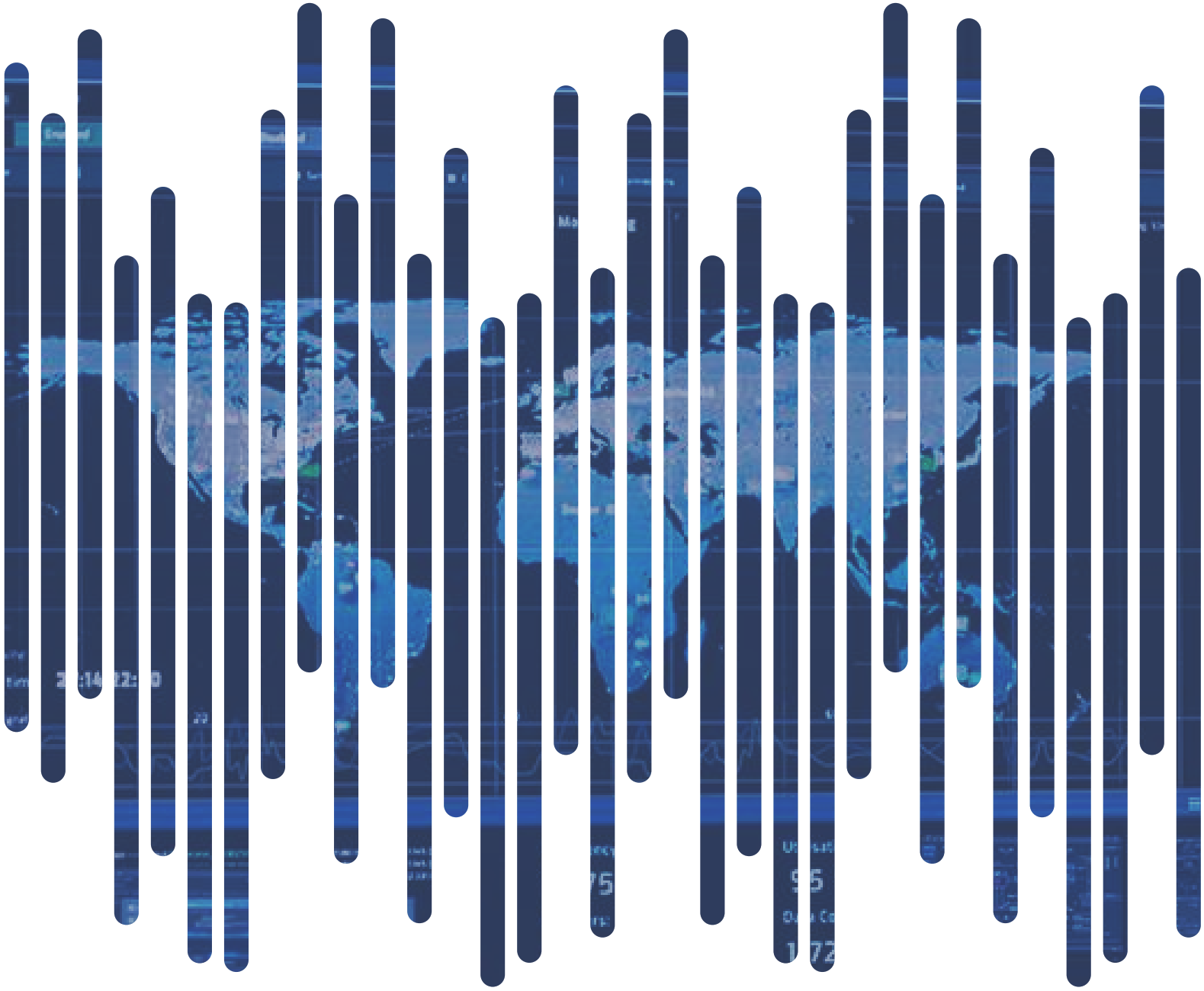
Threat Landscape Report



S21SEC

Durante el primer semestre de 2022 se han identificado un número relevante de ciberamenazas que han supuesto un alto riesgo para entidades público y privadas, las cuales se han podido ver afectadas en menor o mayor medida por la explotación de vulnerabilidades críticas, ciberataques ransomware, distribución de malware destructivo o brechas de datos.

Ante estas ciberamenazas, cabe destacar la explotación de vulnerabilidades que, una vez más, se ha posicionado como una de las ciberamenazas que más preocupan por sus consecuencias.

Una de las situaciones más relevantes a analizar en el primer semestre ha sido el escenario cibernético en el marco del conflicto ruso-ucraniano, donde se han identificado diversas ciberamenazas como una alta participación de grupos hacktivistas, la distribución de *wipers* (malware destructivo) y los ataques ransomware.

Se han mantenido en el foco las amenazas que tienen como objetivo a dispositivos móviles. Estas amenazas, a través de campañas de infección por *smishing* (entre otros), han tenido como objetivo el ciberespionaje, resaltando el caso Pegasus.

S21SEC

CONTENIDOS

Vulnerabilidades

Durante el primer semestre de 2022 han sido publicadas varias vulnerabilidades de criticidad alta, que han sido explotadas activamente por los ciberdelincuentes para la realización de distintos tipos de ataques.

S21SEC

Gran parte de los ciberataques han tenido como vector inicial de entrada la explotación por parte de los cibercriminales de alguna vulnerabilidad en la infraestructura de destino.

En el mes de abril se reveló una vulnerabilidad en el Kernel de Linux, rastreada como CVE-2022-0847, también conocida como "Dirty Pipe", debido al mecanismo para la comunicación entre procesos de Linux. La vulnerabilidad permite la preservación inadecuada de los permisos que afectan al Kernel de Linux, además de un fallo por el que un atacante puede escribir en páginas de la caché de páginas respaldadas por archivos de sólo lectura para posiblemente elevar sus privilegios.

A finales del mes de marzo, una vulnerabilidad zero-day, conocida como Spring4Shell o SpringShell, marcó el panorama de amenazas de seguridad al estar vinculada a una vulnerabilidad de ejecución remota de código (RCE, por sus siglas en inglés) en el entorno de desarrollo de aplicaciones web Java Spring.

Más recientemente, el fallo de seguridad rastreado como CVE-2022-30190, también conocido como "Follina", permitiría a un atacante la instalación de programas, cambio o eliminación de datos, además de la creación de nuevas cuentas en el contexto permitido por los derechos del usuario. Asimismo, según los investigadores, la explotación de esta permitiría a los atacantes la instalación de *malware*.

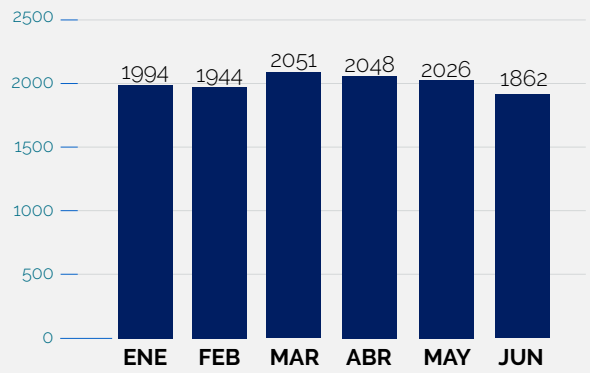
A principios de junio, Atlassian reveló la existencia de una vulnerabilidad crítica de ejecución remota de código sin parchear que afectaba a todas las versiones compatibles con Confluence Server y Data Center, rastreada como CVE-2022-26134, que se está explotando activamente en ataques.

NIVEL DE CRITICIDAD

En total, en el primer semestre de 2022, se han publicado 11.925 vulnerabilidades, de las cuales se registró el mayor número en marzo.

Vulnerabilidades publicadas

Durante el primer semestre de 2022



Nivel de gravedad

Basado en CVSS versión 3

- **Crítico:** 2044
- **Alto:** 4925
- **Medio:** 4807
- **Bajo:** 203
- **Nulo:** 1078

El fallo fue reportado por investigadores que descubrieron su explotación en ataques contra activos estadounidenses.

Tras ser reportado, Atlassian puso a disposición de sus clientes parches de seguridad y ha alertado de la explotación activa del mismo a lo largo del mes de junio.

En los ataques observados, se ha descubierto cómo los actores de amenaza se dirigen contra servidores web conectados a Internet que ejecutaban el software Atlassian Confluence Server, lanzando exploits disponibles públicamente para lograr la ejecución remota de código, mediante la activación de una vulnerabilidad zero-day que afecta a versiones actualizadas de Confluence Server.

Tras explotar con éxito los sistemas de Confluence Server, el atacante implementa una copia en memoria del implante BEHINDER, un popular implante de servidor web con código fuente disponible en GitHub.

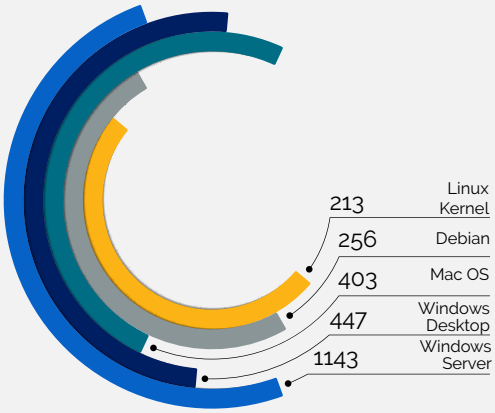
BEHINDER proporciona capacidades avanzadas a los atacantes, incluidos *webshells* solo de memoria y soporte integrado para la interacción con Meterpreter y Cobalt Strike. Una vez que se implementa BEHINDER, el atacante usael *webshell* en memoria para implementar dos *webshells* adicionales en el disco: CHINA CHOPPER y un *shell* de carga de archivos personalizado.

Tras la publicación de los parches de seguridad, diversos medios han reportado, a lo largo del pasado mes de junio la existencia de PoC disponibles públicamente, así como la observación de la explotación de esta vulnerabilidad en diversos ataques.

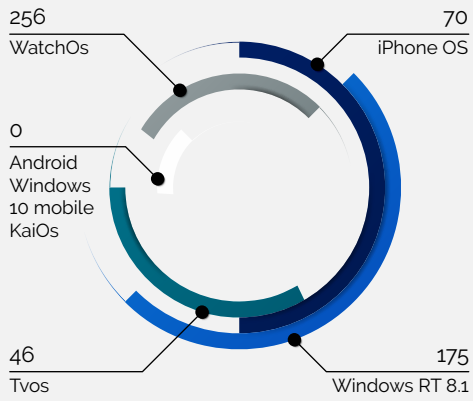
VULNERABILIDADES EN SISTEMAS OPERATIVOS Y VULNERABILIDADES SO EN DISPOSITIVOS INTELIGENTES

Destacan Windows Server y Windows RT 8.1 como los más afectados.

