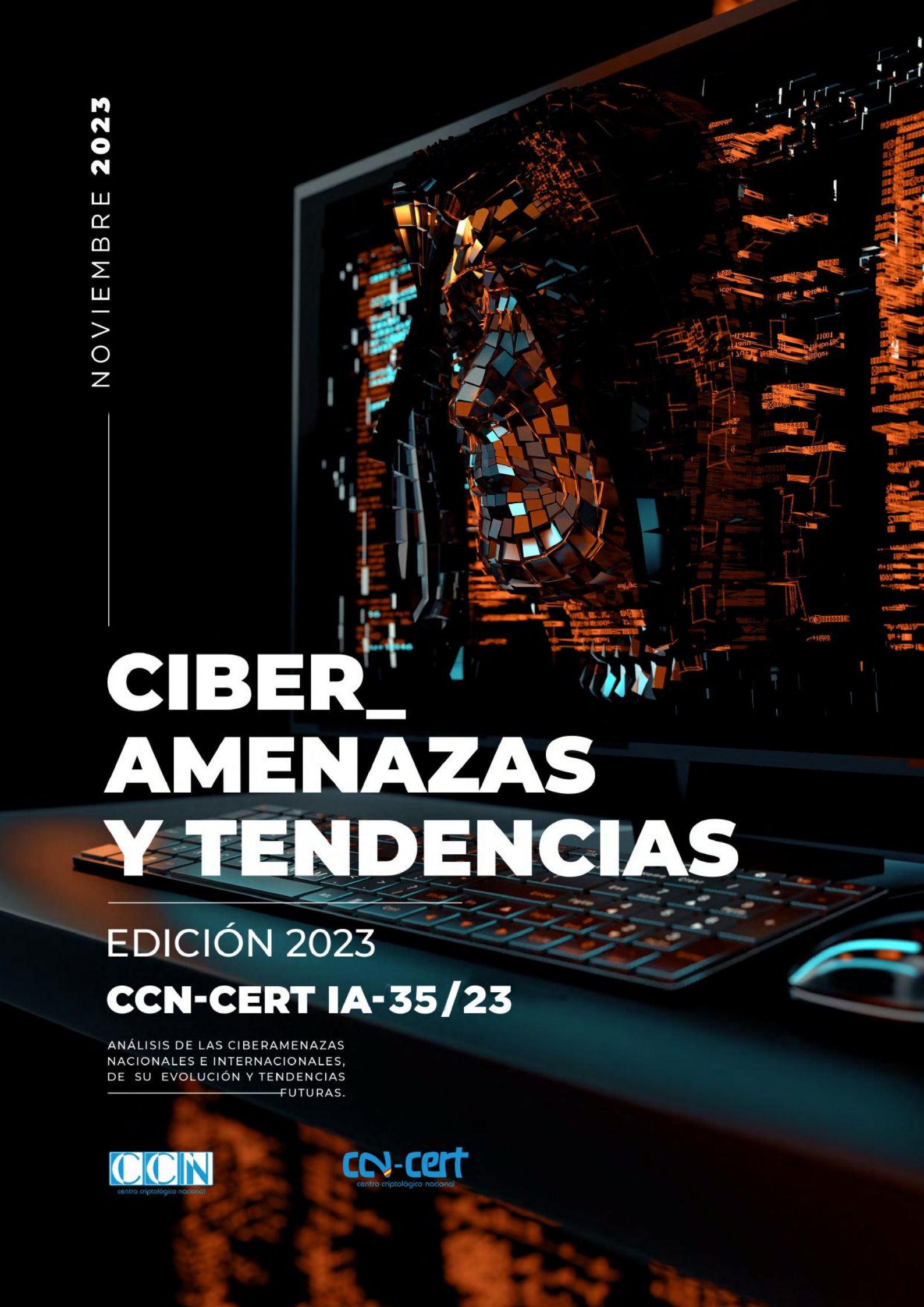
NOVIEMBRE 2023



CIBER_ AMENAZAS Y TENDENCIAS

EDICIÓN 2023

CCN-CERT IA-35/23

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

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

EDITA:

Centro Criptológico Nacional, 2023

Fecha de edición: noviembre de 2023

ÍNDICE

1

Resumen ejecutivo

NO CABE DUDA DE QUE EL AÑO 2022 PASARÁ A LA HISTORIA POR EL INICIO DEL CONFLICTO ARMADO EN UCRANIA A RAÍZ DE LA INVASIÓN POR PARTE DE RUSIA. LIGADO A ESTA ACCIÓN, DESDE ENERO DEL PASADO AÑO PUDIMOS VER UNA CRECIENTE HOSTILIDAD EN EL CAMPO DEL CIBERESPACIO POR PARTE DE GRUPOS PRORRUSOS.

Quizá, es la primera vez que se observa una operación conjunta utilizando el dominio del ciberespacio en madurez. En comparación con el escenario de Georgia en 2008, **en 2022 se ha visto la conjunción de un conflicto multidominio donde los ataques convencionales y los ciberataques se han ejecutado indistintamente**. Un ejemplo de la evolución tecnológica y militar se ha visto no sólo en la coordinación de las operaciones del ciberespacio, sino también en la incorporación de operaciones con drones y el uso de tecnología civil con fines militares. De este modo, se ha visto un modelo de guerra donde se han combinado las campañas de desinformación con campañas de impacto, utilizando tierra, mar, aire y ciberespacio para afectar a los principales servicios ucranianos, desde bancos a agencias de noticias y subestaciones eléctricas que han dejado sin energía a regiones de este país.

También se ha observado la involucración de personal civil en el conflicto mediante campañas de hacktivismo en la que diversos grupos han participado, bien directamente contra organismos ucranianos o contra organismos de países externos al conflicto que han prestado ayuda. En este sentido se han producido numerosas campañas de denegación de servicio utilizando no sólo a voluntarios sino también capacidades obtenidas de forma ilícita como botnets IoT.

En el presente informe **se detallarán las principales tendencias del año 2023, repasando además las campañas de malware, vulnerabilidades e incidentes registrados en 2022**. También se analizarán en profundidad las acciones de mayor relevancia, haciendo hincapié en aquellas que han tenido a Ucrania como objetivo.

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 311/2022, DE 3 DE MAYO, QUE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD.

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

2022, un año marcado por la guerra

LA INVASIÓN DE UCRANIA LLEVADA A CABO POR RUSIA HA TENIDO UN PROFUNDO IMPACTO EN LAS OPERACIONES DEL CIBERESPACIO, NO SÓLO POR LAS CAMPAÑAS INVOLUCRADAS DIRECTAMENTE EN EL CONFLICTO, SINO TAMBIÉN POR LA UTILIZACIÓN DE LA TEMÁTICA EN NUMEROSAS CAMPAÑAS DE PHISHING. SIN EMBARGO, AL MARGEN DE ESTE CONFLICTO, TAMBIÉN HAN COPADO LA ACTUALIDAD OTRAS CUESTIONES RELATIVAS AL CIBERESPACIO; SE DETALLAN A CONTINUACIÓN LAS MÁS RELEVANTES.

Inteligencia artificial

La publicación de ChatGPT 3.5 por parte de la empresa OpenAI provocó una repercusión mediática muy importante, llevando a todo tipo de público a interactuar directamente con la inteligencia artificial. Según OpenAI, ChatGPT obtuvo 1 millón de usuarios sólo 5 días después de su lanzamiento en noviembre de 2022. Dentro del ámbito de la seguridad de la información se identificaron rápidamente las posibilidades de la inteligencia artificial, tomando mucha relevancia las capacidades de desarrollo, tanto de capacidades ofensivas como defensivas, si bien es cierto que a los pocos días muchas funcionalidades fueron bloqueadas con el objetivo de que la tecnología no fuera utilizada con fines dañinos.

Sin embargo, la publicación de ChatGPT sólo apunta a ser el inicio de la participación de la inteligencia artificial en la ciberseguridad, tanto por parte de los atacantes como de los defensores. A esta plataforma se unió la publicación de otras herramientas que, utilizando inteligencia artificial, generan voz, imagen o vídeo. Entre los motores podemos destacar Midjourney o Dall-E, el cual es capaz de crear imágenes con un alto grado de realismo o Whisper, el cual emula la voz humana a través de un entrenamiento con Inteligencia Artificial.

«LA PUBLICACIÓN DE CHATGPT SÓLO APUNTA A SER EL INICIO DE LA PARTICIPACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA CIBERSEGURIDAD, TANTO POR PARTE DE LOS ATACANTES COMO DE LOS DEFENSORES»

Hacktivismo

Tras la invasión rusa de Ucrania se ha podido observar una movilización del personal civil, especialmente para las campañas de hacktivismo. Estos grupos se caracterizan por formar parte previamente de redes asociadas al cibercrimen, utilizando botnets o software para la ejecución de campañas de denegación de servicio. Los grupos, movilizados a través de comunicados por Telegram, han simplificado los procedimientos técnicos para que cualquier simpatizante sea capaz de formar parte del grupo, utilizando herramientas de gran sencillez como es DDoSIA. España ha estado en el punto de mira tras los diversos gestos de respaldo a Ucrania.

Cambio de tendencia en cibercrimen

Si el pasado 2021 se comentó el incremento de malware de minado de criptomoneda derivado del aumento de la cotización, 2022 ha supuesto el caso contrario. El número de muestras se ha visto disminuido significativamente, pues en junio de 2022 el valor de Bitcoin cayó por debajo de 20.000 dólares por primera vez desde 2020, lo que supuso un duro golpe a la rentabilidad de las operaciones de cibercrimen dedicadas al minado de criptomoneda.

Sin embargo, sí que se ha visto un aumento de campañas que han tenido como objetivo la criptomoneda, destacando aquellas de Bluenoroff, de la cual se estima que pueden haberse robado más de 1.700 millones de dólares.

«LAS OPERACIONES DE RANSOMWARE HAN SEGUIDO EN AUMENTO RESPECTO A 2021 Y LAS CAPACIDADES DE POSTEXPLOTACIÓN CADA VEZ TIENEN MAYOR SOFISTICACIÓN Y AUTOMATIZACIÓN»

Sofisticación del Ransomware

Las operaciones de ransomware han seguido en aumento respecto a 2021 y las capacidades de postexplotación cada vez tienen mayor sofisticación y automatización, utilizando procedimientos y metodologías avanzadas comparable a los grupos APT de mayor madurez. Cabe destacar la aparición de la versión Lockbit3, la cual incluye capacidades de propagación muy importantes, provocando que el tiempo para la detección y respuesta a la amenaza disminuya significativamente.

También se han visto algunos de los ataques de mayor impacto por parte de grupos de ransomware. Este fue el caso de Conti y Hive en Costa Rica, el cual afectó a más de 27 entidades gubernamentales y obligó al país a declarar el estado de emergencia.

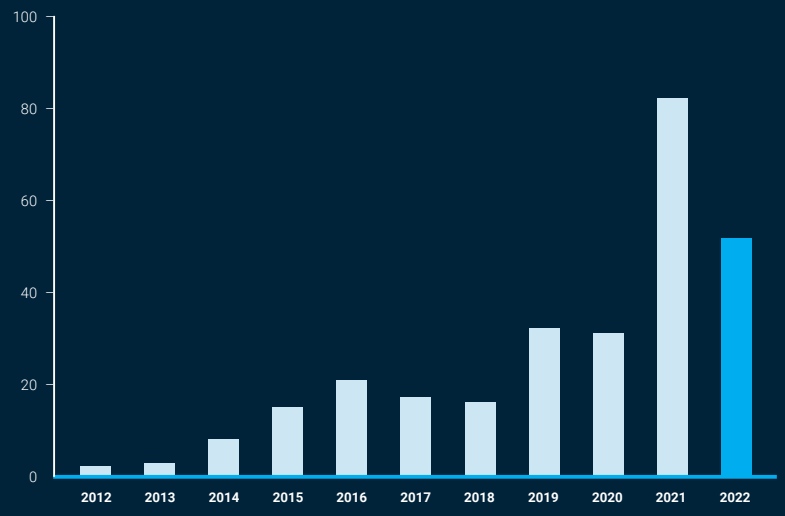
Vulnerabilidades de día 0

El número de vulnerabilidades de día 0 explotadas ha sido muy alto, si bien no alcanza las cifras récord de 2021, si alcanzan valores muy superiores a los registrados en 2020 y años anteriores[1]. Se está observando la creciente importancia dada desde los países a este tipo de vulnerabilidades, cuestión derivada de la mejora del nivel de madurez de las organizaciones.

Este tipo de amenaza supone la necesidad de incluir en la estrategia de protección de la organización la previsión de que pueden ser comprometidos sin una firma que detecte o bloquee la actividad, a través de capacidades de monitorización de Tácticas, Técnicas y Procedimientos.

[1] https://www.mandiant.com/resources/blog/zero-days-exploited-2022

ZERO-DAYS EXPLOITED 2012-2022



4

Agentes de la amenaza

2022 HA SIDO UN AÑO DONDE GRAN PARTE DE LOS ACTORES CON MAYOR ACTIVIDAD HAN LLEVADO A CABO ATAQUES DE MUY ALTA SOFISTICACIÓN. MIENTRAS QUE EN AÑOS ANTERIORES SE PODÍA OBSERVAR LA REUTILIZACIÓN DE SOFTWARE PÚBLICO O TÉCNICAS AMPLIAMENTE DESCRITAS, SE HA REGISTRADO QUE, DURANTE 2022, COMO SE DETALLARÁ POSTERIORMENTE, LOS PRINCIPALES ESTADOS HAN INVERTIDO UN GRAN NÚMERO DE RECURSOS EN IMPLEMENTAR NUEVAS HERRAMIENTAS Y METODOLOGÍAS, ASÍ COMO EN MEJORAR Y OCULTAR AQUELLAS YA CONOCIDAS. EN ESTE APARTADO SE COMENTARÁN LAS PRINCIPALES OPERACIONES REGISTRADAS, TANTO POR PARTE DE ACTORES ESTADO COMO POR PARTE DE AQUELLOS DEDICADOS AL CIBERCRIMEN.

4.1 ACTORES ESTADO

A lo largo de este punto se comentarán también los principales actores involucrados en el conflicto ucraniano, describiendo las diferentes tipologías de campañas ejecutadas a lo largo de 2022, desde acciones de ciberguerra hasta hacktivismo pasando por las campañas de ciberespionaje llevadas a cabo por APT29 o Gamaredon.

Además de los actores rusos, otros actores han realizado campañas de gran importancia, como pueden ser Mustang Panda o Lazarus, los cuales se analizarán en profundidad.

Actividad de grupos rusos durante la guerra entre Rusia y Ucrania

Se ha podido observar una diferencia de actividad y objetivos entre los diferentes grupos, con acciones de ciberespionaje, **ciberguerra** y hacktivismo.

Las acciones de **ciberguerra** dentro de las operaciones combinadas tienen el objetivo de llevar a cabo desde el plano ciber un impacto en el plano físico que forma parte de la línea de operaciones. Así, se ha podido ver la combinación de acciones en los diferentes dominios. De este modo, grupos APT como **Sandworm** y **APT28** han participado en la operación militar contra Ucrania.

En cuanto a las capacidades de **ciberespionaje**, se ha detectado la participación de prácticamente todos los grupos asociados al gobierno ruso, aunque los actores que han tenido la mayor dedicación a estas operaciones han sido **Gamaredon** y **APT29**.

«GRUPOS APT COMO SANDWORM Y APT28 HAN PARTICIPADO EN LA OPERACIÓN MILITAR CONTRA UCRANIA»

Sandworm

Sandworm es un grupo perteneciente a la Unidad 74455 del GRU y todo apunta a que se trata de la unidad dedicada al ciberespacio como dominio de las operaciones combinadas rusas[2]. Esta función estaría asociada a la realización de acciones que permitan realizar impactos sobre objetivos estratégicos ucranianos o, en su defecto, impactos sobre elementos que permitan la continuación de la línea de operaciones. Un claro ejemplo de esto se encuentra en las operaciones registradas por el CERT-UA y ESET, especialmente la de Industroyer2 contra objetivos de control industrial (ICS) o el ataque contra infraestructuras combinando el ciberataque con un ataque con misiles[3].

En esta campaña Sandworm ha utilizado diferentes códigos dañinos de tipo wiper contra bancos, entidades gubernamentales o subestaciones eléctricas que han provocado el corte de energía en Ucrania. También se ha visto afectado el sector de las comunicaciones, pues el 27 de enero se registró otro ataque de Sandworm a Ukrinform, agencia nacional de noticias de Ucrania, donde se desplegaron hasta seis *wipers* como ZeroWipe, Sdelete, AwfulShrind, BidSwipe, SwiftSlicer y, especialmente, CaddyWiper que estuvo muy presente en todo el conflicto[4].

