las que el malware Agent Tesla se está utilizando para distribuir el malware Nanocore.

RACOON STEALER

La primera versión de Raccoon Stealer se vendía como un MaaS (Malware-as-a-Service) en foros underground a principios de 2019, estaba escrita en C++ y su precio rondaba los 75 $ por semana o 200 $ al mes, lo que le ayudó a hacerse popular entre el resto.

A principios de julio de 2022 se empezó a observar una nueva versión de esta familia. A diferencia de la versión antigua, esta nueva versión está escrita en C y ensamblador.

Este stealer es capaz de obtener información del equipo infectado, como contraseñas, cookies, información de autocompletado e información de carteras de criptomonedas.

En los últimos seis meses, las tendencias observadas dentro del panorama de amenazas en relación con un compromiso previo, se ha advertido que los cibercriminales continúan generando ingresos a partir del desarrollo o la venta de familias de malware o botnets que incorporan la funcionalidad de registro de teclas para robar información de interés, aprovechando múltiples vectores de ataque para robar información de instituciones financieras y ejecutar transferencias bancarias fraudulentas.

EMOTET

Emotet ha sido una de las redes de bots más populares en los últimos tiempos y en el segundo semestre de 2022 se ha observado un aumento de la actividad de la misma en comparación con el primer semestre.

En estos meses se han observado múltiples campañas de esta botnet dirigidas a países de todo el mundo utilizando una nueva variante del malware que tiene capacidades de robo de tarjetas de crédito y se dirige también al robo de datos del navegador Chrome.

FAUPPOD

Fauppod es un malware muy ofuscado que también se utiliza para propagar FakeUpdates y escribe Raspberry Robin en unidades USB.

El 27 de julio de 2022, Microsoft identificó algunas muestras detectadas como Fauppod, que tenían árboles de proceso similares a la infección LNK de Raspberry Robin, con archivos DLL escritos en ubicaciones similares y usando convenciones de nomenclatura similares.

Su cadena de infección también liberaba el malware FakeUpdate. Sin embargo, las víctimas que expusieron estas muestras no tenían el vector de infección de archivos LNK tradicional lanzado desde una unidad USB infectada.

QAKBOT

QakBot, también conocido como QBot o Pinkslipbot, es un troyano bancario utilizado principalmente para robar los datos financieros de las víctimas, incluida la información del navegador, las pulsaciones del teclado y las credenciales.

- Una vez que QakBot ha infectado con éxito un entorno, el malware instala una puerta trasera que permite al autor de la amenaza lanzar malware adicional, como ransomware.

- Se entrega a través de campañas de phishing y luego se ejecuta en la memoria.

- QakBot tiene múltiples módulos para ayudar a monetizar sus intrusiones, incluida la propagación, las inyecciones web, la recolección de correo electrónico y otros robos de datos.

- En las últimas campañas se ha observado a actores utilizando QakBot para obtener acceso inicial a un sistema y posteriormente moverse lateralmente dentro de la red de una organización y desplegar el ransomware Black Basta.

- Durante este semestre se ha observado una nueva amenaza a empresas del sector financiero que se propaga a través de USB, llamada Raspberry Robin, que se ha detectado a su vez en conjunto con el malware Fauppod.

RASPBERRY ROBIN

Raspberry Robin es un ransomware con funcionalidades de gusano que se propaga a través de dispositivos USB infectados, y fue detectado por primera vez en septiembre de 2022.

Microsoft afirma que se ha encontrado este gusano de Windows recientemente detectado en las redes de cientos de organizaciones de diversos sectores industriales alrededor del mundo.

Este malware utilizaba dispositivos NAS de QNAP como servidores de comando y control a principios de noviembre.

Los dispositivos USB infectados suelen contener archivos .LNK que, tras ser ejecutados por el usuario de forma inconsciente, descargan otros archivos, como instaladores MSI, mediante el uso de msiexec.exe para contactar con sus servidores de control.

MALWARE MÓVIL

Los teléfonos móviles continúan siendo uno de los objetivos principales de los cibercriminales en este segundo semestre de 2022, habiéndose encontrado numerosas familias de malware que se dirigen contra los sistemas operativos más comunes como Android e IOS.

A pesar de las medidas de seguridad de fabricantes en los mercados oficiales como la PlayStore de Google, los cibercriminales siguen encontrando nuevas formas para introducir malware en dichos mercados, lo que les facilitará obtener miles de descargas. No obstante, también existen otras formas de distribución de esta amenaza, por ejemplo a través de la utilización de anuncios o el uso páginas web que suplantan a empresas legítimas, en las que se engaña al usuario para que descargue el malware.

Generalmente los desarrolladores de malware móvil buscan un beneficio económico, ya que suele diseñarse para el robo de credenciales bancarias cuando un individuo accede a su aplicación bancaria desde el dispositivo infectado.

05

MALIBOT

Se trata de un troyano bancario para Android descubierto en 2022 durante la investigación de otra familia de malware que ha estado muy activa en los últimos años, llamada FluBot.

Los desarrolladores de este malware camuflan la aplicación maliciosa haciéndose pasar por aplicaciones legítimas como Mining X o TheCryptoApp, MySocialSecurity o Chrome.

Las víctimas infectadas parecen haber sido atraídas a webs fraudulentas donde se les engaña para que descarguen el malware en sus dispositivos. Además, los atacantes envían de forma masiva mensajes SMS a todos los contactos del usuario infectado para distribuir la página fraudulenta y conseguir más descargas.

Una vez infectado un dispositivo, tiene la capacidad de realizar ataques de overlay, superponiendo una web phishing durante el proceso de autenticación de una aplicación para llevar a cabo el robo de credenciales. En este caso, el malware se centra en el robo de credenciales bancarias.

