NOVIEMBRE 2025

CIBER_ AMENAZAS Y TENDENCIAS

CCN-CERT **IA-04/25**

EDICIÓN 2025

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

CCN centro criptológico nacional

ccn-cert centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Fecha de Edición: Noviembre de 2025

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1.
SOBRE CCN-CERT

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN.

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 Centro Nacional de Inteligencia, 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 a 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.

Su misión es contribuir a la mejora de la ciberseguridad española.

2. RESUMEN EJECUTIVO

En 2024 se ha registrado una tendencia al alza del número de ciberataques, aumentando su actividad en más de un 75% respecto al año 2023.[1] Uno de los principales motivos del aumento del número de campañas es la integración de la Inteligencia Artificial en muchas de las etapas de la cadena de intrusión de los actores hostiles.[2]

Durante 2024, las sondas de detección de CCN-CERT registraron un total de 263.436.908 alertas, reduciéndose respecto al año 2023, cuando se registraron 1.076.403.582. Este número significativamente más bajo no se debe a una menor actividad por parte de los actores hostiles, sino a la mejora en la calibración de las reglas de seguridad y, en consecuencia, la disminución de falsos positivos.

Analizando el objetivo de las alertas, se ha identificado que el sector con mayor número de alertas es el de **"organismos gubernamentales"**. Sin embargo, esto se debe a que un gran número de sondas están instaladas en esta tipología de organización. Si se disgrega por promedio de afectación por sector, puede observarse un resultado diferente, pues son los **sectores de IT, aeroespacial y Universidad, los que reciben mayor número de alertas** por organismo, quedando organismos gubernamentales en quinta posición.

A continuación, se muestran el número de alertas media por tipo de organismo.

Cabe destacar el alto número de ataques de Denegación de Servicio que ha sufrido España durante 2024, siendo el tercer país del mundo con mayor afectación.

1. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

2. Ver Apartado 5, Tecnologías.

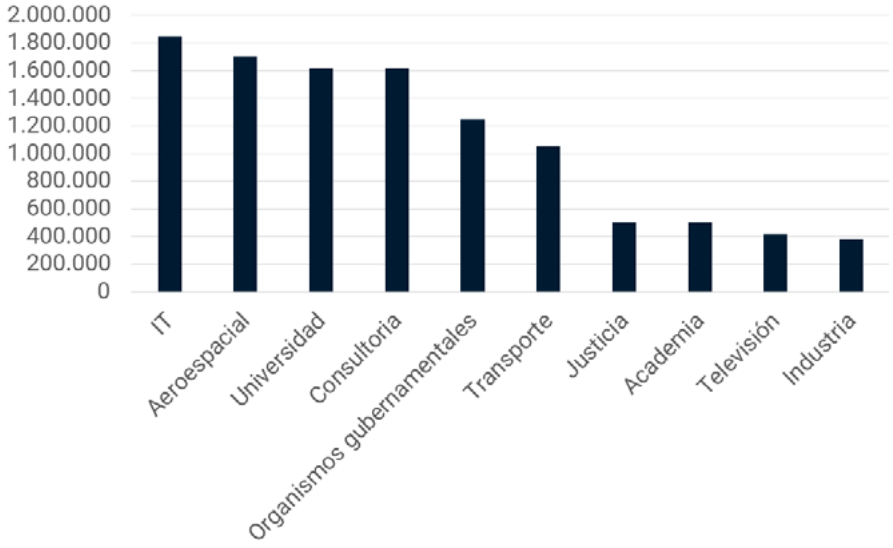


Ilustración 1: Sectores con mayor afectación promedio

Se puede observar cómo el sector IT ocupa el primer lugar en cuanto a alertas generadas, mientras que el segundo sector con mayor afectación es el sector Aeroespacial.

Cabe destacar el alto número de ataques de **Denegación de Servicio** que ha sufrido España durante 2024, siendo el tercer país del mundo con mayor afectación, centrados la mayoría de ellos en organismos gubernamentales, de transporte y financiero.

3.
ACTORES HOSTILES

3.1. ACTORES ESTADO: ATAQUE Y EXPLOTACIÓN

Se clasifican como actores estatales aquellos actores cuya motivación obedece a intereses geoestratégicos relacionados con estados. Este tipo de campañas pueden ser de espionaje (CE), de degradación, disrupción o destrucción (CA).

3.1.1. ACTORES ESTATALES RUSOS

Los actores de origen ruso han aumentado durante los últimos años el número de campañas cuyo objetivo no ha sido el robo de información sino las acciones de ataque.[3] Dentro de los grupos asociados a la Federación Rusa podemos encontrar dos tipologías claramente definidas. En primer lugar, son aquellos grupos que operan dentro de las acciones de **ciberespionaje** y cuyo foco principal es la adquisición de información (grupos asociados al FBS y al SVR). Por otra parte, están aquellos vinculados al GRU, la **inteligencia militar rusa**, la cual ha incorporado, además de las campañas de ciberespionaje habitualmente registradas, campañas contra **objetivos físicos**, considerándose parte de las operaciones combinadas, actividad que ha podido observarse especialmente en Ucrania.[4]

El GRU, la inteligencia militar rusa, ha incorporado, además de las campañas de ciberespionaje habitualmente registradas, campañas contra objetivos físicos, considerándose parte de las operaciones combinadas.

3. Computer Network Attack (CNA). Acciones realizadas mediante el uso de redes informáticas para interrumpir, denegar, degradar o destruir información residente en ordenadores y redes informáticas, o los propios ordenadores y redes mismas; desde su propia definición, las operaciones de CNA son aquellas relativas a acciones más o menos destructivas contra un objetivo.

4. https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

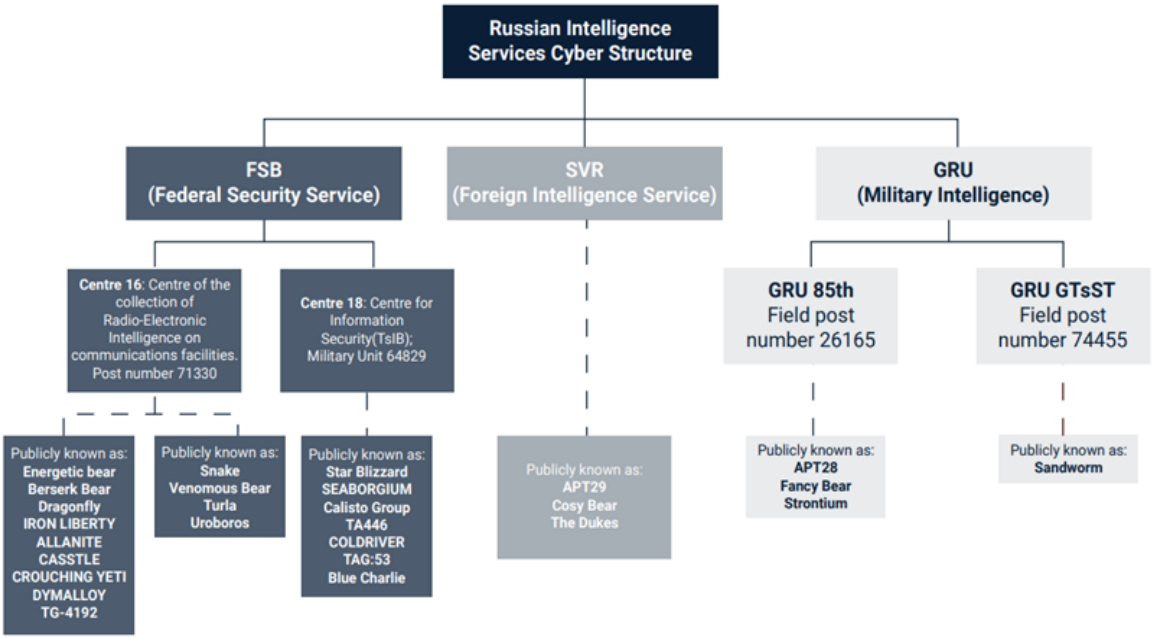


Ilustración 2: Estructura cibernética de los servicios de inteligencia rusos

Entre los grupos rusos con mayor actividad en el periodo pueden observarse los siguientes:

TURLA

Turla es un grupo de alta sofisticación asociado a Centro 16 del FSB ruso[5] y cuyas primeras campañas atribuidas se remontan hasta los años 90.[6] Ha tenido principalmente como objetivo **organismos gubernamentales, infraestructuras críticas y defensa** a través de actividad dirigida al espionaje a largo plazo. En 2024 se le han atribuido diferentes campañas, entre las que se encuentran el compromiso de Ministerios de Asuntos Exteriores europeos y entidades gubernamentales de Oriente Medio.[7]

Entre las técnicas utilizadas en 2024 por Turla cabe destacar la integración de capacidades para dificultar la atribución del grupo. Se ha detectado que este grupo ha comprometido infraestructura de **grupos APT** de otros estados para ocultar el origen del compromiso, por ejemplo, la extracción de información de Afganistán e India desde servidores de SideCopy o Transparent Tribe.[8] El mismo procedimiento se ha registrado utilizando infraestructura de malware dedicado al cibercrimen para la realización de impactos sobre organismos ucranianos.

