S21 SEC

Threat Landscape Report

Primer semestre 2020

Introducción

El año 2020 arrancó con un hecho relevante para la ciberseguridad global que comenzó con un conflicto geopolítico. El ataque con drones de Estados Unidos ocurrido el 3 de enero contra el Aeropuerto Internacional de Bagdad, que llevó al fallecimiento del general Qasem Soleimani, aumentó las tensiones entre ambos países. A principios de enero, Estados Unidos publicó en su boletín de seguridad de amenazas terroristas, que Irán se conformaba como un actor que amenazaba a la seguridad nacional, destacando el ámbito del ciberespacio, debido a la preparación y las capacidades de los grupos de cibercriminales apoyados por el estado y que podrían llevar a cabo acciones contra objetivos americanos.

Sin duda, el 2020 ha estado muy marcado también por otro evento, en este caso sociosanitario: la COVID 19. La pandemia con afectación mundial no solo ha llevado a las empresas a tener que optar por el teletrabajo, aumentando sus riesgos a nivel de ciberseguridad, sino que también los actores maliciosos han aprovechado el miedo y la incertidumbre ante esta nueva enfermedad para lanzar campañas de fraude, malware o phishings.

Durante los 6 primeros meses de 2020 se ha observado un aumento en las campañas de malware, debido principalmente a la pandemia. Desde S21sec, se han analizado casi 400.000 muestras más de malware con respecto al mismo periodo en el año anterior.

En concreto, en cuanto a la actividad de los operadores de ransomware, se ha observado también un aumento de los ataques de este tipo de malware. Tal como predijo el equipo de S21sec en el Threat Landscape Report del segundo semestre de 2019, los operadores de ransomware tenderían cada vez más a realizar también extorsiones a sus víctimas, amenazándoles con la publicación de los datos obtenidos en el ataque para que realicen el pago del rescate. Durante este periodo, se ha observado un aumento del número de grupos que publican sus datos en blogs de la Deep Web, como Nefilim, Nemty, Ako, REvil, Clop, Maze, Dopplepaymer, Sekhmet, Ragnar o Netwalker, entre otros.

Índice

Muestras de Malware

Análisis realizado por el departamento de Cyber Threat Intelligence de S21sec de todas las muestras de malware durante el primer semestre del año.

Estas muestras se encuentran desglosadas según el periodo de estudio y la familia a la que pertenecen.

Total muestras analizadas

Muestras con familia de malware y sin familia de malware

ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO
233.902 muestras	219.011 muestras	184.385 muestras	220.745 muestras	227.182 muestras	222.887 muestras

AGRUPACIÓN DE MUESTRAS POR FAMILIA

COBALT 991 muestras	BUBLIK 1111 muestras	HAWKEYE 1113 muestras	NJRAT 1761 muestras	PONY 2413 muestras	NANOCORE 3204 muestras	TRICKBOT 3641 muestras	ENCRYPTED-URL 5014 muestras	FEODO 13.451 muestras	ENERO
HAWKEYE 1072 muestras	TUSCAS 1165 muestras	BUBLIK 1297 muestras	NJRAT 2300 muestras	ENCRYPTED-URL 2039 muestras	FEODO 2185 muestras	TRICKBOT 2574 muestras	NANOCORE 3522 muestras	DRIDEX 4694 muestras	FEBRERO
TINBA 276 muestras	FORMBOOK 357 muestras	FEODO 530 muestras	PONY 543 muestras	NANOCORE 608 muestras	QAKBOT 659 muestras	URSNIF 971 muestras	ENCRYPTED-URL 1145 muestras	TRICKBOT 1527 muestras	MARZO
NANOCORE 1009 muestras	GANDCRAB 1120 muestras	ENCRYPTED-URL 1519 muestras	ZEROACCESS 1925 muestras	NJRAT 2099 muestras	FEODO 2114 muestras	QAKBOT 4912 muestras	BUBLIK 5340 muestras	TRICKBOT 5827 muestras	ABRIL
ZEUS 1034 muestras	DRIDEX 1013 muestras	BUBLIK 1220 muestras	ENCRYPTED-URL 1241 muestras	NETWIRE 1282 muestras	PONY 1314 muestras	FEODO 1649 muestras	NJRAT 1790 muestras	QAKBOT 3080 muestras	MAYO
PONY 1158 muestras	AZORULT 1443 muestras	NANOCORE 1555 muestras	TRICKBOT 2593 muestras	NJRAT 2673 muestras	FORMBOOK 3225 muestras	REMCOS 3438 muestras	QAKBOT 3559 muestras	ENCRYPTED-URL 4493 muestras	JUNIO

Malware

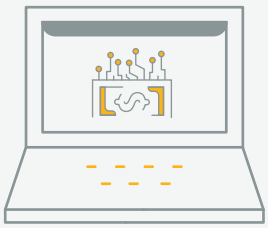
En el primer semestre de 2020 desde el equipo de Threat Intelligence de S21sec se ha detectado que uno de los malware más distribuidos durante este periodo es GuLoader, que será después utilizado para la distribución de otros malware como Formbook o Agent Tesla.

También, en este periodo cabe mencionar el aumento de los denominados bankers brasileños afectando a entidades bancarias de Portugal y España, como Grandoreiro o Casbaneiro.

GuLoader

GuLoader se encarga principalmente de la descarga de Troyanos de Acceso Remoto (RAT), como NanoCore RAT, Netwire RAT, Remcos RAT, Ave Maria/ Warzone RAT, además de Parallax RAT; y spywares como Formbook y Agent Tesla/ Origin Logger.

El funcionamiento más común de GuLoader consiste en almacenar los payloads del malware que va a descargar en algún almacenamiento en la nube, como Google Drive o Microsoft OneDrive. GuLoader funciona como un wrapper, decodificando una shellcode con la funcionalidad principal del downloader, la cual se encuentra cifrada empleando un XOR con una clave de 4 bytes (en la muestra analizada la clave era " =]Rk"). Además, hace uso de técnicas de inyección para dificultar el análisis.



Grandoreiro

Forma parte de un amplio grupo de malware especializado en este tipo de fraude que tiene su origen en Brasil y que llevan en desarrollo activo desde 2014, afectando mayoritariamente a entidades bancarias de Latinoamérica, Portugal y España.

Grandoreiro es un malware especializado en fraude bancario que combina funcionalidades de control remoto y técnicas de ingeniería social para realizar transferencias bancarias desde las aplicaciones web de banca electrónica una vez la víctima ha iniciado sesión en estas.