THE GODFATHER

A finales de 2022 apareció un nuevo troyano bancario de Android que se dirigía contra más de 400 entidades bancarias de todo el mundo, pero en la mayoría de las aplicaciones bancarias.

Su objetivo se encuentra en Estados Unidos (49), Turquía (31), España (30), Canadá (22), Francia (20), Alemania (19) y Reino Unido (17).

El malware se distribuye a través del mercado de aplicaciones de Google y, una vez instalado, simula ser Google Protect y escanear el dispositivo.

El malware pide acceso a los permisos de accesibilidad, lo que le aporta total control sobre el dispositivo.

De esta manera, genera notificaciones falsas de aplicaciones bancarias que se encuentren instaladas en el dispositivo de la víctima para llevarla a una página de phishing, y no tener que esperar así a que la víctima tenga que abrir activamente la aplicación.

06 SECTOR ENERGÉTICO

Las amenazas cibernéticas dirigidas al sector energético durante el segundo semestre de 2022 han incluido operaciones patrocinadas por estados, lleva das a cabo por grupos de amenazas persistentes avanzadas (APT), entre los que destacan la República Popular China y la Federación Rusa, junto con amenazas procedentes de grupos y actores hacktivistas que han ejecutado ataques de denegación de servicios, intrusiones y filtraciones de datos ma sivas de empresas e instituciones pertenecientes al sector.

Durante la segunda mitad de año, se ha apreciado un incremento de las ciberamenazas, especialmente en lo que se refiere a los ataques ransomware dirigidos contra este tipo de infraestructuras, procedentes de diversas familias de ransomware como LockBit, BlackCat (ALPHV), Hive, Daixin, Ragnar Locker, Everest, Lorenz, Industrial Spy, Snatch, BianLian, Royal, Quantum, Vice Society, Play o Cuba.

La focalización de los actores de amenazas ha apuntado principalmente a empresas pertenecientes a todas las verticales del sector, especializadas en servicios de energía eléctrica, solar, gas natural o compañías petroleras.

En agosto y septiembre de 2022 se registró una oleada de ciberataques dirigidos contra empresas y organismos pertenecientes al sector energético italiano reivindicados por la familia de ransomware BlackCat (ALPHV). Entre sus víctimas estaban el organismo Gestore Dei Servizi Energetici (GSE S.p.A.), la multinacional petrolera italiana, Eni SpA, y el Grupo Canarbino, que opera en el sector del gas y la electricidad.

Destacan las campañas de malware llevadas a cabo por el grupo Lazarus (también conocido como Hidden Cobra o ATP38), patrocinado por Corea del Norte y dirigido a los proveedores de energía de Estados Unidos, Canadá y Japón, con el objetivo de infiltrarse para establecer permanencia en las redes y realizar operaciones de espionaje en apoyo de los objetivos del gobierno de Corea del Norte.

Debido a la crisis energética mundial a raíz del conflicto militar de Rusia en Ucrania, los actores de amenazas han estado aprovechando la temática para dirigirse a los consumidores en campañas de phishing, como la registrada en septiembre en la que se suplantaba a organismos reguladores británicos a través de correos electrónicos maliciosos y mensajes de texto SMS, con la finalidad de engañar a las víctimas a que obtengan un presunto descuento en sus facturas de energía para el robo de datos personales.

GRUPOS DE HACKTIVISTAS

En el marco de la invasión militar de Rusia en Ucrania iniciada en febrero de 2022 que marcó el inicio de un panorama de ciberamenazas sin precedentes para el sector, la actividad cibernética existente se ha mantenido junto con la preocupación por parte del resto de países aliados a Ucrania.

Mientras que durante el primer semestre del año pasado se registraron importantes ataques como el dirigido a las redes de comunicación satelital internacional y de Estados Unidos (SATCOM), la segunda mitad de 2022 ha estado marcada por las fugas registradas en infraestructura crítica de los gaseoductos Nord Stream propiedad de Gazprom, una empresa energética estatal rusa.

Dada la evolución del panorama geopolítico tras el inicio del conflicto bélico, existe una alta probabilidad de que Rusia utilice la amenaza de cortes en el suministro de gas, tal y como ocurrió en junio de 2014, para aumentar su influencia sobre el resto de países europeos que dependen energéticamente de este.

ATAQUES DE DENEGACIÓN DISTRIBUIDA DE SERVICIO (DDoS)

De entre los grupos y actores de amenazas más destacados se encuentran KillNet, Xaknet o Cyber Army of Russia.

Los ataques de denegación distribuida de servicio (DDoS) han interrumpido servicios y sus sitios web de diversas entidades del sector, además de compañías de distribución de electricidad y gas de países como Ucrania, entre cuyas víctimas se encuentran el proveedor de electricidad ucraniano, la mayor empresa productora de petróleo del país, el mayor productor de electricidad y operador de las centrales nucleares, además de la compañía distribuidora de electricidad y gas lituana.

BRECHAS DE DATOS

Destaca a principios de noviembre una empresa comercializadora de energía eléctrica española, que fue víctima de un incidente cibernético a raíz de un acceso no autorizado en sus sistemas de TI, tras el cual se vio comprometida información sensible de un número limitado de clientes de la compañía.

SECTOR DEFENSA

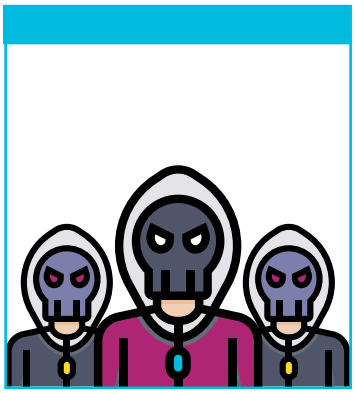
A raíz del conflicto militar entre Rusia y Ucrania, diversos actores de amenazas han proyectado sus acciones, traducidas en ciberataques, a la industria de defensa.

