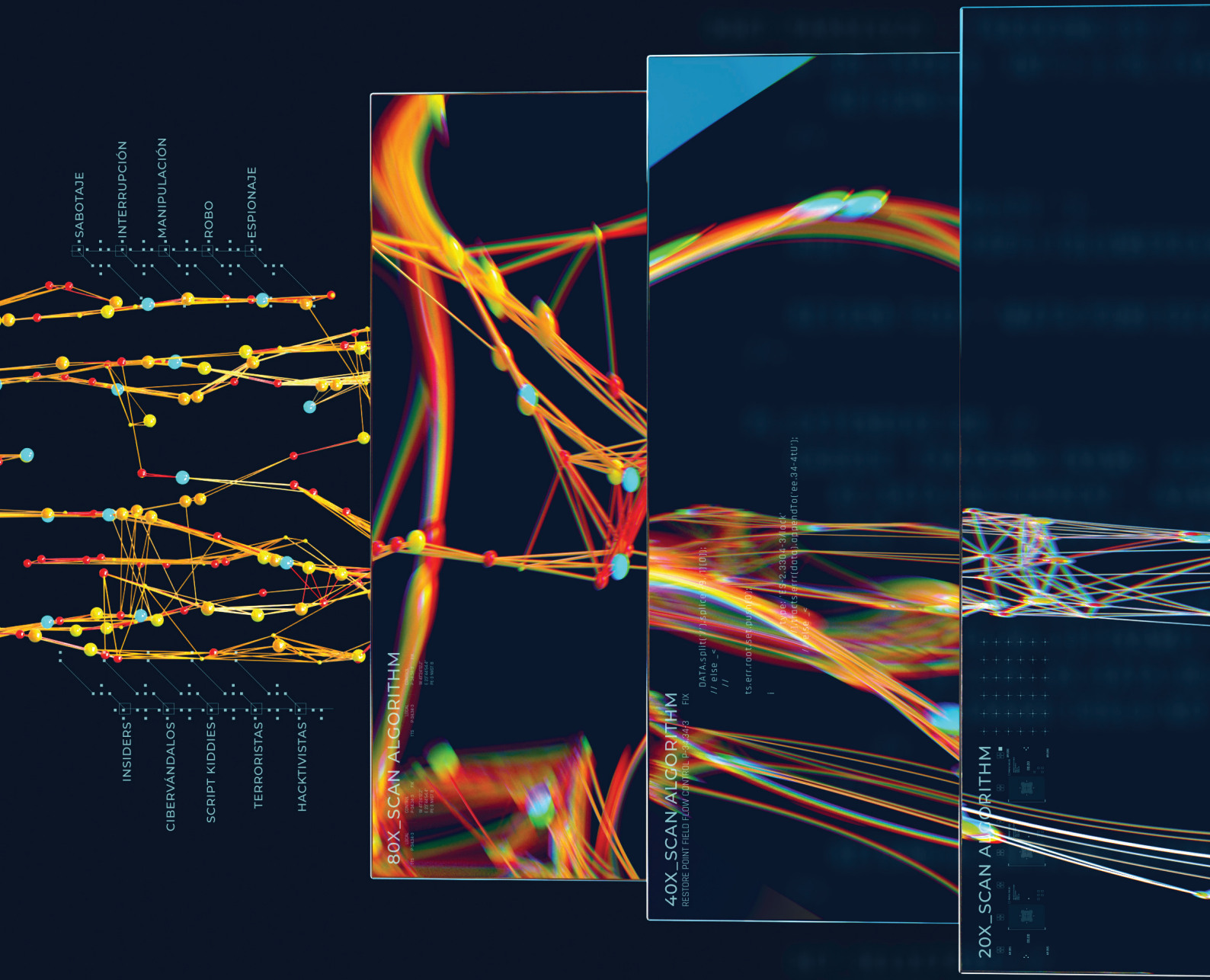
CIBERMENAZAS Y TENDENCIAS

EDICIÓN 2020

CCN-CERT IA-13/20

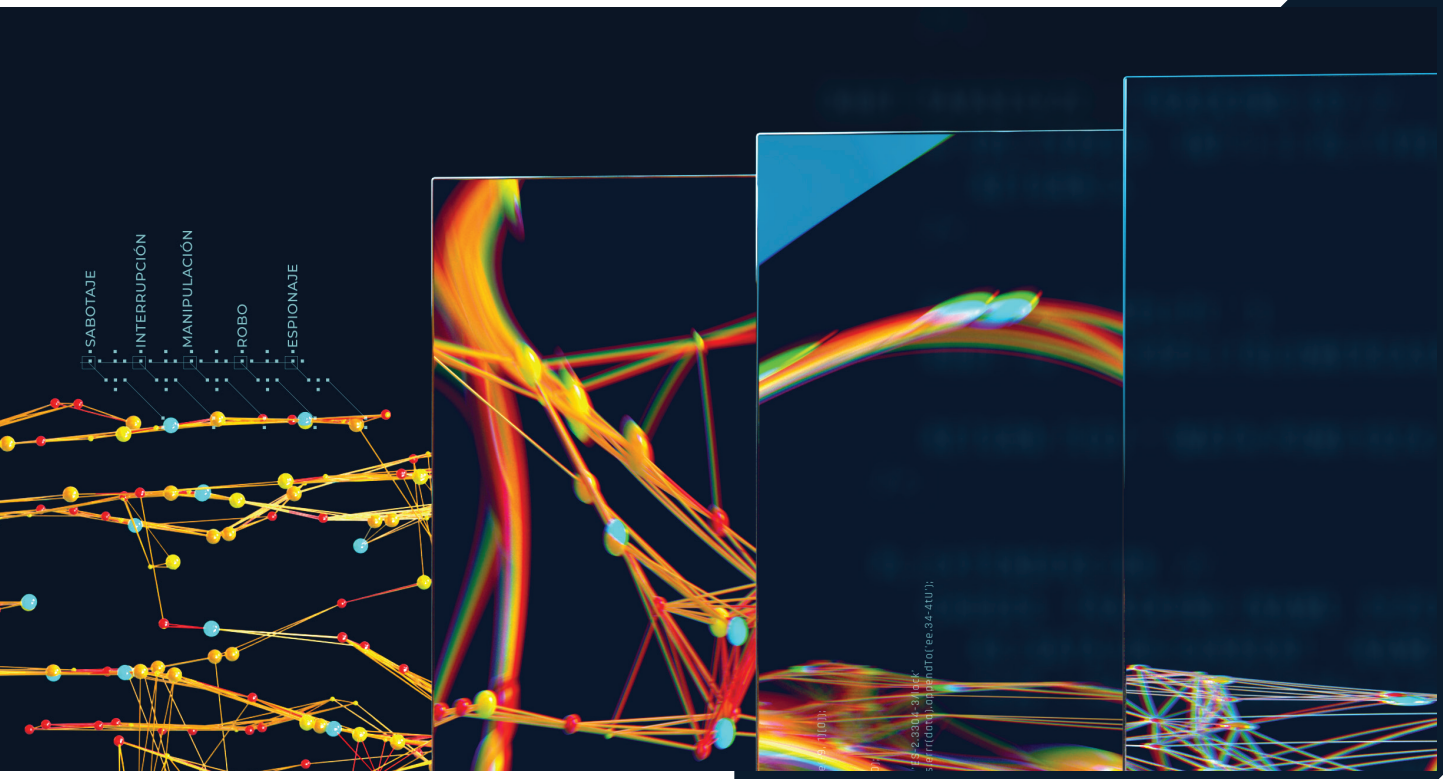


SEPTIEMBRE **2020**

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

CCN centro criptológico nacional

ccn-cert centro criptológico nacional



Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

© Centro Criptológico Nacional, 2020

Fecha de Edición: septiembre de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.09.29 12:02:55 +02'00'

Índice

1 Generalidades 02

Sobre el CCN-CERT 02
Sobre el presente informe 03

2 Resumen ejecutivo 04

3 Antecedentes 05

4 Agentes de la amenaza 08

Actores Estado 08
Ciberdelincuencia 10
Ciberterrorismo 11
Hacktivismo 13
Actores internos 14

5 Incidentes 2019 15

Panorama general 15
Operaciones de adquisición de información. Ciberespionaje 18
Operaciones disruptivas y de control 19
Operaciones de influencia. Desinformación 19
Operaciones delincuenciales 22
Brechas de datos 25

6 Métodos de ataque 26

Actividades de ransomware 26
Botnets 28
Código dañino avanzado 29
Ataques a sistemas de acceso remoto 30
Ataques web 31
Ingeniería Social 32
Ataques contra la cadena de suministro 33
Ataques contra sistemas ciberfísicos 34

7 Tendencias 2020 36

1 Generalidades

1.1 Sobre el CCN-CERT

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**.

1.2 Sobre el presente informe

En el presente informe se presentan los elementos más destacables de las **amenazas** identificadas durante **2019** y principios de **2020**, así como las **tendencias futuras** más relevantes en el ámbito de la ciberseguridad. Se abordan en primer lugar los diferentes agentes de la amenaza, desde los actores Estado hasta los *insiders*, identificando las acciones más significativas en cada caso durante el pasado año.

Con esta visión, se analizan los incidentes más significativos en el periodo establecido, que desde un punto de vista general están causando un mayor impacto o pueden convertirse en una tendencia dañina a las tipologías habituales de incidentes, en este informe es necesario destacar las operaciones de influencia que se están ejecutando en todo el mundo y que pueden generar consecuencias directas e indirectas en el corto plazo. Este apartado proporciona la visión de **qué está sucediendo** nacional e internacionalmente.

Los actores, para materializar los incidentes, hacen uso de herramientas, vulnerabilidades, tácticas y técnicas. En definitiva, las vías de materialización del daño, es decir, **cómo atacan**, que son igualmente descritas en el presente informe y cuyo conocimiento permite potenciar las capacidades de detección de la amenaza o del impacto causado.

Por último, se recogen las **tendencias más relevantes** que se identifican como significativas, tanto en el ámbito ofensivo (nuevos métodos de ataque, tendencias, etc.) como en el defensivo (nuevas capacidades que serán de aplicación en el corto plazo o lo son ya).

Toda la información que ha servido de base para la realización de este documento proviene de fuentes abiertas, de documentos publicados por el CCN-CERT o por organismos homólogos internacionales, así como por terceros (organismos, empresas privadas, particulares...).

2 Resumen ejecutivo

Como cada año, el CCN-CERT publica su informe relativo a ciberamenazas y tendencias, en el que se repasan tanto los elementos más relevantes del año anterior como las tendencias en ciberseguridad observadas en el año en curso. En la presente edición, ya entrado 2020, hay obviamente un elemento disruptivo que marca partes de este documento: la pandemia de **COVID-19** sufrida en todo el mundo. Esta situación ha influido, desde múltiples puntos de vista, en el panorama de la ciberseguridad global; en especial, ha sido aprovechado por actores hostiles para, al amparo de la situación sufrida, potenciar desde operaciones de influencia o robo de información hasta campañas de *ransomware*.

En este documento se contextualiza en primer lugar la **situación actual**, tanto ligada a la situación provocada por la pandemia como ligada a otros factores relevantes para el ámbito de la ciberseguridad, para a continuación exponer, como se ha indicado, los principales elementos relativos a los agentes de la amenaza, vulnerabilidades... hasta acabar con las tendencias previstas a corto plazo -y de nuevo, siendo conscientes de la situación actual-.

Algunos elementos destacables del informe, cuyo detalle puede analizarse en este documento, son los siguientes:

- Incremento de las acciones ligadas a actores Estado en el ámbito de las operaciones de influencia, propaganda, desinformación...
- Mejora significativa de las capacidades técnicas y operativas de actores ligados a la delincuencia económica (fraude al CEO, *Human Operated Ransomware*...).
- Incremento de los impactos contra sistemas ciberfísicos, bien como objetivo final, bien como daño colateral en ataques a infraestructura IT.
- Explotación de sistemas expuestos a Internet por todo tipo de actores, hecho que se ha visto incrementado por la situación de pandemia y el incremento del teletrabajo (y la exposición no controlada de muchas organizaciones a Internet).
- Refuerzo de la normativa y regulación del ámbito de la seguridad, tanto en España como en el panorama internacional.
- Necesidad, y tendencia, de los elementos ligados a inteligencia artificial en el ámbito de la seguridad, tanto para los atacantes como para los defensores.
- Por último, es necesario destacar de manera global la influencia de la pandemia de COVID-19 en la ciberseguridad, sus implicaciones directas y actuales y las posibles implicaciones futuras que esta situación pueda motivar.

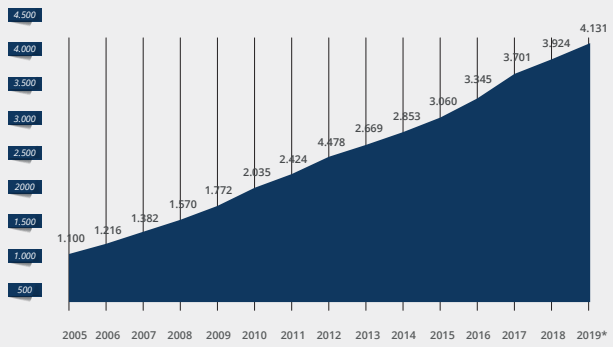
3 Antecedentes

El presente informe se desarrolla durante los primeros meses del año en curso. Tradicionalmente analiza lo esencial de lo acontecido durante el año anterior en materia de ciberseguridad: incidentes, amenazas, actores... y lo que puede suceder el año en curso a la vista del desarrollo tecnológico actual.

Este año la elaboración del presente informe se ha visto afectada, como todo lo demás, por el desarrollo de la pandemia mundial provocada por la COVID-19 que derivó, en España, en la declaración del Estado de Alarma el pasado 14 de marzo, cambiando de forma significativa el devenir habitual de los acontecimientos.

Por este motivo, aunque el núcleo del documento sigue siendo el mismo, resulta imposible obviar lo que está sucediendo tanto en nuestro país como en el mundo, de manera que a lo largo del desarrollo del informe de este año se hará mención a hechos que se consideren relevantes sucedidos como consecuencia de la situación extraordinaria que se está viviendo, siempre relacionados con la seguridad y disponibilidad de la infraestructura digital.

Durante la pandemia se ha podido comprobar la criticidad de nuestras **infraestructuras digitales**. Han prestado un servicio básico a la sociedad permitiendo mantener la comunicación entre personas, la colaboración entre equipos de investigación en cualquier parte del mundo, la compartición inmediata de los datos que se iban conociendo de la COVID-19, el ocio para millones de personas confinadas en sus casas durante semanas, el teletrabajo y por tanto el mantenimiento de cierta actividad productiva, etc. Estas infraestructuras digitales son los cimientos de la nueva sociedad y que ahora, más que nunca, se presentan como unas infraestructuras críticas soporte de servicios esenciales de la sociedad.