Malware COVID19

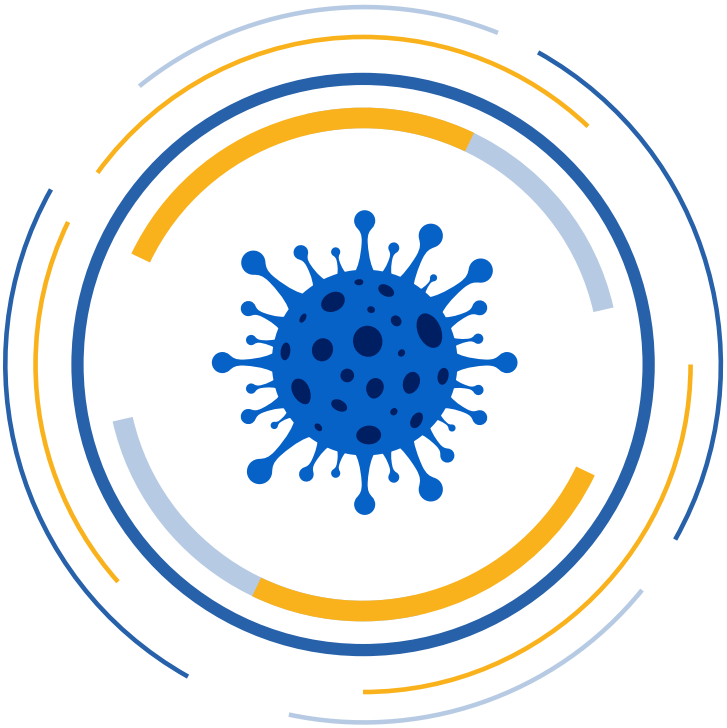
El malware ha aumentado en todas sus variantes durante el primer semestre de 2020, y ha estado estrechamente ligado con la pandemia de la COVID 19.

Los grupos de ciberdelincuentes han aprovechado el miedo de los usuarios, la incertidumbre ante las medidas de seguridad para hacer frente a la enfermedad, e incluso el aumento del trabajo en remoto para el desarrollo de sus campañas.

Durante este periodo, se han encontrado nuevos y antiguos malware de distintos tipos, distribuidos a través de técnicas como el phishing suplantando la identidad de organizaciones internacionales, haciéndose pasar por mapas de evolución de la pandemia, o incluso por empresas de correspondencia alegando la supuesta devolución de un paquete a causa de la crisis sanitaria.

Uno de los ejemplos que ilustran este uso de la COVID 19 para el despliegue de malware es el Covidlocker, malware que contiene el nombre de la enfermedad; o la campaña reciente de D-Dropper que utilizaba como cebo el coronavirus.

Desde el equipo de Threat Intelligence de S21sec se han ido realizando informes semanales titulados "Boletín semanal COVID-19" desde el pasado 20 de marzo, los cuales eran enviados cada viernes. En ellos, se aportaban aquellos nuevos malware que utilizaban el COVID 19 como cebo.



COVIDLOCKER

Es un ransomware de tipo Locker, ya que no llega a cifrar el dispositivo, si no que su funcionalidad consiste en impedir que el usuario pueda usar de forma normal su dispositivo, solo permitiéndole acceder a la aplicación maliciosa.

Este ransomware para Android era distribuido a través de un enlace a una página web fraudulenta (coronavirusapp[.]site) en la que se ofrecía una falsa aplicación para controlar el avance de la COVID-19 mediante un mapa de calor.
Al ser instalada y tras engañar a la víctima para que la añadiera como administrador del dispositivo y en los servicios de accesibilidad, procede a secuestrar el dispositivo, mostrando una nota de rescate que indica que éste ha sido cifrado.

D-Dropper

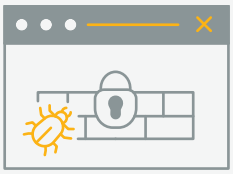
D-Dropper es normalmente distribuido en campañas que hacen uso de técnicas de ingeniería social camuflando el dropper como falsos documentos bancarios, facturas o pedidos. Sin embargo, durante el primer semestre de 2020 el equipo de Threat Intelligence de S21Sec ha detectado una nueva campaña de distribución asociada al COVID 19.

En esta campaña los archivos maliciosos presentaban nombres relacionados con la COVID 19 como: “COVID-19.jar”, “Covid19 Job Scheme.zip”, “Covid-19 Job Retention Scheme.jar”, “VACCINE FOR COVID-19.jar”, o “Coronavirus Job Retention Scheme.jar”. Además, en el caso de la distribución de este malware en España, se ha observado que el malware se ha encontrado alojado en una web vulnerada de una clínica.

Malware móviles

Tal como viene siendo tendencia en los últimos años, los actores maliciosos tienen entre sus objetivos principales dispositivos móviles o smartphones. El hecho de que la mayor parte de la población tenga un teléfono móvil desde donde realiza operaciones bancarias, compras por internet, y por donde se comunica con sus familiares y amigos hacen que estos dispositivos se conviertan en uno de los principales objetivos de los ciberdelincuentes.

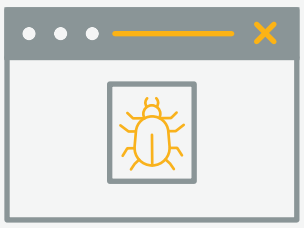
Durante los primeros seis meses de este año, se ha visto un aumento de la actividad del malware móvil para Android destinado al robo de credenciales bancarias. Si bien los troyanos Cerberus y Ginp ya habían sido observados durante el año 2019, en estos primeros seis meses de 2020 han utilizado nuevas técnicas y han mejorado sus funcionalidades.



Cerberus

En el mes de marzo de 2020 se descubre una nueva versión de este malware bancario para Android, que permite a un atacante acceder a todo el contenido del dispositivo infectado.

Aparte de las funcionalidades de malware bancario con las que contaba el año pasado, como el overlay, control de SMS o recolección de listas de contactos; en este periodo se han encontrado nuevas muestras de Cerberus actualizadas con funciones de RAT, que permiten al atacante desbloquear por completo el terminal y acceder a todas las cuentas, incluidas aquellas que utilicen los códigos 2FA generados por Google Authenticator (autentificación de dos pasos de Google). Esto se debe a que Cerberus se aprovecha de una vulnerabilidad en Google Authenticator, que permite la realización de capturas de pantalla a los códigos.



Ginp

Incluye funcionalidades de RAT y Spyware, mediante las cuales el atacante podría obtener los datos de los SMS del teléfono de la víctima, los datos de sus contactos y realizar envío de mensajes maliciosos desde el dispositivo de la víctima, entre otros.

Investigadores descubrieron a finales de octubre de 2019 el malware bancario para Android Ginp. Su funcionalidad principal como banker consiste en efectuar el robo de las credenciales bancarias de las víctimas.

Actualmente, y debido a la pandemia de la COVID-19, Ginp ha incorporado recientemente una nueva funcionalidad que aprovecha esta situación. Así, una vez que se descarga en el teléfono de la víctima, este troyano puede recibir una orden del atacante para abrir una página web titulada "Buscador de Coronavirus", que afirma que hay personas cercanas infectadas con el virus. Para saber dónde están estas personas, se le pide a la víctima que pague 0,75 euros. Si la víctima está de acuerdo, se le transfiere a una página de pago. Sin embargo, una vez que se han introducido los datos de pago, a la víctima no se le cobra esta suma ni recibe ninguna información sobre los "infectados". En cambio, la información de su tarjeta de crédito acaba de ser entregada a los ciberdelincuentes.

Ransomware

El primer semestre de 2020 ha sido, sin duda, el semestre del ransomware. Durante este periodo un gran número de empresas, entidades estatales, particulares e incluso organizaciones sanitarias han sido víctimas del ransomware.