Vulnerabilidades en sistemas operativos



Vulnerabilidades SO dispositivos inteligentes



EXPLOTACIÓN LOG4SHELL

Durante el pasado mes de junio, la CISA (Agencia de Ciberseguridad e Insfraestructuras de Estados Unidos) alertó de la explotación activa de la vulnerabilidad de Log4Shell (CVE-2021-44228) en Servidores VMware Horizon y Unified Access Gateway sin parchear.

Según las investigaciones llevadas a cabo por el Comando Cibernético de la Guardia Costera de los Estados Unidos (CGCYBER, por sus siglas en inglés), actores de amenazas, incluidas amenazas persistentes avanzadas (APT) con patrocinio estatal, han continuado explotando Log4Shell en servidores VMware Horizon y Unified Access Gateway sin parchear durante los últimos meses para obtener acceso inicial a las organizaciones objetivo.

Como parte de esta explotación, las APT implementan *loaders* en sistemas comprometidos con ejecutables integrados que permiten el comando y control remotos (C2).

En ataques observados durante los últimos meses, las APT realizaron movimiento dentro de la red, obtener acceso a una red de recuperación ante incidentes y recopilar y filtrar datos confidenciales.

ADEMÁS DE LA EXPLOTACIÓN DE ESTA VULNERABILIDAD, SE HA OBSERVADO:

En los mismos ataques se ha explotado la CVE-2022-22954, una vulnerabilidad RCE en VMware Workspace ONE Access and Identity Manager, para implantar un *webshell*.

En los ataques, los actores de amenaza extraen datos confidenciales, algunos del entorno de producción de una de las víctimas.

DOGWALK

En el mes de junio, Microsoft parcheó una vulnerabilidad de tipo zero-day de Windows en la herramienta de diagnóstico de soporte de Microsoft (MSDT) a través de la plataforma 0patch.

La vulnerabilidad, denominada informalmente DogWalk, es un fallo transversal de ruta que los atacantes pueden explotar para copiar un ejecutable en la carpeta de inicio de Windows cuando el objetivo abre un archivo .diagcab creado con fines malintencionados (recibido por correo electrónico o descargado de la web).

El ejecutable malicioso implantado se ejecuta automáticamente las siguientes veces que la víctima reinicie Windows.

Aunque la vulnerabilidad fue revelada en 2020, el fallo ha sido redescubierto recientemente y puesto en conocimiento público, instando a Microsoft a parchearlo.

Aunque Microsoft ha asegurado que los usuarios de Outlook no están en riesgo porque los archivos .diagcab se bloquean automáticamente, los investigadores y expertos en seguridad han alertado que explotar este error sigue siendo un vector de ataque significativo.

Si un actor de amenazas entrega el archivo malicioso a través de otro cliente de correo electrónico o en descargas ocultas a través de sitios controlados por atacantes, puede explotar activamente la vulnerabilidad.

Los archivos .diagcab se descargan de Internet e incluyen una Marca de la Web (MOTW), Windows la ignora para este tipo de archivo y permite abrir el archivo sin una advertencia.

SOPHOS

Durante el primer semestre de 2022, investigadores de seguridad han reportado la explotación activa de una vulnerabilidad crítica (CVE-2022-1040) en Sophos Firewall para dirigirse contra conjuntos de organizaciones en el sur de Asia.

Identificada como CVE-2022-1040, se trata de una vulnerabilidad de omisión de autenticación en el Portal de usuario y Webadmin de Sophos Firewall, que puede ser explotada por los atacantes para lograr la ejecución remota de código en dispositivos vulnerables.

La vulnerabilidad afecta a Sophos Firewall v18.5 MR3 (18.5.3) y versiones anteriores.

En cuanto a la explotación de esta vulnerabilidad, se ha observado, desde principios del año, la explotación por parte de grupos de amenazas persistentes avanzadas (APT) chinos.

En sus ataques se hace uso de un exploit de tipo zero-day para comprometer el *firewall* del cliente.

Se implementan *backdoors webshell*, creando una segunda vía de de persistencia y, en última instancia, se lanzan ataques contra el personal de las organizaciones, para impactar en mayor medida en servidores web alojados en la nube que albergan los sitios web públicos de la organización.

THREAT LANDSCAPE REPORT

Primer semestre 2022

Ransomware

Durante los seis primeros meses, se han observado cambios en las tácticas, técnicas y procedimientos de algunos de los operadores de ransomware, mediante la introducción de nuevas tácticas y mejora de sus técnicas.

S21SEC

ESTADÍSTICAS RANSOMWARE

FAMILIAS DE RANSOMWARE

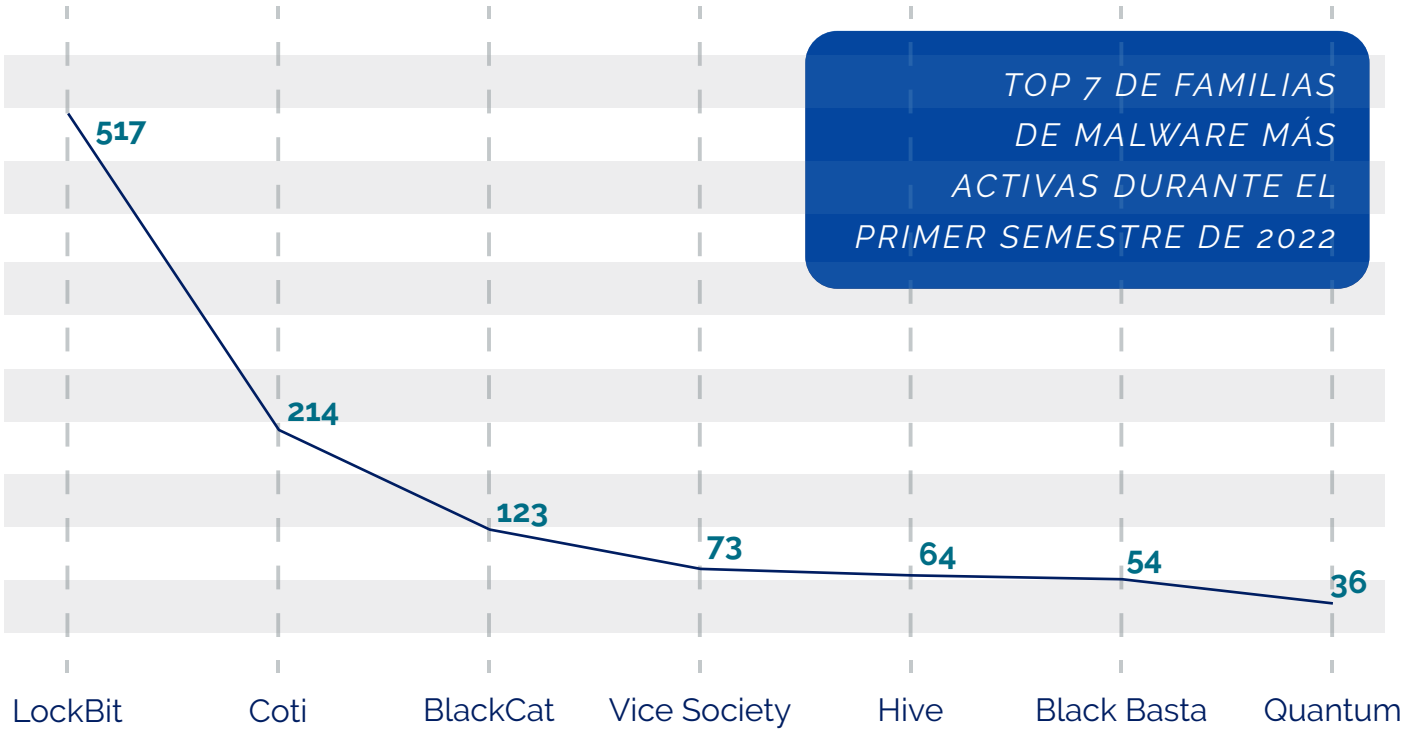
En líneas generales, durante este período los tres grupos de ransomware más activos han sido LockBit, Conti y BlackCat (ALPHV), que han cifrado a un total de 517, 214 y 123 víctimas respectivamente, según los ataques analizados.

Durante este primer semestre se han observado un total de 41 familias diferentes de ransomware.

En líneas generales, cabe destacar la tendencia hacia una aparición de nuevos grupos de ransomware en el panorama de amenazas, entre los cuales destacan Pandora, Night Sky, Haron, Black Basta, Mindware, Cheers, Industrial Spy, Crimson Walrus y Axxes.

Además de la activación del conocido grupo ransomware REVil3.0, que ha mostrado signos de actividad a partir del mes de marzo, tras el arresto en el mes de enero de varios de sus miembros y el cese de su infraestructura.

Otros grupos de amenaza han cesado sus operaciones, como el ransomware Conti que, tras declarar su apoyo a Rusia en febrero de este año, sufrió una filtración por parte de uno de sus miembros, conocida como ContiLeaks, que dio a conocer los registros internos del grupo y ha permitido a los investigadores revelar el funcionamiento, sus operaciones, las víctimas y el código del ransomware.



