CIBER_ AMENAZAS Y TENDENCIAS

EDICIÓN 2021

CCN-CERT IA-23/21

ANÁLISIS DE LAS CIBERAMENAZAS NACIONALES E INTERNACIONALES, DE SU EVOLUCIÓN Y TENDENCIAS FUTURAS.

CCN centro criptológico nacional

ccn-cert centro criptológico nacional

Edita:

Centro Criptológico Nacional, 2021

Fecha de edición: octubre de 2021

01 Resumen ejecutivo

Récord de incidentes de seguridad, digitalización forzosa e incertidumbre: las claves de 2020.

Son muchos los calificativos que podrían describir el año 2020, pero si hubiese que elegir uno, esa palabra sería **incertidumbre**. 2020 fue el año en el que nos enfrentamos a lo desconocido, y no solo en el ámbito sanitario. En tan inédito contexto, este informe tiene un doble objetivo: hacer un recorrido por el mundo de la ciberseguridad de 2020 y plantear las tendencias de 2021.

2020 ha marcado un punto de inflexión a nivel mundial en la forma de entender la vida. Nuestros hábitos, costumbres y formas de trabajar, consumir o cuidarnos ya nunca volverán a ser los mismos. Ya nunca volveremos a pensar que una infección en la otra punta del mundo no puede afectarnos. Ya todos conocemos en primera persona los beneficios de ejercer la **responsabilidad individual**. Esta nueva mentalidad y percepción del riesgo sin duda serán positivas para la seguridad.

El final de la década no solo pasará a la historia por la crisis sanitaria global; 2020 también fue el año en el que hubo **más incidentes de seguridad** que nunca y **más digitalización forzosa** de negocios, sistemas educativos, sanitarios, etc. La proliferación de cambios en tiempo récord ha dado alas a todo tipo de actores hostiles, brindándoles nuevas y numerosas oportunidades de actuar.

Este informe detalla las principales amenazas y métodos de ataque registrados el pasado año. También repasamos las principales vulnerabilidades encontradas y los incidentes de mayor repercusión, tanto en términos de ciberespionaje o ingeniería social, como respecto a intrusiones en sectores que hasta el momento no habían sido un objetivo destacado.

A partir de ese análisis del pasado se ofrecerán claves de futuro, apuntando las tendencias que se observan en 2021 en materia de ciberseguridad. También se proporcionarán recomendaciones y buenas prácticas para minimizar el riesgo y el impacto de las amenazas que vendrán.

02 Sobre CCN-CERT

CERT Gubernamental Nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la **información clasificada** (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del **Sector Público** es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier Organismo o empresa pública. En el caso de **operadores críticos del sector público** la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

03 Vistazo a 2020: ataque a la normalidad

2020 será recordado como un año especialmente disruptivo, de los que marcan un antes y después, y no solo por la crisis sanitaria mundial. La transformación digital ha hecho que estemos hiperconectados, que nuestros días transcurran prácticamente en línea, y que movernos por el ciberespacio sea algo normal, tanto en la vida personal como en la profesional. En esas estábamos cuando un virus le dio un giro inesperado al concepto de normalidad.

El 11 de marzo de 2020 la Organización Mundial de la Salud (OMS) declaraba el brote de coronavirus como pandemia global, e instaba a todos los gobiernos, sociedades y sectores a involucrarse en la lucha contra la COVID-19. Esa lucha ha traído consecuencias indeseadas, entre ellas el **aumento y la aparición de factores de riesgo críticos para la ciberseguridad** de ciudadanos, empresas e instituciones. Estos son algunos de ellos:

TELEBRABAJO VULNERABLE

Tras decretarse el confinamiento, empresas e instituciones desplegaron rápidamente **redes y sistemas para que su personal pudiese trabajar a distancia**, y para que sus servicios permaneciesen operativos. Asimismo, se ha producido una migración más que notoria a infraestructuras en la nube.

Este nuevo escenario, establecido en muchos casos de forma rápida o incluso a marchas forzadas, ha facilitado que los ciberatacantes se aprovechen del aumento de las vulnerabilidades en seguridad para lograr sus propósitos: robar datos, obtener beneficios y ocasionar disfunciones. Destacan vulnerabilidades publicadas a principios de año, relacionadas con Pulse Secure[1], que fueron altamente explotadas, así como las de SonicOS VPN[2].

Tambíen se vivió la eclosión en el uso de **aplicaciones de videollamada y de videoconferencia**, destacando el aumento de usuarios de **Zoom**[3]. Este cambio dejó expuestas numerosas deficiencias de seguridad en este tipo de la aplicaciones, que tuvieron que aumentar su recursos en seguridad para responder a la demanda de los usuarios y para neutralizar los ataques[4] que acompañaron su crecimiento.

MOVILIDAD

El **aumento en el uso de los dispositivos móviles** durante el confinamiento puede ser otra causa del importante crecimiento de las estafas móviles que usan reclamos vinculados a la situación sanitaria y económica. Además, el **mayor uso de dispositivos conectados** (**IoT**) y la **extensión del estándar 5G** crean nuevas opciones de ataque que no pasan desapercibidas para los actores malintencionados.

CIBERPANDEMIA: UN NUEVO DESAFÍO

La **información relacionada con la salud** ya tiene un alto valor de inteligencia. Ejemplo de ello son los intentos de robar información sobre el desarrollo de vacunas, incidentes que han sido reportados por las autoridades de varios países.

Pero en general, la crisis sanitaria ha afectado a la movilidad humana, a la organización de la vida laboral y a cómo nos relacionamos. También ha sido la protagonista de nuestras llamadas, chats y

1. Véase https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101
2. Véase https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-5135
3. Véase https://blog.zoom.us/90-day-security-plan-progress-report-april-22/
4. Véase https://www.cnet.com/news/zoom-security-issues-zoom-buys-security-company-aims-for-end-to-end-encryption/

mensajes, lo cual ha generado grandes volúmenes de datos e información sobre nuestras creencias, miedos y necesidades. Como los atacantes utilizan la actualidad para intentar atraer a sus objetivos, no tardaron en **usar la COVID-19 como tema recurrente en los correos electrónicos de *spear phishing***.

Una tendencia detectada fue el **aumento de aplicaciones fraudulentas para seguir la evolución de la COVID-19** durante los meses de marzo y abril, al principio del estado de alarma y en medio de una gran confusión. Estos engaños tomaron forma de mapas interactivos con contenido dañino o aplicaciones móviles con malware insertado.

En 2020 también aumentaron de forma drástica los **ataques de ransomware**, tanto en su versión clásica como en la cada vez más habitual de **doble extorsión** (cifrado y publicación de datos robados). Fue un año también marcado por los **ataques a la cadena de suministro**, como el de SolarWinds a finales de año, un incidente que pone de manifiesto el alto grado de especialización, técnicas y recursos avanzados de que disponen algunos ciberatacantes.

Todo ello está consolidando un nuevo término que probablemente se convertirá en un nuevo desafío a afrontar durante el próximo año: la **ciberpandemia**.

OBJETIVO: SANIDAD

El sector sanitario ha sufrido una presión constante y ha estado en el punto de mira de los cibercriminales. El año 2020 comenzó con el **final del soporte de Microsoft5 a sistemas Windows 7 y Windows Server 2008**. Esto supuso un nuevo revés para las infraestructuras de hospitales (muchos de ellos todavía con dispositivos Windows XP), que les dejaba expuestos ante nuevas vulnerabilidades y actores dispuestos a explotarlas.

A lo largo del año se fueron sucediendo los ataques al sector salud españoles, hospitales y aseguradoras. Situación no exclusiva a España, como dejaron patente las agresiones similares algunas de ellas con efectos graves[6] sufridas por muchos otros países.

La ciberpandemia es la tendencia de ciberataques surgida de la crisis sanitaria, usando la COVID-19 como gancho

5. Véase https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finalizó-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962

6. Véase https://elpais.com/internacional/2020-10-03/ciberataque-a-un-hospital-aleman-en-tiempos-de-pandemia.html

Avances contra el cibercrimen

Por supuesto, también ha habido luz en la oscuridad, avances muy positivos contra la ciberdelincuencia. Se desarrolló una importante operación conjunta entre fabricantes, gobiernos y agencias de seguridad para acabar con la actividad de Trickbot, una de las botnets que más estragos ha causado en los últimos años[7]. También se desarticuló el grupo que operaba el drástico *ransomware* Netwalker[8], y se han hecho esfuerzos para acabar con los delitos de delincuentes independientes o de grupos APT internacionales[9].

Lecciones aprendidas

Tras el convulso 2020 ha llegado el momento en el que, tanto para las personas como para las organizaciones, **se hace más necesario que nunca extremar todas las precauciones** ante cualquier tipo de comunicación recibida en los dispositivos personales o de trabajo. Se hace vital la tarea de **concienciar, formar y tener procedimientos perfectamente definidos y asimilados** por parte de todo el personal, para tratar de reducir el riesgo o evitar un impacto mayor en las organizaciones.

Y estas por su parte deben **apostar por invertir aún más en ciberseguridad**, máxime si se quiere tener una oportunidad ante los retos anteriormente descritos, con redes forzadas a extender su perímetro para poder continuar dando servicio en un escenario tan disruptivo como ha sido el año 2020.

7. Véase https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/
8. Véase https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware
9. Véase https://www.checkpoint.com/downloads/resources/cyber-security-report-2021.pdf

04 Agentes de la amenaza

Entre los principales agentes de la amenaza cuya actividad se incrementó en 2020 destacan los actores Estado y el cibercrimen.

Salud, investigación, gobierno y sectores estratégicos, en el punto de mira de los actores Estado

4.1 Actores Estado

En los últimos años, los Estados han sido uno de los principales actores de la amenaza, y han evolucionado su actividad para alinearse con los objetivos políticos de los países donde operan. De hecho, implicando un cambio de tendencia, en el último año **el 90% de los objetivos han sido contra organismos públicos, ONG y entidades de políticas sociales o asuntos internacionales**[10].

Por sectores, han sido **objetivos prioritarios** de los actores Estado o grupos patrocinados por estos aquellos vinculados a los actuales conflictos y problemáticas globales, como la **crisis sanitaria** o el escenario multipolar de **política internacional**, entre otros. Estos han sido los principales sectores de interés:

- Gubernamental
- Defensa
- Industria armamentística
- Salud e industria farmacéutica
- Centros de investigación
- Tecnologías de la información y las comunicaciones
- Energía
- Telecomunicaciones
- Inversión financiera
- Comercio internacional

10. Véase https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

4.1.1 ACTIVIDAD DE GRUPOS APT DURANTE 2020

Además de los clásicos objetivos gubernamentales o de defensa, la pandemia ha favorecido el incremento de las **campañas de grupos APT contra organizaciones vinculadas a la investigación científica o la gestión de la salud**. Dichas acciones han tenido como objetivo el **robo de propiedad intelectual, información corporativa y datos sensibles**. A continuación, se detallan las campañas identificadas[11] por distintos organismos gubernamentales o privados cuyos países las han sufrido o las han investigado:

CAMPAÑAS CONTRA ORGANIZACIONES SANITARIAS Y DE INVESTIGACIÓN DE COVID-19 (2020)	**APT41[12]:** La campaña de este grupo se dirigió a organizaciones del sector farmacéutico, mediante la explotación de vulnerabilidades de VPN. El sector sanitario no fue el único objetivo de APT41, como se verá más adelante.
	Grupos APT (varios): La Organización Mundial de la Salud (OMS) reportó durante el mes de abril varias campañas de varios actores contra oficiales de la misma OMS.
	APT32[13]: Grupo que atacó a organizaciones chinas dedicadas a la monitorización y gestión sanitaria de la pandemia.
	APT29[14]: En mayo se detectó una campaña de **este** grupo contra organizaciones médicas de los Estados Unidos. Según constataron autoridades británicas, su objetivo era perpetrar robos de propiedad intelectual relacionados con investigaciones de la COVID-19.
	UNC788: A finales de 2020, investigadores de ciberseguridad detectaron otra campaña de phishing llevada a cabo por este grupo, también conocido como **Charming Kitten**. Sus objetivos fueron **empleados técnicos de la OMS**, y organizaciones del **sector médico y centros de investigación de la salud** de los Estados Unidos[15].
	Kimsuky[16]: Entre septiembre y diciembre se detectó actividad de este grupo, contra organizaciones farmacéuticas de Estados Unidos.
	TEMP.Hermit: Este grupo, también lanzó una campaña contra organizaciones farmacéuticas.
CAMPAÑAS CONTRA INSTITUCIONES GUBERNAMENTALES Y ENTIDADES PÚBLICAS (2020)	**APT28[17]:** Perpetró un ciberataque contra el **Parlamento noruego**[18], conocido como Stortinget, consiguiendo comprometer diversas cuentas de correo de la institución. En mayo de 2020, la Agencia de Seguridad Nacional de los Estados Unidos (NSA) emitió una advertencia sobre el grupo APT28, afirmando que seguía explotando **vulnerabilidades en Exim mail transfer agent (MTA)**, software frecuentemente utilizado en entornos Unix[19].
	APT29[20]: En diciembre de 2020 se hizo público un complejo ataque de cadena de suministro que afectó a **unas 18000 entidades usuarias del software de gestión de TI Orion del fabricante SolarWinds**[21]. Entre las víctimas se encuentran agencias gubernamentales y víctimas del sector privado. A través del compromiso del proveedor de software SolarWinds, los atacantes infectaron a las víctimas mediante la inclusión de código dañino en un paquete de actualización.
	APT Gamaredon[22]: Intensa actividad durante todo 2020 contra **objetivos militares, gubernamentales y diplomáticos en Ucrania**. En la ingeniería social de sus phishings, este grupo suele utilizar temáticas relacionadas con el sector militar o gubernamental. El *toolkit* o herramientas que utilizan consiste en diversos artefactos de malware con objetivos como escanear unidades en busca de archivos específicos del sistema, realizar capturas de pantalla, ejecutar comandos remotos o administrar dispositivos de forma remota[23].

CAMPAÑAS CONTRA INSTITUCIONES GUBERNAMENTALES Y ENTIDADES PÚBLICAS (2020)	**Berserk Bear**[24]**:** La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de Estados Unidos publicó una alerta sobre la intrusión de dicho grupo en las redes de **organizaciones públicas de su sector de la aviación**. Se identificaron exfiltraciones de datos en dos víctimas, y se confirmó que el actor hostil buscaba informaciones sobre configuraciones de red, contraseñas y datos de "partners" y proveedores. Las autoridades alemanas también detectaron actividad dañina por parte de **Berserk Bear** contra organizaciones del **sector industrial alemán**. Estas campañas tenían como principal objetivo establecer persistencia dentro de las redes IT y OT con el posible fin de llevar a cabo operaciones futuras.
	Grupo Turla[25]**:** Lanzó una campaña cuyos principales objetivos fueron **Ministerios de Asuntos Exteriores europeos**. Entre las herramientas utilizadas por este actor se encuentran **ComRAT malware** o **Agent.BTZ**[26].
	APT31[27]**:** El **Parlamento finlandés** sufrió una intrusión por parte de **este** grupo. Esta acción comprometió correos electrónicos de la institución[28]. El mismo grupo fue acusado de llevar a cabo ataques contra la **campaña presidencial de Joe Biden**, mediante el envío de *spear phishing* suplantando a una reconocida empresa de ciberseguridad[29].
	APT40[30]**:** Otro actor que lanzó campañas de phishing contra **organismos gubernamentales**. Su campaña apuntaba a funcionarios del **gobierno de Malasia**, a quienes enviaron un fichero infectado que suplantaba a un evento político local. Los objetivos de APT40 han sido relacionados con organizaciones y países implicados dentro de la ruta **OBOR (One Belt One Road)**[31].
CAMPAÑAS CONTRA SECTORES ESTRATÉGICOS (2020)	**APT41:** ejecutó una campaña a principios de 2020 contra organizaciones de los sectores **bancario, defensa, energético, construcción, legal, salud, investigación, ONG y transporte**[32].

En el apartado 5.6 (Vigilancia CCN-CERT) se incluye más información sobre las actividades de grupos APT en 2020.

