
SEPTIEMBRE 2022
CIBER_
AMENAZAS
Y TENDENCIAS
EDICIÓN 2022
CCN-CERT IA-24/22
ANÁLISIS DE LAS CIBERAMENAZAS
NACIONALES E INTERNACIONALES,
DE SU EVOLUCIÓN Y TENDENCIAS
FUTURAS.
CCN
centro criptológico nacional
ccn-cert
centro criptológico nacional

Edita:

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

CONTENIDO

1. RESUMEN EJECUTIVO.

Un año más, **el devenir de la pandemia del COVID-19 ha marcado la agenda global.** Si bien es cierto que la sociedad ha ido adaptándose a una situación de nueva normalidad, 2021 ha vuelto a ser un año repleto de incertidumbre debido a las sucesivas olas de contagios. **Lo cual no ha sido diferente en el ámbito de la ciberseguridad.**

2021 ha sido el año en el que más incidentes críticos se han gestionado desde el CCN-CERT. A esto además se añade que en líneas generales los incidentes han demostrado una mayor sofisticación, especialmente a través de vulnerabilidades de ejecución remota de código (RCE, del inglés remote code execution) de tipo día cero, pero también mediante el compromiso de la cadena de suministro, tal y como apuntaba la tendencia en 2020.

La utilización del COVID-19 como gancho en 2021 para realizar ataques contra sistemas TIC ha disminuido respecto al año anterior. En este sentido, cabe recordar que durante la primera parte de la pandemia el uso de la temática COVID-19 fue mayoritariamente utilizada en campañas phishing del cibercrimen con un claro fin económico. No fue hasta mediados del año 2020 y durante el 2021 que su uso, entre otras temáticas más dirigidas, también fue observado en grupos APT relacionados con el ciberespionaje entre estados, entre cuyos objetivos también se encontraban conocer los avances en el desarrollo de nuevas vacunas contra la enfermedad.

A lo largo del presente informe se enumerarán estas y otras de las acciones más relevantes del año 2021 en el ámbito de las ciberamenazas, junto a sus tácticas, técnicas y procedimientos, y que irán acompañadas del contexto geopolítico y social en que se desarrollaron. Finalmente, con la información extraída del análisis del año, se facilitarán y comentarán potenciales tendencias para el 2022.

2. SOBRE 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 y actualizado a través del RD 311/2022, de 4 de mayo.

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.

3. 2021: ADAPTACIÓN A UN MODELO SEMIPRESENCIAL.

Si 2020 quedó caracterizado como el año que el mundo sufrió un golpe que paralizó la sociedad, 2021 quedará definido como el año en que el mundo se adaptó a una nueva normalidad. Las sucesivas olas de contagios, así como la disparidad de impacto entre zonas geográficas, plagaban de incertidumbre la realización de cualquier actividad de índole pública, con impacto tanto en las políticas de asistencia a las oficinas como en la celebración de eventos sociales o deportivos.

Un modelo mixto

En esta línea, las organizaciones han seguido en su camino de adaptación de la digitalización de su infraestructura para facilitar el teletrabajo a los continuos cambios de políticas de restricciones a raíz de la COVID-19.

A pesar de que en 2021 el número de empleados utilizando teletrabajo disminuyó respecto lo ocurrido en 2020, según el INE[1], en el primer semestre de 2021 el número de establecimientos que permitían el teletrabajo ha sido del 45,5%, con una media del 35,3%, números inferiores a los existentes durante el estado de alarma, que alcanzaron el 51,4% y 46,7%, respectivamente. Valores que llegaban al 66,8% y 59,5% en Otros Servicios, entre los cuales se incluyen los servicios TI.

Es decir, el teletrabajo se ha convertido en una opción de metodología de trabajo accesible para muchos.

Los cambios en las restricciones sociales han llevado a que sea necesaria la constante adaptación de la asistencia de personal o el teletrabajo remoto. Por ello, durante 2021 las organizaciones han ido adaptando y mejorando los servicios para el trabajo colaborativo, de cara a mejorar la eficiencia de un nuevo modelo que, en muchos casos, ha llegado para quedarse.

Sin embargo, como cualquier migración digital, dicha adaptación ha traído consigo la exposición de nuevos servicios, especialmente para el acceso remoto que, consecuentemente, ha abierto la puerta a nuevos vectores de infección, lo que supone un riesgo adicional.

El año de las vulnerabilidades.

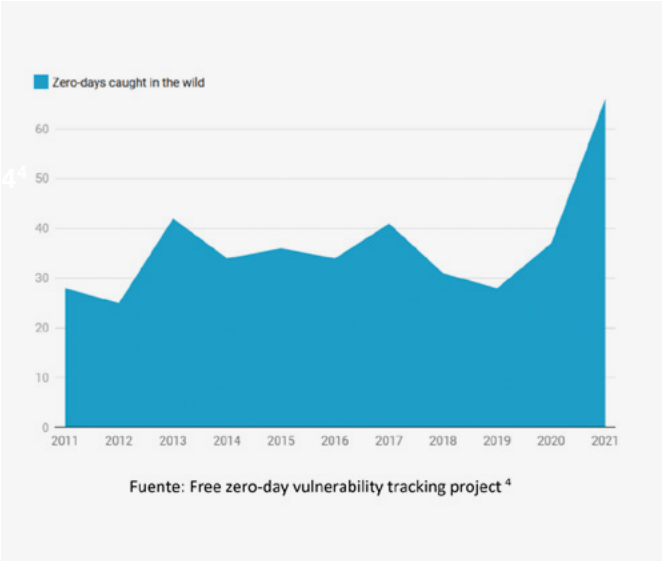
Tal y como se pudo observar desde el primer trimestre de 2021, el término vulnerabilidad ha sido una constante a lo largo de ese año. A raíz de la exposición de los servicios de acceso remoto, los atacantes han focalizado sus esfuerzos en la consecución de

1 - https://www.ine.es/daco/daco42/ice/ice_mod_covid_0121.pdf

una vía de entrada a las organizaciones a través de las oportunidades que ha brindado el teletrabajo, también para ellos. No solo ha sido un año récord en cuanto al número de vulnerabilidades, sino que también han sido de mayor criticidad.

En 2021 se publicaron 28.695 vulnerabilidades, lo que supone un incremento del 23,31% respecto a las 23.269 de 2020[2].

De todas ellas, **4.100 eran explotables de manera remota**, entre las que destacan las vinculadas a productos de amplio alcance que permitían el acceso inicial a gran escala para el atacante en las organizaciones afectadas. Como ejemplo de este tipo están las que han afectado a **Microsoft Exchange**, pasando por **VMware,** ProxyLogony Log4j, que permitían la ejecución remota de código en servicios expuestos y, por ende, la posibilidad de acceso a la organización, lo que demuestra que los principales actores han focalizado el trabajo en la consecución del acceso inicial a través de las oportunidades brindadas por el teletrabajo[3]. Del mismo modo es más que notable la **proliferación de vulnerabilidades de día cero** a lo largo de 2021, año en que **se detectaron un total de 66, alrededor del doble que el año anterior.**



Fuente: Free zero-day vulnerability tracking project [4]

2 - https://www.securityweek.com/over-28000-vulnerabilities-disclosed-2021-report
3 - https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/
4 - https://www.zero-day.cz

El Ransomware sigue al alza

La creciente tendencia de los ataques de **ransomware** que estaba teniendo lugar a finales de 2020 ha continuado durante 2021, siendo **la tipología de ataque que más ha aumentado durante el año**, habiendo tenido uno de los ataques con mayor impacto jamás perpetrados, el ciberataque contra la estadounidense Colonial Pipeline. Dicha organización transporta el 45% de la gasolina, diésel y combustible para aviones consumido por la costa este del país. Este ataque fue llevado a cabo por el grupo Darkside y paralizó la actividad del sistema de oleoductos durante seis días, además del robo de más de 100Gb de información[5].

Además, los grupos de ransomware han comenzado a utilizar diferentes técnicas de extorsión para forzar el pago por parte de sus víctimas, bien a través de la amenaza de filtración de la información robada o llamando por teléfono directamente a las sedes de la organización. A esto se añade la monetización en foros de la Dark Web de la información ex filtrada tras el compromiso de la organización víctima.

Subida del valor de la criptomoneda

Otro de los factores que tuvo cierta incidencia en el escenario de la ciberseguridad ha sido el incremento muy sustancial del precio de ciertas criptodivisas en 2021. Bitcoin superó en dos ocasiones el récord de valor jamás adquirido (ATH, en inglés all time high) y Ethereum también alcanzó valores récord durante el año.

Dicho incremento hizo que el número de amenazas asociadas al minado de criptomoneda sufriera un aumento respecto a los valores manejados anteriormente, pues la rentabilidad del minado de criptomoneda volvió a subir.

5 - https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline?t=1652084748128

En la misma línea, ante la entrada en el mercado de nuevos usuarios menos experimentados, también han proliferado las campañas de robo de **carteras de criptomonedas.**

Los ataques al sector de las criptodivisas se encuentran en un punto bajo actualmente, debido al desplome a principios de marzo de 2022 del valor de las criptomonedas y su posterior estancamiento, de media, por debajo de la mitad de sus ATH tras el inicio de la invasión de Ucrania por parte de Rusia.

Golpe a Emotet

Un golpe muy importante al cibercrimen tuvo lugar en **2021**, pues el año comenzó con la **intervención de la infraestructura de Emotet a finales de enero**, en una operación colaborativa entre las autoridades de Países Bajos, Alemania, Estados Unidos Reino Unido, Francia, Lituania, Canadá y Ucrania, supervisada y coordinada por la Europol[6].

El malware, descubierto en 2014, nació con objetivo de robo de información financiera, pero evolucionó los años posteriores hasta convertirse en un servicio para otras bandas cibercriminales mediante el compromiso inicial de entidades a través de spear phishings, en los que Emotet actuaba como un loader de otras amenazas, entre las que destacan Trickbot y Ryuk[7].

El día 29 de enero de 2021 se llevó a cabo la operación que permitió intervenir la infraestructura de Emotet, a través de la cual se procedió a la desinstalación global del malware tras realizar una modificación en su código el Departamento de Justicia de los Estados Unidos en colaboración con el FBI.

A pesar de ello, **a finales de 2021 se encontraron evidencias de nuevas campañas de Emotet**, recuperando gran parte de su impacto, especialmente en España.

Retorno de los eventos sociales

Los eventos sociales o deportivos siempre están en el punto de mira diferentes agentes de la amenaza para perpetrar ciberataques, especialmente como vector de entrada. Sin embargo, las restricciones sociales debidas a la COVID-19 han supuesto una disminución drástica en el número de estos eventos, lo que se ha traducido en la disminución del número de ciberataques de esta índole.

Un ejemplo lo tenemos con los Juegos Olímpicos de Tokio, pospuestos de 2020 a 2021. A pesar de encontrar un número significativo de ataques con dicha temática, el volumen es mucho menor respecto al de los Juegos Olímpicos de Londres. El número de intentos de ataque durante los Juegos Olímpicos de Tokio fue de unos 600 millones, contra los 2.300 millones que se detectaron en los Juegos de Londres[8] [9].

6 - https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation
7 - https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
8 - https://www.trendmicro.com/en_us/research/21/h/tokyo-olympics-leveraged-in-cybercrime-attack.html
9 - https://www.aa.com.tr/en/asia-pacific/about-450m-cyberattacks-prevented-during-tokyo-olympics/2383969

4. AGENTES DE LA AMENAZA.

Durante 2021 los principales agentes de la amenaza han sido los grupos de ciberespionaje vinculados a Estado y los grupos dedicados al cibercrimen. Por su parte, el hacktivismo ha tomado una nueva dirección a través de la plataforma de mensajería instantánea Telegram.

4.1 Actores Estado

Los ataques más sofisticados, así como de mayor duración en el tiempo, están relacionados con acciones de ciberespionaje, llevadas a cabo principalmente por grupos asociados a intereses de ciertos Estados. Dichos ciberataques tienen como fin obtener información sensible que proporcione ventaja estratégica y que ayude a alcanzar los intereses y objetivos de un Estado.