ESTADÍSTICAS RANSOMWARE

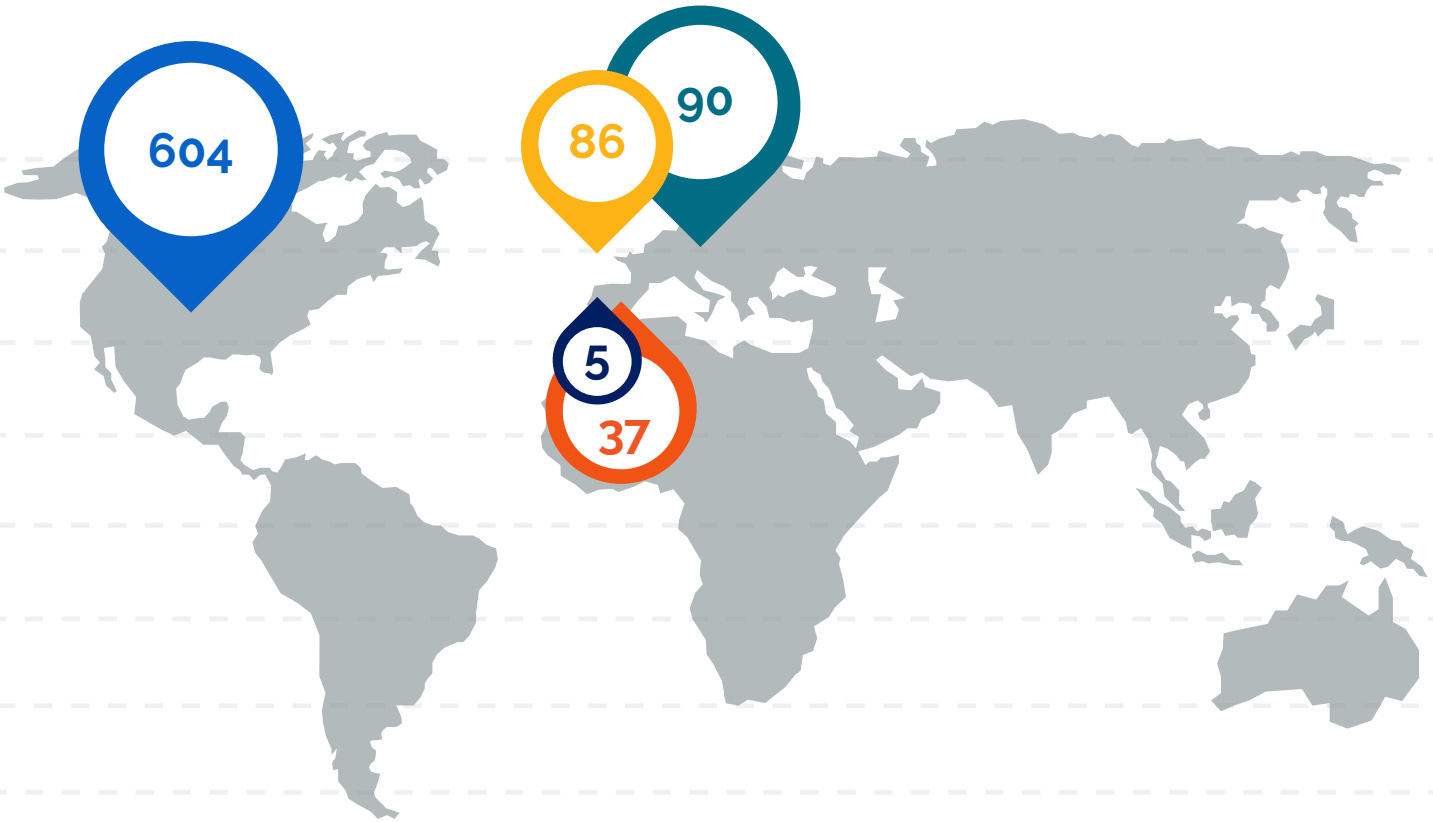
PAÍSES

El equipo de Threat Intelligence de S21sec ha monitorizado la actividad llevada a cabo por parte de actores de amenazas en más de 50 blogs de grupos ransomware en la *deep web*, *dark web* y foros clandestinos. Hay que tener en cuenta que la cifra de ataques observada abarca exclusivamente la actividad pública observada que ha sido realizada por los actores de amenazas.

Con un total de 1466 ataques en todo el mundo durante el primer semestre de 2022, el continente más afectado es América del Norte, con un total de 689 ataques, seguido de Europa con 485, y Asia, que ha sufrido 161 ataques durante este periodo de tiempo.

Centrándonos en los países, Estados Unidos registra el mayor número con 604 ataques, seguido de Alemania y Reino Unido, con 90 y 86.

España ha recibido 34 ataques durante el primer semestre del 2022 y Portugal, 5, colocándolos en el puesto 7 y 37 del ránking mundial de ciberataques, respectivamente.



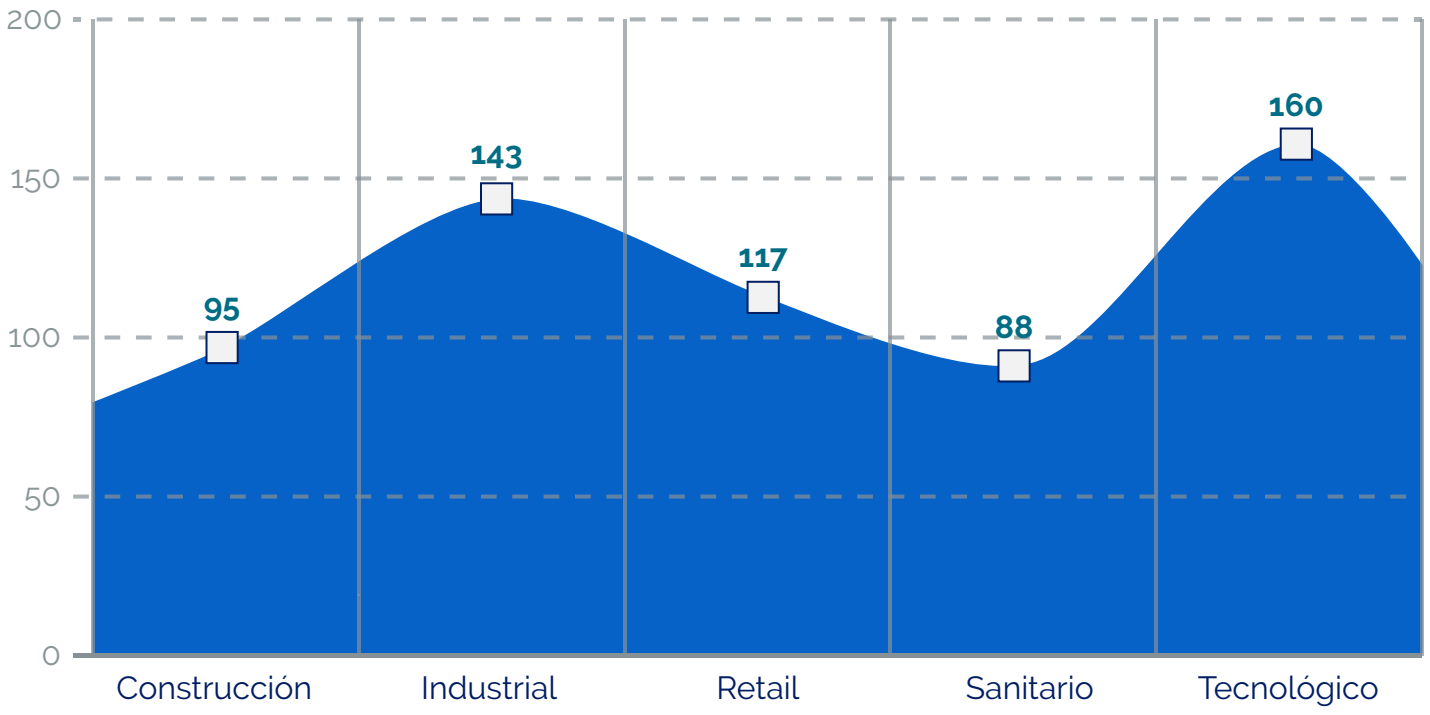
ESTADÍSTICAS RANSOMWARE

SECTORES

Los resultados arrojan un total de 1466 ataques ransomware registrados entre enero y junio de 2022. En cuanto a las verticales de las industrias más destacadas a las que pertenecen las 1.466 víctimas de estos ransomware, se encuentran sobre todo empresas de los sectores tecnológico, industrial, retail, y de construcción.

Se han destacado las anteriores por superar las 90 víctimas en este periodo; sin embargo, otros sectores como el sanitario, transporte y logística, gobierno y administración y financiero, superan las 70 víctimas en su conjunto.

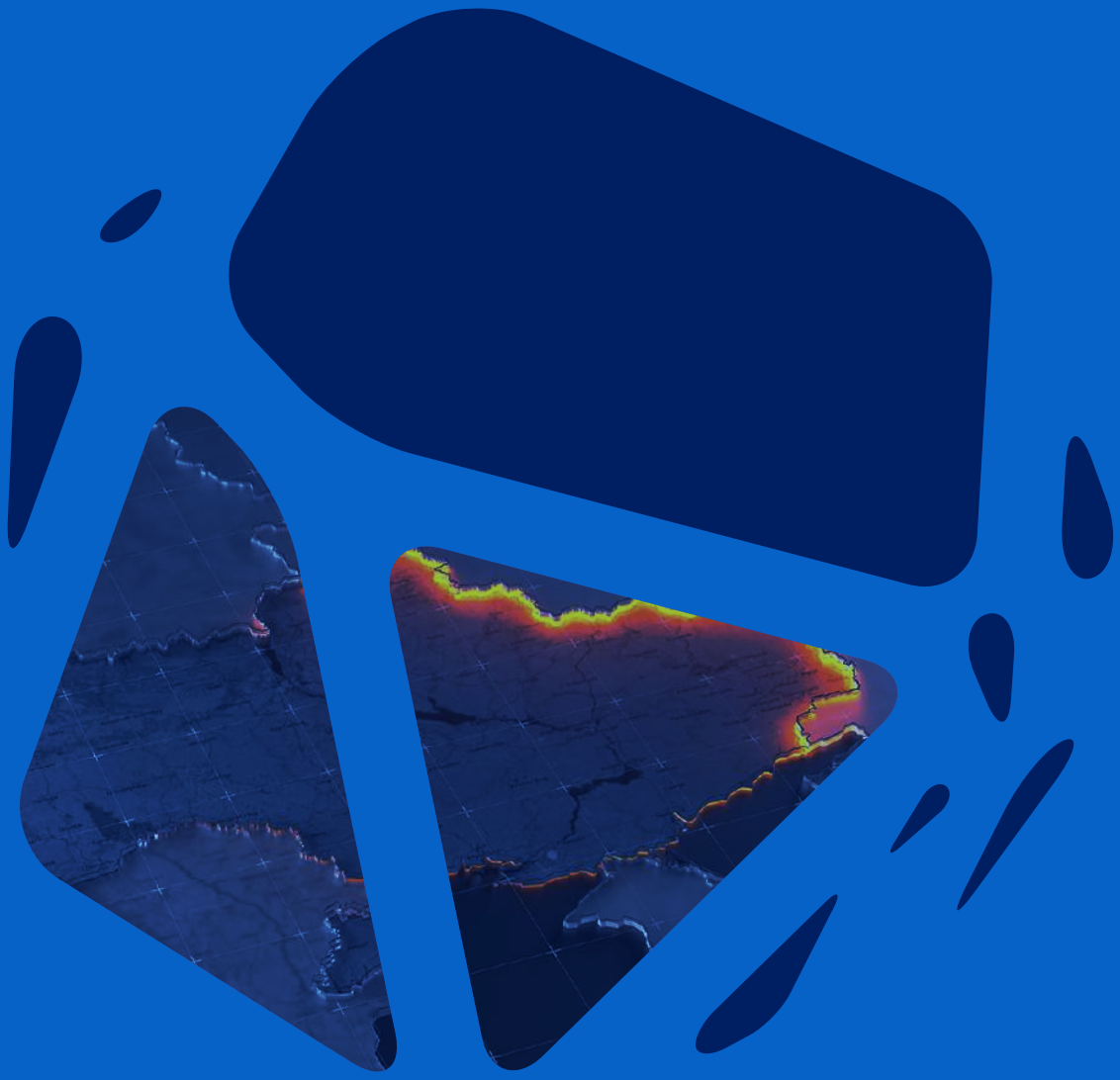
TOP 5 DE SECTORES MÁS AFECTADOS POR RANSOMWARE DURANTE EL PRIMER SEMESTRE DE 2022



THREAT LANDSCAPE REPORT

Primer semestre 2022

Conflicto Rusia-Ucrania



El conflicto entre Rusia y Ucrania se ha convertido en un claro ejemplo de lo que se denomina una guerra híbrida, en la que el campo de batalla no se encuentra exclusivamente en el ámbito físico, sino que también ha pasado al ciberespacio.