11. Véase https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html)
12. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
13. https://securityaffairs.co/wordpress/102124/apt/apt32-target-china-covid19.html
14. El grupo APT29 ha sido vinculado por diferentes servicios de Inteligencia (especialmente por los EEUU) al Servicio de Inteligencia Exterior (SVR) de la Federación Rusa: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ , https://crsreports.congress.gov/product/pdf/IF/IF11718
15. Véase https://threatpost.com/charming-kitten-pounces-on-researchers/ 165129/
16. El grupo Kimsuky ha sido vinculado por Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de Estados Unidos a Corea del Norte : https://us-cert.cisa.gov/ncas/alerts/aa20-301a
17. El grupo APT28 ha sido vinculado por diferentes países (especialmente por los EEUU y Reino Unido) al Servicio de Inteligencia Militar (GRU) de la Federación Rusa: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-expose, https://crsreports.congress.gov/product/pdf/IF/IF11718
18. Véase https://www.pst.no/alle-artikler/pressemel dinger/datainnbruddet-mot-stortinget-er-ferdig-etterforske
19. Véase https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
20. El 15 de abril de 2021 el gobierno de los Estados Unidos de América atribuyó este ataque al grupo conocido como APT29, del Servicio de Inteligencia Exterior (SVR) ruso: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/
21. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
22. El grupo Gamaredon ha sido vinculado por los EEUU al Servicio de Seguridad Federal (FSB) de la Federación Rusa: https://crsreports.congress.gov/product/pdf/IF/IF11718
23. Véase https://securelist.com/apt-trends-report-q1-2020/96826/
24. El grupo Bersek Bear ha sido vinculado por los EEUU al Servicio de Seguridad Federal (FSB) de la Federación Rusa: https://crsreports.congress.gov/product/pdf/IF/IF11718
25. El grupo Turla ha sido vinculado por diferentes servicios de Inteligencia (especialmente por los EEUU y Reino Unido) a la Federación Rusa: https://us-cert.cisa.gov/ncas/current-activity/2019/10/21/nsa-and-ncsc-release-joint-advisory-turla-group-activity
26. Véase https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
27. El grupo APT31 ha sido vinculado por Reino Unido al Gobierno de China: https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking
28. Véase https://supo.fi/en/-/supo-identified-the-cyber-espionage-operation-against-the-parliament-as-apt31
29. Véase https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
30. El grupo APT40 ha sido vinculado por Reino Unido al Gobierno de China: https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking
31. Véase https://www.elastic.co/es/blog/advanced-techniques-used-in-malaysian-focused-apt-campaign
32. Véase https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html)

4.2 Ciberdelincuencia

En 2020, el cibercrimen se ha mantenido como uno de los actores más habituales y dinámicos. Por supuesto, la crisis sanitaria también ha influido en su actividad. Han puesto el foco en organismos públicos, la industria e infraestructuras críticas, usando **distintos tipos de ransomware** para extorsionar a sus víctimas y obtener un gran rendimiento económico. También han recurrido al envío de **campañas masivas de phishing** y ***Business Email Compromise* (BEC)**.

RANSOMWARE MÁS EFECTIVO

Un año más, el ransomware se erige en la **vía de ataque preferida de los ciberdelincuentes**, que tienden hacia **métodos de secuestro de la información cada vez más sofisticados y selectivos**. Los ataques se han dirigido tanto a sectores públicos como privados, de diversos tamaños y nacionalidades. Esto ha permitido a los atacantes incrementar tanto el importe del rescate solicitado como la probabilidad de que la víctima pague el rescate[33].

Cabe destacar que no solo se ha detectado una escalada en los intentos de ataque, sino que la **alta efectividad de sus técnicas de intrusión y de los tipos de ransomware utilizados** ha supuesto un aumento significativo del número de organizaciones infectadas, muchas de las cuales han tenido que detener totalmente su actividad ante la amenaza de pérdida total de los sistemas.

Acerca de estas infecciones, **sorprende y preocupa que hayan afectado a grandes corporaciones con sistemas de defensa y cierta madurez TIC**. Si bien estas compañías han podido recuperarse de los ataques, no han salido del todo indemnes, pues han sufrido **fugas de información, importantes daños reputacionales y grandes costes indirectos**.

Por otro lado, **pequeñas empresas y administraciones públicas locales** tampoco han escapado a estas infecciones. Aunque no se dispone de datos formales acerca del número de sistemas comprometidos, en los ataques se han dado factores comunes: falta de concienciación frente a amenazas de seguridad (especialmente por reutilización de credenciales o por phishings), nivel de actualizaciones de software insuficiente y serios **problemas en la gestión de copias de seguridad** o por ser estas muy limitadas o porestar conectadas a los sistemas de producción y ser alcanzadas por la infección.

Como respuesta a estas situaciones, el **CCN-CERT ha publicado durante el año diferentes informes de código dañino tipo ransomware**, como **RobbinHood, Avaddon, NetWalker, Maze, Snake locker y Vcript**.

Mención especial merece la aplicación **microCLAUDIA**, añadida en 2020 al catálogo de herramientas del CCN-CERT y que proporciona protección directa contra infecciones por ransomware. Esta solución instala un agente ligero en equipos Windows y complementa a los antivirus habituales y soluciones EDR (no los sustituye), desplegando vacunas concretas contra las variantes más habituales de ransomware. Estas vacunas son liberadas

33. Véase https://www.europol.europa.eu/iocta-report

directamente por CCN-CERT, disponiendo cada organismo de un panel centralizado donde gestionar las vacunas aplicadas en los diferentes equipos (**https://microclaudia.ccn-cert.cni.es**).

BEC: AUMENTO DEL PHISHING CORPORATIVO

El BEC (*Business Email Compromise*) sigue siendo un mecanismo cada vez más utilizado por los ciberdelincuentes, y **se ha aprovechado especialmente de la situación de teletrabajo** derivada de la pandemia, que facilita la credibilidad de los engaños utilizados (simulación de problemas para tramitar solicitudes por mecanismos oficiales, necesidades urgentes de transferencias o imposibilidad de localizar a los interlocutores habituales).

Una de las dificultades para detectar este tipo de amenazas es que pueden tener un **bajo componente tecnológico**, **se orienta directamente al factor humano**, por lo que las medidas TIC implantadas no consiguen los niveles de protección adecuados.

La preparación de un ataque BEC es minuciosa, ahí reside la clave de su éxito: los atacantes pasan un tiempo relevante investigando a la víctima y su entorno profesional, realizando reconocimientos y configurando la infraestructura antes de ejecutar el ataque. En muchos casos se utiliza directamente el teléfono (en el idioma de la víctima) o la documentación postal, lo cual hace mucho más creíble el engaño.

Solo en mayo de 2020, **los ataques BEC se incrementaron en un 200%**. También **aumentó en un 36% el número de organizaciones afectadas**[34]. Así pues, resulta imprescindible continuar con la formación y concienciación de los empleados, siendo recomendable ampliar estas prácticas a contratistas, proveedores y clientes.

Conviene asimismo establecer canales oficiales y procedimientos formales para notificar cambios en cuentas bancarias, comunicación de datos fiscales o reclamaciones de facturas pendientes. Se recomienda igualmente la implantación de sistemas que permitan comprobar la autenticidad de remitentes y destinatarios en comunicaciones electrónicas, siendo la **firma digital del correo electrónico** una práctica robusta y poco extendida entre sectores no vinculados a las TIC.

MALWARE A MEDIDA

Junto al ransomware y al BEC, los ciberdelincuentes han aprovechado la crisis sanitaria para lanzar **campañas masivas de phishing con la pandemia como reclamo**[35], y también han hecho uso del **malware** en un sentido más amplio, llegando a convertir troyanos conocidos en malware modular para cubrir una superficie de ataque mayor.

Hace ya tiempo que estos mecanismos se comercializan directamente en la Dark Web como un servicio contratable, conocido como ***Malware as a Service* (MaaS)** y operado directamente por el crimen organizado. Esta oferta de malware "a medida" permite a delincuentes no expertos utilizar funcionalidades de malware avanzado en todo tipo de crímenes.

34. Véase https://abnormalsecurity.com/blog/invoice-payment-fraud-bec-attacks-are-on-the-rise/
35. Véase https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/9716-ccn-cert-al-05-20-repunte-campanas-de-phishing-por-covid-19.html

4.3 Hacktivismo

Aunque durante 2020 **la actividad relacionada con grupos hacktivistas ha mantenido su tendencia decreciente**, se han registrado múltiples incidentes, derivados muchos de ellos de la evolución de la pandemia. Se siguen utilizando las mismas Técnicas, Tácticas y Procedimientos (TTP) observadas en operaciones de años anteriores, como el uso de herramientas *open source* para[36]:

- Ejecutar **ataques de denegación de servicio** (DoS y DDoS), provocando que los activos web no estén disponibles (principalmente se dirigen a sitios web de gobiernos).
- Realizar ***defacements*** (desconfiguraciones web), modificando la apariencia del sitio web y publicando contenido relacionado con la operación, en ocasiones indicando el *hashtag* de la misma.
- Realizar **inyecciones SQL** (SQLi) para exfiltrar información de las bases de datos y publicarla.
- **Doxxing**, que consiste en obtener la máxima información privada relacionada con un objetivo para publicarla después en fuentes públicas.

TWITTER, TERRITORIO HACKTIVISTA

Entre los canales de comunicación empleados para distribuir propaganda o información de movimientos hacktivistas destaca el uso de **Twitter**. Esta plataforma permite llegar a una gran audiencia a nivel mundial, algo idóneo tanto para dar notoriedad al movimiento como para captar seguidores. Habitualmente, estos movimientos hacen uso de un hashtag formado por la adición de la cadena "#Op" ante algún elemento identificativo de su causa. Cabe destacar que, debido a los términos de servicio (ToS) de Twitter, con frecuencia las cuentas relacionadas con movimientos hacktivistas acaban siendo suspendidas.

En este sentido, una de las operaciones más relevantes de 2020 ha sido la desencadenada tras la muerte de George Floyd en Minneapolis el 25 de mayo de 2020. Como apoyo al movimiento **Black Lives Matter** se generó una operación hacktivista que empleaba el hashtag **OpGeorgeFloyd**[37]. El 28 de mayo de 2020, Anonymous publicó un vídeo[38] en Facebook en el que se anunciaban ataques dirigidos a los departamentos de policía de todo Estados Unidos[39].

36. Véase https://corporatefinanceinstitute.com/resources/knowledge/other/hacktivism
37. Véase https://securityboulevard.com/2020/06/analysis-of-the-top10-hacktivist-operations/
38. Véase https://www.facebook.com/anonews.co/videos/285581555919237/
39. Véase https://www.the-parallax.com/anonymous-kpop-hacktivism-2020/

En 2020 también se han detectado grupos de hacktivistas como **Ghost Squad Hackers** (GSH), una rama del grupo hacktivista **Anonymous** que ha reactivado su actividad con el objetivo de agravar las tensiones sociales y políticas, comprometiendo sitios web de gobiernos en respuesta a su gestión de la pandemia[40]. Los ataques de GSH tuvieron lugar en **Australia, India, Pakistán, Tailandia y Zimbabue**. Principalmente se trató de *defacements*, aunque también llegaron a contar con permisos de administrador en un servidor del gobierno indio y a filtrar cuentas administrativas del gobierno australiano[41].

En julio de 2020, Twitter sufrió uno de sus mayores ataques hasta la fecha[42], quedando expuesta información de personas muy influyentes y de diferentes cuentas de empresas.

ELECCIONES DE EXCEPCIÓN

En el ámbito electoral, en España se celebraron elecciones en el País Vasco y en Galicia. Inicialmente, los comicios estaban previstos para el 5 de abril, pero fueron retrasados al 12 de julio por motivos sanitarios.

En ninguno de los casos se registraron incidentes relevantes en términos de hacktivismo.

4.4 Actores internos

El **62%** de los incidentes de ciberseguridad están relacionados o causados por empleados que han cometido alguna **negligencia de seguridad**. Este dato revela que los *insiders* **involuntarios** son la amenaza interna más común dentro de las organizaciones. Un porcentaje menor de incidentes procedería de los **actores internos intencionados,** que representarían un **14%**.

En el primer caso (*insiders* involuntarios), expertos en ciberseguridad declaran que el phishing representa el **vector de ataque** más utilizado contra los actores internos más vulnerables de una organización; hasta en un **38%** de los incidentes involuntarios provocados por actores internos se han originado a través de este vector de ataque[43]. Todo ello sitúa al personal interno como uno de los agentes de amenaza más presente en los próximos periodos.

Asimismo, los actores vinculados a Estados están **adaptando cada vez más sus TTP** a los escenarios y organizaciones que tienen como objetivo. Estos actores buscan persistentemente a los **usuarios más vulnerables** dentro de la organización para desarrollar sus campañas, en muchas ocasiones convirtiéndoles parte del vector de entrada mediante ataques

40. Véase https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf
41. Véase https://www.darkreading.com/attacks-breaches/could-return-of-ghost-squad-hackers-signal-rise-in-covid-19-related-hactivism/d/d-id/1337588
42. Véase https://www.dfs.ny.gov/Twitter_Report
43. Véase https://financesonline.com/insider-threat-statistics/

de *spear phishing*. En 2020, más del **35%** del total de infracciones y filtraciones de datos cibernéticos fueron el resultado directo de amenazas internas[44].

Las amenazas o actores internos pueden tener un severo impacto negativo en la organización en materia de **espionaje económico, sabotaje, fraude y pérdida de recursos corporativos**. Los principales atacantes interesados en llevar a cabo este tipo de acciones serían servicios de **inteligencia extranjeros** o **criminales** con intereses económicos. También hay que tener en cuenta que las negligencias o las faltas de atención por parte de los empleados, también pueden incrementar los casos de amenazas internas dentro de una organización.

La principal amenaza interna en las organizaciones son los empleados que cometen negligencias de forma involuntaria

RIESGOS INTERNOS EN PANDEMIA

La situación de pandemia ha incrementado ciertos factores de riesgo asociados a los actores internos:

- Han aumentado los niveles de **estrés psicológico** de los profesionales de ciertos sectores como **sanidad**, **centros de investigación** o **seguridad**, entre otros. Esta nueva situación de estrés podría incrementar significativamente las **alteraciones de conducta** de los empleados de una organización. Dichas alteraciones podrían aumentar la probabilidad de que los empleados no siguiesen rigurosamente los **protocolos de ciberseguridad**.

- Por otro lado, la **situación sociofamiliar individual** de cada miembro de la organización, combinada con el mencionado **estrés de ciertos puestos de trabajo**, puede tener un impacto negativo en la correcta aplicación de las medidas de ciberseguridad corporativas.

- El **teletrabajo** también puede incrementar los niveles de riesgo respecto a los actores internos. La significativa **interdependencia** hacia los dispositivos tecnológicos y de información podría hacer que se utilicen dispositivos menos seguros, algo que podría ser aprovechado por actores internos y externos para comprometer los sistemas de una organización.

44. Véase https://perspecta.com/sites/default/files/2021-01/Cybersecurity%202021%20trends%20and%20rec%20wp_online.pdf

05 Incidentes 2020

En lo que respecta a ciberseguridad, en 2020 se han superado los peores pronósticos. Ha sido **el año del apogeo de los ciberatacantes más avanzados**. La COVID-19 ha tenido un efecto catalizador que ha puesto de manifiesto la situación de vulnerabilidad de la gran mayoría de las empresas y organismos: en términos generales, muchas de estas entidades no estaban preparadas en términos de ciberseguridad.

En este escenario, la industria del **cibercrimen** ha visto una gran oportunidad y ha actuado con dureza, modificando los cebos y objetivos de sus ataques y mejorando sus técnicas para robar dinero o información a empresas o pedirles un rescate por liberar sus recursos,

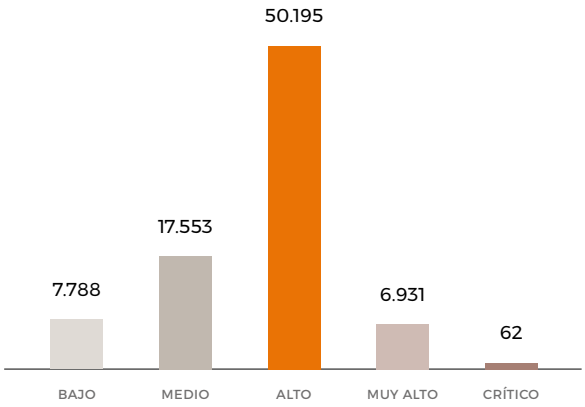
Por su parte los **actores APT**, como era de esperar, se han adaptado de manera muy ágil al nuevo escenario para **espiar, robar la propiedad intelectual o cumplir otros propósitos gubernamentales**.

En cuanto al panorama actual a nivel nacional, los datos presentados por el CCN-CERT en las XIV Jornadas STIC no dejan de ser alarmantes: no solo se ha registrado un aumento más que notorio de ciberincidentes, sino que también ha aumentado la gravedad de estos.

CIBERINCIDENTES EN CIFRAS

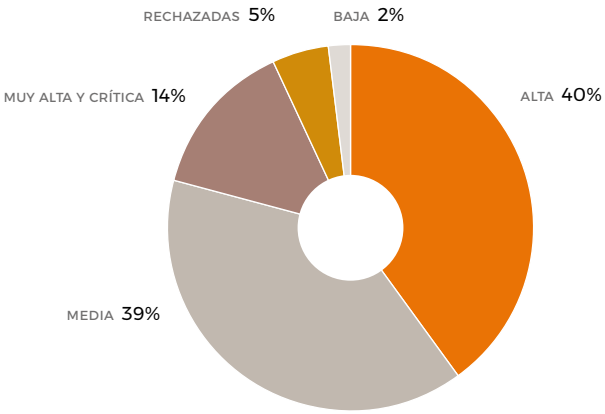
Poniendo el foco en las cifras, en 2019 se detectaron 3.172 ciberincidentes de peligrosidad muy alta, mientras que en 2020 se han duplicado hasta alcanzar casi los 7.000. El CCN-CERT ha detectado **82.530 incidentes durante el año 2020**, mientras que en el año anterior se reportaron en torno a 43.000. Esto supone un **crecimiento** respecto a los años previos, también fruto de la automatización introducida en los sistemas de detección de ataques del CCN-CERT que le ha permitido notificar más incidentes.