Pese a que tradicionalmente estos actores solo llevaban a cabo campañas de ciberespionaje y/o ciberguerra, durante el año 2021 se ha observado como algunos de ellos han llevado a cabo también campañas de cibercrimen, cuya motivación ha sido puramente monetaria y en las que se ha observado:

- El uso de información sensible robada como método de extorsión.
- El minado de criptomoneda.
- El uso de ransomware:
    - APT27 estuvo llevando a cabo el despliegue de ransomware en diversas organizaciones entre finales de 2020 y principios de 2021, especialmente contra compañías dedicadas al desarrollo de videojuegos.[10]

En cualquier caso, estas acciones han sido realizadas de manera puntual, presumiblemente para una autofinanciación esporádica, dado que los principales objetivos de los ataques siguen siendo las organizaciones gubernamentales, de defensa, ONGs o Think Tanks.

10 - https://shared-public-reports.s3-eu-west-1.amazonaws.com/APT27+turns+to+ransomware.pdf

Actividad de grupos APT durante 2021

En cuanto a la actividad realizada por los grupos APT, podemos señalar a **APT29** (NOBELIUM) como **una de las amenazas con mayor número de campañas realizadas durante el año**, de igual modo que **Lazarus**, que también ha llevado a cabo una amplia diversidad de acciones. Aunque, tal vez, el grupo con **mayor impacto de 2021 ha podido ser HAFNIUM a través de la explotación de una vulnerabilidad de día cero de Microsoft Exchange** entre marzo y abril[11].

11 Se detalla en el apartado 5.1

Principales campañas de grupos APT detectadas en 2021
APT35/Charming Kitten – Campañas de phishing para obtener credenciales de servicios como Gmail, Yahoo! y Outlook de individuos pertenecientes a organizaciones del Golfo Pérsico, Europa y los Estados Unidos. Esta campaña se caracterizaba por redirigir a sus víctimas desde sitios legítimos asociados a Google hacia sitios maliciosos controlados por el atacante.[12]
APT-C-36 - Campañas principalmente contra el gobierno colombiano y contra otras organizaciones privadas principalmente asociadas a la energía y el sector de la metalurgia. Destaca el uso de packers como AutoIT o Agent Tesla y herramientas como njRAT, AsyncRAT y Remcos.[13]
CedarAPT - Campañas contra compañías de Israel, Egipto, Jordania, Arabia Saudita, Emiratos Árabes Unidos y Estados Unidos. Se caracterizan por el uso de Caterpillar Web Shell y Explosive RAT,dos herramientas que solo han sido visto usadas por este grupo.[16] [15]
Lazarus - Campañas contra analistas de ciberseguridad. Se destaca el uso de redes sociales como Twitter o LinkedIn para engañar a los analistas, así como el uso de vulnerabilidades de día 0, entre las que se encuentran algunas relacionadas con Chrome.[16] [17]
HAFNIUM18 - Agresiva campaña de explotación masiva de vulnerabilidades de Exchange y la subida de la webshell ChinaChopper[19]en marzo.
Mustang Panda - Campañas contra compañías de telecomunicación en Europa, Estados Unidos y el sudeste de Asia. Se destaca el uso de CobaltStrike en estas campañas y la ausencia del backdoor PlugX,ampliamente utilizado en otras campañas de este actor.[20]
TA456 (Tortoiseshell) - Campañas contra trabajadores de empresas del sector defensa y aeroespacial de Estados Unidos, Inglaterra y otros países de Europa. Se destaca el uso de LEMPO y del protocolo SMTPS para exfiltrar información. [21]
Charming Kitten - Campañas contra profesionales del sector médico estadounidense e israelí especializados en investigación de genética, neurología y oncología. Esta campaña se caracteriza por el robo de credenciales de cuentas de OneDrive, el sistema de almacenamiento en la nube de Microsoft.

12 - https://www.cybersecurity-help.cz/blog/1870.html
13 - https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/
14 - https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf
15 - https://www.cybersecurity-help.cz/blog/1899.html
16 - https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/
17 - https://www.cybersecurity-help.cz/blog/2025.html
18 - https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
19 - https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
20 - https://www.cybersecurity-help.cz/blog/1993.html
21 - https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

Nobelium (APT29) – Campañas contra proveedores de servicios TIC de diferentes compañías. Se destaca el uso del backdoor SUNBURSTy los malware TEARDROP, GoldMax, Sibot, y GoldFinder.
The Dukes (APT29) – Durante el segundo trimestre de 2021, serie de ataques contra organizaciones internacionales, Think Tanks y diplomáticos europeos de más de 12 países diferentes, principalmente a través del uso de Cobalt Strike.
A41APT - Campaña que tiene como objetivo compañías de Japón. Destaca por su abuso de VPN como vector inicial y el uso de herramientas como DESLoader, FYAntiLoader y xRAT.[22]
LightBasin UNC1945 - Campaña contra el sector de telecomunicaciones, como en la mayoría de sus anteriores campañas. Se destaca el uso del backdoor TinyShell,que es enrutado a través de puntos de acceso GPRS con el uso de otras herramientas como CordScan, SIGTRANslator, Fast Reverse Proxy, ProxyChains, etc.[23]
Lazarus - Campaña que tiene como objetivo el sector de defensa. Se destaca el uso del malware ThreatNeedle,directamente asociado con el grupo Lazarus,así como herramientas legitimas como PSCP (PuTTY Secure Copy Client) y una copia modificada de TightVNC.
LazyScripter - Campaña contra entidades importantes en Europa. Destaca por el uso de su propi loader llamado KOCTOPUS,así como el uso de RATs comerciales como Quasar, Luminosity Link, Remcos, njRAT, Adwind y RMS.[24]
Harvester group - Campaña contra los sectores de telecomunicaciones, gubernamentales y de TI del sudeste de Asia. Destaca el uso de la infraestructura de Microsoft para la conexión con su servidor de mando y control (C2)y de herramientas como Cobalt Strike o Metasploit.[25]
Turla - En enero de 2021 se encontró actividad relacionada con Turla en diferentes Ministerios de Asuntos Exteriores de países europeos. Cabe destacar la utilización de OneDrive. como servidor de mando y control.
Lazarus - Durante el primer trimestre de 2021, Lazarus llevó a cabo una campaña de phishing a través de la plataforma Linkedin,donde ofrecían trabajo a personal vinculado con la organización que querían comprometer. Cabe destacar la utilización de binarios firmados digitalmente en fases de pos explotación.
Gamaredon - Campaña que ha tenido como principal objetivo diferentes organizaciones gubernamentales de Ucrania.
FamousSparrow - Campaña de espionaje contra gobiernos, organizaciones gubernamentales y hoteles a través de la explotación de la vulnerabilidad ProxyLogon, además del uso de una variante de Mimikatz, ProcDump, Nbtscan y el backdoorSparrowDoor.[26]
OilRig - Se han encontrado evidencias de ataques de este grupo contra diferentes organizaciones ubicadas en Israel.

22 - http://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_en.pdf

23 - https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/

24 - https://lab52.io/blog/very-very-lazy-lazyscripters-scripts-double-compromise-in-a-single-obfuscation/25https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia

25 - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia

26 - https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/

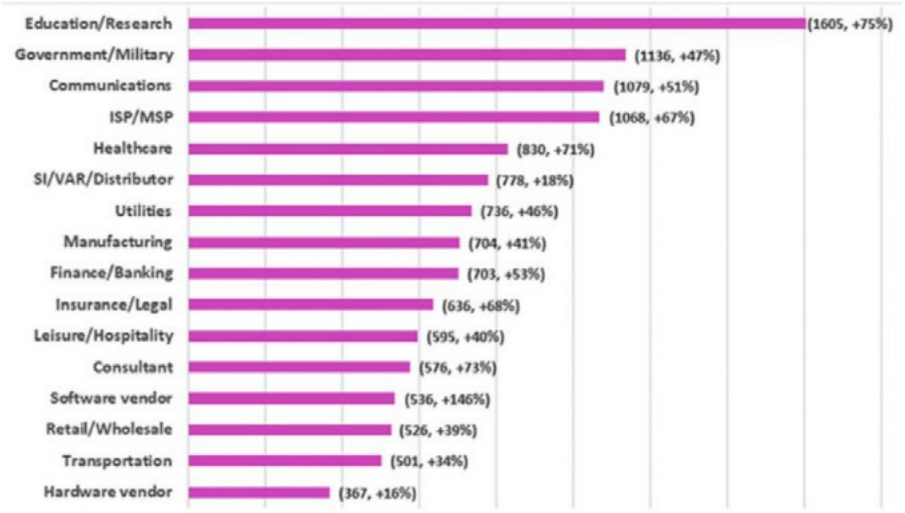
4.2 Ciberdelincuencia

Durante el año 2021 se ha podido determinar cómo la **tendencia al alza del ransomware** observada a finales de 2020 se ha mantenido a lo largo de 2021. **Los grupos han aumentado el número de operaciones, así como en su sofisticación.**

En 2021 los principales objetivos de los ataques han sido organizaciones dedicadas a la investigación, así como para la defensa nacional o gobiernos. Datos que suponen un 75% y un 47% más que en 2020 respectivamente, y que permiten dilucidar un interés por la vacuna de la COVID-19 y sus posibles tratamientos.

Los ataques por industria se han realizado del siguiente modo:

Promedio de ataques semanales por organización por sector (2021)

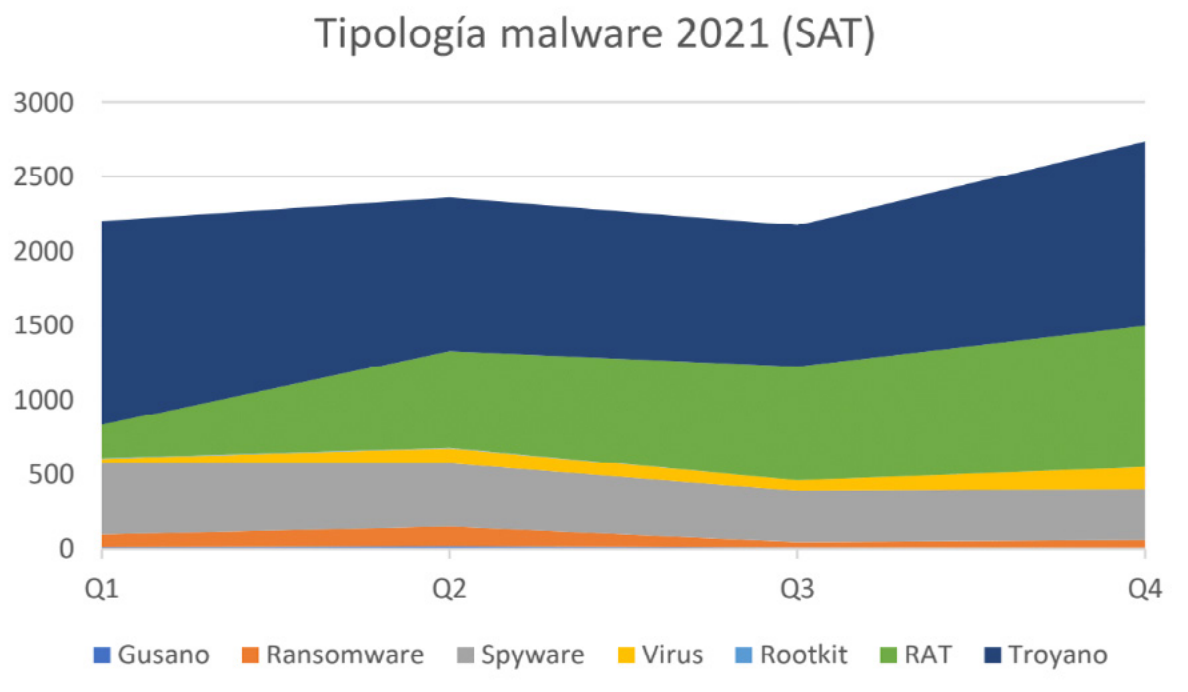


Tipología de código dañino

De las **estadísticas** extraídas del número de notificaciones realizadas a través **del servicio de alerta temprana (SAT) del CCN-CERT**, podemos distribuir la **tipología del malware empleado durante el año 2021** de la siguiente manera:

Tipología de malware	Q1 2021	Q2 2021	Q3 2021	Q4 2021
Gusano	10	17	8	5
Ransomware	87	131	37	53
Spyware	474	424	343	340
Virus	33	102	70	149
Rootkit	3	3	0	0
RAT	224	651	768	665
Troyano	1370	1034	949	1238

Tal y como se puede observar, destaca el uso de troyanos, RATs y spyware, con una ligera tendencia al alza a lo largo del año del total de notificaciones realizadas.