Número de usuarios de Internet en el mundo desde 2005 a 2019 (en millones)
Fuente: ITU "Key 2005-2019 ICT Data for the World"

El desarrollo de esta infraestructura digital está marcado por elementos como la hiperconectividad, los avances tecnológicos o la incorporación incesante de nuevos ciudadanos al mundo tecnológico.

La evolución de la población mundial sigue al alza y de la misma forma el número de internautas y, por tanto, la población digital, también crece sin parar. Según datos de Naciones Unidas más de 7.750 millones de personas habitan el planeta

en 2020[1] de los que el 67 % disponen de un dispositivo móvil, el 59 %, 4.450 millones, un 7 % más que el año anterior, son ciudadanos digitales y un 49 %, 3.800 millones, un 9,2 % más que el año anterior son usuarios de redes sociales en el mundo[2].

Focalizándonos en España, según datos de la misma fuente, en enero de 2020 había 42,4 millones de usuarios de internet, un 4,3 % superior al año anterior, alcanzando una tasa de uso del 91 % de la población. Más de 29 millones de personas en España usaban las redes sociales, con un incremento anual del 3,1 %, suponiendo un 62% de la población y el número de conexiones móviles suponían un 116 % de la población con más de 54 millones. Estas cifras ponen de manifiesto el uso intensivo de las TIC en general por parte de la población española y su incremento año tras año a pesar de estar ya en niveles muy altos de tasa de penetración.

En paralelo, el sector TIC en España sigue en pleno crecimiento tal y como demuestran las cifras presentadas por el informe publicado por ONTSI en 2019 sobre datos de 2018[3]. El número de empresas sube un 3,2 % respecto al año anterior hasta situarse en 25.065. También sube un 8,3 % el número de personas que tienen empleo en este sector hasta llegar a la cifra de **423.541 empleados**, así como el volumen de negocio que mueve en conjunto, el cual sube un 4,1 %, alcanzando la cota de los **91.894 millones de euros**. Esto es una muestra de la fortaleza del sector y de cómo la tecnología, año tras año, va introduciéndose en todas las actividades.

Al igual que el sector TIC y el uso de la tecnología siguen su tendencia alcista, también se incrementan los problemas de ciberseguridad; desde un punto de vista internacional más del 80% de las organizaciones han experimentado al menos un ciberataque con éxito durante 2019[4], y focalizándonos en España, según el informe de la ONTSI "Dossier de Indicadores sobre Ciberseguridad y Confianza Digital en España y Europa"[5] publicado en mayo de 2020, **el 23 % de las empresas grandes en España ha sufrido algún incidente de seguridad durante el último año**. En el caso de las PYMES el porcentaje baja hasta el 12 % y en el caso de ciudadanos sube hasta situarse en el 28 % por debajo de la media europea que se sitúa en el 34 %.

1 Véase https://population.un.org/wpp/

2 Véase https://wearesocial.com/digital-2020

3 Véase https://www.ontsi.red.es/index.php/es/estudios-e-informes/Sector-TIC/Informe-Anual-del-Sector-TIC-y-de-los-Contenidos-en-Espana-2019

4 Véase https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf

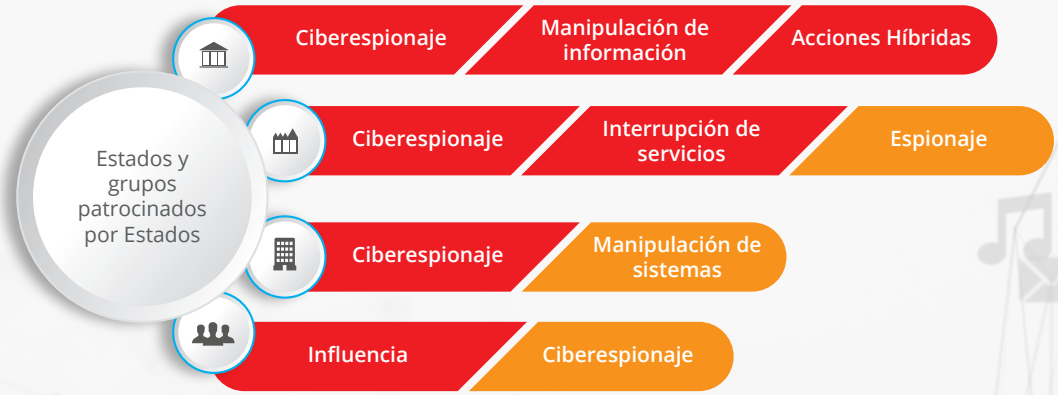
5 Véase https://www.ontsi.red.es/sites/ontsi/files/2020-06/DossierSeguridadEspa%C3%B1aCCAAEuropa.pdf

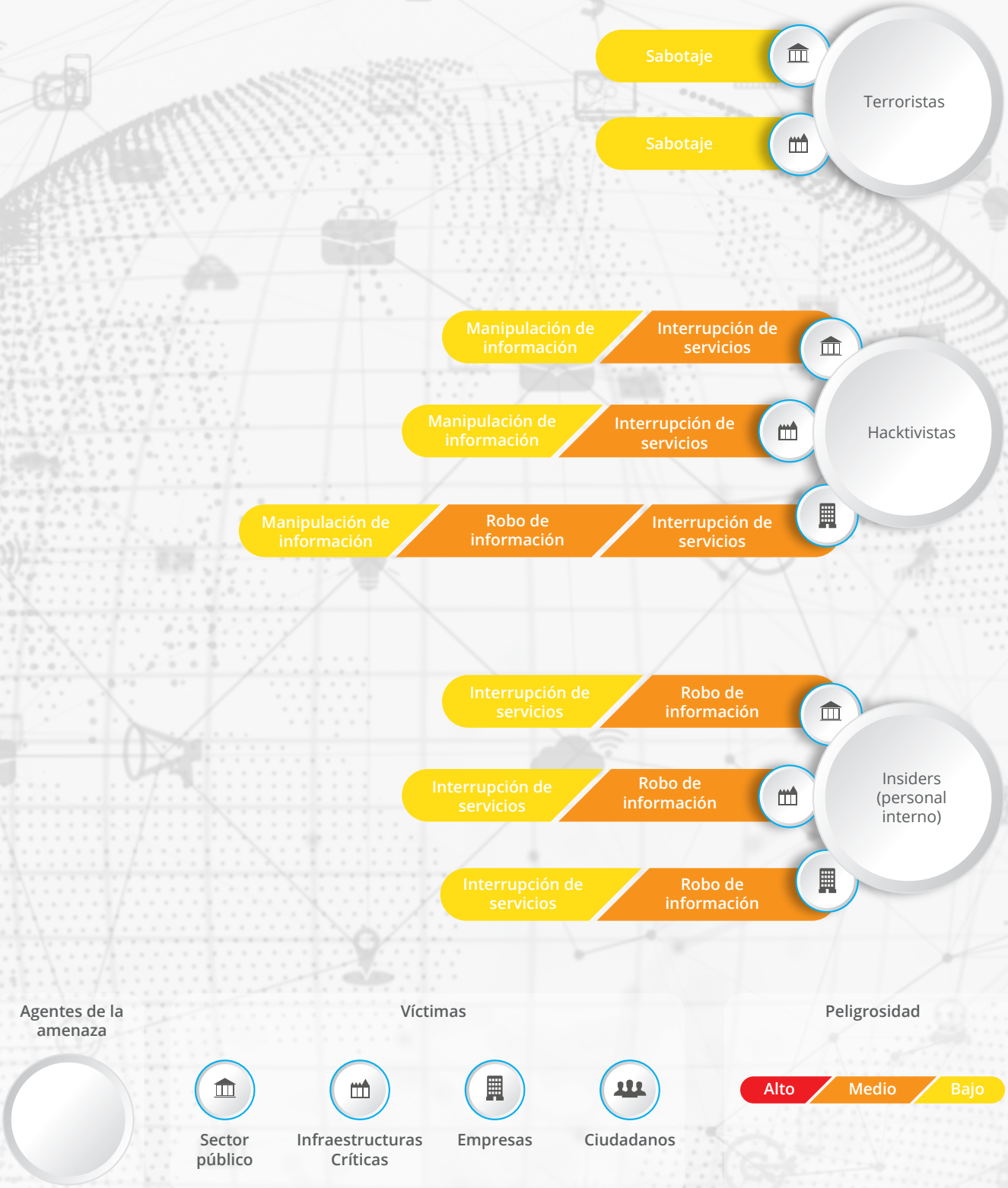
Estos porcentajes de incidentes relevantes, ponen de manifiesto la necesidad de proporcionar seguridad en el ciberespacio: seguridad de la información, del negocio, de las personas… Y es que, en un entorno hiperconectado, donde la tecnología avanza y se expande a todos los niveles, la convergencia IT/OT -e incluso CT, *Customer Technology*, introduciendo en la ecuación al usuario en su entorno personal- se debe hablar de una seguridad global, que proporcione protección a todos los niveles, desde el doméstico hasta el profesional.

En este contexto, donde la necesidad de protección en el ciberespacio es palpable, es donde desarrolla su actividad el CCN-CERT, junto al resto de actores del ecosistema de ciberseguridad o tecnología nacionales e internacionales: empresas, organismos públicos, otros CERT, servicios homólogos de otros países… En definitiva, en un contexto de requisitos y necesidades de ciberseguridad crecientes, en la que los actores de la amenaza amplían cada día más sus capacidades y los ataques son cada vez más numerosos y de mayor impacto. Afortunadamente, los esfuerzos para protegernos como país, como organización, como ciudadanos también lo son, y gracias a estos esfuerzos individuales y colectivos podemos seguir trabajando y aprovechando la tecnología en situaciones como la motivada por la COVID-19.

4 Agentes de la amenaza

Como en ediciones anteriores del presente informe, durante 2019 se han identificado los **objetivos de los principales agentes de la amenaza**, presentando la relación entre dichos agentes y sus víctimas:





Como novedad, se ha querido incluir la **influencia como objetivo de los actores estado contra el ciudadano**, dado que los principales grupos identificados no solo ejecutan operaciones ofensivas contra infraestructuras, sino que han demostrado ser capaces de ejecutar operaciones de influencia hacia la sociedad, tal y como hemos visto en el apartado previo.

4.1 Actores Estado

Los actores Estado han focalizado sus operaciones en el ciberespacio en **tres ámbitos**: la ciberguerra, el ciberespionaje y las operaciones de influencia.

En el primero de ellos, el de la **ciberguerra**, las unidades militares dedicadas al dominio ciber están presentes en la mayor parte de ejércitos de países desarrollados, dada la importancia de este dominio de conflicto –junto a tierra, mar, aire y espacio– y la necesidad de protección a ciudadanos, empresas y organismos públicos.

En el ámbito del **ciberespionaje**, de nuevo los Estados presentan una amenaza significativa, tal y como se ha indicado con anterioridad, por las enormes capacidades y recursos materiales de los que pueden disponer. Si esto se une al bajo riesgo para el actor hostil, y al enorme beneficio que se puede obtener en una campaña, convierte el ciberespacio en un terreno clave para las operaciones de obtención de información y de inteligencia en general.

En estas campañas, durante 2019 se ha evidenciado el aprovechamiento de infraestructura de terceros para llegar al objetivo final, así como la explotación de vulnerabilidades y debilidades de sistemas expuestos a Internet para lograr comprometer a sus objetivos.

En las **operaciones de influencia** por parte de los Estados juegan también un papel clave las redes sociales, que se han convertido en un medio para orquestar campañas de manipulación, con unos 70 estados identificados en este ámbito, lo que supone un incremento del 150 % durante el intervalo 2017-2019, según la Universidad de Oxford[6].

Estas operaciones, que no suelen requerir capacidades ofensivas avanzadas, afectan tanto a la población en general como a grupos específicos –militar, política...–, y suelen tener entre sus objetivos la generación de inseguridad en una población, el control o refuerzo de narrativas particulares o la generación de desconfianza en las instituciones[7].

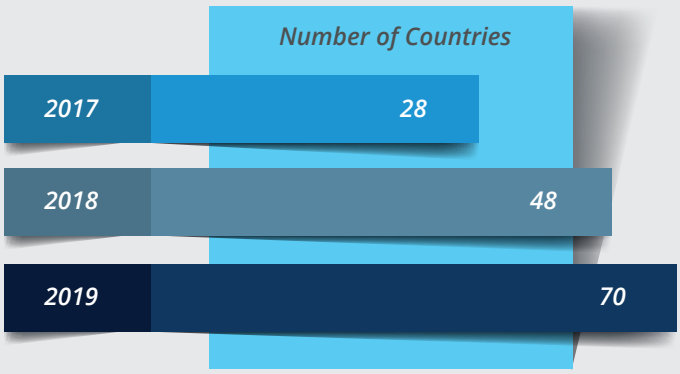


Ilustración 1. Países ejecutando campañas de manipulación 2017-2019.[8]

6 Véase https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

7 Véase https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf

8 Véase The Global Disinformation Order. Oxford University.

4.2 Ciberdelincuencia

Durante 2019 la ciberdelincuencia ha tenido como principales acciones **dos modalidades de ataque**: por un lado, el uso de ransomware para cifrar los discos de las víctimas y solicitar un rescate, especialmente en campañas definidas como ***Human Operated Ransomware*** (**HOR**); y por otro el conocido como fraude del CEO, (***BEC, Business E-Mail Compromise***).

HOR	**BEC**
Human Operated Ransomware	*Business E-Mail Compromise*

En el ámbito del ransomware, además del formato clásico en el que un código dañino es remitido por correo electrónico, generalmente de forma no dirigida a un número de víctimas, durante 2019 se han incrementado de manera significativa los casos de ransomware operado por humanos, HOR.

En esta modalidad, el atacante compromete la infraestructura de la víctima, generalmente mediante la explotación de vulnerabilidades o debilidades en sistemas expuestos a Internet (concentradores VPN, sistemas de terminal remota, etc.), y se mueve lateralmente dentro de dicha infraestructura hasta tomar el control para, en un momento determinado, ejecutar el código dañino y cifrar la información.

Adicionalmente, estos actores exfiltran información sensible de la víctima para publicarla en Internet, incrementando así el grado de amenaza y causando impacto con independencia de las copias de seguridad o de la capacidad de la víctima para recuperar técnicamente el entorno.