Cronología

A continuación se observan algunos de los incidentes más notorios de ransomware durante este periodo

ENERO

La empresa de intercambio de divisas Travelex es atacada por el ransomware REvil / Sodinokibi. La cantidad del rescate alcanzó la cifra de 4.6 millones de libras. A pesar de las amenazas del grupo, los datos no han sido filtrados.

FEBRERO

La empresa australiana de logística Toll Group sufre el ataque del ransomware MailTo. Esta misma empresa será atacada en el mes de mayo por el ransomware Nefilim, grupo que ha filtrado los archivos del ataque en su blog de la Deep Web.

MARZO

La empresa Visser Precision, fabricante de piezas de grandes empresas como Tesla o Boeing sufrió el ataque de Dopplepaymer. Este grupo filtró los datos en su blog de la Deep Web.

ABRIL

TI Cognizant sufre el ataque del ransomware Maze. Ese mismo mes, la petrolera estatal de Portugal, EDP, sufre el ataque del ransomware Ragnar Locker. Ambas empresas han visto sus datos expuestos en la Deep Web.

MAYO

Uno de los despachos de abogados más grandes de Estados Unidos, Grubman Shire Meiselas & Sacks es atacado por REvil/Sodinokibi. El grupo subasta los datos de clientes del despacho como Madonna o Donald Trump, comenzando la apuesta en un millón de dólares. Este mismo mes, se produce un ataque a una de las empresas de soluciones bancarias más importantes, Diebold Nixdorf, por parte del ransomware ProLock.

JUNIO

La empresa de automoción japonesa Honda es víctima de un incidente de ransomware producido por el ransomware Snake. El mismo ransomware atacó un mes antes al grupo de hospitales Fresenius, y filtró la infomación robada en un paste en la Deep Web.

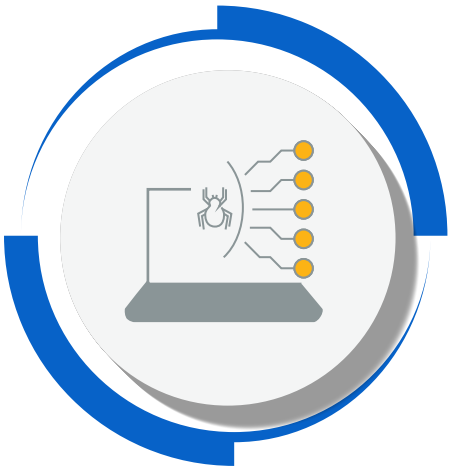
Este ransomware fue descubierto en septiembre de 2019. Sin embargo, debido al brote del coronavirus, los actores de Netwalker incrementaron su actividad durante las fechas del brote de la pandemia y lanzaron campañas de spam contra hospitales y empresas del sector sanitario. Dicha campaña llamó tanto la atención por las repercusiones que podría tener una infección de este tipo de malware en un hospital que incluso salió en los medios de comunicación.

El principal objetivo de los actores detrás de este ransomware es dirigir el ataque a empresas para cifrar el máximo número posible de equipos conectados a la red empresarial y de esta forma dejar inoperativa la organización y solicitar un precio de rescate más elevado que si solo se cifrara un equipo personal. Además de cifrar los archivos, los atacantes amenazan con hacer pública información sensible de las organizaciones afectadas en el caso de que las víctimas no paguen el rescate.

Ragnar Locker apareció por primera vez en diciembre de 2019. No obstante, últimamente ha ganado notoriedad tras el ataque realizado contra una gran empresa de Portugal. El modus operandi del grupo detrás de Ragnar Locker consiste en el hackeo y el compromiso de las redes de sus víctimas. Una vez consiguen acceso, proceden a descargar la mayor cantidad de datos confidenciales posibles, para después lanzar el ransomware que cifrará los archivos de la víctima.

Cabe destacar que, en la nota de rescate, además de indicar la cantidad que piden para el rescate de los archivos, tal y como están haciendo otras familias de ransomware, los actores detrás de Ragnar Locker están extorsionando a sus víctimas, siendo estas extorsiones en forma de amenaza, asegurando que en caso de que su víctima no pague el rescate, harán públicos los documentos robados en el ataque.

Nuevas tendencias de Ransomware

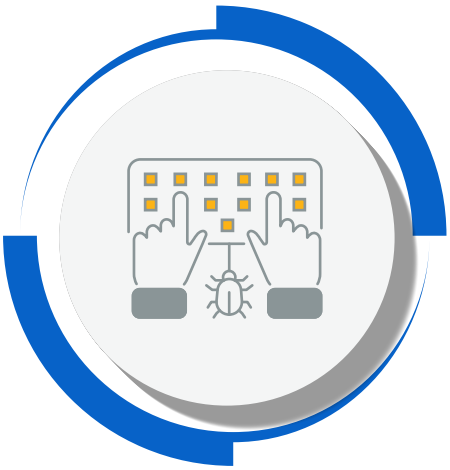


RANSOMWARE AS A SERVICE

Al alza

VARIOS ACTORES USAN DISTINTOS RANSOMWARE

Para aumentar sus beneficios



CREACIÓN DE BLOGS

Para la publicación de información

UNIÓN DE FUERZAS ENTRE OPERADORES DE RANSOMWARE

Creación del Cartel de Maze

MAXIMIZACIÓN DE LOS BENEFICIOS

REvil/Sodinokibi crea un sitio de subasta de información

OBJETIVOS CONCRETOS

Y más grandes

Hacktivismo

El panorama hacktivista internacional en estos últimos seis meses ha tenido una actividad relevante en el marco de las protestas que se han desarrollado en diversos países por motivos político- sociales. Estas protestas, debido a su difusión en redes sociales y su impacto en sectores poblacionales, han tenido la involucración de colectivos hacktivistas internacionales.

Los colectivos hacktivistas identificados, en su mayoría relacionados con el movimiento Anonymous, han construido o reactivado Operaciones con el objetivo de realizar ataques cibernéticos contra instituciones gubernamentales y organismos públicos supuestamente contrarios a movimientos de protesta, o por ser los supuestos responsables de alguna situación de inestabilidad.

Con el inicio del año 2020 colectivos hacktivistas ligados a Anonymous intensificaron sus acciones en diversas Operaciones, entre las que destacan:

#OpChile
#OpBolivia
#OpArgentina
#Op25Abril
#OpNicaragua

Por otro lado, otras operaciones también han experimentado un repunte momentáneo:

#OpCatalonia
#OpIsrael

De la misma forma, se destacan otras con menor incidencia:

#OpRussia
#OpHongKong

Una de las operaciones más recientes y la que está teniendo un repunte de considerable importancia se centra en objetivos estadounidenses en el marco de las protestas que se han llevado a cabo en Estados Unidos bajo el movimiento "Black Lives Matter". Esta operación se denomina con diversas etiquetas como:

#OpMinneapolis
#OpFloyd
#OpGeorgeFloyd

La activación de estas operaciones y la actividad en torno a las mismas ha incrementado la actividad del colectivo Anonymous a nivel mundial aumentando sus acciones y, por lo tanto, suponiendo una amenaza de alto nivel.