La siguiente gráfica muestra la distribución de ciberincidentes de 2020 según su peligrosidad[45]:



45. Véase https://www.ccn-cert.cni.es/pdf/documentos-publicos/xiv-jornadas-stic-ccn-cert/ponencias-1/5641-s19-d30-01-informe-anual-retos-2021/file.html

Por otro lado, el Instituto Nacional de Ciberseguridad (**INCIBE**), a través de INCIBE-CERT, ha gestionado **133.155 incidentes de ciberseguridad durante el año 2020**, de los cuales 106.466 hacen referencia a ciudadanos y empresas, 1.190 a operadores estratégicos y 25.499 a la Red Académica y de Investigación Española **(RedIRIS).** La siguiente gráfica muestra la distribución de estos incidentes según su criticidad [46]:



En cualquier caso, hay que tener en cuenta que estos datos son solo los que se han comunicado y detectado mediante canales oficiales, pero no hay que olvidar que existen muchos otros incidentes que no llegan a ser contabilizados, por lo que **la imagen real puede ser incluso peor**. Estas tasas tan **alarmantes con actores de la ciberamenaza cada vez más organizados hacen que e**l sector de la ciberseguridad se enfrente a retos cada vez más complejos, y sin duda los esfuerzos para combatir los ciberataques deberán ser cada vez mayores.

2020 ha sido el año de apogeo de los ciberataques: más ciberincidentes y más peligrosos que nunca

46. Véase https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2020_incibe.pdf

5.2 Ciberespionaje

La crisis sanitaria también ha supuesto un cambio fundamental en las tendencias de **ciberespionaje** en 2020. Con todos los países invirtiendo sus recursos en el desarrollo de una vacuna contra la COVID-19, el hecho de **ser el primer país en disponer de una vacuna eficaz tiene un componente geopolítico indiscutible**. Por ello, hay Estados que han convertido la obtención de información sobre la vacuna en una de sus máximas prioridades, poniendo a laboratorios, centros de investigación y empresas farmacéuticas en el punto de mira de sus grupos de ciberespionaje.

Sobre AstraZeneca se ha publicado que ha sufrido estos intentos de **ataque**. Asimismo, datos relativos a las vacunas de Pfizer fueron **robados** de la EMA (*European Medicines Agency*). Moderna tampoco se ha salvado de los intentos de **intrusión**.

La COVID-19 ha sido un gran pretexto para el ciberespionaje: se han detectado cientos de dominios falsos suplantando a entidades gubernamentales relacionadas con la pandemia, usados para el envío de ataques dirigidos con correos dañinos.

ATAQUE A LA CADENA DE SUMINISTRO (EL CASO SOLARWINDS)

Sin duda, el protagonista indiscutible de las operaciones de ciberespionaje en 2020 ha sido la compañía **SolarWinds**, que ofrece, entre otros tipos de software, productos de gestión de redes utilizado por más de 30.000 clientes de múltiples sectores a nivel internacional. En primavera de 2020 sufrió una intrusión atribuida al grupo APT29[47], en la que los atacantes lograron modificar el código de una de sus aplicaciones de gestión de red para introducir una puerta trasera. Esta modificación fue transmitida a todos los clientes, lo que desplegó la puerta trasera en miles de organizaciones y afectó a casi 18000 entidades del sector público y privado, entre ellas diversos departamentos del gobierno americano. El incidente tuvo múltiples derivadas, siendo una de las más importantes el acceso de los atacantes a parte del código fuente de la **nube** de Microsoft.

Este ataque ha supuesto un punto de inflexión entre las relaciones entre Estados Unidos y Rusia. El presidente Joe Biden ha declarado que establecerá un conjunto de **sanciones** contra Rusia,

El ataque a SolarWinds ha sido el incidente más importante de robo de información

47. El 15 de abril de 2021 el gobierno de los Estados Unidos de América atribuyó este ataque al grupo conocido como APT29, del Servicio de Inteligencia Exterior (SVR) ruso: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

continuando con la política instaurada por el Departamento de Justicia estadounidense contra los ciberataques (por ejemplo, con las acusaciones contra siete ciudadanos chinos por intrusiones en más de un centenar de compañías estadounidenses bajo el paraguas del grupo APT41). Tanto la Unión Europea como el Reino Unido han establecido **sanciones** contra Rusia por la intrusión en 2015 en el Parlamento Federal alemán, por lo que se espera que esta tendencia siga consolidándose en los próximos años como una medida de presión (imposición de costes) sobre otros Estados sobre los que se pueda realizar una debida atribución.

ACCESOS REMOTOS, NUEVA PUERTA DE ENTRADA

Los accesos remotos son un punto de entrada que ha sufrido un aumento exponencial en 2020: la pandemia ha forzado a muchas empresas al **despliegue del teletrabajo**, en muchos casos de forma precipitada, haciendo uso de arquitecturas no seguras y/o sin prestar la debida atención a una configuración segura de las mismas. Los grupos de ciberespionaje se han volcado en los diversos sistemas de acceso remoto, encontrando y explotando múltiples vulnerabilidades en diversos productos. Cabe destacar el uso de CVE-2019-19781 por parte de APT41 en una campaña masiva de infecciones a principios de 2020, o el empleo de múltiples vulnerabilidades, por parte de numerosos grupos a lo largo del año, lo cual resalta la importancia de la seguridad del acceso remoto en todas sus facetas.

Los ataques al correo electrónico han sido también un vector de entrada muy importante: una **vulnerabilidad** en el servidor de correo Exchange fue empleada por diversos actores para el despliegue de *webshells*, estableciendo accesos a nivel de servidor que permitían a los atacantes acceder a todo el correo (incluso después de aplicar el parche). Los servicios de correo también han sufrido en 2020 un incremento destacable en los ataques de *password spraying* (modalidad en la que los atacantes prueban una única contraseña en cientos de cuentas, evitando su bloqueo), detectados en centenares de direcciones IP.

CIBERESPIONAJE CON RANSOMWARE

Pero quizás la tendencia más inquietante es la observada en un incidente con el grupo APT27, que procedió al despliegue de un **ransomware** sobre la organización atacada. Todavía es pronto para ver si los grupos de ciberespionaje adoptan esta táctica (razonable desde un punto de vista táctico, ya que obliga a los defensores a centrar sus esfuerzos en el ransomware), pero incita a extremar la precaución en las medidas de seguridad.

El ciberespionaje ha tenido un objetivo claro en 2020: la vacuna contra la COVID-19

5.2 Operaciones disruptivas y de control

Una de las acciones con más impacto en las víctimas de grupos, tanto de ciberdelincuentes como de actores esponsorizados por gobiernos, son los **ataques disruptivos**. Se trata de ataques que emplean malware, generalmente de tipo **ransomware**, así como **minado de criptomonedas**, y se apoyan en artefactos de control remoto para dejar inutilizados tanto sistemas como procesos productivos. Perpetrar una acción de este tipo no solo es posible mediante software dañino, sino que se pueden utilizar cantidades ingentes de tráfico generado de diversas formas para atacar los sistemas de una organización expuestos en Internet. Es lo que se denomina **DDoS**, o **denegación de servicio distribuida**. En 2020, este tipo de operaciones han mantenido su tendencia al aumento.

LA DOBLE EXTORSIÓN, UNA TÉCNICA AL ALZA

En el ámbito internacional, el 27 de julio de 2020 la empresa tecnológica de soluciones de navegación **Garmin** informó que varios de sus sistemas (web, atención al cliente y comunicaciones internas de la compañía) quedaron bloqueados e inutilizados por un ataque que consiguió paralizar sus sistemas de producción.

Otro ejemplo que confirma la tendencia de las bandas de ciberdelincuentes hacia la **doble extorsión** y que se comenzó a observar en 2019 es el caso del gigante alemán del software **AG**. Esta técnica **consiste tanto en la disrupción de los procesos productivos como en el robo y publicación de información confidencial de la compañía**. El 3 de octubre de 2020 los sistemas de la compañía dejaron de funcionar por el ransomware Clop (variante de CryptoMix), para posteriormente ser instados a pagar un rescate de 20 millones de dólares, a lo cual la compañía se negó.

La doble extorsión combina la disrupción de los procesos productivos con la publicación de información confidencial

Los ciberdelincuentes cumplieron su promesa e hicieron pública la información sustraída, que consistía en información financiera, pasaportes de los empleados y correos electrónicos internos. Los operadores de Clop no son los únicos que utilizan la doble extorsión para materializar sus acciones ofensivas: muchas bandas de cibercriminales en este ámbito lo están haciendo, confirmando la tendencia al alza de este tipo de amenazas.

Estos casos presentan la similitud de que **los atacantes utilizan software dañino** para realizar las acciones de disrupción. No obstante, en 2020 también se han identificado **ataques DoS o DDoS** de los denominados **de agotamiento**; en este sentido, y continuando en el plano internacional, se han registrado numerosos casos durante el año: plataformas de videojuegos como Blizzard, Xbox o Steam, empresas de telecomunicaciones como la noruega Telenor o la francesa OVH, escuelas y universidades o incluso plataformas online de criptomonedas, como bitcoint.org, han sido víctimas de este tipo de ataques.

Los actores que normalmente se encuentran detrás de este tipo de acciones siempre están buscando **nuevas maneras de realizar denegación de servicio con un caudal de tráfico mayor y más sostenido en el tiempo**. Los atacantes necesitan identificar nuevos dispositivos y software conectado a la red de Internet que les permita amplificar el caudal de tráfico de una manera más significativa. Para ello se suele optar por servicios publicados que se comuniquen mediante el protocolo UDP en el que se pueda suplantar la dirección IP origen para asociarla a la víctima. La empresa de ciberseguridad Kaspersky ha identificado el uso durante 2020 de un nuevo servicio expuesto que hace uso del protocolo mencionado y que corresponde con el interfaz DTLS (*Datagram Transport Layer Security*) de los dispositivos Citrix ADC (*Application Delivery Controller*); la explotación de este servicio permite al atacante amplificar hasta 36 veces el tráfico remitido, obteniendo una ratio bastante importante en los ataques, dentro de las técnicas de agotamiento, denominados de amplificación.

5.3 Influencia y noticias falsas

El uso de Internet y las redes sociales se ha multiplicado durante la crisis sanitaria. Tan solo en **España** se han contabilizado **42,5 millones de usuarios de Internet** y un **aumento de casi el 30% de usuarios en redes sociales**. Estos aumentos son extrapolables a nivel mundial[48]. Una de las causas de dicho incremento ha sido la ampliación del teletrabajo en la población española: mientras que en años anteriores solo un 4% de los españoles teletrabajaba, el confinamiento y las restricciones de movilidad han hecho aumentar ese porcentaje hasta el 16,4%.

48. Véase https://wearesocial.com/es/blog/2020/01/digital-2020-el-uso-de-las-redes-sociales-abarca-casi-la-mitad-de-la-poblacion-mundial

TELETRABAJO E INGENIERÍA SOCIAL

La eclosión del **teletrabajo** ha conllevado un gran **aumento del número de potenciales objetivos para las campañas de ingeniería social**. También ha supuesto que usuarios poco familiarizados con la tecnología tengan que usarla a diario en su trabajo, siendo más vulnerables[49]. En esta situación han aparecido muchos actores hostiles que usan el nombre de una marca u organización para hacer creer al usuario que ha recibido un mensaje legítimo. El objetivo de esta estrategia es engañar a la víctima para que realice una acción no deseada, como la descarga de malware en el equipo corporativo, la revelación de sus credenciales de acceso, el envío de información personal o el despliegue de publicidad no deseada en su dispositivo.

En 2020, estos factores han registrado un aumento del 200% respecto al año anterior y a este tipo de amenazas, dejando constancia del poder que ejercen sobre los usuarios los actores hostiles que se aprovechan del temor a la pandemia para sacar beneficio.

NOTICIAS FALSAS, AMENAZA EMERGENTE

Por otra parte, la **excepcionalidad** que ha caracterizado a 2020, tanto por el gran consumo de información de origen virtual debido al confinamiento, como por el carácter emocional de la situación, ha supuesto una **ventana abierta a las noticias falsas, que se han propagado rápidamente entre los ciudadanos**, en algunos casos con graves consecuencias para su salud y su seguridad.

La información no contrastada, las advertencias mal interpretadas y las teorías de la conspiración han generado **confusión** entre la población, facilitando en muchos casos el éxito de los ciberataques[50]. Según datos de INTERPOL, cerca del 30 % de los países que participaron en una encuesta mundial sobre ciberdelincuencia confirmaron la circulación de información falsa sobre la COVID-19. Asimismo, se reportaron casos de noticias falsas vinculadas al comercio ilegal de productos médicos no legítimos[51].

La información falsa sobre la COVID-19 y las teorías de la conspiración han generado confusión y han propiciado ataques

49. Véase https://elpais.com/economia/2020-09-17/el-teletrabajo-se-triplica-en-espana-por-la-pandemia.html
50. Véase https://www.muyseguridad.net/2021/01/02/desinformacion-ciberseguridad/
51. Véase https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

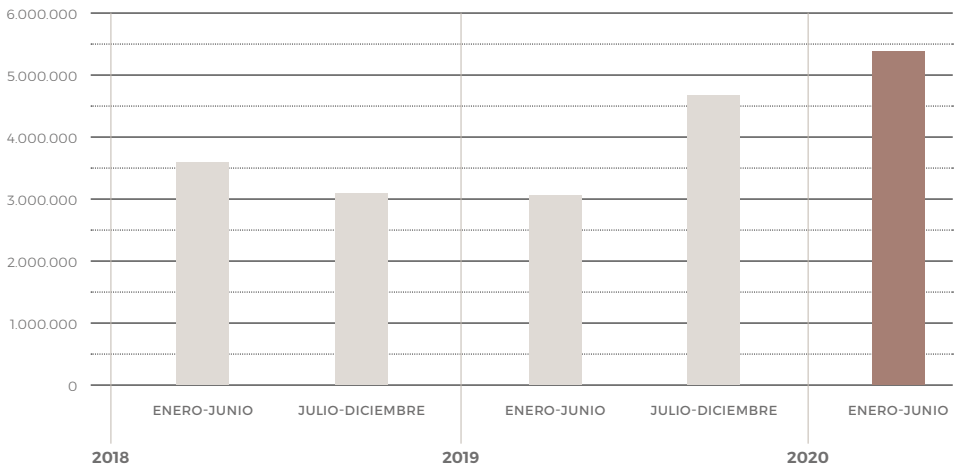
TWITTER: UN PASO ADELANTE EN VERIFICACIÓN

Una de las plataformas más afectadas por las noticias falsas es **Twitter**, que sigue siendo una de las redes sociales más utilizadas, de ahí que su uso no legítimo también se vea incrementado. Esta actividad ilegítima incluye, entre otros, spam, automatizaciones dañinas y cuentas falsas. En el último informe de transparencia de esta red social se puede observar el crecimiento de esta tendencia: solo en la primera mitad del año 2020 se detectaron más de 5,4 millones de intentos de uso no legítimos de la plataforma[52]:

En consecuencia, durante 2020 **Twitter ha actualizado sus políticas contra la desinformación incluyendo etiquetas de advertencia sobre el contenido del tuit**. Se ha comenzado a etiquetar a aquellos medios que están controlados por un Estado (según la propia investigación y evaluación de Twitter en base a un conjunto de criterios desarrollados para este propósito). De este modo, el usuario queda advertido de que puede estar ante información que no es totalmente imparcial o contrastada[53]. Otras redes sociales como Facebook o Instagram también han reforzado su postura respecto a la tendencia creciente de las noticias falsas y los perfiles con objetivos malintencionados.

A pesar de la mejora de las defensas en ciertas redes sociales, los atacantes siguen innovando en las técnicas para pasar desapercibidos. Resulta especialmente relevante el uso del aprendizaje automático (*machine learning*) y la inteligencia artificial para la generación de imágenes de perfil de cuentas falsas. Se trata de una técnica detectada por el Observatorio de Internet de la Universidad de Stanford en más de 1.500 cuentas generadas entre enero y mayo de 2020[54].

INTENTOS DE USO NO LEGÍTIMO DE LA PLATAFORMA TWITTER



52. Véase https://transparency.twitter.com/en/reports/platform-manipulation.html#2020-jan-jun
53. Véase https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.html
54. Véase https://cyber.fsi.stanford.edu/io/news/twitter-takedown-october-2020

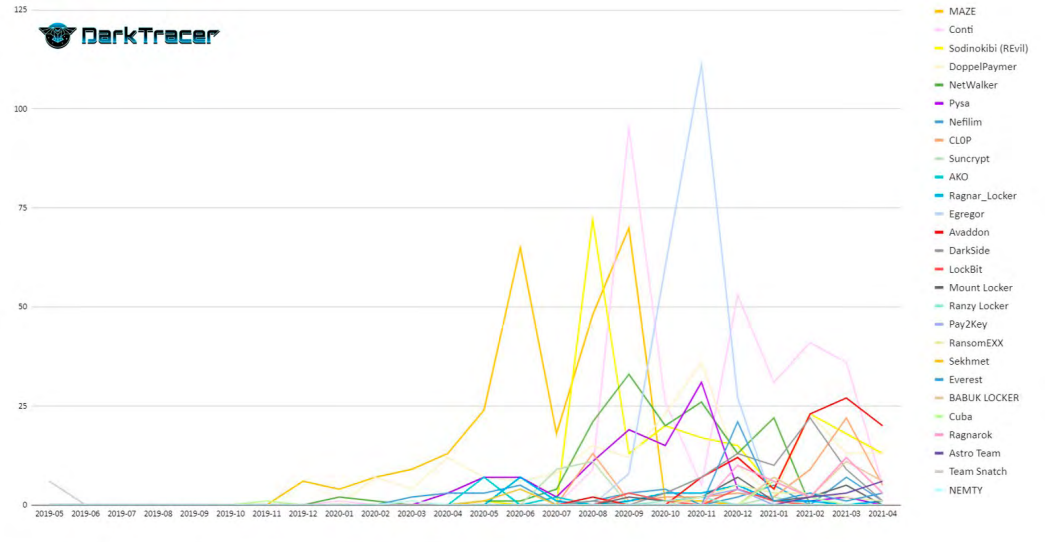
5.4 Operaciones delincuenciales

Ya hemos visto que uno de los métodos de ataque que sigue reinando es el **ransomware**. En 2020 se ha presentado no solo en su formato más habitual, consistente en el envío de código dañino a un número elevado de potenciales víctimas, sino que cada vez es más frecuente encontrar versiones sofisticadas y perfeccionadas, como los **HOR (*Human Operated Ransomware*)**, con objetivos más claros y dirigidos.