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

6. http://greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=001OIE

7. https://www.hivepro.com/wp-content/uploads/2024/05/LunarWeb-and-LunarMail-The-Secret-Weapons-of-the-Turla-APT_TA2024191.pdf

8. https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

Entre los artefactos identificados asociados a Turla durante el periodo se encuentran LunarWeb y LunarMail.[9] Mientras que LunarWeb es un backdoor que se instala en servidores, que se comunica con el servidor de Comando y Control imitando comunicaciones legítimas, LunarMail es un RAT[10] integrado como complemento de Outlook que se instala en las estaciones de trabajo de los equipos de usuario y que, a través de la comunicación por correo electrónico, recibe comandos de los atacantes y exfiltra información. El atacante externo, a través de una cuenta de correo comprometida obtiene finalmente la información.

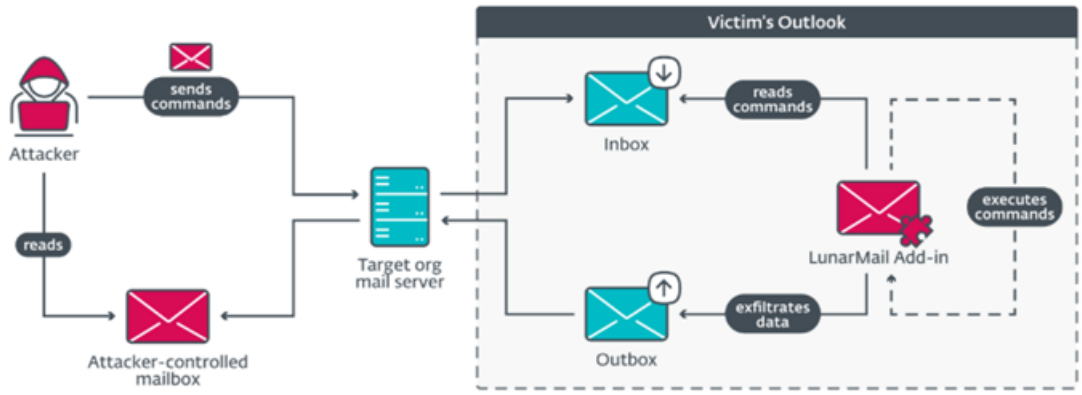


Ilustración 3: Comportamiento de LunarMail

APT28

El grupo APT28, vinculado a la Unidad Militar 26165 del Centro Principal de Servicios Especiales de la Dirección Principal de Inteligencia (anteriormente conocido como GRU) del **Estado Mayor General de Rusia.** Durante el 2024 APT28 ha realizado campañas dirigidas **contra instituciones gubernamentales, militares o infraestructuras críticas,** especialmente en el contexto de la guerra ruso-ucraniana y Polonia, aunque también han realizado campañas contra Europa, Asia Central y América del Norte, así como en países occidentales que han ofrecido apoyo a Ucrania en el conflicto, como Alemania, Francia y Estados Unidos. También se identificaron objetivos en India y en Asia Central, regiones de interés estratégico para Rusia.

En el plano operacional, el ***phishing*** ha sido la principal técnica utilizada para el acceso inicial a la red, aunque también se han empleado técnicas de fuerza bruta contra servicios expuestos públicamente. Esta estrategia permitió al grupo obtener información sensible como contraseñas, cookies, el historial de navegación y otros datos personales almacenados en navegadores como Chrome y Edge. Además, aprovechó vulnerabilidades de programas legítimos como Outlook o Windows para ejecutar el código dañino de forma silenciosa, eliminando los scripts tras su ejecución y evitando así ser detectado por los sistemas de seguridad.

---

9. https://www.welivesecurity.com/es/investigaciones/lunarweb-lunarmail-dos-backdoors-comprometieron-misiones-diplomaticas-europeas/

10. Remote Access Trojan - https://en.wikipedia.org/wiki/Remote_desktop_software#Malicious_variants

Para mantener la persistencia en los equipos infectados, utiliza técnicas como la modificación de las claves de registro, la creación de tareas programadas o el uso de archivos aparentemente legítimos para cargar malware. El **uso de servicios legítimos** como MEGA y Mockbin para comunicarse con su infraestructura de comando y control (C2), también ha sido una técnica habitualmente utilizada por APT28.

Otra de las técnicas, ha sido el ***geofencing***, utilizadas para delimitar el alcance de las víctimas en función de su ubicación geográfica y redirigir el tráfico de red a través de sistemas comprometidos con el fin de ocultar su actividad

APT29

Durante 2024, APT29, también conocido como Cozy Bear y vinculado al **Servicio de Inteligencia Exterior (SVR)** de Rusia, centró su actividad en operaciones de ciberespionaje contra entidades gubernamentales, diplomáticas, militares y corporativas en Europa, Asia y Estados Unidos. Sus acciones, alineadas con los intereses estratégicos de Rusia, buscaron recopilar inteligencia política, militar, tecnológica y económica. Sus campañas reflejaron el objetivo de obtener información estratégica relevante para el contexto internacional de Rusia, especialmente en relación con Ucrania, la OTAN y la región de Asia-Pacífico.

Sus objetivos principales han sido entidades gubernamentales y diplomáticas de Europa Occidental, especialmente de Francia, Alemania y Reino Unido, así como ONG, ministerios de defensa y entidades militares en Estados Unidos, Australia, Ucrania y Japón.

Asimismo, ha dirigido sus actividades hacia organismos de investigación, infraestructuras críticas y los sectores energético y científico de China y el Sudeste Asiático.

Entre las técnicas utilizadas por parte de APT29 se observa el empleo de **ingeniería social avanzada,** con las que consiguen que las víctimas descarguen malware de acceso remoto. Dichas acciones les permiten controlar los sistemas comprometidos, mantener el acceso sin ser detectado y continuar con la cadena de infección.

Aprovechan vulnerabilidades de software conocidas, modifican configuraciones del sistema para mantener la persistencia en los dispositivos comprometidos y utilizan herramientas legítimas, como utilidades de red y servicios en la nube, para evadir los sistemas tradicionales de seguridad y minimizar las posibilidades de ser detectados.

GAMAREDON

Gamaredon, está vinculado al **Servicio Federal de Seguridad (FSB) de Rusia.** Durante el año 2024 centró sus operaciones de ciberespionaje en instituciones militares, gubernamentales y políticas, principalmente en Ucrania, en el marco del conflicto armado con Rusia. Sus campañas han tenido como objetivo obtener inteligencia y ejercer presión sobre infraestructuras clave del Estado ucraniano, aunque también se han observado campañas contra Estados Unidos y Europa, especialmente Polonia.

Aunque tradicionalmente su actividad se ha limitado al conflicto con Ucrania, en 2024 se dirigió a otros países de la región, como Polonia, Bulgaria, Lituania y Letonia, así como hacia antiguos estados soviéticos como Uzbekistán y Kazajistán. En estos países, el grupo ha dirigido campañas contra sectores estratégicos como defensa, diplomacia, medios de comunicación y Administración pública.

En el ámbito operacional, ha llevado a cabo campañas masivas de ***phishing*** mediante correos que suplantaban la identidad de organismos oficiales ucranianos, distribuyendo malware a través de archivos en formatos como PDF y ZIP. Además, se ha observado el uso de código dañino en dispositivos Android, empleado para recolectar información sensible mediante la monitorización de SMS, llamadas, archivos multimedia y la ubicación.

Gamaredon ha empleado también herramientas legítimas del sistema operativo de Windows como powershell.exe, mshta.exe y wscript.exe para ejecutar código malicioso y poder mantener la persistencia mediante la creación de tareas programadas, scripts que se ejecutan al iniciar los dispositivos y la modificación de las claves de registro. Además, emplea distintos canales de comunicación con sus servidores de comando y control (C2), incluyendo servicios como MEGA, Telegram, Telegraph, Cloudflare Tunnels o Filetransfer.io, lo que le permite evadir mecanismos de detección.

Durante el año 2024, Gamaredon centró sus operaciones de ciberespionaje en instituciones militares, gubernamentales y políticas, principalmente en Ucrania, en el marco del conflicto armado con Rusia.

3.1.2. ACTORES ESTATALES CHINOS

A pesar de existir un gran número de actores con diferentes sets de intrusión asociados a China, pueden diferenciarse dos objetivos diferentes. Por una parte, se encuentra el **MPS (Ministry of Public Security)**, organismo dedicado a la seguridad interna del país, tal y como se puede observar en la filtración de la empresa contratista I-Soon.[11]

Por otra parte, el **MSS (Ministry of State Security)** dedicado a la inteligencia exterior y contrainteligencia, registrándose campañas en 2024 contra países occidentales y contra Oriente Medio, África o países pertenecientes al Mar de China Meridional. Entre estos grupos se encuentran Volt Typhoon, APT15, APT27 o APT41.