Las operaciones mencionadas responden a reivindicaciones distintas utilizando los medios tecnológicos para realizar acciones desestabilizadoras contra gobiernos, instituciones públicas y privadas. Tres de los casos más destacados son:

#OpChile
#OpNicaragua
#OpColombia

se ha observado una importante actividad hacktivista enfocada en difundir información sensible contra las instituciones objetivo y en realizar ataques cibernéticos, en su mayoría, de tipología DDoS y Desfiguración (defacement), así como publicar bases de datos de personal de estas instituciones.

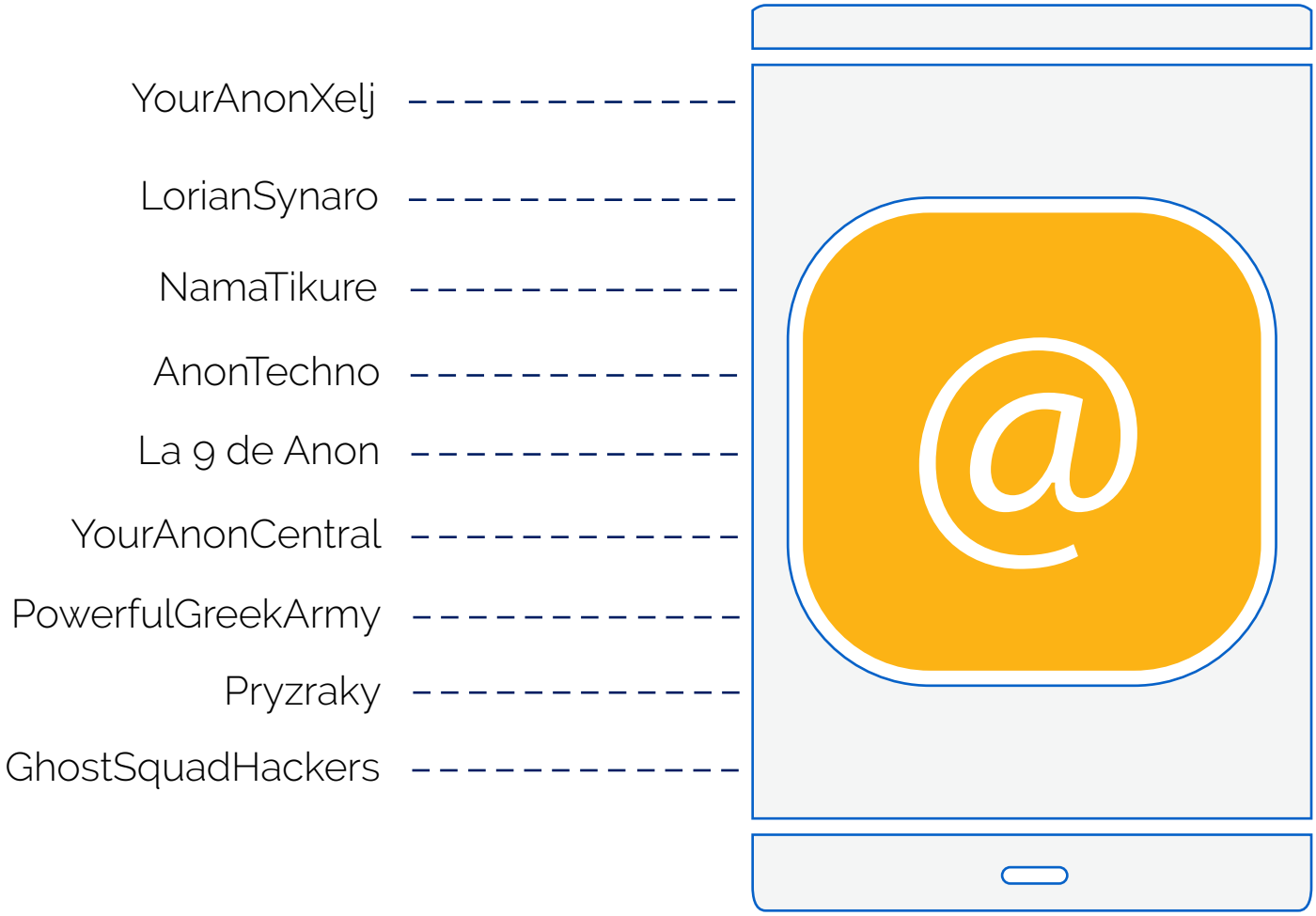
En cuanto a las operaciones relacionadas con Estados Unidos, estas han seguido el mismo patrón con la realización de ataques DDoS contra páginas web de organismos gubernamentales, exfiltración de información y la difusión de contenido multimedia que dañe la imagen de las instituciones o autoridades objetivo.

Por otra parte, las últimas operaciones reactivadas mantienen una baja incidencia:

#OpCatalonia
#OBolivia

Es posible que las mismas experimenten un repunte en caso de producirse nuevos movimientos de protesta relacionados con dichas operaciones.

Los actores/colectivos participantes en dichas operaciones han tenido una alta intervención a nivel internacional, tanto en la ejecución de ataques cibernéticos como en la difusión de información de estos últimos. Entre los actores/ colectivos hacktivistas más relevantes se encuentran los siguientes (activos en la mayoría de las Operaciones mencionadas).



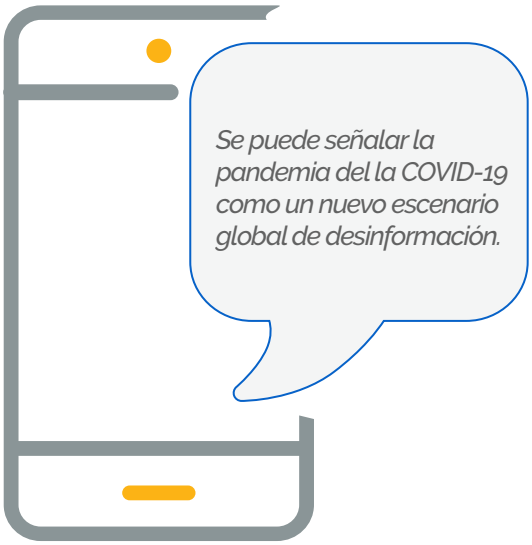
En este sentido, el hacktivismo se considera como una amenaza latente con una mayor actividad y con una capacidad notable de organización para la realización de ataques e inicio de operaciones a nivel internacional. Se estima muy probable el aumento de sus acciones aprovechando situaciones de inestabilidad social o política, publicando sus objetivos de ataque en plataformas como pastebin y hastebin (o compartiéndolos en privado) para después ejecutar los ataques informáticos correspondientes y con la difusión de información y contenido multimedia que pueda comprometer a sus objetivos.

Desinformación

Desde que en enero de 2020 comenzaran a conocerse los primeros casos de enfermedad por coronavirus, miles de noticias falsas y contenido desinformativo han empezado a difundirse a través de medios digitales, como portales de información, redes sociales, o servicios de mensajería, generando lo que la OMS ha denominado una "infodemia".