DOBLE EXTORSIÓN

Como ya se ha nombrado al hablar de la disrupción de servicios, la **doble extorsión** es el nuevo filón del ransomware. Si bien un ransomware común suele cifrar los datos a cambio de solicitar un rescate, cada vez es más frecuente sustraer esos datos y amenazar a las víctimas con hacerlos públicos, normalmente en sitios de la Dark Web administrados por los propios operadores del ransomware. Aunque esta técnica se inició en 2019 con las familias "Team Snatch" y "Maze", el año 2020 ha sido el de la consolidación de esta técnica de ataque, con más de 1.800 víctimas[55], como se puede ver en la siguiente imagen[56]:

HISTORIA DE LAS ACTIVIDADES DE DIVULGACIÓN DE LAS VÍCTIMAS DE LAS BANDAS DE LA DARKWEB



Fuente: https://twitter.com/darktracer_int/status/1382622655052869637

55. Véase https://drive.google.com/file/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3/view
56. Fuente: https://twitter.com/darktracer_int/status/1382622655052869637

RANSOMWARE EXPRÉS

Siguiendo con los *Human Operated Ransomware*, otro hito que han conseguido los atacantes en 2020 ha sido la **velocidad** a la que han conseguido moverse por las redes de las víctimas para hacer el **máximo daño posible en el mínimo tiempo**. En este aspecto, el claro vencedor es el ransomware **Ryuk**, del que se han documentado casos en los que han tardado 5[57] e incluso 2[58] horas desde el despliegue del malware inicial hasta el cifrado completo de los datos de la organización. Con estos tiempos, incluso los equipos de seguridad más competentes sufrirían para ser capaces no solo de generar las alertas necesarias, sino de procesarlas y escalarlas para tomar las medidas de contención adecuadas. Ante este contexto, urge aplicar medidas de automatización en el despliegue de medidas de seguridad, las conocidas como herramientas SOAR (*Security Orchestration, Automation and Response*).

Los ciberdelincuentes también están **diversificando los objetivos** de sus acciones con ransomware. A los ataques a sistemas Windows han ido añadiendo ataques a sistemas bajo otros sistemas operativos, entornos virtuales, despliegues IoT. Por objetivos, tanto infraestructuras críticas o esenciales e incluso instituciones destinadas a combatir la pandemia se han visto amenazadas. En el caso de las instituciones sanitarias, su objetivo no es tanto la sustracción de los datos en sí, sino imposibilitar el acceso a los mismos y obligar a las víctimas a pagar grandes sumas económicas para ver restablecidas sus operaciones.

Tal como se desprende del informe de amenazas ransomware de Palo Alto Networks[59], en 2020 los ciberataques de este tipo han ocasionado un aumento del 171% en el precio medio que se pide por el rescate. Además, como indica Kaspersky en uno de sus informes[60], aunque más de la mitad de las víctimas pagó rescates relacionados con ataques de ransomware durante 2020, solo alrededor de una cuarta parte de las víctimas consiguieron recuperar todos los datos cifrados. Conviene destacar este dato, que demuestra que **pagar el rescate no implica que se vayan a recuperar los datos**. Además, y sin entrar en el ámbito legal, lo único que se consigue es perpetuar las actividades de los delincuentes.

2020 también pasará a la historia por ser el año en el que se produjo la **primera víctima mortal relacionada con un ataque de ransomware**. Según indican las autoridades alemanas, se trataría de un paciente que murió durante el traslado desde un hospital afectado por un ransomware a otro centro donde iba a ser atendido[61].

Pese a que estos datos indiquen que los atacantes del ransomware siempre ganan, **también hay noticias positivas**: por ejemplo, los responsables del ransomware Maze, uno de los más prolíficos hasta

57. Véase: https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/
58. Véase: https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/
59. Véase https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/
60. Véase: https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned
61. Véase https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/

el momento, decidieron dejar de operar a partir del mes de octubre[62]. Otro de los grupos que cesó su actividad, en abril de 2020, fue el encargado del ransomware Shade[63].

A modo de conclusión sobre el ransomware, son de mención obligada los dos principales sitios con información relativa a este tipo de amenazas: **ID Ransomware**[64] y **No More Ransom!**[65], y la herramienta **microCLAUDIA**[66]**,** del CCN-CERT, cuyo objetivo principal es vacunar a los equipos Windows contra las principales técnicas usadas por las variantes de ransomware existentes.

El ransomware es cada vez más sofisticado, con variantes como la doble extorsión y ataques más rápidos y dañinos

FRAUDE DEL CEO

Otro mecanismo de estafa que ha visto incrementado su uso ha sido el conocido como **fraude del CEO**, un tipo de táctica BEC (*Business Email Compromise*). En este ataque, el delincuente, para ganar credibilidad ante sus víctimas, suplanta la identidad del propietario o director de la empresa (también conocido como CEO, siglas en inglés de *Chief Executive Officer*), o bien de un responsable de una empresa u organización, para defraudar a la empresa y a sus empleados, clientes, proveedores, etc.

En la mayoría de los casos, **estos ataques se dirigen hacia personal relacionado con la contabilidad y las finanzas** de las empresas, ya que el foco suele estar en la realización de transferencias bancarias fraudulentas, el secuestro de conversaciones con proveedores o la modificación de datos de facturas para redirigir los pagos a un proveedor, de manera que el montante económico termine en manos de los atacantes.

Para socavar las finanzas de las empresas, los atacantes falsifican cuentas y sitios web corporativos (normalmente mediante ligeras modificaciones del nombre), envían correos de phishing dirigido (*spear phishing*) o introducen malware específico para analizar previamente los correos y no levantar sospechas, o bien para acceder a datos confidenciales de las potenciales víctimas[67].

62. Véase https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/
63. Véase https://www.cyberdefensemagazine.com/shade-ransomware-gang-shut-down-operations-and-releases-750k-decryption-keys/
64. Véase https://id-ransomware.malwarehunterteam.com/
65. Véase https://www.nomoreransom.org/es/index.html
66. Véase https://www.ccn-cert.cni.es/soluciones-seguridad/microclaudia.html
67. Un ejemplo de este tipo de ataques se puede ver en la sesión de VANESA "Cómo te levantan 100.000€ sin pestañear"

El fraude del CEO está en auge: tan solo entre el segundo y tercer trimestre de 2020 experimentó un crecimiento del 15%[68]. Dentro de esta modalidad, los ataques que empleaban **fraude en facturas o pagos** aumentaron en un 155%, lo que lo convierte en el tipo de táctica BEC más utilizada. En el caso de **administraciones públicas españolas y sus proveedores**, los atacantes se han servido de datos obtenidos en los portales de contratación pública para dar más credibilidad a sus estafas y conseguir engañar a sus víctimas.

El fraude del CEO es la táctica BEC más habitual. Se suplanta a un superior para engañar al empleado

CRYPTOJACKING

La última de las técnicas de estafa que queremos destacar es el ***cryptojacking***, también conocido como **criptominería** o minería de criptomonedas maliciosa. Consiste en el uso no autorizado de los recursos de un dispositivo para minar criptomonedas mediante la ejecución de código dañino, sin necesidad de interacción por parte del usuario víctima, por lo que no es fácil de detectar y puede pasar desapercibido.

Aunque pueda parecer una actividad no delictiva, ya que lo único que se consume es la potencia del ordenador de la víctima, lo cierto es que se utiliza **con fines delictivos y sin el conocimiento ni consentimiento de las víctimas**. El delincuente obtiene un beneficio: crea divisas de manera ilícita, lo cual le reporta un beneficio económico directo.

Aunque en muchos casos las herramientas de minado se instalan en servidores comprometidos, este tipo de ataque no tiene consecuencias negativas en cuanto a pérdida de información o secuestro de datos, aunque sí puede tener un impacto económico en las organizaciones: aumentarán sus costes de TI y su consumo de electricidad, y sus sistemas informáticos se verán degradados.

Ya en 2019 se percibió un descenso de esta práctica, según indica el informe de ENISA sobre el tema[69]. Esto se debió en parte a una gran redada coordinada por INTERPOL que, entre finales de 2019 y principios de 2020, consiguió reducir drásticamente el número de mineros[70] en el sudeste asiático. Aunque parecía relegada a un segundo plano, **la revalorización de las criptomonedas desde el mes de marzo de 2020 ha comportado el incremento de esta estafa en más de un 160%**, según investigaciones de Symantec[71].

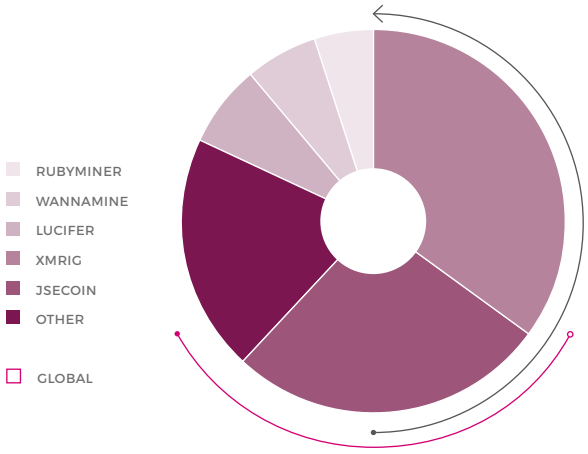
68. Véase https://info.abnormalsecurity.com/rs/231-IDP-139/images/AS_Qtrly_BEC_Report_Q3_2020.pdf
69. Véase https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cryptojacking
70. Véase https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-led-action-takes-aim-at-cryptojacking-in-Southeast-Asia
71. Véase https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-trends-q2-2020

A nivel global, entre el malware de criptominería destaca **XMRig**. Aunque es una herramienta de código abierto[72] que originalmente se diseñó con fines legítimos, su funcionalidad y versatilidad ha hecho que un gran número de atacantes la utilicen con fines malintencionados. También cabe mencionar la aparición de **Lucifer**[73], un malware multiplataforma que integra minería de criptomonedas Monero con otro tipo de ataques DDoS o ejecución remota de código, y del grupo **TeamTNT**[74], que creó una versión personalizada de una herramienta de gestión de infraestructuras Docker, Kubernetes y en la nube para poder minar en estas plataformas sin ser descubierto.

Por último, hay que mencionar el malware **KingMiner**[75]: en su afán por no ser descubiertos, estos atacantes actualizaban los equipos que infectaban, para evitar que otros atacantes consiguieran comprometerlos y utilizarlos para sus estafas al mismo tiempo que ellos[76].

El mundo del criptominado es oscilante: hacia el último trimestre de 2020, coincidiendo sobre todo con el lanzamiento de las nuevas series de tarjetas gráficas por parte de NVidia y AMD, la producción de criptomonedas ha virado de nuevo hacia el uso de tarjetas gráficas, y ya no es tan provechoso realizar tareas de minado en equipos de oficina o servidores, que no suelen contar con tarjetas gráficas potentes. No obstante, en el futuro es factible contemplar periodos de más actividad asociada a esta problemática si aparecen nuevas monedas de fácil minado o si se detectan problemas con los sistemas de minado actuales.

PRINCIPALES MALWARE DE CRIPTOMINERÍA A NIVEL MUNDIAL



72. Véase https://github.com/xmrig/xmrig
73. Véase https://unaaldia.hispasec.com/2020/08/lucifer-el-malware-para-criptominado-y-ddos-llega-a-linux.html
74. Véase https://www.bleepingcomputer.com/news/security/hackers-use-legit-tool-to-take-over-docker-kubernetes-platforms/
75. Véase https://www.bleepingcomputer.com/news/security/kingminer-patches-vulnerable-servers-to-lock-out-competitors/
76. Véase fuente: https://www.checkpoint.com/downloads/resources/cyber-security-report-2021.pdf

5.5 Brechas de datos

En cuanto a incidentes concretos relacionados con **brechas de seguridad que afectan a datos personales**, es destacable que todas las fuentes señalan que este tipo de incidentes **se produce casi a diario, aunque en muchos casos no salen a la luz**. En la mayoría de los casos, la motivación es económica: cuando los ciberdelincuentes, a través de malware, phishing, técnicas de ingeniería social o cualquier otro método, consiguen acceder a los datos, piden un rescate a cambio de que éstos no sean publicados. La AEPD gestionó, durante el periodo comprendido **entre el 1 de enero y el 31 de diciembre de 2020**, un total de **1.370 de brechas de seguridad**.

A continuación, se citan **las brechas de datos que más repercusión han tenido** a lo largo de 2020:

- Empezábamos 2020 con la confirmación por parte de **Microsoft** de un incidente que puso al descubierto casi **250 millones de registros**, que contenían conversaciones entre el equipo de soporte técnico de Microsoft y clientes. Parece ser que una mala configuración de un servidor permitió la exposición de los datos.

- Posteriormente conocimos la noticia de que **20 de millones de registros con datos personales y contraseñas de usuarios de Aptoide**, una alternativa a Google Play, fueron publicados en un conocido foro. Según el atacante, lo publicado era solo una parte de la información que había obtenido.

- En febrero de 2020, una empresa de ciberseguridad notificó a **Decathlon** la localización de un servidor perteneciente a Decathlon España en el que quedaban expuestos alrededor de **123 millones de registros con datos de tiendas, empleados y usuarios** se encontraban expuestos en servidor propiedad. Entre los datos que se podían obtener se encontraban números de teléfono, fechas de nacimiento, números de la Seguridad Social direcciones, nacionalidades, períodos de contratación etc.

- También **Nintendo** sufría una brecha de seguridad de **comprometía las cuentas de cerca de 160.000 usuarios**. Los atacantes consiguieron suplantar el inicio de sesión de Nintendo Network ID, consiguiendo así información personal de los usuarios.

En 2020 se han producido casi a diario brechas de seguridad que han comprometido datos personales

- En verano de 2020 tuvimos conocimiento de un grave fallo de seguridad en **Twitter** que permitió el acceso a numerosas **cuentas de famosos, políticos y otras personas influyentes**. Se publicaron *tweets* en nombre de estas personalidades a fin de estafar a sus seguidores. Por suerte, meses más tarde se consiguió detener al culpable del ataque.

- Otro de los grandes problemas que pueden derivar en una filtración de datos es la **falta de estrictas medidas de seguridad de los servidores y bases de datos** que almacenan dicha información. Eso es lo que ocurrió, también durante el verano de 2020, cuando se filtró una **base de datos con cerca de 115.000 registros de habitantes argentinos con datos relacionados con el COVID-19**. En este caso, la base datos no tenía contraseña ni ninguna otra medida de seguridad.

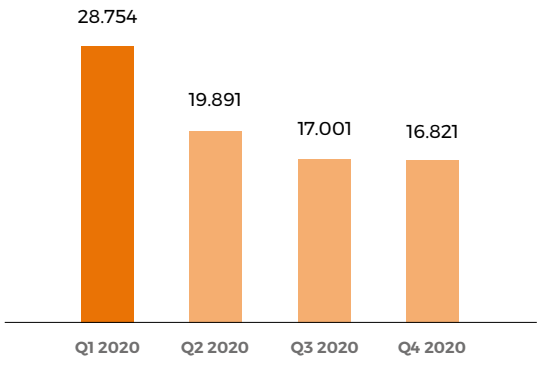
- En un entorno más cercano, y centrándonos en las resoluciones de la AEPD, durante el mes de septiembre de 2020 se notificó a esta entidad una brecha de seguridad que contenía información sensible relativa a **presupuestos, información personal e información privada del Real Madrid Club de Fútbol**.[77]

77. Véase https://www.aepd.es/es/documento/e-07796-2020.pdf

5.6 Vigilancia CCN-CERT

Dentro de los servicios del Sistema de Alerta Temprana (SAT), en 2020 destaca el incremento global del número de incidentes notificados con respecto a 2019. No obstante, a pesar de este aumento en el número de notificaciones con respecto al año anterior, en 2020 se pudo observar un descenso paulatino del número de incidentes notificados de forma trimestral, tal y como se muestra en la siguiente gráfica. Esta tendencia a la baja en 2020 se debe al intenso trabajo de depuración y mejora de las capacidades de detección que se llevaron a cabo a lo largo del año en el SAT, que permitió que la notificación de incidentes a lo largo de 2020 fuera reduciendo en número y mejorando en capacidades de identificación de amenazas de mayor impacto.