En los últimos 6 meses actores de amenazas de diversa índole han protagonizado acciones cibernéticas que han tenido impacto en la industria de defensa, incluyéndose organismos estatales, empresas de defensa y activos tecnológicos militares, entre otros.

07

Al mencionar a los actores de amenazas responsables de dichos ciberataques hay que identificar su naturaleza, objetivos y motivaciones.

Durante este último semestre se ha identificado la participación de los siguientes grupos de actores de amenazas en operaciones contra la industria de defensa:



Grupos de cibercriminales organizados

Grupos hacktivistas

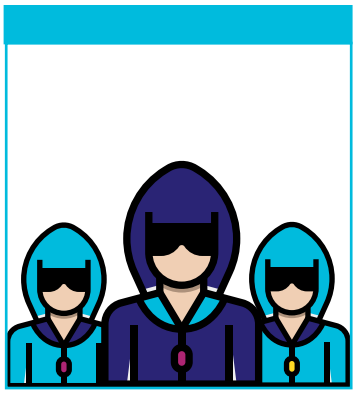
Amenazas persistentes avanzadas

Dentro de los denominados grupos cibercriminales organizados se incluyen tanto grupos ransomware como grupos o individuos con menores capacidades operativas pero con un impacto muy relevante para la entidad objetivo.

- En el primero de los casos, los grupos ransomware desde el inicio del conflicto ruso-ucraniano han dirigido su actividad contra el sector de defensa, afectando principalmente a empresas del sector.

- El posicionamiento de algunos grupos ransomware en el conflicto y la tensión internacional y regional surgida a raíz del mismo ha creado un escenario donde los ciberataques ransomware se han convertido en una de las mayores amenazas para empresas y organismos del sector. Entre los ransomware más relevantes y con mayor actividad se encuentran LockBit 3.0, BlackCat (ALPHV) y Black Basta.

Grupos de cibercriminales organizados



Grupos hacktivistas

Amenazas persistentes avanzadas

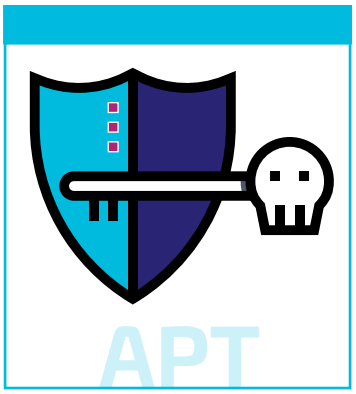
De entre estos grupos, fuera del conflicto entre Rusia y Ucrania destaca la agrupación denominada Guacamaya, cuya actividad se ha centrado en Latinoamérica y contra empresas u objetivos del sector de la Defensa.

Entre sus ataques se encuentra los realizados contra las páginas web y servidores de las Fuerzas Armadas de Chile, Perú, Colombia, El Salvador y México, a través de la explotación de vulnerabilidades en Exchange y Zimbra.

El grupo Adrastea también se ha convertido en una de las principales amenazas del sector en el segundo semestre de 2022 tras su ataque a una compañía europea de manufactura de misiles. Tras el ataque, el grupo consiguió exfiltrar información confidencial de proyectos de la compañía, y publicó parte de la información en foros underground.

Grupos de cibercriminales organizados

Grupos hacktivistas



Amenazas persistentes avanzadas

Los grupos APT son una de las ciberamenazas con mayor nivel de criticidad, con altas capacidades de actuación e infección y un constante proceso de actualización de sus Tácticas, Técnicas y Procedimientos (TTP).

El patrocinio que reciben de sus Estados de origen y su involucración con agencias de seguridad e inteligencia de éstos, crea un escenario donde las APT siguen unas líneas de actuación con ciberataques de alto nivel a entidades y organismos críticas, como a las del sector de Defensa.

La situación actual a nivel internacional y nacional ha dado lugar a que numerosos grupos APT realicen operaciones de diversa índole contra objetivos militares y de Defensa.

Dichas operaciones están basadas en ciberataques con malware destructivo (los denominados wipers), en campañas de ciberespionaje y en la inyección de malware para robar información o mantener persistencia con el objetivo de identificar posibles vulnerabilidades.

En agosto de 2022 se publicaron varias noticias sobre el "posible hackeo" de los sistemas de lanzamiento de misiles HIMARS operados en Ucrania, derivándose de una operación conjunta entre grupos hacktivistas prorrusos y un grupo del Gobierno ruso no identificado.

Durante el verano de 2022 y hasta septiembre del mismo año, el grupo norcoreano APT 37 (AKA Konni) lanzó una campaña de spear phishing denominada STEEP#MAVERICK, contra empresas de armamento y defensa en Estados Unidos y Europa.

Entre las amenazas más relevantes dentro de los grupos APT, destaca el grupo Gamaredon, que se ha centrado durante los últimos 6 meses en realizar acciones de ciberespionaje contra entidades del sector de defensa de la Unión Europea y Ucrania.

SECTOR SANITARIO

VVVVV

Los cibercriminales mantienen una actividad muy elevada contra el sector sanitario. En los últimos años, se han observado altos índices de ciberataques y acciones disruptivas contra los sistemas informáticos de hospitales, centros sanitarios, proveedores de material médico y clínicas privadas, entre otros organismos del sector.