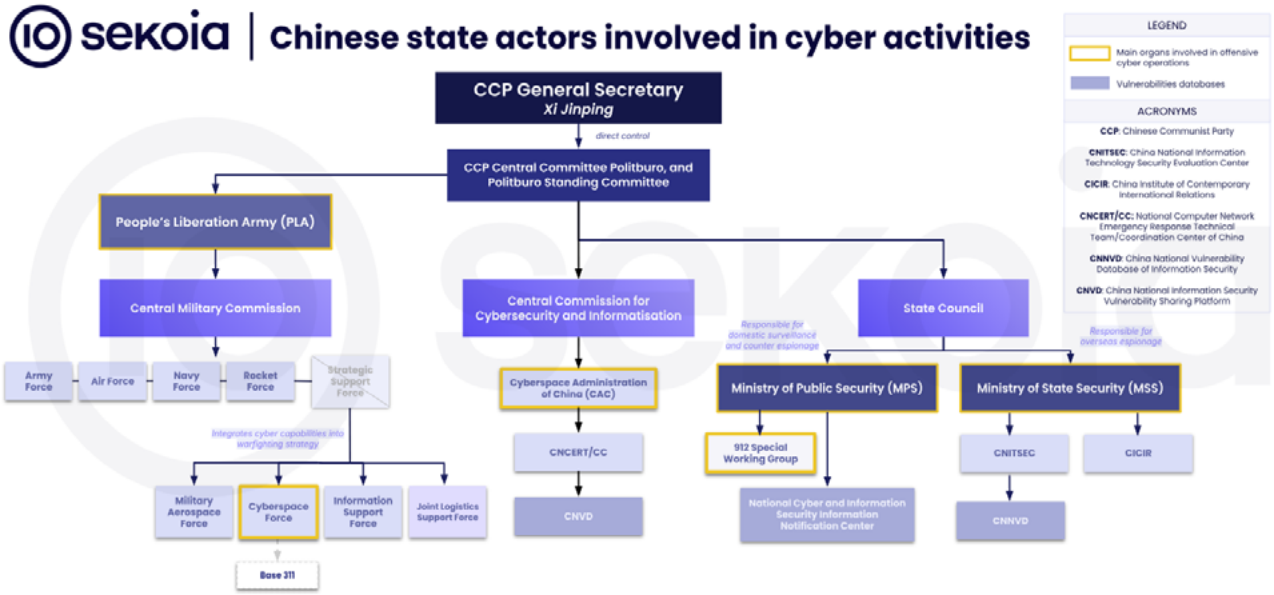


Ilustración 4: Atribución de actores asociados a China[12]

Históricamente se ha asociado la actividad de grupos de origen chino al Ejército Popular de Liberación (PLA)[13], fuerza armada controlada por el Partido Comunista Chino (PCCh). Sin embargo, diversas fuentes señalan que, desde la reforma del PLA en 2015, la actividad de los actores asociados al MSS ha aumentado significativamente, mientras que la actividad asociada al PLA ha disminuido.[14]

No cabe duda de que las técnicas utilizadas por los grupos de origen chino han sido mejoradas durante el año 2024, especialmente debido a la incorporación de las redes ORB.

---

11. https://go.recordedfuture.com/hubfs/reports/cta-2024-0320.pdf

12. https://news.risky.biz/risky-biz-news-mss-now-dominates-chinas-cyber-activity/

13. https://services.google.com/fh/files/misc/mandiant-apt1-report.pdf

14. https://t7f4e9n3.delivery.rocketcdn.me/wp-content/uploads/2024/11/A-three-beat-waltz-The-ecosystem-behind-Chinese-state-sponsored-cyber-threats.pdf

REDES ORB

Los actores cada vez incorporan capacidades de mayor sofisticación es sus tácticas, técnicas y procedimientos para dificultar la atribución. Se ha podido detectar durante el año 2024 que, especialmente los grupos de origen chino, han integrado entre sus capacidades las redes ORB (Operational Relay Box Networks).

Estas son redes formadas por **servidores VPS y dispositivos IoT comprometidos** formando una malla que permite la constante evolución a través de la integración de nuevos nodos. Este tipo de redes son administradas por entidades externas a los grupos APT, las cuales gestionan los accesos de los diferentes actores. Lo que hace que la capacidad otorgue un nuevo nivel de complejidad tanto a la detección como a la atribución, es el cambio constante de los nodos de salida, junto a la rapidez de caducidad de los mismos (con un tiempo de vida útil de alrededor de un mes). **Esto impide a las víctimas la detección y bloqueo de las amenazas a través de indicadores atómicos como direcciones IPv4**, además de dificultar la atribución a partir de su infraestructura.[15][16]

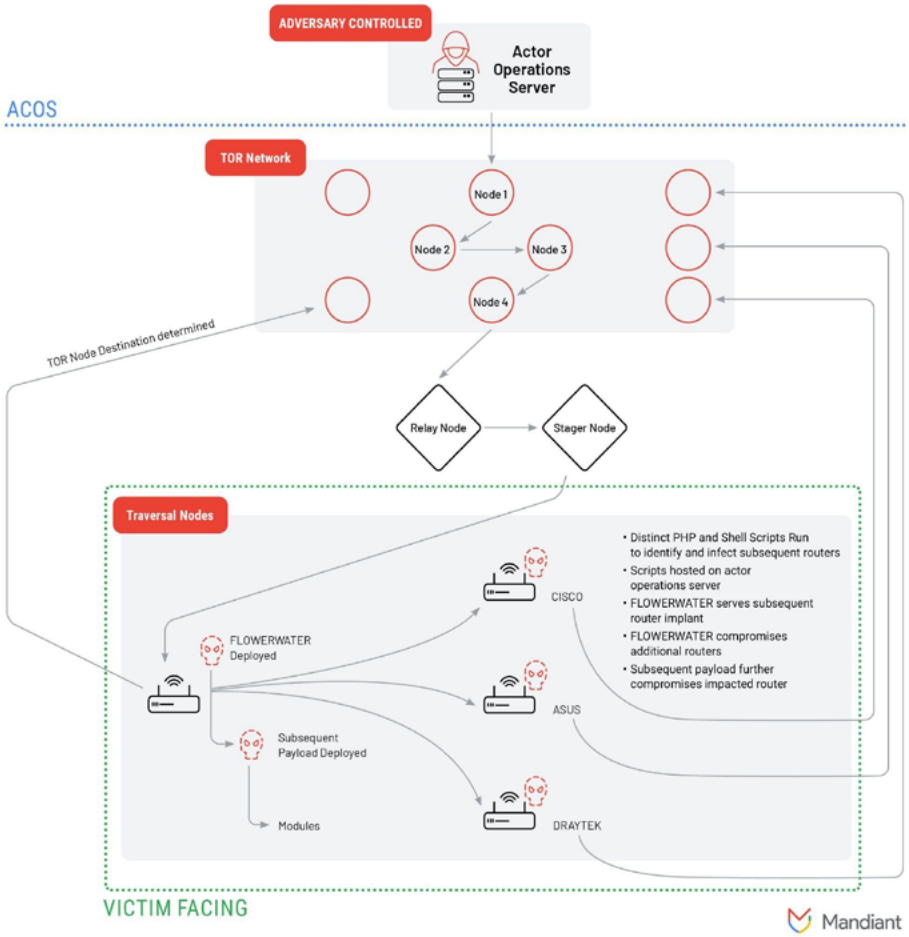


Ilustración 5: Redes ORB[17]

15. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks

16. https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/

17. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks

Cabe destacar que el código dañino orientado a dispositivos IoT no persiste tras un apagado o reinicio del dispositivo, por lo que un mismo dispositivo puede formar parte de diferentes botnets en un corto periodo de tiempo, incluso con diferentes objetivos, de ahí que el rotado de los indicadores de compromiso sea muy alto.

VOLT TYPHOON

Volt Typhoon es un grupo que tiene como principal objetivo infraestructuras críticas, telecomunicaciones, empresas de transporte, marítimo, así como contra organismos gubernamentales. Este grupo ha sido **atribuido al MSS**.[18]

Entre las técnicas observadas está la **explotación de vulnerabilidades** para el acceso inicial a la organización. Entre las más destacadas se encuentra la vulnerabilidad de día 0 **CVE-2024-39717**, que afecta a Versa Director, un software dedicado a la gestión remota de redes SD-WAN[19]. No obstante, también han utilizado vulnerabilidades de mayor antigüedad como CVE-2022-42475[20], asociado al firewall FortiGate 300D, o las que afectaban a productos Ivanti Connect Secure (CVE-2024-22024, CVE-2023-46805 y CVE-2024-21887).

Volt Typhoon ha orientado sus campañas a un **espionaje a largo plazo**, utilizando técnicas que puedan pasar desapercibidas. Esto puede observarse en su preferencia por los **ataques LOTL** (Living Off The Land), pues en la fase de postcompromiso, rara vez emplea sus propios artefactos, sino que utiliza línea de comandos u otras herramientas y procesos nativos del sistema, como cmd, netsh, nltest, netstat, ntdsutil, PowerShell, WevUtil o Wmic, entre otros.