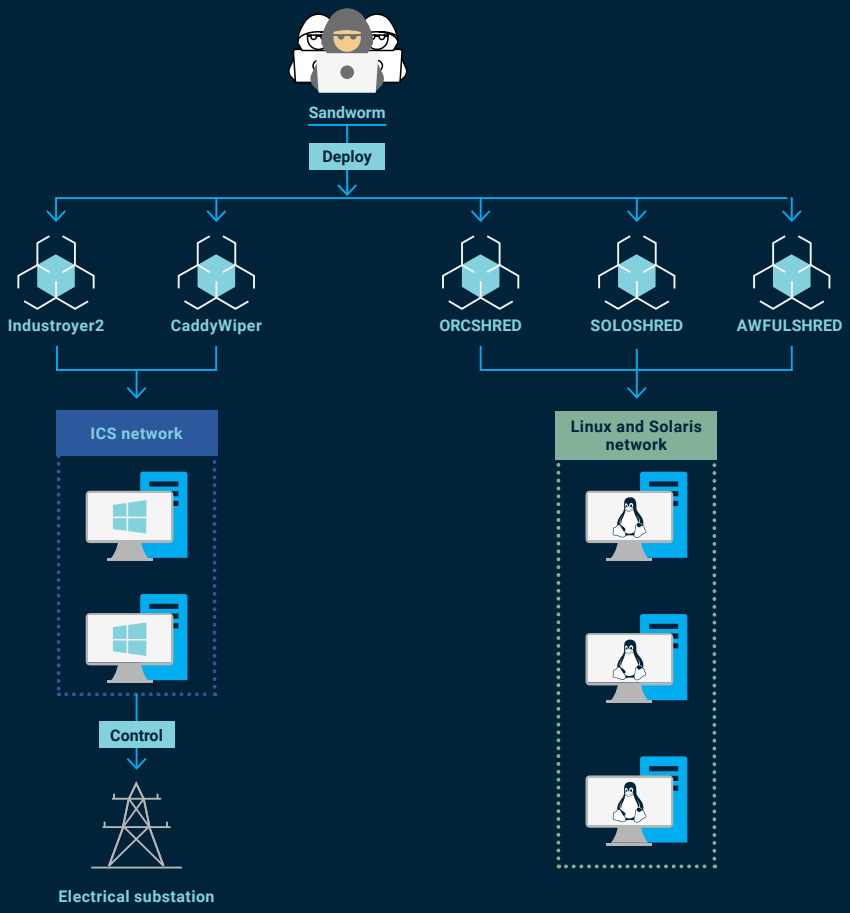
Como ejemplo de las capacidades de estos *wipers*, CaddyWiper en particular es un código dañino destructivo que borra todos los ficheros bajo la ruta C:\Users y en cualquiera de las unidades de la D: a Z:, y elimina la información en unidades físicas, incluyendo la MBR, GPT y entradas de partición.[5]

[2] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[3] https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-russian-apt-groups-including-sandworm-continue-their-attacks-against-ukraine-with-wipe/

[4] https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

[5] https://attack.mitre.org/software/S0693/



Algunas de las actividades atribuidas a Sandworm son las siguientes:

CAMPAÑAS DE WIPERS EN UCRANIA		
	23/02/2022	Ataques de los wiper HermeticWizard, Hermetic Ransom e Isaac Wiper
		Detección de wiper CyclopsBlink
	24/02/2022	Comienzo de la invasión rusa
	02/03/2022	Ataque de HermeticWiper y PartyTicket
	14/03/2022	Despliegue de CaddyWiper contra un banco ucraniano
	31/03/2022	Despliegue de AcidRain contra la comunicación satélite
	01/04/2022	Despliegue de CaddyWiper contra un banco ucraniano
	08/04/2022	Despliegue de CaddyWiper contra proveedor eléctrico

APT28

También conocido como Fancy Bear, es un grupo asociado al GRU ruso, perteneciente a la Unidad 26165 y uno de los actores con mayor actividad registrada desde su aparición, en 2004.

Según los registros, la actividad de APT28 ha tenido como objetivo principalel ciberespionaje, aunque ciertos artículos apuntan a que también ha desplegado *wipers* en ciertas campañas contra Ucrania. Sin embargo, existe una diferencia respecto a otros grupos APT, y es que el robo de información se centra especialmente en la fase de *targeting* de una operación combinada, es decir, la fase de obtención de inteligencia de cara al planeamiento de una misión multidominio[6].

Según diferentes fuentes, APT28 ha desplegado CredoMap, un stealer desarrollado en .NET a través de documentos Word que explotan la vulnerabildad de Follina (CVE-2022-30190). Para ello se hacía uso de spear phishings que usan como temática la guerra, con títulos como «*Nuclear Terrorism A Very Real Threat.rtf*», cuyo contenido apoyaba la idea de que una escalada en la tensión del conflicto ruso-ucraniano podría llevarlo a una escala nuclear[7].

También directamente asociada las hostilidades rusas contra Ucrania, Mandiant[8] reportó una campaña que utilizó el compromiso de la cadena de suministro como vector de entrada, mediante la compartición a través de plataformas de Torrent de instaladores de Windows 10 infectados en formato de ficheros ISO. En su informe se apunta a que la autoría de este ataque también podría corresponder a APT28[9].

«APT28 HA DESPLEGADO CREDOMAP, UN STEALER DESARROLLADO EN .NET A TRAVÉS DE DOCUMENTOS WORD QUE EXPLOTAN LA VULNERABILDAD DE FOLLINA»

6 https://www.nato.int/nrdc-it/magazine/2009/0911/0911d.pdf

7 https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine

8 https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government

9 https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government

Gamaredon

Gamaredon es un grupo asociado a la unidad 64829 del FSB, el cual ha tenido una actividad muy importante durante 2022. A diferencia de las funciones de Sandworm y APT28, las funciones de Gamaredon han estado más orientadas al espionaje, la contrainteligencia y las operaciones de influencia[10].

Durante la guerra, Gamaredon ha llevado a cabo un gran número de acciones contra Ucrania. En este sentido, entre los objetivos de sus campañas de phishing se encuentran los Servicios de Seguridad de Ucrania, el sector militar y el gubernamental, utilizando señuelos relacionados con la guerra y haciéndose pasar por remitentes de la Academia Nacional del Servicio de Seguridad de Ucrania.

APT29

APT29 es un actor de ciberespionaje asociado al SVR ruso, dedicado a la inteligencia exterior. APT29 es uno de los grupos con mayor actividad contra el sector gubernamental y defensa, detectando durante el año 2022 varias campañas contra personal de embajadas de la Unión Europa y OTAN[11].

En cuanto a las técnicas utilizadas, es común encontrar la utilización de phishing como vector de acceso inicial. Estos correos estarían remitidos desde cuentas legítimas de embajadas correspondiente a diferentes países aliados de la OTAN. Los phishing suelen utilizar ficheros pdf o html para la descarga de ficheros ISO, los cuales cuentan con un binario legítimo, una dll y el shellcode cifrado. La carga maliciosa tiene el objetivo de desplegar un Cobalt Strike que, tras garantizar la evasión de la seguridad y validar el equipo comprometido como de interés, terminará desplegando el payload final que llevará a cabo la exfiltración de la información.

Es interesante destacar el uso de plataformas en la nube de uso común para la exfiltración de información. Entre las más utilizadas podemos destacar Google Drive, Dropbox, Trello, Slack o Notion.

9 https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government

10 https://www.bbc.com/news/world-europe-60472889

11 https://www.securityweek.com/russia-linked-apt29-uses-new-malware-in-embassy-attacks/

En algunas de las campañas del año pasado también se ha observado la explotación de la vulnerabilidad de día 0, CVE-2022-30170. El ataque es especialmente relevante debido a esta utilización de una vulnerabilidad de día cero para la escalada de privilegios vía Credential Roaming. El fallo, parcheado por Microsoft en septiembre de 2022, permite a los atacantes tomar el control del atributo *msPKIAccountCredentials* de LDAP y, tras añadir un Roaming Token, escribir un número arbitrario de bytes en cualquier fichero del sistema[12].

Turla

Este actor, asociado al FSB ruso, es considerado como uno de los más sofisticados en cuanto a capacidades se refiere. A lo largo del año 2022 ha realizado numerosas actividades contra organismos ucranianos, especialmente a través de sus artefactos Kazuar y Capibar[13].

Capibar es un backdoor escrito en .NET distribuido a través de spear phishing y que cuenta con la capacidad de ejecutar payloads embebidos dentro de hojas de estilo XSLT. El equipo de Microsoft reportó que, además del despliegue de herramientas de recolección y exfiltración como rclone, también se ha observado su utilización como etapa previa al despliegue de Kazuar[14].

Sin embargo, Turla no sólo ha llevado actividades en Ucrania, pues tal y como publicó CISA, este actor ha seguido utilizando el implante Snake contra organismos gubernamentales y de defensa a través del despliegue de infraestructura basada en nodos P2P[15].

«A LO LARGO DEL AÑO 2022 HA REALIZADO NUMEROSAS ACTIVIDADES CONTRA ORGANISMOS UCRANIANOS, ESPECIALMENTE A TRAVÉS DE SUS ARTEFACTOS KAZUAR Y CAPIBAR»

Debido a la modularidad del implante, Snake tiene la capacidad de mantener un alto grado de confidencialidad en las acciones llevadas a cabo, utilizando piezas de información cifradas hasta su ejecución a través de un binario WerFault, también facilitado por la sofisticación implementada en fases previas. Entre los ejemplos se encuentran la rutina de desempaquetado de la segunda etapa se realiza a través de una versión modificada del software opensource JPEGView[16] o la implementación de un algoritmo de autenticación en tres pasos a través de la interceptación de las sesiones TCP a nivel de kernel.

13 https://cert.gov.ua/article/5213167

14 https://twitter.com/msftsecintel/status/1681695399084539908?s=12&t=tDVP3ULf1Ou5szxCQAKqjA

15 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

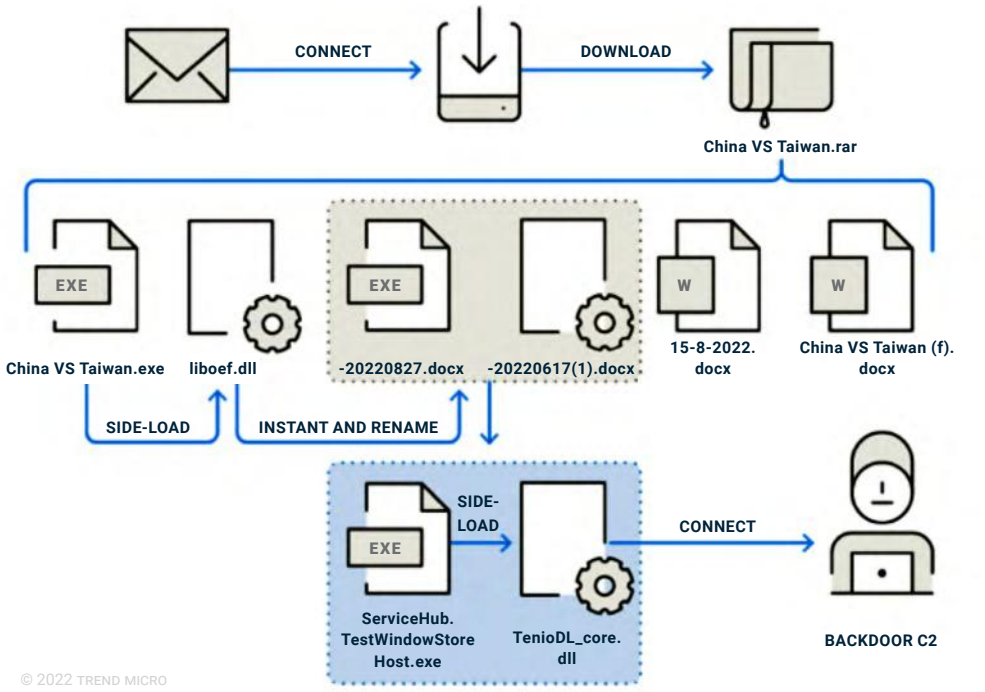
16 https://community.carbonblack.com/t5/Threat-Advisories-Documents/PNG-Dropper-Analysis/ta-p/62542

Mustang Panda

Durante 2022 ha habido un aumento de operaciones asociadas a Mustang Panda, especialmente contra organismos gubernamentales, tal y como se ha podido observar en las temáticas utilizadas en las campañas de phishing, donde gran parte de ellas suplantaban documentos de eventos diplomáticos y situaciones geopolíticas de actualidad.

Estas campañas han ido evolucionando durante el año, tanto en el acceso inicial como en los métodos empleados para el despliegue del RAT PlugX. Destacan dos formas para el acceso inicial, la propagación vía USB, técnica ya utilizada durante años anteriores, y el *spear phishing*[17].

En cuanto al despliegue de PlugX, suele comenzar con la utilización de un binario legítimo para la carga de una DLL con el código dañino. Estos binarios tienen el mismo nombre de la carpeta del phishing y han ido cambiando a lo largo de las campañas. desde binarios de antivirus como Symantec o Avast, hasta visores de código PDF[18]. Tras ello, renombran los ficheros como docx, con el objetivo de pasar inadvertidos y obtener persistencia para, finalmente, contactar con el C2 y descargar ya finalmente PlugX.



[17] https://www.avira.com/en/blog/new-wave-of-plugx-targets-hong-kong

[18] https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html

Lazarus Group

Finalmente, el último de los grupos de mayor interés es Lazarus, un grupo de origen norcoreano asociado al Reconnaissance General Bureau (RGB), concretamente al área de inteligencia extranjera.

Durante 2022 Lazarus ha estado llevando a cabo ataques contra Europa, especialmente contra la industria aeroespacial y naval, muy en la línea de lo comentado en el informe de 2021. Sin embargo, durante este año han variado ligeramente sus TTP. El acceso inicial suele ser aplicando técnicas de ingeniería social en el que, a través de un contacto vía LinkedIn, solicita la descarga de un fichero ISO ubicado en un servicio en la nube.

Una vez descargado y ejecutado un binario, ésta carga una DLL, en primer lugar legítima. Sin embargo, es la carga de una segunda DLL llevada a cabo por parte de la primera la que, finalmente, ejecuta la carga maliciosa.

Mientras que anteriormente era recurrente la suplantación de empresas como Lockheed Martin o Raytheon (dedicadas a la industria de la defensa), durante 2022 también se ha visto la suplantación de empresas del sector tecnológico como META.

«DURANTE 2022 LAZARUS HA ESTADO LLEVANDO A CABO ATAQUES CONTRA EUROPA, ESPECIALMENTE CONTRA LA INDUSTRIA AEROESPACIAL Y NAVAL»

Robo de criptomoneda

A pesar de que las acciones de cibercrimen por parte de grupos asociados al gobierno norcoreano no son una novedad, durante 2022 se este tipo de operaciones se han visto incrementadas sustancialmente. De hecho, algunas investigaciones apuntan a que, durante 2022, el grupo llegó a robar más de 1.700 millones de dólares en criptomoneda. El Departamento de Justicia de los Estados Unidos llegó a acusar a tres personas de formar parte de una trama de blanqueo de dinero asociada a estos robos[19] [20]. Todo apunta a que el grupo asociado con estas actividades es BlueNoroff, también conocido como APT38, y sería el grupo responsable de llevar a cabo acciones con motivación financiera dentro del RGB. Es necesario destacar que Corea del Norte es uno de los pocos estados que ha sido identificado ejecutando operaciones ligadas al beneficio económico directo (Operationally-motivated APT).

BlueNoroff estaría llevando a cabo ataques de tipo spearphishing, aunque también han contactado directamente con las víctimas a través de LinkedIn, WhatsApp, Discord o Twitter, del mismo modo que Lazarus. Un ejemplo es la utilización de ficheros Word para el acceso Inicial. Además, dentro de ficheros .iso o .vhd se dropean binarios legítimos o scripts legítimos, como son mshta, rundll32 o SyncAppvPublishingServer.vbs, ejecutando técnicas de bypass MOTW.

En la misma línea, también implementa funcionalidades para deshabilitar el EDR y antivirus, sobrescribiendo la sección .text de la librería ntdll precargada[21].

Con el mismo objetivo se han identificado ataques de suplantación de cadena de suministro, identificando aplicaciones de criptomoneda (en este caso QTBincoinTrader) que tienen instaladores MSI dentro del mismo, que despliega el malware AppleJeus[22].