Esta tendencia se ha mantenido durante segundo semestre de 2022. Durante los seis meses de análisis presentados en este documento se han identificado diversos tipos de ciberataques y actores implicados.

08

RANSOMWARE

Por un lado, el ransomware se mantiene como una de las amenazas más graves y que mayor riesgo presentan para el sector sanitario. Sus consecuencias han resultado en la paralización de servicios, cancelación de operaciones y desconexión de aparatos médicos de monitorización y gestión.

Durante el segundo semestre, operadores de diversos grupos ransomware han puesto entre sus objetivos a centros médicos y proveedores de material para uso médico, destacando el ataque de Karakurt en julio contra un grupo hospitalario de Estados Unidos y el ataque por parte de los operadores del ransomware Sparta en septiembre contra una compañía especializada en proveer tecnología de radiofrecuencia para uso médico.

Además, entre septiembre y diciembre, varios centros hospitalarios de Francia se vieron afectados por ataques ransomware de diversa consideración, teniendo impacto en el hospitales y compañías proveedoras de servicios médicos.

Además, se resalta la participación de grupos ransomware Daixin y Royal por su supuesta participación en ciberataques contra organizaciones sanitarias, principalmente en Estados Unidos.

BRECHAS DE DATOS

Durante el segundo semestre, las brechas de datos en el sector sanitario han mantenido su tendencia, principalmente a la alza.

Dichas brechas de datos se dieron a raíz de algunos de los ciberataques previamente ocurridos, donde los ciberdelincuentes pudieron obtener datos para su venta o su uso malicioso en campañas de phishing.

Ante la distribución de ciberataques a nivel global contra el sector sanitario por parte de grupos cibercriminales de diversa especialización y grupos APT, se estima probable que durante los próximos seis meses la tendencia de ciberincidentes relacionados se mantenga constante, pudiendo aumentar contra empresas de la cadena de suministro.

Asimismo, no se descarta una mayor explotación de vulnerabilidades por parte de actores de amenazas, como las APT, pudiendo tener impacto en el sector.

GRUPOS APT

Por otro lado, las amenazas de grupos APT han llamado la atención de agencias gubernamentales nacionales e internacionales por su supuesta participación en ciberataques contra centros hospitalarios y compañías proveedoras de servicios a dichos centros.

En este caso, desde la Agencia de Seguridad en Ciberseguridad e Infraestructuras de Estados Unidos (CISA), así como desde el Centro de Coordinación de Ciberseguridad del Sector Sanitario de Estados Unidos se advirtió sobre las diferentes acciones que estaban llevando a cabo grupos APT, en conjunto con grupos Ransomware, teniendo impacto en el sector sanitario.

A través de comunicados de dichas agencias, así como de la actividad analizada de grupos APT, se han detectado varios grupos/colectivos de interés:

- Grupos APT de Corea del Norte, con capacidad para robar información en el campo sanitario y obtener datos.
- APT41, por su actividad contra sistemas de diagnóstico y centros hospitalarios en diferentes países.
- Mustang Panda, APT10 y Winnti, por su uso de malware especializado y desarrollado por estos grupos para dirigirlo contra entidades del sector sanitario y centros de investigación en dicho campo.

09

El sector de producción industrial ha sido el sector más atacado por grupos de ransomware durante el segundo semestre del año 2022, con un incremento del 34 % respeto a la primera mitad del año.

SECTOR INDUSTRIAL

Durante la segunda mitad del año 2022, los sistemas de control industrial (ICS) y la tecnología operativa (OT), encargados de supervisar y controlar los dispositivos y procesos de los sistemas operativos físicos, han presentado diferentes vulnerabilidades que permitían a los ciberdelincuentes tomar el control de los mismos o acceder a ellos para obtener información sensible de las empresas.

Algunos de los acontecimientos más relevantes durante este periodo en el sector industrial han sido:

01 La vulnerabilidad conocida como AttachMe, una vulnerabilidad de aislamiento de la nube en Oracle Cloud Infraestructure (OCI) que permitía a los atacantes realizar diferentes actos destructivos como obtener y filtrar datos confidenciales o alterar el código y escalar privilegios.

02 La vulnerabilidad conocida como CVE-2022-38465 en el controlador lógico programable (PLC) de Siemens Simatic, que permitía a los atacantes recuperar las claves criptográficas privadas globales codificadas y tomar el control de los dispositivos.

03 Vulnerabilidades críticas en R-SeeNet de Advantech: las vulnerabilidades identificadas como CVE-2022-3386 y CVE-2022-3385 permitían a los atacantes eliminar archivos en el sistema de forma remota o ejecutar de forma remota código en las versiones afectadas. Dichas vulnerabilidades afectaban a sectores de infraestructura crítica como sistemas críticos de fabricación, energía, agua y aguas residuales en todo el mundo.

04 Vulnerabilidades F5 en productos BIG-IQ y BIG-IP: En el mes de noviembre, la compañía F5 Networks publicó un aviso sobre dos vulnerabilidades que afectaban a varios de sus productos como los dispositivos de red BIG-IP y BIG-IQ, que podrían provocar la ejecucuón remota de código.

05 En diciembre se publicó una herramienta conocida como Simantic-Smackdown, que permitía interrumpir las operaciones de los controladores lógicos programables (PLC) SIMATIC S7 a través del envío de una señal que apagaba la unidad central de procesamiento (CPU) del PLC.

10

HACKTIVISMO

El hacktivismo se refiere a la acción de un individuo o un grupo que abusa de una red o una aplicación web con en aras de promover una causa social o política. Los ataques por parte de grupos se basan generalmente en la realización de ataques de denegación de servicio, de defacement, o la filtración de datos.