También se han identificado el uso de herramientas forenses y de administración de red no nativas legítimas como **Magnet RAM Capture** (MRC) en controladores de dominio, para obtener un volcado de la memoria y de ahí extraer las credenciales del dominio. También se ha observado que Volt Typhoon implanta Fast Reverse Proxy (FRP) para el comando y control.

La información recopilada y exfiltrada por Volt Typhoon incluye **información crítica como diagramas y documentación relacionada con los equipos de OT**, incluidos los sistemas de control

---

18. https://www.atcorp.com/products/cyrin/newsletter/cybersecurity-volt-typhoon-and-the-grid/

19. https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation/

20. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

de supervisión y adquisición de datos (SCADA), los relés y diversos switches de control, protección y aislamiento de sistemas de energía.

Debido a las técnicas observadas, agencias estadounidenses afirman que Volt Typhoon no está llevando a cabo acciones de ciberespionaje al uso, sino que, debido a la tipología de información sustraída, apuntan a que el objetivo del actor es poder ejecutar acciones de disrupción y/o destrucción en caso de que las tensiones entre China y Estados Unidos aumenten. [21]

Además de Volt Typhoon, otros grupos con técnicas similares han sido asociados al MSS. Por ejemplo, **Flax Typhoon**, a quien se le ha atribuido la botnet Rapdor Train o **Salt Typhoon**, que ha afectado a empresas como Verizon, T-Mobile, AT&T y Lumen Technologies, y asociado a la empresa Sichuan Juxinhe Network Technology Co., LTD., motivo por el cual la empresa fue sancionada por la OFAC. [22]

Tanto a Volt Typhoon como a Flax Typhoon se le han asociado redes ORB como KV-botnet o Rapdor Train, respectivamente.[23]

SALT TYPHOON

El grupo APT de origen chino Salt Typhoon ha llevado a cabo una campaña contra distintas empresas de telecomunicaciones de países como Estados Unidos. Algunos investigadores afirman que el acceso a los sistemas duró meses, permitiendo **robar tráfico sustancial de Internet** de los **proveedores de servicios**. Los actores pudieron acceder a comunicaciones privadas, principalmente de figuras gubernamentales y políticas. Salt Typhoon es un grupo de amenazas persistentes avanzadas (APT) que se centra en actividades de ciberespionaje. Entre sus TTP más conocidas destaca el envío de ***spear-phishing*** para el acceso inicial, explotación de **vulnerabilidades zero-day, malware personalizado** y uso de infraestructura legítima.

Salt Typhoon es un grupo de amenazas persistentes avanzadas (APT) que se centra en actividades de ciberespionaje.

21. https://www.infosecurity-magazine.com/news/china-disrupt-us-infrastructure/

22. https://home.treasury.gov/news/press-releases/jy2792

23. https://breached.company/edge-wars-unpacking-the-escalating-exploitation-of-network-perimeters-in-2024/

APT15

APT15, también conocido como Ke3chang, Mirage o Nylon Typhoon, es un grupo presuntamente asociado al **MSS chino**, del cual se han observado campañas para el robo de información de organismos gubernamentales. Este actor está activo desde 2014[24] y es uno de los que registran una mayor actividad.

Durante el año 2024 se han registrado diferentes campañas, siendo una de las más destacadas el compromiso del **Ministerio de Relaciones Exteriores de Guatemala**, además de otros países de América Central[25].

Entre las técnicas identificadas para el acceso inicial destaca el uso de ***spear phishing*** suplantando dominios legítimos con cambios de TLD. Las credenciales robadas en la campaña son utilizadas para acceder a la organización a través de VPN. Para la persistencia del acceso a la organización APT15 despliega webshells en Microsoft Exchange.

Cabe destacar que APT15 también dispone de **capacidades para dispositivos móviles**, tanto iOS como Android, a través del código dañino BadBazaar, el cual fue registrado con el objetivo de rastrear actividades dentro de las comunidades tibetanas y uigur.[26]

PLUGX

Uno de los principales artefactos utilizados por los actores de origen chino es PlugX. Este es un RAT que proporciona al atacante una gran variedad de capacidades sobre el dispositivo infectado y cuyo uso se ha registrado en más de 30 campañas diferentes.[27][28]

Más de 15 grupos han utilizado en alguna de sus campañas PlugX como artefacto, todos ellos atribuidos al MSS o al PLA (anteriormente).

Entre las técnicas vistas en el despliegue del backdoor se encuentra la instalación a través de un fichero MSI o la propagación a través de dispositivos USB. Una vez desplegados los ficheros y a través de la técnica de DLL Side-Loading, el binario legítimo carga una DLL que descifra y carga, finalmente, el artefacto.

---

24. https://www.securityartwork.es/2016/06/01/apt-grupo-ke3chang/

25. https://dialogo-americas.com/articles/guatemala-us-thwart-china-spy-threat/

26. https://www.lookout.com/threat-intelligence/article/badbazaar-surveillanceware-apt15

27. https://www.darktrace.com/blog/plugx-malware-a-rats-race-to-adapt-and-survive

28. https://attack.mitre.org/software/S0013/

3.2. GRUPOS DELINCUENCIALES

Los actores considerados dentro de esta categoría son aquellos cuya motivación final no es política, sino económica, bien a través del robo o la extorsión.

3.2.1. RANSOMWARE

Entre los grupos delincuenciales, se destacan aquellos con un impacto de mayor severidad contra sus víctimas, como pueden ser los actores de ransomware. Estos grupos tienen un objetivo económico a partir de la extorsión a sus víctimas.

RANSOMHUB

RansomHub se consolidó durante 2024 como uno de los actores de **Ransomware as a Service (RaaS)** más activos, dirigiendo sus campañas contra distintos sectores críticos a nivel internacional, como telecomunicaciones, energía, salud, transporte, tecnología, educación, servicios financieros y Administraciones públicas.

En el ámbito operacional, el grupo ha utilizado correos de ***phishing*** y la **explotación de vulnerabilidades conocidas** de Citrix, Fortinet y Zerologon para obtener el acceso inicial. Además, combina distintas herramientas legítimas para evadir los sistemas de detección y poder asegurar la ejecución del código dañino. Utiliza recursos como Powershell, Mimikatz o Nmap para desactivar las defensas de los sistemas, escalar privilegios, realizar movimientos laterales y exfiltrar información.[29]

Una vez dentro de la red, interrumpe los procesos de monitoreo de seguridad mediante técnicas como EDRKillShifter, elimina registros del sistema y emplea herramientas de acceso remoto como AnyDesk o RDP para mantener el control.[30] Respecto a la exfiltración de datos, utiliza plataformas legítimas como AWS o Google Cloud, cifrando los archivos e incluyendo notas de rescate en los directorios afectados.

Europa ha sido la región más afectada por su actividad, destacando entre sus campañas la exfiltración de aproximadamente 270 GB de datos a una empresa española de telecomunicaciones, y el cifrado y exfiltración de información confidencial, además de 200 organizaciones de infraestructuras críticas y servicios esenciales, en los últimos meses de 2024.

Desde su aparición, RansomHub ha llevado a cabo numerosos ataques, afectando a más de 200 organizaciones en sus primeros seis meses de actividad. Entre las víctimas se incluyen empresas de sectores críticos, como la salud, la tecnología, los servicios financieros, la manufactura y las telecomunicaciones. En 2024, se estima que el grupo estuvo detrás de 89 incidentes confirmados, con otros 443 ataques no confirmados. Estos ataques comprometieron más de 5 millones de registros, lo que refleja el impacto y la amplitud de las operaciones del grupo.

---

29. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

30. https://www.trendmicro.com/en_us/research/24/i/how-ransomhub-ransomware-uses-edrkillshifter-to-disable-edr-and-.html

LOCKBIT3

Durante el año 2024 se llevó a cabo en distintas fases el desmantelamiento del grupo de ransomware LockBit en una **operación internacional conjunta denominada Operación Cronos.** Esta acción conjunta fue liderada por la Agencia Nacional contra el Crimen del Reino Unido (NCA) y el FBI, con la colaboración de al menos diez países, incluyendo Francia, Alemania, Países Bajos, Suecia, Australia, Canadá, Japón, Estados Unidos y Suiza.[31]

Como resultado, se incautaron 34 servidores ubicados en distintos países, se arrestó a al menos 15 miembros del grupo y se incautaron más de 200 cuentas de criptomonedas asociadas a la organización. Además, confiscaron el código fuente del ransomware LockBit, claves de cifrado y datos internos del grupo, incluyendo información detallada sobre sus víctimas.

A pesar del impacto de esta operación, el grupo consiguió reanudar parte de su actividad, centrando sus ataques en las entidades gubernamentales y cuerpos de seguridad de los países que participaron en el desmantelamiento de su infraestructura. Además, se filtró el código fuente de su ransomware LockBit 3.0, lo que permitió a otros actores desarrollar variantes personalizadas del mismo.