En la siguiente tabla presentamos las **campañas destacadas** de 2020:



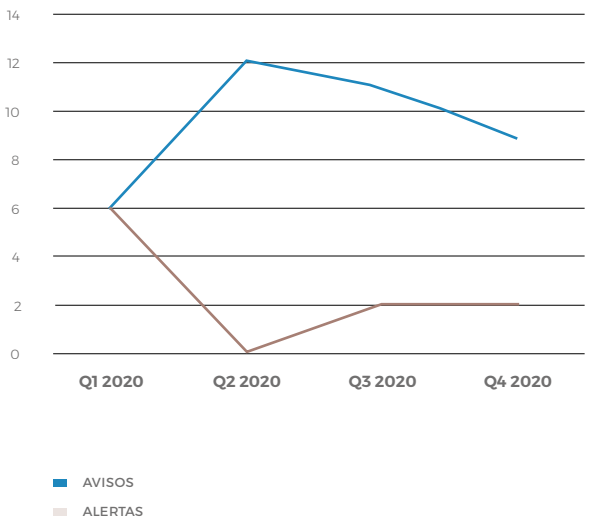
TRIMESTRE	CAMPAÑA
Q1 2020	Repunte de campaña Emotet
	Campañas de phishing
	Campaña de smishing suplantando al SEPE, con el gancho de los ERTE
Q2 2020	Phishing de suplantación del Ministerio de Trabajo
	Campaña de malware mediante correos maliciosos con información de falsos pedidos
	Phishing de suplantación de la Agencia Tributaria
	Campaña de malware suplantando a la Inspección de Trabajo
Q3 2020	Campaña de correos maliciosos suplantando a Correos
	Continúan las campañas de malware a través de correo electrónico suplantando la Agencia Tributaria
Q4 2020	Continúa la campaña de phishing suplantando la Agencia Tributaria
	Campaña de phishing suplantando a la Dirección General de Tráfico
	Campaña de malware de suplantación del Ministerio de Sanidad
	Campañas de malware donde se despliega AgentTesla y Raccoon (malware tipo *stealer* para el robo de información)
	Campañas de ransomware Emotet + Conti ransomware y Emotet + Ryuk ransomware
	Campañas de Phorpiex + Avaddon ransomware

Durante todo 2020 se han producido **campañas de malware** continuamente. En la tabla anterior se destacan las más relevantes. Se puede observar que alguna ha sido especialmente persistente, como los intentos de phishing suplantando a la Agencia Tributaria durante los Q2, Q3 y Q4.

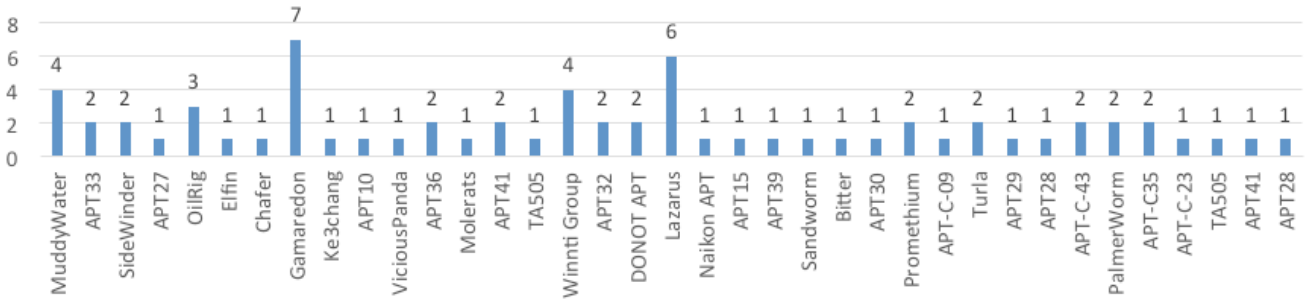
En 2020, el **número de avisos** emitidos por el CCN-CERT osciló entre seis y doce, dependiendo del trimestre. Por otra parte, el **número de alertas** comunicadas empezó en seis, reduciéndose este número a lo largo del año.

En relación con las **actividades de grupos APT a nivel globlal, en 2020** se han identificado los siguientes grupos y operaciones:

COMUNICACIONES CCN-CERT SOBRE VULNERABILIDADES Y CAMPAÑAS



GRUPOS APT ACTIVOS Y NÚMERO DE OCURRENCIAS EN 2020



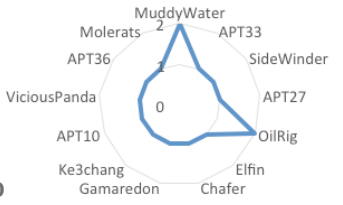
Un total de **27 grupos APT estuvieron activos en 2020**, siendo Gamaredon, Lazarus, MuddyWater y Winnti Group los que perpetraron un mayor número de ocurrencias.

En el primer trimestre de 2020, el mayor número de ataques que se han hecho público de tipo APT fueron perpetrados por los grupos MuddyWater y OilRig. En el segundo trimestre, el grupo más activo fue Gamaredon, con un total de tres. En el tercer trimestre, Lazarus lideró el número de ocurrencias, y en el último trimestre los más destacados fueron MuddyWater, Lazarus, APT-C35 y Gamaredon, en dos ocasiones cada uno.

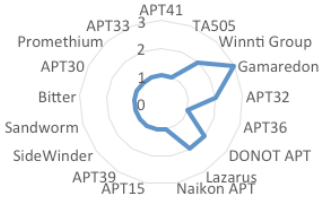
En cualquier caso, dada la sigilosidad con la que habitualmente operan estos grupos los datos reales puede ser muy diferentes.

Respecto a los sectores afectados, **el mayor número de ataques se ha concentrado en el ámbito gubernamental**. Le siguen defensa, energético, entretenimiento digital e industrial, que mostraron el mayor número de ataques.

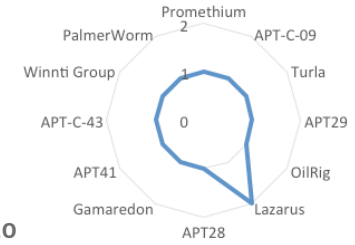
OCURRENCIAS DE GRUPOS APT ACTIVOS



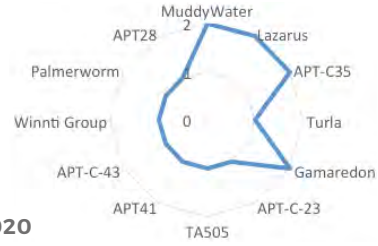
Q1 2020



Q1 2020

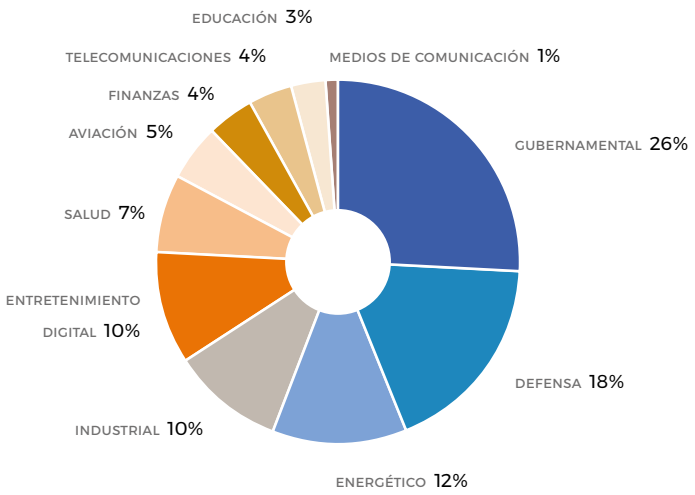


Q1 2020



Q1 2020

SECTORES Y NÚMERO DE OCURRENCIAS AFECTADOS POR APT EN 2020



06 Métodos de ataque

6.1 Ransomware

Como ya se ha comentado a lo largo de este informe, el **ransomware** es uno de los métodos de ataque que sigue consolidándose en el panorama actual No solo adopta su formato más habitual, consistente en el envío de código dañino a un número elevado de potenciales víctimas, sino que cada vez es más frecuente encontrar versiones innovadoras, como los HOR anteriormente referenciados, con objetivos más claros y dirigidos.

A lo cual se añade la técnica de la mencionada doble extorsión (cifrado más sustracción y publicación de datos en la DarkWeb). Lo que ha provocado un **aumento significativo del precio medio que se pide por un rescate**. Además, se observa como grupos de ciberdelincuentes empiezan a establecer su **cartel de operaciones de ransomware independiente**, esto es, la unión de distintos grupos de actores de ransomware específicos que deciden compartir sus plataformas de ***dataleaks*** utilizadas para la extorsión. Este sistema otorga más credibilidad, sofisticación y beneficios al compartir tácticas, conocimientos y plataformas de ***dataleaks***. Un ejemplo de cartel es la fusión producida entre los grupos detrás de la amenaza *Maze* junto con *LockBit* y *RagnarLocker*[78]. Además, existe una rivalidad entre diferentes uniones de grupos de ransomware, en la que se compite por ver quién genera más beneficios y tiene más éxito en sus ataques.

78. Véase https://www.bleepingcomputer.com/news/security/maze-ransomware-adds-ragnar-locker-to-its-extortion-cartel/

HUMAN OPERATED RANSOMWARE (HOR)

Como vector inicial de entrada se siguen empleando **ataques de tipo *spear phishing***, así como la **explotación de servidores RDP expuestos y mal configurados**. Sin embargo**, en muchas ocasiones, el ransomware resulta ser el último estadio** de un proceso de infección **en el que los atacantes llevan días dentro de la red a través de otras amenazas previas**. En este tipo de casos, el ransomware es el último artefacto desplegado por los actores, y suele verse en los activos que puedan ser más críticos para la organización comprometida (controladores de dominio, servidores de copias de seguridad, etc.), buscando ocasionar el máximo impacto. Este modo de actuación es el conocido como **Human Operated Ransomware**, un modelo de actuación en el que los actores consiguen penetrar la red manejando código dañino junto con herramientas ofensivas con la finalidad de establecer persistencia, realizar movimiento lateral, exfiltrar información y finalmente cifrar la información, como se ha indicado.

Surge una nueva generación de ransomware más dirigido y sofisticado, buscando más beneficios: es el Human Operated Ransomware (HOR)

Entre los ransomware más activos en 2020, además de los mencionados *Maze*, *LockBit* y *RagnarLocker*, cabe citar a *Ragnarok*, *NetWalker*, *Nemty*, *Tycoon*, *SNAKE*, *Avaddon*, *Thanos*, *Phobos*, *BlackKingdom*, DoppelPaymer, *REvil*, *TinyCryptor*, *Ryuk*, *RansomExx*, *Conti*, *Egregor*, *Pay2Key* o *Zeppelin*, entre otros[79]. Estas amenazas, en su mayoría, cuentan con capacidad de decisión de cifrado en función del idioma que disponga el equipo del usuario infectado, excluyéndose el cifrado en equipos de usuarios ubicados en Rusia u otros países que formen parte de la Comunidad de Estados Independientes o CEI (Bielorrusia, Ucrania, Armenia, Azerbaiyán, Kazajistán, Kirguistán, Moldavia, Tayikistán, Turkmenistán o Uzbekistán). Hay una alta probabilidad de que esto se deba a que estas amenazas son creadas por desarrolladores que pertenecen a alguno de los países de la CEI. En el caso del ransomware *Ragnarok*, se excluye el cifrado en equipos de usuarios que utilicen como idioma el chino además del ruso, aunque se desconoce si el ransomware opera desde ambos países[80]. En cualquier caso, CCN-CERT quiere hacer hincapié en que **la configuración de estos idiomas no representa una protección contra la amenaza, especialmente si se configuran como secundarios** en el equipo.

Entre los ámbitos más afectados por amenazas de tipo ransomware en 2020 se encuentra principalmente el sector sanitario, aunque también se han visto afectados sectores como logística, educación, pymes, industria automovilista, energético, administración pública, telecomunicaciones o ferroviario, entre otros[81].

6.2 Botnets y el IoT

El **Internet de las Cosas** (o IoT, por sus siglas en inglés), está cada vez más presente en nuestro día a día. Con la llegada del 5G se está haciendo un uso cada vez más generalizado de dispositivos interconectados como altavoces, asistentes de voz, enchufes o bombillas. En la actualidad se estima que **en torno al 33% de los dispositivos englobados en esta categoría ya han sufrido algún tipo de incidente de seguridad**, frente al 19% del año anterior[82]. Este crecimiento sin precedentes se debe principalmente a estos factores:

- Crecimiento exponencial de dispositivos IoT.
- Implementación insegura de dispositivos IoT a los que es fácil acceder directamente desde Internet.
- Falta de actualizaciones de seguridad para estos dispositivos, lo cual los deja expuestos a *exploits* comunes de muchos actores de amenazas.
- Falta de un enfoque de seguridad de dispositivos IoT por parte de los propietarios de dichos activos.
- Dispositivos con contraseñas predeterminadas, conocidas públicamente, que en la mayoría de los casos no se reemplazan.

79. Véase https://resources.infosecinstitute.com/topic/top-6-ransomware-strains-to-watch-out-for-in-2020/
80. Véase https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-targets-citrix-adc-disables-windows-defender/
81. Véase https://www.kaspersky.com/resource-center/threats/top-ransomware-2020
82. Véase https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html

BOTNETS DE IOT NUEVAS Y MODIFICADAS

Ante este crecimiento en el número de dispositivos, las **amenazas de botnet de IoT nuevas y modificadas** son una de las categorías de amenazas que más rápido ha crecido en la primera mitad de 2020. Entre las botnets más destacadas se encuentra *Dark Nexus*, descubierta en abril de 2020. De ella destacan sus elaborados mecanismos para obtener información de los procesos que están corriendo en el activo infectado[83]. Asimismo, otras botnets como *Mukashi*, *LeetHozer*, *Hoaxcalls* y *Mozi.m* han seguido siendo un problema a lo largo de 2020.

Un pequeño avance importante en esta materia tuvo lugar en 2020, con la **aprobación de la *"Ley de mejora de la seguridad cibernética de Internet de las cosas (IoT)"*** en Estados Unidos, por la que el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) desarrollará estándares de seguridad para el uso y administración de dispositivos IoT federales[84]. Aunque por el momento esta normativa esté orientada a un grupo reducido, este tipo de acciones pone de manifiesto una nueva estrategia que deberá ser tenida muy en cuenta en los próximos años, pues **se estima que para 2025 se superen los 30.000 millones de conexiones IoT, con un promedio de cuatro dispositivos de esta categoría por persona**. Esto supone una superficie de ataque enorme; protegerla con tantos estándares diferentes como existen actualmente no es tarea sencilla, además de ser todo un filón para muchos ciber-delincuentes[85].

BOTNETS CON MALWARE

Otro tipo de botnets con un impacto más que relevante son aquellas cuyo objetivo son las **campañas de infección con diferentes tipos de malware, generalmente de tipo troyano y *stealer***. Durante el primer trimestre de 2020, desde Spamhaus Malware Labs se identificaron un total de 2.738 nuevos servidores de mando y control (C&C) de botnets. De ellos, 2.014 (una media de 671 al mes) estaban bajo el control directo de ciberdelincuentes. Esto supone un descenso del 57% en comparación con el cuarto trimestre de 2019[86].

A pesar de este descenso durante el primer trimestre, esta cantidad de nuevos servidores ha ido fluctuando durante todo 2020, volviendo a situarse en cifras muy parecidas a las de 2019. Donde sí hay una diferencia importante es en las amenazas que hay detrás de las campañas de estas botnets, principalmente debido al **notable impacto de Emotet**. Esta amenaza, tras una elevada actividad en 2019, prácticamente desapareció en febrero de 2020. Sin embargo, tras unos meses de descanso, Emotet regresó para realizar una importante campaña de infección cinco meses después, en julio. Durante esos meses, aunque tuvo mucho impacto a nivel global, destacó especialmente en su campaña de *malspam* en inglés enviada al Reino Unido y a los Estados Unidos. Durante dicha actividad llegó a enviar más de 250.000 mensajes de phishing. Tras un prolífico verano, Emotet se tomó otro breve descanso, para volver el 14 de octubre y empezar a causar estragos de

83. Véase https://www.bitdefender.com/box/blog/iot-news/iot-botnet-attacks-rise-2020/
84. Véase https://www.ssa.gov/legislation/legis_bulletin_092220.html
85. Véase https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/?sh=8b9ac135d500
86. Véase https://www.spamhaus.org/news/article/800/spamhaus-botnet-threat-update-q1-2020

nuevo, usando temática del coronavirus en sus campañas de *malspam*, aprovechando noticias relevantes sobre la salud de Donald Trump o las ya comunes facturas falsas y notificaciones de envío de paquetes (**https://heimdalsecurity.com/blog/emotet- malware-history/**).