«ALGUNAS INVESTIGACIONES APUNTAN A QUE, DURANTE 2022, EL GRUPO LLEGÓ A ROBAR MÁS DE 1.700 MILLONES DE DÓLARES EN CRIPTOMONEDA»

[19] https://www.bbc.com/news/world-asia-64494094

[20] https://www.theregister.com/2023/04/26/doj_treasury_sanctions_north_korea/

[21] https://www.ired.team/offensive-security/defense-evasion/how-to-unhook-a-dll-using-c++

[22] https://www.volexity.com/blog/2022/12/01/buyer-beware-fake-cryptocurrency-applications-serving-as-front-for-applejeus-malware/

Casos de interés de actores estado

De manera adicional a los datos expuestos en este apartado, en la siguiente tabla se describen las actividades de los grupos APT de mayor relevancia ocurridos en 2022[23]:

PRINCIPALES CAMPAÑAS DE GRUPOS APT DETECTADAS EN 2022	
GALLIUM	Actividad maliciosa utilizando la explotación de la vulnerabilidad ProxyLogon para la instalación del módulo BlackMoule, actualización de BlackMould, la cual se trataría de una webshell nativa para servidores IIS similar a ChinaChopper.
Donot	Campaña contra países del sur de Asia utilizando los frameworks Gedit y DarkMusical, los cuales se distribuían a través de phishing con adjuntos de tipo PowerPoint y RTF, respectivamente.
APT41	Campañas contra el sector del videojuego ubicadas en Corea del Sur y Taiwán. Estas campañas utilizaban variantes de PipeMon, las cuales se virtualizaban utilizando Oreans' Code Virtualizer y persistían como un procesador de impresión fuera de la ruta dedicada al procesador de impresión nativo.
APT10	Campaña del grupo chino con el malware LODEINFO, en la cual ha modificado sus TTP, utilizando un archivo SFX en lugar de un fichero Word, como se ha visto en campañas anteriores. Los principales objetivos de esta campaña son los medios de comunicación, organizaciones diplomáticas y gubernamentales, y el sector público japoneses.
OceanLotus	Durante el año 2022 se han observado campañas en las que se observa la utilización de la plataforma de hosting y desarrollo web colaborativo Glitch como servidor de C2.
UNC4191	Campaña de ciberespionaje dirigido contra empresas y organismos públicos del sudeste asiático, Europa y Estados Unidos. La infección se llevó a cabo a través de un dispositivo USB, el cual descarga malware (entre los que se encuentran MISTCLOAK, DARKDEW y BLUEHAZE), permitiendo el despliegue de una puerta trasera. La propagación del malware se lleva a cabo a través de su autoreplicación.
APT37	Campaña contra Corea del sur utilizando el backdoor Dolphin. Se trataría de una campaña especialmente dirigida donde sólo se desplegaría una vez seleccionada a la víctima tras el despliegue de malware previo. Dolphin tiene capacidades de monitorización del dispositivo, exfiltración de archivos, robo de credenciales, registro de pulsaciones de teclas o realizar capturas de pantalla.
Goblin Panda	Campaña contra organización gubernamental de la Unión Europea utilizando el backdoor TurboSlate. Este backdoor utiliza tres ficheros, la aplicación Gigabyte Technology, vulnerable a DLL search-order hijacking, el loader y el shellcode cifrado.
APT35	Campaña contra diversos sectores israelíes. Esta campaña se caracteriza por la utilización del framework open-source NorthStarC2 y la ofuscación de sus backdoors a través de ConfuserEx.
APT27	Campaña contra compañía ubicada en Hong Kong a través de un ataque a la cadena de suministro modificando una actualización. En esta campaña se pudo observar una variante del RAT PlugX.
UNC4166	También directamente asociada las hostilidades rusas contra Ucrania, Mandiant[24] reportó una campaña que utilizaba el compromiso de la cadena de suministro como acceso Inicial, infectando instaladores de Windows 10 mediante ficheros ISO que eran compartidos a través de plataformas de Torrent. Como metodologías, es interesante destacar el uso de capacidades open source. Por ejemplo, STOWAWAY para la deshabilitación de las protecciones de sistemas Microsoft[25] [26], o SPAREPART para el *parseo* de la tabla de firmware[27]. Además, el uso del script gathernetworkinfo.vbs, instalado por defecto en sistemas Windows permite la obtención de información de red del equipo donde se ejecuta.
Cloud Atlas	Rusia también ha sido objeto de acciones de ciberespionaje, como por ejemplo las que ha llevado a cabo Cloud Atlas contra Rusia, Bielorrusia y Transnitria[28]. El grupo, activo desde 2014, lleva a cabo el acceso Inicial a través de phishings dirigidos con documentos de Microsoft Office y utilizando servicios de correo como Yandex, Mail.ru o Outlook.com. Tras esto, la infección se inicia con el backdoor PowerShower, un implante utilizado en otras campañas de Cloud Atlas[29] [30], la cual dispone de capacidades de reconocimiento de proxy.

23 Se omite la actividad comentada en apartados anteriores

24 https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government

25 https://github.com/DeltoidDelta/Remove-MS-Telemetry-and-Annoyances/blob/master/remove_MS_telemetry.cmd

25 https://gist.github.com/poudyalanil/ed1a7ed5603805833ca41cbaccefe0d5

27 https://github.com/microsoft/Windows-universal-samples/blob/main/Samples/CustomCapability/Service/Client/smbios.cp

28 https://research.checkpoint.com/2022/cloud-atlas-targets-entities-in-russia-and-belarus-amid-the-ongoing-war-in-ukraine/

29 https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/

30 https://securelist.com/recent-cloud-atlas-activity/92016/

4.2 CIBERCRIMEN

El número de incidentes ligados al cibercrimen detectados durante los años de la pandemia (2020-2022) disminuyó por diferentes factores. Algunas fuentes apuntan a que esta disminución está relacionada con la interrupción de las actividades criminales debido a las restricciones, así como la falta de visibilidad sobre la actividad de los usuarios por parte de las organizaciones y la consecuente imposibilidad de identificar el número real de incidentes[31].

Durante el primer semestre de 2022 se siguieron viendo campañas de Emotet, también contra España. Fue a partir del segundo semestre donde Emotet se mantuvo sin actividad hasta noviembre, momento en el que volvió a detectarse su actividad, esta vez con algunas técnicas diferentes. Entre estas técnicas podemos encontrar la utilización de un aumento intencionado del tamaño de las muestras con el objetivo de evadir los análisis estáticos de antivirus y EDRs o la solicitud al usuario de que copie el fichero a una ruta verificada por Microsoft Office[32].

[31] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[32] https://www.proofpoint.com/uk/blog/threat-insight/comprehensive-look-emotets-fall-2022-return

4.2.1.
TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPS) MÁS OBSERVADOS

Las principales tácticas, técnicas y procedimientos (TTPs), referenciados según el estándar MITRE ATT&CK[33], observados en el mundo del cibercrimen durante el año 2022 incluían:

PRINCIPALES TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPS) EN 2022

T1588	Obtención de capacidades (malware, exploits, vulnerabilidades…)
T1587	Desarrollo de capacidades (malware, exploits, certificados digitales…)
T1190	Explotación de aplicaciones y servicios expuestos de forma pública
T1585	Establecimiento, creación y mantenimiento de cuentas en servicios del objetivo
T1591	Obtención de información de la organización víctima (roles, relaciones, etc.)
T1595	Escaneo activo de la red (vulnerabilidades, bloques de direcciones IP, etc.)
T1583	Adquisición de infraestructura (dominios, servidores DNS, VPS, botnets, ads)
T1212	Acceso a red vía explotación de credenciales comprometidas
T1133	Uso de servicios de acceso remoto para ganar acceso inicial o persistencia en red

Entre las principales técnicas utilizadas destacaban la obtención y desarrollo de capacidades técnicas por parte de los principales actores y grupos de amenaza y que incluían el uso de nuevas familias de malware (principalmente aquellas enfocadas al robo de información –stealers– y las dedicadas al cifrado y posterior extorsión de información –ransomware–) así como plataformas como servicio dedicadas a su uso en campañas de phishing o actividades de fraude bancario.

[33] https://attack.mitre.org/

La adquisición de estas capacidades o herramientas por parte de los actores y grupos de amenaza requería la presencia de estos en los principales foros, mercados y comunidades de cibercrimen disponibles, lo que permitía obtener indicadores de posibles tendencias.

La presencia de técnicas dirigidas a la obtención de información de organizaciones víctima o el escaneo activo de redes a través del análisis de la superficie de exposición de estas sugería que la motivación de un gran número de actores era principalmente oportunista. Por ello, empresas con una elevada e insegura superficie de exposición son más susceptibles de sufrir las acciones de estos actores, debido a la capacidad de estos para explotar dichas debilidades.

Además, y principalmente debido al rápido desarrollo tecnológico sufrido por las diferentes organizaciones para adaptarse a los años de pandemia (2020-2022) así como la implantación del conocido como «teletrabajo», los actores de amenaza comenzaron a explotar de forma activa aquellos servicios de acceso remoto (por ejemplo: redes virtuales privadas (VPN) como Citrix, Global Protect, Pulse Secure, etc.) o accesos a paneles web de administración expuestos de forma pública en Internet para obtener acceso inicial o mantenimiento en las redes víctima.

«LOS ACTORES DE AMENAZA COMENZARON A EXPLOTAR DE FORMA ACTIVA AQUELLOS SERVICIOS DE ACCESO REMOTO O ACCESOS A PANELES WEB DE ADMINISTRACIÓN EXPUESTOS DE FORMA PÚBLICA EN INTERNET»

4.2.2.
TENDENCIAS EN EL ÁMBITO DEL CIBERCRIMEN

Auge del malware dedicado al robo de información

El uso de familias de malware dedicadas al robo de información de los equipos víctima, también conocidos como *infostealers* o, simplemente, *stealers*, lleva siendo una actividad habitual en el mundo del cibercrimen y normalmente, las diferentes familias incluyen funcionalidades muy similares, que incluyen: la recolección de cookies, contraseñas almacenadas o datos de pago en navegadores web; el robo de credenciales de acceso a servicios de correo electrónico y cuentas de mensajería instantánea; el acceso a diferentes soluciones de software de almacenamiento e intercambio de criptomonedas o la obtención de información del sistema operativo.

Aunque existen familias de malware *infostealer* de código abierto, es habitual que los diferentes operadores ofrezcan su uso como servicio (malware-as-a-service), con diferentes opciones de alquiler a gusto de sus clientes. La notoriedad o uso de este tipo de malware depende, en gran medida, de la credibilidad y reputación de las mismas en foros de cibercrimen, por lo que sus operadores son abiertos a realizar pruebas de concepto o descuentos en sus primeros días de existencia en dichas comunidades. Los afiliados u operadores del malware *infostealer* monetizan sus compromisos a través de la venta de información o credenciales comprometidas.

Desde principios de 2022, el número de familias de malware *infostealer* anunciadas en foros de cibercrimen aumentó de forma drástica en comparación con los registros observados en 2021. Este crecimiento podría estar relacionado con la alta demanda de los actores de cibercrimen, así como el elevado beneficio de su uso. Una de las familias de este tipo de malware más conocidas, Raccoon Stealer, pausaron sus operaciones tras el inicio de la invasión de Ucrania, asegurando que uno de sus principales desarrolladores había fallecido a causa del conflicto. Este vacío en el mercado fue cubierto por otras familias como RedLine Stealer, Meta Stealer o Vidar Stealer.

Sin embargo, en junio de 2022, el principal portavoz o responsable de la administración de Raccoon Stealer volvió a aparecer en uno de los foros de cibercrimen de habla rusa más conocidos para anunciar la vuelta a las operaciones y el lanzamiento de una nueva versión.

Compromiso de información y servicios de acceso remoto

El mercado de compraventa de información comprometida continúa siendo uno de los negocios del cibercrimen más lucrativos en el panorama actual. En los últimos años, tanto los actores de amenaza reconocidos como los recién llegados al negocio han visto como dichas actividades permitían incrementar sus ganancias económicas producto de la realización de actividades ilícitas relacionadas con la venta de información confidencial y datos de carácter personal (PII) en los principales foros, mercados y comunidades de cibercrimen.

Durante el año 2022, se observó el auge de mercados de cibercrimen especializados en la venta de productos relacionados con el acceso remoto a redes corporativas. Estos mercados sirven como escaparate para operadores de malware infostealer (enfocados al robo de información de sus víctimas), donde se ofrece la venta de lotes o paquetes de credenciales para servicios de correo web (ej. Google, Outlook, Microsoft 365, etc.), servicios de entretenimiento online (ej. Apple, DAZN, Netflix, HBO, etc.), paneles de administración web (ej. cPanel) o acceso a redes corporativas vía red virtual privada (VPN) (ej. Citrix, Global Protect, Pulse Secure, etc.) o el protocolo de escritorio remoto (RDP) (ej. TeamViewer, AnyDesk, etc.).

El incremento en la venta de credenciales a servicios de acceso remoto ha permitido también establecer vínculos directos entre aquellos actores de cibercrimen implicados en su obtención (a través del uso de dichas familias de malware, su obtención en otros mercados o comunidades y posterior venta en foros de cibercrimen) con operadores o afiliados de ransomware, dedicados a su compra y posterior explotación para lograr así el cifrado de las redes comprometidas.

Dicha relación entre vendedores de accesos comprometidos a redes corporativas y operadores u afiliados de ransomware ha sido una de las más importantes en 2022, pues permitió que el negocio del ransomware se convirtiese en una «máquina de automatización» de compromisos. Se observó que los operadores de familias de ransomware conocidas limitaron el tiempo que necesitaban dedicar en las primeras fases del compromiso (desarrollo de campañas de phishing para obtener y mantener acceso inicial) para operar en un modelo de «subcontratación» con los vendedores de accesos comprometidos en foros y mercados de cibercrimen.

Transición de los actores de amenaza

La gran variedad de actividades ilícitas disponibles ha permitido que algunos de los principales actores de amenaza en seguimiento modificasen su ámbito de actuación habitual, observándose su transición entre la venta de información, la venta de accesos comprometidos o su implicación en incidentes de ransomware, entre otros. Este tipo de transiciones han estado motivadas por el beneficio económico ilícito que dichos actores obtenían de sus actividades.

Regiones e industrias más afectadas

En el año 2022, Estados Unidos continuó siendo la región más afectada por actividades de cibercrimen relacionadas con brechas de información e incidentes de ransomware, seguida de cerca por Europa, donde los principales países objetivos fueron Alemania, Reino Unido, Italia, Francia y España. Se observó un incremento en la afectación de países de Asia y América Latina.

Los sectores e industrias más afectados por el negocio del cibercrimen en todo el mundo incluían: consumo y productos industriales, manufacturación, telecomunicaciones, tecnologías de la información (IT), consultoría y servicios profesionales, público y gubernamental, financiero, energía, salud y educativo–científico.

Foros, mercados y comunidades de cibercrimen

Durante el año 2022, los foros de cibercrimen que más actividades ilícitas de interés alojaron fueron los conocidos foros Exploit y XSS, de habla rusa, los ahora extintos foros de habla inglesa Raid Forums y Breached, y el foro de cibercrimen RAMP, que fue inicialmente creado para alojar contenido relacionado con el negocio del ransomware tras su prohibición en otras comunidades. Con respecto a España, el foro conocido con el nombre Nodo313 fue una de las principales comunidades que alojaron actividades ilícitas en nuestro país.

Los mercados especializados en la venta de credenciales para servicios de acceso remoto más relevantes en 2022 incluían Genesis Market y Russian Market. Otros mercados de interés fueron TwoEasy, Lufix Shop, xLeet o Olux Premium Shop, entre otros.

El uso de servicios de mensajería instantánea como Telegram sufrió un incremento exponencial, disparándose el número de grupos y canales enfocados en actividades de cibercrimen que incluían la venta de información, la venta de accesos, el alquiler de servicios de cibercrimen o actividades relacionadas con el fraude bancario. Telegram continúa siendo la aplicación de mensajería preferida por los actores de cibercrimen debido a sus funcionalidades y su capacidad de ser utilizada en múltiples dispositivos de forma sencilla. Sin embargo, el uso de otros servicios de mensajería como Tox, Matrix, Element, Session o Discord han aumentado en 2022.