De la actividad que se le ha podido atribuir al grupo durante 2024 se incluyen el uso de técnicas de ***phishing*** que incluían ZIP maliciosos que contenían la variante LockBit Black, distribuido mediante la botnet Phorpiex, así como el envío de currículums falsos en documentos de Word con macros maliciosas.

PLAY

Play es un grupo de ransomware activo desde mediados de 2022 que, durante el año 2024, dirigió sus ataques a sectores críticos como salud, telecomunicaciones, infraestructuras tecnológicas y empresarial, en países de América y Europa mayoritariamente. Se consolidó como uno de los grupos cibercriminales más activos del año pasado.

Una de las principales características de sus ataques es la capacidad para **comprometer entornos virtualizados,** especialmente aquellos basados en VMware ESXi. Se ha observado que una variante de su ransomware diseñada para entornos Linux ESXi tiene la capacidad de detener máquinas virtuales, escanear recursos críticos y cifrar discos virtuales. Esta versión incorpora técnicas que le permiten verificar el entorno antes de ejecutarse y, en caso de no detectar un sistema compatible, autodestruirse para evitar su detección.

Además, utiliza un modelo de doble extorsión, robando datos confidenciales de las víctimas con la amenaza de publicarlos o venderlos y cifrando los archivos para forzar el pago de un rescate. La cadena de infección comienza mediante el uso de credenciales comprometidas, correos de *phishing* o la explotación de vulnerabilidades conocidas. Una vez dentro de los sistemas, utiliza herramientas como Mimikatz o PsExec para realizar movimientos laterales, escalar privilegios y mantener el acceso a los equipos comprometidos. Otra característica distintiva es que, al cifrar los datos, añade la extensión ".PLAY".

---

31. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

3.3. HACKTIVISMO

NoName057(16) es un grupo hacktivista prorruso que emergió en marzo de 2022, coincidiendo con la invasión rusa de Ucrania. Desde entonces, ha llevado a cabo cada día ataques de **Denegación de Servicio Distribuido (DDoS)** contra países de la OTAN y aliados de Ucrania, como Polonia, Lituania, Italia, España y Alemania. Su motivación principal es interrumpir y desestabilizar infraestructuras críticas en naciones que apoyan a Ucrania, como respuesta a políticas y declaraciones percibidas como hostiles hacia Rusia.

El grupo opera principalmente a través de **canales de Telegram**, donde coordina ataques, comparte herramientas y se comunica con sus seguidores. Una de sus herramientas clave es **DDoSia, un software de código abierto** que permite a los usuarios participar en ataques DDoS desde dispositivos Windows, Linux y Android. Este software se distribuye a través de Telegram, aunque anteriormente poseían un repositorio de Github dedicado a esta herramienta. Además, NoName057(16) ha demostrado adaptabilidad al modificar su infraestructura de mando y control (C2) en respuesta a las medidas de defensa implementadas por las organizaciones objetivo.

Aunque se presenta como una red descentralizada de voluntarios impulsados por el nacionalismo ruso, la estructura operativa de NoName057(16) sugiere un alto grado de organización y coordinación. La frecuencia, escala y sincronización de sus ataques, así como la gestión efectiva de canales de Telegram y actualizaciones constantes de herramientas como DDoSia, indican que detrás del grupo podría haber una entidad con mayores recursos y capacidad de dirección. A pesar de que su enfoque en ataques DDoS sea menos sofisticado que otras líneas de ataque, ha demostrado ser efectivo para interrumpir servicios y generar atención mediática. Esto ha llevado a varios analistas a sospechar que, aunque empleen una fachada de hacktivismo espontáneo, es probable que cuenten con el respaldo o la supervisión de actores más poderosos, posiblemente vinculados al aparato estatal ruso o a estructuras de inteligencia afines.

Aunque se presenta como una red descentralizada de voluntarios impulsados por el nacionalismo ruso, la estructura operativa de NoName057(16) sugiere un alto grado de organización y coordinación.

3.4. OTROS ACTORES RELEVANTES

3.4.1. LAZARUS GROUP

Lazarus Group, clúster de actores vinculado a la **Comisión de Asuntos de Estado de Corea del Norte**, centró sus campañas de 2024 en el ciberespionaje, el sabotaje digital y la minería de criptomonedas, con el objetivo de fortalecer las capacidades de defensa y la economía del país, así como hacer frente a las sanciones y a la presión política internacional.

Sus operaciones se dirigieron principalmente a los sectores gubernamental, tecnológico, financiero, militar y de investigación, enfocándose en compañías relacionadas con las criptomonedas. Sus países objetivo fueron mayoritariamente estados de la región asiática, particularmente Corea del Sur y Estados Unidos.

Respecto al ámbito operacional, Lazarus **ha empleado técnicas de ingeniería social avanzada,** suplantando empresas legítimas u ofreciendo ofertas laborales falsas. Para ello, ha utilizado plataformas reconocidas como Telegram, LinkedIn y WhatsApp, lo que le ha permitido poder comprometer sistemas y desplegar código dañino diseñado para recolectar información sensible, como credenciales de acceso, datos financieros y activos en criptomonedas.

Además, ha mantenido la persistencia en los equipos infectados aprovechando vulnerabilidades de software y ocultando su actividad mediante el uso de herramientas y servicios legítimos modificados. El grupo ha mejorado sus capacidades de exfiltración de datos y blanqueo de fondos, empleando servicios descentralizados para transferir criptomonedas robadas y atacar infraestructuras estratégicas.

Lazarus ha empleado técnicas de ingeniería social avanzada, suplantando empresas legítimas u ofreciendo ofertas laborales falsas.

4. TECNOLOGÍAS

4.1. CÓDIGO DAÑINO

Se ha identificado en el periodo analizado que **las tipologías** de artefactos más activos **son *stealer* y botnet,** especialmente este último, observándose un aumento notable de actividad a partir de octubre.

Otros tipos como los **Remote Acces Trojan (RAT)** tienen una presencia constante, pero en niveles menores. Los restantes tipos de códigos dañinos, como loaders, backdoors, ransomware y frameworks de post explotación, se mantienen en cantidades estables durante todo el periodo.

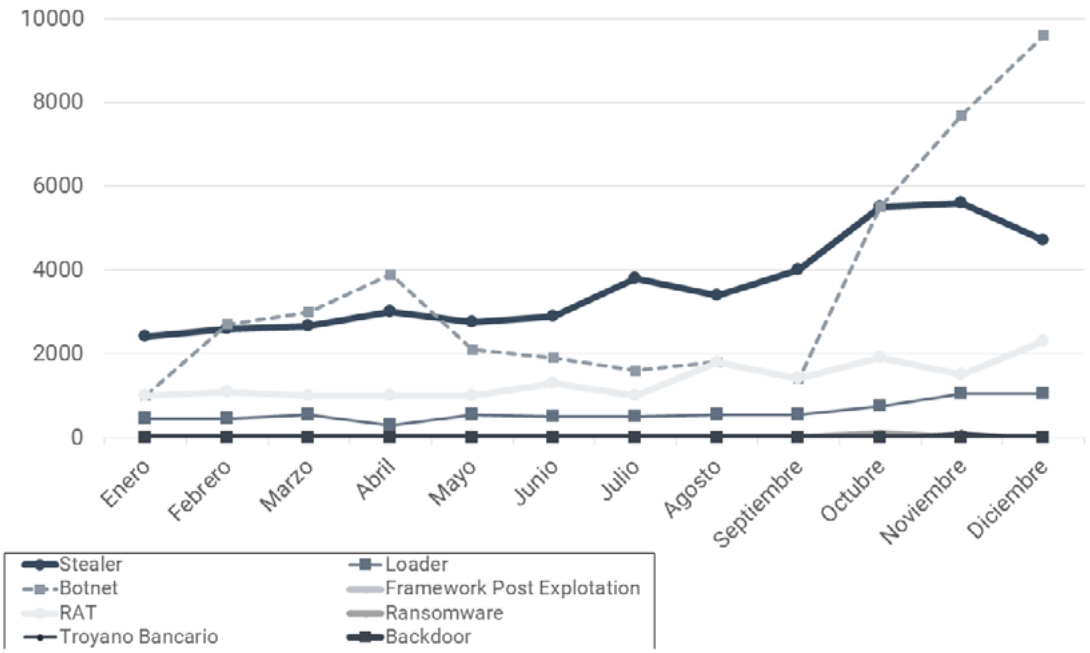


Ilustración 6: Tipología de código dañino más activa

Los malwares de tipo botnet han mostrado una tendencia al alza a lo largo de 2024, con un incremento durante el último cuatrimestre del año. Este repunte en la actividad parece vinculado a la aparición y expansión de una nueva amenaza conocida como "Murdoc_Botnet".[32] Esta botnet es una variante adaptada del conocido código dañino **Mirai**. Sin embargo, este incremento no puede desligarse a la proliferación de las redes ORB por parte de actores estado de origen chino.