La desinformación sobre el virus ha sentado un nuevo precedente en cuanto a los riesgos sobre desinformación por su rápidez y alcance mundial.

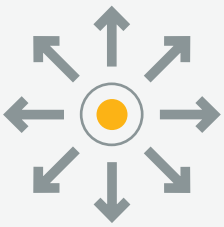
Si bien aún no es posible medir el impacto real de la desinformación durante la pandemia, empiezan a verse las consecuencias que dejan las fake news en la credibilidad de las autoridades y de los profesionales sanitarios, cuyas informaciones sobre salud pierden eficacia.



En este sentido, ya en 2019 un estudio elaborado por #SaludsinBulos en colaboración con Doctoralia demostró que el 67% de los profesionales sanitarios consideraban que los bulos de salud estaban minando su credibilidad entre los pacientes.

Los mensajes con contenido alarmista son los que primero consiguen impactar sobre los ciudadanos, aumentando el flujo de desinformación entre usuarios de nuevas tecnologías y erigiéndose como un potencial riesgo público.

Esta coyuntura ha unificado la generación de desinformación a escala mundial, pudiendo identificarse tendencias comunes en todos los países:



Carácter viral de los contenidos con un alto nivel de impacto.

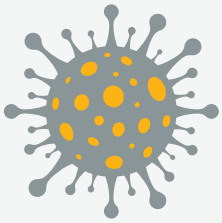
Homogeneidad en temas y mensajes.

Uso de nuevos canales de comunicación y difusión de este contenido desinformativo en plataformas como redes sociales o servicios de mensajería instantánea (que se suman a los portales de comunicación como nuevas fuentes de obtención de información en tiempo real).

Tipos del bulos

La amplia difusión que han tenido estos eventos desinformativos ha provocado que las autoridades hayan tenido que contrarrestar, de manera periódica, este tipo de contenidos, llegando a declarar todo este tipo de eventos como teorías de la conspiración con un importante impacto para la salud pública. Por ejemplo, instituciones médicas españolas han publicado diversas declaraciones sobre las teorías que vinculan las redes 5G de telefonía y la transmisión del coronavirus, después de que se extendieran las teorías que vinculaban ambos eventos.

Este tipo de riesgo cibernético es más complejo en cuanto a su análisis o naturaleza, con la dificultad añadida de identificar a los actores maliciosos detrás de su generación.



Desinformación referente al origen del coronavirus

Cuya veracidad permite hablar de bulos o fake news tan diversas como las que especulan que se trata de un arma biológica o de una estrategia de control de la población. Por ejemplo, en el servicio de mensajería instantánea WhatsApp, se replicaron diversos vídeos sobre la enfermedad: dos de los más difundidos tienen relación con el origen del coronavirus.

En el primero de ellos, unos comensales saborean sopa de murciélago y en el vídeo se comenta que en ese convite en Wuhan está el germen de la epidemia. Dicho vídeo es real pero antiguo y no corresponde a una cena en la región china: en realidad, se trata de una celebración en 2016 en una isla del Pacífico.

Desinformación sobre las formas de contagio y sus tratamientos

Como la supuesta existencia de vacunas en Rusia, que la cocaína cura los síntomas de la COVID-19 o que la lejía inyectada en vena combate el virus.

Desinformación atribuida a supuestos profesionales sanitarios

En esta pandemia han aparecido numerosos audios, vídeos o comunicados de falsos expertos que detallaban sus vivencias en centros médicos o aportaban soluciones falsas o no comprobadas que han supuesto un potencial riesgo para la salud, al incurrir en conflicto con lo planteado por autoridades científicas y sanitarias.

Desinformación sobre la gestión de la pandemia y de la crisis

Que ha mostrado particularidades en cada uno de los diferentes países. En México, se detectó una importante cantidad de desinformación relativa a las medidas adoptadas por el Gobierno, con diferentes grados de confinamiento que supuso compras masivas en supermercados.

Vulnerabilidades

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

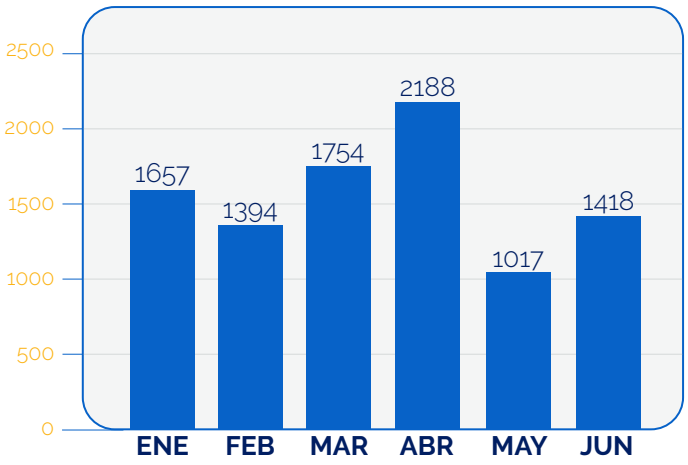
Nivel de criticidad de vulnerabilidades

Por tipo y por SO

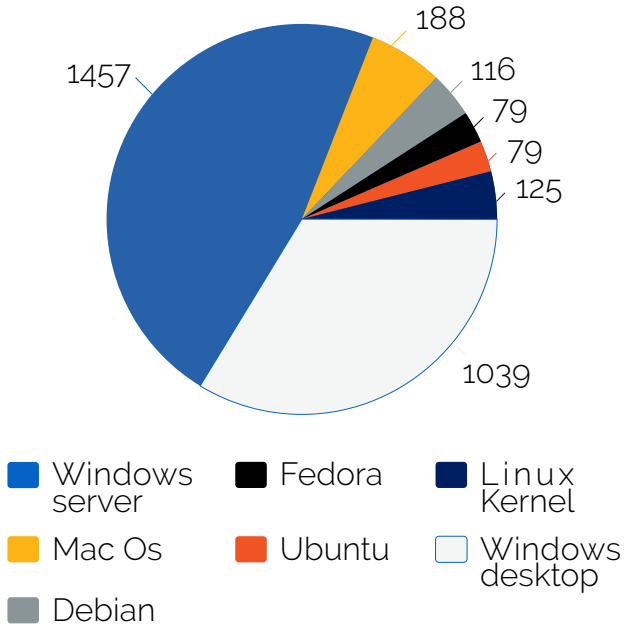
Durante el primer semestre de 2020 se han publicado 9428 vulnerabilidades.
A continuación, se presenta una visión global de las mismas.