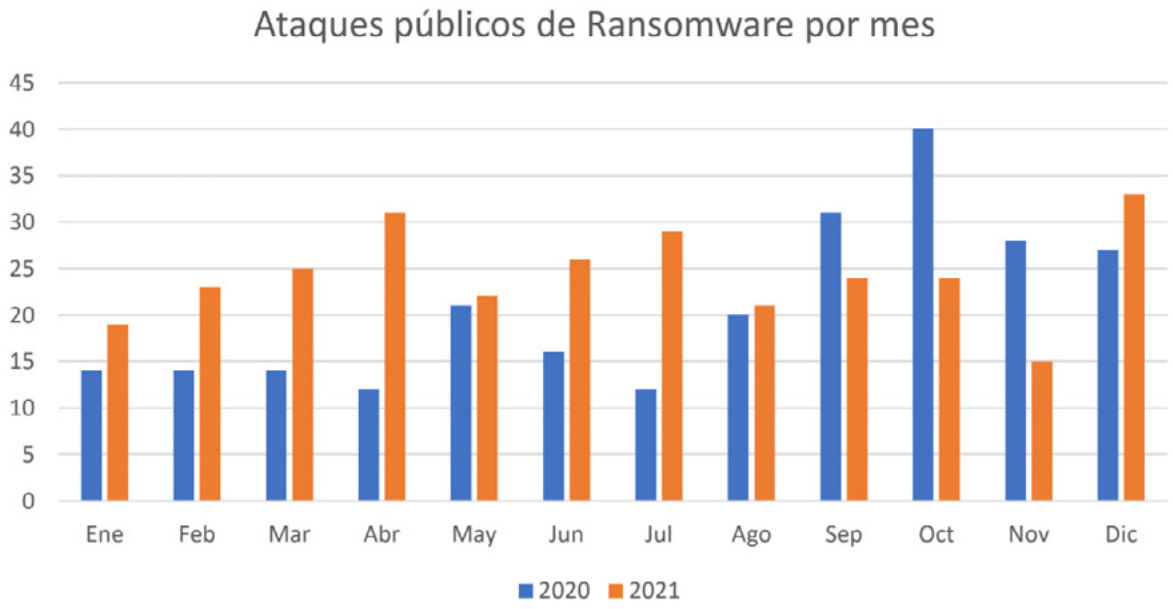


Ransomware

No cabe duda de que la principal preocupación del año por parte de los equipos de seguridad de las organizaciones ha sido la constante amenaza de los grupos de ransomware

Durante 2021, el número de ataques ha seguido la tendencia de finales de 2020, la cual tuvo un incremento muy importante respecto al primer semestre. Sin embargo, el segundo semestre es algo inferior en cuanto a incidentes, probablemente vinculado al desmantelamiento de Emotet.

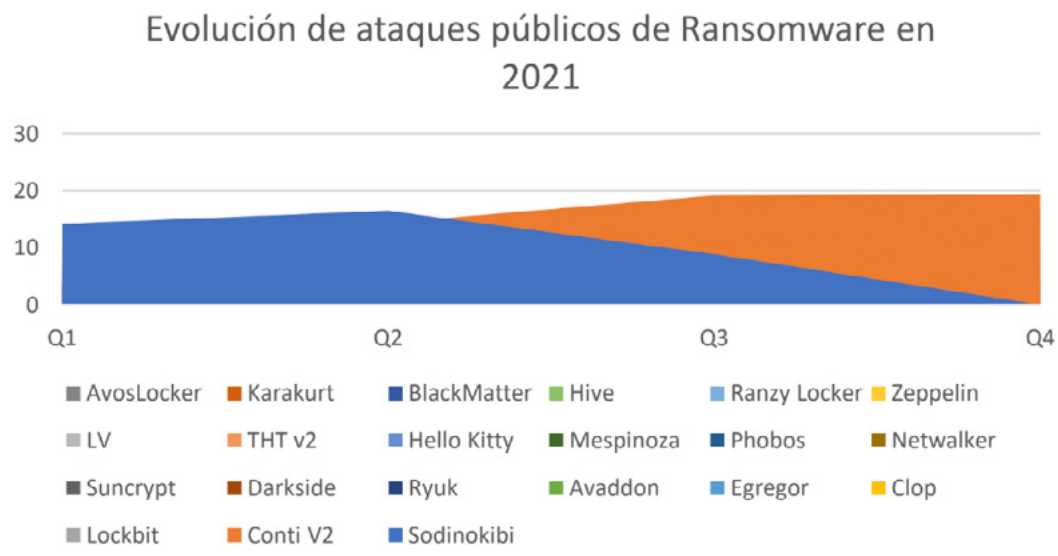
A pesar de ello, los números son muy similares entre trimestres, habiendo una variación de apenas un 1%.



Si analizamos la distribución de ataques por grupo, podemos encontrar que, a excepción de Conti, el resto de grupos operan en intervalos de tiempos determinados.[27] [28]

Mientras que Sodinokibi o Ryuk llevaron a cabo compromisos durante el primer semestre de 2021, Mespinoza sólo tiene durante el Q3. [29] [30]

27 - https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
28 - https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
29 - https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
30 - https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021



Colonial Pipeline

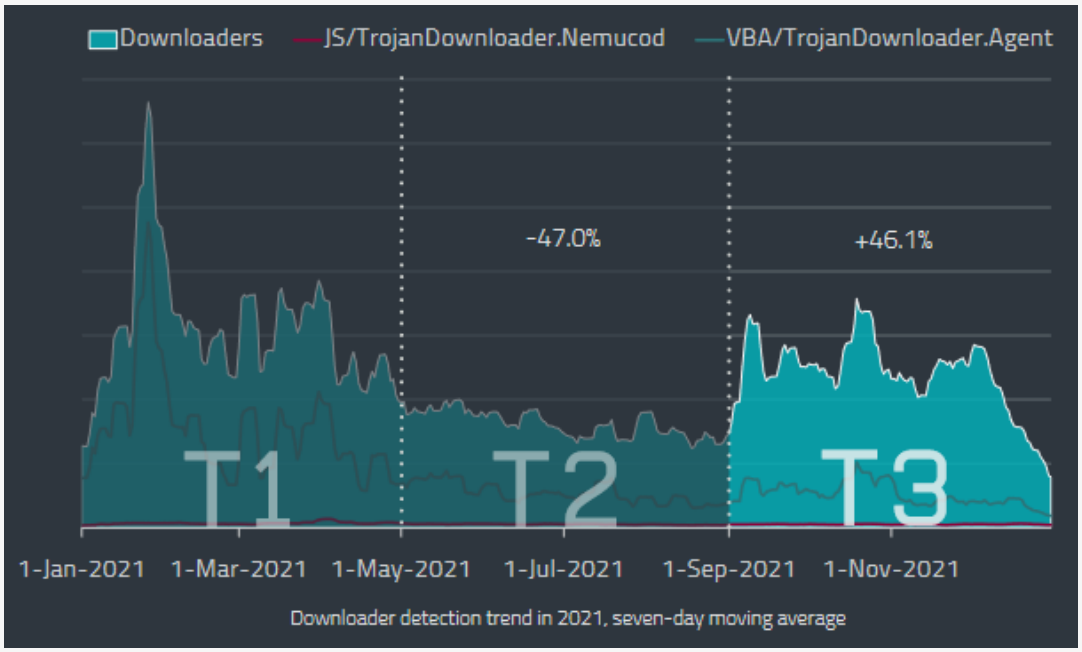
Uno de los casos más destacados de este año fue el ciberataque al sistema de oleoductos más grande de EEUU, operado por la empresa Colonial Pipeline[31]. Este sistema abarca más de 8.500 km de tuberías, y transporta el 45% del combustible consumido en la costa este del país. Este ataque provocó el cierre del oleoducto durante cerca de 6 días, lo cual impactó en el precio de combustibles, así como el desabastecimiento intermitente de diésel, gasolina y combustible de avión. El ataque fue llevado a cabo, presumiblemente, por el grupo criminal DarkSide, el cual consiguió su objetivo al obtener los 4,4 millones de dólares que pedían de rescate por parte de la empresa[32]. Es interesante hacer notar que el ransomware no se propagó a los sistemas OT implicados en la operación de la infraestructura, pero al carecer de planes de contingencia para estos sistemas, la compañía decidió desconectarlos por temor a que se viesen afectados. No obstante, la industria petrolera no ha sido la única que ha sufrido el impacto del ransomware. Durante este año 2021, han sido publicados numerosos incidentes en otros sectores, como son los ataques a la empresa cárnica estadounidense JBS[33]; la empresa holandesa de transporte alimentario Bakker Logistek[34]; empresas alimenticias como las estadounidenses Molson Coors[35] o Schreiber Foods[36]o la cervecera española Damm[37]o a una planta de tratamiento de agua en Florida, EEUU[38]. Todas estas empresas tuvieron que parar todas sus operaciones debido a infecciones

31 - https://www.welivesecurity.com/la-es/2021/05/11/ataque-ransomware-compania-oleoducto-colonia-pipeline-afecta-suministro-combustible-estados-unidos/
32 - https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html
33 - https://www.businessinsider.es/suministro-global-carne-podria-ver-afectado-ciberataque-875919
34 - https://threatpost.com/ransomware-cheese-shortages-netherlands/165407/
35 - https://www.bleepingcomputer.com/news/security/molson-coors-brewing-operations-disrupted-by-cyberattack/
36 - https://eu.wisfarmer.com/story/news/2021/10/26/schreiber-foods-hit-cyberattack-plants-closed/8558252002/
37 - https://blog.elhacker.net/2021/11/un-ataque-de-ransomware-obliga-detener-cerveza-damm.html
38 - https://www.darkreading.com/attacks-breaches/florida-water-utility-hack-highlights-risks-to-critical-infrastructure

por ransomware. La industria manufacturera ha sido la gran perjudicada durante este año, siendo Conti y Lockbit 2.0 los dos grupos cibercriminales que han realizado el mayor porcentaje de los ataques producidos[39].