S21SEC

Cabe destacar que, antes de la entrada de Rusia en Ucrania se produjeron ciberataques en los que se utilizó malware destructivo contra organizaciones e infraestructuras críticas ucranianas: los denominados *wipers*.

Este tipo de ataques destructivos los llevan a cabo grupos APT (amenazas persistentes avanzadas, por sus siglas en inglés) patrocinados por gobiernos y que cuentan con grandes capacidades técnicas.

Debido a la amenaza rusa en el ciberespacio, el gobierno ucraniano llevó a cabo un reclutamiento masivo de expertos en seguridad informática que implicó la participación de hackers a nivel mundial.

Estos voluntarios cibernéticos se unieron a un ejército llamado **IT Army of Ukraine**.

En este conflicto cibernético, actores individuales o grupos hacktivistas a favor de Rusia o Ucrania han estado implicados en la realización de ciberataques contra el bando contrario.

También es reseñable el hecho de que el alcance de los ataques se ha extendido a otros países y organizaciones internacionales que no están participando activamente en el conflicto armado.

AMENAZAS

El panorama de amenazas surgido de la guerra en Ucrania es amplio y comprende:
- Ataques de malware destructivo
- Ransomware
- Campañas de phishing
- Malspam
- Ataques hacktivistas.

ATAQUES DE MALWARE DESTRUCTIVO

Durante el conflicto, se ha observado la utilización por parte de Rusia de distintos tipos de malware de tipo *wiper*, cuyo objetivo principal es el de destruir los sistemas a los que se dirige o la eliminación de datos dentro de los mismos, provocando grandes daños a las empresas y organizaciones afectadas.

El primer *wiper* observado en el contexto de la guerra fue el llamado WhisperGate, el pasado 13 de enero de 2022, previo a la invasión.

Posteriormente, el 24 de febrero, los atacantes rusos lanzaron el malware IsaacWiper.
El 14 de marzo se observó un ataque con CaddyWiper. Además, se observaron otros malware conocidos como Hermetic Wiper, HermeticWizard y HermeticRansom.

En marzo se detectaron también los malware DoubleZero y Cyclops Blink.

Posteriormente, a mediados del mes de abril, se informó de un ciberataque a gran escala contra subestaciones eléctricas de una compañía energética ucraniana, en el que se utilizó una nueva variante del malware Industroyer desplegado por Rusia en Ucrania en el año 2016, conocida como Industroyer2.

HACKTIVISMO

En este conflicto se ha producido una reactivación del hacktivismo internacional, con Anonymous como uno de los actores más relevantes en esta categoría.

Anonymous mostró desde el inicio del conflicto su apoyo a Ucrania, llevando a cabo una gran cantidad de ataques basados en la realización de *defacements* de sitios web, ataques DDoS y filtraciones de bases de datos e información confidencial de organismos gubernamentales y empresas pertenecientes a diversos sectores.

Estos ataques se enmarcan dentro de la denominada #OpRusia, operación que no solo se centra en empresas o instituciones rusas, sino también empresas occidentales que realicen actividades en Rusia.

El colectivo formado a través del llamamiento del gobierno ucraniano, el IT Army of Ukraine, también ha llevado a cabo numerosos ataques hacktivistas dirigidos contra instituciones rusas.

El colectivo AgainstTheWest/BlueHornet también ha efectuado varios ciberataques, como filtraciones y brechas de datos contra objetivos pertenecientes a países que han mostrado su apoyo al Kremlin.

Por otro lado, encontramos también a colectivos hacktivistas que apoyan a Rusia, como XakNet, un colectivo hacktivista que se denomina a sí mismo como "grupo de patriotas rusos", y KillNet, uno de los colectivos más activos en este conflicto, con ataques dirigidos a Letonia, Italia, Alemania, Polonia, Rumanía, Ucrania, Estados Unidos, República Checa, entre otros.

Cabe destacar que a mediados de mayo, Killnet publicó a través de su canal de Telegram una amenaza dirigida a Italia y España, tras la cual realizaron numerosos ataques de Denegación de Servicio a sitios italianos.

Sector Bancario

Durante el primer semestre de 2022, se han detectado diferentes campañas de distribución de troyanos bancarios, de los que se tiene conocimiento desde varios años antes y que han protagonizado algunas de las campañas más significativas en 2021

S21SEC

La detección de nuevas operaciones de distribución de estos troyanos bancarios refleja la prevalencia de estos códigos maliciosos, que se han mantenido activos y se han distribuido a lo largo del primer semestre de 2022 utilizando nuevas plantillas y temáticas en sus comunicaciones fraudulentas, suplantando diversos servicios, compañías y organizaciones y haciendo uso de nuevos artefactos que faciliten su distribución.

GRANDOREIRO

El troyano Grandoreiro se ha convertido desde 2021 en una amenaza relevante en el sector bancario en España y varios países de la Unión Europea. Como troyano, este malware está diseñado para tener múltiples utilidades. La más común es crear un backdoor en el equipo infectado para poder descargar actualizaciones y nuevas funcionalidades.

Desarrollado en lenguaje Delphi, este troyano realiza la captura y exfiltración de información sensible del equipo comprometido, para esto emplean como vector de distribución el envío de correos de tipo phishing que llevan adjuntos archivos que con la interacción del usuario desencadenan la instalación de este troyano en el equipo. Entre sus características, destaca la velocidad con la que sus autores actualizan su código, existiendo diferentes variantes que se han extendido internacionalmente desde 2019 y han afectado a bancos de España, México y Portugal.

Durante el primer semestre de 2022, las campañas de distribución de Grandoreiro se han mantenido activas, reutilizando plantillas de correo electrónico utilizadas en las operaciones de 2021 e introduciendo nuevas temáticas de engaño a las víctimas.

Además de correos electrónicos de malspam que fingen contener facturas e información financiera de compañías suplantadas, como proveedores de telefonía móvil o proveedores de servicios, las operaciones más significativas de distribución de Grandoreiro han suplantado a instituciones y organizaciones públicas.

LA INFECCIÓN CUENTA CON VARIAS ETAPAS

La distribución se realiza mediante correos electrónicos fraudulentos que contienen una URL de acceso a una página maliciosa o un archivo adjunto.

Cuando se accede al enlace, se procede a la descarga de un fichero instalador que, a su vez, descarga el payload que contiene el troyano bancario.

Iced ID

IcedID, también conocido como BokBot, es un troyano bancario aparecido en 2017. Este malware posee distintas capacidades, como el robo de información personal o el robo de credenciales.

Además, se utilizó como vector de entrada de otros códigos maliciosos. Operado por la APT por Luna Spider, también conocida como Gold Swathme, este malware ha sido utilizado como medio de distribución en campañas del ransomware REvil/Sodinokibi.

Este vínculo con operaciones de ransomware, además de su exponencial distribución en 2021, ha llevado a la comunidad experta a sugerir que este malware puede actuar como sucesor de Emotet en sus campañas de infección masivas.

Entre sus medios de distribución, destacan las operaciones de phishing mediante las cuales los operadores del malware hacen llegar a las víctimas correos electrónicos de phishing que contienen un documento adjunto malicioso de Microsoft con Macros 4.0 (XML), que conduce a una segunda fase para descargar el malware, tras abrir el documento y habilitar las macros.

Junto a este medio, se ha detectado la distribución mediante el envío de formularios de contacto. Este medio de infección permite a los atacantes realizar actividades de seguimiento, además de moverse lateralmente a través de redes afectadas para seguir distribuyendo código malicioso adicional.

En febrero se detectó una nueva actividad de IcedID ligada a la carga de Cobalt Strike en un tiempo reducido de apenas 20 minutos tras la infección. En esta operación, una vez ejecutado, IcedID aplica comandos de descubrimiento para capturar información del sistema, el dominio y la red.

Estos son comandos comunes ejecutados por malware precursor y probablemente se usen para priorizar puntos de apoyo para futuras acciones de intrusión. Menos de 20 minutos después de la infección inicial, el host ejecuta comandos remotos de PowerShell para implementar Cobalt Strike.

En marzo también se detectó la utilización de servidores de Microsoft Exchange comprometidos para la distribución de malspam diseñado para infectar equipos con IcedID. Esta operación, detectada a mediados de mes, estuvo dirigida contra organizaciones del sector energético, sanitario, legal y farmacéutico.

En la distribución se hacía uso de servidores desactualizados, que permitían a los delincuentes explotar vulnerabilidades de ProxyShell para hacerse cargo de los equipos y enviar malspam con el código IcedID.

ADEMÁS DE ESTAS INFECCIONES, A FINALES DE MAYO SE DETECTARON

Nuevos vectores de distribución e infección, relacionados con el uso un archivo en formato ZIP que contenía embebido otro archivo con extensión .lnk (archivos de acceso directo en Microsoft Windows) que empleaba el binario legítimo mshta.exe con el propósito de descargar IcedID en el equipo objetivo.

Esta operación, además, hacía uso de DarkVNC, una distribución maliciosa del programa VNC (Virtual Network Computing) que permitía al malware controlar remotamente el equipo de una víctima.

Sector Energético

En el primer semestre de 2022 se han producido ciberataques de diversa índole contra empresas del sector energético. Cabe destacar que las infraestructuras energéticas de un país se consideran infraestructuras críticas, y que un ataque contra las mismas puede suponer riesgos no sólo para la empresa atacada, sino también para la ciudadanía.

S21SEC

Como se ha comentado, en este periodo se han dado ataques contra empresas del sector energético por parte de actores con distintos objetivos. Algunos de ellos buscaban un beneficio financiero, mientras otros tenían como objetivo la destrucción o la paralización de las infraestructuras eléctricas para causar el mayor daño posible.

De entre los ataques más significativos durante este período destacan los ocurridos en febrero.

El sector fue víctima de una serie de ciberataques dirigidos a las empresas alemanas Oiltanking GmbH y Mabanaft GmbH y la compañía belga Sea-Invest, a los cuales se le sumaron otra serie de ataques dirigidos a infraestructuras críticas, como el ataque ransomware sufrido por el grupo italiano Dolomiti Energia que dejó inoperativo sus sistemas de TI o la compañía de servicios de aviación con sede en Suiza, Swissport International.

Los ataques tuvieron como objetivo empresas de la cadena de suministro, proveedores, instalaciones o sistemas, por parte de actores de amenazas con motivaciones principalmente económicas.

Otras empresas fueron presuntamente atacado por el ransomware LockBit 2.0

El Grupo Energético del Sureste (Grupo GES), localizado en Campeche (México), que forma parte de la Industria comerciante al por Mayor de Petróleo y Productos Petrolíferos, además del National Petroleum Group of Vietnam (Petrolimex), quien fue víctima de los actores de amenazas detrás del ransomware BlackByte en el mes de febrero.