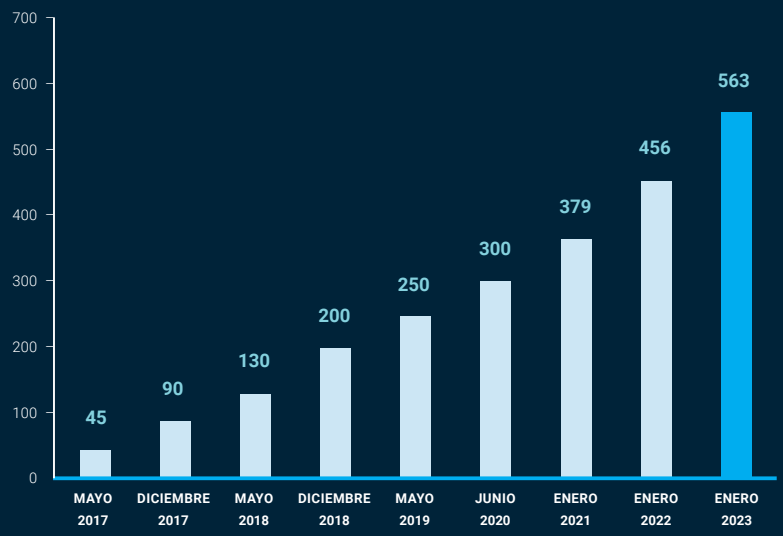
En lo relativo al uso de **Telegram**, cabe destacar que esta plataforma ya venía presentando un aumento de usuarios a lo largo de años anteriores. En consecuencia, durante 2022 y tras la invasión de Ucrania, numerosos canales se crearon para la distribución de contenido relativo al conflicto. Incluso comenzó a verse cómo varios grupos «hacktivistas» de origen prorruso, como KillNet, NoName057(16) o Anonymous Sudan, entre otros, utilizaban dicha plataforma para llevar a cabo sus comunicaciones y notificación de objetivos contra los que atacar. De igual modo, grupos como Gonjeshke Darande también habrían estado haciendo uso de esta plataforma como medio a través del cual notificar la intención de sus ciberataques. Destaca el uso de Telegram para la promoción y venta de kits de phishing, así como la capacitación del desarrollo de configuraciones personalizadas de los mismos.

Por otro lado, en el caso de Discord se estimó que para enero de 2023 la plataforma tendría aproximadamente 563 millones de usuarios registrados, lo cual suponía un aumento de más del 87% en comparación con los 300 millones de usuarios reportados en junio de 2020. En este sentido se muestra a continuación una imagen donde se puede observar ese incremento del número de usuarios durante estos últimos años.

Esta amplia utilización de **Discord** también se ha visto reflejada en el empleo que se ha hecho de la plataforma con fines dañinos. Durante una investigación llevada a cabo en 2022 se detectó que el *wiper* del malware WhisperGate (empleado en la guerra entre Rusia y Ucrania) mostró la aplicación de un fragmento de lenguaje intermedio de Microsoft (MSIL) como mecanismo de diseminación del malware, que abusaba de la red de entrega de contenido (CDN) de Discord.

«SE ESTIMÓ QUE PARA ENERO DE 2023 LA PLATAFORMA TENDRÍA APROXIMADAMENTE 563 MILLONES DE USUARIOS REGISTRADOS, UN AUMENTO DE MÁS DEL 87% EN COMPARACIÓN CON LOS 300 MILLONES DE USUARIOS REPORTADOS EN JUNIO DE 2020»

INCREMENTO DEL NÚMERO DE USUARIOS DE DISCORD
(millones de usuarios)



4.2.3.
GRUPO DE CIBERCRIMEN LAPSUS$

El grupo de cibercrimen LAPSUS$ (aka DEV-0537, UNC3661, Slippy Spider) estuvo en el radar de los investigadores de ciberseguridad desde el año 2020, ganando especial notoriedad en diciembre de 2021 cuando se atribuyó el ataque al Ministerio de Salud de Brasil.

Algunos investigadores clasifican a LAPSUS$ como un grupo de ransomware, sin embargo, no existían pruebas de que utilicen malware para cifrar datos. Las publicaciones oficiales del grupo han señalado sus actividades como «compromiso de información» y no como un despliegue de ransomware. El 22 de marzo de 2022, el equipo de detección y respuesta (DART) perteneciente al Microsoft Threat Intelligence Center (MSTIC) publicó un artículo sobre el grupo cibercriminal, señalando el uso de un modelo puro de extorsión y destrucción de información sin identificarse la implementación de cargas útiles de ransomware.

El grupo operaba principalmente en el servicio de mensajería instantánea Telegram, donde sus operadores eran responsables de varios canales de comunicación públicos donde publicaban anuncios oficiales y filtraciones de información exitosas.

El grupo mostró especial interés en la obtención de credenciales de acceso válidas para redes corporativas en el sector de las telecomunicaciones, desarrollo del software y proveedores de hosting de todo el mundo, con especial afectación en Estados Unidos y países de América Latina. El grupo también estaba interesado en ofrecer una recompensa económica a cambio de que empleados desleales –*insiders*–, facilitaran credenciales o acceso interno a sus empresas.

Sus principales técnicas incluían el uso de la ingeniería social en campañas de smishing; el SIM-Swapping; el acceso a cuentas de correo electrónico personales de empleados en organi-

zaciones objetivo; el pago a empleados desleales, proveedores o socios comerciales (insiders) de las organizaciones objetivo a cambio del acceso remoto vía uso de credenciales y la aprobación de la autenticación multifactor (MFA); así como la infiltración de sus operadores en los canales de comunicación de gestión de crisis de sus objetivos.

En marzo de 2022, el medio de comunicación BBC aseguró que la policía de la ciudad de Londres había llevado a cabo la detención de siete personas de entre 16 y 21 años en relación con una investigación sobre un grupo de cibercrimen. Todos los sospechosos fueron puestos en libertad bajo investigación.

4.2.4.
COMPROMISO DEL PUNTO NEUTRO JUDICIAL (PNJ)

En diciembre de 2022, el actor de origen nacional theskull77 aseguró disponer de un acceso comprometido al sistema de gestión de cajeros automáticos para una institución financiera en España. El seguimiento de las actividades del actor reveló que theskull77 era miembro de un grupo de cibercrimen localizado en España que también había comprometido la red interna del Punto Neutro Judicial (PNJ), perteneciente al Consejo General del Poder Judicial (CGPJ).

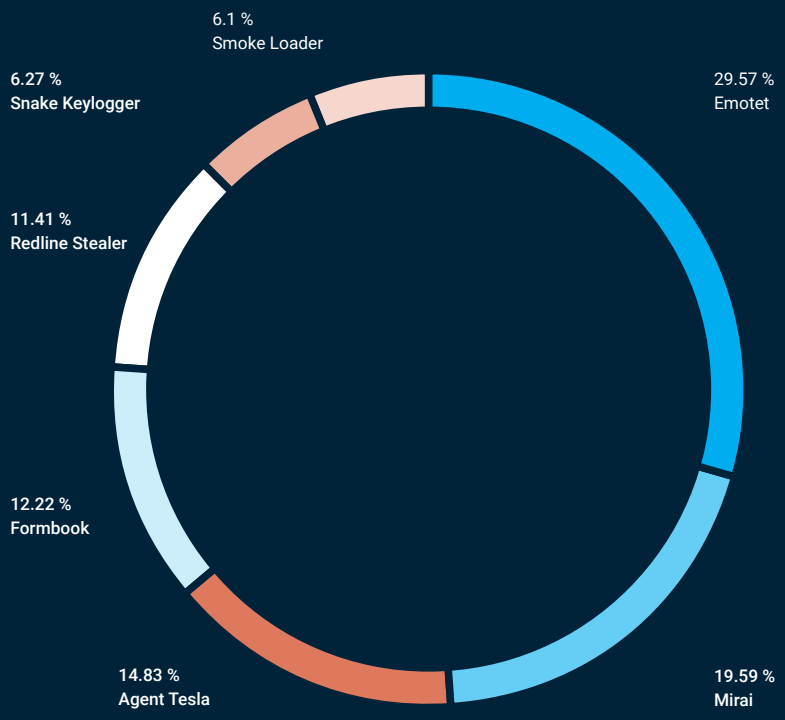
En relación con este compromiso, en marzo de 2023, la Policía Nacional española detuvo a una persona en Madrid por su presunta participación en un delito contra altas instituciones del Estado, descubrimiento, revelación de secretos (acceso ilegítimo a bases de datos) y blanqueo de capitales de manera continuada[34].

[34] https://www.interior.gob.es/opencms/eu/detalle/articulo/La-Policia-Nacional-detiene-a-un-peligroso-delincuente-informatico-que-realizo-un-ciberataque-al-Consejo-General-del-Poder-Judicial-junto-a-otras-graves-intrusiones-en-instituciones-publicas/

4.2.5.
TEMAS DE ACTUALIDAD COMO GANCHO

La utilización de temas de actualidad es una cuestión recurrente en los grupos de cibercrimen. En 2022 tuvo lugar el mundial de futbol de Catar, observándose un incremento de actividad desde diferentes tipos de grupos[35]. Se ha podido observar la venta de información asociada a dominios legítimos de la organización, la cual contenía cookies de sesión, rangos de IP y accesos utilizados en ataques como parte de la escalada de privilegios o la suplantación de identidades para campañas de Business Email Compromise (BEC)[36]. En la misma línea, también se ha observado el registro de dominios utilizando técnicas de typosquatting para la suplantación de dominios asociados con la FIFA, así como aplicaciones para dispositivos móviles catalogadas como spyware. Para más información sobre amenaza contra dispositivos móviles es recomendable la lectura del informe informe de amenazas del CCN-CERT de este año.

TOP MALWARE DETECTADO EN 2022



[35] https://www.politico.eu/article/qatar-world-cup-app-data-warning/

[36] https://socradar.io/fifa-world-cup-2022-qatar-dark-web-phishing-landscape-analysis/

Otra de las amenazas que sigue con una tendencia al alza es Mirai. Tal y como se ha comentado, algunas de las variantes de la botnet IoT está siendo utilizadas por hacktivistas, los cuales buscan el compromiso de cada vez más dispositivos, con el objetivo de causar el mayor impacto en sus víctimas. Es interesante comentar que Formbook, Redline Stealer, Snake Keylogger y Guloader están llevando a cabo campañas contra España.

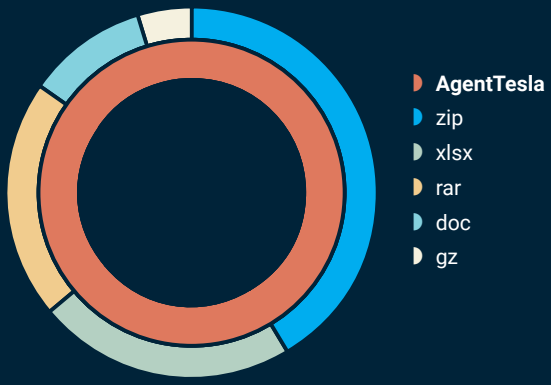
A lo largo del primer trimestre de 2022 se ha podido observar un gran número de campañas contra España y Latinoamérica, especialmente con temáticas asociadas al ámbito bancario y financiero. Es interesante destacar la proliferación de la utilización de Telegram como método de exfiltración de la información, además de la utilización de dominios dinámicos. Entre los organismos más suplantados encontramos los bancos españoles Santander, BBVA y Sabadell.

Un actor que destacar en Latinoamérica es APT-C-36, del cual se han observado campañas contra personal colombiano utilizando documentos que suplantan notas del juzgado civil. Estas notas ejecutan ficheros vbs para el despliegue del framework de post-explotación FSociety para, finalmente, desplegar la herramienta de control remoto. Estas herramientas han ido evolucionando, pues han pasado de njrat a asyncrat o limerat.

«ES INTERESANTE DESTACAR LA PROLIFERACIÓN DE LA UTILIZACIÓN DE TELEGRAM COMO MÉTODO DE EXFILTRACIÓN DE LA INFORMACIÓN, ADEMÁS DE LA UTILIZACIÓN DE DOMINIOS DINÁMICOS»

AgentTesla

AgentTesla es un malware de tipo RAT y escrito en .NET, que presenta funcionalidades de acceso remoto, además de capacidad para el robo de información sensible, keylogging o captura de pantalla y video. Este malware, activo desde 2014, ha implementado diferentes métodos a lo largo del tiempo, siendo el método más común de distribución la utilización de ingeniería social. Tanto la extensión utilizada en el phishing como la temática va variando sustancialmente entre campañas. Se puede observar una gran variedad de extensiones utilizadas en 2022, destacando .zip, .xlsx y rar.



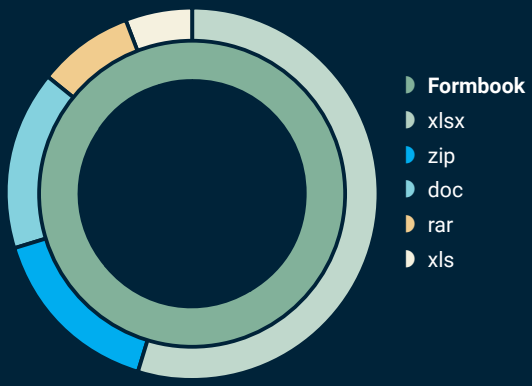
Estos son los diez nombres de fichero más utilizados por AgentTesla durante el periodo:

NOMBRE DE FICHERO	Nº MUESTRAS
SOA.exe	122
Invoice.exe	93
New Order.exe	81
Purchase Order.exe	72
PO.exe	42
SOA.zip	33
Swift Copy.exe	28
Invoice.exe	24
DHL Delivery Invoice.pdf.exe	23
Quotation.exe	23

AgentTesla utiliza métodos de suplantación generalista, tratando un objetivo de amplio alcance relacionando las temáticas con facturas, envíos u órdenes de compra.

Formbook

Formbook es un RAT diseñado para el robo de información de usuarios que lleva en activo desde 2016. Entre sus características destaca el keylogging, el robo de formularios y que se distribuye principalmente a través de phishing. De manera muy similar a AgentTesla, las dos extensiones más utilizadas por Formbook han sido xlsx y zip, aunque en este caso, más destacado el primero.

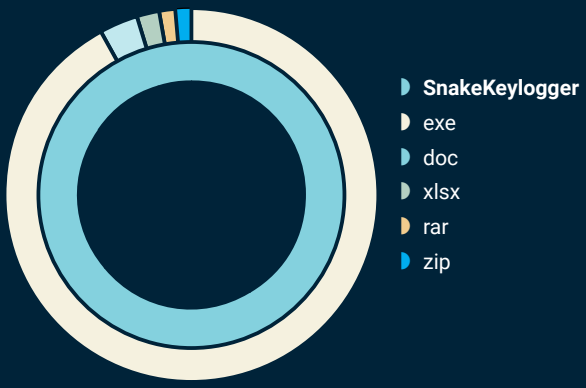


NOMBRE DE FICHERO	Nº MUESTRAS
DHL Notification_pdf.exe	64
Ziraat Bankasi Swift Mesaji.exe	64
vbc.exe	53
SOA.exe	30
Purchase Order.exe	26
PAYMENT COPY.exe	25
Quotation.exe	23
Quotation.xlsx	22
Purchase_Order.exe	18
Invoice.exe	16

En cuanto a las temáticas utilizadas, la suplantación de envíos y facturas copan las primeras posiciones, aunque destaca la suplantación del banco turco Ziraat Bankasi, así como el binario de compilación de Visual Basic.

Snake Keylogger

Snake Keylogger es un malware modular escrito en .NET que lleva en activo desde noviembre de 2020. Entre las capacidades que dispone el malware está el keylogging, el robo de credenciales, la captura de pantalla o el robo del portapapeles[37]. Snake Keylogger se propaga habitualmente a través de campañas de phishing suplantando ficheros de diversos tipos de fichero, siendo en realidad de tipo ejecutable.



De manera muy similar que las amenazas anteriores, Snake Keylogger utiliza como temática principal el ámbito financiero.

NOMBRE DE FICHERO	Nº MUESTRAS
Invoice.exe	33
file.exe	28
SOA.exe	21
Remittance Advice.exe	17
vbc.exe	17
854F1E97-5DBB-4A87-A566-33D9012B05E2 pdf.exe	14
Purchase Order.exe	13
Ödeme Detaylari.exe	13
Invoice.exe	12
e-dekont.exe	12

Utilización de archivos OneNote

A mediados de 2022 se empezó a observar la aparición de campañas utilizando la extensión .one en ficheros adjuntos a campañas de phishing, correspondientes a ficheros del software de notas de Microsoft OneNote[38].