Downloaders

Las tendencias en cuanto al malware de tipo downloader se ven afectadas por la caída y resurgimiento de Emotet, pues tras la desinstalación, el número total de infecciones por Emotet cayó casi un 50%. Sin embargo, un nuevo auge comenzó a lo largo del tercer trimestre, recuperando cuotas previas a la desinstalación del malware Emotet. De hecho, a mediados de noviembre una nueva campaña de Emotet tuvo lugar, siguiéndole una segunda oleada entre el 6 y el 10 de diciembre, afectando especialmente a Japón, España e Italia. Es de relevancia comentar que España ha sido el país del mundo más afectado por downloaders durante el tercer trimestre de 2021 con una cuota del 9,4%.[40]

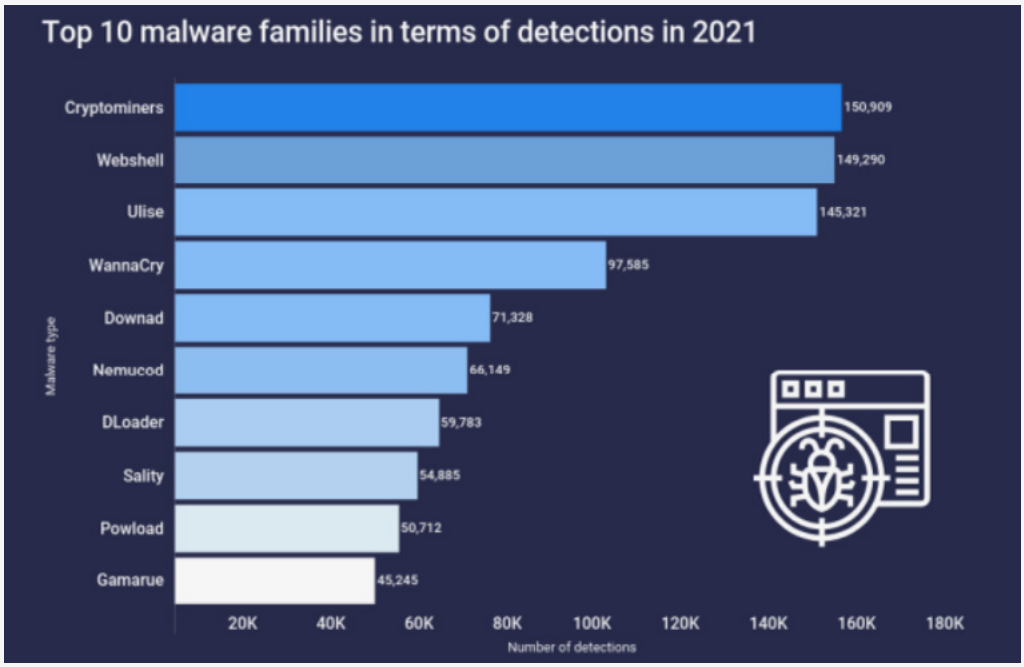


La otra familia de malware de tipo downloader cuyo impacto ha sido muy relevante durante el año han sido las macros dañinas a través de código VBA (Visual Basic for Applications).

39 - https://www.dragos.com/blog/dragos-2021-industrial-cybersecurity-year-in-review-summary/
40 - https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf

Criptohijacking

Tal y como se ha comentado al comienzo del informe, el incremento del valor de ciertas criptomonedas en 2021 creó una tendencia muy importante en la utilización de este tipo de amenaza durante el pasado año, convirtiéndose en la tipología de malware más extendido del año.[41]



Esto se debe, fundamentalmente, a que en 2021 el Bitcoin superó en dos ocasiones el valor máximo (ATH) alcanzado por la criptomoneda. Mientras que el 1 de enero de 2021 la moneda contaba con un valor de 26.500 €, el 12 de marzo alcanzó los 51.260€ y el 12 de noviembre los 56.280€.[42]

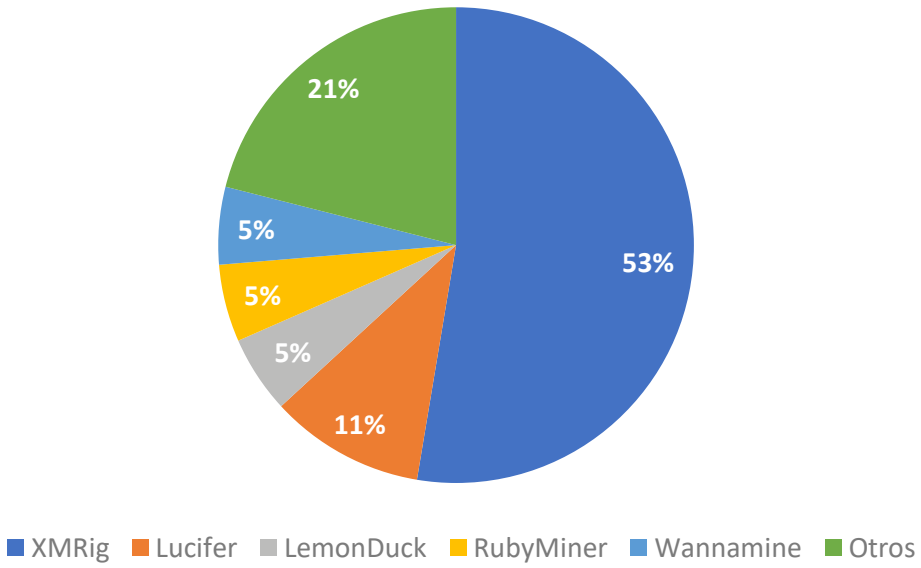
41 - https://financialit.net/news/security/cryptominers-were-most-common-malware-family-2021
42 - https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-price-history/

Estas subidas del valor de la criptomoneda, así como el incremento durante el mes de abril de Ethreum y la multiplicación un 1000% del valor del Dodgecoin a raíz de un tuit de Elon Musk, demuestra la volatilidad de las criptodivisas y la enorme influencia de los personajes públicos en su valor.

También es de relevancia comentar el aumento en la utilización de Monero como criptomoneda tras el cifrado que tuvo lugar a Colonial Pipeline por parte del grupo DarkSide. El FBI participó en el pago de alrededor de 75 Bitcoins, las fuerzas de seguridad pudieron seguir el rastro y pudieron confiscar gran parte del pago.

Por hechos como este, grupos como REvil sólo han aceptado Monero como forma de pago en 2021, pues ésta fue lanzada como proyecto open source con el objetivo de dotar de una capa de anonimización e indistinguibilidad que pudiera evitar acciones como las llevadas a cabo por el FBI con DarkSide. [43] [44]

En cuanto a las familias de criptomineros, se detectó un incremento en la utilización de XMRig, llegando a una cuota de más del 50% sobre el malware de minado. En otro orden de magnitud están Lucifer, LemonDuck y RubyMiner.



Otra de las amenazas vinculadas con el sector de las cripto y que apuntan a una tendencia creciente es el robo de carteras de criptomonedas o activos de tipo NFT, tal y como se observó en la campaña perpetrada por Babadeda a través de Discord.[45] No obstante, el crecimiento de dicho tipo de ataques se vio frenado tras la caída del valor de las principales criptomonedas en el primer trimestre de 2022.

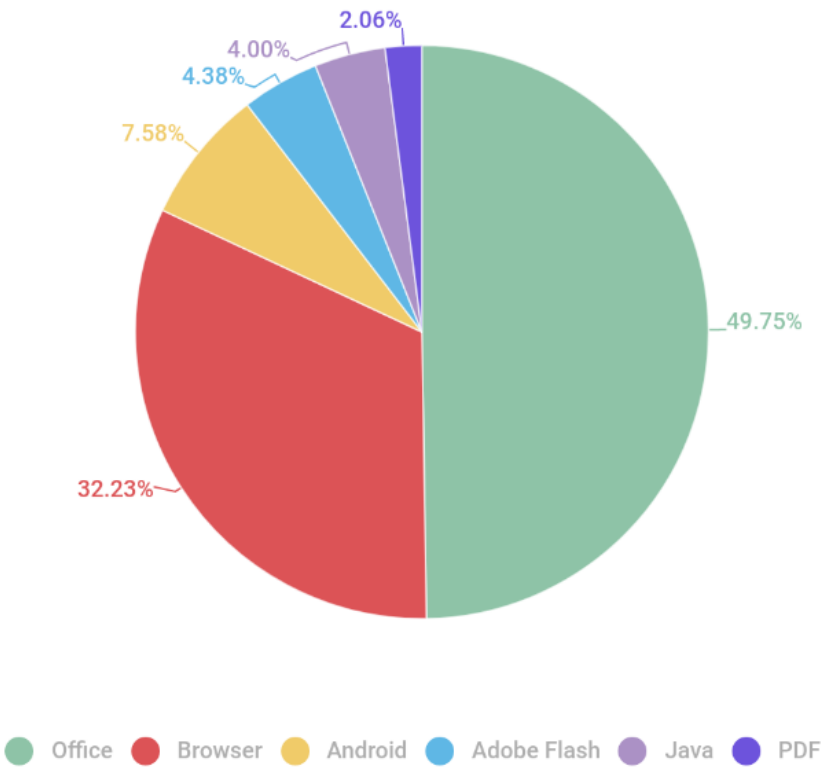
43 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport
44 - https://techmonitor.ai/technology/cybersecurity/cryptojacking
45 - https://www.bleepingcomputer.com/news/security/discord-malware-campaign-targets-crypto-and-nft- communities/

Exploits

En cuanto a los exploits utilizados en 2021, **el framework de Microsoft Office sigue siendo el objetivo principal**, especialmente debido a su amplia utilización en los entornos laborales. Los exploits más utilizados fueron los ya reportados en 2017 y 2018 (CVE-2017-11882, CVE-2018-0802, CVE-2017-8570 y CVE- 2017-0199).[46]

En segundo lugar, se encuentra la explotación de las vulnerabilidades en navegadores, que han supuesto un aumento del 16,41% respecto el año anterior.

Y, en **tercer lugar, destaca la explotación de vulnerabilidades de dispositivos Android**, utilizadas un 2,35% menos.



Telegram y el asalto al Capitolio

El hacktivismo es un fenómeno que adquiere cierta relevancia en la sociedad ya que se presenta como una forma de protesta contra medidas o actuaciones llevadas a cabo por gobiernos o grandes corporaciones privadas, utilizando para ello una serie de herramientas digitales mediante las cuales conseguir unos fines, que estarían determinados según la perspectiva de justicia social del grupo. Más concretamente y según la Red Europea de Prevención de la Delincuencia, el hacktivismo sería el "uso subversivo de ordenadores y redes para promover una agenda política". [47]

46 - https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_eng.pdf

Algunos de los mecanismos **digitales que emplean los grupos hacktivistas para conseguir sus fines** son:

- **Ataques de denegación de servicio distribuido (DDoS):** Aumentar el tráfico de la página web de una institución pública o compañía privada para colapsar sus servidores y dejarla inoperativa.

- **Defacements:** Reemplazar el contenido de la página seleccionada, por mensajes elaborados por el grupo hacktivista, con fines reivindicativos.

- **Filtración de la información,** empleando vulnerabilidades mediante las cuales acceder a los dispositivos y sistemas.

Durante estos últimos años hemos podido observar cómo ciertos grupos hacktivistas, empleaban redes sociales como Twitter donde hacían eco de sus actuaciones y promovían ciertas campañas a golpe de tweets y hasthags. Por ejemplo, en 2021 los grupos hacktivistas que han registrado una mayor actividad en redes sociales han sido los siguientes[48]:

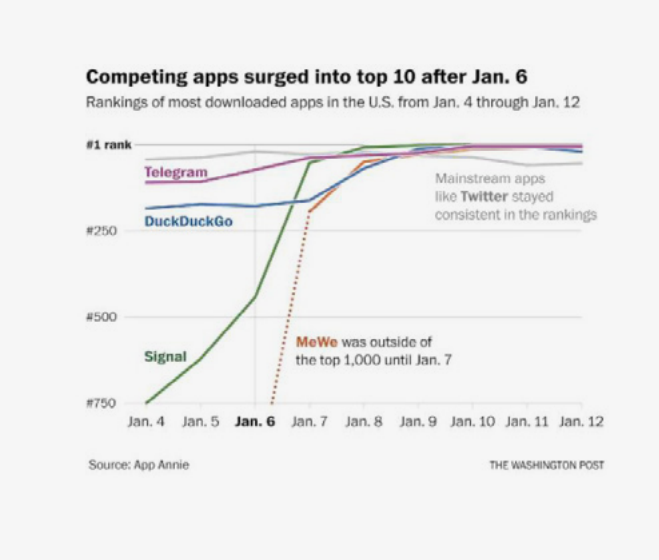
- **Anonymous:** Este grupo ha llevado a cabo varias campañas en Twitter, dando soporte a movimientos sociales tales como el #ParoNacional en Colombia durante el mes de mayo.

- **CyberPartisans:** Grupo hacktivista de origen bielorruso contrario al gobierno bielorruso, instituciones y agencias gubernamentales. En los meses de julio y agosto llevaron a cabo ciberataques contra el Ministerio del Interior de Bielorrusia[49].

Si durante 2020 se produjo un auge en la utilización de Twitter para fines de hacktivismo político, en 2021 ha sido Telegram la que ha experimentado un incremento de dicha utilización de similar índole.