Ataques del ransomware Hive

A principios del mes de marzo, Rompetrol, una compañía petrolera rumana que opera en Europa, Asia Central y África del Norte, especializada en el refinamiento de productos petroquímicos, fue víctima de un ataque ransomware por parte de los operadores de Hive, impactando en la mayoría de los servicios de TI.

Otra empresa mencionada por el ransomware Hive durante el mes de marzo ha sido Pan American Energy S.L., Sucursal Argentina, el principal productor de gas del país. Hasta el momento no se han filtrado ninguna información de la compañía. Además de la empresa Noble Oil, una empresa privada de reciclaje de servicios de aceite de motor usado, anticongelante y filtros, localizada en Estados Unidos.

Conflicto Rusia - Ucrania

Desde el inicio del conflicto bélico a raíz de la invasión de Rusia a Ucrania, el panorama de amenazas cibernéticas dirigidas contra el sector estratégico e infraestructuras críticas ha ido en aumento y los actores de amenazas han ido ampliando sus objetivos hacia otros países europeos, especialmente aquellos que han brindado apoyo a Ucrania.

Algunos grupos de ciberdelincuentes se han comprometido apoyar tanto a Ucrania como al gobierno ruso. En el caso de los actores cibernéticos alineados con Rusia, estos han amenazado con realizar operaciones en el ciberespacio en represalia por las supuestas ofensivas cibernéticas contra el gobierno ruso o el pueblo ruso, además de operaciones cibernéticas dirigidas contra países y organizaciones que brindan apoyo a Ucrania.

La gran mayoría de los ataques observados durante el desarrollo de la guerra híbrida responden a motivaciones hacktivistas y consisten en desfiguraciones de sitios web, ataques DDoS y DoS y filtraciones de bases de datos e información confidencial de organismos gubernamentales, e infraestructuras críticas como aeropuertos.

En este contexto, se han producido 43 ataques de ransomware contra empresas del sector energético desde enero de 20222.

En febrero se produjeron tres ciberataques a empresas europeas dedicadas a la generación de energía eólica por parte de grupos de ransomware que se han declarado afines al gobierno ruso, como Conti o Black Basta. Estos ataques se produjeron en la fase inicial del conflicto entre Rusia y Ucrania y, aunque el incentivo detrás de estos grupos generalmente es económico, no se puede descartar que haya tenido también motivaciones políticas, con el fin de interrumpir el funcionamiento de empresas de generación de energía en Europa.

También en el inicio del conflicto, el ransomware Blackcat, vinculado con grupos cibercriminales de origen ruso, se dirigió contra empresas dedicadas a la producción y al transporte de petróleo y gas.

Campañas de *malspam*

Por otro lado, el sector se ha visto afectado por campañas de malspam, en la que actores de amenazas estaban distribuyendo el malware formbook, apuntando a empresas de petróleo y gas, mediante el envío de correos electrónicos maliciosos suplantando a la compañía pública de petróleo y gas natural de Arabia Saudí, Saudi Aramco, que contenían archivos maliciosos en formato PDF y Excel con el malware Formbook.

BLACKCAT

El ransomware Blackcat, también conocido como ALPHV, comenzó su actividad en noviembre de 2021, siendo distribuído a través de correo electrónico. Cuando la víctima descarga y abre el archivo adjunto a estos correos, el malware comienza a ejecutarse en la máquina.

Blackcat cifra los archivos de su víctima y los renombra añadiendo la extensión .sykffle . Como es común con otras muestras de ransomware, BlackCat dejará caer notas de rescate en los sistemas comprometidos para informar la víctima de lo que ha sucedido y cómo proceder para restaurar sus datos.

Los archivos de texto con el nombre RECOVER-sykffle-FILES.txt que muestran la nota de rescate se encontrarán en el sistema comprometido y estos contendrán información y las instrucciones que deberá seguir la víctima.

ANTES DE CIFRAR LOS ARCHIVOS, EL ATACANTE EXFILTRARÁ LOS ARCHIVOS CONTENIDOS EN LA MÁQUINA

Aplica la técnica de doble extorsión, amenazando con publicar los datos extraídos en su blog de la Deep Web.

Además, si el anterior método de extorsión no funciona, el atacante usará otro método de extorsión, el cual consistirá en amenazar a las víctimas con un ataque de DDoS contra sus activos con la finalidad de que paguen. Mediante esta técnica de triple extorsión, el atacante se asegura de que las víctimas paguen el rescate.

S21SEC

THREAT LANDSCAPE REPORT

Primer semestre 2022

Sistemas de Control Industrial

En el primer semestre de 2022, los sistemas de control industrial se han convertido en uno de los objetivos prioritarios para diferentes actores de amenaza a nivel internacional.

S21SEC

La amplia utilización de los sistemas de control industrial (ICS, por sus siglas en inglés), desde la fabricación, las instalaciones de procesamiento hasta las plantas energéticas, ha convertido a esta tecnología en uno de los objetivos de los actores de amenazas para impactar en organizaciones de gran envergadura y posición estratégica.

A lo largo de los últimos meses se han detectado campañas, herramientas, código malicioso y tácticas destinadas a impactar contra estos sistemas y crear disrupciones de gran envergadura en las organizaciones que los utilizan.

En el marco del conflicto entre Rusia y Ucrania, se ha detectado la realización de actividades disruptivas en estos sistemas con el objetivo de impactar masivamente en las organizaciones que hacen uso de estas tecnologías.

INCONTROLLER

INDUSTROYER2

S21SEC

INCONTROLLER

Durante este periodo, se ha descubierto la existencia de una serie de herramientas (toolkits) llamadas Pipedream o Incontroller, que permiten obtener acceso completo al sistema a múltiples dispositivos del Sistema de control industrial (ICS).

El pasado mes de abril, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Agencia de Seguridad Nacional (NSA), la Oficina Federal de Investigaciones (FBI) y el Departamento de Energía (DOE) emitieron un aviso de seguridad cibernética conjunto que advierte sobre las amenazas respaldadas por gobierno o actores de amenazas persistentes avanzadas (APT), utilizando estas herramientas, que permiten obtener el acceso a los controladores lógicos programables (PLC) de Schneider Electric, PLC OMRON Sysmac NEX, y a servidores de arquitectura unificada de comunicaciones de plataforma abierta (OPC UA).

Con estas herramientas, los actores de amenazas son capaces de realizar movimientos laterales, escalada de privilegios e interrupción del servicio después de obtener acceso completo a los entornos de los dispositivos ICS/SCADA.

El toolkit de Incontroller está constituido esencialmente por 3 herramientas principales.

TAGRUN

Esta herramienta sirve para buscar servidores OPC. Enumera y etiqueta estructuras OPC y genera ataques de fuerza bruta.

CODECALL

Este módulo se comunica a través de Modbus y CodeSys. Contiene funcionalidades para interactuar, escanear y atacar, al menos, tres modelos distintos de controladores lógicos (PLC) de Schneider Electric.

OMSHELL

Contiene funcionalidades para interactuar y escanear algunos tipos de PLC Omron a través de HTTP, Telnet, y Omron FINS. Esta herramienta también puede interactuar con los servo-accionamientos de Omron.

S21SEC

INDUSTROYER2

En abril se hizo pública una investigación del CERT ucraniano sobre un ciberataque a gran escala contra subestaciones eléctricas de una compañía energética ucraniana que habría tenido lugar durante ese mismo mes, y que podría atribuirse a la APT de origen ruso conocida como Sandworm.

El despliegue de malware en los Sistemas de Control Industrial (ICS, por sus siglas en inglés) de la subestación eléctrica afectada probablemente se produjo el día 8 de abril de 2022.

No obstante, los ciberdelincuentes habrían obtenido acceso semanas antes por lo que no se descarta que estuvieran realizando acciones para ganar persistencia y conseguir movimiento lateral para distribuir el malware Industroyer2.

El malware Industroyer2 se despliega como un ejecutable de Windows denominado 108_100.exe.

En este caso, el malware solo hace uso del protocolo IEC-104 a través del cual se comunica con el equipo industrial.

Tras conectar con los dispositivos y equipo informático objetivo, el malware comienza a añadir la extensión .MZ a las aplicaciones que se usan en las operaciones diarias de los equipos y dispositivos afectados.

Tras este proceso, Industroyer2 podría acceder al control de sistemas ICS con diversos objetivos, como cortar el suministro eléctrico.

La información presentada muestra que la cadena de ataque del 8 de abril de 2022 se inició de la siguiente manera:

- Despliegue del malware CaddyWiper en sistemas Windows, Linux y Solaris del proveedor de energía objetivo.
- El grupo Sandworm inicia la secuencia para el despliegue del malware Industroyer2 con el objetivo de cortar el suministro eléctrico en una región de Ucrania.
- Posterior ejecución del malware CaddyWiper en las mismas máquinas afectadas por Industroyer2 para eliminar rastro de este último.

Sector Sanitario

Desde el inicio de la pandemia por la COVID-19 en 2020, el sector sanitario (inclúyanse hospitales, centros de investigación médica, clínicas privadas y centros de salud) se ha posicionado como uno de los principales objetivos de ciberataques, poniendo en relieve la sensibilidad de este sector ante amenazas cibernéticas.

S21SEC

En ediciones anteriores del Threat Landscape de S21sec se han mencionado las ciberamenazas a las que se ha visto expuesto el sector sanitario y se han propuesto escenarios de futuro entorno a dicha situación.

Entre las ciberamenazas mostradas en el documento, se encuentran mayoritariamente los ataques de tipo ransomware y las campañas de phishing para robo de credenciales, lo cual siguen siendo una ciberamenaza con graves repercusiones.

No obstante, con el inicio del año 2022, se ha identificado 2 ciberamenazas cuya notoriedad ha aumentado y han llamado la atención:

- Brechas de datos de centros hospitalarios y clínicas.
- Ventas/subastas de accesos de entidades del sector sanitario.

En el caso de las brechas de datos, estas suelen darse tras un ciberataque previo, ya sea por campañas de phishing, intrusión, ransomware o infección por otro tipo de malware. Además, los actores de amenazas pueden realizar acciones de mera intrusión para recabar información/ datos con el objetivo de usarla con fines maliciosos.

De acuerdo con los datos recopilados por S21sec, se considera que las brechas de datos se han posicionado entre las principales ciberamenazas contra hospitales, ambulatorios y clínicas privadas de cualquier especialidad, entre otros.

Con ello, desde S21sec se han podido identificar más de 50 brechas de datos en los primeros 6 meses de 2022.