A diferencia de Word o Excel, OneNote no tiene soporte para macros, manera en la que los actores solían ejecutar la carga maliciosa en estas aplicaciones. Sin embargo, OneNote permite a los usuarios insertar adjuntos que se ejecutarán cuando el usuario haga doble click; de esta forma, los actores hostiles están utilizando esta capacidad de OneNote para adjuntar ficheros VBS que, al iniciarse, descargan remotamente la carga maliciosa y la ejecutan.

[37] https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/snake-keylogger-malware/

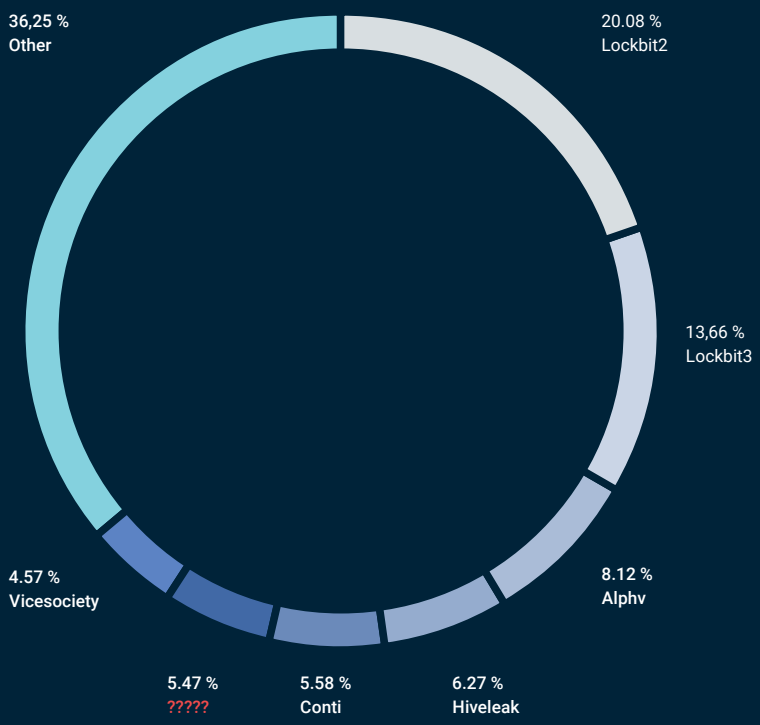
[38] https://www.bleepingcomputer.com/news/security/hackers-now-use-microsoft-onenote-attachments-to-spread-malware/

4.2.6.
RANSOMWARE

El número de ataques de ransomware se ha visto incrementado en 2022 un 42%, mientras que el total del coste de los incidentes ha disminuido respecto a 2021, pasando de 4,63 millones de dólares a 4,54[39], la frecuencia de las brechas vinculadas a ransomware se ha visto incrementada del 7,8% al 11%. Estos datos apuntan a que el número de ataques continúa aumentando año tras año, pero las empresas se encuentran cada vez mejor preparadas para dar respuesta, disminuyendo así la rentabilidad de las operaciones[40].

Tal y como se puede observar en la gráfica, los grupos de ransomware con mayor número de ataques fueron LockBit2 y LockBit3. En base a las estadísticas, LockBit ha estado detrás de 1 de cada 3 ataques de ransomware ocurridos en 2022.

TOP GRUPOS RANSOMWARE POR NÚMERO DE INCIDENTES



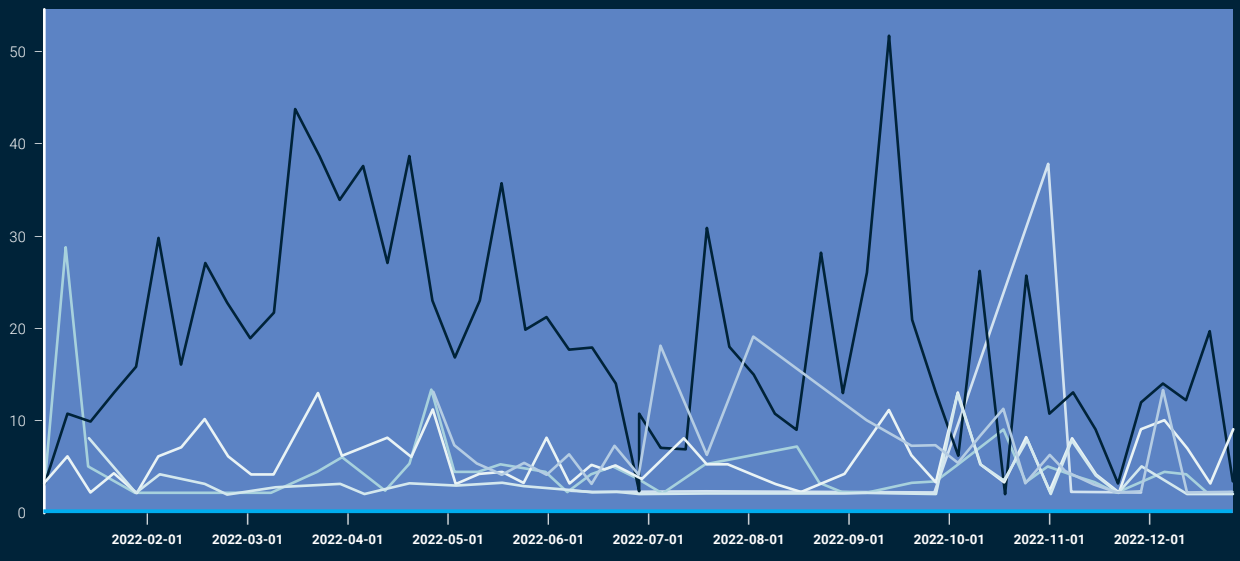
[39] El coste del ransomware contempla el coste de la detección y la pérdida de servicio

[40] https://www.bcs.org/articles-opinion-and-research/ransomware-trends-for-2022/

Junto a LockBit, los grupos con mayor número de víctimas fueron ALPHV, Hive, Conti y Vice Society, representando el 63% de los ataques de ransomware detectados durante 2022.

Observando los datos a lo largo de los meses se ven periodos de mayor o menor actividad de algunos grupos. Por ejemplo, el comienzo del año de Vice Society supera en mucho la media de ataques realizado el resto del año. Caso contrario ocurre con Cuba ransomware, cuyo pico de actividad está entre octubre y noviembre. Estos datos apuntan a que los grupos interrumpen voluntariamente sus actividades debido a evitar los focos en su actividad pues, tal y como se pudo ver con el grupo Conti, puede ejercerse una presión por parte de los servicios de seguridad de diferentes países.

EVOLUCIÓN DE ACTIVIDAD DE GRUPOS RANSOMWARE EN 2022



- alphv
- lockbit2
- vicecociety
- cuba
- blackbasta
- hiveleak
- lockbit3

LockBit ransomware

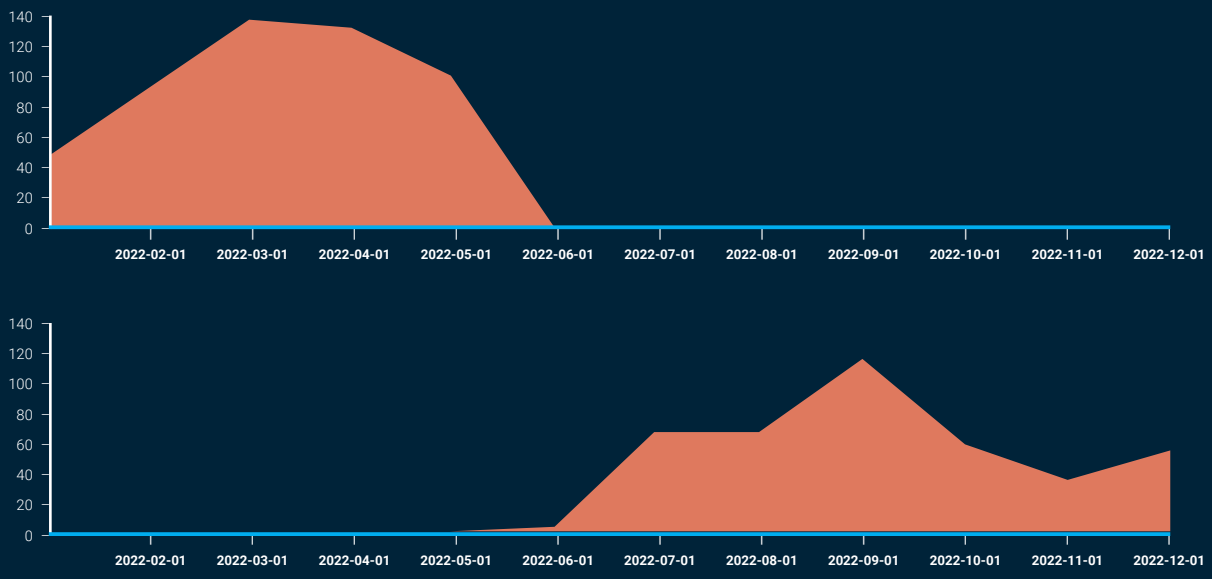
LockBit es uno de los grupos con más sofisticación dedicado al RaaS (Ransomware as a Service), lo que puede ser indicador del número de incidentes que han causado a lo largo del año. En el malware desarrollado por LockBit las fases de la post-explotación se encuentran programadas, auto propagándose por la organización y evitando la interacción manual por parte del atacante. Esta propagación se realiza después de comprometer inicialmente la red y obtener el control de alguno de los dispositivos críticos, como puede ser el controlador de dominio.

Las partes interesadas dejan un depósito para usar los ataques personalizados que se contratan y obtienen beneficios en un marco de afiliados. Los pagos del rescate se dividen entre el equipo de desarrolladores de LockBit y los afiliados, que reciben hasta el 75% de los fondos del rescate. El malware surgió por primera vez como ransomware ABCD en septiembre de 2019, mejorando hasta convertirse en una de las familias de ransomware más importantes en la actualidad.

Otra faceta de las operaciones de LockBit es la captación de afiliados. Se sabe que contrata a intermediarios para penetrar en las organizaciones, coopera con otros grupos criminales (como el ya desaparecido Maze), recluta a personas internas de la empresa y patrocina concursos clandestinos de escritura técnica para reclutar a desarrolladores con talento. Utilizando estas tácticas, LockBit se ha convertido en una de las organizaciones criminales más profesionales del panorama criminal.

En junio de 2022, el grupo dejó de operar la versión de LockBit 2.0 para pasar a utilizar LockBit 3.0, también conocido como LockBit Black, que comparte similitudes con el código de las familias de ransomware DarkSide y BlackMatter. Entre las mejoras observadas en el cambio de versión se encuentra la mejora en la modularidad y las capacidades de evasión, además de incorporar la posible configuración de diferentes tipos de compilación y el cifrado de la carga dañina hasta el momento de la ejecución, dificultando así la detección de la muestra.

EVOLUCIÓN ACTIVIDAD DE LOCKBIT2 (arriba)
VS LOCKBIT3 (abajo)



El 25 de septiembre de 2022, la red interna del Poder Judicial de Chile fue comprometida por un incidente ransomware que el equipo de respuesta a incidentes de seguridad informática del gobierno de Chile (CSIRT-CL) identificó como una variante de LockBit Black, también conocido como LockBit 3.0. Dicha familia de ransomware fue anunciado por primera vez el 27 de junio de 2022 por el actor LockBitSupp, representante del programa de afiliados de ransomware como servicio (RaaS) del grupo LockBit en los foros de cibercrimen desde septiembre de 2019.

El análisis de los indicadores de compromiso obtenidos de las notas de rescate del incidente permitió identificar que el ID del servicio de mensajería privada Tox estaba vinculado al conocido actor de amenaza Bassterlord, que previamente había sido identificado con los nombres de usuario alternativos FishEye y Editor en foros de cibercrimen de habla rusa, y cuyas actividades en dichas comunidades estaban relacionadas con la compra-venta de credenciales de acceso no autorizado a organizaciones y el despliegue de ransomware LockBit 3.0 como afiliado. El alias alternativo utilizado por el actor, FishEye, también se observó en la nota de rescate.

Incidente de Vice Society contra el CSIC

Vice Society es un grupo de ransomware activo y sofisticado, con escasa exposición pública o conocida en foros de cibercrimen y que se caracteriza por llevar a cabo ataques de ransomware de doble extorsión, cifrando los datos de los equipos de sus víctimas y publicando la información exfiltrada en su blog de víctimas. La localización del grupo era desconocida, aunque el grupo estaría formado por antiguos miembros del programa de afiliados de la familia de ransomware-as-a-service (RaaS) Five Hands, previamente conocida como Hello Kitty, organizados de forma descentralizada. Firmas de ciberseguridad aseguran que Vice Society podría tener cierta relación con el grupo de cibercrimen UNC2447, que también operaba las familias de ransomware Five Hands, Hello Kitty y vinculado por Cisco Tales al grupo de ransomware Yanluowang.

El 18 de julio de 2022, un mes antes del anuncio del compromiso en el sitio web de Vice Society, el Consejo Superior de Investigaciones Científicas (CSIC) notificó la identificación de un incidente de ciberseguridad en su red interna relacionada con el despliegue de dicho ransomware.

A lo largo de 2022, Vice Society anunció alrededor de 71 víctimas, con un pico de 17 víctimas en abril de 2022. Los países más afectados por sus actividades eran Estados Unidos, Reino Unido, Brasil y España. Instituciones gubernamentales, educativas, sanitarias y empresas de mediana dimensión eran sus principales objetivos. El análisis de las tácticas, técnicas y procedimientos (TTPs) habituales de Vice Society reveló el grupo adquiría de forma habitual credenciales comprometidas para servicios de acceso remoto de actores de amenaza implicados en su venta en foros de cibercrimen conocidos.

RansomEXX ransomware compromete el Consorcio Sanitario Integral (CSI)

El 7 de octubre de 2022, medios de comunicación reportaron que un ciberataque estaba provocando serios problemas en la red pública sanitaria de servicios del Consorcio Sanitario Integral (CSI), que se encarga, entre otros, de la gestión de numerosos hospitales en la zona. El grupo de ransomware responsable del incidente era conocido como RansomEXX, que fue observado por primera vez en 2018 bajo el nombre de Defray777 y renombrado en 2020 por la comunidad tras encontrar el string «ransom.exx» en su binario.

El grupo de ransomware estaba operado por el grupo de cibercrimen de motivación financiera GOLD DUPONT, activo desde 2018. El grupo utiliza herramientas como RansomEXX, Defray777, Cobalt Strike, Metasploit, LaZagne o Mimikatz. En sus campañas ofensivas, GOLD DUPONT utiliza otras familias de malware conocidas como Vatet Loader, PyXie RAT, IceID o TrickBot. Como principal característica, RansomEXX codificaba el nombre de la víctima en el propio binario, demostrando como sus ataques implican una preparación y adaptación a la víctima.

El vector de entrada utilizado por el grupo consistía, generalmente, en el uso de credenciales de acceso comprometido a servicios de acceso remoto (en este caso, el uso de credenciales comprometidas para el servicio de acceso remoto VPN Citrix) y campañas de spear phishing con adjuntos dañinos. Para la ejecución de sus campañas, los atacantes suelen orquestar sus acciones desde herramientas de control remoto tales como Cobalt Strike, o el software comercial Connectwise/ScreenConnect (herramienta legítima utilizada en los últimos años por diversos grupos de atacantes). En 2022, determinados grupos afiliados a RansomEXX habrían utilizado, como vía de entrada, ciertas vulnerabilidades en productos VMware ESXi para cifrar la red mediante la familia de ransomware, algo que fue observado en el incidente.

Incidente de Conti y Hive contra Costa Rica

WIZARD SPIDER es un grupo de cibercrimen activo y sofisticado, conocido originalmente por la creación y operación del malware bancario TrickBot. También se atribuyen a este grupo el uso de otros malware como servicio como Emotet o BazarLoader. El grupo también ha desplegado con éxito el ransomware Ryuk. En 2020, el grupo adoptó el sucesor de Ryuk, denominado «Conti», pasando a ser conocido por la comunidad como «Conti ransomware».

El incidente de Conti ransomware contra el gobierno de Costa Rica comenzó en abril de 2022, siendo el Ministerio de Finanzas el primer afectado y llegando a 27 las instituciones públicas afectadas, incluyendo el Ministerio de Hacienda o el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

El 8 de mayo el presidente de Costa Rica, Rodrigo Chaves, decretó el estado de emergencia nacional. Según el blog de víctimas de Conti ransomware, el grupo pedía 10 millones de dólares por el rescate de sus sistemas y amenazó con publicar la información robada del Ministerio de Hacienda. El rescate subió a 20 millones tras la negativa.