El hecho que marcó un punto de inflexión en cuanto a la expansión de Telegram, fue el asalto al capitolio el 6 de enero de 2021[50], ya que los días posteriores a este suceso 25 millones de nuevos usuarios se dieron de alta en dicha plataforma debido a las reacciones de Twitter y Facebook, que eliminaron las cuentas de aquellos que consideraban responsables de haber incitado a la violencia, difundido desinformación, o promovido ciertas ideologías extremistas.

A continuación se muestra un gráfico donde se pueden observar las plataformas de comunicación que tuvieron gran auge tras el 6 de enero de 2021.[51]

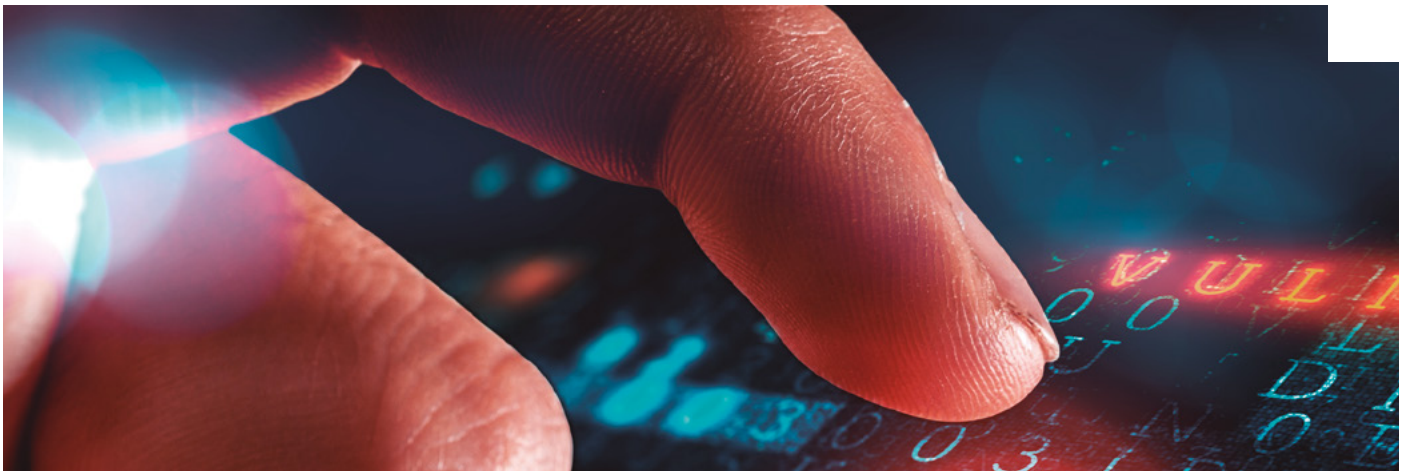


47 - https://eucpn.org/sites/default/files/document/files/theoretical_paper_cybercrime_.pdf

48 - https://www.sentinelone.com/labs/hacktivism-and-state-sponsored-knock-offs-attributing-deceptive-hack-and-leak- operations/ 49https://www.dw.com/en/belarusian-cyber-partisans-want-to-overthrow-the-regime-through-hacking/a-59068288

50 - https://www.nytimes.com/2021/01/26/world/europe/telegram-app-far-right.html

51 - https://www.washingtonpost.com/technology/2021/10/22/jan-6-capitol-riot-facebook/



El aumento en el uso de Telegram también ha supuesto que los cibercriminales usen esta plataforma como herramienta mediante la cual llevar a cabo actividades delictivas y vender cualquier tipo de datos robados, ya que es bastante fácil acceder a los canales por parte de sus usuarios. Además, la creación de canales y grupos de Telegram evita que los delincuentes se registren en un servidor web o servicio de dominio, siendo más accesible que la DarkWeb[52].

Algunas de las consecuencias de las facilidades que ofrece Telegram han sido las siguientes[53]:

- La aplicación es fácil de usar y sus canales, que pueden ser públicos y privados, permiten la comunicación entre decenas de miles de usuarios. Telegram también es elegido por delincuentes porque tiene un enfoque más laxo en la moderación de contenido que otras plataformas de redes sociales.

- Se ha observado un incremento en la cantidad de enlaces a grupos de Telegram o canales compartidos en foros de cibercrimen y piratería de la DarkWeb, pasando de 172.035 en 2020 a más de un millón en 2021. Se cuadruplicaron las palabras utilizadas para referirse a credenciales robadas y otros productos ilegales, llegando a casi 3400.

- Varios son los canales de Telegram utilizados para el intercambio de datos robados como, por ejemplo, datos de tarjetas de crédito, credenciales de inicio de sesión para cuentas bancarias y otros servicios en línea, y copias de pasaportes. Uno de los casos conocidos de canales públicos de Telegram empleados por actores maliciosos para comprar, vender y filtrar volcado de datos fue el canal "combolist"[54].

- De igual modo, se han observado grupos de Telegram empleados por estafadores para vender exploits, códigos y software dañino. [55]

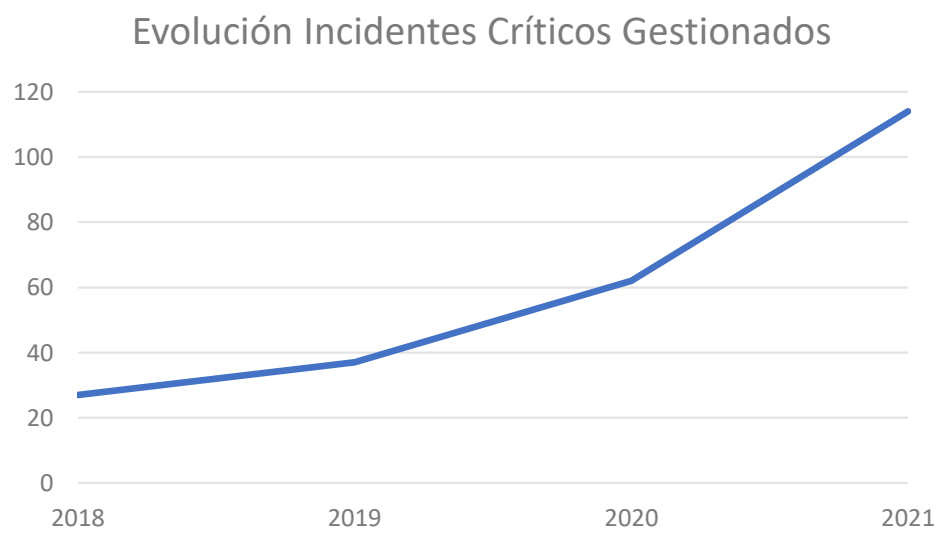
Aunque Twitter continúe siendo una de las herramientas empleadas por grupos hacktivistas a la hora de declarar sus actuaciones y dar a conocer su actividad, Telegram se postula como el medio con mayor alcance poblacional a la hora de coordinar movimientos sociales, así como mecanismo útil de gestión y operatividad para grupos hacktivistas.

52 - https://www.welivesecurity.com/la-es/2021/09/22/cibercriminales-utilizan-telegram-alternativa-dark-web/
53 - https://securityaffairs.co/wordpress/122609/cyber-crime/telegram-cybercrime.html
54 - https://www.ft.com/content/cc3e3854-5f76-4422-a970-9010c3bc732b
55 - https://blog.checkpoint.com/2021/04/22/turning-telegram-toxic-new-toxiceye-rat-is-the-latest-to-use-telegram-for- command-control

5. INCIDENTES 2021.

De manera paralela a la publicación del gran número de vulnerabilidades, especialmente las de día cero, se han encontrado un aumento en el número de incidentes detectados durante el pasado año, evidenciando una relación proporcional entre ambos datos.

Un ejemplo lo tenemos en el número de **incidentes críticos gestionados por el CCN-CERT**, habiéndose gestionado un total de **118** durante el año 2021, lo que supone **prácticamente el doble de los gestionados en 2020**.[56]



56 - https://www.youtube.com/watch?v=UyfCnaOiv0g

5.1 Ciberespionaje

En 2020 el espionaje adquirió una nueva dimensión debido a la relevancia de la pandemia COVID-19 en el contexto internacional. Muchas campañas tuvieron el objetivo de obtener información privilegiada de departamentos sanitarios, especialmente sobre el desarrollo de la vacuna contra el COVID-19, pero también sobre índices de infección y tratamientos.[57]

Tal y como se ha comentado a lo largo del informe, el número de incidentes críticos ha sido muy alto. De ellos, debido a su impacto y contexto, se va a profundizar en HAFNIUM y Lazarus.

HAFNIUM

Especial relevancia ha tenido la actividad de HAFNIUM entre los meses de marzo y abril de 2021. Algunos de sus objetivos han sido organismos gubernamentales, contratistas de defensa, Think Tanks u ONGs, entre otros.

El 2 de marzo de 2021, Microsoft alertó de la salida a la luz de las vulnerabilidades críticas de Exchange Server en versiones on premise, las cuales estaban siendo explotadas a nivel mundial por parte de HAFNIUM.[58]

Tras el acceso inicial a través de la vulnerabilidad comentada, HAFNIUM desplegaba una webshell escrita en lenguaje ASP, comúnmente conocida como ChinaChopper y ampliamente utilizada anteriormente por grupos como APT27 o Ke3chang.

Posteriormente, los atacantes llevaban a cabo el reconocimiento del equipo a través de herramientas del sistema, recolectando dicha información y a través del software 7-Zip, comprimiendo los ficheros generados con el objetivo de exfiltrarlos posteriormente.

El principal objetivo de los atacantes fueron los buzones de correo, encontrando capacidades de PowerShell para el volcado de los mismos y la posterior exfiltración.

De esto modo, las principales técnicas empleadas por HAFNIUM son:

ID	Técnica	Procedimiento
T1190	Exploit Public-Facing Application	Explotación de vulnerabilidades de Exchange
T1059.001	Command and Scripting Interpreter: PowerShell	Utilización de PowerShell para el volcado de buzones de correo
T1505.003	Server Software Component: Web Shell	Utilización de la Web Shell ChinaChopper para la persistencia en la organización
T1003.001	OS Credential Dumping: LSASS Memory	Utilización del binario procdump para el dumpeo de credencia-les en memoria del proceso LSASS
T1560.001	Archive Collected Data: Archive via Utility	Utilización del binario 7-Zip para la compresión de los archivos recolectados en fases anteriores
T1095	Non-Application Layer Protocol	Utilización del protocolo TCP como mecanismo de comando y control

57 - https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development
58 - Se detallará en el apartado 5.2 de este informe

Lazarus

Otra de las campañas que más impacto ha tenido durante el año ha sido la del grupo APT Lazarus.[59]

Si bien en 2021 han llevado a cabo campañas de diferente tipo, incluso de índole cibercriminal, quizá la operación más extendida y de mayor impacto ha sido la realizada contra personal asociado a contratistas de defensa a través de la suplantación de grandes firmas de defensa como Lockheed Marting o Raytheon.