Durante los últimos años, se ha observado una reducción de los ataques de tipo hacktivistas dirigidos contra empresas, ya que los actores centraban su actividad contra entidades gubernamentales o incluso contra individuos concretos.

Sin embargo, en el segundo semestre de 2022 se ha producido un aumento de las acciones hacktivistas alrededor del mundo dirigidas contra empresas, como ha ocurrido en el caso de los actores hacktivistas que participan en la guerra de Ucrania, pero también han aparecido grupos en otras localizaciones geográficas cuyas acciones han tenido un gran impacto.

GUACAMAYA

Guacamaya es un grupo hacktivista que ha estado activo desde al menos marzo de 2022, cuyos miembros han llevado a cabo operaciones cibernéticas basadas principalmente en la filtración de datos.

Su nombre original, o por el cual se dieron a conocer en su primera filtración, es Guacamaya roja, un ave característica de Centro América. La motivación de sus ataques apunta a una ideología claramente marcada por conceptos ecologistas anticapitalistas.

Según el grupo, las razones por las que ejecutan sus ataques van desde la injusticia en general, los delitos criminales contra la población y el territorio, el sistema y las multinacionales, considerando que la lucha de un territorio es la defensa de la vida, la especie humana y seres vivos que habitan el planeta.

Según los ataques observados del grupo, sus objetivos se localizan en América del Norte (México), América Central (Guatemala, El Salvador) y América del Sur (Venezuela, Colombia, Brasil, Chile, Perú y Ecuador).

GHOSTSEC

Ghostsec es un grupo hacktivista que lleva activo desde el año 2015 y se formó para la realización de ataques hacktivistas contra organizaciones terroristas, realizando ataques de doxing (publicación de información personal) de afiliados a Daesh, Boko Haram o a Al-Qaeda.
Si bien el grupo comenzó teniendo estos objetivos, en los últimos años ha cambiado su agenda política y se muestra crítico contra los gobiernos de Israel e Irán, países a los que ha dirigido la mayor parte de su actividad en el último semestre.

En septiembre, el grupo anunciaba haber comprometido 55 controladores lógicos programables (PLC) Berghof utilizados por organizaciones israelíes, como parte de una campaña hacktivista denominada #FreePalestine.

Tras el fallecimiento de Mahsa Amini y las protestas derivadas por este hecho, los integrantes de Ghostsec han realizado múltiples ataques contra el país islámico, llegando a proclamar haber accedido a sistemas industriales y gubernamentales.

El grupo también ha apoyado a otras causas hacktivistas como la #OpNicaragua y la #OPRussia, contra el gobierno nicaragüense y en apoyo a Ucrania.

11 APTs

Este tipo de ataques son llevados a cabo por actores con patrocinio estatal o nacional con el fin de realizar tareas de espionaje o sabotaje contra organizaciones que supongan una competición (estratégica o política) contra los intereses del patrocinador.

APT COREANAS

En el segundo semestre de 2022, se ha registrado una gran actividad de grupos de amenazas persistentes avanzadas de origen coreano, especialmente ciberataques de grupos APT norcoreanos dirigidos a Corea del Sur, destacando, principalmente, los grupos Lazarus, Kimsuky y APT37.

LAZARUS GROUP

También conocido como Guardians of Peace o Whois Team, es el grupo APT de origen norcoreano más activo del segundo semestre de 2022. Se trata de un grupo de amenazas persistentes avanzadas financiado por la inteligencia militar de Corea del Norte que cuenta con numerosos subgrupos, como AndAriel y BlueNorOff.

Se ha observado a Lazarus explotando una vulnerabilidad Log4j en VMWare Horizont con la finalidad de obtener un punto de apoyo inicial en las organizaciones objetivo, muchas de las cuales pertenecían al sector energético de Estados Unidos, Canadá y Japón.

La explotación exitosa de esta vulnerabilidad permite la implementación de malware personalizado por el grupo de amenazas, como la backdoor VSingle, el malware YamaBot, o MagicRAT, un implante de malware previamente desconocido.

En este periodo de tiempo, Microsoft ha informado que Lazarus emplea software legítimo de código abierto (PuTTY, KiTTY, TightVNC, Sumatra PDF Reader y el instalador de software muPDF/-Subliminal Recording) para dirigirse a sus objetivos a través de la backdoor BLINDINGCAN, conocida como ZetaNIle, en ataques de ingeniería social dirigidos a ingenieros y profesionales de soporte técnico que trabajaban en organizaciones de TI y medios de comunicación en Reino Unido, India y EE. UU.

Los subgrupos de Lazarus también han estado activos en los últimos seis meses de 2022.
A mediados de agosto, se descubrió un nuevo ransomware denominado Maui atribuido al subgrupo de Lazarus llamado AndAriel. Este subgrupo, activo desde al menos 2015, habría utilizado este ransomware desde abril de 2021 para dirigir ciberataques a empresas surcoreanas de los sectores de la construcción, manufactura y medios de comunicación, así como a empresas proveedoras de servicios de red.

No se trata del único ransomware detectado en este periodo con afectación a Corea del Sur; en agosto de 2022, se detectó un nuevo ransomware denominado GwisinLocker, utilizado por actores de amenazas para encriptar servidores Linux ESXi y Windows de únicamente empresas surcoreanas. No ha sido aún asignado a ningún grupo APT conocido, aunque todo apunta a que se trata de una herramienta fabricada por un grupo de amenazas persistentes avanzadas de origen norcoreano.

Por otra parte, en diciembre de 2022 se detectó una campaña de phishing dirigida a empleados de startups atribuida al subgrupo BlueNorOff de Lazarus, para la cual habrían creado más de 70 dominios falsos imitando a bancos conocidos y firmas de capital de riesgo de origen japonés, vietnamita y estadounidense.