Una de las metodologías utilizada por los grupos de ransomware es la doble extorsión, llegando a solicitar a los propios ciudadanos costarricenses que instaran al gobierno el pago del rescate.

El análisis del incidente permitió identificar que el 18 de abril de 2022, un actor de cibercrimen que utilizaba el nombre unc1756, miembro del foro de cibercrimen de habla rusa Exploit.in que era utilizado por un individuo de origen ruso que había reconocido en el negocio del cibercrimen y que había formado parte de diferentes grupos de ransomware, publicó un mensaje solicitando la venta de accesos comprometidos a redes «especiales» en Costa Rica, mencionando de forma directa al Ministerio de Hacienda en Costa Rica. El nombre del actor posteriormente apareció en la publicación del blog de víctimas de Conti ransomware, confirmando su implicación como afiliado del grupo de cibercrimen. El 27 de abril de 2023, el grupo de ransomware Conti publicó un anuncio bajo el título «For Peru» donde anunciaba el compromiso de la Dirección General de Inteligencia (DIGIMIN) del Perú, que también pudo ser atribuido al actor unc1756.

Apenas un mes después de este ataque, el país recibió un segundo ataque contra sus infraestructuras, en este caso por parte del grupo Hive. Esta nueva operación tuvo como objetivo la Caja Costarricense de Seguro Social, y paralizó algunos servicios médicos debido a la imposibilidad de acceso a los servicios administrativos, incluyendo los expedientes médicos.

Cabe resaltar que la presión ejercida sobre Conti ransomware tras el ciberataque condujo al cese de la actividad del grupo en junio de 2022, el cual desconectó su infraestructura dedicada a la publicación de las brechas de información y la negociación con las víctimas. Según la información publicada, Conti ransomware no ha vuelto a realizar ningún ataque desde el 7 de junio de 2022[41].

#CONTILEAKS

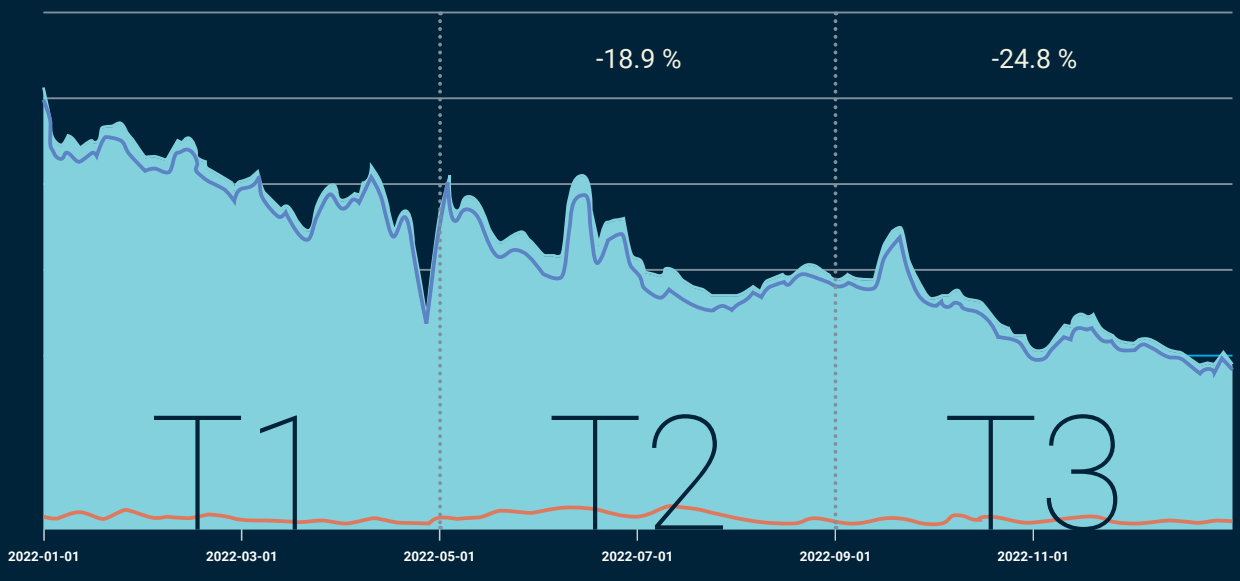
El 25 de febrero de 2022, el grupo de ransomware realizó un comunicado público asegurando estar a favor de la defensa de Rusia en el conflicto actual, amenazando a Ucrania y los países de la OTAN con tomar represalias si observaban ciberataques contra ciudadanos y organismos rusos. Dos días después, un miembro del grupo no identificado, posiblemente descontento con el anuncio político, comenzó a publicar información interna referente a información de carácter personal (PII) de los miembros del grupo, conversaciones internas, herramientas e infraestructura utilizada, etc. Dicha filtración fue conocida de forma pública con el nombre asociado #ContiLeaks. Dicho miembro también publicó información interna sobre los miembros del grupo encargados de la creación del malware bancario Trickbot. En total, información personal de alrededor de 27 posibles miembros de WIZARD SPIDER fue expuesta de forma pública en la red social Twitter. Como consecuencia, el grupo WIZARD SPIDER sufrió una desestructuración de sus equipos internos y operaciones, provocando la creación de nuevos grupos de ransomware con nombres alternativos cuyos miembros habían abandonado el uso de Conti ransomware. Otros afiliados al grupo Conti comenzaron a trabajar para otros programas de afiliados del mercado como los promocionados por LockBit o Hive ransomware, entre otros. Algunas firmas de inteligencia señalan que antiguos miembros de WIZARD SPIDER fundaron Karakurt (Karakurt Hacking Team). El análisis de las filtraciones #ContiLeaks permitió comprender la estructura interna de un grupo de ransomware, los roles de cada uno de sus miembros, los procedimientos internos a la hora de elegir futuras víctimas y llevar a cabo sus compromisos, así como la relación del grupo con actores estatales o miembros de organizaciones gubernamentales en países aliados.

[41] https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/

4.2.7.
CAÍDA DEL CRIPTOHIJACKING

Si el pasado año este tipo de amenaza se convirtió en la tipología de malware más extendido debido a la subida del valor de mercado de ciertas criptomonedas, durante 2022 ha caído por el motivo contrario, la caída en picado del valor de estas criptomonedas a mediados del pasado año. En junio cayó por debajo de 20.000 dólares por primera vez desde 2020. De esta manera, los actores detrás de la amenaza perdieron gran parte de la rentabilidad de las operaciones y, con ello, su interés en las mismas.

EVOLUCIÓN ACTIVIDAD DE MALWARE DE TIPO CRIPTOHIJACKING[44]



[44] https://www.welivesecurity.com/wp-content/uploads/2023/02/eset_threat_report_t32022.pdf

4.3 HACKTIVISMO

Se ha podido observar cómo, a lo largo de 2022, los grupos hacktivistas prorrusos han tenido una implicación directa en la guerra entre Rusia y Ucrania a través de campañas de denegaciones de servicio. Si bien es cierto que varios grupos han estado focalizados en actividades dentro de las fronteras ucranianas, otros han utilizado estos ataques como método coercitivo sobre los Estados que han participado en las ayudas con material militar o de cualquier otro tipo al gobierno de Zelensky.

«A LO LARGO DE 2022, LOS GRUPOS HACKTIVISTAS PRORRUSOS HAN TENIDO UNA IMPLICACIÓN DIRECTA EN LA GUERRA ENTRE RUSIA Y UCRANIA A TRAVÉS DE CAMPAÑAS DE DENEGACIONES DE SERVICIO»

KILLNET

El grupo operaba inicialmente como un equipo especializado en el despliegue de ataques de denegación de servicio distribuido (DDoS) que ofrecía sus servicios en foros de cibercrimen, a través del servicio de mensajería instantánea Telegram y del sitio web killnet.io, ya desaparecido. El grupo operaba la botnet «Passion Botnet», que constaba de miles de ordenadores infectados con el malware Mirai. El primer mensaje relacionado con su motivación hacktivista apareció en febrero de 2022 tras la invasión rusa de Ucrania. En marzo de 2022, el actor KillMilk supuestamente reunió al resto de operadores detrás del grupo KillNet para atacar sitios web gubernamentales en países que, según afirmaba, amenazaban a Rusia, incluyendo Letonia, Polonia, Ucrania y Estados Unidos. Desde entonces, los miembros del grupo han realizado ataques de denegación de servicio distribuido (DDoS) contra múltiples instituciones gubernamentales, medios de comunicación, empresas financieras y de telecomunicaciones en Europa. El grupo supuestamente también tenía un largo historial de asociación con otros grupos hacktivistas prorrusos que actuaría con los nombres de XakNet Team, HakNet Team y FuckNet. Además, el grupo KillNet habría unido sus fuerzas con un nuevo equipo denominado LEGION RUSSIA (aka LEGION) para realizar ataques de denegación de servicio distribuido (DDoS) conjuntos contra infraestructuras de la OTAN. El equipo LEGION RUSSIA (aka LEGION) se transformó rápidamente en lo que parecía ser la principal división encargada de este tipo de operaciones del grupo KillNet. El grupo enumeraba regularmente los miembros participantes en los ataques de denegación de servicio (DDoS) por medio de la publicación de sus nombres de usuario en Telegram, que eran limitados en comparación con el posible número de miembros del grupo, permitiendo identificar gran parte de la estructura interna del grupo. El análisis ha permitido considerar que probablemente exista un pequeño núcleo de operadores con sólidos conocimientos de técnicas de hacking y ataques de denegación de servicio y que el resto del grupo estaba formado por «script kiddies» o individuos con poca aptitud técnica. Los cinco países más atacados eran Letonia, Alemania, Rumanía, Polonia y Ucrania.

XAKNET

Se ha detectado a este actor trabajando junto con KillNet en varias ocasiones compartiendo los mismos objetivos; de hecho, ambos grupos han estado involucrados en misiones paralelas pero separadas más de una vez. Estos sucesos sugieren que existe o ha existido cierta coordinación entre ambos grupos por parte de un mismo organismo o cúpula organizadora. El actor KillMilk estuvo asociado durante mucho tiempo con el líder del equipo XakNet Team, el actor Admin_XNT, que utilizaba el alias de Telegram @xaknetru. El grupo hacktivista XakNet Team se formó poco después de que Rusia iniciara la guerra contra Ucrania a finales de febrero de 2022. Los miembros del grupo afirmaron ser un equipo de «patriotas» rusos no patrocinados, que organizaron ataques contra infraestructuras críticas y sitios web gubernamentales. Los miembros del grupo mantienen el canal de Telegram @xaknet_team y el grupo de Telegram para el chat entre miembros @membersofxaknet «XakNet. Общий чат». Las víctimas de XakNet estaban principalmente localizadas en Ucrania e incluían sitios gubernamentales y sectores estratégicos como financiero, sanidad o seguridad.

CYBER ARMY OF RUSSIA

Este grupo hacktivista está formado en su gran mayoría por patriotas rusos carentes de información técnica; no obstante, son altamente activos en el campo de las denegaciones de servicio. Su canal de Telegram cuenta con un enlace que redirige a información relativa a cómo descargar y ejecutar la herramienta que permite realizar ataques DDoS. Este actor centra sus esfuerzos mayoritariamente en organizaciones ucranianas. Al igual que XakNet, es posible que tenga cierta relación con APT28, debido a que han sido detectados filtrando información referente a compañías previamente atacadas por el grupo APT.

NONAME057(16)

NoName057(16) se detectó por primera vez en marzo de 2022, una vez iniciado el conflicto bélico entre Rusia y Ucrania. El grupo operaba como un equipo especializado en la comisión de ataques de denegación de servicio distribuido (DDoS) contra Ucrania y otros países relacionados. Desde sus inicios, NoName057(16) estuvo relacionado con los operadores detrás del grupo hacktivista prorruso KillNet, con los que se coordinaba para atacar sitios web gubernamentales en países que, según afirmaba, amenazaban a Rusia, incluyendo Austria, España, Alemania, Francia, Reino Unido, Letonia, Polonia, Ucrania y Estados Unidos, entre otros. Desde entonces, NoName057(16) han llevado a cabo ataques de manera independiente contra numerosas instituciones gubernamentales, medios de comunicación, empresas financieras, de transportes y de telecomunicaciones en

países de Europa. El grupo enumeraba regularmente las futuras víctimas de los ataques de denegación de servicio (DDoS) por medio de la publicación de los sitios web objetivo en la herramienta conocida como DDosia Project, DDosia, o simplemente Dosia, que fue desarrollado internamente y anunciada por primera vez el 15 de agosto de 2022, donde el grupo buscó reclutar un grupo experimentado para la comisión de ataques DDoS. El proyecto disponía de un grupo propio en el servicio de mensajería Telegram, donde se encontraba el código fuente de la herramienta a disposición de sus miembros, que debatían sobre el uso y próximos objetivos del grupo. Inicialmente, el análisis del grupo permitió considerar que las capacidades destructivas de sus campañas de ataques DDoS eran de menor consideración o escala que las observadas en KillNet. Sin embargo, las capacidades de NoName057(16) se vieron incrementadas a lo largo del año. A diferencia de KillNet, NoName057(16) no realiza comunicados en Telegram para animar a sus seguidores a unirse a las futuras campañas, sino que simplemente anuncia el éxito de sus compromisos una vez han sido realizados. El 14 de octubre de 2022, el grupo hacktivista prorruso NoName057(16) promocionó a través de sus canales oficial de Telegram en ruso e inglés el supuesto ataque de denegación de servicio distribuido (DDoS) llevado a cabo por miembros o voluntarios afines al grupo contra la página web principal del Ministerio de Defensa, en el sitio web defensa.gob.es. El grupo aseguró que el ataque era en represalia por el envío de armas a Ucrania por parte del gobierno de España.

También se han identificado a lo largo del conflicto a diferentes actores que apoyaban la causa ucraniana; grupos como Anonymous, Ukranian Hacktivists, o Ukranian IT Army, entre otros, han protagonizado operaciones contra intereses rusos o bielorrusos ligados al conflicto, siendo importante el uso de las plataformas Telegram y Discord en la coordinación de estos grupos.

A mediados de octubre de 2022, el actor Ziyaettin anunció un ataque de denegación de servicio distribuido (DDoS) contra el sitio web del Banco de España y del Presidente del Gobierno y el Consejo de Ministros en España, La Moncloa. El actor ofreció la venta de un acceso a un servidor de base de datos MySQL no revelado que supuestamente era operado por dicha entidad. El actor operaba un servicio botnet denominado Ziyaettin Botnet Service para la automatización de ataques DDoS bajo demanda de sus clientes o como parte de otras campañas hacktivistas.

5

¿Qué se ha visto en 2022?

5.1 TENDENCIAS EN EL CIBERCRIMEN

El negocio del ransomware continúa siendo la principal amenaza en todo el mundo y se espera que el auge de este modelo de cibercrimen siga aumentando en 2023 en comparación con lo observado en 2022. Comienza a observarse un movimiento por parte de los afiliados de grupos de ransomware de grandes dimensiones a grupos más pequeños de reciente creación, lo que sugiere que aquellos actores más prolíficos buscan desarrollar u operar sus propias familias de ransomware una vez han conseguido las nociones básicas del negocio. Por ello, se espera un aumento en el número de grupos de ransomware activos y una continuación en el número de individuos involucrados en este tipo de negocio, que se espera siga siendo dominado por grupos como LockBit o ALPHV, cuya infraestructura y estructura sugiere mayor profesionalidad.

«SE ESPERA UN AUMENTO EN EL NÚMERO DE GRUPOS DE RANSOMWARE ACTIVOS Y UNA CONTINUACIÓN EN EL NÚMERO DE INDIVIDUOS INVOLUCRADOS EN ESTE TIPO DE NEGOCIO»

Uno de los puntos más relevantes durante el año ha sido el crecimiento y movimiento de los actores entre foros, mercados y comunidades de cibercrimen. Destaca la inestabilidad en la comunidad de habla inglesa, con la apertura y cierre periódico de comunidades, algo que no se observa en la comunidad de cibercrimen de habla rusa, con foros especializados más longevos. Dichos actores buscarán aumentar sus beneficios ilícitos con aquellas actividades que sean más lucrativas en cada momento, destacando hoy en día la venta de accesos comprometidos a redes corporativas y la venta de información confidencial exfiltrada de empresas e instituciones públicas, destacando la importancia de los datos de carácter personal en este tipo de *leaks*.