Este modo de operación es similar al de actores avanzados a la hora de comprometer y persistir en sus objetivos; aunque su grado de complejidad no sea tan alto, las fases del ataque son equivalentes, convirtiéndose el ransomware en la última etapa de la operación. Estos ataques representan otra vuelta de tuerca frente a los ataques de ransomware no dirigidos y causan en la víctima mucho mayor impacto, por lo que los grupos delincuenciales los están ejecutando de forma sistemática, obteniendo unos enormes beneficios en cada operación.

Además del ransomware, el fraude del CEO es otro de los principales mecanismos de fraude que se han desarrollado durante 2019. Aunque en su denominación coloquial sigue haciéndose referencia al CEO, es cierto que los atacantes están marcando objetivos de menor nivel en la jerarquía de las organizaciones. Según el FBI, este tipo de estafas sufrió un incremento del 100 % desde mediados de 2018 hasta mediados de 2019,[9] con miles de millones de pérdidas para las organizaciones víctimas. Aunque existen variantes técnicamente más complejas y que implican compromisos de emisor, receptor o transporte, la modalidad más simple del ataque es una cuestión pura de ingeniería social, por lo que se ha de insistir de nuevo en la necesidad de la concienciación para detectar este tipo de operaciones y minimizar su impacto.

9 Véase https://www.ic3.gov/media/2019/190910.aspx

Desde el punto de vista delincuencial, el correo electrónico sigue siendo la principal vía de entrada de los atacantes, aunque los mensajes de texto –SMS– también han sido explotados con éxito durante 2019, según el *Internet Crime Complaint Center*, del FBI estadounidense.[10]

Tanto en los ataques BEC como en los de ransomware no operado el correo electrónico juega un papel fundamental, aunque es cierto que en los HOR los atacantes aprovechan sistemas expuestos a Internet, con vulnerabilidades o debilidades, para tomar el control de la infraestructura de la víctima. Es especialmente significativo, en este ámbito, el aprovechamiento de sistemas de terminal remota (**RDP**, ***Remote Desktop Protocol***) expuestos, como indica la propia EUROPOL.[11]

La capacidad de organizaciones criminales o delincuentes individuales de hacer uso de herramientas de ciberataques sin necesidad de contar con especialistas en la materia está generalizándose de forma global. La proliferación del ***Malware as a Service*** (**MaaS**) permite que cualquiera pueda adquirir recursos para llevar a cabo estos actos. El uso de la *Dark Web* y de criptomonedas para el pago facilita la ocultación de la contratación de estos servicios.

La ciberdelincuencia afecta a todo tipo de organizaciones, incluyendo pequeñas empresas o entidades locales, que en muchos casos sufren un impacto enorme en proporción a su tamaño. Como ante cualquier otro delito, en todos los casos es siempre necesaria la denuncia de los hechos, tanto si el fraude se ha materializado como si ha sido en grado de tentativa.

4.3 Ciberterrorismo

En marzo de 2020 el CCN-CERT publicó el **informe anual sobre hacktivismo y ciberyihadismo**, **CCN-CERT IA-04/20**,[12] en el que se indicaba que durante 2019 no se identificaron operaciones de ciberyihadismo y sigue sin haber evidencias de capacidades ofensivas de estos grupos en el ámbito ciber.

Aunque no haya constancia de capacidad operativa en el ciberespacio por parte de grupos terroristas, el uso de servicios legítimos para la difusión de **mensajes ligados al terrorismo** por parte de estos actores sigue siendo un hecho destacable, al igual que en años anteriores. Grupos terroristas usan estos servicios con el objetivo de **reclutar miembros**, **potenciar su imagen** –en cualquiera de los sentidos posibles–, **establecer redes online de simpatizantes a efectos de comunicación y diseminación e incluso obtener dinero**. EUROPOL, en su informe *Internet Organised Crime Threat Assessment (IOCTA) 2019*,[13] destaca la rápida adopción de nuevos servicios y tecnologías por parte de estos grupos, lo que en ocasiones dificulta el trabajo de eliminación o bloqueo de estos contenidos dañinos. Redes sociales, sitios de intercambio de ficheros, servicios de mensajería y *streaming* son aprovechados por estos actores con los fines anteriormente expuestos.

10 Véase https://pdf.ic3.gov/2019_IC3Report.pdf

11 Véase https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

12 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4714-ccn-cert-ia-04-20-informe-anual-2019-hactivismo-y-ciberyihadismo-1/file.html

13 Véase https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Estos grupos están aprovechando para sus actividades plataformas pequeñas o de reciente creación como vía alternativa a las ya consolidadas, lo que dificulta los procesos judiciales y técnicos de bloqueo o eliminación, y por tanto mantiene operativa durante más tiempo la infraestructura dañina. En este sentido, la colaboración público-privada es, de nuevo, crítica para hacer frente a estas acciones, en especial entre fuerzas de seguridad y empresas que proporcionan servicios digitales.

4.4 Hacktivismo

En el informe CCN-CERT IA-04/20, anteriormente referenciado, se pone de manifiesto la ausencia de una estructura hacktivista en España que presente una capacidad coordinada para planear y ejecutar ciberataques con un mínimo de peligrosidad; la única identidad digital capaz de orquestar operaciones, mínimamente estructurada y con capacidad técnica, es "La 9ª compañía", comúnmente conocida como "La9" o "La9deAnon".

El marco de #OpCatalunya, con sus diferentes denominaciones, ha catalizado las actividades de identidades ligadas a ideologías independentistas, aunque con una reducción significativa de dichas actividades con respecto a 2018. Se han identificado perfiles ofensivos (***defacements***, **inyecciones SQL**, **denegaciones de servicio**, etc.), de baja peligrosidad en términos generales, así como también perfiles desinformativos cuyo objetivo es la difusión de propaganda secesionista en redes sociales. Estos últimos perfiles pueden estar ligados a actores con capacidades más avanzadas y con los que trabajan de manera coordinada, como se ha evidenciado en otras operaciones ajenas a la situación política de Cataluña.

Otro hecho especialmente relevante y que suele generar actividad hacktivista es la celebración, en 2019, de diferentes **procesos electorales en España**; desde el CCN-CERT no se ha evidenciado actividad hacktivista significativa durante estos, más allá de iniciativas en redes sociales orientadas a desinformación, pero sin impacto relevante en ninguno de los procesos.

Ya en el ámbito internacional, en el mismo informe CCN-CERT IA-04/20, se identifica la actividad de grupos hacktivistas ligados al ámbito del **yihadismo**, con operaciones de *defacement* durante 2019, pero sin mayor repercusión. Al igual que en España, en el panorama internacional los aspectos generales del *hacktivismo* referencian a grupos escasamente organizados y con poca capacidad ofensiva.

No obstante, es necesario destacar la actividad de identidades muy concretas (*Phineas Fisher* o *PokemonGo*, entre otros) cuyo comportamiento, aparentemente hacktivista, no se ajusta a los patrones habituales de estos grupos, que disponen de capacidades técnicas avanzadas y aparentemente no buscan una notoriedad personal. Diferentes analistas trabajan con la hipótesis de que estas identidades estén manejadas por actores avanzados manejando la información que previamente hayan podido robar, con propósitos de propaganda, desinformación o similares.

Toda la información referente a hacktivismo durante 2019 puede ampliarse en el informe **CCN-CERT IA-04/20**, publicado en marzo de este año por el Centro Criptológico Nacional.

4.5 Actores internos

Durante 2019 el actor interno sigue suponiendo una preocupación para los responsables de seguridad de la mayoría de organizaciones. El pasado año se produjo un **incremento de aproximadamente el 28 %** en relación a incidentes derivados de los usuarios (empleados o contratistas). [14] La mayor parte de estos incidentes están ligados no a una intención dañina por parte de las personas que trabajan en una organización, sino a errores y a la falta de concienciación, formación y entrenamiento de los usuarios.[15]

La mayor parte de los incidentes ha causado un **impacto reputacional** en las organizaciones que los han sufrido, especialmente por la exposición de datos sensibles. El **impacto económico**, tanto directo en forma de fraude como indirecto en forma de robo de la propiedad intelectual o industrial, son también daños a considerar al hablar de la amenaza interna.

La principal medida a adoptar en las organizaciones es la **concienciación** en un sentido amplio[16]. Dado que la mayor parte de los incidentes no son intencionados, sino derivados de errores, es fundamental la capacitación de todos los usuarios, desde los administradores de sistemas hasta los perfiles que a priori no tienen un perfil de seguridad. Por supuesto, los controles técnicos –DLP, IAM, etc.– son básicos, pero su utilidad siempre debe ser reforzada por la actitud y aptitud de los usuarios de la organización.

14 Véase https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

15 Véase https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

16 Véase https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

5 Incidentes 2019

5.1 Panorama general

En 2019, el CCN-CERT gestionó **42.997 ciberincidentes** –más de un 11 % con respecto al año anterior–, de los cuales casi **un 7,5 %** fueron de **peligrosidad muy alta o crítica**, como se observa en las gráficas a continuación.

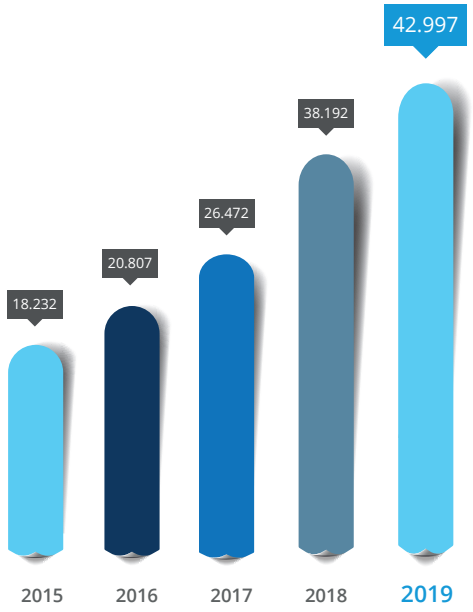


Ilustración 2. Incidentes gestionados por el CCN-CERT entre 2015 y 2019

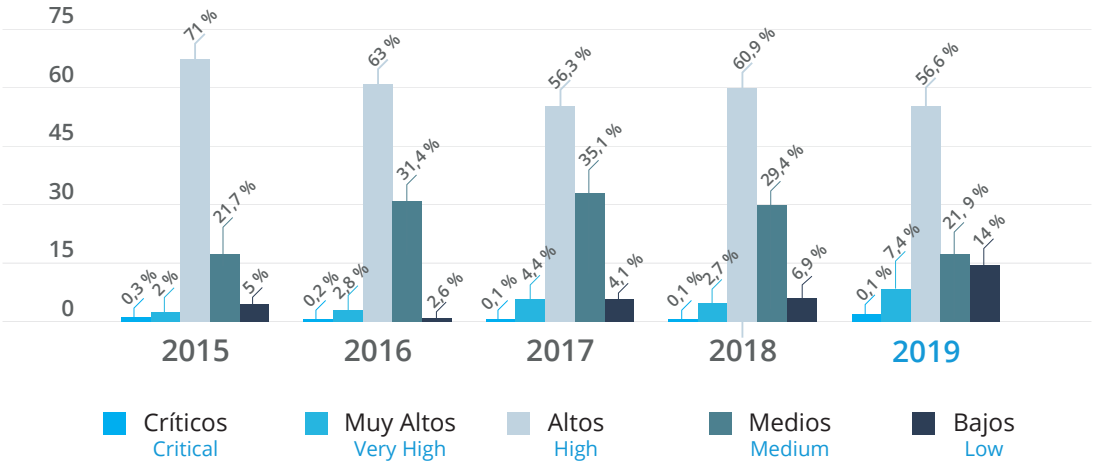


Ilustración 3. Peligrosidad de los incidentes gestionados por el CCN-CERT entre 2015 y 2019

Respecto a la tipología de los incidentes, destacan de manera clara los incidentes relacionados con **intrusiones** y **código dañino**, sumando entre ambos un **64%** del total, como se muestra a continuación:

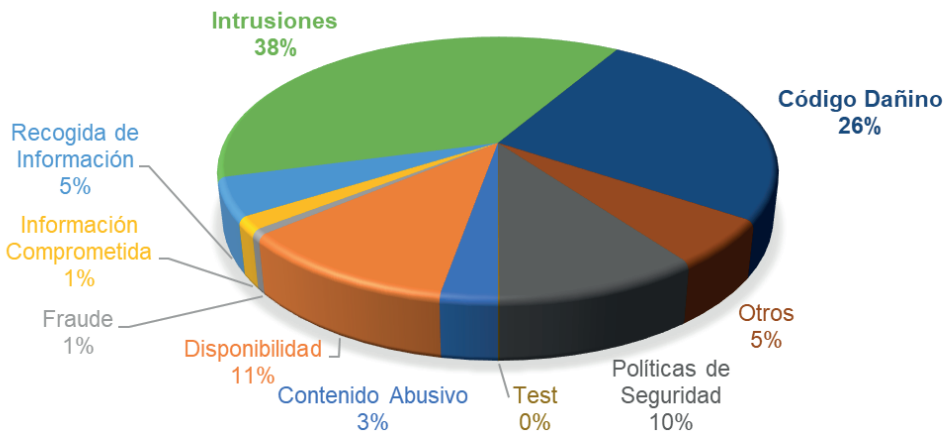


Ilustración 4. Incidentes gestionados en 2019 por el CCN-CERT por tipología

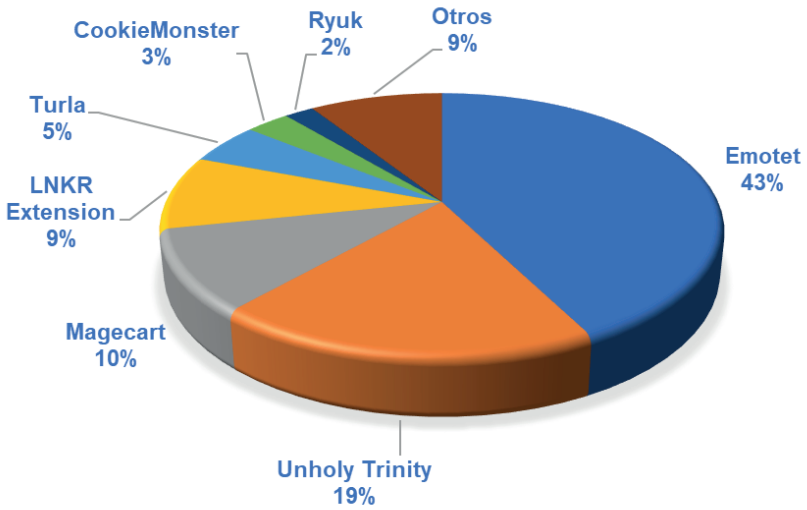


Ilustración 5. Familias de malware detectadas en los incidentes gestionados por el CCN-CERT en 2019

Si analizamos los incidentes de **código dañino**, se pueden identificar las diferentes **familias de malware** detectado:

En particular, en los datos de 2019 se advierte cómo el malware ***Emotet*** destaca de manera significativa sobre el resto, siendo el **responsable de más del 40% de los incidentes gestionados por el CCN-CERT en este ámbito**. Durante el pasado año, estos programas dañinos se utilizaron

en múltiples campañas de ataques a organizaciones de todo tipo, con especial incidencia en el último trimestre del año. Debido a ello, el 7 de octubre el CCN-CERT emitió una alerta[17] avisando de la existencia de una campaña muy agresiva de ataques del troyano *Emotet* contra los usuarios finales.