32. https://blog.qualys.com/vulnerabilities-threat-research/2025/01/21/mass-campaign-of-murdoc-botnet-mirai-a-new-variant-of-corona-mirai

La campaña de distribución asociada a este malware ha explotado vulnerabilidades ya documentadas, como la CVE-2024-7029, que afecta a cámaras AVTECH, y la CVE-2017-17215, presente en routers Huawei, vulnerabilidades que han sido integradas, permitiendo un aumento de potenciales objetivos.[33]

Durante 2024, se identificó una tendencia creciente pero sostenida en las **detecciones de stealers y RAT.** A diferencia de otros tipos de malware con aumentos puntuales, como los troyanos bancarios, los stealers y RAT muestran una presencia constante a lo largo del año. Esto se debe principalmente a la eficiencia económica que suponen. Se distribuyen comúnmente mediante campañas masivas de ***phishing*** **o falsos instaladores,** siendo utilizados frecuentemente como etapa inicial de infecciones más complejas.

Además, la disponibilidad de estas herramientas en modelos de **Malware-as-a-Service (MaaS),** como es el caso de RedLine, Raccoon o Lumma para stealers, y de NjRAT o Quasar para RAT, ha facilitado su adopción por cualquier tipo de actor, incluyendo aquellos con un nivel técnico más bajo. Bajo esta tipología se ha visto la incorporación de nuevas técnicas para la evasión de defensas, como el cifrado de payloads o el uso de canales de comunicación de plataformas legítima, como Telegram o Discord.

Respecto a los **troyanos bancarios**, se observan repuntes puntuales que coinciden con campañas estacionales. Un ejemplo es el mes de mayo, donde muchos países atraviesan el periodo de **declaración de impuestos,** motivación recurrentemente utilizada en campañas de distribución de malware. También se puede observar este tipo de campañas en noviembre, con campañas como el **Black Friday o el inicio de la época navideña.**

La baja presencia de loaders, frameworks de post-explotación y backdoors en los datos de 2024 no responde a una falta de relevancia, sino a un uso más dirigido y de menor alcance, orientado a **campañas de mayor sofisticación.** Su diseño está orientado a la evasión y a un uso más sigiloso, muchas veces por parte de actores sofisticados o APT.

Los stealers y RAT muestran una presencia constante a lo largo del año debido principalmente a la eficiencia económica que suponen

33. https://www.revistaciberseguridad.com/2025/01/descubierta-una-nueva-campana-de-la-botnet-mirai-que-afecta-a-camaras-avtech-y-routers-huawei/

Las familias de malware más detectadas durante 2024 junto con su volumetría son las siguientes:

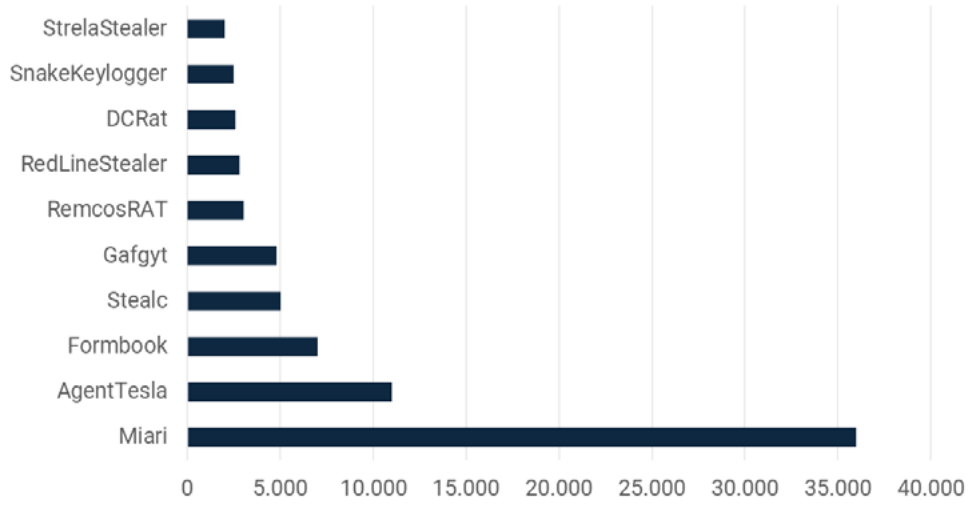


Ilustración 7. Familias de malware más detectadas en 2024

4.1.1. AMENAZAS EMERGENTES MÁS DESTACADAS DURANTE 2024

El panorama de la ciberseguridad ha seguido evolucionando a un ritmo acelerado durante el periodo analiazdo.

Entre las nuevas amenazas de mayor sofisticación se encuentra **Xehook Stealer**, malware de tipo infostealer desarrollado en .NET, identificado por primera vez en enero de 2024. Su diseño muestra una evolución desde proyectos previos como Cinoshi y Agniane, evidenciado por similitudes en el código y la infraestructura de comando y control (C&C) compartida.

Este stealer **está orientado a sistemas Windows** y entre sus funcionalidades destacan la recopilación dinámica de información de navegadores basados en Chromium y Gecko, el robo de credenciales, cookies, datos de autocompletado, tarjetas de crédito y sesiones de aplicaciones como Telegram y Discord. Además, es capaz de extraer información de más de 110 criptomonedas y extensiones de autenticación de dos factores (2FA), así como de diversas billeteras de criptomonedas de escritorio. Incluye también una API para la creación de bots de tráfico personalizados y una función para recuperar cookies de Google expiradas.

La cadena de infección típica de Xehook tiene como vector de entrada campañas de *phishing* o malspam, empleando archivos comprimidos que contienen accesos directos, Una vez ejecutado, el malware se inyecta en procesos legítimos del sistema como RegAsm.exe. [34]

34. https://cyble.com/blog/xehook-stealer-evolution-of-cinoshis-project-targeting-over-100-cryptocurrencies-and-2fa-extensions/
https://darfe.es/ciberwiki/index.php?title=Xehook

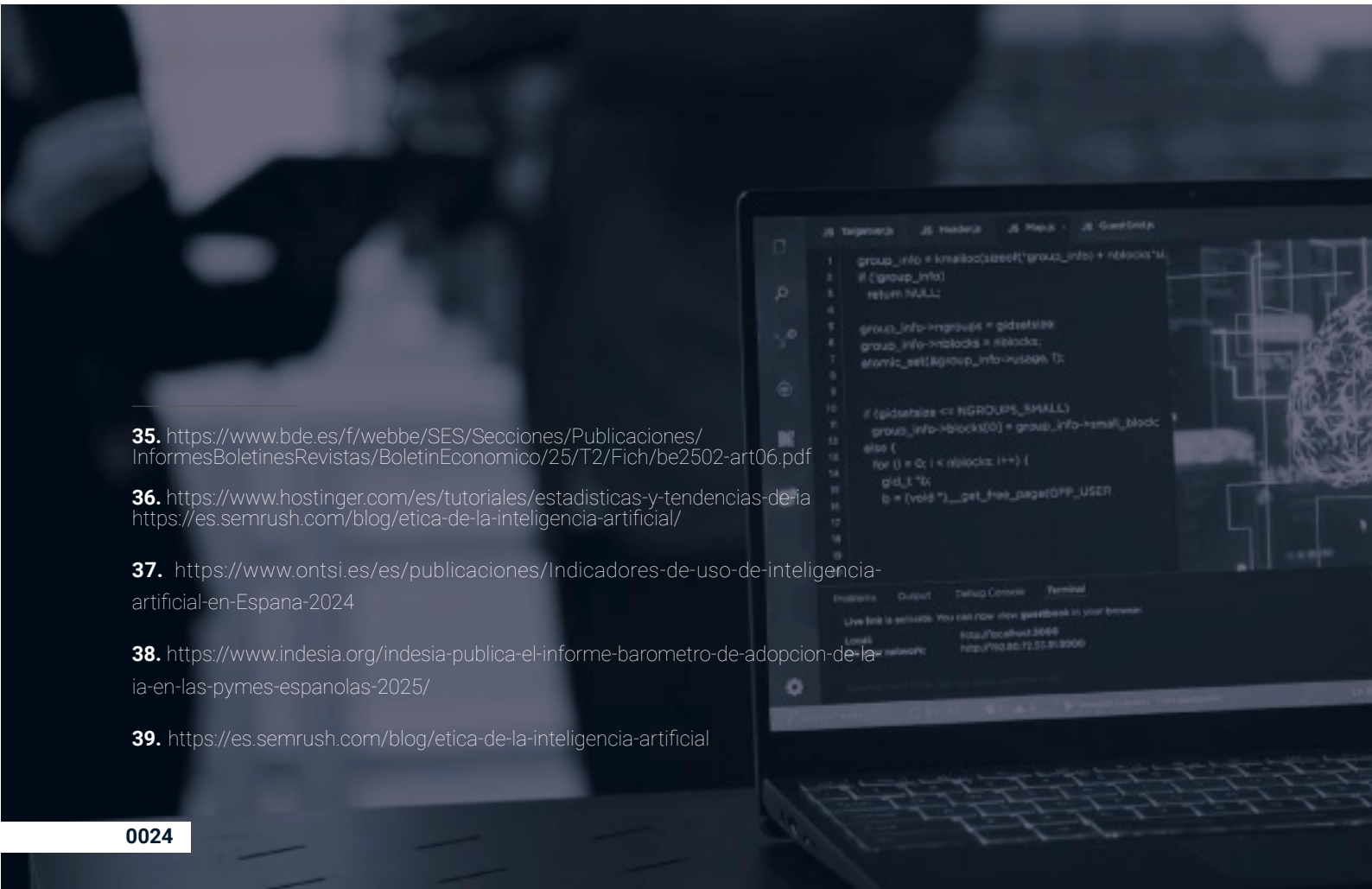
4.2. INTELIGENCIA ARTIFICIAL

En 2024, el uso de la Inteligencia Artificial experimentó un crecimiento significativo a nivel global y nacional. La adopción empresarial de IA ha aumentado del 55% al 72%, destacando el auge de la **IA generativa**, cuyo uso se duplicó en un año.[35] Su mercado global mantiene una tasa de crecimiento anual del 37%, reflejando su creciente influencia en sectores como marketing, ventas y desarrollo de productos.[36]