Como consecuencia del auge de dichos accesos comprometidos, cada vez son más las familias de malware de tipo infostealer (especializadas en el robo de información de los equipos víctima) disponibles en el mercado. Este tipo de negocio, ofrecido como servicio, es contratado por actores de cibercrimen en foros especializados. Posteriormente, dichos actores ofrecen la venta de los datos comprometidos en mercados especializados o promocionan su consumo en grupos, canales o bots privados de Telegram a cambio de un modelo de suscripción mensual.

El movimiento hacktivista de origen prorruso continuará siendo una amenaza para los países occidentales que muestren un apoyo directo al gobierno de Ucrania, aunque se espera que el desgaste temporal asociado a una guerra provoque un descenso en la actividad observada durante los primeros meses del conflicto. La facilidad de uso o adquisición de servicios dedicados a la denegación de servicio distribuido en foros, mercados y comunidades de cibercrimen hará que actores de amenaza con menores capacidades técnicas puedan participar de estas acciones, lo que provocará además el establecimiento de otras comunidades hacktivistas.

«EL MOVIMIENTO HACKTIVISTA DE ORIGEN PRORRUSO CONTINUARÁ SIENDO UNA AMENAZA PARA LOS PAÍSES OCCIDENTALES QUE MUESTREN UN APOYO DIRECTO AL GOBIERNO DE UCRANIA»

5.2 ANÁLISIS DE ALERTAS

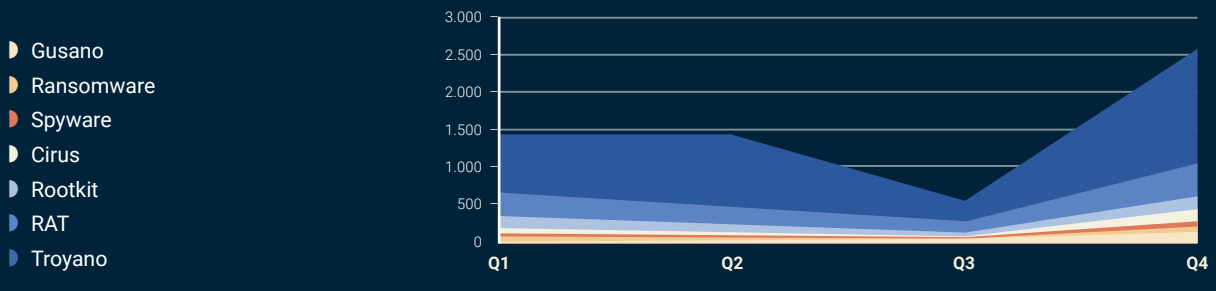
Tipología de código dañino

En las estadísticas extraídas del número de notificaciones realizadas a través del servicio de alerta temprana (SAT) del CCN-CERT, podemos comprobar que la tipología de malware utilizada por amenaza se distribuye durante el año 2022 de la siguiente manera:

TIPOLOGÍA DE MALWARE	Q1 2022	Q2 2022	Q3 2022	Q4 2022
Gusano	67	13	5	220
Ransomware	36	71	20	41
Spyware	85	58	34	179
Virus	151	116	70	162
Rootkit	3	0	0	4
RAT	308	246	132	453
Troyano	786	916	279	1513

Tal y como se puede observar, el número de incidentes detectados ha crecido durante el año, especialmente a lo que se refiere a Troyanos y RATs, habiendo una tendencia al alza a lo largo del año. Esta misma tendencia se pudo observar en las estadísticas del año 2021.

EVOLUCIÓN TIPOLOGÍA MALWARE DETECTADO POR EL SISTEMA DE ALERTA TEMPRANA DEL CCN-CERT



5.3 VULNERABILIDADES

A lo largo del informe se ha comentado el amplio impacto que han tenido las vulnerabilidades críticas durante el año 2022. En este apartado se comentarán las principales publicadas durante el año, así como el detalle de aquellas con mayor impacto en los sistemas de información.

Tendencias de vulnerabilidades 2022

Las vulnerabilidades críticas no desaparecerán del panorama de la amenaza en el futuro cercano y se espera que la explotación de aquellas vulnerabilidades con afectación a servicios de acceso remoto sean las más explotadas por los actores de cibercrimen y grupos de ransomware. Este tipo de operadores continuará buscando vulnerabilidades en servicios y aplicaciones expuestas de forma pública a Internet. Como consecuencia, empresas e instituciones públicas deberán enfrentarse a actualizaciones periódicas de sus soluciones de software para evitar riesgos. Se ha observado la identificación de un menor número de vulnerabilidades, pero de mayor impacto.

Vulnerabilidades más explotadas

Las vulnerabilidades más explotadas en los ataques durante el año 2022 han sido las siguientes:

TOP 10 VULNERABILIDADES MÁS EXPLOTADAS	
ZeroLogon (CVE-2020-1472)	Esta vulnerabilidad permite a un atacante no autenticado, con acceso de red a un controlador de dominio, establecer una sesión Netlogon vulnerable y, eventualmente, obtener privilegios de administrador de dominio. La vulnerabilidad es especialmente grave ya que el único requisito para una explotación exitosa es la capacidad de establecer una conexión con un controlador de dominio.
ICMAD (CVE-2022-22536)	Mediante la explotación de esta vulnerabilidad, un actor hostil puede ejecutar funciones haciéndose pasar por la víctima o envenenar cachés Web intermediarias. Una explotación exitosa podría comprometer completamente la confidencialidad, integridad y disponibilidad del sistema. Los equipos afectados son SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53 y SAP Web Dispatcher.
ProxyLogon (CVE-2021-26855)	Vulnerabilidad en Microsoft Exchange que permite a un atacante evitar la autenticación y suplantar al administrador en cualquier servidor Exchange con el puerto 443 abierto.
Spring4Shell (CVE-2022-22965)	Vulnerabilidad que permite la ejecución remota de código en versiones 5.3.0 a 5.3.17, 5.2.0 a 5.2.19 y versiones posteriores del framework Spring de Java. Esta vulnerabilidad es de especial importancia debido a que el 60% de los desarrolladores utilizan este framework en sus aplicaciones Java[45].
Atlassian Confluence Vulnerability (CVE-2022-26134)	Esta vulnerabilidad crítica permite la ejecución remota de código sin autenticación. Así un atacante no autenticado podría ejecutar código arbitrario en una instancia de Confluence Server o Data Center. Este CVE era una vulnerabilidad activa en todas las versiones de Confluence Servers y Data Center antes de la distribución de una versión parcheada.
VMware vSphere (CVE-2021-21972)	Vulnerabilidad contra el plugin de vCenter Server que permite a un atacante con visibilidad sobre el puerto 443 explotar sin autenticación una serie de comandos en los sistemas operativos alojados. Grupos como Memento han utilizado esta vulnerabilidad para desplegar campañas de ransomware.
Google Chrome (CVE-2022-0609)	Publicada el 4 de abril de 2022, permite a un atacante explotar una corrupción de memoria a través de una página HTML corrupta, permitiendo utilizar valores no esperados por la aplicación o la ejecución de código.
Follina (CVE-2022-30190)	Vulnerabilidad de la herramienta Microsoft Windows Support Diagnostic Tool (MSDT), la cual puede ser explotada a través de documentos de Microsoft Office. Un gran número de atacantes están utilizando esta vulnerabilidad como método de acceso inicial a la red objetivo a través de campañas de phishing.
PetitPotam (CVE-2021-36942)	Vulnerabilidad que permite la explotación el control completo de un dominio con AD CS (Active Directory Certificate Service). El objetivo del ataque es engañar a un equipo de Windows para que se autentique contra otro a través de LSARPC. La explotación exitosa significa que el servidor destino realizará la autenticación NTLM a un servidor arbitrario, teniendo la capacidad de realizar cualquier acción sobre el dominio.

[45] https://www.dynatrace.com/news/blog/anatomy-of-spring4shell-vulnerability/

Vulnerabilidades más explotadas

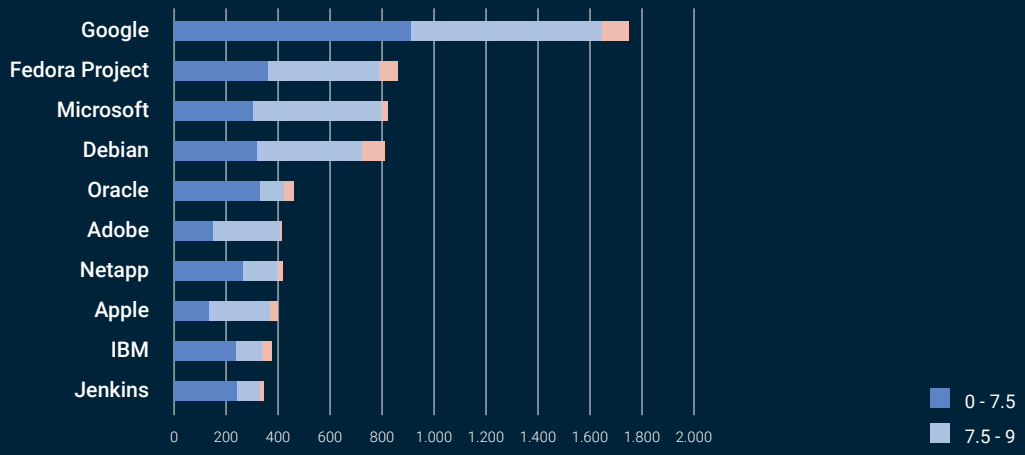
Las vulnerabilidades más explotadas en los ataques durante el año 2022 han sido las siguientes:

TRIMESTRE/ INFORMACIÓN	CVE	ALCANCE	SOFTWARE AFECTADO
ENERO - MARZO	CVE-2022-22965	Vulnerabilidad que permite la Ejecución Remota de Código en aplicaciones Spring MVC o Spring WebFlux que se ejecutan en JDK 9+	Spring MVC o Spring WebFlux
	CVE-2022-1040	Vulnerabilidad de omisión de autenticación en el portal de usuarios y Webadmin permite a un atacante remoto ejecutar código en Sophos Firewall.	Sophos Firewall todas las versiones hasta 18.5.3
ABRIL - JUNIO	CVE-2022-30190	Vulnerabilidad que permite la Ejecución Remota de Código arbitrario a través de aplicaciones como Word. El exploit aprovecha los gestores de URL de Microsoft integrados para activar el proceso msdt.exe.	Windows 7, 8.1 y 10, 11.
	CVE-2022-26134	Existe una vulnerabilidad de inyección OGNL que permitiría a un atacante no autenticado ejecutar código arbitrario en una instancia de Confluence Server o Data Center.	Atlassian Confluence Server y Atlassian Confluence Data Server versiones afectadas 1.3.0 anterior a la 7.4.17, la 7.13.0 anterior a la 7.13.7, la 7.14.0 anterior a la 7.14.3, la 7.15.0 anterior a la 7.15.2, la 7.16.0 anterior a la 7.16.4, la 7.17.0 anterior a la 7.17.4 y la 7.18.0 anterior a la 7.18.1.
	CVE-2022-0609	Vulnerabilidad de tipo "use-after-free" (UAF) que se produce después de liberar la memoria puede provocar que un programa utilice valores inesperados, corrompa datos válidos, se bloquee o ejecute código.	Versiones de Google Chrome anteriores a 98.0.4758.102
	CVE-2022-22954	VMware Workspace One Access y Identity Manager contienen una vulnerabilidad de ejecución remota de código debido a la inyección de plantillas en el lado del servidor.	VMware workspace One Access versiones 20.10.0.0, 20.10.0.1, 21.08.0.0, 21.08.0.1
	CVE-2022-1388	Vulnerabilidad en F5 BIG-IP que provoca que las solicitudes no reveladas pueden eludir la autenticación REST de iControl.	F5 BIG-IP 16.1.x versiones anteriores a 16.1.2.2, 15.1.x versiones anteriores a 15.1.5.1, 14.1.x versiones anteriores a 14.1.4.6, 13.1.x versiones anteriores a 13.1.5, y todas las versiones 12.1.x y 11.6.x

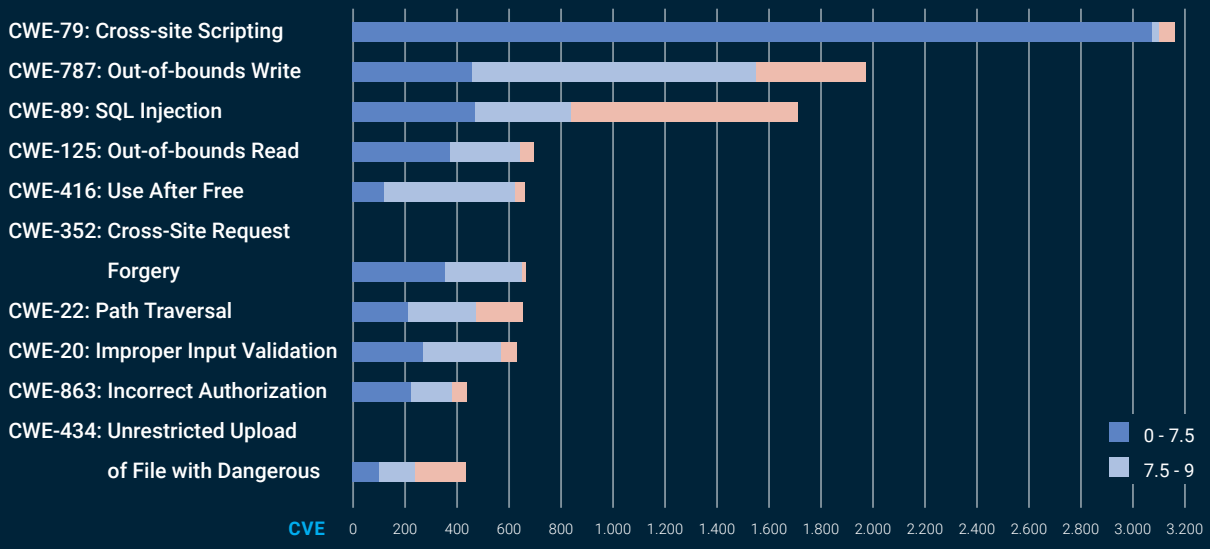
TRIMESTRE/ INFORMACIÓN	CVE	ALCANCE	SOFTWARE AFECTADO
JULIO - SEPTIEMBRE	CVE-2022-22029	Vulnerabilidad de ejecución remota de código en el sistema de archivos de red de Windows	Microsoft Exchange Server 2013, 2016, 2019
	CVE-2022-34721 CVE-2022-34722	Vulnerabilidad de ejecución remota de código en las extensiones del protocolo Windows Internet Key Exchange (IKE)	Windows 7, 8.1 y 10, 11.
OCTUBRE - DICIEMBRE	CVE-2022-41080 CVE-2022-41082	Un atacante remoto autenticado puede aprovechar una vulnerabilidad de escalada de privilegios de Exchange Server (CVE-2022-41080) para obtener permiso para ejecutar PowerShell en el contexto del sistema en un endpoint OWA. A continuación, puede ejecutar código arbitrario en el sistema de destino a través de la vulnerabilidad de ejecución remota de código de Exchange Server (CVE-2022-41082).	Microsoft Exchange Server 2013, 2016, 2019
	CVE-2022-42827	Un problema de escritura fuera de los límites permite la ejecución de código arbitrario con privilegios del kernel.	Versiones anteriores a iOS 15.7.1, iPadOS 15.7.1, iOS 16.1 y iPadOS 16

Vulnerabilidades por proveedor

Si se analizan las vulnerabilidades por proveedor, encontramos que Google es el más afectado en cuanto a número de vulnerabilidades. Sin embargo, la proporción de vulnerabilidades de alto impacto es mucho menor que en otros entornos tecnológicos, como pueden ser Debian o Fedora, el cual incluye proyectos relativos a workstations o servidores, pero también de entornos IoT, cloud o de contenedores[46].



En esta gráfica se pueden observar los diferentes CWE[47] [48] divididos según la puntuación de los CVE. Podemos comprobar que, a pesar de que el Cross-site Scripting es la debilidad más común, la criticidad general de los Out-of-bounds Write y de las inyecciones SQL es mucho mayor, por lo que los desarrolladores y equipos de seguridad deberían centrarse en evitar estos fallos.



[46] https://fedoraproject.org/

[46] El CWE es un listado de tipologías de vulnerabilidades de software o hardware desarrollado por la comunidad. Permite utilizar un lenguaje común para la medición de las herramientas de seguridad y línea base para la identificación de debilidades, mitigaciones y esfuerzos de prevención.