Sin embargo, el número de estas podría ser mayor, doblando la cifra de 50, mientras que algunas de ellas no se han podido identificar debido a 2 principales casuísticas:

- Diversas clínicas no reportan la brecha de datos a los organismos correspondientes debido al desconocimiento de la misma o bien por motivos de daño reputacional.
- Los cibercriminales responsables de la brecha de datos no anuncian en blogs y foros underground la venta o exposición de los datos robados, pudiendo desconocerse sin un análisis informático previo si se ha sido víctima de una intrusión y robo de datos.

En los primeros 6 meses de 2022 se pueden destacar las brechas de datos del Hospital Centro de Andalucía, que notificó una brecha de datos tras un ciberataque el pasado enero.

A su vez, el grupo hospitalario estadounidense Shields Health Care sufrió a principios de junio una brecha de datos que afectó a más de 2 millones de pacientes a raíz de un ciberataque que se produjo en el mes de marzo, teniendo un importante impacto en su infraestructura y datos de pacientes y empleados.

A través de foros y chats de la *Deep* y *Dark Web* se ha podido identificar un aumento de la venta y/o subasta de accesos con privilegios de administrador a centros hospitalarios y clínicas del sector sanitario. Estas ventas se suelen llevar a cabo de 2 formas:

- Como paso posterior a la infección de los equipos informáticos de la entidad objetivo donde se recopilan credenciales de acceso a sistemas críticos/ sensibles de la entidad objetivo.
- A raíz de una brecha de datos previa donde los actores de amenaza extraen los datos de las víctimas con el objetivo de vender o subastar dichos datos e información en foros underground de la *Deep* y *Dark Web*.

En el segundo caso, los actores de amenazas publican en foros más accesibles (sin tener que crear una cuenta o sin tener que interactuar) bases de datos de manera gratuita.

Asimismo, la venta y posterior adquisición de los datos robados pueden usarse con diferentes motivos por otros actores maliciosos, como realizar otros ciberataques, suplantar la identidad de los usuarios, lanzar campañas de phishing contra los usuarios comprometidos o proceder a comprometer datos bancarios para desviar el dinero de la víctima a cuentas del actor de amenazas.

INFORMACIÓN ADICIONAL

Según los datos recopilados desde S21sec, en los primeros meses se han detectado 33 publicaciones de ventas/subastas de accesos relacionados con el sector sanitario, aunque no se descarta que existan más ventas de esta tipología a través de foros con mayores restricciones o por canales privados.

Para ilustrar dichas ventas de accesos y datos, en el primer semestre de 2022 diversos actores de amenazas han publicado la venta y subasta de accesos con privilegios de administrador de diversos centros hospitalarios de Estados Unidos, Canadá, Francia y Reino Unido, por un precio inicial de entre 3 000 y 5 000 dólares. Asimismo, también se ha identificado la venta de accesos a compañías biotecnológicas y farmacéuticas, destacando en este caso empresas del sudeste asiático.

Si incluimos en el sector sanitario a plataformas web médicas, a entidades tecnológicas con dedicación exclusiva a la industria sanitaria y a empresas farmacéuticas y biotecnológicas, los casos de brechas de datos y ventas de accesos se disparan. En parte, es debido a que los actores de amenazas se enfocan más en este tipo de entidades por la rentabilidad que puede dar la venta de sus datos e información, así como también diversos grupos cibecriminales se encuentran alineados en no realizar acciones cibernéticas contra Hospitales y centros médicos.

En cuanto a las consecuencias de las 2 ciberamenazas expuestas, brechas de datos y venta de accesos se distinguen por tener una potencial mayor afectación sobre los ciudadanos, específicamente el paciente. En este tipo de ciberincidentes, además de comprometerse credenciales de acceso, también se vulnera información médica, historias clínicas y datos bancarios, lo cual supone una amenaza para la persona afectada y a la cual se debe de dar aviso para que tome las medidas de protección más adecuadas.

Construcción

La industria de la construcción representa uno de los pilares fundamentales de la economía a nivel mundial, representando una de las áreas en mayor crecimiento y estímulo de algunas de las principales economías mundiales, como la Unión Europea.

S21SEC

En la Unión Europea, el sector proporciona 18 millones de puestos de trabajo directos y aporta alrededor del 9% del PIB de la UE.

Esto hace que el sector de la construcción se haya convertido en uno de los principales objetivos de grupos cibercriminales, especialmente de grupos de ransomware que buscan un beneficio económico, y grupos APT destinados al ciberespionaje.

RANSOMWARE

Una de las principales amenazas contra el sector de la construcción ha sido el peligro que entrañan los ataques de tipo ransomware. Durante el último semestre el sector de la construcción ha sido uno de los sectores más impactados por este tipo de ataques, habiendo sufrido un total de 95 ataques.

Entre los grupos de ransomware más activos contra organizaciones del sector destacan:

LOCKBIT

Los ataques de Lockbit durante el primer semestre de 2022 se han centrado en organizaciones localizadas en Estados Unidos, con incidentes tan relevantes cuyas pérdidas ascienden a millones de dólares a causa de las disrupciones en sus servicios y de la importancia de la información filtrada.

CONTI

Uno de los actores de amenaza más activos en la primera mitad de 2022 en impactar contra organizaciones del sector de la construcción, localizadas sobre todo en EE.UU. Destacan la infección a una empresa dedicada al desarrollo de materiales en la construcción que se encuentra entre las 500 compañías más influyentes de Oriente Medio.

BLACKCAT (ALPHV)

Lanzado en noviembre de 2021, se ha distribuido a través de *emails* en inglés, permitiendo que el malware se extienda a todo el mundo, afectando a organizaciones de distintos sectores y países como Australia, Francia, India, Alemania, Italia, España, UK, EE.UU. y Bahamas. Sus ataques contra el sector de la construcción se han centrado principalmente en corporaciones de Estados Unidos.

CIBERESPIONAJE

Con respecto a las campañas de ciberespionaje dirigidas contra el sector de la construcción, el principal riesgo de ciberseguridad para organizaciones de la industria lo protagonizan las campañas APT.

Estos ataques se caracterizan por el uso de un amplio abanico de técnicas avanzadas diseñadas para el robo de información confidencial de las organizaciones.

El seguimiento de las campañas de APT contra el sector muestra el creciente interés de los actores de amenaza con patrocinio chino contra organizaciones del sector. Destacan las campañas de las APT:

01

APT20

También conocida como Twivy, explota el compromiso de webs estratégicas por parte alojadas en sitios web que tratan temas como la democracia, los derechos humanos, la libertad de prensa, las minorías étnicas en China y otros temas.

02

APT24

Conocida como PittyTiger, su objetivo son organizaciones en países como EE.UU. y Taiwán. Explota la utilidad de archivo RAR para cifrar y comprimir datos robados antes de transferirlos fuera de la red. El robo de datos extraído de este actor se centra en documentos con importancia estratégica, lo que sugiere que su intención es controlar los movimientos de varios estados sobre cuestiones aplicables a la disputa territorial o de soberanía en curso de China.

03

APT31

Este actor de ciberespionaje chino está centrado en obtener información que pueda proporcionar al gobierno y a las empresas estatales ventajas políticas, económicas y militares. APT31 ha explotado vulnerabilidades en aplicaciones como Java y Adobe Flash para comprometer los entornos de las víctimas.

S21SEC

Móvil

Los teléfonos móviles se han convertido en uno de los principales objetivos de los cibercriminales, y como viene ocurriendo en los últimos años, en los primeros seis meses de 2022 se ha producido un aumento de la actividad del malware móvil.

S21SEC

Cabe destacar que el malware dirigido a usuarios de teléfonos móviles se distribuye principalmente mediante cuatro vías:

Ataques de *smishing* donde los cibercriminales suplantan la identidad de aplicaciones, entidades bancarias o empresas de mensajería.

Estos mensajes incluyen un enlace a una página fraudulenta en la que se pedirá al usuario información personal para el robo de credenciales, o una URL que dirige a una página en la que se descargará un malware.

Utilización de *pop-ups* o anuncios en páginas web en los que se insta a los usuarios a descargar una aplicación.

Se han observado muchos casos en los cuales los cibercriminales instan a instalar falsas actualizaciones de *software* comunes, como Adobe Flash Player o antivirus.

Los mercados no oficiales de aplicaciones se tratan de uno de los principales lugares de distribución de *malware*.

En estos mercados aparecen numerosas aplicaciones con apariencia legítima, e incluso se tratan de una copia de la aplicación real, pero a la que los actores han añadido código malicioso.

Mercados oficiales como Google Play o Apple Store

Aunque cuentan con medidas de seguridad internas para evitar que existan aplicaciones con código malicioso disponibles para descarga, aún se encuentran casos en los que una aplicación con apariencia legítima se trata en realidad de una aplicación que contiene algún tipo de *malware*.

DENTRO DE LOS ATAQUES A TELEFONÍA MÓVIL DESTACAN LOS SIGUIENTES:

PEGASUS
Spyware

XENOMORPH
Troyano bancario

FLUBOT
Malware

S21SEC

PEGASUS

El spyware Pegasus, desarrollado por la empresa de seguridad israelí NSO Group, ha tomado relevancia los últimos 3 años por su uso contra miembros de gobiernos estatales y autonómicos, así como contra periodistas, ciudadanos de relevancia y personal diplomático. El objetivo de este malware es el de espionaje.

La explotación de las tres vulnerabilidades permitía a los atacantes infectar el dispositivo cuando el usuario accede a la URL enviada previamente por los atacantes a través de un ataque de smishing. Estos mensajes enviados tanto como SMS o como mensaje en redes sociales, utilizaban como señuelos avisos de aerolíneas y de instituciones públicas.

Una vez el usuario accede a la URL maliciosa, el software malicioso lleva a cabo acciones para ejecutar los exploits y proceder a realizar un ataque de jailbreak. Una vez el ataque jailbreak se ha realizado, el paquete de software espía se instala automáticamente.

Tras su instalación, el spyware compromete las aplicaciones previamente instaladas por el usuario para la recopilación de información y datos. A través de la técnica de hooking, Pegasus puede modificar el comportamiento de aplicaciones y sistemas operativos.

Pegasus también es capaz de comprometer dispositivos Apple con el envío de falsas imágenes en formato GIF a través de la aplicación iMessage.

Para esta infección, los atacantes utilizan exploits del tipo zero-click y aprovechan vulnerabilidades en el analizador de CoreGraphics PDF.

XENOMORPH

Xenomorph es un troyano bancario de Android descubierto por primera vez en febrero de 2022, distribuido con el nombre de aplicación FastCleaner, disfrazándose de aplicación legítima.

Tras la instalación de la aplicación, se solicita al usuario una ventana en la que se le pide que dé permisos de servicio de accesibilidad a la aplicación FastCleaner. El permiso de servicios de accesibilidad solo debe utilizarse para ayudar al desarrollo de aplicaciones para usuarios con discapacidades.