Más de treinta organismos públicos y empresas españolas sufrieron en un breve período de tiempo este tipo de ataques, solicitando colaboración al CCN-CERT. No obstante, se detectó que no todos los casos reportados eran *Emotet*; en algunos de ellos la ejecución de código dañino era la última etapa de una campaña de fraude en la que, para evitar ser descubierto, el atacante ejecutaba un ransomware con la intención de ocultar sus acciones.

Para hacer frente a esta campaña, el **CCN-CERT** llevó a cabo una intensa actividad; desarrolló una **vacuna** (***Emotet-stopper***[18]), publicó **5 informes** (entre los que se incluían las familias de código dañino involucrados: *Emotet*, *Trickbot* y *Ryuk*) y emitió **3 avisos y alertas a su comunidad**. Además, recopiló en diversas listas negras indicadores para facilitar la detección y el bloqueo de las actividades maliciosas (listas de direcciones IP, dominios y hashes de las muestras empleadas) y desplegó equipos propios en las sedes de algunos de los organismos afectados. Toda esta información la compartió en el grupo de equipos de ciberseguridad y gestión de incidentes españoles, CSIRT.es[19], un ejemplo de colaboración público-privada.

Adicionalmente a la información de los incidentes gestionados, el CCN-CERT puso en marcha en 2008 el **Sistema de Alerta Temprana** (**SAT**), para la detección rápida de incidentes y anomalías en la Administración Pública y las empresas de interés estratégico, y que muestra también datos interesantes.

En lo relativo a incidentes en infraestructuras críticas nacionales, se mantiene la tendencia al alza observada en años anteriores. Como se recoge en el Informe anual de seguridad nacional del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, se pasó de los 17 ataques detectados en 2013 a los 6.954 en 2018. Así, en 2019 se reportaron al **Centro Nacional de Protección de Infraestructuras Críticas** (**CNPIC**) un total de **8.086 incidentes de ciberseguridad en operadores críticos**, **de servicios esenciales o estratégicos**. Si bien estos incidentes no llegaron a causar un impacto en los servicios esenciales prestados por los operadores afectados. Los sectores más afectados fueron el financiero y tributario, energético y transporte, que alcanzan conjuntamente un 50% de los incidentes totales gestionados.[20]

Es importante destacar que estos datos recogen una visión parcial de la situación; conocer el grado exacto de exposición de un país a las ciberamenazas y ciberincidentes es una tarea de gran

17 Véase https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/8730-ccn-cert-al-06-19-campana-troyano-emotet.html

18 Véase http://ccn-cert.net/emotet2019

19 Véase https://www.csirt.es/index.php/es/

20 Véase Informe anual de seguridad nacional. Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno. Marzo de 2020

complejidad no exenta de dificultades. Para ello sería necesario contabilizar la totalidad de los ataques sufridos, no solo por todo el sector público, sino también por el conjunto de las empresas y la propia ciudadanía, sin olvidar que no todos los ataques se detectan o se comunican y, por tanto, siempre existirá un factor importante de indeterminación.

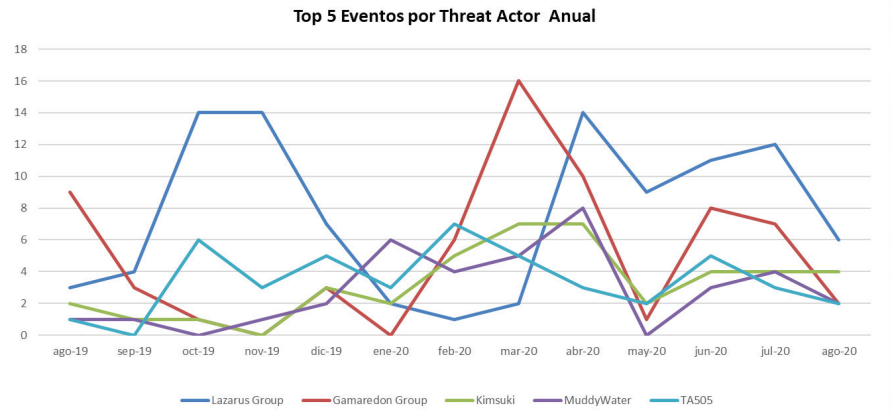
Sin embargo, los datos disponibles sí nos permiten construir una imagen aproximada del escenario actual, para lo que se ha hecho el ejercicio de recopilación a modo de muestreo de un listado de los ciberincidentes más significativos de 2019 –incluidos los acontecidos en España–, agrupados por las motivaciones de los agentes de las amenazas. En los siguientes epígrafes se exponen los ciberincidentes más significativos de 2019, agrupados por las motivaciones de los agentes de las amenazas.

5.2 Operaciones de adquisición de información. Ciberespionaje

La situación geopolítica de los últimos años marca una tendencia creciente en relación con las operaciones de ciberespionaje, una progresión que viene confirmada por el incremento del número de países que ha adquirido la capacidad de recopilar inteligencia del ciberespacio. Estas capacidades las componen los denominados grupos de **APT** (**amenaza persistente avanzada, de inglés *"Advanced Persistent Threat"***), que consisten en personal muy especializado, con grandes conocimientos técnicos y dotados de muchos recursos económicos y materiales, que llevan a cabo las intrusiones en las redes objetivo para permanecer ocultos durante el mayor tiempo posible y extraer información de ellas.

En la actualidad, son ya más de cien países los que presentan la capacidad de desarrollar ataques de ciberespionaje, y su especialización sigue creciendo, de la misma forma que lo hace la amenaza que representan. Esta capacidad, está dirigida tanto al sector público como al privado, y suele provenir de países que desean mejorar su posición a nivel político, estratégico o económico. Todo ello, sin olvidar las mafias organizadas y grupos de mercenarios cuyos grandes beneficios no hacen prever una disminución de este tipo de actividades.[21]

Esta actividad creciente se puede observar en el gran número de informes disponibles sobre este tipo de actores publicados por las principales empresas dedicadas a la ciberseguridad:



Fuente: Elaboración propia con información de REYES (CCN-CERT)

21 Véase https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/3573-ciberespionaje-una-amenaza-al-desarrollo-economico-y-la-defensa/file.html

Los **actores más activos** durante el año **2019** han sido los siguientes:

- **Grupo Snake**: uno de los grupos más activos en los últimos años, centrado principalmente en el Sector Público y en empresas del sector defensa.
- **Grupo APT27/Emissary Panda**: grupo muy activo contra empresas tecnológicas y del sector aeroespacial, su principal objetivo es el robo de propiedad intelectual.
- **Grupo APT28/Sofacy**: grupo muy activo contra el Sector Público y sector defensa, con numerosos intentos de intrusión a través de campañas de spear-phishing.
- **Grupo APT39**: ataques contra empresas y proveedores del sector aeronáutico. En estos casos la finalidad del ataque es la obtención de información personal de individuos.
- **Grupo APT33**: ataques contra empresas del sector privado como vía de entrada a objetivos de otros países y empresa tecnológicas mediante acciones de sabotaje.
- **Grupo APT41**: ataques contra la Adminstración Pública y entidades privadas con motivación económica.
- **Grupo Winnti**: ataques contra empresas de diversos sectores industriales.

Es importante destacar que la actividad de los grupos APT no se limita a atacar a sus víctimas, sino que también comprometen otros sistemas para usarlos como parte de su infraestructura de ataque, bien como servidores de mando y control, bien como máquinas de salto y/o gestión.

Las empresas sanitarias son otro de los objetivos del ciberespionaje. Sin embargo, los grupos de ciberespionaje no solo están interesados en este sector, sino también en adquirir cualquier tipo de tecnología avanzada que apoye el desarrollo de sus capacidades en cualquier sector: espionaje industrial.

Así, el pasado 4 de marzo salía a la luz una publicación de **FireEye** en la que se identificaba al grupo **APT40** como autor de una serie de ciberataques sobre universidades, en particular focalizadas en la investigación en el sector naval y tecnologías marítimas.[22]

Por último, durante 2019 se ha registrado un sustancial incremento contra dispositivos y **sistemas IoT** que, sin duda, veremos incrementarse en un futuro próximo. Los ataques contra los componentes ciberfísicos de estos sistemas se tratan en detalle en el punto 6.7.

5.3 Operaciones disruptivas y de control

Durante 2019 se puso de manifiesto, una vez más, el gran impacto que puede tener un ciberataque en los sistemas ciberfísicos o incluso en el plano físico, y cómo la convergencia tecnológica hace que un ataque tradicionalmente considerado típico de los entornos tecnológicos puede acabar teniendo un impacto sobre procesos industriales, tal y como veremos en el punto 4 con los casos de ransomware no específico.

22 Véase https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

Es un hecho que los ataques a las redes eléctricas pueden causar estragos, tanto a nivel económico como a la población, lo que las convierte en blanco de ciberataques por parte de diferentes actores, tanto de occidente como de oriente.

Otro de los sectores más estratégicos para la sociedad es la industria petrolera; una interrupción brusca del funcionamiento de cualquier compañía de este tipo tendría una gran implicación para la economía mundial.

5.4 Operaciones de influencia. Desinformación

España sufre diariamente ciberataques de peligrosidad crítica o muy alta contra el sector público y empresas estratégicas. Algunas de estas acciones provienen de otros Estados, que tienen entre sus motivaciones debilitar la capacidad política, tecnológica y económica nacional. El impacto de estos ataques puede ocasionar desde pérdidas millonarias en empresas privadas hasta interferir en el normal funcionamiento de servicios públicos esenciales para la ciudadanía.

Sin embargo, los ataques que utilizan el ciberespacio no solo tienen como objetivo los sistemas informáticos de empresas e instituciones, sino que cada vez más están dirigidos a influir o alterar la opinión pública.

Tal y como se refleja en el *Informe Anual de Seguridad Nacional 2019* publicado por el Departamento de Seguridad Nacional[23], se ha detectado un aumento en las actividades realizadas por otros Estados que tienen como objetivo influir en los procesos sociales y políticos en Europa, incluida España. Este tipo de acciones pretenden, fundamentalmente, desacreditar las instituciones democráticas a través de la polarización social y la generación de desconfianza en los medios de comunicación, en las instituciones públicas y en la soberanía del ciudadano.

De especial importancia son las acciones de desinformación desplegadas, principalmente en redes sociales y otros medios digitales de similar naturaleza. Tal y como se expone en el informe ***CCN-CERT BP/13 Desinformación en el ciberespacio***,[24] las técnicas de propaganda y desinformación[25] se han ido perfeccionando, lo que ha supuesto que a los métodos tradicionales se sumen herramientas automáticas de divulgación cuyo bajo coste, facilidad de uso y compleja trazabilidad incrementan de forma considerable su utilización y repercusión.

El grupo de investigación de la Universidad de Oxford, COMPROP (The Computational Propaganda Project), publicaba un estudio[26] que revelaba que, en al menos 70 países, ya existen **campañas de desinformación en redes sociales**.

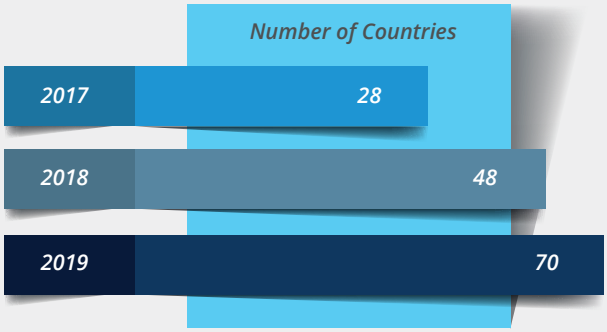
23 Véase https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2019

24 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3552-ccn-cert-bp-13-desinformacion-en-el-ciberespacio-1/file.html

25 Véase https://www.ccn-cert.cni.es/pdf/documentos-publicos/xiii-jornadas-stic-ccn-cert/ponencias/4435-s21-11-03-desinformacion-2-0/file.html

26 Véase https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Illustración 6. Incremento del número de países que emplean campañas de desinformación en redes sociales[27]



150%

the increase in countries using organised social media manipulation campaigns over the last two years

Twitter es una de las plataformas que más operaciones de este tipo ha venido sufriendo, y en enero de 2019 la compañía revelaba[28] algunas de ellas. Llaman la atención los datos que ofrece Twitter en su informe de transparencia: solo **en el primer semestre de 2019 canceló más de 97 millones de cuentas por intentos de manipulación en la plataforma**.[29]

Number of accounts challenged monthly Jan 1 - Jun 30, 2019

Month	Challenges
January	19,522,273
February	17,036,751
March	16,552,753
April	13,787,154
May	14,848,125
June	15,376,611
TOTAL	**97,123,667**

Ilustración 7. Cuentas canceladas por Twitter por intentos de manipulación[30]

Si bien Twitter y Facebook son consideradas las principales redes en las que se llevan a cabo operaciones de desinformación, **Instagram** comienza a ser una plataforma muy usada para tales fines, sobre todo en el contexto de operaciones militares; el empleo del recurso gráfico es clave en la producción propagandística. Instagram, al proporcionar una síntesis entre imagen y palabra, hace más rico el lenguaje comunicativo.[31]

Asimismo, como menciona el Real Instituto Elcano,[32] la pandemia actual es un terreno fértil para la ***infodemia***, la acumulación de demasiada información por la COVID-19, así como para la desinformación. Sin embargo, dentro de ese flujo de conversaciones en redes sociales, que se entiende dentro de la normalidad considerando el escenario de preocupación global respecto de la COVID-19, no se observan líneas disruptivas de la tendencia principal.[33]

27 Véase https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf
28 Véase https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html
29 Véase https://transparency.twitter.com/en/platform-manipulation.html
30 Véase https://transparency.twitter.com/en/platform-manipulation.html
31 Véase http://www.ieee.es/en/Galerias/fichero/docs_opinion/2019/DIEEEO90_2019JAVJAS_Instagram.pdf
32 Véase http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari-58-2020-milosevich-analizar-y-comprender-campanas-desinformacion-china-rusia-covid-19
33 Véase https://www.ccn-cert.cni.es/soluciones-seguridad/elisa.html

5.5 Operaciones delincuenciales

El informe de Europol de 2019 *Evaluación de Amenazas del Crimen Organizado por Internet (IOCTA)*[34] refleja el panorama actual de las principales amenazas. Entre ellas se encuentran el uso de la red para la explotación sexual de menores, fraude en los métodos de pago, uso delictivo de la Dark Web, la convergencia entre el mundo ciber y el terrorismo, o el denominado "delito ciberdependiente", aquel delito que solo se puede cometer usando tecnología, y que incluye la difusión de malware, robo de datos, ataques de denegación de servicio, secuestro de datos (ransomware) o daño a la reputación, entre otros.