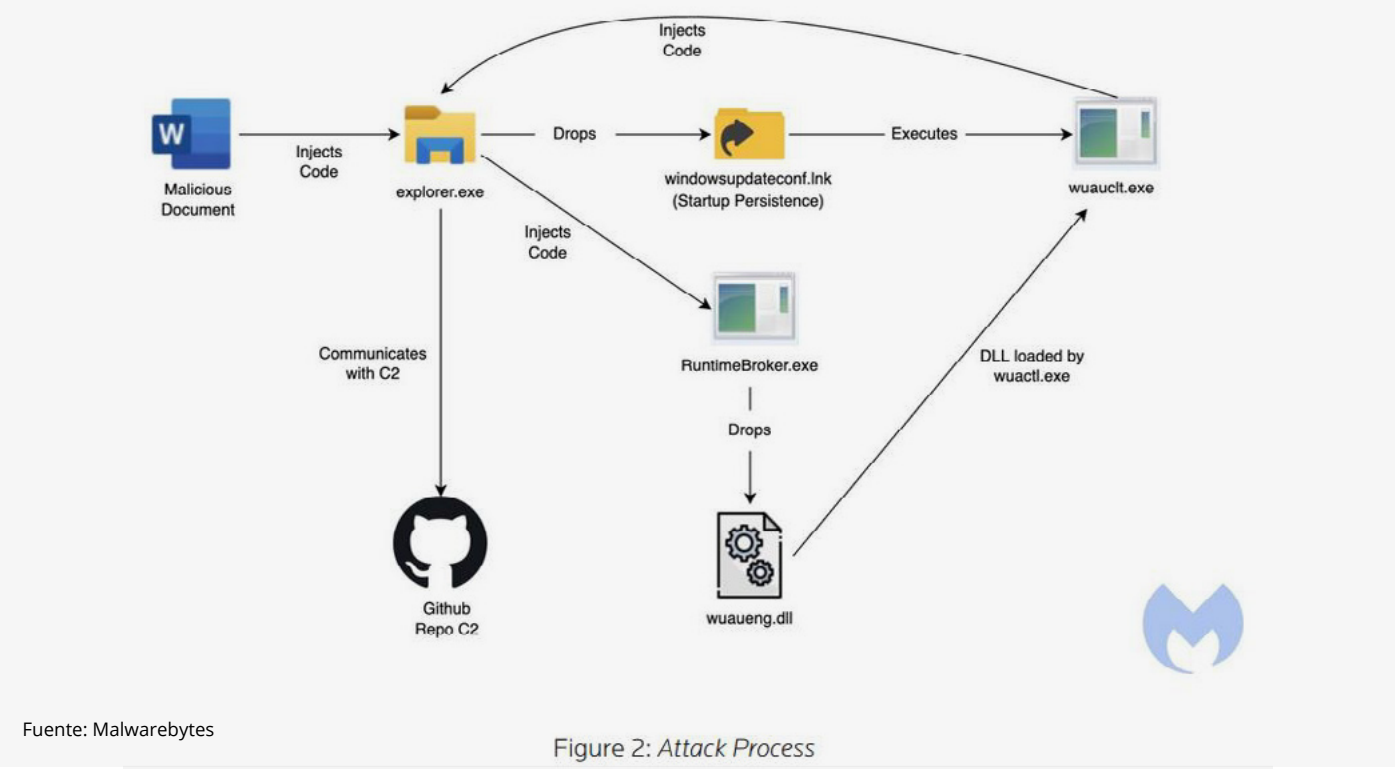
Con el objetivo de comprometer una organización, Lazarus ha utilizado, principalmente, dos vías de infección. La primera de ellas es a través de spear phishings con adjuntos con títulos como "Lockheed_Martin_JobOpportunities.docx" o "Salary_Lockheed_Martin_job_opportunities_confidential.doc", documentos de Microsoft Word que llevaban a cabo la ejecución de macros.

Sin embargo, otro método más dirigido has sido mediante el contacto a través de la plataforma LinkedIn, ofreciendo los mismos empleos comentados anteriormente y, por tanto, haciendo llegar de un modo más elaborado y directo los documentos infectados.

Una de las principales técnicas a destacar del compromiso es la modificación del PEB (Process Environment Block), concretamente de la KernelCallbackTable, a través de la función WMIsAvailableOffline de la dll wmvcore.dll. La macro lleva a cabo el remplazo de la callback USER32!_fnDWORD existente por la función maliciosa, la cual llevará a cabo las sucesivas inyecciones.

Cabe destacar la utilización del binario de Windows Update para la ejecución del código malicioso y la utilización de Github como mecanismo de Comando y Control.

Estas cuestiones, junto a las técnicas comentadas anteriormente, dotan a la campaña de Lazarus de una especial sofisticación respecto a lo observado en años anteriores.



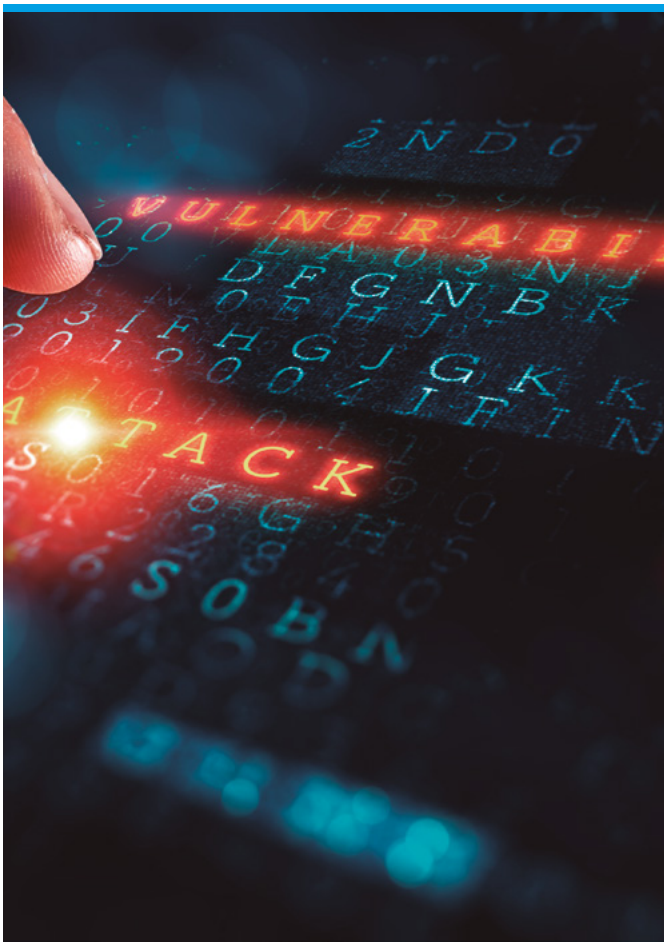
Fuente: Malwarebytes

Figure 2: *Attack Process*

59 - https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update- client-github-in-latest-campaign/

Las técnicas empleadas por Lazarus en dicha campaña son las siguientes:

ID	Técnica	Procedimiento
T1585.001	Establish Accounts: Social Media Accounts	Utilización de cuentas en LinkedIn para ataques de ingeniería social
T1059.005	Command and Scripting Interpreter: Visual Basic	Utilización de scripts vbs en macros de ficheros Word
T1574.013	Hijack Execution Flow: KernelCallback Trace	Utilización de la llamada a la API KernelCallBackTrace para el control del flujo de procesos y posterior ejecución de shellcodes
T1070	Indicator Removal on Host	Restauración de KernelCallbackTable a la original tras el hijack del flujo del proceso en ejecución
T1104	Multi-Stage Channels	Utilización de malware multietapa para la inyección en diferentes procesos del sistema
T1583.006	Acquire Infraestructure: Web Services	Utilización como mecanismo de Comando y Control de la plataforma Github



5.2 Vulnerabilidades

A lo largo del informe se ha comentado el amplio impacto que han tenido las vulnerabilidades críticas durante el año. En este apartado se comentarán las principales vulnerabilidades publicadas en 2021, así como el detalle de aquellas con mayor impacto en los sistemas de información.

Vulnerabilidades destacadas en 2021

TRIMESTRE	VULNERABILIDAD	ALCANCE	SOFTWARE AFECTADO
AFECTADO ENERO - MARZO	CVE-2021-21972	Ejecución remota de código	VMware vCenter
	CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065 Exchange Server SSRF Vulnerability	Cadena de vulnerabilidades que permite ejecutar código remoto para tomar el control del sistema afectado u obtener información confidencial	Microsoft Exchange Server 2013, 2016 y 2019
	CVE-2021-26411 Internet Explorer Memory Corruption Vulnerability	Permite al atacante ejecutar código remoto si un usuario accede a un HTML dañado	Microsoft Edge Internet Explorer
	CVE-2021-22986 CVE-2021-22987 CVE-2021-22991 CVE-2021-22992		F5 BIG-IP
	CVE-2021-1732 Windows Win32k Elevation of Privilege Vulnerability	Permite al atacante obtener privilegios elevados	Windows 10 Windows Server
	CVE-2021-26897 Windows DNS Server Remote Code Execution Vulnerability	Un fallo en el servidor DNS de Windows permite la ejecución remota de código	Windows Server 2008, 2012
	CVE-2021-24074 CVE-2021-24094 Windows TCP/IP Remote Code Execution Vulnerability	Ejecución de código remota por atacantes no autentificados, debido a un fallo de la implementación TCP/IP de Windows	Windows 7, 8 y 10 Windows Server 2008 y 2012
AFECTADO ABRIL - JUNIO	CVE-2018-13379 CVE-2019-5591 CVE-2020-12812		FortiOS (Fortinet SSL VPN)
	CVE-2021-26897 Windows DNS Server Remote Code Execution Vulnerability	Un fallo en el servidor DNS de Windows permite la ejecución remota de código	Windows Server 2008, 2012
	CVE-2021-22893	Vulnerabilidad del software VPN Pulse Secure. Utilizada junto a otras publicadas anteriormente permite a un usuario autenticado con derechos de administrador sobrescribir archivos de manera arbitraria	Pulse Secure
AFECTADO JULIO - SEPTIEMBRE	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	Vulnerabilidades conocidas como ProxyShell. Su combinación permite a un atacante ejecutar comandos en los servidores Exchange a través de un puerto 443 expuesto	FortiOS (Fortinet SSL VPN)
	CVE-2021-40444 Microsoft MSHTML Remote Code Execution Vulnerability	Vulnerabilidad de severidad alta que permite ejecución de código remota en Internet Explorer	Windows 7, 8.1 y 10. Windows Server 2012, 2008, 2016.20H2, 2004, 2022 y 2019.
AFECTADO OCTUBRE - DICIEMBRE	CVE-2021-26897 Windows DNS Server Remote Code Execution Vulnerability	Un fallo en el servidor DNS de Windows permite la ejecución remota de código	FWindows Server 2008, 2012
	CVE-2021-44228 CVE-2021-45046 CVE-2021-4104	Vulnerabilidad Log4Shell que permite la ejecución remota de código en el servidor	Librería Log4j de Java Apache

Microsoft Exchange

Además de **HAFNIUM, distintos actores como LuckyMouse, Tick o Calypso, han estado explotando activamente diferentes vulnerabilidades en servidores de Microsoft Exchange** localizados en diversos países. Una de las **más representativas**, conocida como **ProxyLogon,** consiste en el encadenamiento de diferentes vulnerabilidades que pueden dar acceso a servidores Exchange, robar las credenciales de acceso al correo electrónico, introducir malware o desplegar un ransomware. A continuación, se muestran las descripciones correspondientes a las vulnerabilidades mencionadas:

- CVE-2021-26855: vulnerabilidad de falsificación de solicitudes del lado del servidor (SSRF) en Exchange que permite al atacante enviar solicitudes HTTP arbitrarias y ejecutarlas en el contexto de privilegio del servicio de Exchange.

- CVE-2021-26857: vulnerabilidad de deserialización en el servicio de mensajería unificada implementado en Microsoft Exchange Server.

- CVE-2021-26858 y CVE-2021-27065: vulnerabilidades que permiten al atacante subir ficheros después de conseguir una autenticación aprovechando las vulnerabilidades anteriores. Se puede utilizar estos fallos para escribir un archivo en cualquier ruta del servidor, subir una Webshell para un control más efectivo del sistema o la ejecución de scripts que permitan múltiples acciones de exfiltración o movimientos laterales, entre otros.

Según diversos medios[60], estos ataques afectaron a más de 250.000 servidores Exchange a nivel global.

Del total de 31 vulnerabilidades publicadas en 2021 que están relacionadas con los servidores Exchange, 4 se consideran críticas y permiten la ejecución remota de código. De entre todas ellas, cabe destacar el impacto de **ProxyShell**, de nuevo un nombre general para referirse a los CVE-2021-34473, CVE-2021-34523 y CVE-2021-31207:

- CVE-2021-34473: un problema de pre-autenticación que permite evadir las ACL.

- CVE-2021-34523: una vulnerabilidad de escalada de privilegios a través del binario PowerShell.

- CVE-2021-31207: una configuración incorrecta que permite la escritura de archivos arbitrarios.

Estas vulnerabilidades funcionan en tándem, proporcionando a los atacantes la **capacidad de ejecutar comandos en los servidores Exchange** a través de un puerto 443 expuesto, lo que incrementa de manera exponencial el número de infraestructuras susceptibles a ser atacadas.