En España, el 11,4% de las empresas implementó tecnologías de IA,[37] con un notable incremento del 36,2% en su adopción por parte de las pymes.[38] En paralelo, se estima que estas tecnologías podrían automatizar entre el 60% y el 70% del tiempo dedicado por los trabajadores.[39]

Durante el último año, han surgido nuevas **tendencias funcionales o evolutivas** de la inteligencia artificial a partir del desarrollo de modelos base (como GPT, BERT o PaLM), adaptados para resolver tareas específicas o potenciar capacidades humanas en distintos contextos desligadas del uso puramente generativo característico de periodos anteriores.

Entre las tendencias funcionales más destacadas durante el periodo se encuentran las siguientes:



35. https://www.bde.es/f/webbe/SES/Secciones/Publicaciones/InformesBoletinesRevistas/BoletinEconomico/25/T2/Fich/be2502-art06.pdf

36. https://www.hostinger.com/es/tutoriales/estadisticas-y-tendencias-de-ia https://es.semrush.com/blog/etica-de-la-inteligencia-artificial/

37. https://www.ontsi.es/es/publicaciones/Indicadores-de-uso-de-inteligencia-artificial-en-Espana-2024

38. https://www.indesia.org/indesia-publica-el-informe-barometro-de-adopcion-de-la-ia-en-las-pymes-espanolas-2025/

39. https://es.semrush.com/blog/etica-de-la-inteligencia-artificial

4.2.1. IA GENERATIVA MULTIMODAL

Los modelos multimodales pueden procesar una amplia variedad de entradas (como texto, imágenes y audio) en forma de instrucciones y convertirlas en varias salidas, no solo en el tipo de fuente. Ejemplos de este tipo de modelos son Sora de OpenAI, capaz de generar vídeos realistas a partir de texto, y Veo 2 de Google.[40]

4.2.2. AGENTES ESPECIALIZADOS

Un agente personalizado de inteligencia artificial es un sistema basado en IA diseñado para realizar tareas específicas adaptadas a las necesidades de un usuario, empresa o contexto particular. A diferencia de los modelos generalistas (como ChatGPT en su forma básica), estos agentes están entrenados o configurados con conocimientos, reglas y comportamientos orientados a resolver problemas concretos, interactuar en un entorno determinado o automatizar procesos repetitivos.[41]

4.2.3. IA PREDICTIVA

La IA predictiva es una rama de la inteligencia artificial que utiliza datos históricos, aprendizaje automático (Machine Learning) y algoritmos estadísticos para predecir eventos futuros, comportamientos o tendencias. Su objetivo principal es anticiparse a lo que ocurrirá con base en patrones observados en grandes volúmenes de información. Un ejemplo de esta sería el uso de un agente especializado en diagnosticar enfermedades que afecten a la piel. Los modelos predictivos suelen estar también especializados en una tarea en específico.[42]

4.2.4. INTELIGENCIA ARTIFICIAL AUTÓNOMA

La inteligencia artificial autónoma (IA Autónoma) se refiere a sistemas de IA capaces de tomar decisiones y ejecutar acciones por su cuenta, sin supervisión humana directa y constante, especialmente en entornos dinámicos, inciertos o abiertos. A diferencia de los asistentes virtuales o herramientas predictivas que requieren intervención o aprobación del usuario, la IA autónoma percibe, razona y actúa de manera continua y adaptativa.[43]

---

40. https://es.wikipedia.org/wiki/Inteligencia_artificial_multimodal

41. https://rpatechnologies.es/soluciones/inteligencia-artificial-ia-especializada-ia-generativa/

42. https://www.blueprism.com/es/resources/blog/generative-ai-vs-predictive-ai/

43. https://konfuzio.com/es/inteligencia-artificial-autonoma/

4.3. IA EN LA CIBERDEFENSA

En 2024, la inteligencia artificial ha desempeñado un papel crucial en la evolución de la ciberseguridad, transformando tanto las estrategias defensivas como las tácticas ofensivas. La IA se ha convertido en una **herramienta esencial para detectar amenazas, automatizar respuestas y mejorar la eficiencia operativa** en entornos digitales cada vez más complejos. Los principales usos que ha adoptado la IA en el ámbito de la ciberseguridad durante el último año han sido los siguientes:

4.3.1. DETECCIÓN Y RESPUESTA A AMENAZAS EN TIEMPO REAL

La IA permite analizar grandes volúmenes de datos para identificar patrones anómalos y detectar amenazas emergentes. Por ello, las capacidades de respuesta han empezado a integrar la detección a partir de IA de amenazas en tiempo real, así como el desarrollo de modelos para la detección específica de amenazas de alta sofisticación.[44]

4.3.2. AUTOMATIZACIÓN DE PROCESOS DE SEGURIDAD

La automatización impulsada por IA reduce la carga de trabajo de los equipos de seguridad, permitiendo una gestión más eficiente de incidentes. Nuevas líneas de investigación apuestan por el desarrollo de herramientas de IA generativa que asisten a los equipos de seguridad en la toma de decisiones de cara a agilizar la respuesta de amenazas.[45]

4.3.3. ANÁLISIS PREDICTIVO Y PREVENCIÓN PROACTIVA

La IA se utiliza para prever posibles ataques y vulnerabilidades, permitiendo a las organizaciones adoptar medidas preventivas. Puede observarse en la integración de redes neuronales dedicadas a la detección conductual, interactuando directamente en los dispositivos de los usuarios para identificar comportamientos no legítimos.[46] [47]

---

44. https://itresit.es/inteligencia-artificial-deteccion-respuesta-amenazas/

45. https://www.fortinet.com/lat/solutions/enterprise-midsize-business/fortiai

46. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

47. https://www.kaspersky.com/enterprise-security/wiki-section/products/machine-learning-in-cybersecurity

4.4. INTEGRACIÓN DE IA EN LOS PROCESOS DE LOS ACTORES HOSTILES

En 2024, se ha detectado que los grupos APT han realizado una integración de la Inteligencia Artificial en todos sus procesos.[48]

Uno de los principales usos de la inteligencia artificial ha sido el reconocimiento para la planificación de una campaña, encontrando potenciales víctimas como redes asociadas a organismos gubernamentales o de defensa, así como la investigación de expertos, o la obtención de infraestructura que pueda utilizarse para el Mando y Control de los artefactos desplegados posteriormente.

La mejora en este apartado ha permitido también a los actores integrar procesos de automatización de ataques, tanto la investigación y detección de vulnerabilidades que puedan ser explotadas en las víctimas, como la propia ejecución, reduciendo la necesidad de intervención humana y aumentando la eficiencia.

Otro de los usos ha sido la adecuación de las técnicas de ***phishing***, especialmente en las **tareas de traducción.** Uno de los principales ejemplos puede observarse en APT42, grupo asociado a Irán, el cual ha integrado los servicios de Gemini en la traducción de hebreo, persa o inglés, permitiendo una mejor realización de *phishing* dirigidos. También APT43, asociado a Corea del Norte, que ha integrado el mismo tipo de servicio para la creación de cartas de presentación.

Por supuesto, el desarrollo de capacidades ofensivas también ha sido objeto de mejora a partir de la aplicación de inteligencia artificial. Se ha registrado que los grupos de origen ruso ha utilizado la inteligencia artificial para la **reescritura de software público en otros lenguajes de programación,** permitiendo así evadir firmas de detección basadas en el análisis estático. También el desarrollo de scripts en etapas de post-explotación, así como para el acceso remoto y gestión de Active Directory.

Sin embargo, la integración que dota de mayor sofisticación en las amenazas ha sido la integración en el desarrollo de **capacidades ofensivas.**[49] El desarrollo de malware adaptativo ha permitido modificar el comportamiento y evadir soluciones de seguridad de manera adaptada a la víctima. Con el mismo objetivo los actores de ransomware han integrado estas funcionalidades, los cuales están mejorando la eficiencia en el cifrado de los datos.

Finalmente, también se han detectado la mejoría en las **botnets**, las cuales han utilizado IA para la optimización de ataques, la selección de objetivos y mejorar la evasión frente a las defensas de la organización.