Junto con Emotet, se han seguido identificando campañas de otras amenazas como AZORult, Lokibot, Racoon y especialmente el Stealer AgentTesla, malware desarrollado en .Net Framework y muy enfocado en el robo de credenciales de todo tipo. En este ámbito, ha entrado en escena una **nueva familia de malware: QNodeService**. Apareció por primera vez en marzo de 2020, y se instala en los equipos víctima a través de script malicioso desarrollado en JavaScript Node.js. El uso de Java + JavaScript tiene algunas ventajas desde el punto de vista del actor de la amenaza, como los bajos índices de detección de antivirus y la compatibilidad con múltiples sistemas operativos.[87]

BOTNETS PARA ANDROID

Por último, **otro objetivo de botnets cada vez más codiciado es el sistema operativo Android**, que es muy similar en la tipología de ataques y malware objetivo a las botnets de IoT. Durante este último año las amenazas IPStorm primero[88] y Matryosh posteriormente[89] han sido las que más han intentado infectar este tipo de dispositivos. La vía de infección de este tipo de amenazas suele ser la interfaz de depuración que en ocasiones se encuentra expuesta en dispositivos con Android, como Smart TV, en el puerto 5555. Generalmente se utilizan con los mismos fines que las botnets de IoT, ya sea ataques DDoS o campañas de envío masivo de correos maliciosos.

Se estima que en 2025 habrá más de 30.000 millones de conexiones IoT y una media de cuatro dispositivos por persona. Protegerlos es urgente.

87. Véase https://www.spamhaus.org/news/article/800/spamhaus-botnet-threat-update-q2-2020).
88. Véase https://blog.barracuda.com/2020/10/01/threat-spotlight-new-interplanetary-storm-variant-iot/
89. Véase https://blog.netlab.360.com/matryosh-botnet-is-spreading-en/

6.3 Código dañino avanzado

En el caso del código dañino avanzado, la sofisticación y elaboración de nuevas técnicas y amenazas mantiene la tendencia de los últimos años, en lo que podría considerarse casi como un proceso de I+D+i por parte de los atacantes. Los grupos más avanzados aprovechan cualquier acontecimiento que sucede en un país, región, continente, etc. para llevar a cabo campañas dirigidas. Este año, como no podía ser de otra manera, la **pandemia de coronavirus** y el **desarrollo de las vacunas** han sido algunos de los pretextos más utilizados por todos los ciberdelincuentes, entre ellos los actores más avanzados.

Estas son las tendencias en técnicas de código dañino observadas en 2020:

- Cabe destacar el uso, por parte de actores avanzados, de **vulnerabilidades críticas en dispositivos expuestos** por parte de las organizaciones, como Citrix NetScaler and Gateway (CVE-2019-19781), Microsoft SharePoint (CVE-2020-0931) o Microsoft Exchange (CVE-2020-16875), etc. Estas vulnerabilidades están sirviendo como punto de entrada a la organización de **diferentes grupos con motivaciones diferentes**. Se ha observado que estos actores están especialmente atentos a este tipo de vulnerabilidades, dado que intentan aprovecharlas horas después de que se publique un *exploit* o de que exista suficiente conocimiento sobre la vulnerabilidad, para crear dicho *exploit* ellos mismos. Con este modus operandi, **cualquier retraso en aplicar el parche es aprovechado por los atacantes**, desplegando (si el sistema vulnerable lo permite) *webshells* para interactuar con el propio equipo y con parte de la organización.

- Otra de las técnicas destacadas de código dañino avanzado es **DLL side-loading,** que permite a un atacante ejecutar su código a través de la carga de un fichero de tipo DLL en un ejecutable firmado y legítimo. Un ejemplo es el uso realizado por el grupo **Mustang Panda** en diferentes **campañas** llevadas a cabo en el año 2020.

- El uso de frameworks de post-explotación como **CobaltStrike, Powershell Empire, Covenant** y **Mythic** está siendo otra de las tendencias observadas. Estos frameworks ofrecen una gran versatilidad, eficiencia y ahorro de costes para los ciberdelincuentes.

- Por otra parte, se sigue viendo el **giro hacia el desarrollo de malware en .NET.** Algunos factores que lo propician son la velocidad de desarrollo, el menor conocimiento por parte de las soluciones de seguridad para detectar código malicioso desarrollado en este lenguaje, la posibilidad de cargar, de un modo sencillo, código en memoria dinámicamente (assemblies) o el poder aprovechar código con técnicas novedosas de frameworks como Covenant.

- En 2020 también se han observado implantes utilizando **DNS over HTTPS (DoH)**, por ejemplo **PowerPepper,** utilizado por el grupo DeathStalker. Esta tecnología está diseñada para proteger la navegación del usuario y que no se sepa qué dominios está visitando, encapsulando el tráfico DNS en peticiones HTTPS.

- En relación con las **amenazas persistentes avanzadas (APT)**, algunas de las muestras de malware de especial interés analizadas durante 2020 corresponden a grupos como Turla o APT27. En mayo de 2020 se hizo pública[90] una muestra del **malware Penquin del grupo Turla** en su versión de 64 bits. Este malware, desarrollado para sistemas GNU/Linux, permite a los atacantes controlar servidores Linux donde se haya desplegado la muestra. Pese a que este malware se descubrió en el año 2014, lo que muestra este hallazgo de 2020 es la versión de 64 bits y, por tanto, que el grupo detrás de su desarrollo continúa avanzando. Además, este informe abre la puerta a realizar escaneos para detectar posibles víctimas de este malware. Kaspersky indica en su **informe de tendencias Q2 del año 2020** que existen gran variedad de sitios en Internet comprometidos por Penquin en su versión x64.

- Grupos como **APT27** continúan desarrollando y cambiando sus capacidades. Entre ellas destacan los avances en el **ZxShell RootKit**, donde los atacantes han introducido un mínimo de ofuscación y han modificado la firma de su driver para trabajar a nivel de kernel.

- En enero de 2020 se **destapó** una campaña en la que se estaba utilizando el **malware LightSpy**, utilizando *exploits* para el sistema operativo iOS. Esta campaña contra usuarios de Hong Kong muestra el nivel de sofisticación de algunos actores, ya que disponer de un *exploit* de ejecución remota para iOS es complicado y costoso. Asimismo, a principios de 2020 el grupo **Sofacy** desplegó su variante .NET del malware **XTUNNEL** y diferentes *loaders* en este lenguaje, hecho que muestra la tendencia y evolución hacia .NET.

Grupos como APT27 continúan desarrollando y cambiando sus capacidades

90. Véase https://www.leonardocompany.com/en/news-and-stories-detail/-/detail/knowledge-the-basis-of-protection

- En diciembre de 2020 se hizo público el descubrimiento del **malware SunBurst**, que fue introducido mediante un **ataque contra la cadena de suministro** en software desarrollado por la compañía **SolarWinds**, software utilizado por empresas como FireEye, Cisco, etc.

- Otra de las amenazas de código dañino utilizada por actores avanzados es **PlugX**, que pese a estar presente desde hace muchos años, sigue siendo una de las amenazas más utilizadas por diferentes actores. Lo que los **actores varían es el modo de despliegue de PlugX** para evitar la detección del software de seguridad. Mustang Panda es uno de los actores más activos desplegando PlugX y Cobalt Strike mediante la técnica DLL sideloading.

- Finalmente, en la parte más baja del sistema, **MosaicRegressor** es uno de los *frameworks* descubiertos que tenía como objetivo la Interfaz de Firmware Extensible Unificada o UEFI (Unified Extensible Firmware Interface). Los ataques identificados con este código se dirigieron a diplomáticos y miembros de oenegés de África, Asia y Europa.

6.4 Ataques a sistemas de acceso remoto

Tal como venimos indicando en apartados anteriores, la pandemia ha contribuido a la **proliferación del uso de diferentes servicios de conectividad remota**. Un número considerable de organizaciones se han visto obligadas, en un corto periodo de tiempo, a migrar de manera masiva hacia entornos más descentralizados, habilitando infraestructuras de acceso remoto no auditadas ni bastionadas correctamente. Este factor, junto al **importante número de CVE publicados en 2020** relacionados con vulnerabilidades en este tipo de entornos, se ha traducido en un aumento significativo de la superficie de ataque expuesta a Internet y, en consecuencia, a distintos actores maliciosos.

Una simple búsqueda en portales como Shodan o ZoomEye arroja datos muy interesantes en este aspecto. Si se compara el número de dispositivos asociados al trabajo remoto expuestos a finales de 2020 con la exposición previa a la declaración de la pandemia, se puede observar como el número se ha multiplicado de manera muy significativa, llegando a superar el 100% para algunos productos y fabricantes concretos.

El escaneo y la explotación de este tipo de vulnerabilidades se ha convertido, según IBM X-Force[91], en el **método más común y exitoso para obtener acceso inicial a una red**. De hecho, este método de infección **ha superado incluso a los correos electrónicos de phishing**, y parece haber desplazado en gran medida al **robo de credenciales** como método más fiable con el que los atacantes se infiltran en las redes privadas corporativas.

Destacan principalmente **tres grupos de vulnerabilidades** que muestran el creciente interés de los grupos APT por investigar y explotar aquellos sistemas expuestos que sirvan de pivote hacia las redes internas de las organizaciones: **VPNs**, **firewalls** y **entornos de trabajo remotos**[92].

Por último, también se ha observado el uso intensivo de diferentes *exploits* sobre servicios más concretos, como pueden ser Telerik UI (CVE-2019-18935), o diversos servidores web como Oracle (CVE-2020-14882) y Apache (CVE-2020-1938), permitiendo la ejecución remota de código en servicios comúnmente expuestos a Internet.

VPNS	Un ejemplo son las diversas vulnerabilidades críticas relacionadas con productos de Citrix (CVE-2019-19781, CVE-2020-8193, CVE-2020-8209), Pulse Secure (CVE-2019-11510) y Draytek (CVE-2020-8515), entre otros[93]. Dada la idiosincrasia de este tipo de soluciones, una ejecución remota de código como la que permitían la mayoría de las vulnerabilidades mencionadas supone una vía de acceso directa a la red interna de la organización objetivo.
FIREWALLS	En cuanto a los cortafuegos, se ha observado el uso de *exploits* contra vulnerabilidades descubiertas en productos de Palo Alto Networks (CVE-2020-2021), F5 Big-IP (CVE-2020-5902), Cisco (CVE-2020-3452, CVE-2020-3187) o SonicWall (CVE-2020-5135), entre otros[94]. En este sentido, cabe destacar el volumen de ataques tratando de utilizar la vulnerabilidad en Big-IP, CVE-2020-5902, que como se ha comentado anteriormente permite la ejecución remota de código, otorgando a un atacante control total sobre el sistema vulnerable. Esta vulnerabilidad ha sido utilizada principalmente para la instalación de malware IoT y criptominería, y ha sido incluida en la lista de las más explotadas por actores patrocinados por el Estado chino, según la Agencia de Seguridad Nacional (NSA) de los Estados Unidos.
TRABAJO REMOTO	Se han producido ataques contra la infraestructura tradicional de trabajo remoto desarrollada por Microsoft, que comprende, entre otros, el uso de servidores de correo Exchange (CVE-2020-0688, CVE-2020-17132) y SharePoint (CVE-2020-16952). Concretamente, los servidores Exchange se han visto en riesgo por la publicación de diversas vulnerabilidades críticas, número que no ha hecho más que aumentar en 2021.

91. Véase https://securityintelligence.com/posts/top-10-cybersecurity-vulnerabilities-2020/
92. Véase https://www.rapid7.com/research/report/vulnerability-intelligence-report/
93. Véase https://www.techrepublic.com/article/top-5-remote-access-threats/
94. Véase https://us-cert.cisa.gov/ncas/alerts/aa20-133a

Todo ello, sumado a la publicación de *exploits* críticos como Zerologon y SMBGhost, ha supuesto un verdadero reto para los equipos de seguridad de muchas organizaciones. Los CVE que figuran en este apartado son de 2020, con dos excepciones: Telerik UI CVE-2019-18935 y Citrix NetScaler ADC / Gateway CVE-2019-19781, que se publicaron a finales de 2019 y han experimentado una explotación de manera recurrente a lo largo de 2020.

También se ha seguido observando el uso de técnicas cuyo objetivo es la **obtención de credenciales legítimas de acceso remoto a distintos sistemas como VPN, repositorios de información, escritorios remotos o correos electrónicos**[95]. Este tipo de ataques no solo se basan en las ya tradicionales campañas de ingeniería social, en masa o dirigidas, sino también en la compraventa de credenciales en mercados a los que se puede acceder principalmente desde la Dark Web. Si bien la implementación de un **segundo factor de autenticación (2FA)** contribuye a limitar este tipo de ataques, los actores maliciosos han identificado diversas técnicas[96] (8) que permiten evadir dicho mecanismo de autenticación, demostrando una vez más que en seguridad nada es 100% seguro

VIDEOCONFERENCIAS EN EL PUNTO DE MIRA

En otro orden de cosas, ciertas aplicaciones cuyo uso se ha extendido de manera exponencial durante la pandemia, como es el caso de Zoom, han venido a demostrar que los actores maliciosos se focalizan en la **investigación de debilidades en productos cuyo uso se ha extendido de manera vertiginosa en un corto periodo de tiempo**. Así pues, se han publicado varias vulnerabilidades (CVE-2020-6109, CVE-2020-6110 entre otras)[97] que permitían, por ejemplo, comprometer la seguridad de la aplicación enviando un mensaje especialmente diseñado, que se aprovecha de una anomalía en la gestión de las rutas de los archivos que utilizaba Zoom. Cabe destacar que **la gran mayoría de estas vulnerabilidades se subsanan mediante la aplicación de una actualización publicada por el fabricante.** Esto demuestra que el ciclo de actualizaciones y parcheos se sucede a una velocidad considerablemente inferior a la que los actores maliciosos desarrollan *exploits* funcionales y se aprovechan de estas debilidades.

La explotación de vulnerabilidades en servicios de conectividad remota se ha convertido en el método más exitoso de acceso inicial a una red

95. Véase https://www.incibe.es/protege-tu-empresa/avisos-seguridad/detectada-campana-correos-fraudulentos-difunden-malware
96. Véase https://www.forbes.com/sites/forbestechcouncil/2020/08/21/how-threat-actors-are-bypassing-two-factor-authentication-for-privileged-access/
97. Véase https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=zoom

6.5 Ataques web

Las **aplicaciones y tecnologías web** se han convertido en una parte fundamental de Internet, adoptando diferentes usos y funcionalidades. La situación atípica provocada por la pandemia en todos los sectores y actividades ha provocado una mayor exposición de activos a Internet, en algunos casos de forma precipitada y sin los controles de seguridad oportunos.

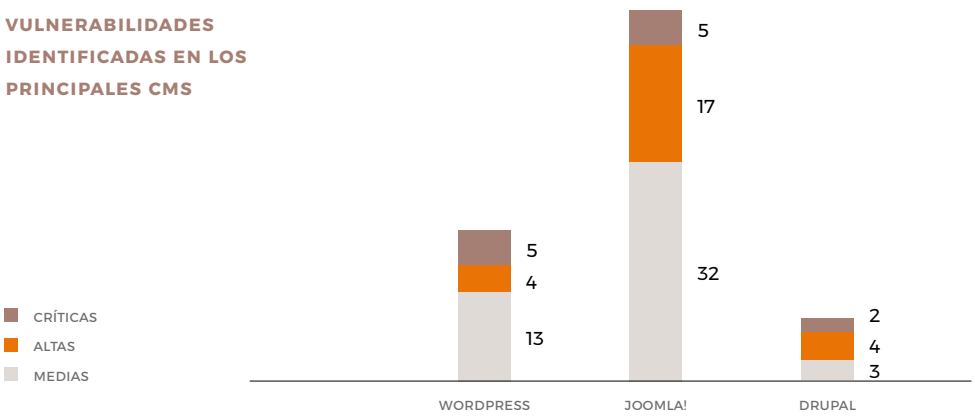
El aumento en la complejidad de las aplicaciones web y sus servicios crea desafíos para protegerlos contra amenazas de diversa motivación, desde daños económicos o de reputación hasta el robo de material crítico o información personal.

Los servicios y aplicaciones web dependen principalmente de **bases de datos** para almacenar o servir la información requerida. Los **ataques del tipo inyección SQL (SQLi)** son un ejemplo bien conocido e incluido por OWASP en su top 10. Otro ejemplo son los **ataques de *Cross-Site scripting* (XSS)**, en los que un actor hostil hace un mal uso de las debilidades en formularios u otras funcionalidades de entrada de las aplicaciones web, que derivan en acciones maliciosas como ser redirigido a un sitio web malicioso o un robo de sesión.

Con la finalidad de aumentar la funcionalidad y la productividad, el desarrollo y uso de API está más extendido que nunca. La introducción de estos entornos complejos impulsa la adopción de nuevos servicios de seguridad y auditoría para las aplicaciones web. Se estima que aproximadamente **el 80% de las organizaciones que adoptan API han desplegado controles de seguridad en su tráfico de entrada**.

Durante el año 2020 y comienzos de 2021 se han notificado vulnerabilidades críticas en los principales gestores de contenido (CMS) utilizados en España, como muestran los siguientes gráficos.

Para poner estos datos en contexto, sirva indicar que WordPress está presente en el 38% de los sitios web del índice Quantcast Top 10k. La compañía especializada en proteger esta plataforma, Wordfence, ha informado de un aumento de ata-



ques exponencial en los últimos años. Destaca la acción del 3 de mayo de 2020, cuando se realizaron de forma automatizada 20 millones de ataques sobre medio millón de sitios web diferentes.