Destacables, en este sentido, son los datos del estudio publicado por el Ministerio del Interior, ***Estudio sobre la Cibercriminalidad en España 2019***,[35] que indica que se han identificado un total de **218.302 hechos relacionados con la cibercriminalidad**, un 35,8 % más con respecto al año anterior, con cerca de 9.000 detenidos e investigados. De esta cifra, el 88,1 % corresponde a fraudes informáticos, y cerca de un 6 % a amenazas y coacciones.

La cibercriminalidad en España, tal y como apunta el Sistema Estadístico de Criminalidad (SEC), **representa un 9,9 % sobre el total de infracciones penales**, más de 5 puntos por encima con respecto al 2016, donde se situaba en un 4,6 %.

A continuación, se expondrá un **muestreo de las principales operaciones ciberdelincuenciales** que han tenido lugar en el periodo que abarca el presente informe.

5.5.1 Secuestro de información: Ciberataques por Ransomware

El **ransomware** ha sido el tipo de código dañino más destructivo en la última década. De afectar a equipos personales, ha pasado a ser una de las grandes amenazas para grandes empresas y para infraestructuras críticas (hospitales, infraestructuras energéticas, etc.).

En los últimos años, las acciones dañinas de este malware han evolucionado, dando lugar a nuevas generaciones de ransomware con el objetivo de cifrar el mayor número de equipos en grandes empresas y estructuras de un país. La extensión de este tipo de malware, así como el crecimiento de variantes, se debe en parte a lo que se conoce como ***Ransomware as a Service***, servicio por el que los criminales facilitan la creación de ransomware a cualquiera que lo solicite a cambio de un porcentaje de las ganancias que la campaña obtenga.[36]

El **ransomware desplegado como último *stage* más avanzado** sigue siendo una de las amenazas más características en el ámbito del cibercrimen, reforzando la tendencia de infectar proveedores de servicios gestionados (MSP) para aumentar el impacto operativo en las empresas cliente. Este es, por ejemplo, el caso de ***ConnectWise Control***, aplicación muy usada para conectar de forma

34 Véase https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

35 Véase http://www.interior.gob.es/documents/10180/8736571/Informe+2018+sobre+la+Cibercriminalidad+en+Espa %C3 %B1a.pdf/0cad792f-778e-4799-bb1f-206bd195bed2

36 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

remota con otros equipos y utilizada para propagar ransomware.[37,38]

De la mano de *Emotet*, *Ryuk* ha sido un ransomware muy activo durante 2019, sobre todo en el último semestre, y se han detectado numerosas campañas de intento de propagación de *Emotet* por todo el mundo. Una vez el atacante ha obtenido el acceso a la red de la víctima, el *dropper* de *Emotet* analiza el entorno y a partir de ese momento, continúa la infección utilizando para etapas posteriores *Trickbot* o *Ryuk*.[39,40]

Según el objetivo de la campaña, puede ser un **ataque activo** o bien tener como objetivo el **compromiso de un equipo**, para posteriormente vender el acceso en el mercado negro. En ambos casos, el atacante también trata de robar credenciales e infectar más sistemas para obtener un punto de apoyo más sólido en la red de las víctimas. Una vez el atacante ha infectado suficientes sistemas u obtenido credenciales con alto nivel de privilegios (como el administrador de dominio de Windows), despliega el temido ransomware.[41]

Otro ejemplo del impacto que los ataques por ransomware tienen en la sociedad y en la prestación de servicios esenciales se vio en el incidente sufrido por **City Power**, uno de los mayores proveedores de electricidad de Johannesburgo, que provocó que algunos residentes se quedaran sin electricidad.[42]

Ilustración 8. Fuente: Twitter

Este caso dibuja un nuevo escenario, en el que el impacto sobre los sistemas eléctricos de potencia de un país o región no tiene que provenir necesariamente de un ataque dirigido contra sistemas de control industrial.

En la misma línea argumental, es necesario destacar el alto impacto que los ataques por ransomware tienen en el sector sanitario, tanto público como privado.

37 Véase https://csirt.utpl.edu.ec/node/358

38 Véase https://www.thiber.org/wp-content/uploads/2019/12/Numero_15_Diciembre_Ciberataques.pdf

39 Véase https://www.csirtcv.gva.es/sites/all/files/downloads/CSIRT-CV_Informe_Emotet.pdf

40 Véase https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/8730-ccn-cert-al-06-19-campana-troyano-emotet.html

41 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4294-ccn-cert-ia-76-19-medidas-de-actuacion-frente-al-codigo-danino-emotet-1/file.html

42 Véase https://www.tripwire.com/state-of-security/security-data-protection/johannesburg-electricity-provider-falls-victim-to-ransomware-attack/

5.5.2 Súpermercados ilegales

El año 2019 vio cómo se ponía fin a varios de los supermercados ilegales más grandes en Internet, considerados el imperio de la venta de drogas online:[43,44]

Este tipo de plataformas ofrecen venta de drogas ilegales, armas, servicios de *hacking as a service*, documentos falsos, malware, bases de datos de usuarios o tarjetas de crédito robadas, entre otros.[45]

5.5.3 Ataques BEC. Fraude al CEO

Los ataques de ***Business Email Compromise*** (**BEC**), habitualmente conocidos como "Fraude al CEO", son un tipo de ataques en auge en los últimos años, ya que requieren por lo general poco conocimiento técnico e inversión en infraestructura –fundamentalmente el engaño se basa en ingeniería social–, pero pueden llegar a reportar grandes cantidades de dinero a los delincuentes.

Ilustración 11. Fraude al CEO. Europol.

De acuerdo con el *Internet Crime Report* de 2019[46] publicado por el FBI's Internet Crime Complaint Center (IC3), en 2019 se registraron **pérdidas por valor de 1.700 millones de dólares por incidentes de tipo BEC**, lo que supuso el 40 % del total de pérdidas provocadas al negocio del cibercrimen durante el pasado año.

43 Véase https://www.france24.com/fr/20190506-darknet-wall-street-market-arrestation-drogue-arme-internet-supermarche
44 Véase https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces
45 Véase https://dialnet.unirioja.es/descarga/articulo/7046412.pdf
46 Véase https://www.us-cert.gov/ncas/current-activity/2020/02/12/fbi-releases-ic3-2019-internet-crime-report

En dicho informe se indica que se ha detectado un aumento de las técnicas relacionadas con el desvío de pago de la nómina, en las que el departamento encargado de pagar las nóminas en una empresa es engañado para que el pago a un determinado empleado (la víctima suplantada) se redirija a otro número de cuenta. En 2019 ha habido casos sonados de ataques BEC en todos los sectores y localizaciones.

5.5.4 Otras operaciones ciberdelincuenciales

Donde hay dinero online, hay ciberdelincuentes. Y uno de estos sectores es el de los eSports, que, con una audiencia de más de 5 millones de espectadores, mueve solo en España más de 1.5 millones de euros al año. Según un informe de la compañía S2 Grupo, entre los **peligros de los videojuegos online** destacan el robo de nombres y direcciones, tarjetas de crédito y datos biométricos, el acceso a la webcam, micrófono y ubicación en tiempo real del jugador, infecciones por malware, además de otras amenazas como el *ciberbullying*, *grooming, sexting* y *sextorsión*, ciberacoso o acceso a contenidos inapropiados.[47]

También están comenzando a ser habituales los esquemas de blanqueo de capitales aprovechando monedas virtuales y de juegos online, ya que en general son fáciles de transferir y vender sin demasiada supervisión.

5.6 Brechas de datos

Al igual que en años anteriores, las brechas de datos continúan siendo habituales, y el 25% de las mismas estarían relacionadas con el **espionaje**, según asegura el ***Verizon Data Breach Investigation Report (DBIR) 2019***.[48] Dicho informe está basado en el análisis de 41.686 incidentes de seguridad, de los cuales 2013 se confirmaron como brechas de datos. Según el estudio, el 34 % de estas brechas está relacionado con **actores internos**, el 39% con **organizaciones criminales** y en el 23% de los casos las figuras responsables fueron **Estados**.

Según datos ofrecidos por la ***Agencia Española de Protección de Datos***,[49] en España se han analizado, gestionado y evaluado **1.459 notificaciones de brechas de seguridad**. Las notificaciones de brechas de seguridad trasladadas a inspección se han visto incrementadas en casi un 400 %, pasando de 16 en 2018 a 79 en 2019.

En 2019 se han producido importantes brechas de datos en organizaciones de todo el mundo.

Ningún actor está a salvo de esta amenaza.

47 Véase https://s2grupo.es/es/ciberpeligros-videojuegos-online-edad-jugador/
48 Véase https://enterprise.verizon.com/resources/reports/2019/2019-data-breach-investigations-report.pdf
49 Véase https://www.aepd.es/sites/default/files/2020-05/memoria-AEPD-2019.pdf

6 Métodos de ataque

6.1 Actividades de ransomware

El ransomware es uno de los tipos de ciberataque más extendidos y peligrosos, y durante 2019 se pudo ver una escalada de ataques sofisticados de este tipo, dirigidos a múltiples sectores, entre los que se encuentra la Administración Pública.

La mayoría de los ataques dirigidos fueron el resultado de la cooperación entre varias "amenazas", y un ejemplo de ello es la distribución masiva de ***Emotet/Trickbot***[50,51,52] a través de sucesivas campañas de distribución de correos maliciosos. Otro ejemplo análogo sería la distribución masiva de ***Dridex*** como primera fase de la infección, con ***Bitpaymer*** como último estadio de la misma. En puntos sucesivos se detallará el *modus operandi* de estos grupos de cibercriminales, puesto que han sido los que han tenido más impacto en España en el último año.

El método del "alquiler" de botnets no es el único empleado como vector inicial de entrada. Algunos otros son el spear-phishing, servidores RDP expuestos y mal configurados, o incluso el abuso de los proveedores de servicios gestionados (*Managed Service Providers, MSP*) de las compañías para, a través de su compromiso, llegar a sus clientes.

Una vez se ha accedido a la organización víctima, los ciberdelincuentes pasan días explorando la red comprometida para localizar los activos de mayor valor (por ejemplo, los Controladores de Dominio, copias de seguridad, etc.) y distribuir el ransomware de forma que el impacto ocasionado sea el máximo. En este sentido, se habla de ***Human Operated Ransomware***, modelo en el cual el atacante maneja el código dañino combinado con otras herramientas ofensivas para comprometer a la víctima (por ejemplo, explotando vulnerabilidades o aprovechando contraseñas débiles en sistemas expuestos a Internet), obtener persistencia en su infraestructura y, finalmente, exfiltrar y cifrar la información.

Entre los ransomware más activos en 2019, además de los mencionados *Ryuk* o *BitPaymer*, es remarcable citar a *Bad Rabbit*, *Cerber*, *Dharma/CrySiS*, *Phobos*, *GrandCrab*, *Jigsaw*, *Katyusha*, *LockerGoga*, *PewCrypt*, *SamSam*, *STOP Ransomware*, *Revil/Sodinoki*, *GlobeImposter*, *Maze*, *Buran* o *MegaCortex*, entre otros.[53]

50 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4183-ccn-cert-id-23-19-emotet/file.html

51 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4294-ccn-cert-ia-76-19-medidas-de-actuacion-frente-al-codigo-danino-emotet-1/file.html

52 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4294-ccn-cert-ia-76-19-medidas-de-actuacion-frente-al-codigo-danino-emotet-1/file.html

53 Véase https://meterpreter.org/the-10-most-popular-ransomware-in-2019/

El CCN-CERT publicó en 2019 un total de **26 informes de Código Dañino** en su portal,[54] de los que son de especial interés en este punto los relacionados con los principales tipos de ransomware del periodo que abarca el presente informe: ***Sodinokibi*** y ***Ryuk***, publicados a finales de 2019, a los que habría que añadir los informes publicados a principios de 2020 que analizan ***Ransomware Netwalker*** y ***MBR Locker***.

6.1.1 Emotet - Trickbot - Ryuk

El origen del troyano *Emotet* se remonta a 2014, cuyo principal objetivo era el robo de credenciales bancarias. Actualmente su modelo de negocio ha evolucionado y se usa también como servicio de distribución de otros códigos dañinos como el troyano bancario *Trickbot* o el ransomware *Ryuk*.[55,56] Así pues, a finales de 2019 dieron comienzo una serie de campañas en las que estaban involucradas *Emotet-Trickbot-Ryuk*, que tuvieron un gran impacto en empresas y organizaciones de todo el mundo.

En este caso, la vía de infección más común utilizada por los atacantes es el correo electrónico, principalmente mediante un documento ofimático con macros que, al ser habilitadas por el usuario, ejecutarían comandos *powershell* que descargarían ***Emotet***. A su vez, este descargaría *Trickbot*, que es el que tiene las **capacidades** de movimiento lateral y propagación a través de *exploits* como *EternalBlue*, *EternalRomance*, o *EternalChampion*. Por su parte, *Emotet* presenta una gran arquitectura modular con múltiples capacidades: servicio de *malspam* a la lista de contactos de la víctima, servicio de propagación a otros equipos mediante fuerza bruta a partir de diccionarios de contraseñas, servicio DDoS, propagación a otras redes WLAN, etc.

Una vez se ha propagado por la organización, habitualmente *Trickbot* instala una herramienta de control remoto y un proxy para la exfiltración de datos. Los atacantes determinan entonces si la víctima es apta para la infección con *Ryuk,* y en caso afirmativo descargan finalmente el *payload* de *Ryuk*, que busca evadir y deshabilitar sistemas antimalware, adquirir persistencia, eliminar copias de seguridad y finalmente cifrar los archivos. *Ryuk* también está diseñado para que al ingresar en una red LAN valide los segmentos de la misma y compruebe qué dispositivos tienen activa la función *Wake-on-Lan*, lo que le permitiría realizar el encendido de los equipos y posteriormente cifrarlos.