Acceso remoto

La proliferación de los servicios de conectividad remota que despuntó de manera especial en el inicio de la pandemia de la COVID-19, ha supuesto que este tipo de servicios haya seguido siendo uno de los objetivos principales para los atacantes en 2021:

1. Se reportaron 2 vulnerabilidades críticas de ejecución remota de código en VMware vCenter, una plataforma centralizada para controlar los entornos de vSphere.

La primera de ellas, CVE-2021-21972, permite que un atacante con acceso al puerto 443 ejecute cualquier tipo de código a través de una petición específica al servidor. De esta manera, es posible acceder a

60 - https://edition.cnn.com/2021/03/10/tech/microsoft-exchange-hafnium-hack-explainer/index.html

información confidencial alojada en la plataforma, pudiendo llegar a tener también el control del propio servidor que soporta el aplicativo.

Por su parte, el CVE-2021-21985 permite explotar el cliente HTML5 de vSphere debido a la falta de validación en uno de los plugins utilizados, que se encuentra habilitado por defecto en VCenter Server.

2. Por otra parte, durante el mes de marzo, fueron reportadas 7 vulnerabilidades, 4 de ellas críticas, relacionadas con los productos F5 BIG-IP, software con una amplia gama de productos que incluyen firewalls, control de acceso o protección contra amenazas y BIG-IQ, software de administración centralizada[61].

A continuación, se exponen brevemente las vulnerabilidades catalogadas como críticas:

- CVE-2021-22986 y CVE-2021-22987: vulnerabilidad que permite a atacantes no autenticados con acceso de red a la interfaz REST de iControl ejecutar código arbitrario, crear o eliminar archivos y deshabilitar servicios.

- CVE-2021-22991: vulnerabilidad que puede desencadenar un desbordamiento de búfer, pudiendo provocar una denegación de servicio. En ciertas situaciones puede incluso permitir eludir el control de acceso basado en URL o la ejecución remota de código.

- CVE-2021-22992: una respuesta HTTP maliciosa puede desencadenar un desbordamiento de búfer, provocando de esta forma una denegación de servicio. Un atacante debe tener control sobre los servidores web back-end o la capacidad de manipular las respuestas HTTP del lado del servidor para aprovechar esta vulnerabilidad.

3. Adicionalmente, tanto la CISA como el FBI[62] reportaron la explotación intensiva de múltiples vulnerabilidades relacionadas con la solución VPN de Fortinet SSL VPN:

- CVE-2018-13379: provocada por la falta de validación de acceso a determinados archivos internos del servidor, y que permite a un atacante no autenticado obtener archivos del propio sistema operativo FortiOS.

- CVE-2019-5591: que permite interceptar información confidencial dentro de la red haciéndose pasar por el servidor LDAP.

- CVE-2020-12812: una vulnerabilidad que permite iniciar sesión sin el segundo factor de autenticación (FortiToken).

4. Por otro lado, tal y como informó Mandiant[63] se detectó que una vulnerabilidad de día cero en el software de VPN de Pulse Secure (CVE-2021-22893) se estaba explotando de manera activa por diferentes actores maliciosos. Esta vulnerabilidad, junto con vulnerabilidades ya conocidas anteriormente (CVE-2019-11510, CVE-2020-8243 y CVE-2020-8260), podrían haber sido el vector de entrada en diferentes organizaciones.

De explotarse, estas vulnerabilidades permiten que un usuario autenticado con derechos de administrador sobrescriba archivos arbitrarios de la plataforma. Una vez comprometida, los atacantes habrían recopilado credenciales de los inicios de sesión en los dispositivos y estableciendo persistencia en las redes comprometidas mediante el empleo de scripts y binarios modificados.

61 - https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/10895-ccn-cert-al-03-21-vulnerabilidades-en-big-ip-y- big-iq.html
62 - https://www.cisa.gov/uscert/ncas/current-activity/2021/05/28/fbi-update-exploitation-fortinet-fortios- vulnerabilities
63 - https://www.mandiant.com/resources/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day

Log4j

Si bien Apache ha tenido otras vulnerabilidades identificadas durante 2021 (CVE-2021-41773, relacionada con path transversal), si por algo será recordado este servidor web durante 2021 es por la famosa Log4Shell o Log4Jam, CVE-2021-44228, y categorizada con un CVSS de 10.0.

Asociada a la vulnerabilidad CVE-2021-44228 se han identificado además diversas vulnerabilidades, como por ejemplo la CVE-2021-45046, o CVE-2021-4104.

Esta vulnerabilidad afecta a la librería de registro de Java Apache Log4j 2, herramienta desarrollada por Apache Foundation que ayuda a los desarrolladores de software a escribir mensajes de registro, cuyo propósito es dejar constancia de una determinada transacción en tiempo de ejecución.

Log4shell tiene un alto impacto, ya que la solución Log4j 2 se usa ampliamente en muchas aplicaciones y está presente, como dependencia, en muchos servicios, incluyendo aplicaciones empresariales y servicios en la nube. Este componente se utiliza también con mucha frecuencia en el software Java, pudiendo afectar potencialmente, según Google, a más de 35.000 paquetes de Java.[64] Esto hace que exista un número muy alto de infraestructuras que pueden ser comprometidas mediante la explotación de Log4shell, aunque es muy difícil de cuantificar. Adicionalmente, la vulnerabilidad fue publicada directamente en Twitter, lo que incrementó de manera exponencial el impacto de esta.[65]

Log4shell aprovecha una validación de entrada incorrecta al procesar solicitudes LDAP, lo que podría permitir la ejecución remota de código, comprometer totalmente el servidor y, por tanto, la confidencialidad e integridad de los datos, así como la disponibilidad del propio sistema.

64 - https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html
65 - https://appsecphoenix.com/the-impact-of-log4shell-vulnerability

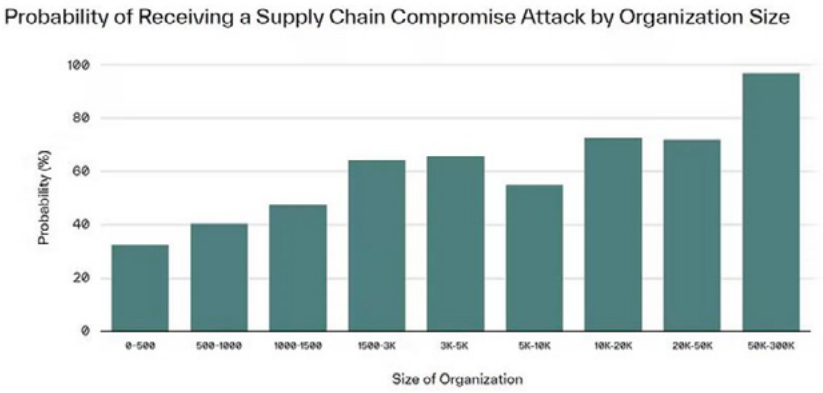
6. MÉTODOS DE ATAQUE. NOVEDADES EN 2021

6.1 Cadena de Suministro

Desde el ataque contra SolarWinds a finales de 2019, se ha observado un aumento en la **sofisticación de los ataques a través de cadena de suministro, siendo las empresas de servicios software las más afectadas.**

La utilización de este tipo de campañas proviene de la confiabilidad de las comunicaciones entre los proveedores de servicios y los clientes, además de la combinación con técnicas de ingeniería social. De esta manera, conseguir una vía de infección de estas características parece haberse convertido en una de las prioridades de los atacantes, pues permite llevar a cabo un compromiso a largo plazo y de mayor probabilidad de éxito.[66]

Como es lógico, se ha encontrado una correlación directa entre el tamaño de la organización y la probabilidad de sufrir un ataque de estas características, pues se dispone de un mayor número de contratas que pueden ser comprometidas.[67]



Uno de los compromisos más importantes que ha tenido lugar en 2021 ha sido el ataque a Kaseya.

66 - https://www.zdnet.com/article/supply-chain-attacks-are-the-hackers-new-favourite-weapon-and-the-threat-is- getting-bigger/
67 - https://abnormalsecurity.com/blog/new-research-supply-chain-compromise-attack

Ataques a través de la cadena de suministro: Kaseya

A mediados de 2021 se descubrió un ataque ejecutado por el grupo de ransomware REvil en el que se explotó una vulnerabilidad de día cero de los servidores Kaseya VSA[68]. Este software facilita la administración de endpoints y la monitorización de redes de forma remota.

El ransomware fue dirigido a la cadena de suministro del software, aprovechando una vulnerabilidad de evasión de autenticación en la interfaz web de Kaseya. Los atacantes lograron cargar malware y ejecutar comandos a través de inyecciones SQL.

Dado que este software cuenta con un alto grado de confianza en las redes de los clientes, y a pesar de que la compañía indicó que únicamente algunas docenas de clientes se habían visto afectados, se sospecha que esta cifra fue bastante mayor, estimándose en más de 1.500 empresas de todo el mundo. Un ejemplo de su impacto lo tenemos en la cadena de supermercados sueca Coop, la cual tuvo que cerrar durante varios días dado que se habían visto afectados por este ransomware y no podían acceder a sus registros[69].

El grupo criminal REvil desapareció tras este ataque, puesto que las autoridades rusas desmantelaron al grupo tras arrestar a varios de sus miembros[70].

6.2 Operaciones disruptivas

Durante 2021 las operaciones disruptivas y de control, en especial contra sistemas industriales, han seguido incrementándose como lo vienen haciendo desde hace más de cinco años[71]. En este sentido, el CERT gubernamental de Singapur (SingCERT) publicó en octubre de 2021 un informe sobre tales operaciones con especial foco en los sistemas ciberfísicos[72], por su potencial impacto en servicios esenciales.

Algunas de estas operaciones que han salido a la luz en 2021[73] son las mostradas en la tabla siguiente. Se incluyen en este listado operaciones tanto ligadas a actores estado como delincuenciales que han impactado de forma significativa en infraestructuras o servicios básicos para la población:

68 - https://securityboulevard.com/2021/07/the-kaseya-vsa-revil-ransomware-supply-chain-attack-how-it-happened- how-it-could-have-been-avoided/
69 - https://www.securityweek.com/swedish-supermarket-closed-kaseya-cyberattack
70 - https://www.bbc.com/news/technology-59998925
71 - Véase el informe ENISA Threat Landscape 2021, publicado en octubre de 2021.
72 - Véase https://www.csa.gov.sg/en/singcert/Publications/disruptive-threats-against-business-operations-and-their- impact---focus-on-cyber-physical-systems
73 - Véase https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Mes	Descripción	País objetivo	Sector objetivo	Táctica	Actividad
ENERO	Ataques DDoS contra agencias gubernamentales rusas y ucranianas afectan a servicios públicos esenciales	RU/UA	Guberna-mental	Interrupción	Desconocido
FEBRERO	Intento de manipulación del suministro de agua potable de Oldsmar, Florida	US	Aguas	Manipulación	Desconocido
MARZO	Operaciones de reconocimiento para posteriores ataques al sistema de transporte eléctrico indio	iN	Energía	Recon	Estado
MARZO	Ransomware contra Nine Entertainment, medio de comunicación australiano	AU	Audiovisual	Destrucción	Delincuencial
ABRIL	Código dañino que causa caída de sistemas de reservas de veinte aerolíneas de bajo coste en todo el mundo	Multi	Transporte	Interrupción	Desconocido
MAYO	Ataque ransomware contra Volue, empresa noruega, que causa parada de plantas de tratamiento de aguas en unas doscientas localidades y afecta al 85% de la población noruega	NO	Aguas	Destrucción	Delincuencial
MAYO	Ataque ransomware contra el Sistema Nacional de Salud irlandés	IR	Salud	Destrucción	Delincuencial
MAYO	Ataque ransomware contra JBS, empresa brasileña de procesamiento cárnico, con afectación a varios países	BR	Alimentación	Destrucción	Delincuencial
JUNIO	Ataque ransomware contra los servicios públicos de la ciudad de Lieja que interrumpe sistemas de gestión administrativa	BE	Guberna-mental	Destrucción	Delincuencial
JULIO	El Ministerio de Transporte iraní sufre un ataque que causa cientos de cancelaciones de trenes en todo el país	IR	Guberna-mental	Interrupción	Desconocido
SEPT	Ataque contra los sistemas electorales húngaros tras la apertura de colegios electorales, que obliga al gobierno a ampliar dos días las elecciones	HU	Guberna-mental	Interrupción	Desconocido
OCTUBRE	Ataque contra las tarjetas electrónicas usadas en Irán para comprar combustible, mostrando mensajes en contra del régimen	IR	Guberna-mental	Degradación	Desconocido
DICIEMBRE	Ataque ransomware contra CS Energy, empresa australiana	AU	Energía	Destrucción	Delincuencial

Como podemos ver, el ámbito gubernamental, como prestador de servicios esenciales, ha sido especialmente atacado en 2021, aunque sectores también críticos, como el energético, también han sido objetivos relevantes de los actores hostiles. Un ejemplo es el ataque anteriormente comentado contra Colonial Pipeline.