Los **ataques distribuidos de denegación de servicio DDoS** son un vector de ataque común y en alza. El año 2020 nos ha dejado dos récords de este tipo de acciones: uno en febrero, reportado por Amazon, que ascendió a 2,3 terabits por segundo, y otro en julio, cuando se identificó un ataque en la capa 7 que generó 689.000 solicitudes por segundo, duplicando los registros de 2019.

El sector bancario se encuentra en el punto de mira de esta amenaza: en 2020 se ha identificado el incremento de ataques tipo **RDDoS** (Ransom Distributed Denial-Of-Service Attacks) ligados a actores como Fancy Bear y Lazarus Group, en los que se extorsiona a grandes corporaciones para que paguen un rescate, con la amenaza de un ataque distribuido de denegación de servicio dirigido.

A principios de 2021 se pone de manifiesto la vulnerabilidad que suponen las **técnicas de *scraping* automatizadas a gran escala en las redes sociales**, con la filtración masiva de datos personales de plataformas como TikTok, YouTube, Facebook, Clubhouse y LinkedIn. Se trata de la mayor colección de información privada conocida hasta la fecha extraída mediante el abuso de funcionalidades y favorecida por la laxa configuración de privacidad por defecto de los perfiles de usuarios. Esta información será sin duda utilizada en futuras campañas de phishing y smishing.

98. Véase https://www.welivesecurity.com/la-es/2021/01/07/2020-duplico-detecciones-ataques-ingenieria-social/

6.6 Ingeniería social

La situación excepcional de 2020 no solo no ha pasado desapercibida, sino que ha supuesto un gran filón para las campañas de ingeniería social, que ya en 2019 fueron uno de los principales vectores de ataque. El objetivo es engañar a la víctima para que, sin ser consciente de ello, realice alguna acción dañina en beneficio del atacante: la descarga de *malware* en su dispositivo, el robo de sus credenciales o la revelación de información personal serían algunas de esas acciones.

En 2020, esta tendencia se ha materializado en la detección de un **200% más de este tipo de amenazas que en el año anterior**. No solo llaman la atención las cifras, también queda constancia de la utilización de **temáticas relacionadas con la pandemia**, y del poder que otorgan los usuarios a aquellos delincuentes que se aprovechan del temor al virus para obtener beneficio[98].

EL AÑO DE LOS BULOS

Por otro lado, las técnicas de ingeniería social adquieren también una especial relevancia en las **campañas de noticias falsas** a nivel global vinculadas a la excepcionalidad de 2020. En un momento de alarma, novedad e incertidumbre, las informaciones de falsas curas, remedios urgentes y teorías de la conspiración han campado a sus anchas. Estas informaciones y teorías no contrastadas han generado en muchos casos el caos entre la población, y esto es de nuevo un **problema de seguridad**, dado que ese clima de confusión

puede llegar a promover **descargas de malware, reenvío de enlaces maliciosos**... y de nuevo facilitar los ciberataques[99].

Otros ejemplo relacionado son las **estafas** que, aprovechando la situación de necesidad de muchos usuarios, a causa de la crisis económica derivada de la crisis sanitaria, enviaban mensajes de texto con falsas ofertas relacionadas con descuentos, ventajas en supermercados, alimentación y otros bienes. Por otro lado, la necesidad de muchos negocios, entre ellos pymes, de estar en Internet, ha hecho que algunas de las marcas cuenten con principiantes en el uso de las tecnologías, algo que también ha sido aprovechado para generar confusión y promover fraudes online.

De cara a los próximos años, queda por ver **qué ocurrirá cuando la excepcional situación sanitaria desaparezca de nuestra realidad**. Un efecto podría ser la disminución sustancial de la parte digital de nuestras vidas, adquiriendo de nuevo hábitos más "físicos" o presenciales que digitales, por contraposición y rechazo a todo lo vivido en 2020. Por el contrario, puede que esta intensificación de nuestra vida digital haya llegado para quedarse, y se mantenga o incluso aumente en nuestro día a día, y por consiguiente sigan avanzando los ataques de ingeniería social y las noticias falsas.

99. Véase https://www.muyseguridad.net/2021/01/02/desinformacion-ciberseguridad/

6.7 Ataques contra la cadena de suministro

La seguridad de la cadena de suministro es uno de esos aspectos de la seguridad de la información que está a nuestro alrededor desde hace varios años. Su importancia está más que reconocida por la industria (y demostrada, muy a nuestro pesar, por incidentes reales con un impacto muy significativo), pero en la práctica no acaba de desarrollarse.

Lo cierto es que hoy en día todavía son pocas las organizaciones que tienen implantado un proceso maduro y eficaz de seguridad de la cadena del suministro. Varios factores explican esta situación: la asimetría entre el cliente y el proveedor en algunos procesos de contratación, la todavía escasa concepción de la seguridad de la información como un proceso transversal de las organizaciones o la complejidad y el volumen de recursos necesarios para asegurar entornos empresariales cada vez más externalizados y distribuidos.

Por si esta falta de desarrollo efectivo no fuese ya un problema lo bastante serio, el crecimiento del **Shadow IT**, de la mano de la abundancia de herramientas Cloud en los últimos años, ha venido a agravar el escenario: ahora **no solo es necesario gestionar la cadena de suministro que conocemos, sino también aquella que queda fuera del radar de los equipos de TI y ciberseguridad**.

Estas fueron las tendencias destacadas de 2020 en este tipo de ataques:

El efecto SolarWinds:

Por desgracia, 2020 ha sido un año especialmente memorable en lo que se refiere a los ataques a la cadena de suministro, donde un acontecimiento destaca particularmente por su importancia: el ataque efectuado contra **SolarWinds**, que ya hemos mencionado en otras secciones de este informe.

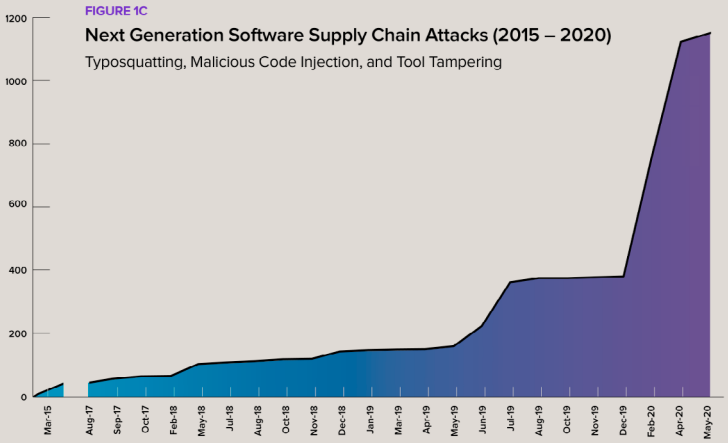
Mediante la **modificación maliciosa de un paquete de actualización de Orion**, una de las herramientas de gestión TI del fabricante, los atacantes obtuvieron acceso potencial a miles de organizaciones, incluyendo agencias del gobierno estadounidense y otros importantes proveedores de tecnología como Cisco, FireEye, Microsoft o Malwarebytes.

Actualmente se desconoce el impacto real del ataque, pero se estima que **podría haber alcanzado a numerosas organizaciones**, con algunas implicaciones relevantes, como el acceso de los atacantes a código fuente de Microsoft. Aunque esto cae en el ámbito de la especulación, no deberíamos descartar que el impacto de un ataque de este calibre se extienda muchos años en el futuro, muchas veces sin el conocimiento de sus víctimas.

Más proactividad:

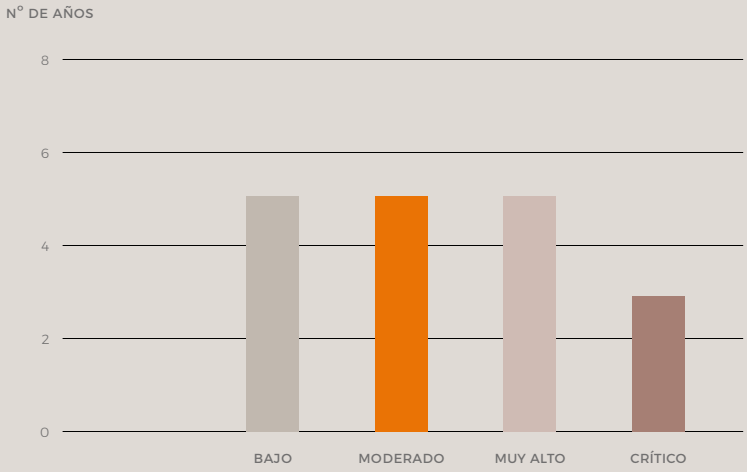
Otro elemento que podemos destacar de 2020 es la tendencia que señala el **6º Informe Global Anual sobre el Desarrollo de Software de Código Abierto**, que muestra cómo los atacantes están asumiendo un **comportamiento más proactivo** e **introduciendo vulnerabilidades en el código fuente en los repositorios de código abierto**, frente a la búsqueda y explotación de vulnerabilidades en productos existentes.

Aunque esta mecánica no es exactamente nueva, como mostró el **ataque a ESLint en 2018**, dicho informe sí refleja un importante crecimiento, de más del 400%, durante 2020 respecto al mismo periodo del año anterior, junto con otros datos preocupantes como el alto volumen de paquetes npm (*node package manager*) con código potencialmente vulnerable, o el retraso que se produce entre que una vulnerabilidad es detectada en un paquete *open source* y el momento en el que los desarrolladores son conscientes de ella.



6TH ANNUAL REPORT ON GLOBAL OPEN SOURCE SOFTWARE DEVELOPMENT, SONARTYPE

A pesar de este incremento, el informe **State of the Octoverse 2020**, publicado por GitHub, la mayor plataforma de código abierto del mundo, muestra que este problema es todavía limitado. Según dicho informe, a partir del análisis de una muestra de 517 avisos, un 17% de ellos estaban relacionados con vulnerabilidades introducidas maliciosamente en los paquetes de software, pero fueron responsables apenas de un 0,2% de las alertas de seguridad. Esto apunta a que, en general y a pesar de esta tendencia, **las vulnerabilidades introducidas por errores de programación (83%) siguen siendo más abundantes** y se encuentran en los paquetes más utilizados.



TIEMPO TRANSCURRIDO (EN AÑOS) ENTRE IDENTIFICAR Y PARCHEAR UNA VULNERABILIDAD DE SOFTWARE OPEN SOURCE. *THE 2020 STATE OF THE OCTOVERSE REPORT*, GITHUB

Código abierto, el desafío a seguir:

Esto no hace necesariamente más peligroso al software de código abierto, sino que pone de manifiesto el **alto volumen de desarrolladores y proyectos de código abierto**, así como la necesidad de estandarizar e incrementar las pruebas de seguridad sobre el código abierto utilizado, especialmente si atendemos a la presencia que tiene en todos los ámbitos de las TI. En este sentido, y como nota positiva (aunque no para las personas implicadas de uno y otro lado), es reseñable mencionar que **a principios de 2021, la Universidad de Minnesota fue bloqueada y apartada del desarrollo del kernel de Linux** al detectar, precisamente, que había tratado de introducir vulnerabilidades y errores en el código, como parte de un proyecto de investigación que analizaba la capacidad de estos equipos para detectar vulnerabilidades.

Dos casos destacan en este ámbito. Por un lado, como ejemplo de esta nueva tendencia, en marzo de 2020 el GitHub's Security Incident Response Team (SIRT) detectó un malware bautizado como **Octopus Scanner**, cuya función era buscar en GitHub proyectos de NetBeans, abrir puertas traseras en ellos, y utilizar el proceso de construcción y sus artefactos resultantes para propagarse. Este malware llegó a afectar a un total de 26 proyectos.

Por otro lado, en julio de 2020 se parcheó una **vulnerabilidad alta (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H) en el paquete de software npm lodash**, que llevaba presente desde la versión 0.1.0, liberada en 2012. Aunque tres meses después, en torno a un 45% de los desarrolladores habían parcheado con la versión no vulnerable, al ser uno de los paquetes más utilizados (con una media de más de 25 millones de descargas semanales en 2020), esto implica un número significativo de instalaciones vulnerables.

A estos incidentes cabe sumar, previsiblemente, otros cuyo origen no se asocia a la cadena de suministro, y de los que evidentemente no hay datos. Tampoco hay que olvidar el problema que supone, desde un punto de vista geopolítico, que ciertos **países fabricantes de hardware o software a gran escala tengan la posibilidad de influir en su desarrollo,** lo que facilitaría potencialmente la utilización de la cadena de suministro como un vector de ataque masivo.

En definitiva, la cadena de suministro es un ámbito al que **urge prestar más atención** de la que se le viene prestando hasta ahora. Es previsible que en los años venideros sigamos viendo cómo se incrementa no solo el número de ataques, ya sea por parte de actores Estado u organizaciones criminales, sino también el alcance e impacto de estos.

Pocas organizaciones tienen implantado un proceso maduro y eficaz de seguridad de la cadena del suministro

6.8 Ataques a sistemas ciberfísicos

En relación con **sistemas ciberfísicos e infraestructuras críticas**, se han confirmado las tendencias observadas en 2019 y principios de 2020 que se recogieron en la edición de 2020 de este informe[100], sobre todo en lo relacionado con tres líneas principales:

- El **abuso de vulnerabilidades asociadas al acceso remoto** a través del perímetro a sistemas de control industrial, en un contexto de pandemia que ha restringido en muchos casos el acceso físico a los sistemas.
- La selección como **objetivo** de **infraestructuras sanitarias y centros de investigación** relacionados con la lucha contra el SARS-COV-2.
- Los **ataques de ransomware contra infraestructuras industriales** con impacto en las operaciones de producción.

100. Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html

ACCESOS REMOTOS A INFRAESTRUCTURAS

En relación con los accesos remotos, el **abuso de vulnerabilidades relacionadas con Pulse Secure, CitrixNetscaler y F5** ha sido especialmente relevante. Por ejemplo, según ha señalado la Agencia de Ciberseguridad e Infraestructura (CISA), se ha identificado su uso por parte de un actor iraní para atacar infraestructuras críticas (II.CC.) estadounidenses.[101]

De hecho, este mismo organismo difundió en septiembre de 2020 una alerta señalando las acciones que debían adoptar los operadores de II.CC. y compañías industriales estadounidenses ante el aumento de exposición de estos sistemas como consecuencia del cambio en su modo de gestión.[102]

Esta exposición y sus potenciales efectos se han puesto de manifiesto a comienzos de 2021 con la publicación del **ataque contra una estación de tratamiento de agua potable en Florida**. El atacante aprovechó un uso deficiente del software de acceso remoto (por ejemplo, TeamViewer o similares, este detalle no ha sido revelado) para modificar la dosificación de reactivos en el agua con que se abastece a la población. La alerta publicada por la CISA muestra el riesgo asociado al uso de Windows 7 una vez finalizado el soporte oficial del fabricante, un factor ya mencionado en la edición de 2020 de este mismo informe.[103]

Estos servicios de gestión remota también se han explotado en una **campaña de phishing dirigida a compañías industriales** que emplea como gancho en correos electrónicos capturas de pantalla de la aplicación DIGSI, del fabricante Siemens y utilizada por compañías eléctricas para hacer configuración de relés en subestaciones. Los archivos adjuntos a los correos electrónicos ejecutaban un malware que instalaba una versión del software TeamViewer modificada por los atacantes para ganar control sobre el sistema infectado.

La gran mayoría de los sistemas atacados son **empresas industriales que operan en los siguientes sectores de la economía**:[104]

- Fabricación
- Petróleo y gas
- Industria del metal
- Ingeniería
- Energía
- Construcción
- Minería
- Logística

RANSOMWARE

En cuanto al impacto del ransomware en organizaciones industriales, es una tendencia que continúa al alza, como ha quedado demostrado a lo largo de este informe.

101. Véase https://us-cert.cisa.gov/ncas/alerts/aa20-259a
102. Véase https://us-cert.cisa.gov/ncas/alerts/aa20-205a
103. Véase https://us-cert.cisa.gov/ncas/alerts/aa21-042a
104. Véase https://ics-cert.kaspersky.com/reports/2020/11/05/attacks-on-industrial-enterprises-using-rms-and-teamviewer-new-data/

Durante 2020, varias empresas multinacionales, entre las que se encuentran algunas pertenecientes al **sector energético**, se han visto afectadas por rastros de actividad maliciosa del ransomware **Netwalker**. Esta variante funciona como un RaaS (*Ransomware as a Service*) de acceso cerrado. .