6.1.2 Dridex - BitPaymer

Otra combinación que se ha podido ver estos últimos meses es la formada por el malware *Dridex* y el ransomware *BitPaymer*. En este caso, el grupo de cibercriminales que opera *BitPaymer* suele aprovechar *Dridex* como etapa previa a la activación del ransomware. La vía de entrada habitual suele ser un correo malicioso con enlaces o archivos adjuntos, que en ocasiones van ligados a la descarga de falsas actualizaciones para complementos del navegador.

54 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html

55 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4183-ccn-cert-id-23-19-emotet/file.html

56 Véase https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4294-ccn-cert-ia-76-19-medidas-de-actuacion-frente-al-codigo-danino-emotet-1/file.html

Una vez la víctima cae en el engaño y se ha infectado con *Dridex,* este trata de obtener persistencia en la red y moverse lateralmente haciendo un reconocimiento complejo de la red y recolectando información de la misma, como credenciales del *Directorio Activo*, usuarios, inventario de equipos, etc. En esta fase se suele hacer uso de *PowerShell Empire* como software de post-explotación y de *Mimikatz* para el robo de credenciales.

El **objetivo final** del ataque es **comprometer los Controladores de Dominio para distribuir el ransomware por toda la red**. Se ha detectado que este último paso de la infección suele producirse generalmente durante el fin de semana, de forma que el ransomware tenga tiempo suficiente para propagarse por todos los servidores y retrasar a su vez la posible respuesta al incidente por parte del personal técnico de la organización.

Una vez el ransomware ha sido ejecutado emite la nota de rescate, incluso particularizada para la compañía afectada.

Por último, algunas investigaciones apuntan a la existencia de cierta conexión entre *Emotet, Dridex, Ursnif* y *BitPaymer*.[57]

6.2 Botnets

En el ámbito de las botnets, es interesante comenzar por el informe ***Botnet Threat Report 2019***[58] de Spamhaus Malware Labs, quien señala un **incremento de un 71.5 %** en el número de ***C&C* de botnets identificados** con respecto al año anterior.

Las **principales familias de malware asociadas a botnets**, de acuerdo al informe mencionado, serían las relacionadas con robo de credenciales como *LokiBot, AZORult, Pony* o *Predator*, malware de tipo *Remote Access Tool (RAT)* como *NanoCore, RemocsRAT, Adwind/ Jbifrost, NetWire, NjRAT* o *QuasarRAT* o las ya mencionadas botnets de *Emotet* y *Trickbot*.

Rank	Malware	Note	% change
1	Lokibot	Credential Stealer	+74%
2	AZORult	Credential Stealer	+190%
3	NanoCore	Remote Access Tool (RAT)	+181%
4	Pony	Dropper/Credential Stealer	–23%
5	TrickBot	e-banking trojan	+173%
6	Gozi	e-banking trojan	+76%
7	Emotet	Dropper/Backdoor	–23%
8	RemocsRAT	Remote Access Tool (RAT)	+147%
9	Predator Stealer	Credential Stealer	—
10	Adwind/JBifrost	Remote Access Tool (RAT)	–78%
11	NetWire	Remote Access Tool (RAT)	+98%
12	KPOTStealer	Credential Stealer	—
13	ArkeiStealer	Credential Stealer	+197%
14	NjRAT	Remote Access Tool (RAT)	+290%
15	AgentTesla	KeyLogger/Credential Stealer	–4%
16	QuasarRAT	Remote Access Tool (RAT)	—
17	Dridex	e-banking trojan	—
18	HawkEye	Credential Stealer	—
19	IcedID	e-banking trojan	—
20	CoinMiner	Various crypto currency miners	–8%
—	Others	Other malware families	—

Ilustración 12. Listado de familias de malware asociadas a botnets en 2019.[59]

57 Véase https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/

58 Véase https://www.spamhaustech.com/custom-content/uploads/2020/04/2019-Botnet-Threat-Report-2019-LR.pdf

59 Véase https://www.spamhaustech.com/custom-content/uploads/2020/04/2019-Botnet-Threat-Report-2019-LR.pdf

6.3 Código dañino avanzado

En el caso del código dañino avanzado, la sofisticación y elaboración de nuevas técnicas y amenazas continúa la tendencia de los últimos años, en lo que podría considerarse casi como un proceso de I+D+i por parte de los ciberdelincuentes.

Living off the Land (LotL), una técnica que hace uso de las propias herramientas que tiene una organización para llevar a cabo el ataque, sin necesidad de desarrollar archivos maliciosos desde cero, es un método de ataque cada vez más frecuente. En este caso se deben aprovechar las puertas de entrada ya existentes en los sistemas informáticos, explotando la presencia en los sistemas de herramientas (legítimas) como *PowerShell, WMI* o *PsExec*, entre otras.

Un ejemplo de ello sería el caso de *Petya/NotPetya* visto en Ucrania en 2017, en el que los que los atacantes comprometieron una herramienta de contabilidad –*MeDoc*– a través de una falsa actualización de software. Este método de ataque está muy ligado a los ataques a la cadena de suministro (*Supply Chain Attack*).

También el uso del ***fileless malware*** está en un momento de auge que comienza a ser preocupante. Este se caracteriza por la carga y ejecución del malware principalmente en la memoria del equipo, sin que exista algo como un fichero residente en el disco duro del equipo. Como es evidente, este tipo de mecanismos dificultan la detección y eliminación, principalmente por parte de los antivirus.

Además de hacer uso de las técnicas citadas anteriormente, los actores de amenazas avanzadas continúan mejorando su arsenal de herramientas. A continuación, se citará un **muestreo de piezas de malware de especial interés**, surgidas en 2019 y atribuidas a grupos de Amenazas Persistentes Avanzadas.

Turla, uno de los actores más activos de los últimos años como se ha comentado anteriormente, continúa utilizando malware basado en .NET. Un ejemplo de ello es el lanzamiento de *Topinambour*,[60] un nuevo set de herramientas en .NET que está usando para propagar y descargar *KopiLuwak* a través de la infección de paquetes de instalación para programas de software legítimos, como puede ser VPN.

APT32/OceanLotus, estaría utilizando esteganografía[61] para distribuir sus piezas de malware. Este grupo continúa actualizando su arsenal de herramientas, incluyendo incluso amenazas para los usuarios de Mac.[62]

En noviembre de 2019, la empresa ptsecurity dio a conocer una amenaza llamada ***Twein*** con capacidades de RAT, y que estaría siendo distribuido por TA505, grupo relacionado con el cibercrimen.[63] Entre los módulos de los que hace uso, destaca un *rootkit* que se encargaría de bloquear la carga de *drivers* peligrosos para la amenaza, evitar la modificación de sus persistencias en el registro y monitorizar la creación de nuevos procesos con el fin de inyectar en estos la amenaza escogida, que estaría almacenada en el registro. De esta forma, se obtiene persistencia sin dejar la amenaza en el disco, protegiéndose de las soluciones antimalware tradicionales. El punto más débil de esta amenaza se encuentra en el

60 Véase https://securelist.com/turla-renews-its-arsenal-with-topinambour/91687/
61 Véase https://threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html
62 Véase https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/
63 Véase https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/operation-ta505-part4/

almacenamiento del *driver* en el disco para ser posteriormente cargado, dado que al no estar ofuscado y contener código coincidente con el del conocido *rootkit* de la botnet *Necurs* hace saltar las firmas de los antivirus.

En 2019 saltó a la palestra una muestra de malware perteneciente al *toolset* del grupo ***APT Grey Energy***.[64]. Se trataría de un malware modular y muy complicado de neutralizar, y cuya principal *backdoor* se denomina ***Felixroot***. Entre sus capacidades destacan el movimiento lateral y la escalada de privilegios.

Kaspersky publicó en 2019 un informe[65] sobre un framework altamente sofisticado denominado ***TajMahal*** y orientado al ciberespionaje, que cuenta con más de 80 módulos distintos orientados al robo de ficheros, control remoto, monitorización de la pantalla y el micro, captación de las pulsaciones del teclado, etc. Podría haber estado activo al menos durante los últimos cinco años, y de acuerdo con la información de Kaspersky, solo se habría identificado una víctima, una sede diplomática ubicada en un país de Asia Central. Se desconoce qué grupo o Estado estaría tras este framework.

Por último, señalar que el uso de **canales encubiertos** (*covert channels*) continúa siendo utilizado por los grupos APT para esconder sus comunicaciones o llevar a cabo la exfiltración de datos. La herramienta ***ElectricFish***,[66] atribuida al grupo norcoreano ***Lazarus***, es un ejemplo de ello. Se trata de una utilidad capaz de tunelizar tráfico cifrado entre dos direcciones IP implementando un protocolo personalizado.

6.4 Ataques a sistemas de acceso remoto

El CCN-CERT ha observado que durante 2019 y los primeros meses de 2020 los atacantes emplearon como vectores de entrada en numerosas ocasiones sistemas de acceso remoto a las redes corporativas. Además de campañas globales en las que los atacantes lanzaron escaneos masivos, se ha observado que atacantes más avanzados, de tipo APT, también se han servido de la explotación de este tipo de sistemas para acceder a las redes objetivo.

Ejemplos de esto son la explotación de la vulnerabilidad del sistema de VPN Pulse Secure (**CVE-2019-11539**)[67], de Citrix (**CVE-2019-19781**)[68] o de Microsoft Exchange (**CVE-2020-0688**)[69]. Este tipo de vulnerabilidades se convierten, tras su publicación, en lo que coloquialmente se conoce como **vulnerabilidades de "día 1"**: aquellas que han sido publicadas, pero para las que o bien no existe todavía una solución del fabricante, o bien las potenciales víctimas no han aplicado las actualizaciones y parches necesarios para su mitigación.

Otra forma de acceso mediante este tipo de sistemas es la obtención de credenciales legítimas

64 Véase https://yoroi.company/research/greyenergy-welcome-to-2019/
65 Véase https://securelist.com/project-tajmahal/90240/
66 Véase https://www.us-cert.gov/ncas/analysis-reports/ar19-252b
67 Véase https://nvd.nist.gov/vuln/detail/CVE-2019-11539
68 Véase https://nvd.nist.gov/vuln/detail/CVE-2019-19781
69 Véase https://nvd.nist.gov/vuln/detail/CVE-2020-0688

de acceso remoto a los sistemas de la víctima, tales como **VPN**, sesiones de **escritorio remoto** o **acceso vía web al correo electrónico**. Se ha observado que los grupos de APT las obtienen mediante técnicas de ***phishing*** o, cada vez en mayor medida, mediante la **obtención de credenciales** disponibles en internet y la *darkweb*. Este tipo de ataques son exitosos debido a la mala praxis de reutilización de contraseñas por parte de los usuarios.

6.5 Ataques web

Se apunta a los ataques web como una de las **principales amenazas** detectadas durante 2019. Estos pueden ser divididos en dos bloques principales: los ataques de **Denegación de Servicio Distribuidos** (**DDoS**), y los ataques a **servidores web**, fundamentalmente a través del intento de carga de ficheros que permitan tomar el control del sitio, o de ataques de inyección SQL, con el objetivo de manipular o extraer las bases de datos del servicio.[70]

Tanto los ataques DDoS como los ataques de desfiguración de webs (*Defacements*) se han convertido en las principales amenazas utilizadas por los hacktivistas y otros atacantes cuyo objetivo es dañar la reputación de la víctima o aprovecharse de la caída de los servicios de sus adversarios.

En este caso, los gestores de contenido (CMS) son un gran blanco para los atacantes, ya que su uso está muy extendido. Además, cuentan habitualmente con una gran variedad de módulos[71] que amplían sus funcionalidades pero que, en ocasiones, no están lo suficientemente protegidos ni soportados, convirtiéndose en foco de potenciales puertas de entrada para los atacantes. Los CMS más atacados son Drupal, Wordpress y Joomla, cuyo compromiso se realiza con fines variados, entre los que se encuentran tomar el control del sitio web para formar botnets para minar criptodivisas, pivotar a otros sitios de la red interna o incluso la formación de infraestructuras de *C&C*, como es el caso del *APT Turla*.[72]

Basándose en resultados de más de 10.000 escaneos, Acunetix publicó en 2019 un informe sobre las principales tendencias detectadas[73] en cuanto a explotación de vulnerabilidades de tipo web. Las vulnerabilidades *Cross-site Scripting (XSS),* las librerías vulnerables de *JavaScript* y los fallos de seguridad en Wordpress representaban un 30 % de los resultados obtenidos por Acunetix en su estudio, reforzando el argumento de que las aplicaciones web son un vector de entrada viable y que supone poco esfuerzo para los atacantes.

Las técnicas para explotar vulnerabilidades web se sofistican con el paso de los años, existiendo incluso rankings anuales de las más impactantes como el que publica *Portswigger*.[74]

70 Véase https://www.csirtcv.gva.es/sites/all/files/downloads/CSIRT-CV_Informe_Actividad_2019.pdf

71 Véase https://www.csirtcv.gva.es/es/noticias/cuidado-con-los-plugins-y-temas-gratuitos-de-wordpress-algunos-podr %C3 %ADan-contener-malware

72 Véase https://securelist.lat/ksb-2019-review-of-the-year/89932/

73 Véase https://www.acunetix.com/blog/articles/acunetix-web-application-vulnerability-report-2019/

74 Véase https://portswigger.net/research/top-10-web-hacking-techniques-of-2019

6.6 Ingeniería Social

El uso de técnicas de ingeniería social sigue siendo uno de los **principales vectores de ataque** utilizados. Los incidentes de seguridad relacionados con esta están en auge: oleadas de llamadas de falsos técnicos de empresas que intentan hacerse con el control del equipo de la víctima, "*Fraude al CEO*", *spear-phishing* basados en información pública o robada sobre las víctimas, correos con falsas facturas o multas, correos que extorsionan con supuestos vídeos privados, etc.

En un escenario en el que el mercado negro de datos está en plena expansión debido al incremento del valor comercial de los datos personales, las fugas de información de datos financieros (tarjetas de pago, cuentas de servicios de pago online), credenciales de acceso a diferentes servicios online, direcciones de correo electrónico, perfiles de usuarios/ identidades, es información muy valiosa para los ingenieros sociales. En este sentido, en 2019 tuvo lugar una importante filtración de este tipo de datos con más de 2.200 millones de registros,[75] que contenían entre otros datos direcciones de correo, nombres de usuarios y contraseñas.

Pasando al funcionamiento de estos ataques, en estos el correo electrónico destaca con claridad como el canal más utilizado, a través del que se realizan campañas de *phishing* que, mediante la suplantación de servicios o personas, incitan al receptor del correo electrónico a descargar un fichero adjunto, pulsar en un enlace, facilitar determinada información o incluso a realizar una acción concreta; por ejemplo: una transferencia bancaria.