KIMSUKY

Kimsuky, también conocido como Thallium, Black Banshee o Velvet Chollima, es un grupo de amenazas persistentes avanzadas de origen norcoreano activo desde, al menos, el año 2012.

Durante este periodo, se ha atribuido a este grupo APT la campaña de phishing conocida como Gold-Dragon, que tuvo lugar a principios de 2022, en la que se dirigían ciberataques a entidades políticas y diplomáticas ubicadas en Corea del Sur para implementar una backdoor de Windows para el robo de información (listas de archivos, pulsaciones de teclas del usuario y credenciales de inicio de sesión del navegador web almacenadas).

Por otra parte, se ha observado al grupo utilizando tres cepas diferentes de malware de Android denominadas FastFire, FastViewer y FastSpy. El malware FastFire se disfraza como un complemento de seguridad de Google, FastViewer se oculta como Hancom Office Viewer y FastSpy es una herramienta de acceso remoto basada en AndroSpy.

Por último, se ha detectado una campaña de spear-phishing dirigida a más de 900 expertos surcoreanos en asuntos exteriores occidentales con la finalidad de obtener información sobre el posible movimiento de la política occidental hacia Corea del Norte. Los correos incluían un enlace a un sitio web falso y un archivo adjunto que provocaba la descarga de malware.

APT37

APT37, también conocido como Scarcruft o Reaper, es un grupo APT patrocinado por el estado de Corea del Norte que ha estado activo desde al menos el año 2012, fecha desde la cual este grupo ha dirigido ciberataques a Corea del Sur y a países localizados en Medio Oriente.

En octubre de 2022, este grupo de amenazas persistentes avanzadas dirigió una campaña de phishing a usuarios localizados en Corea del Sur utilizando archivos maliciosos que explotaban una vulnerabilidad zero-day en el intérprete de JavaScript de Internet Explorer denominada CVE-2022-41128.

Utilizaban como nombre de archivo "221031 Seoul Yongsan Itaewon accident response situation (06:00).docx", aludiendo a la estampida de Halloween de Seúl. La vulnerabilidad fue parcheada por Microsoft en noviembre de 2022.

Asimismo, en noviembre de 2022 se detectó una campaña en la que APT37 utilizaba una backdoor denominada Dolphin para comprometer los sistemas de usuarios localizados en Corea del Sur con la finalidad de llevar a cabo espionaje cibernético.

APT RUSAS

Si bien el conflicto ruso-ucraniano ha sido uno de los responsables de que se haya visto incrementada la actividad de los grupos APT de origen ruso durante el segundo semestre de 2022, esta no es la única motivación de los grupos que han dirigido ciberataques en este periodo de tiempo. Destacan la actividad de los grupos APT28, APT29, TA505, Sandworm, FIN7 y UAC-0142.

APT28

Investigadores de la Agencia de Seguridad de Ciberseguridad e Infraestructura de Estados Unidos (CISA) descubrieron a finales de 2022 que el grupo de amenazas persistentes avanzadas denominado APT28, de origen ruso, estuvo infiltrado en los sistemas de una empresa estadounidense proveedora de comunicaciones por satélite.

Muchos de los clientes de la entidad afectada son empresas del sector de las infraestructuras críticas de los Estados Unidos, lo cual podría estar relacionado con las motivaciones de este grupo. La infiltración, que pasó desapercibida durante varios meses de 2022, pudo resultar en la exfiltración de datos confidenciales.

FIN7

En noviembre de 2022 se vinculó al grupo de amenazas persistentes avanzadas de origen ruso FIN7 con el ransomware denominado Black Basta, uno de los ransomwares más utilizados en el año 2022. Además, se ha observado que este grupo ha estado explotando vulnerabilidades de Microsoft Exchange para crear una plataforma denominada Checkmarks.

Este sistema de ataque escanea vulnerabilidades de Microsoft Exchange para descubrir puntos vulnerables dentro de las redes de sus potenciales víctimas que puedan ser explotados para obtener acceso a sus sistemas.

APT29

La APT29 agregó a mediados de 2022 a su arsenal de tácticas el uso de servicios de almacenamiento en la nube como Google Drive o DropBox para implementar malware en los sistemas comprometidos de sus objetivos.

Asimismo, en noviembre de 2022 se detectó un ataque de spear-phishing llevado a cabo por este grupo de amenazas persistentes avanzadas contra una entidad diplomática europea no identificada.
Para ello explotaron una función de Windows denominada Credential Roaming. Credential Roaming o Itinerancia de Credenciales es un mecanismo que permite a usuarios tener acceso a sus credenciales (privadas o certificados) de forma segura en diferentes estaciones de trabajo de un dominio de Windows.

Además, durante este periodo de tiempo se ha observado un nuevo malware utilizado por este grupo APT denominado MagicWeb, una evolución del malware FoggyWeb, que afecta al software de autenticación de Microsoft denominado Active Directory Federation Services (ACFS).

Sustituye una DLL legítima utilizada por ADFS por una versión maliciosa para manipular los certificados de autenticación de usuario y modificar las reclamaciones pasadas en los tokens generados por el servidor comprometido.

TA505

En este periodo de tiempo se han identificado dos botnets asociadas al grupo TA505, también conocido como Evil Corp. Estas botnets implementan malware como el troyano FlawedGrace, Cobalt Strike o el ransomware Clop y que han tenido impacto en entidades de todo el mundo, particularmente aquellas situadas en Estados Unidos, México, Pakistán y Brasil.