Ya en los primeros días del año 2021, se ha hecho evidente la aparición de un **nuevo ransomware** conocido como **Babuk Locker**, que ha afectado a una serie de empresas de todo el mundo. Entre las organizaciones víctimas se encuentran compañías del sector industrial, sobre todo empresas manufactureras dedicadas a la fabricación de ascensores y escaleras eléctricas/mecánicas, muebles de oficina, piezas para automóviles, productos para pruebas médicas, aire acondicionado y calefacción, etc.[105]

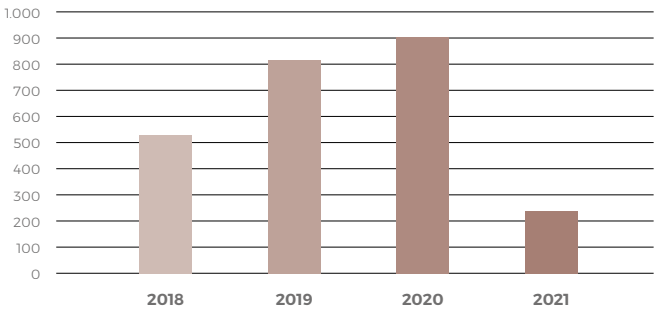
ATAQUES A LA CADENA DE SUMINISTRO

Otros incidentes destacados están asociados a ataques a la cadena de suministro. En septiembre de 2020 se informó sobre la publicación de **6 nuevas vulnerabilidades críticas** en el **producto para la administración de licencias y antipiratería CodeMeter de Wibu-Systems AG**. Se trata de una solución ampliamente utilizada por los principales fabricantes (Rockwell y Siemens) en el ámbito de los Sistemas de Control Industrial (ICS). Estos fallos de seguridad pueden conducir a la ejecución remota de código (RCE) y ataques de denegación de servicio (DoS). Dichas vulnerabilidades pueden ser aprovechadas de forma remota y sin autenticación, y **proporcionan a los atacantes el equivalente al acceso de administrador a sistemas críticos**. El resultado final puede ir desde la parada de dispositivos industriales hasta el despliegue de malware en una fase de explotación. Rockwell Automation y Siemens confirmaron que se ven afectados por estas fallas[106].

VULNERABILIDADES

Respecto a **vulnerabilidades de carácter técnico específico**, se mantiene la tendencia creciente observada en los últimos años. A efectos comparativos, una búsqueda en el catálogo NVD de NIST arroja en 2019 un total de 815 vulnerabilidades relacionadas con sistemas de control industrial (ICS), y **904 en 2020**[107]. Conviene tener en cuenta que este último número variará a lo largo de 2021, cuando se publiquen CVE en estudio notificadas durante 2020 pero no incluidas en la actualidad en el catálogo.

VULNERABILIDADES ASOCIADAS A ICS EN EL CATÁLOGO NVD DE NIST EN LOS AÑOS 2018, 2019, 2020 Y 2021 (HASTA ABRIL)



105. Véase https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/
106. Véase https://www.claroty.com/2020/09/08/blog-research-wibu-codemeter-vulnerabilities/
107. Véase https://nvd.nist.gov/vuln/search

6.9 Vigilancia CCN-CERT

Como se puede observar en esta tabla, los métodos de ataque más habituales durante 2020 fueron la **explotación de vulnerabilidades de software, la inyección SQL y el uso de troyanos**. Por el contrario, los tipos de incidentes menos habituales fueron los de gusano, fraude y *rootkit*.

TIPOLOGÍA DE INCIDENTES DETECTADOS POR CCN-CERT	Q1 2020	Q2 2020	Q3 2020	Q4 2020
Explotación de vulnerabilidad SW	8100	7619	7780	7544
Inyección SQL	3101	2964	2649	2448
Troyano	2756	2434	1298	1561
Otros	1673	1581	1085	938
Intrusiones	1449	901	862	922
Malware	1392	1799	1294	1122
RFI	749	672	525	556
Identificación de vulnerabilidades	82	71	117	322
Acceso no autorizado a red	121	238	265	290
Spyware	933	630	493	373
DoS/DDoS	1656	234	126	160
Ataque de fuerza bruta	383	278	202	150
RAT	5645	391	147	137
Recopilación de información	1	0	70	125
Acceso a servicios no autorizados	3	14	57	48
Sistema no actualizado	1	0	0	13
Phishing	593	9	8	68
Ransomware	86	46	11	32
Política de seguridad	12	2	3	4
Exfiltración de información	5	7	7	5
Gusano	11	1	2	3
Fraude	1	0	0	0
Rootkit	1	0	0	0

07 Qué esperar en 2021

2020 ha sido un punto de inflexión a nivel global en muchos aspectos. Como muestra este informe, el mundo de la ciberseguridad no ha sido una excepción. El panorama en este ámbito se ha recrudecido, y no cabe duda de que los profesionales del sector tenemos por delante desafíos cada vez más numerosos y complicados.

Dado que la pandemia y sus consecuencias aún seguirán siendo un tema recurrente en el corto y medio plazo, no es aventurado asegurar que el próximo periodo será aprovechado por los ciberdelincuentes para obtener beneficios. Las ciberamenazas a las que tendrán que hacer frente particulares, empresas y organismos públicos seguirán evolucionando a la par que nuestro entorno social y económico.

Sin duda, el año 2021 sigue planteando **amenazas constantes para el sector sanitario** en temas de ciberseguridad. Al cierre de este informe la vacunación progresa a buen ritmo, pero la aparición de nuevas oleadas puede dificultar el trabajo de hospitales y demás organismos del sector de la salud, lo que hará que algunos ciberdelincuentes sigan focalizando muchos de sus ataques contra este sector, debido a la falta de tiempo y recursos que en muchos casos existen para mantener sus sistemas actualizados y debidamente securizados.

Nueva normalidad, nuevos riesgos

Por otro lado, el traslado forzoso de empleados y estudiantes al hogar desde el inicio de la pandemia provocó un aumento cada vez mayor de dispositivos conectados, aplicaciones y servicios web que utilizamos en nuestra vida personal y profesional. Este cambio sigue muy presente en 2021 y supone un **aumento de la superficie de ataque de la casa conectada**. En este entorno, y aprovechando la falta de medidas de seguridad, las políticas de privacidad débiles, las vulnerabilidades y la susceptibilidad del usuario a la ingeniería social, los atacantes dirigirán sus campañas no solo al ámbito doméstico sino al de las empresas[108].

108. Véase https://www.welivesecurity.com/wp-content/uploads/2020/12/Cybersecurity_Trends_2021_ES.pdf

Del mismo modo, la **presencia en la nube de una amplia mayoría de empresas**, especialmente tras este último año, va a suponer que muchas de ellas tengan que ampliar y/o mejorar las medidas adoptadas en materia de seguridad. En muchos casos, **las necesidades de negocio han primado sobre los controles necesarios de seguridad**, y muchas de las amenazas en la nube son las mismas que se encuentran en las redes internas. En 2021 se espera que los ataques a la nube sigan ejecutándose a través del robo de credenciales y de la explotación de vulnerabilidades y malas configuraciones de la nube y sus aplicaciones[109].

Del mismo modo que las personas y las organizaciones involucran a potenciales consumidores en sus plataformas sociales mediante la recopilación de información, el desarrollo de contenido especializado y la realización de interacciones específicas con los clientes, los actores malintencionados pueden usar esas plataformas de manera similar para dirigirse a empleados de alto valor. El **aumento acusado del uso de las redes sociales**, tanto en el ámbito privado como en el profesional, lleva a pensar que éste puede convertirse en un vector de ataque creciente durante este año.

A medida que los usuarios se vuelven cada vez más dependientes de los pagos móviles, los ciberdelincuentes buscarán cada vez más explotar y defraudar a los usuarios con mensajes fraudulentos de phishing o smishing que contengan URL de pago maliciosas. Habrá un **aumento en las vulnerabilidades de pago móviles basadas en la recepción de un correo electrónico de phishing, un mensaje directo o un mensaje smishing** que le indica al usuario que puede recibir un pago, un reembolso de la transacción o un premio en efectivo haciendo clic en una URL engañosa, siendo estafado para que envíe un pago desde su cuenta.

Los **ataques de phishing**, en todas sus formas, ya sean correos electrónicos para toda la empresa, ataques al empleado dirigidos a su correo electrónico corporativo (BEC) o, la más reciente en el mundo de la ingeniería social, el ataque de *vishing* (phishing de voz), seguirán muy presentes en 2021.

109. Véase https://content.fireeye.com/predictions/rpt-security-predictions-2021

También cabe mencionar que la evolución abrumadora de la tecnología está haciendo que los avances en términos de **inteligencia artificial** sean cada vez mayores, y se podría acelerar considerablemente la identificación de nuevas amenazas y sus respuestas para frenar los ataques antes de que puedan propagarse. Sin embargo, estos mismos avances tomados desde la perspectiva contraria pueden hacer que el perfeccionamiento de las técnicas para esquivar los controles biométricos y el uso de estas para cometer fraudes vaya en aumento.

En cuanto al **ransomware**, como se ha visto, seguirá siendo bastante relevante durante 2021, especialmente en sus formas más evolucionadas y avanzadas, teniendo como claros objetivos grandes organizaciones o sectores vulnerables. La facilidad de éxito y la eficacia en la obtención de grandes sumas de dinero hará de este uno de los puntos candentes, evolucionando cada vez más al modelo de ransomware como servicio (RaaS). En este sentido, es destacable que muchas de las familias de ransomware que más impacto han causado apenas tienen un año de vida, lo cual nos lleva a un escenario en constante evolución, en el que se combinará tanto el uso de nuevos malware de manera independiente como en combinación con otros ya conocidos.

El traslado de empleados y estudiantes al hogar comporta un nuevo riesgo: el aumento de la superficie de ataque de la casa conectada

El aumento de la popularidad y el éxito de las técnicas de **doble extorsión** durante 2020, en las que además del secuestro de datos se amenaza con el filtrado de los mismos, lleva a pensar que muchas nuevas variantes se decanten por esta tendencia[110].

Un aspecto positivo es la **desarticulación de la infraestructura de Emotet** a comienzos de año, en un labor coordinada de las autoridades policiales y judiciales de ocho países de Europa y Norteamérica junto a Europol y la Agencia Europea para la Cooperación Judicial Penal. Posteriormente, Europol lanzó una actualización a esta botnet con una DLL que elimina el malware Emotet de los equipos infectados (aunque no los posteriores que este hubiera podido descargar en la víctima).

Con respecto al **ciberespionaje**, los actores patrocinados por Estados seguirán su tendencia habitual de perfeccionamiento de técnicas y adaptación al entorno y objetivos. A esto hay que añadir que sus acciones se producirán en un entorno global mucho más expuesto como se ha comentado, facilitando la labor de los grupos APT más relevantes que aumentarán sus operaciones y las ejecutarán de manera más eficiente.

El ataque a SolarWinds exige máxima atención ante una amenaza de alto impacto: los ataques a la cadena de suministro

110. Véase https://www.welivesecurity.com/la-es/2020/12/04/tendencias-ciberseguridad-2021-que-esperar-proximo-ano/

Los ataques a la **cadena de suministro** o cadena de valor, especialmente tras el incidente de SolarWinds a finales de 2020, representan una amenaza no solo para las grandes empresas sino también para las personas, dado que en los hogares altamente interconectados de hoy en día: cualquier error en las empresas de electrónica de consumo puede provocar que los atacantes usen su acceso a dispositivos inteligentes como televisores, asistentes virtuales y/o teléfonos para sustraer información o actuar como puerta de enlace para atacar empresas mientras los usuarios trabajan de forma remota desde casa[111].

Con toda probabilidad, los actores malintencionados van a seguir explorando nuevas técnicas para comprometer la cadena de valor en 2021.

El aumento exponencial de despliegue de **dispositivos y sistemas IoT** de estos años y los venideros, no hace sino abrir más opciones al atacante, especialmente en entornos donde o por falta de conocimientos o de recursos no se lleve a cabo un mantenimiento y securización adecuados. En este sentido, se hace fundamental que los nuevos diseños tengan en cuenta unos principios mínimos de seguridad, para no tener que aplicar medidas reactivas a posteriori.

En este escenario, se espera que los costes asociados a los incidentes de ciberseguridad se incrementen en torno a un 15% de cara a 2021 y que mantengan la tendencia ascendente, llegando a superar los 8 billones de euros a nivel global en 2025[112].

111. Véase https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report/

112. Véase https://cybersecurityventures.com/cybercrime-will-cost-the-world-16-4-billion-a-day-in-2021/

08 Conclusiones

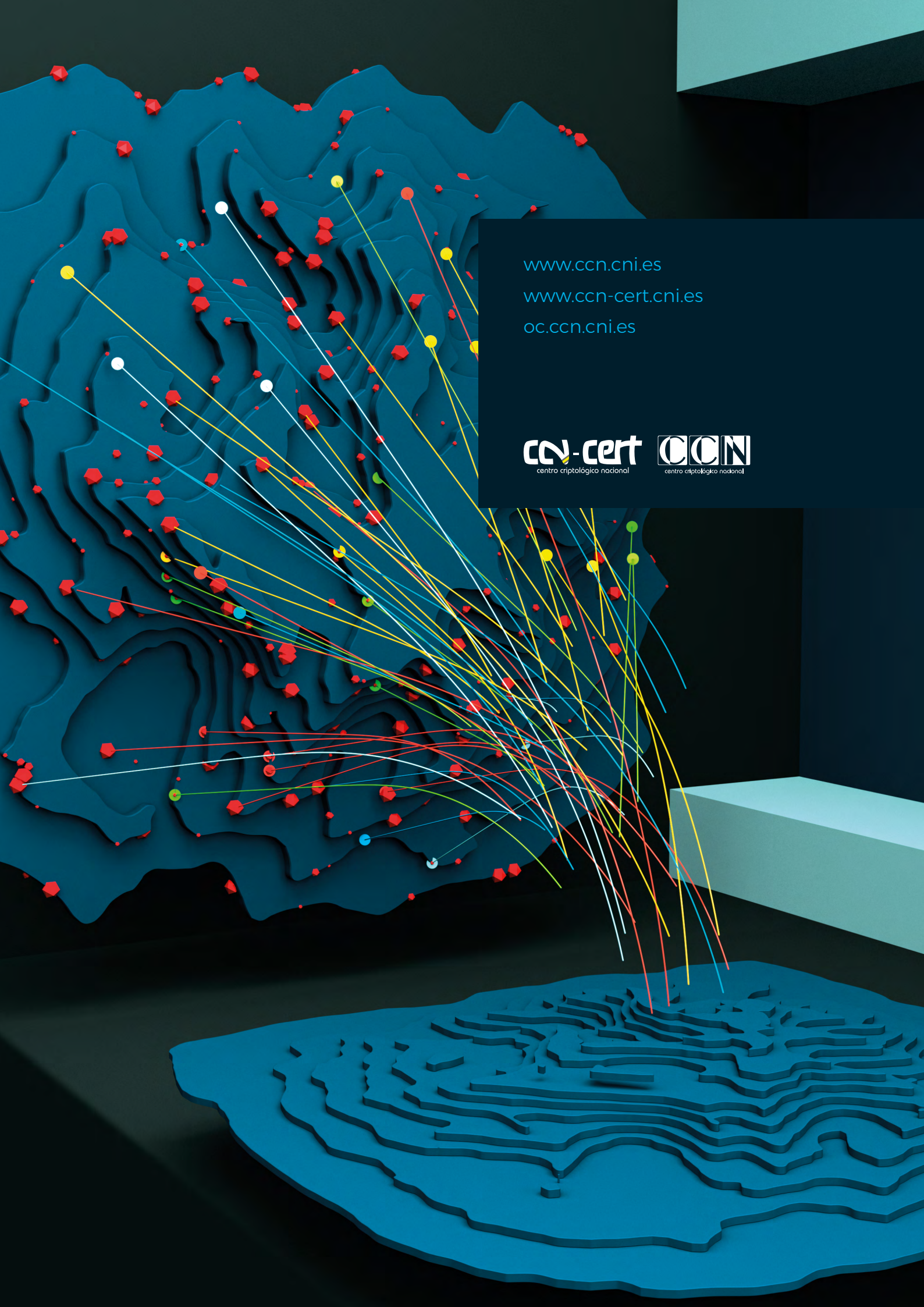
La pandemia ha demostrado, como nunca antes, que la ciberseguridad es un pilar para empresas, instituciones y ciudadanos.

A lo largo de este informe se ha puesto de manifiesto que la ciberseguridad sigue siendo uno de los pilares fundamentales para cualquier empresa, organismo o institución. Es un sector cada vez más en alza, con agentes de amenaza cada vez más preparados, capaces de orquestar ataques de un alto nivel de complejidad y alto impacto, como ha quedado reflejado en todos los incidentes acontecidos durante 2020 a nivel internacional.

La pandemia de COVID-19 en este periodo ha tenido un impacto incalculable en todos los sentidos, y está teniendo muchos efectos duraderos. Uno de ellos es que ahora sabemos cuán importante es la ciberseguridad, especialmente en momentos en los que somos más vulnerables. Es por ello que hoy en día resulta crítico para todos nosotros aprender las mejores formas de protegernos, tanto en el ámbito privado como en el empresarial.

Los ataques dirigidos a grandes corporaciones, a secciones gubernamentales, empresas públicas, proveedores, etc. han puesto de manifiesto la necesidad de una cooperación más estrecha entre los sectores público y privado, con el fin de atajar eficazmente el peligro que la COVID-19 supone para nuestra salud, también desde la perspectiva de la ciberseguridad.

Con una tendencia cada vez más al alza y especialización de los ciberatacantes, y con un mundo tan cambiante en poco tiempo, no cabe duda de que se avecinan grandes retos para los profesionales de la ciberseguridad, que seguirán siendo una pieza fundamental en el día a día de todos.


www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es
ccn-cert
centro criptológico nacional
CCN
centro criptológico nacional