Las campañas masivas de **phishing** que buscan comprometer al mayor número de víctimas posible suelen ser más sencillas de detectar al utilizar métodos de suplantación de identidad poco sofisticados. Suelen estar relacionadas con el cibercrimen por el hecho de desplegar ransomware o troyanos bancarios, pero también cabe la posibilidad de que algunas de ellas tengan como objetivo la obtención de financiación para la ejecución de otro tipo de ataque por parte de actores diferentes.

Sin embargo, el escenario es diferente en el caso de ***spear-phishing***, o ataques dirigidos contra personas u organizaciones específicas, en los que su mayor preparación y sofisticación los hace más difíciles de detectar. En este caso, la suplantación de servicios o personas con quien la víctima del ataque es muy probable que haya mantenido comunicaciones anteriores otorga una alta dosis de credibilidad al falso correo electrónico, incrementando las posibilidades de éxito.

La preparación de este tipo de ataques conlleva un estudio previo de la víctima, para obtener información que permita dar credibilidad al engaño. Para ello, los atacantes hacen uso de técnicas de obtención de información en fuentes abiertas (**OSINT**) y técnicas de acercamiento por redes sociales mediante perfiles falsos.

Aunque como se ha indicado el uso del correo electrónico es el mecanismo habitual, estos métodos de ataque pueden hacer uso de otros canales de comunicación como el SMS, en cuyo caso se trata de ***smishing***, así como aplicaciones de mensajería instantánea o redes sociales.

Otro método a tener en cuenta es el engaño mediante llamadas telefónicas (***vishing***), a través de la que se pretende engañar a un empleado con el objetivo de que ejecute una acción para la cual tiene permisos, sin necesidad de explotar ninguna vulnerabilidad tecnológica, pero que

75 Véase https://www.welivesecurity.com/la-es/2019/02/04/millones-direcciones-correo-contrasenas-filtradas-collection/

puede suponer un grave riesgo para la organización. Por ejemplo, una orden para la realización de una transferencia bancaria, la publicación de determinada información, el arranque o parada de un proceso, etc.

También se emplean técnicas de ingeniería social para conseguir que una persona, de manera inconsciente, introduzca *malware* o incluso provoque un daño físico directo sobre un sistema mediante la conexión de dispositivos USB previamente comprometidos. Esta técnica es conocida como ***baiting***.

Por tanto, a pesar de seguir siendo el método más utilizado, es importante tener en cuenta que los ataques de ingeniería social pueden utilizar diferentes mecanismos, incluso combinados entre sí para una mayor eficacia.

Desde un enfoque distinto, y como hemos visto en apartados anteriores, las técnicas de ingeniería social también adquieren especial relevancia en las campañas de desinformación; la generación de noticias falsas y su difusión mediante redes sociales y aplicaciones de mensajería "explotan" determinados sesgos cognitivos de las personas, como son los sesgos de confirmación o membresía (pertenencia a grupo) para conseguir su objetivo.

6.7 Ataques contra la cadena de suministro

Los **ataques de la cadena de suministro**, también llamado ataques de cadena de valor o de terceros, constituyen una amenaza emergente y se prevé que sigan en aumento en próximos años.

Existen **diferentes tipos de ataques** de la cadena de suministro, como el de herramientas de creación de software comprometidas, código robado (firma de certificados o aplicaciones malintencionadas firmadas con la identidad de la empresa de desarrollo), malware preinstalado en dispositivos, código especializado comprometido que se envía a componentes de hardware o firmware, etc.[76]

A diferencia de otro tipo de ataques, los dirigidos a las cadenas de suministro permiten evadir ciertos controles de prevención y detección al comprometer directamente a los proveedores externos, socios o clientes. Las regulaciones de riesgo de terceros aún están en sus inicios, y la mayoría de las empresas no controlan ni validan el software o hardware que utilizan, ni a sus propios proveedores o socios desde el punto de vista de la ciberseguridad. Los atacantes, sobre todo los grupos más avanzados, aprovechan estas debilidades para perpetrar sus intrusiones en las redes objetivo valiéndose de que los proveedores o entidades asociadas disponen de algún tipo de interconexión o acceso a la red objetivo. Mención especial tienen los **riesgos de seguridad de los proveedores en la nube**, en línea con la tendencia al alza de trasladar a la nube desde los centros de datos hasta las aplicaciones, exponiendo a las empresas y fabricantes a riesgos de terceros.

76 Véase https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/supply-chain-malware

Dentro del ámbito industrial, este tipo de ataques pueden desarrollarse en varios momentos del ciclo de vida de los sistemas, teniendo en cuenta la alta especialización existente. Inevitablemente, esto resulta en una alta dependencia de las organizaciones respecto de fabricantes e integradores, desde el mismo diseño e implantación de proyectos de automatización o supervisión.

Existen riesgos asociados al propio desarrollo de despliegues SCADA en los laboratorios o talleres de fabricantes de automatización, que se extienden a las operaciones de mantenimiento, no siendo infrecuente, por ejemplo, que las copias de seguridad de las lógicas en ejecución sean realizadas y custodiadas por terceras empresas. En el ámbito industrial es muy frecuente la existencia de accesos remotos para estas terceras empresas, en ocasiones no controlados por el propietario o explotador de los sistemas.

Una de las formas más comunes de ataque a la cadena de suministro es el secuestro de actualizaciones de software.

6.8 Ataques contra sistemas ciberfísicos

Como ya se ha comentado, en este documento se ha adoptado una visión global que parte del reconocimiento de que las organizaciones o infraestructuras industriales dependen para su operación tanto de **sistemas de información TI**, en el sentido tradicional del término, como de sistemas de control industrial o SCADA, comúnmente agrupados bajo el término **OT**.

La convergencia tecnológica ha hecho que la separación entre ambas tecnologías y conocimiento del personal encargado de su diseño, construcción y operación ya no sean tan claras como hasta hace algunos años. Por esta razón, se ha considerado como incidente de ciberseguridad industrial todo aquel que afecte a la continuidad de los procesos físicos de una compañía o infraestructura, independientemente de la naturaleza de los sistemas tecnológicos objeto del ataque.

Existen aspectos tecnológicos específicos en sistemas ciberfísicos —considerados a efectos de este documento como aquellos que permiten el control o la supervisión de un proceso físico por medio de sistemas de procesamiento y sus comunicaciones asociadas— que merecen ser analizados de forma independiente.

En este ámbito, el hecho más notable de 2019 fue el descubrimiento del interés de los atacantes por afectar a la operación de

sistemas ciberfísicos por medio de campañas de ransomware. En diciembre la compañía Dragos detectó y analizó una muestra de ransomware al que bautizó como ***EKANS***. El análisis reveló que cuando el malware se ejecuta en un sistema, antes de proceder al cifrado de información, detiene una serie de procesos listados en su código.

Entre ellos, además de procesos asociados a aplicaciones de propósito general (como bases de datos) se encuentran procesos específicos de sistemas SCADA, asociados a proveedores como GE y Honeywell, entre otros. Si en el sistema objetivo se encontrasen esos procesos en ejecución, el resultado de esta acción sería una pérdida de capacidad de supervisión por parte del operador (*loss-of-view*).

El posible impacto, por tanto, es limitado, ya que, al no dirigirse contra componentes de los sistemas de control automático, instrumentación o actuadores no tendría un impacto inmediato sobre procesos físicos, si bien sí podría forzar al operador a modificar el estado del sistema realizando paradas controladas si la pérdida de capacidad de supervisión así lo aconsejase.

En cualquier caso, EKANS muestra el interés de las organizaciones criminales en afectar a la operación de compañías industriales e infraestructuras, algo sospechado hace tiempo, pero verificado por primera vez. Lo limitado del alcance de EKANS no debe disminuir la alerta, toda vez que la evolución lógica de este tipo de herramientas se dirigirá previsiblemente hacia la afección de los niveles de control automático y campo, enviando órdenes directas o produciendo cambios de configuración en controladores, instrumentación o actuadores. Esta posibilidad es algo que ya se ha desarrollado como prueba de concepto[77] y que podría materializarse en un futuro próximo.

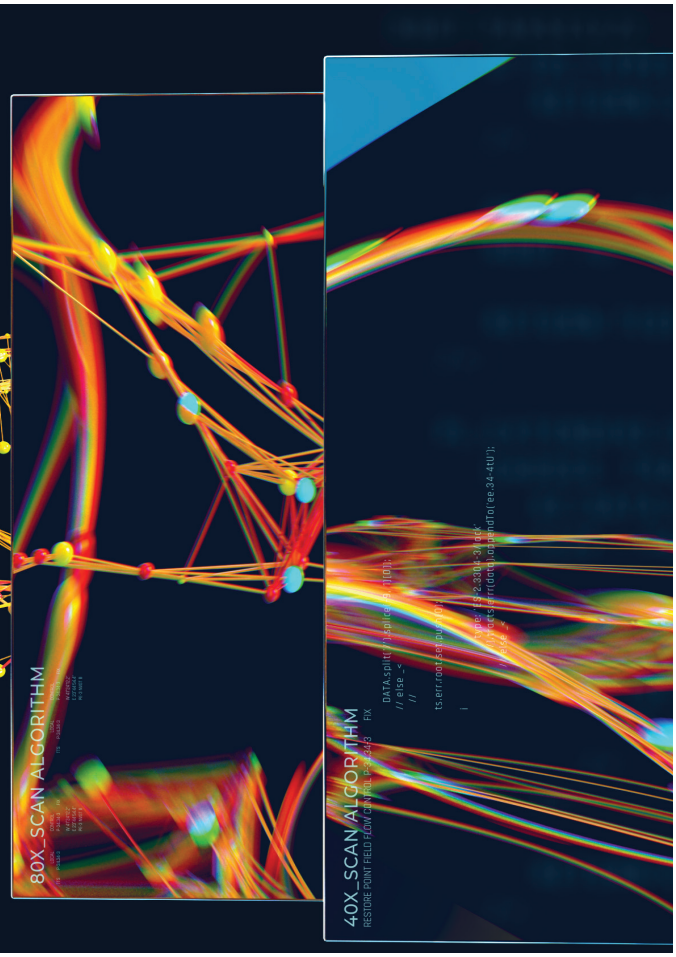
En lo relativo a dispositivos y sistemas IoT, cabe destacar que 3 años después de la aparición de *Mirai* siguen registrándose ataques por este malware y variantes del mismo.[78] Esto se debe principalmente a los diseños inseguros de estos dispositivos y a la dificultad de su parcheo o, cuando este es posible, a la falta de gestión realizada tanto por consumidores como por organizaciones de todo tipo, lo que hace que sigan siendo vulnerables frente a este tipo de ataques.

En un escenario con una convergencia IT/OT creciente y una tendencia al alza del número de dispositivos IoT en un ámbito que ya se cuenta por miles de millones, estos ejemplos son solo una pequeña muestra del tipo de amenazas que veremos en años venideros, tanto en el ámbito de los sistemas ciberfísicos como de IoT, y que requerirán un gran esfuerzo por parte de todos los actores implicados para hacerles frente.

77 Véase https://www.tripwire.com/state-of-security/latest-security-news/new-proof-concept-ransomware-can-target-plcs-industrial-sites/

78 Véase https://www.computerweekly.com/news/252470509/Mirai-descendants-dominate-IoT-threat-environment

7 Tendencias 2020



Obviamente, no es posible hablar de tendencias 2020 sin hacer referencia a la situación provocada por la **pandemia de la COVID-19** y las medidas de confinamiento adoptadas. Estas han propiciado un **enorme despliegue de entornos tecnológicos de teletrabajo** para salvaguardar la continuidad de actividades y negocios; desde el punto de vista de ciberseguridad, esta situación conllevará nuevas situaciones previsibles.

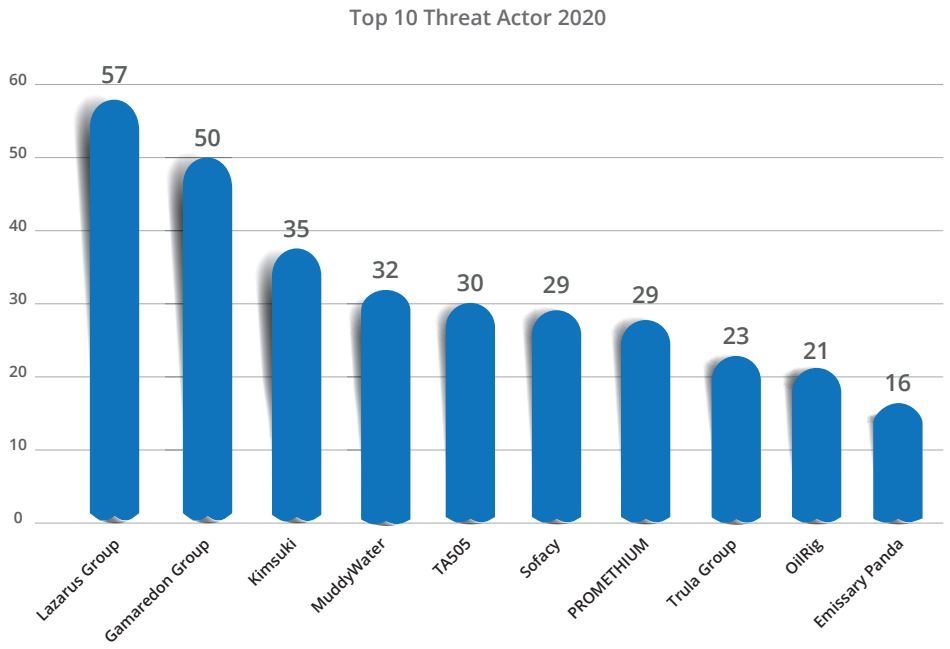
La forma tan apresurada en la que muchas organizaciones han puesto en marcha el teletrabajo ha provocado que **no se hayan evaluado de forma adecuada los riesgos asociados**, ni las soluciones ni los protocolos de actuación, incorporando numerosas deficiencias de seguridad que los ciberatacantes tratarán de explotar en 2020.

El aumento del uso de soluciones en la nube, conexiones VPN, servicios de escritorio remoto virtual (VDI), redes de confianza cero y gestión de identidades, servicios y tecnologías para el acceso remoto, uso de herramientas colaborativas, aplicaciones de videoconferencia, etc. generará que los ataques a estos entornos, en especial a los sistemas públicamente expuestos, sigan creciendo.

Igualmente, se incrementarán las vulnerabilidades detectadas sobre los mismos, ya que diferentes actores han puesto el foco en la seguridad de estos dispositivos. Ya se ha visto durante la primera mitad de 2020 esta tendencia (vulnerabilidades en sistemas como Zoom, tecnologías VPN, etc.) y previsiblemente se consolidará e incrementará durante todo el año. En la misma línea se enmarca el ataque a los servicios en nube (almacenamiento, ofimática, etc.), servicios que también han visto un incremento en su uso durante la pandemia.