Cuando la instalación de FastCleaner se completa finalmente y el usuario ha habilitado los servicios de accesibilidad, la aplicación parece no tener ningún comportamiento. Si un usuario intenta abrir la aplicación, esta simplemente devuelve al usuario a la pantalla de inicio y, si el usuario intenta desinstalar la aplicación, la ventana emergente para confirmar si el usuario quiere desinstalarla se cierra automáticamente.

Tal y como ocurre con otros troyanos bancarios para Android, cuando el usuario abre su aplicación bancaria, el *malware* Xenomorph realizará un ataque de *overlay*, superponiendo una página falsa que suplanta a la página de acceso del banco, con el objetivo de que las víctimas introduzcan sus claves de inicio de sesión.

Los ciberdelincuentes utilizarán estas claves de inicio para acceder a la cuenta y proceder al robo de dinero.

FLUBOT

Descubierto en diciembre de 2020 y con una importante expansión en los dos últimos años, Flubot se distribuía mediante mensajes de texto SMS, suplantando a diferentes entidades con el objetivo de difundir enlaces maliciosos donde se descargaba el malware como falsos programas de rastreo de envíos de paquetería u otros servicios.

Los operadores de FluBot utilizan mensajes SMS que afirman contener enlaces a correo de voz, notificaciones de llamadas perdidas o alertas sobre la entrada de dinero de una transacción financiera desconocida.

Los enlaces en estos mensajes llevan a la víctima a un sitio web que aloja la APK de FluBot, que las víctimas deben descargar e instalar para conocer los detalles de la transacción.

Una vez descargada, la aplicación solicita a las víctimas ciertos permisos, como acceder a datos de SMS, administrar llamadas telefónicas y leer la libreta de direcciones del usuario.

Los actores de amenazas utilizan la lista de contactos de la víctima para enviar un SMS con un mensaje que contiene un enlace malicioso.

Debido a que estos mensajes provienen de una fuente conocida, es más probable que los destinatarios los abran e infecten sus dispositivos.

El pasado mes de mayo, la infraestructura detrás de Flubot fue desactivada por la policía holandesa y a principios del mes de junio la Europol anunció la eliminación total del *malware* para Android Flubot.

Las autoridades policiales europeas detallaron cómo la operación policial internacional habría involucrado a once países con el objetivo de desmantelar al *malware*.

APT

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.

S21SEC

Su actividad se basa en la persistencia, buscando permanecer sin ser detectados por períodos prolongados de tiempo.

Las actividades de las APT se desarrollan en el marco de eventos sociopolíticos estratégicos, así como en escenarios geopolíticos determinados.

En este sentido, las principales actividades de APT durante el primer semestre de 2022 han estado enmarcadas por diferentes escenarios estratégicos en curso, como han podido ser la puja por el liderazgo internacional chino o la invasión rusa de Ucrania.

Entre un amplio número de amenazas, un conjunto de ellas ha protagonizado los incidentes y campañas más significativas en los primeros meses de 2022.

APT Rusas

Los grupos de Amenazas Persistentes Avanzadas (APT) de origen ruso han mantenido una actividad destacable por sus acciones anteriores a la invasión de Ucrania y en el marco del conflicto entre Rusia y Ucrania.

APT Chinas

Durante los últimos meses, se ha observado cómo las APT chinas han protagonizado algunos de los principales incidentes y campañas internacionales en el panorama de amenazas cibernéticas.

Emotet

En los primeros meses de 2022, se ha registrado un importante aumento de las amenazas informáticas, derivadas del regreso del *malware* Emotet.

S21SEC

APT Rusas

A raíz de la monitorización y detección de actividad en el primer semestre de 2022, se considera que la distribución de los denominados Wiper por parte de APT rusas, entre objetivos estratégicos de países europeos y estados que conforman la OTAN, ha supuesto una de las principales amenazas para infraestructuras críticas debido a su potencial destructivo en el plano cibernético.

El escenario del conflicto militar entre Rusia y Ucrania ha supuesto un incremento de la actividad cibernética de las APT rusas como APT28, APT29 y Gamaredon, distribuyendo campañas de infección con malware destructivo y de ciberespionaje.

Asimismo, desde las APT rusas como Turla o DoppleSpider, conocidas por su actividad en tareas de ciberespionaje y extorsión, se ha obtenido información limitada lo cual podría demostrar la opacidad de su actividad, aunque no se descarta que sus acciones se hayan visto limitadas por motivos internos del grupo.

En este sentido, desde S21sec se destaca la actividad del grupo APT28 (Fancy Bear, Strontium, Pawn Storm, Sednit, Tsar Team, Iron Twilight, Sofacy). A continuación, se muestran algunas características identificadas del grupo:

El origen de las actividades de la APT 28 se remonta al año 2007-2008, cuando se identificaron diversos ataques informáticos con distribución de malware para tareas de ciberespionaje en el marco del conflicto de Rusia y Georgia.

Actúa como un ente patrocinado por un Estado (Rusia, en este caso) y se atribuye a personal de la unidad militar 26165 de El Directorio Principal del Alto Estado Mayor de las Fuerzas Armadas de la Federación de Rusia.

La motivación principal de la APT 28 en sus acciones se enfoca en obtener información privilegiada y confidencial de sectores estratégicos del país o industria objetivo por motivos geopolíticos.

Asimismo, no se ha identificado la existencia de motivación económica.

S21SEC

Los objetivos del actor de amenazas en cuestión se distinguen por ser de alto nivel estratégico como el aeroespacial, gubernamental, tecnológico y energético, entre otros.

Su actividad durante 14 años ha derivado en ciberataques contra entidades gubernamentales de países alineados con la Unión Europea y la OTAN, destacando sus últimas acciones en el marco del conflicto ruso-ucraniano con la distribución de campañas de phishing con malware destructivo y de ciberespionaje.

El grupo APT 28 se caracteriza por el uso de varios *malware* desde 2008 en los que ha implementado mejoras constantes con el objetivo primordial de que los sistemas de la víctima no puedan detectar la ejecución y presencia del *malware*.

En cuanto al impacto de estos ataques informáticos se considera de alto riesgo para las entidades objetivo debido a la capacidad de la APT 28 de evadir defensas y ganar persistencia, la capacidad de exfiltrar información confidencial, la recopilación de credenciales y accesos, así como la difusión de malware en sistemas críticos.

Ante las capacidades de las APT rusas y sus últimas acciones en escenarios de disputas geopolíticas, se estima probable que su actividad se mantenga a alto nivel con potenciales ciberataques pudiendo diversificar sus TTP, lo cual supondría un riesgo para infraestructuras las críticas objetivo.

S21SEC

APT Chinas

A estos actores de amenaza se les atribuye patrocinio del estado nacional chino, que ofrece recursos y apoyo para que se lleven a cabo actividades de intrusión, espionaje y sabotaje contra diferentes objetivos estratégicos para el país.

Con importantes campañas a lo largo de los últimos años, en el primer semestre de 2022 han ampliado sus objetivos aprovechando el escenario de amenazas internacionales, la explotación de nuevas vulnerabilidades y el uso de nuevas tácticas para llevar a cabo ataques sobre importantes organizaciones de todo el mundo.

MAYO

Diversos actores vinculados a China han sido identificados explotando la vulnerabilidad Follina (CVE-2022-30190) de la herramienta de diagnóstico de soporte de Microsoft (MSDT) contra organizaciones en diferentes países, entre los que se encuentran Bielorrusia y Rusia, así como la región del Tíbet.

Entre los actores de amenazas explotando la vulnerabilidad, se ha identificado a las APT chinas Twisted Panda y TA413.

JUNIO

Expertos en ciberseguridad identificaron una actividad presuntamente atribuida a la APT con patrocinio estatal chino, BackdoorDiplomacy (CloudComputating), que explotaba la misma vulnerabilidad en campañas de phishing dirigidas contra Arabia Saudí.

La cadena de infección primero cargaba un archivo HTML que contiene el exploit Follina de una infraestructura comprometida asociada con la universidad de Arabia Saudí Effat University y finalmente recuperaba una carga útil secundaria, el backdoor personalizado del grupo, Turian.

S21SEC

En este semestre, además, las APT chinas han desarrollado diferentes códigos maliciosos con el objetivo de perpetrar ataques contra objetivos determinados.

En este periodo, por ejemplo, se ha descubierto que el malware WinDealer, difundido por la APT LouYu, tiene la habilidad de introducirse a través de un ataque man-on-the-side.

Este innovador desarrollo permite modificar el tráfico de red en tránsito para insertar cargas útiles maliciosas.

Estos ataques son especialmente peligrosos y nocivos porque no requieren de ninguna interacción con el objetivo para que la infección tenga éxito.

Además de la explotación de vulnerabilidades y el uso de nuevos códigos maliciosos, las APT chinas han diversificado su actividad, introduciéndose en la realización de estafas sofisticadas de robo de criptomonedas que utilizan tácticas de ingeniería social para atraer a las víctimas de las aplicaciones de citas (apps) a las plataformas fraudulentas.

Este tipo de campañas han sido llevadas a cabo por grupos APT chinos como APT41, que en los últimos meses han participado en delitos cibernéticos motivados financieramente, como el robo de criptomonedas.

Emotet

Esta amenaza que se propaga a través de correos electrónicos maliciosos (*malspam*) con campañas masivas de infección, regresó a su actividad después de los intentos por interrumpir su operación el año pasado.

Tras un cese de actividad de varios meses, desde principios de 2022 sus operaciones se han multiplicado exponencialmente.

- Sus operadores han llevado a cabo constantes campañas de malspam en América Latina (con especial afectación a México) y Europa (con actividad en países como Italia o Alemania) en el primer trimestre de 2022.
- Por las características de sus campañas y los mecanismos que utiliza para distribuirse, Emotet ha diversificado el uso de downloaders, y del uso de amenazas a través del correo electrónico (principalmente phishing).
- En estas nuevas operaciones, se ha hecho uso de señuelos tan diversos como las notificaciones electrónicas de presuntas facturas bancarias o la felicitación de eventos sociales y festivos.

^

Este programa malicioso se distribuye a través de correos electrónicos con un archivo de Excel o Word con macros (o como un archivo Zip protegido por contraseña que contiene dicho archivo).

^

Recientemente, se han detectado casos en los que se descargan archivos maliciosos de Excel y Word a través de enlaces en el cuerpo del correo o a través de enlaces que fingen contener instaladores de aplicaciones Windows.

S21SEC

THREAT LANDSCAPE REPORT

Primer semestre 2022

Medios de Comunicación

La industria de los medios de comunicación y el entretenimiento es uno de los principales sectores estratégicos para los diferentes países y un área comercial en crecimiento que acumula millones de euros en ganancias en todo el mundo.

S21SEC

Este papel clave ha convertido a las organizaciones de la industria en uno de los principales objetivos de ciberataques para actores de amenazas, actores cibernéticos con patrocinio estatal, cibercriminales y hacktivistas que buscan visibilidad.