Asimismo, se han asociado nuevas tácticas al grupo, como el uso del malware Raspberry Robin, la explotación de la vulnerabilidad conocida como CVE-2022-31199 que afecta al software Netwrix Auditor, así como la utilización del panel de control de software TeslaGun, utilizado para implementar una puerta trasera denominada ServHelper.

SANDWORM

Este grupo APT, también conocido como Iridium, ha dirigido la mayoría de sus ciberataques en este periodo de tiempo a Ucrania.

En este semestre se ha observado que el grupo ha explotado la vulnerabilidad CVE-2022-30190, que afecta a la herramienta Microsoft Windows Support Diagnostic Tool (MSDT) para dirigir ciberataques a Ucrania.

Asimismo, han dirigido ciberataques de tipo ransomware a entidades del país haciendo uso de un nuevo ransomware denominado RansomBoggs, cuya nota de rescate hace referencia a la película de Pixar denominada Monsters, Inc (2001).

UAC-0142

Este grupo APT dirigió un ciberataque en diciembre de 2022 al Centro de Innovación y Desarrollo de Tecnologías de Defensa del Ministerio de Defensa de Ucrania.

El ataque consistió en el envío de un correo electrónico de spear phishing en el que se utilizaba una dirección de correo comprometida de un miembro del Ministerio de Defensa del país en el que se instaba al destinatario a actualizar los certificados del sistema DELTA, un software militar utilizado por el gobierno ucraniano.

En el correo venía adjunto un documento PDF y un archivo ZIP malicioso alojado en un dominio Delta falso que incluía dos archivos, denominados FateGrab y StealDeal, que recopilan y exfiltran datos de los sistemas comprometidos.

APT CHINAS

Los grupos APT con patrocinio de China o de origen chino se han posicionado en los últimos seis meses como uno de los colectivos con mayor actividad a nivel global, teniendo como objetivo labores de ciberespionaje e intrusión. Sus acciones dirigidas contra sectores estratégicos como el financiero, industrial, de telecomunicaciones, defensa, manufactura y gobierno hacen que sus ciberataques tengan mayor riesgo y graves consecuencias. En este sentido, la actividad durante los últimos seis meses de 2022 se ha centrado en tres grupos APT, APT41 y Mirror Face.

APT41

Este grupo mantiene una importante operatividad y suma nuevos subgrupos a su equipo de operadores, como Earth Longhzhi, Earth Baku, Grayfly y Blackfly.

Aunque por el momento no se han identificado nuevas campañas activas de la APT41, es muy probable que mantengan sus operaciones con campañas anteriores y a través de subgrupos.

MIRRORFACE

Esta APT puso en marcha una campaña de spear-phishing dirigida contra entidades y personalidades políticas enmarcada en la Operación LiberalFace.

Entre los objetivos de la campaña se encontraba el órgano electoral de la Cámara de Consejeros de Japón.

El uso de herramientas propias como MIrrorStealer crea un escenario de mayor riesgo por posibles robos de información y campañas de intrusión con objetivos de ciberespionaje.

12 TELCO

Durante este segundo semestre, se ha podido observar un gran número de ciberataques contra empresas de telecomunicaciones, así como un número elevado filtraciones de datos de clientes de grandes empresas de telecomunicaciones en países miembros de la Unión Europea como España o Portugal.

A principios del mes de septiembre, el usuario PoCExploiter, Admin (owner) del canal de Telegram del grupo de amenazas conocido como KelvinSecurity, informó que tenía en su poder y ponía a la venta 309 GB de datos de una empresa de telefonía de Italia que contenían alrededor de 295 969 archivos.

Entre la información que el usuario ofrecía como muestra, se encontraron documentos de identidad, propuestas de abono y contratos telefónicos.

En Septiembre, Samsung emitió un comunicado en el que indicaba que a finales del mes de julio de 2022, un tercero no autorizado consiguió obtener información de varios sistemas estadounidenses de la compañía.

En ese mismo comunicado, indicaron que el atacante no obtuvo información sobre los números de Seguridad Social o información sobre las tarjetas de débito y crédito, pero existía la posibilidad de que pudiera haber accedido a otro tipo de información sensible como el nombre, la información demográfica y de contacto, la fecha de nacimiento o la información de registro del producto.

Se trata del segundo incidente relacionado con brechas de datos que la empresa ha sufrido durante los últimos meses, tras la brecha del pasado mes de marzo.

Durante la primera semana de noviembre, una empresa de telecomunicaciones española comunicó que uno de sus proveedores había sido víctima de un ciberataque mediante el cual el actor de amenazas podría haber conseguido acceder a datos personales de los clientes como nombre, apellidos, dirección postal, número de documento de identidad, código IBAN de la cuenta corriente, etc.

Grandes empresas de telecomunicaciones australianas fueron víctimas de ciberataques durante los meses de septiembre y octubre.

En septiembre, los datos de más de 10 000 clientes de Optus, una empresa subsidiaria de Singtel (Singapore Telecommunications Ltd), fueron filtrados por el actor conocido como optusdata durante un breve periodo de tiempo en el foro de la Deep Web Breachforums.

Posteriormente, Dialog, una empresa de consultoría de servicios TI con sede en Australia y tambien subsidiaria de Singtel, fue víctima de un ciberataque mediante el cual los ciberdelincuentes obtuvieron información de diversos clientes y trabajadores de la entidad para posteriormente publicarlos en la Deep Web durante el mes de octubre.

En último lugar, Telstra, una de las compañías de telecomunicaciones más grandes de Australia reveló una brecha de datos a través de uno de sus proveedores externos.