También ligado a la situación actual con un fuerte incremento del teletrabajo, es previsible que los **ataques y vulnerabilidades relacionados con redes domésticas o dispositivos personales** se incrementen, con el objetivo de acceder a la infraestructura de la organización del empleado y, una vez dentro de ella, establecer persistencia.

Una de las actividades que más aumentará derivada de esta situación será sin duda el **ciberespionaje**. Las entidades han aumentado su superficie de exposición y por tanto **los actores patrocinados por Estados dispondrán de nuevas vías de entrada** a sus objetivos y es lógico pensar que aumentarán su actividad. Esta tendencia ya se refleja en los informes publicados por los principales vendedores de productos y servicios de ciberseguridad como se refleja en la siguiente imagen:



Fuente: Elaboración propia con información de REYES (CCN-CERT)

Con el objetivo de **facilitar el seguimiento de personas infectadas por la COVID-19**, se están estudiando en Europa diferentes propuestas de monitorización automática de proximidad de personas, como el *Pan-European Privacy-Preserving Proximity Tracing*,[79] en las que juegan un papel determinante las redes de telefonía, los terminales móviles, el bluetooth y la criptografía.

Por último, en el marco de la pandemia, es de esperar que los **ataques a farmacéuticas, laboratorios de investigación dedicados al COVID-19** o víctimas relacionadas con el sector aumenten con diferentes objetivos: ciberespionaje, extorsión, destrucción de información o incluso operaciones de influencia hacia la opinión pública.

En el ámbito industrial, el final de 2019 y principio de 2020 ha visto un incremento de ataques publicados con impacto sobre la producción u operación de compañías industriales. Es previsible que esta tendencia se incremente a lo largo del resto de 2020, especialmente teniendo en cuenta la concurrencia de circunstancias como el fin del soporte de Windows 7 y las dificultades de parcheo de los sistemas industriales que lo emplean.

79 Véase https://www.pepp-pt.org/

También aquí es previsible que la crisis del COVID-19 sea un factor importante a tener en cuenta, derivado del riesgo generado por las necesidades de trabajo remoto de técnicos de mantenimiento, operación, y terceras empresas como consecuencia del estallido. Desde el primer trimestre de 2020 se ha producido un incremento de los accesos remotos a través del perímetro a sistemas de control industrial.

También en **entornos industriales**, y como hemos visto a lo largo de este documento, la creciente integración tecnológica y organizativa entre tecnologías IT y OT hace previsible un incremento en los casos de afectación a sistemas industriales haciendo uso de ransomware no especialmente dirigido contra estos sistemas.

Por otra parte, la detección por vez primera de un **ransomware con capacidades específicas dirigidas a componentes de sistemas ICS** (*EKANS*) demuestra el interés de los cibercriminales por extender de forma deliberada este tipo de ataques a compañías que operan procesos industriales, una nueva estrategia en la que la presión para realizar el pago no solo se basa en un daño económico sino en el potencial impacto sobre vidas humanas al afectar a infraestructuras críticas.

El *Primer estudio sectorial sobre el estado de la Ciberseguridad en la industria española*,[80] publicado por el Centro de Ciberseguridad Industrial (CCI), permite estimar la magnitud de la amenaza del ransomware en la industria y sectores críticos españoles. Según este informe, basado en encuestas a los responsables de las organizaciones industriales participantes, el 44 % no tiene instalados antivirus, el 47 % no realiza copias de seguridad y un 49 % no dispone de una adecuada gestión de incidentes.

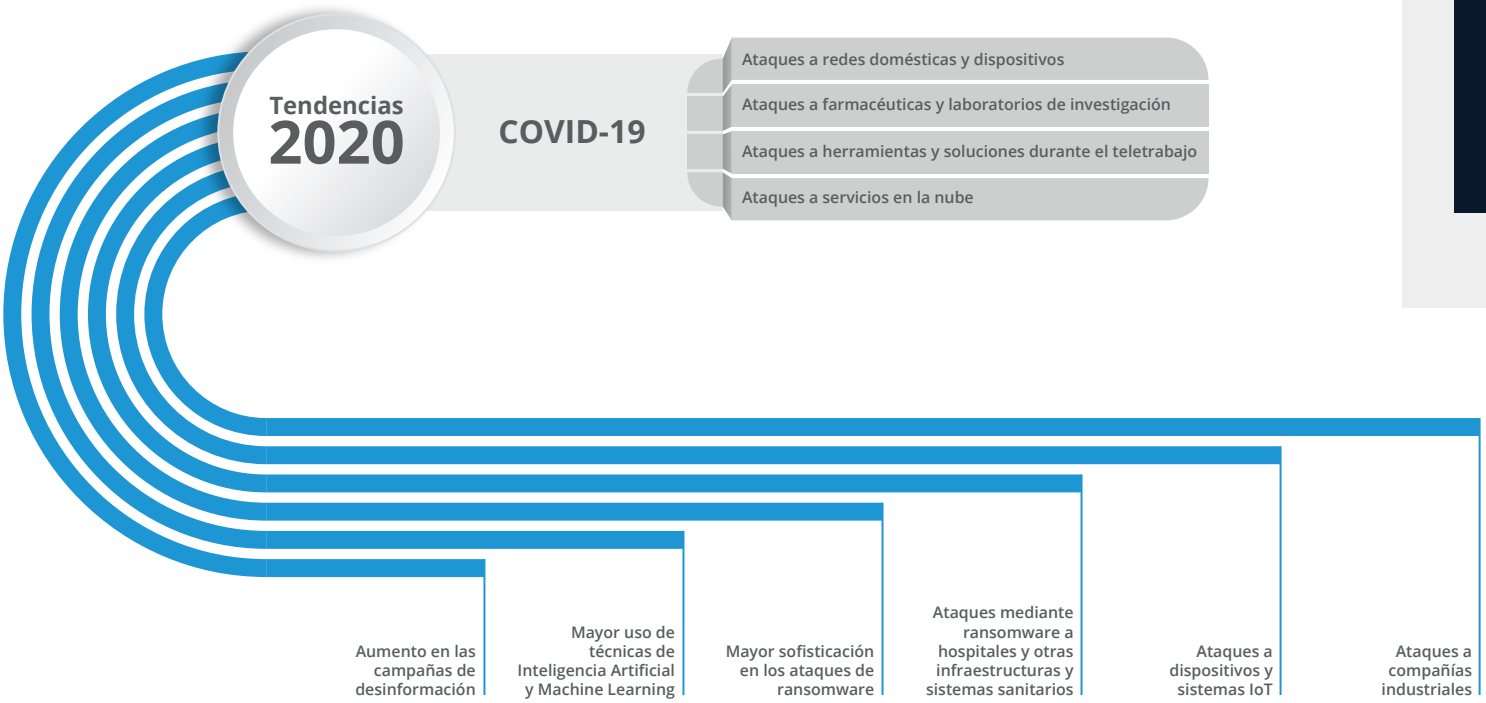
Los escenarios considerados para afectar a un servicio esencial como es el suministro eléctrico a la población pasaban por ataques dirigidos contra las tecnologías OT que permiten su operación: sistemas de gestión de energía (EMS), centros de control, equipamiento en subestaciones, centrales de generación, etc.

80 Véase https://www.cci-es.org/informes-y-analisis-estategicos

De forma más general, este tipo de casos tenderá a aumentar al mismo paso que la integración tecnológica y funcional en las organizaciones, lo que va a exigir una aproximación convergente en los conceptos de ciberseguridad IT y OT, hasta ahora considerados como ámbitos adyacentes pero separados.

En lo relativo a **dispositivos y sistemas IoT**, con un número de dispositivos conectados a Internet que según algunas estimaciones a finales de 2019 era superior a 9.500 millones[81], es previsible que se mantenga la tendencia observada en el aumento del número de ataques, especialmente teniendo en cuenta la penetración creciente en el mercado, especialmente doméstico, de este tipo de productos.

Esta tendencia se ve agravada por la dificultad a que se enfrentan las organizaciones para gestionar un parque creciente de dispositivos heterogéneos con gran diversidad de propósitos y necesidades de conectividad.



En cualquier caso, se debe tener en cuenta que en la actualidad los dispositivos tradicionalmente considerados como IoT constituyen en la actualidad un subconjunto dentro de un amplio espectro de equipamiento que incluye sistemas típicamente industriales a los que se añaden interfaces para su gestión remota (grupos electrógenos, equipos de climatización, etc.), sistemas de seguridad física y hasta equipamiento médico.

Este último elemento sirve para introducir otra de las tendencias detectadas durante 2019, año en el que se constató un incremento notabilísimo de **ataques mediante ransomware a hospitales y otras infraestructuras y servicios sanitarios**.

81 Véase https://iot-analytics.com/iot-2019-in-review/

Un análisis realizado por una compañía aseguradora ha cifrado en un 350 % este incremento durante 2019.[82].[83] Es previsible que esta tendencia se mantenga o acelere durante 2020, y de hecho, ya se han registrado ataques contra organizaciones y laboratorios implicados en la lucha contra el coronavirus.[84] Hay que tener en cuenta que, si bien hasta el momento estos ataques han tenido un impacto relativo sobre las operaciones al afectar a sistemas de información (historias médicas, citas, etc.), es previsible un impacto potencial todavía mayor si el malware se extiende desde las redes de propósito TI hasta los segmentos en los que se encuentran otros sistemas imprescindibles para la operación de un hospital, como son el sistema SCADA de gestión del edificio (BMS, *Building Management Systems*), los sistemas de generación de energía de emergencia, los equipos de diagnóstico por imagen o tratamiento, de almacenamiento y distribución de gases medicinales, etc. Estos sistemas comparten un buen número de factores de riesgo de ciberseguridad con los sistemas industriales tradicionales empleados en otros sectores como la manufactura, etc., por lo que deberán ser objeto de especial atención durante 2020.

También **en relación a los ataques de ransomware, es necesario señalar una tendencia, ya consolidada, como es la sofisticación de dichos ataques**. Como ya se ha indicado, los actores están abordando acciones completamente dirigidas en las que se actúa con un modus operandi similar al de las APT: tras un reconocimiento inicial, se compromete a la víctima –generalmente a través de sistemas vulnerables expuestos a Internet–, y una vez el atacante controla la infraestructura, persiste en ella y se mueve lateralmente adquiriendo y exfiltrando información.

En este modelo de ataque, el ransomware no es más que el punto final, en el que se cifra la información y se solicita un rescate, pero se aplican otras amenazas como la publicación –que en ocasiones se materializa– de información sensible robada a la víctima. De esta forma, se reduce drásticamente la utilidad de salvaguardas como las copias de seguridad, y se incrementan las posibilidades de obtener un rescate.

La escena pública es previsible que sea otro de los ámbitos en los que veamos una **consolidación de las campañas de desinformación** en el ciberespacio, aumentando tanto en cantidad como en impacto en la opinión pública. Como hemos referenciado en este informe, cada vez son más los actores involucrados en operaciones de influencia, y factores como el uso masivo de redes sociales o la cantidad de información disponible sobre cualquier asunto, imposible de procesar por una persona y que acaba creando el efecto denominado *infoxicación*, hacen que la efectividad de dichas operaciones se multiplique.

En este ámbito cabe destacar el uso de tecnologías *Deep Fake*, por ejemplo, para ejecutar ataques de phishing mucho más sofisticados, simulando la voz de directivos de la organización o su forma de redactar, para hacer más creíbles los cebos, elemento que liga de forma directa con el ámbito de la inteligencia artificial.

82 Véase https://info.corvusinsurance.com/hubfs/Security %20Report %202.2 %20- %20Health %20Care %20.pdf

83 Véase https://www.elmundo.es/ciencia-y-salud/salud/2020/01/21/5e274be1fdddffcf088b462d.html

84 Véase https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/

Para acabar, no es posible olvidar a la que será probablemente la tecnología que más influencia tendrá en la ciberseguridad en los próximos años, tanto en los procesos de defensa como en los de ataque: la **Inteligencia Artificial**.

Es prácticamente seguro que los atacantes ya están utilizando técnicas de inteligencia artificial y *Machine Learning* para ejecutar sus ataques, utilizando técnicas como *self-learning automated malware* para mejorar sus ataques de *ransomware*, ingeniería social o *phishing*. Un atacante puede lanzar *malware* que recoja información para determinar por qué un ataque no ha tenido éxito y utilizar esta información para lanzar un segundo ataque mejor adaptado a la organización objetivo. Esta tecnología, a pesar de ser avanzada, está disponible para los atacantes, tanto en herramientas comerciales como de Open Source.

Asimismo, esta tecnología está sirviendo para desarrollar nuevas técnicas como el ***Targeted Attack Analysis***, con la que se ponen a prueba las organizaciones objetivo, estudiando su respuesta ante determinados estímulos y definiendo un perfil de funcionamiento de la organización desde el punto de vista de su defensa frente a ataques, lo que les permite adaptar y refinar esos ataques a las especificidades de la víctima.

En el lado de las organizaciones, la IA también tiene un papel importante en los mecanismos de defensa, que veremos cómo se incrementa en el futuro. Por un lado, un uso avanzado es el del **UEBA** (***User and Entity Advanced Behavioral Analysis***), en el que se monitoriza el comportamiento de los usuarios y los equipos dentro de una infraestructura, a partir de la que establecer una línea base de funcionamiento normal, y detectar desviaciones de esta producidas por comportamientos anómalos o intrusiones desde el exterior.

También el ***Adaptive Cybersecurity*** permite adaptar las herramientas de uso general a las peculiaridades de cada organización, de manera continua, mediante la utilización de técnicas de *Machine Learning*. Una de las principales ventajas de la utilización de dichas técnicas en estos casos es que facilita una respuesta en tiempo real, independientemente de la disponibilidad de los técnicos especialistas.

Aun así, la IA está todavía lejos de poder considerarse un sustituto de los expertos humanos, y sería un error considerarla como tal. Incluso teniendo en cuenta las ventajas y potencia que aporta, su utilización puede generar una sensación de falsa seguridad, que empeora si su *entrenamiento* no se realiza de la manera adecuada.

En cualquier caso, la utilización de inteligencia artificial en el ámbito de la ciberseguridad se debe considerar como una especie de carrera de armamento, en la que ambos bandos intentan disponer de los avances tecnológicos más significativos. Ignorar que los actores hostiles están dispuestos a utilizar estas tecnologías en su beneficio es una arriesgada decisión de consecuencias desastrosas.

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es