En el primer semestre 2022, este sector ha experimentado un aumento en el número de ciberamenazas, actividades maliciosas e incidentes contra sus sistemas informáticos. Algunos de los principales incidentes contra medios de comunicación e industria audiovisual han sido:

ATAQUES RANSOMWARE

ATAQUES DE GRUPOS DE DELINCUENCIA

ATAQUES DE COLECTIVOS HACKTIVISTAS

ATAQUES RANSOMWARE

Los ataques ransomware contra la industria de los medios de comunicación han aumentado exponencialmente durante el primer semestre del año, con incidentes internacionales de gran relevancia, como el ataque contra uno de los periódicos financieros más grandes del mundo en el mes de mayo.

Diferentes grupos de ransomware han estado detrás de estos ataques, como por ejemplo Everest o Conti, que han filtrado información de sus víctimas.

S21SEC

ATAQUES DE GRUPOS DE DELINCUENCIA

Los grupos de ciberdelincuencia también han protagonizado ataques contra medios de comunicación en la primera mitad del año, con ataques significativos.

En enero de este año, un grupo de medios de comunicación portugués, poseedor de canales de televisión y periódicos, fue víctima de un ciberataque por parte del grupo Lapsus$, en el cual los ciberdelincuentes habrían obtenido información privada que filtrarían si no recibían un rescate.

Además, también realizaron acciones de defacement, un tipo de ataque dirigido a un sitio web, caracterizado por modificar la apariencia visual de una página web.

ATAQUES DE COLECTIVOS HACKTIVISTAS

En el primer semestre del año, la industria de los medios de comunicación ha sido una de las principales afectadas por los ataques perpetrados por colectivos hacktivistas, especialmente en el marco de la invasión rusa a Ucrania.

Tanto medios rusos como medios ucranianos han sido víctimas de la acción de colectivos hacktivistas organizados que han utilizado los ataques para un amplio abanico de actividades con motivación política: interrumpir servicios, distribuir contenido fraudulento o propagandístico o robar información.

Desde ataques de intrusión y sabotaje, hasta actividades de desfiguración, los medios de países involucrados en el conflicto armado se han convertido en objetivos de estos colectivos.

Algunos de los ataques más relevantes incluyen el hackeo a la televisión rusa y el proveedor de contenido en vídeo RuTube o la compañía estatal de radiodifusión y televisión de toda Rusia.

THREAT LANDSCAPE REPORT

Primer semestre 2022

Telecomunicaciones

El inicio de la guerra de Ucrania ha supuesto la proliferación de diversos ataques a la infraestructura crítica y empresas del sector.

S21SEC

Durante el mes de mayo, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y la Oficina Federal de Investigaciones (FBI) hizo pública la atribución de diversos ciberataques ocurridos a finales del mes de febrero contra redes comerciales de comunicación por satélite, a actores de amenazas patrocinados por el estado ruso.

Según la evaluación, Rusia habría lanzado ataques cibernéticos a finales de febrero contra redes comerciales de comunicaciones satelitales que afectaron al servicio de banda ancha satelital Viasat KA-SAT para el borrado de los módems SATCOM, con la finalidad de interrumpir las comunicaciones en Ucrania durante la invasión.

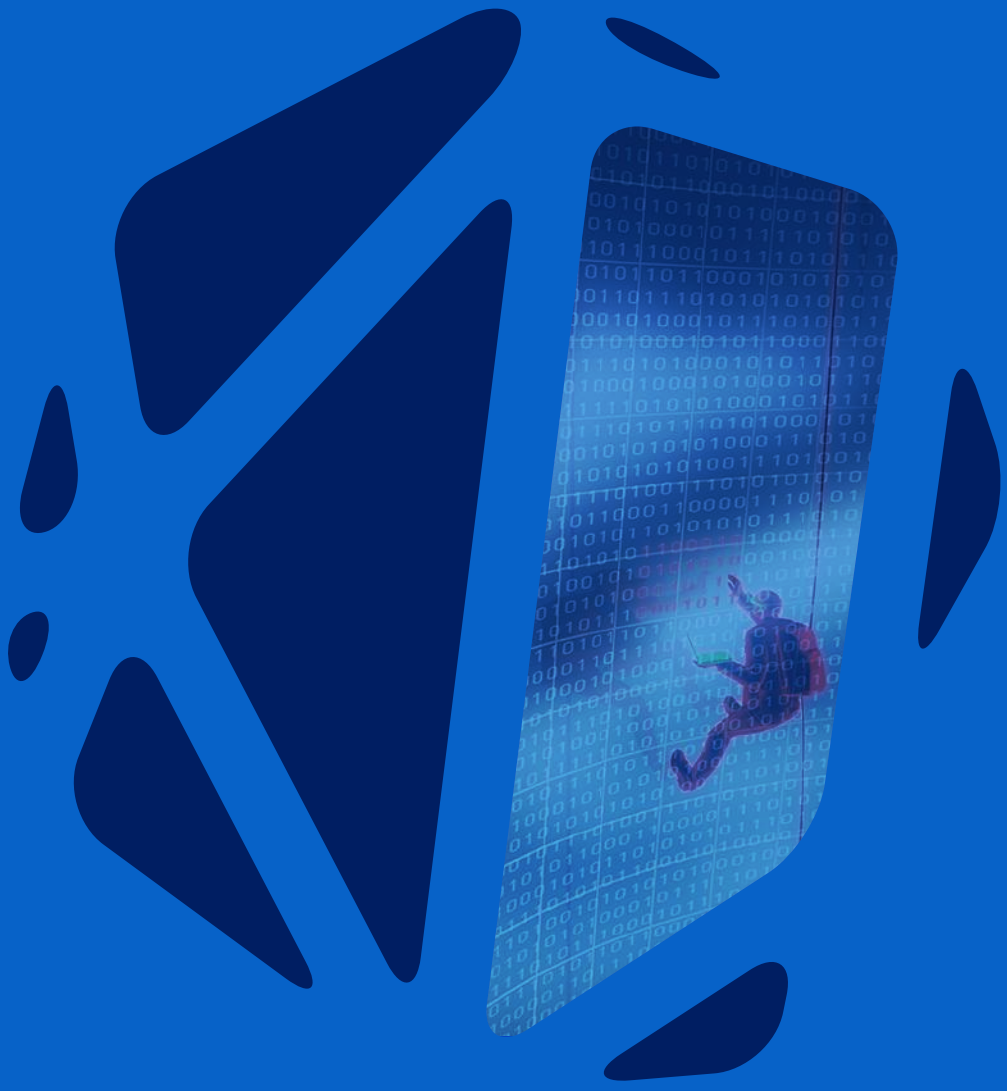
Los ataques impactaron de manera indirecta en otros países europeos, provocando que terminales en Ucrania y en toda Europa se vieran inoperativas y afectando a los servicios e infraestructura que soportan turbinas eólicas y brindan servicios de Internet.

Las amenazas cibernéticas a las redes de comunicación por satélite a nivel internacional pueden suponer riesgos en los entornos de los clientes y proveedores de redes.

En la situación geopolítica actual y el escenario cibernético de guerra híbrida, las organizaciones de infraestructura crítica y otras organizaciones que son proveedores o clientes de la red SATCOM han de aumentar sus defensas de ciberseguridad.

S21SEC

Brechas de Datos



Durante el primer semestre de 2022, en el caso de los incidentes de seguridad que han derivado en brechas de datos debido a la naturaleza de la exposición de la información, responden principalmente a motivaciones económicas por parte de los ciberdelincuentes, quienes pretenden obtener un beneficio por la información extraída de las víctimas.

S21SEC

Las principales técnicas utilizadas son la ingeniería social, ataques de fuerza bruta, relleno de credenciales, malware u otro tipo de ataques.

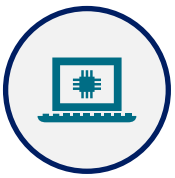
Entre los datos comprometidos en las brechas de datos durante el primer semestre, destacan información personal (nombres completos, direcciones, correos electrónicos, números de teléfono, etc.).

Entre las principales brechas de datos por sectores afectados destacan las siguientes:

ENERO

La organización internacional Cruz Roja, fue víctima de un ciberataque que expuso datos e información personal de más de medio millón de personas. Los datos procedían de al menos 60 sociedades de la Cruz Roja y de la Media Luna Roja a nivel mundial. Según los datos oficiales, el ataque tenía como objetivo, a una empresa externa en Suiza que el CICR contrata para almacenar datos.

FEBRERO



Operador croata de telefonía, 'A1 Hrvatska, fue víctima de un incidente de seguridad tras el cual, se vio expuesta información confidencial que afecta a aproximadamente 200.000 clientes. De entre la información accedida se incluyen nombres completos, números de identificación personal, direcciones físicas y números de teléfono.

T-Mobile, proveedor de telecomunicaciones estadounidense, reveló que un atacante desconocido obtuvo acceso a la información de la cuenta de los clientes, incluida la información personal y los números de identificación personal (PIN), añadiendo que un número desconocido de clientes aparentemente se vieran afectados por ataques de SIM swapping.

MARZO

Ikea Canadá confirmó que en el mes de marzo habría sufrido una brecha de datos que involucra información personal de aproximadamente 95,000 clientes.

S21SEC

ABRIL

La empresa multinacional Coca Cola en el mes de abril comenzó la investigación de una brecha de datos a gran escala supuestamente llevada a cabo por parte del grupo Stormous. El grupo de publicó en su sitio web esta semana que había pirateado con éxito los servidores del gigante de los refrescos y robado 161 GB de datos. También ofreció los datos a la venta por más de 64 000 dólares, o 1,6467 bitcoins.

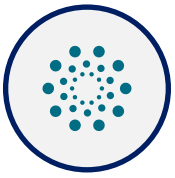
El fabricante de automóviles estadounidense General Motors reveló haber sido víctima de un ataque de relleno de credenciales ocurrido en abril, que expuso la información de algunos clientes y permitió a los piratas informáticos canjear puntos de recompensa por tarjetas de regalo.

MAYO

La Asociación de Bancos del Perú (Asbanc) alertó sobre una posible filtración de datos personales de un organismo público peruano, que estarían siendo comercializados a través de redes sociales, como Facebook, WhatsApp y Telegram.

En mayo de 2022, una auditoría estatal reveló una fuga de datos en el Departamento de Seguros de Texas, que comprometió a 1,8 millones de personas. Los datos en cuestión, incluidos los números de seguro social y otra información personal confidencial, estuvieron ampliamente disponibles en el sitio web del departamento desde marzo de 2019 hasta enero de 2022.

JUNIO



La farmacéutica Novartis sufrió una brecha de datos tras un incidente de seguridad llevado a cabo por el grupo de amenazas Industrial Spy, un colectivo que cuenta con un mercado en la *deep web* en el que pone a la venta información extraída en sus ataques. En este caso, el grupo menciona haber obtenido 7.7 MB de información.

S21SEC

S21SEC

www.s21sec.com