- **Critical:** 1445
- **High:** 4017
- **Medium:** 3769
- **Low:** 197
- **None:** 0

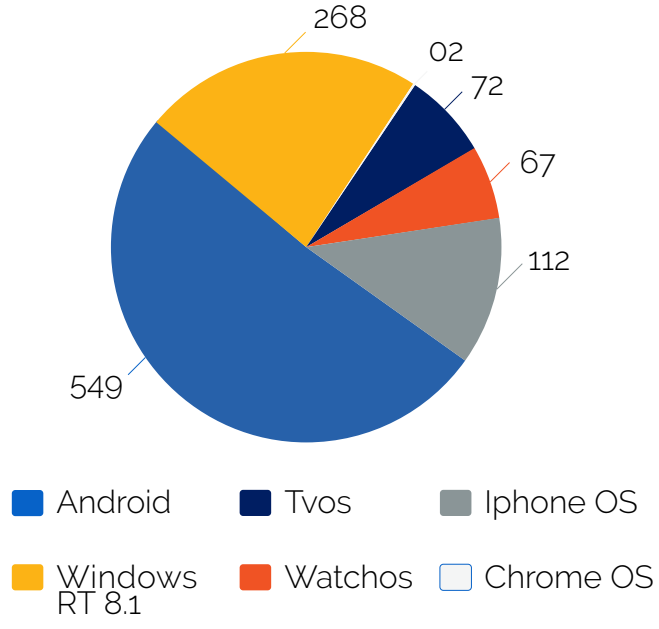
Vulnerabilidades publicadas durante el primer semestre de 2020 por mes



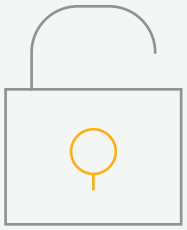
Vulnerabilidades en sistemas operativos de escritorio y server



Vulnerabilidades SO dispositivos inteligentes



Vulnerabilidades
Primer semestre 2020



SMBV3

El pasado 10 de marzo se publicó accidentalmente información sobre una nueva vulnerabilidad en el protocolo SMBv3 de Windows. Sin embargo, la información no fue publicada por Microsoft si no por uno de los proveedores de seguridad que forman parte del Programa de Protección Activa de Microsoft y que tuvo acceso temprano a la información de la vulnerabilidad.

Identificada como CVE-2020-0796, se trata de una vulnerabilidad de ejecución de código remoto generada por un error al manejar cierto tipo de peticiones. Para explotar la vulnerabilidad contra un servidor SMB, un atacante no autenticado enviaría un paquete especialmente diseñado al servidor SMBv3 objetivo -en concreto, el error se da al manejar paquetes de datos comprimidos maliciosos-, permitiendo la ejecución de código arbitrario.

Ghostcat

En marzo se descubrió una vulnerabilidad en Tomcat, uno de los servidores middleware más populares de Java. Esta vulnerabilidad también se conoce como Ghostcat (CVE-2020-1938).

Debido a un fallo en el protocolo Tomcat AJP, un atacante puede leer o incluir cualquier archivo en los directorios "webapp" de Tomcat. Esta vulnerabilidad afecta, al menos, a las versiones 6,7, 8 y 9 de Tomcat. De acuerdo con las estadísticas, existen 1.263.126 servidores Tomcat que están utilizando este protocolo.

SweynTooth

En este periodo se publicó la vulnerabilidad SweynThooth, que se trataba de una serie de agujeros de seguridad que se descubrieron en los chips de Bluetooth de varios proveedores.

Muchos de los fallos en SweynTooth no son serios, y requieren que el atacante esté dentro del rango del Bluetooth de baja energía (Bluetooth Low Energy por sus siglas en inglés). Solo 9 de los 10 fallos pueden ser explotados provocando su reinicio o bloqueo; sólo uno puede ser potencialmente abusado por los delincuentes para acceder a su dispositivo sin necesidad de que se les deje emparejarse con él primero.

Uno de los fallos más peligrosos es la conocida como CVE-2019-19194. Esta vulnerabilidad crítica es una variación del Key Size Overflow y afecta a todos los productos que utilizan la implementación Telink SMP con soporte para la conexión segura habilitada.

En teoría, una aplicación que quiera conectarse a un dispositivo debería pasar primero por el emparejamiento. Cada lado recuerda el LTK asociado con el otro dispositivo, y con ese LTK pueden conectarse de forma segura en el futuro. Pero, para evitar usar la propia LTK en cada ocasión en que se conecten, usan un SK, abreviatura de "llave de sesión", calculada a partir de la LTK. Para asegurarse de que el SK sea diferente cada vez, los dos dispositivos que se conectan, primero se ponen de acuerdo en 16 bytes aleatorios llamados "diversificador de clave de sesión", o SKD. Pero los investigadores descubrieron que podían engañar al firmware del chip para que hiciera un cortocircuito en el proceso de emparejamiento.

Infraestructuras críticas

La importancia del sector le convierte en un objetivo principal para los ciberataques de grupos con patrocinio estatal, terroristas y ciberdelincuentes que buscan aprovecharse de él para sus propios objetivos políticos o económicos.

Hospitales

Tras el comienzo de la crisis sanitaria de la COVID-19, los centros hospitalarios se han visto amenazados a través de diversas técnicas cibernéticas que pretenden alcanzar una serie de objetivos (políticos y económicos) afectando negativamente al centro.

El pánico creado a raíz de la implantación del estado de alarma y la saturación de los centros hospitalarios se ha convertido en una oportunidad para que ciberdelincuentes distribuyan programas maliciosos entre sus potenciales víctimas.

Los ciberdelincuentes han aprovechado la pandemia por la COVID-19 para realizar ataques cibernéticos a proveedores hospitalarios y empresas relacionadas con el sector hospitalario, destacando el ataque cibernético a dos compañías que colaboraban en la construcción de hospitales de campaña en Reino Unido; el ataque de ransomware a dos hospitales en las ciudades de Ostrava y Olomouc, República Checa; o el intento de ciberataque a la Autoridad Hospitalaria de París.

El ransomware ha sido una de las técnicas más usadas para realizar ataques contra el sector hospitalario en este periodo. El objetivo de los atacantes era el de conseguir un posible beneficio económico y la recopilación de información y bases de datos útiles para realizar actividades maliciosas complementarias.

RANSOMWARE EKANS

El caso más sonado en este periodo es el ataque al grupo hospitalario Fresenius, quién posee diversos hospitales privados en Europa. El ransomware utilizado en esta ocasión fue Snake, también conocido como Ekans.

Este ransomware se caracteriza por atacar Sistemas de Control Industrial y SCADA. Este malware primero apunta a un sistema y luego elimina las instantáneas de volumen; posteriormente mata todos los procesos relacionados con los sistemas SCADA, máquinas virtuales, sistemas de control industrial, herramientas de administración remota, software de administración de red y otros. Finalmente, el malware comienza a cifrar archivos y muestra la nota de rescate con el título "Fix-Your-Files.Txt".

Red eléctrica

A parte de los hospitales, durante los primeros seis meses de 2020 se ha observado un aumento de los ataques dirigidos contra otro tipo de infraestructuras críticas, siguiendo la tendencia creciente ya observada durante el año anterior. Uno de los sectores que también ha sido el objetivo de los cibercriminales han sido empresas que controlan la red eléctrica o el suministro de energía.

En el mes de marzo, la Red Europea de Operadores de Sistemas de Transmisión de Electricidad (ENTSO-E) admitió que fue víctima de un ataque cibernético. En una declaración publicada en su sitio web, la organización dice que ha encontrado evidencia de una "intrusión cibernética exitosa" que afectó a su red de oficinas.