La empresa realizó un comunicado informando que los datos que habían sido filtrados datan del año 2017 e incluían los nombres, apellidos y direcciones de correo electrónico de empleados que se habían registrado en un programa para recompensas de empleados que actualmente se encontraba obsoleto.

No existe evidencia de que los incidentes estén relacionados entre sí, debido a que el actor detrás de la filtración de Optus eliminó el contenido y pidió perdón a los usuarios que se vieron afectados.

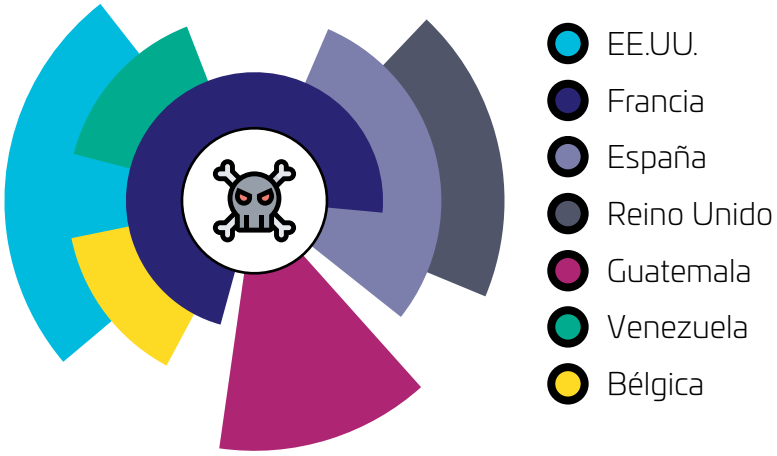
SECTOR ASEGURADORAS

En líneas generales, el número de amenazas cibernéticas que impactan al sector de las aseguradoras se ha visto incrementado en la segunda mitad de 2022.

>> 13

Desde julio hasta diciembre de 2022, el sector de las aseguradoras se ha visto afectado principalmente por un aumento de ciberataques de tipo ransomware, dirigiéndose especialmente contra empresas ubicadas en los Estados Unidos, seguido de Francia, España y Reino Unido.

Afectación por país de ataques de ransomware al sector aseguradoras



Afectación sector aseguradoras por grupo de ransomware

El grupo ransomware que más ha afectado a este sector en el segundo semestre de 2022 ha sido LockBit, seguido de Royal y BlackBasta.

Los accesos más vendidos a entidades de este sector son de tipo RDP, VPN o de explotación de vulnerabilidades de Citrix.

El acontecimiento de ciberseguridad dentro de este sector que más ha marcado el año 2022 ha sido el ciberataque de tipo ransomware sufrido por uno de los mayores proveedores de seguros privados de salud de Australia, que sufrió un ataque ransomware perpetrado por el grupo de amenazas REvil, que publicó 5G de archivos que incluían datos personales de cerca de 9 millones de clientes de la entidad.

El incidente cibernético ha supuesto un antes y un después en la historia del derecho de la ciberseguridad, ya que, como consecuencia del ataque, el gobierno australiano ha aprobado un proyecto de ley denominado Proyecto de Ley de Enmienda de la Legislación de Privacidad (Aplicación y Otras Medidas) 2022, que aumenta la pena económica para todas aquellas empresas que sufran brechas de datos.

Por último, destaca una brecha de datos sufrida por una empresa aseguradora española, de la cual filtraron datos confidenciales como nombres, apellidos, DNI, direcciones y números de teléfono, tanto de clientes actuales como de clientes antiguos de la entidad.

El asunto fue tratado por la Agencia Española de Protección de Datos y la Brigada Central de Investigación Tecnológica de la

ATAQUES RELEVANTES

DEL SEGUNDO SEMESTRE DE 2022

14 V V

S21SEC
Cyber Solutions by Thales

Desde el departamento de Cyber Threat Intelligence de S21sec presentamos un resumen de los ataques más sonados durante el segundo semestre de 2022.

La tipología de ataques más utilizados oscila entre brechas de datos, ataques de denegación distribuida de servicios (DDoS) y ransomware, siendo este último el más empleado por los cibertacantes.

BRECHAS DE DATOS

FECHA	SECTOR	ACTOR DE AMENAZAS
JULIO 2022	Hostelería	Group with No Name (GNN)
DICIEMBRE 2022	Financiero	Grupo APT de origen chino desconocido

DDoS

FECHA	SECTOR	ACTOR DE AMENAZAS
OCTUBRE 2022	Transporte	KillNet
OCTUBRE 2022	Gobierno	KillNet
NOVIEMBRE 2022	Gobierno	KillNet
NOVIEMBRE 2022	Religioso	Grupo hacktivista de origen ruso desconocido

RANSOMWARE

FECHA	SECTOR	ACTOR DE AMENAZAS
JULIO 2022	Telecomunicaciones	LockBit
JULIO 2022	Construcción	BlackBasta
JULIO 2022	Investigación	Vice Society
JULIO 2022	Tecnológico	LockBit
AGOSTO 2022	Manufactura	LV
AGOSTO 2022	Gobierno	Play
AGOSTO 2022	Oil & Gas	ALPHV Black Cat
AGOSTO 2022	Gobierno	Conti
SEPTIEMBRE 2022	Manufactura	RansomHouse
SEPTIEMBRE 2022	Transporte	Ragnas Locker
OCTUBRE 2022	Aseguradoras	REvil
OCTUBRE 2022	Energético	Hive
NOVIEMBRE 2022	Retail	BlackBasta
NOVIEMBRE 2022	Transporte	Daixin Team Group
NOVIEMBRE 2022	Sanitario	WannaCry
DICIEMBRE 2022	Tecnológico	LockBit


S21
SEC
Cyber Solutions by Thales
www.s21sec.com