[47] https://cwe.mitre.org/

Explotación de vulnerabilidades de día 0

Otra de las cuestiones a destacar en 2022 ha sido la cada vez mayor utilización de vulnerabilidades de día 0 por parte de los grupos estado, dado que sus objetivos cada vez tienen una mayor madurez en su seguridad y deviene necesario la utilización de acciones de mayor sofisticación. A pesar de que el número de vulnerabilidades de día 0 explotadas durante 2022 es algo menor que el de 2021, la tendencia es al alza respecto a 2020.

Analizando en profundidad estas vulnerabilidades se detecta que, en su mayoría, han sido explotada por actores de origen chino; sin embargo, también se ha observado esta utilización por parte de Lazarus y APT28.

El 32% de las vulnerabilidades de día 0 corresponden a Microsoft, mientras que le siguen Google y Apple con el 18%. Entre el resto podemos encontrar fabricantes como Fortinet, Mozilla, Sophos o Trend Micro. Esto demuestra que las vulnerabilidades asociadas a los principales sistemas operativos, así como dispositivos de seguridad o navegadores están realmente cotizadas.

Entre los casos más destacados del año 2022 se encuentran los siguientes:

RCE CRÍTICO EN FORTIOS «IN THE WILD»

Fortinet advirtió de una vulnerabilidad que abusa del desbordamiento de memoria heap que permite a un atacante no autenticado en ejecutar comandos en FortiOS SSL-VPN. Esta vulnerabilidad estaba siendo explotada activamente previamente a la notificación.

0-DAY EXPLOTADO POR APT37

El CVE-2022-41128 es una vulnerabilidad derivada de un error en el motor de scripting del lenguaje JScript9, explotado por APT37, según Microsoft[49]. La explotación requiere que una versión no actualizada de Windows visite una página web o un servidor compartido, probablemente a través de una descarga o un enlace derivado de un phishing. En ese punto, un atacante puede ejecutar código. Debido al escenario, es probable que sea utilizado en exploit kits.

APT29 CREDENTIAL ROAMING

El ataque es especialmente relevante debido a la utilización de una vulnerabilidad de día cero para la escalada de privilegios vía Credential Roaming. La vulnerabilidad fue parcheada por Microsoft en septiembre (CVE-2022-30170) y permite a los atacantes tomar el control del atributo *msPKIAccount-Credentials* de LDAP y, tras añadir un Roaming Token, escribir un número arbitrario de bytes en cualquier fichero del sistema.

[49] https://blog.google/threat-analysis-group/internet-explorer-0-day-exploited-by-north-korean-actor-apt37/

6

Novedades en los métodos de ataque durante 2022

6.1 CADENA DE SUMINISTRO

La seguridad de las grandes corporaciones cada vez se encuentra en un mayor grado de madurez y para los atacantes les resulta cada vez más complejo, por ello, tal y como se ha comentado en ediciones anteriores de este informe, han ido produciéndose cada vez más los compromisos de sus dependencias, como proveedores o librerías desarrolladas por terceros.

Entre los principales objetivos de este tipo de ataques están las librerías de Python. Así, entre los ataques sufridos durante 2022 se puede destacar el compromiso de la librería ctx o la librería PyTorch, de ML[50]. En este caso, estas operaciones tenían el objetivo de robar información sobre servicios y usuarios, destacando las claves privadas de AWS de la organización[51].

También se ha observado un aumento en la sofisticación de actividad contra la cadena de suministro a través de sistemas de control industrial (ICS). En este sentido, PIPEDREAM es el primer framework de ataque ICS multiplataforma que permite el escaneo, explotación y control de dispositivos industriales, implementando el 38% de las técnicas ICS conocidas y el 83% de las tácticas, e implementando sofisticadas capacidades para servidores OPC, Schneider Electric Modicon y PLC OMRON[52].

«ENTRE LOS ATAQUES SUFRIDOS DURANTE 2022 SE PUEDE DESTACAR EL COMPROMISO DE LA LIBRERÍA CTX O LA LIBRERÍA PYTORCH, DE ML»

[50] https://www.fortinet.com/blog/threat-research/supply-chain-attack-new-malicious-python-package-shaderz

[51] https://www.bleepingcomputer.com/news/security/popular-python-and-php-libraries-hijacked-to-steal-aws-keys/

[52] https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/

6.2 CAMPAÑAS CONTRA ENTORNOS CLOUD

Gartner ha estimado que la inversión en el despliegue de infraestructura en entornos cloud aumentará en 2023 un 20% respecto a 2022[53], convirtiéndose, cada vez más, en un objetivo de los distintos tipos de actores hostiles debido a su importancia.

Entre los riesgos que presentan estos entornos se encuentran los errores en la configuración, que son la principal causa de la mayoría de las brechas de seguridad. A modo de ejemplo, el grupo asociado a intereses norcoreanos Temp.Hermit desarrolló el artefacto CLOUDBURST, el cual despliega scripts en PowerShell a través de la herramienta cloud de gestión de endpoint Microsoft Intune[54]. También grupos de cibercrimen como 8220 Gang comprometieron más de 30.000 activos cloud[55].

6.3 BOTNET IOT

Los grupos hacktivistas prorrusos han comenzado a utilizar las botnets dentro del conflicto rusoucraniano, llevando a cabo ataques de DDoS contra organismos gubernamentales ucranianos, así como contra organismos pertenecientes a Estados que han proporcionado ayuda a Ucrania. De este modo, todo apunta a que en 2023 el malware IoT, como puede ser Mirai y sus variantes, seguirá en aumento.

En la misma línea, tal y como ya realizó APT28 con VPNFilter, es muy probable que grupos de mayor sofisticación empiecen a realizar compromisos de routers y dispositivos IoT, proporcionándoles una capa adicional entre el dispositivo infectado y la infraestructura dedicada al C2.

[53] https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

[54] https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970

[55] https://cloudsecurityalliance.org/blog/2022/08/09/from-the-front-lines-8220-gang-massively-expands-cloud-botnet-to-30-000-infected-hosts/

6.4 PARTICIPACIÓN CIVIL EN CONFLICTOS

Durante el año 2022 hemos visto la participación de personal no militar en el conflicto ruso-ucraniano. Diversos perfiles de hacktivistas se han coordinado a través de herramientas mensajería instantánea y la utilización de software de extrema sencillez con el objetivo de hacer partícipes incluso a personal no especializado en las campañas de denegación de servicio contra diversos gobiernos y organizaciones contrarios a Rusia. También encontramos a grupos y perfiles asociados al cibercrimen que han dado un respaldo a Rusia y se han puesto dispuestos a utilizar los recursos como malware, infraestructura y botnets a favor del ejército.

«ENCONTRAMOS A GRUPOS Y PERFILES ASOCIADOS AL CIBERCRIMEN QUE HAN DADO UN RESPALDO A RUSIA DISPUESTOS A UTILIZAR LOS RECURSOS COMO MALWARE, INFRAESTRUCTURA Y BOTNETS A FAVOR DEL EJÉRCITO»

7

Tendencias 2023

Nuevos métodos de guerra multidominio

La invasión de Rusia ha puesto sobre la mesa las capacidades de la guerra multidominio, llevando a cabo operaciones combinadas utilizando los métodos de guerra convencionales junto a las capacidades del ciberespacio o los UAS (Unmanned Aerial Systems, Sistemas de Vehículos Aéreos no Tripulados). De esta manera el enfrentamiento entre ejércitos ha incorporado las capacidades de C6ISR (*command, control, communications, computers, cyber-defense and combat systems and intelligence, surveillance, and reconnaissance*)[56]. El objetivo de estos sistemas es la completa integración de todas las fuentes de información provenientes de tierra, mar, aire, espacio o ciberespacio con la capacidad de inteligencia, reconocimiento y monitorización, con el objetivo de facilitar una toma de decisiones en las operaciones combinadas.

También cabe destacar el uso de la tecnología civil en el conflicto, pues durante estos meses se ha visto el uso de varios proyectos que se han integrado dentro de los sistemas de mando y control del ejército ucraniano. Un ejemplo de ello lo tenemos con eVorog, un chatbot de Telegram donde ciudadanos y colaboradores envían información e imágenes y han permitido al ejército ucraniano geolocalizar a fuerzas rusas. También Delta, mapa del territorio de operaciones que permite ubicar diferente tipo de información con el objetivo de proporcionar un análisis situacional del campo de batalla.

El conflicto ruso-ucraniano es el primer escenario donde se están poniendo a prueba estas capacidades, las cuales posiblemente se seguirán viendo en futuros conflictos.

«EL OBJETIVO DE ESTOS SISTEMAS ES LA COMPLETA INTEGRACIÓN DE TODAS LAS FUENTES DE INFORMACIÓN PROVENIENTES DE TIERRA, MAR, AIRE, ESPACIO O CIBERESPACIO CON LA CAPACIDAD DE INTELIGENCIA, RECONOCIMIENTO Y MONITORIZACIÓN»

[56] https://www.trentonsystems.com/blog/c2-c4isr-c5isr-c6isr-differences

Operaciones asociadas a actores Estado

La continuidad del conflicto entre Rusia y Ucrania y el carácter de guerra multidominio ha hecho que muchas de las capacidades a la vanguardia desarrolladas por actores asociados a intereses rusos se hayan visto en dicho escenario. Esta dinámica y por las diferentes etapas de estancamiento en el frente, es muy probable que se sigan viendo nuevas campañas y capacidades de grupos rusos durante los próximos meses. Se espera que Turla, Gamaredon, APT28 o Sandworm tengan participación directa en el conflicto, mientras que APT29 tenga como objetivos entidades gubernamentales de países que hayan manifestado su respaldo en el conflicto a Ucrania.

Sin embargo, también se espera que la temática de la guerra forme parte de campañas con un origen distinto al ruso, pues dado que muchos de los objetivos de otros grupos APT tienen un interés directo o indirecto en el conflicto, puede formar parte del gancho en campañas de phishing, tal y como se ha observado en Mustang Panda.

Por su parte, la actividad del resto de actores APT sigue siendo muy activa y seguirán intentando satisfacer las necesidades informativas o disruptivas de quienes las dirigen. En este sentido, hay un foco muy claro de muchos actores en acceder al servicio de correo electrónico expuesto a internet de las víctimas o a sus accesos remotos vía VPN/VDI, muchas veces sin la adecuada protección con un segundo factor de autenticación (2FA).

«SE ESPERA QUE TURLA, GAMAREDON, APT28 O SANDWORM TENGAN PARTICIPACIÓN DIRECTA EN EL CONFLICTO»

Utilización de vulnerabilidades de día 0

Tal y como se ha comentado a lo largo del informe, los actores de mayor sofisticación siguen utilizando vulnerabilidades de día cero como vector de entrada. Respecto a ello, tecnologías como Citrix, Fortinet o Microsoft Exchange son los objetivos de mayor interés especialmente para grupos como HAFNIUM[57], Volt Typhoon[58] o APT28[59].

[57] https://www.ccn-cert.cni.es/informes/abstracts/5753-zero-day-exchange-server-hafnium/file.html

[58] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[59] https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-outlook-zero-day-used-by-russian-hackers-since-april-2022/

Ransomware operado

Respecto al ransomware, se espera que siga en aumento el número de ataques, así como el número de grupos activos que llevan a cabo ataques de triple extorsión.

Tal y como se ha podido observar a principios de 2023, grupos como Cl0p han aumentado significativamente el número de ataques, especialmente a través de la explotación de vulnerabilidades.

Inteligencia artificial

No cabe duda de que la inteligencia artificial es una tecnología que ha venido a cambiar la manera de entender muchos de los procesos informáticos. También en el área de la seguridad de la información.

Se ha visto un aumento en integración de algoritmos no supervisados en las herramientas de seguridad, especialmente en lo relativo a la detección de amenazas aplicando análisis de clusters y redes neuronales.

Además, la idea de chat ofrecida por OpenAI ha impulsado la aplicación del Machine Learning como herramienta de soporte para analistas. De esta manera, ya se está viendo la utilización de ChatGPT (o derivados) por parte de las herramientas y servicios de seguridad en la detección de amenazas.

Sin embargo, este salto tecnológico no sólo es utilizado en la detección de amenazas, sino también por parte de los atacantes, los cuales están utilizando las capacidades de la Inteligencia Artificial para mejorar sus capacidades, pero también para ser más rápidos llevando a un nuevo nivel la automatización de los procesos.

«YA SE ESTÁ VIENDO LA UTILIZACIÓN DE CHATGPT (O DERIVADOS) POR PARTE DE LAS HERRAMIENTAS Y SERVICIOS DE SEGURIDAD EN LA DETECCIÓN DE AMENAZAS»

Actividad contra sistemas ICS

La actividad de los grupos ransomware contra sistemas de control industrial se ha visto sustancialmente aumentada durante 2022, tendencia que sigue al alza en 2023 debido al impacto económico que provoca un ataque de estas características sobre sectores como la agricultura, la logística y el transporte o la energía.

Además, también se prevé la aparición de más capacidades específicas contra ICS de más alta sofisticación. En mayo de 2023, Mandiant publicó el análisis de COSMICENERGY, un malware OT con capacidades para la interrupción del suministro eléctrico a través de la interacción con dispositivos IEC-104 y RTU[60].

Utilización de plataformas y servicios legítimos

Durante el año 2022 ya se vio un aumento significativo en la utilización de plataformas comúnmente utilizadas para la exfiltración de información, pero no sólo en los grupos APT. También en el malware asociado a cibercrimen encontramos la proliferación de muestras de Guloader o Snake Keylogger que utilizan bots de Telegram para la comunicación con el servidor de Comando y Control. La plataforma de VoIP y mensajería Discord también ha sido ampliamente utilizada por varios actores de cibercrimen debido a la facilidad por parte de los usuarios de subir ficheros a un canal y tomar un enlace del CDN de Discord, el cual puede ser utilizado por parte de cualquier usuario fuera de la plataforma para descargar el malware[61].

[60] https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response

[61] https://twitter.com/BleepinComputer/status/1189994159647711232?s=20

8

Conclusiones

A LO LARGO DE 2022 SE HA PODIDO OBSERVAR QUE EL CIBERESPACIO YA REPRESENTA UN DOMINIO DE BATALLA DE GRAN IMPORTANCIA Y DONDE LOS GRANDES ACTORES ASOCIADOS A ESTADOS ESTÁN LLEVANDO A CABO UNA INVERSIÓN MUY IMPORTANTE PARA DISPONER DE CAPACIDADES DE LA MÁS ALTA SOFISTICACIÓN, ESPECIALMENTE EN LA UTILIZACIÓN DE VULNERABILIDADES DE DÍA 0. AUNQUE DICHA MEJORA NO SÓLO SE ESTÁ LLEVANDO A CABO DESDE LOS ACTORES ESTADO, PUES EL CIBERCRIMEN TAMBIÉN ESTÁ INVIRTIENDO EN LA AUTOMATIZACIÓN DE SUS PROCESOS CON EL OBJETIVO DE MINIMIZAR EL MARGEN DE ERROR Y DISMINUIR EL TIEMPO DE COMPROMISO DE LA ORGANIZACIÓN, CON EL OBJETIVO DE AUMENTAR EL MARGEN DE BENEFICIO DE LAS CAMPAÑAS DE ATAQUE QUE LANZA.

También es de destacar la capacidad de adaptación y reorientación de las amenazas, pues se está observando, tanto la rápida integración en sus procedimientos tras la publicación de capacidades que puedan suponer un aumento en su ratio de éxito, como la migración hacia diferentes objetivos, tal y como demuestra la variabilidad del número de campañas en la minería de criptomoneda en función su valor de mercado o la utilización de temáticas de actualidad como gancho, lo que hace necesario tener en consideración el contexto económico y social del contexto internacional para una aplicación ágil de medidas de defensa y respuesta.

Por otra parte, la protección de dichos entornos cada vez adquiere mayor importancia en el contexto de la organización. La diversidad de entornos y sus diferentes características añaden complejidad a la obtención de visibilidad sobre el comportamiento para la evaluación del estado y riesgo de la infraestructura, por lo que será necesario que las organizaciones dispongan de una estrategia para afrontar los retos que ofrece las tecnologías en la nube.

Finalmente, la inclusión de nuevas capacidades de combate multidominio, así como el avance de las tecnologías de Inteligencia Artificial desarrollados en 2022 permite vislumbrar nuevas cotas de sofisticación en las capacidades contra el ciberespacio, capacidades que deberán ser implementadas dentro de los sistemas de seguridad de las organizaciones.

Es por ello por lo que existe la necesidad de desarrollo de los planes de prevención de amenazas, así como los planes de contingencia y el desarrollo de las capacidades de detección, siendo necesaria la colaboración entre los organismos públicos y privados en materia de ciberdefensa.

CCN-CERT

https://www.ccn-cert.cni.es/