En el mes de mayo, Elexon, la compañía que desempeña un papel central en el equilibrio y la solución del sistema de energía del Reino Unido, fue golpeada por un ciberataque. Los operadores del ransomware REvil/Sodinokibi publicaron la información extraída en el ataque, al no haberse realizado el pago del rescate. También el mes de junio el ransomware Snake afectó a la empresa energética Enel.

REVIL

Este ransomware, que fue uno de los más activos durante el año 2019, durante este primer semestre de 2020 ha conseguido convertirse en uno de los más relevantes en el panorama cibercriminal.

Además de continuar con la tendencia de los ransomware de publicar la información sustraída en los ataques, este ransomware ha dado un paso más allá en la extorsión y ha comenzado a subastar la información de las empresas atacadas.

Industria petroquímica

El sector del petróleo y el gas ha sufrido varios incidentes de seguridad durante este periodo, reflejando la tendencia de los cibercriminales de dirigirse a sectores críticos, bien con el objetivo de conseguir un mayor beneficio económico o con el de interrumpir servicios esenciales.

En el mes de febrero un operador de gas natural de Estados Unidos se vio obligado a cerrar durante dos días, después de que un ransomware se extendiera en su red OT, sistema con el que se monitorizan y controlan los procesos físicos de las plantas. En el mes de abril, una gran empresa del sector del gas y el petróleo fue víctima de ransomware: W&T Offshore fue víctima del ransomware Nefilim. El ataque conllevó el cifrado de sus archivos e impidió el acceso de la compañía a sus equipos de manera temporal. Además, los atacantes filtraron documentos extraídos en el ataque.

También durante este periodo se han producido ataques a empresas nacionales de la industria petroquímica, como el ocurrido en el mes de mayo en la compañía energética estatal de Taiwán (CPC Corp.) y la empresa petrolera Formosa Petrochemical de Taiwan, o el ataque sufrido por la compañía Energías de Portugal (EDP) por parte del ransomware Ragnar.

NEFILIM RANSOMWARE

Este ransomware parece estar vinculado a los operadores del ransomware Nemty.

El ransomware Nefilim ha aparecido en el primer semestre de 2020 y se ha convertido en uno de los ransomware que más información y ataques están haciendo públicos en su sitio web de la Deep Web.

Industria del transporte

En este primer semestre de 2020 desde empresas de transporte de mercancías, de construcción de carreteras y redes urbanas, hasta organismos públicos de transporte se han visto afectadas por incidentes de seguridad.

Sin duda, una de las empresas más afectadas en este periodo ha sido Toll Group, gigante logístico de Australia, que fue el blanco de un ataque por parte del ransomware Mailto y vio sus sistemas comprometidos en el mes de febrero; y unos meses más tarde, en el mes de mayo, volvía a ser víctima de otro ransomware, en este caso Nefilim.

No obstante, este no se trata de un caso aislado, en el mes de enero la empresa Railworks Corporation hizo público que había sido víctima de un ataque de ransomware que podría haber resultado en una brecha de seguridad, dejando expuesta información personal. También en el ámbito del transporte terrestre, Stadler Rail sufría un ataque por parte de Nefilim; y más allá de las empresas, organismos públicos como el Departamento de Transporte de Texas también ha sido víctima de un incidente de seguridad de esta índole.

TRANSPORTE AÉREO

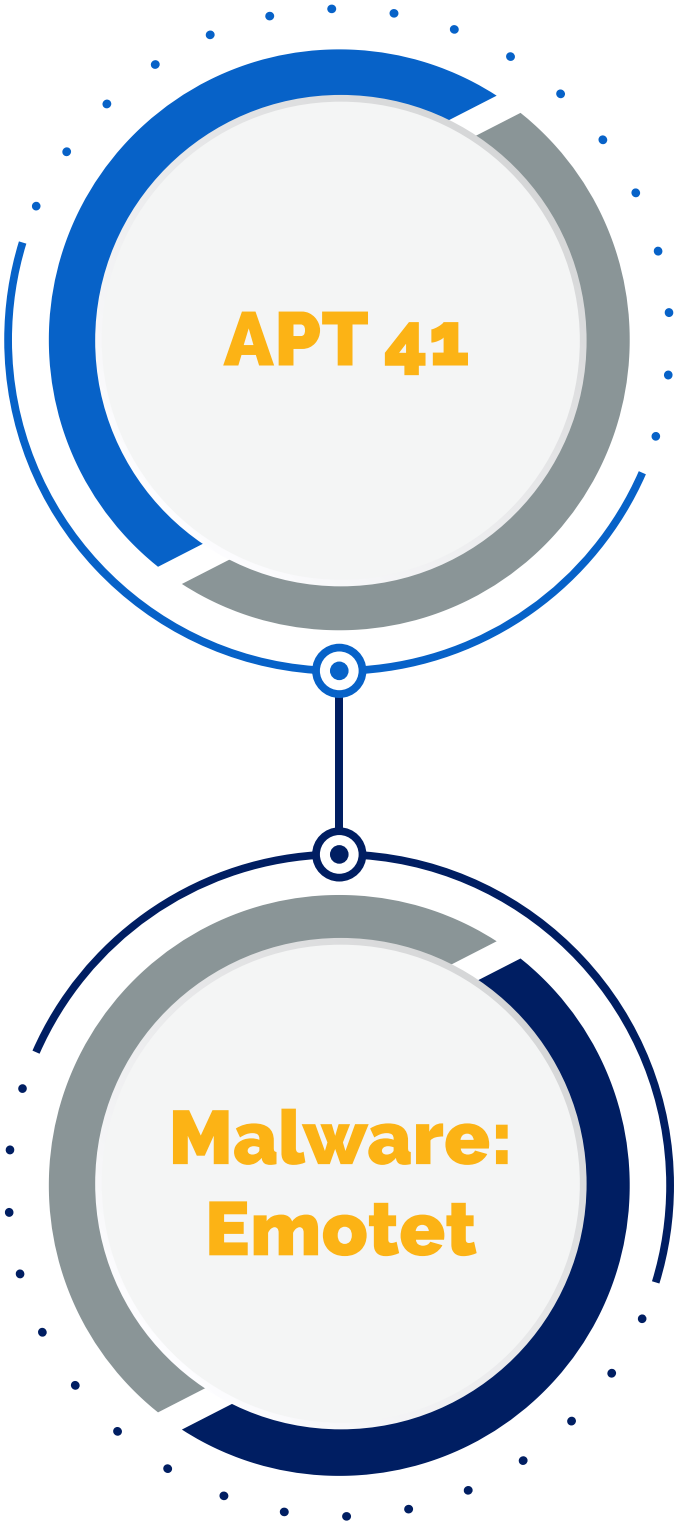
En cuanto al transporte aéreo, la aerolínea británica de bajo coste easyJet también sufrió un ciberataque que llevó a una posterior brecha de datos, entre los que se encontraban tarjetas de crédito y direcciones de correo electrónico de aproximadamente 9 millones de usuarios.