En función de las aproximaciones empleadas para lograr el objetivo, en el caso de destrucción sin duda el uso de ransomware es la más relevante; en este caso, el abuso de sistemas expuestos a Internet sin una seguridad adecuada (especialmente sin doble factor de autenticación) es la técnica más utilizada por los delincuentes, aunque algunas más clásicas, como el phishing, también han resultado efectivas.

Otras técnicas delincuenciales como el ransom DDoS (RDDos) no son tan habituales, aunque es destacable el número de ataques DDoS sin actor conocido mostrado en la tabla anterior, lo que podría implicar el uso de esta técnica sin que se haga público el detalle. La utilización de herramientas de destrucción, como los wiper, no es tan habitual.

7. QUÉ ESPERAR EN 2022

2022 se presenta como un año donde se espera una vuelta paulatina a la normalidad en lo referente a la COVID-19, recuperando toda actividad social, pero manteniendo algunas posibilidades que trajo consigo la pandemia, como es el caso del teletrabajo, especialmente en el sector TI.

En cuanto a la actividad cibercriminal, se espera que siga manteniendo el número de ataques de tipo ransomware, especialmente con la vuelta de Emotet, pero, como ya han demostrado, también a través de la utilización de metodologías de compromiso cada vez más sofisticadas.

En la misma línea, debido a la codependencia entre los diferentes actores dentro de la organización, especialmente tras la pandemia, hace prever que el número de ataques a través del compromiso de la cadena de suministro siga aumentando durante el año respecto a años anteriores.[74]

Por el contrario, con el aumento de los precios de la energía y, con ello, el incremento del coste del minado de criptomonedas, es de esperar que el número de malware con un objetivo enfocado al robo de criptodivisas disminuya fuertemente su crecimiento y su uso por parte de los cibercriminales. Ciertos entornos industriales tienen gran relevancia estratégica, especialmente si están relacionados con entidades estatales y/o infraestructuras críticas. En estos casos, los entornos industriales se convierten en objetivo potencial de campañas y acciones de ciberguerra. Tal y como se ha documentado, el número de atacantes que están llevando a cabo acciones contra los sistemas industriales está creciendo a un ritmo tres veces superior a la media.[75]

Por otra parte, la guerra entre Rusia y Ucrania hacen prever una mayor actividad vinculada a grupos como APT28, APT29, Turla o Gamaredon especialmente contra los países limítrofes con la Federación Rusa y países miembros de la OTAN. A pesar de que se espera que esta actividad sea fundamentalmente ciberespionaje, no se descarta que se lleven a cabo acciones puntuales de ciberguerra a través de un impacto en los sistemas de comunicación ucranianos, como fue el caso de HermeticWiper, ejecutado el día 23 de febrero de 2022 sobre sistemas informáticos ucranianos.

74- https://www.forbes.com/sites/forbestechcouncil/2022/03/11/cybersecurity-predictions-for- 2022/?sh=24bef8f77749
75 - https://hub.dragos.com/2020-year-in-review-download

7.1 Conflicto en Ucrania

Desde que se iniciara la ofensiva rusa en Ucrania el 24 de febrero de 2022, varias son las repercusiones internacionales que está teniendo el conflicto en los distintos ámbitos como el político, económico, social y militar, tanto a nivel regional como mundial. De igual modo, todo ello está trascendiendo de manera significativa en el ámbito cibernético.

En este sentido, ya que el enfrentamiento aún persiste y puesto que España pertenece a organismos internacionales tales como la OTAN[76] o la UE[77] que han sancionado las actuaciones llevadas a cabo por determinados actores en la contienda, es recomendable permanecer alertas y seguir las recomendaciones de autoridades en cuanto a la posible recepción de ciberataques por parte de grupos de amenazas persistentes, tal y como se ha mencionado en apartados previos.

7.2 Operaciones disruptivas

El inicio de 2022 ha venido también marcado por algunas operaciones disruptivas y de control muy significativas. Algunas de ellas se muestran en la siguiente tabla:

Mes	Descripción	País objetivo	Sector objetivo	Táctica	Actor
ENERO	Ataque disruptivo contra sistemas gubernamentales ucranianos haciéndose pasar por ransomware	UA	Gubernamental	Destrucción	Desconocido
ENERO	Ataques DDoS contra servidores Minecraft que impacta en Andorra Telecom y deja sin servicio de comunicaciones a sus clientes	AD	Telecomunicaciones	Interrupción	Desconocido
ENERO	Ataques DDoS contra Corea del Norte que cortan el tráfico del país hacia o desde el resto del mundo	KP	Telecomunicaciones	Interrupción	Desconocido
ENERO	Ataque destructivo contra la empresa de ferrocarriles bielorrusa	BY	Transporte	Destrucción	Hacktivismo
FEBRERO	Interrupción de vuelos tras compromiso por ransomware en el aeropuerto internacional de Zurich	CH	Transporte	Destrucción	Desconocido
FEBRERO	Interrupción de servicios de compañías energéticas en puertos de Bélgica y Alemania	BE, DE	Energía	Interrupción	Desconocido
FEBRERO	Ataque DDoS contra el Ministerio de Defensa ucraniano y sistemas bancarios del país	UA	Gubernamental, Finanzas	Interrupción	Estado
FEBRERO	Ataque destructivo, vía wiper, contra sistemas gubernamentales y financieros ucranianos	UA	Gubernamental, Finanzas	Destrucción	Estado

76 - https://www.nato.int/cps/en/natohq/news_194319.htm?selectedLocale=en

77 - https://www.consilium.europa.eu/es/policies/sanctions/restrictive-measures-against-russia-over-ukraine/

Como se puede observar, en los primeros meses de 2022, y motivados por la invasión rusa de Ucrania, se produjo un incremento de operaciones disruptivas, aunque lejos tal vez de lo que a priori se podría haber estimado.

Desde el inicio del conflicto ruso-ucraniano se han identificado operaciones de interrupción contra infraestructura ucraniana, pero también operaciones destructivas mediante el despliegue de tres wipers diferentes y de posible atribución rusa: Hermetic Wiper, Isaac Wiper y Caddy Wiper. En cualquier caso, es necesario recordar que el wiper es el último paso de una operación destructiva, por lo que es necesario el trabajo en fases previas de la operación para poder detectar y mitigar la amenaza de forma efectiva.

Igualmente, Bielorrusia ha sido objeto de operaciones destructivas, supuestamente hacktivistas, ligadas a su participación en la invasión de Ucrania y con el objetivo de dificultar esta.

A lo largo del año no es descartable que estas acciones continúen o se incrementen en todos los ámbitos, incluyendo el cibercrimen, y por supuesto el ligado a actores estado, en especial por la situación desencadenada en Ucrania y su repercusión en el panorama internacional. En este sentido, en 2022 pueden ser especialmente relevantes los siguientes elementos:

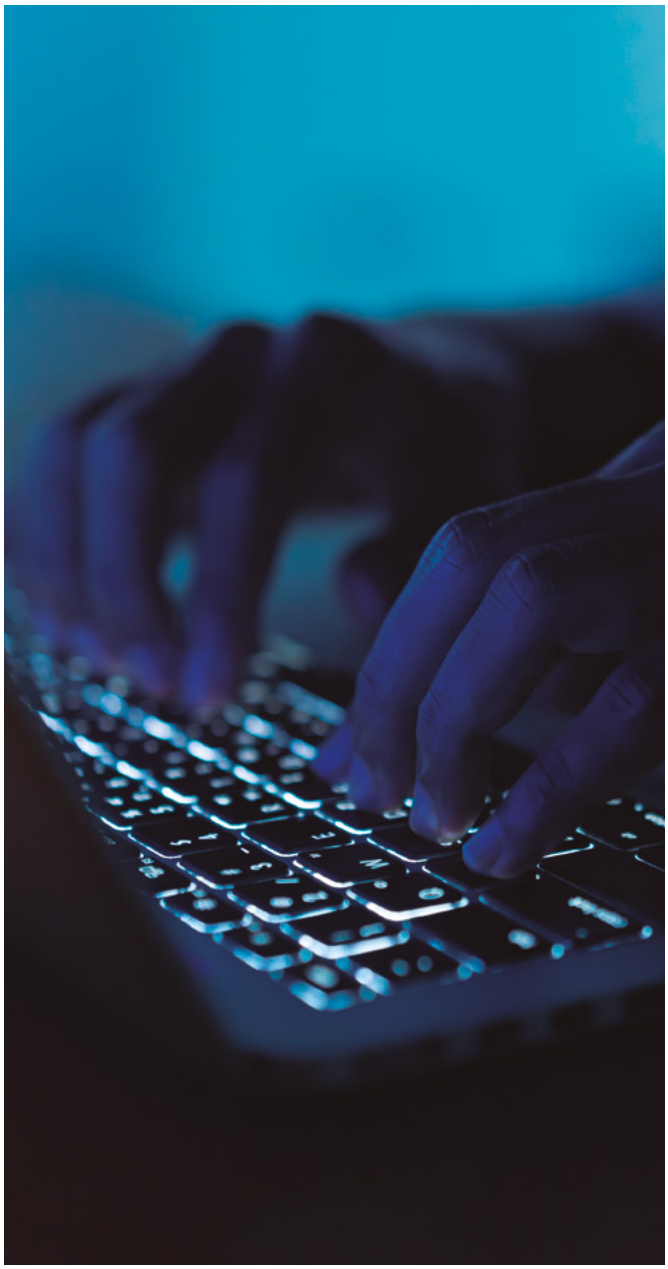
- Incremento de compromisos mediante ransomware en campañas de cibercrimen, incluyendo impactos en sistemas ciberfísicos que pueden degradar servicios esenciales para la sociedad.

- Posibles compromisos de la cadena de suministro en operaciones no solo de ciberespionaje, sino también destructivas y de manipulación. El uso de esta técnica está yendo en aumento en los últimos meses y es previsible que lo siga haciendo durante todo 2022.

- Operaciones CNA de actores estado contra infraestructuras críticas de países no aliados, tanto en el ámbito IT como en el OT.

8. CONCLUSIONES

Tal y como se ha mostrado a lo largo de este informe, los retos que tiene por delante la ciberseguridad en materia defensiva son cada año más complejos. Las ciberamenazas, además de ser cada vez más sofisticadas técnicamente han demostrado focalizar más sus recursos contra las organizaciones, cuestión que se evidencia en que el número de ataques y su impacto vaya en aumento.



El impacto de la COVID-19 está disminuyendo en la agenda global, pero las mejoras en cuanto a las capacidades de digitalización que ha traído consigo se mantienen en las organizaciones, puertas que están utilizando los atacantes como método de entrada.

De este modo, se pone en evidencia no sólo la necesidad de una mejora constante de las capacidades de detección y respuesta, sino también de la prevención de las amenazas, los planes de contingencia y la colaboración entre los organismos públicos y privados para la defensa de los sistemas de información.

Es importante destacar que un aumento de las capacidades no tiene efecto por sí mismo sin un Centro de Operaciones de Ciberseguridad (COCS) con personal experto interprete y actúe ante las potenciales amenazas