En el mes de marzo, el aeropuerto internacional de San Francisco (SFO) sufrió un ataque cibernético por parte de un grupo de hackers ruso conocido como "Energetic Bear" (DragonFly), que atacó a dos de sus sitios web: SFOConnect.com y SFOConstruction.com, a través del cual algunos usuarios. Las credenciales de inicio de sesión de Windows probablemente fueron robadas.

Telco

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

En este periodo, en el que la mayor parte de las empresas han optado por el teletrabajo, servicios como los accesos remotos y VPNs han sido necesarios para el desempeño de las tareas de los trabajadores. No obstante, la rapidez o la falta de conocimientos a la hora de utilizar estos servicios, ha servido a los ciberdelincuentes para una mayor eficacia de sus ataques.



APT 41

Durante estos meses, este grupo cibercriminal ha estado explotando distintas vulnerabilidades, entre las que se encuentran la vulnerabilidad existente en Citrix NetScaler/ADCm (CVE-2019-19781), routers de Cisco, y Zoho ManageEngine Desktop Central (CVE-2020-10189).

La APT41, un grupo de actores vinculados con el gobierno de China, habría estado intentando explotar vulnerabilidades en Citrix NetScaler / ADCm (CVE-2019-19781), routers de Cisco, y Zoho ManageEngine Desktop Central (CVE-2020-10189). Estos ataques habrían comenzado el 20 de enero prolongándose hasta el mes de marzo de 2020. Los ataques se habrían dirigido a Australia, Canadá, Dinamarca, Finlandia, Francia, India, Italia, Japón, entre otros. Entre los sectores afectados se encuentran el financiero, la construcción o el sector sanitario entre otros.

Malware: Emotet

En cuanto a las novedades de malware relacionado con telecomunicaciones, se destaca que en estos primeros seis meses de 2020 se ha detectado la distribución de una versión de Emotet que cuenta con un módulo para buscar redes wifi cercanas al dispositivo infectado e infectar los dispositivos conectados a las mismas.

Una vez Emotet obtiene la información sobre los diferentes puntos de acceso WiFi disponibles, lleva a cabo un ataque de fuerza bruta intentando crear un perfil para conectarse a todas las redes disponibles. Si es capaz de conectarse a alguna de las redes, el siguiente paso es enumerar los dispositivos conectados a la misma y sus carpetas compartidas. Tras este paso, comienza el ataque de fuerza bruta para determinar los nombres de usuario y contraseñas para acceder a los recursos compartidos. Tras conseguir acceso a los recursos compartidos, ejecuta el payload que se encarga de realizar la infección del nuevo dispositivo.

Brechas de seguridad

Durante el primer semestre de 2020

DICIEMBRE 2019

ENERO

Microsoft revela una brecha de seguridad en una de sus bases de datos de soporte a clientes. 250 millones de emails e IPs se vieron comprometidos.

FEBRERO

Estée Lauder se vio envuelta en una brecha de datos en la que se comprometieron 440 millones de registros, incluyendo correos electrónicos internos de la compañía y direcciones de correo electrónico de no consumidores.

MARZO

La compañía de telefonía T-Mobile anunció que había sufrido un ataque en el cual los atacantes accedieron a los servicios de email de la compañía, llevando al compromiso de la información de los consumidores y de la propia empresa.

La cadena hotelera Marriot fue víctima de una brecha de seguridad tras el acceso de ciberdelincuentes a información de 5,2 millones de huéspedes en una base de datos de un programa de "loyalty" de la cadena hotelera. En este mes, Nippon Telegraph & Telephone (NTT), sufrió una brecha de seguridad a mediados de mayo de 2020, tras la intrusión de piratas informáticos en varias capas de su infraestructura IT que culminaron con el robo de información de 621 clientes de su subsidiaria de Comunicaciones.

ABRIL

La Administración de Pequeñas Empresas de EE. UU. (SBA) hizo pública una brecha de seguridad que afectaba aproximadamente 8,000 personas que habían solicitado préstamos comerciales de emergencia debido a la interrupción de la COVID-19.

MAYO

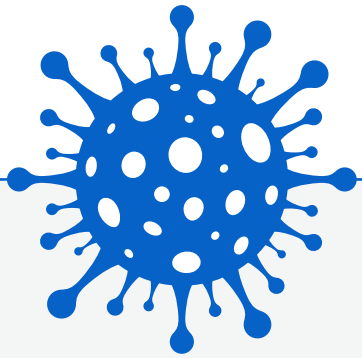
easyJet reveló que había sufrido un ciberataque que llevó a una brecha de seguridad que afectaba a nueve millones de pasajeros cuyos datos podrían haber sido expuestos, incluyendo detalles de tarjetas de crédito.

JUNIO

Nintendo confirma que desde el mes de abril hasta el mes de junio cibercriminales habrían tenido acceso a 300.000 cuentas, obteniendo acceso a información personal como fechas de nacimiento y direcciones de correo electrónico, pero no a detalles de tarjetas de crédito.

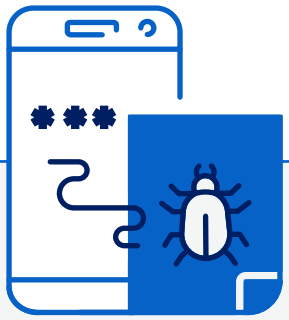
JULIO 2020

Conclusiones



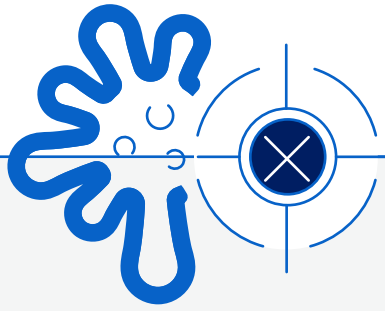
Coronavirus

Los grupos de ciberdelincuentes han aprovechado el miedo de los usuarios, la incertidumbre ante las medidas de seguridad para hacer frente a la enfermedad, e incluso el aumento del trabajo en remoto para el desarrollo de sus campañas. Cabe destacar la cantidad de ataques cibernéticos a hospitales donde los cibercriminales han aprovechado la ola del coronavirus para llevar a cabo sus ataques.



Ransomware Covidlocker

Durante el primer semestre de 2020 se ha observado cómo el ransomware ha aumentado en todas sus variantes, estando este aumento estrechamente ligado con la pandemia de la COVID 19. Destaca el despliegue de ransomware Covidlocker, el cual contiene el nombre de la enfermedad que ha asolado a la población mundial.



easyjet

Estos últimos seis meses se han producido múltiples brechas de seguridad entre las que destacan la brecha de seguridad que sufrió la compañía aérea easyJet, que afectó a nueve millones de pasajeros.

SweynThooth

Este semestre se ha caracterizado por un incremento en el número de vulnerabilidades detectadas. Destacan en este periodo la vulnerabilidad conocida como SweynThooth, la cual se trataba de una serie de agujeros de seguridad que se descubrieron en los chips de Bluetooth de varios proveedores; así como la vulnerabilidad existente en el protocolo SMBv3 de Windows.

S21SEC

www.s21sec.com | 902 020 222 | marketing@s21sec.com