---

48. https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai

49. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

4.5. VULNERABILIDADES

Durante el año 2024 se publicaron un total de 40.220 vulnerabilidades, lo que representa un aumento significativo con respecto al ejercicio anterior y confirma la tendencia ascendente de los últimos años.

El número de vulnerabilidades por mes tiene un comportamiento no regular, siendo una actividad mayor especialmente en el mes de mayo, pero también en noviembre, superando las 5.000 y 4.000, respectivamente. Esto puede deberse a los eventos de tipo ***bug bounty*** que se concentran en estas fechas, lo que hace que se publican en masa numerosas vulnerabilidades. Por otra parte, el mes con menor número de publicaciones fue septiembre, con algo más de 2.500 registros, evidenciando el impacto postvacacional de las investigaciones en las fallas de software.

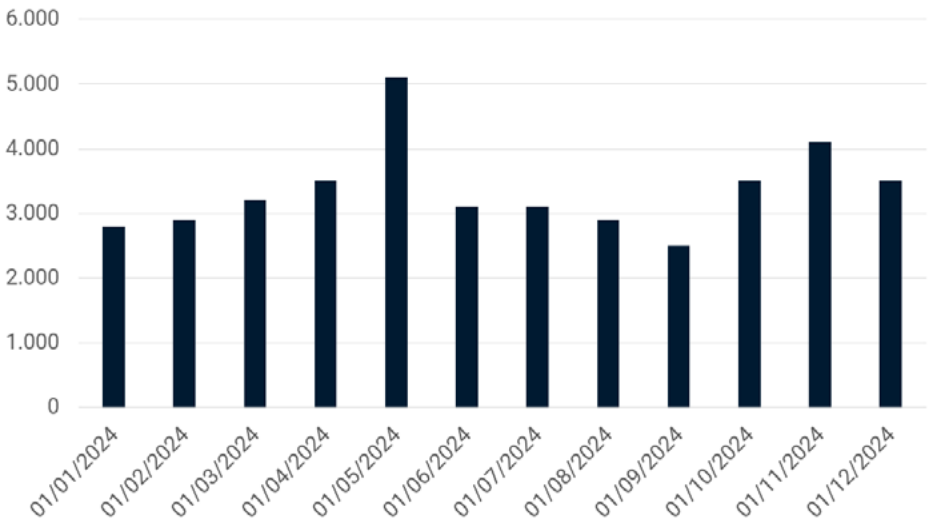


Ilustración 8: Evolución de las vulnerabilidades publicadas en 2024

Sin embargo, filtrando el análisis a las **vulnerabilidades clasificadas como críticas,** se observa una disminución respecto al año anterior, con 3.286. En enero tuvo lugar el registro más elevado, con más de 500 casos, seguidos por octubre y agosto. Por el contrario, diciembre presentó el menor número, con menos de 200 vulnerabilidades críticas detectadas. Esto puede deberse a que, debido a la integración de desarrollo seguro y detección temprana por fabricantes de software, vulnerabilidades teóricamente consideradas críticas en el pasado ya vienen mitigadas en la configuración base del software, degradando su CVSS a alto o medio.

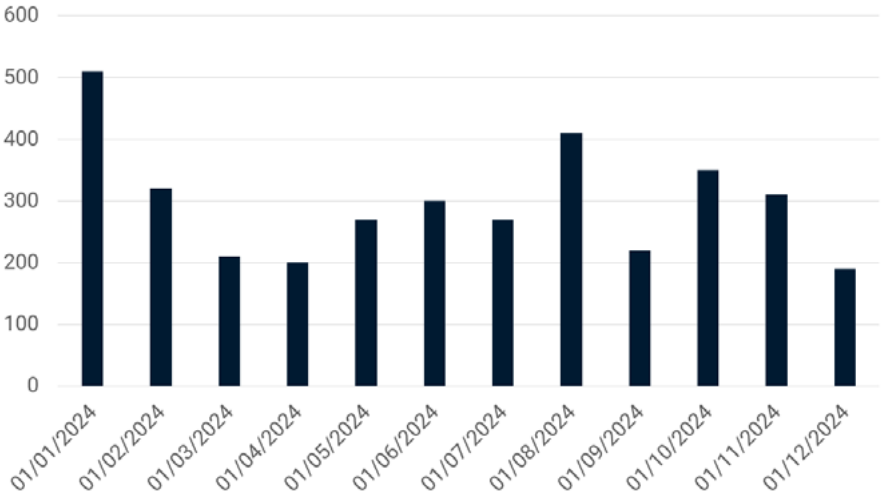


Ilustración 9: Evolución de las vulnerabilidades críticas en 2024

En el análisis de fabricantes, **Linux se posiciona como el proveedor con mayor número de vulnerabilidades publicadas** (3.978), seguido de **Microsoft** (1.123), **Google** (863), y **Adobe** (760). Esta tendencia muestra que los sistemas operativos con mayor cuota de mercado siguen siendo los principales objetivos de los investigadores.

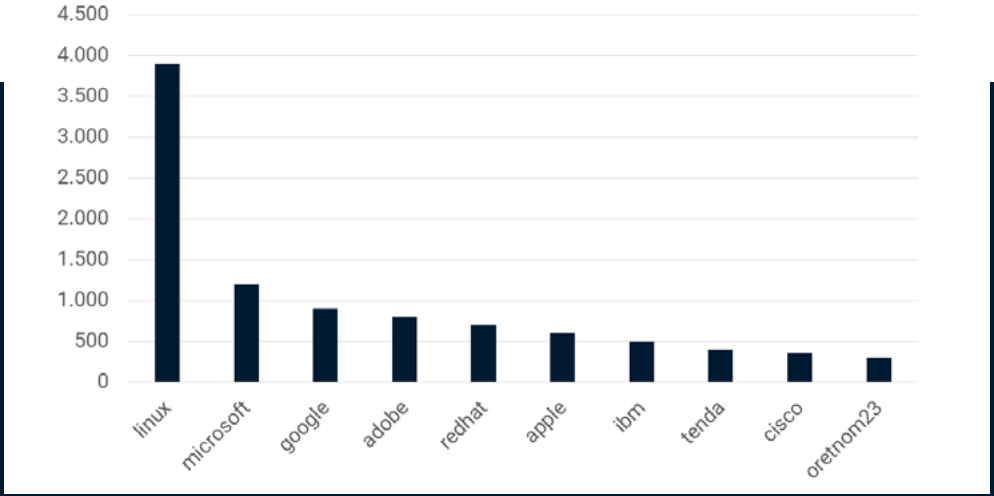


Ilustración 10: Vulnerabilidades publicadas en 2024 por fabricante

Respecto al **vector de explotación** de las vulnerabilidades, puede observarse que la mayor parte de ellas pueden ser explotadas de forma remota, evidenciando la necesidad de una rápida gestión en la actualización de éstas.

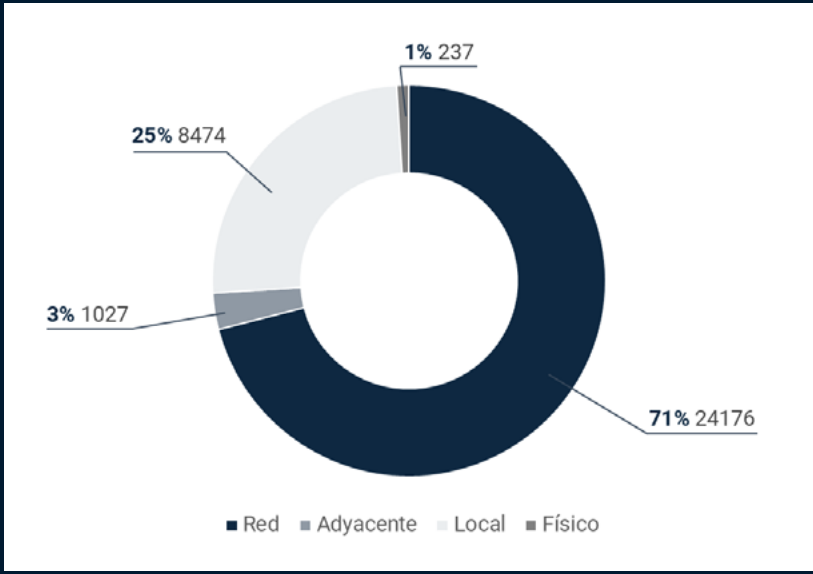


Ilustración 11: Vector de explotación de las vulnerabilidades de 2024

Analizando las vulnerabilidades a través del sistema **Common Weakness Enumeration** (CWE),[50] se observa que la mayor parte de vulnerabilidades del periodo están asociadas al **Cross-Site Scripting (XSS),** mientras que la segunda posición la ocupa la clasificación asociada a la **falta de información** suficiente para la clasificación. En tercer lugar, se encuentra la tipología de **inyección SQL.** Esto se debe a que este tipo de vulnerabilidades tienen una fuerte dependencia respecto a las prácticas de desarrollo inseguras, siendo las más susceptibles de quedar expuestas sin una correcta validación de las entradas.

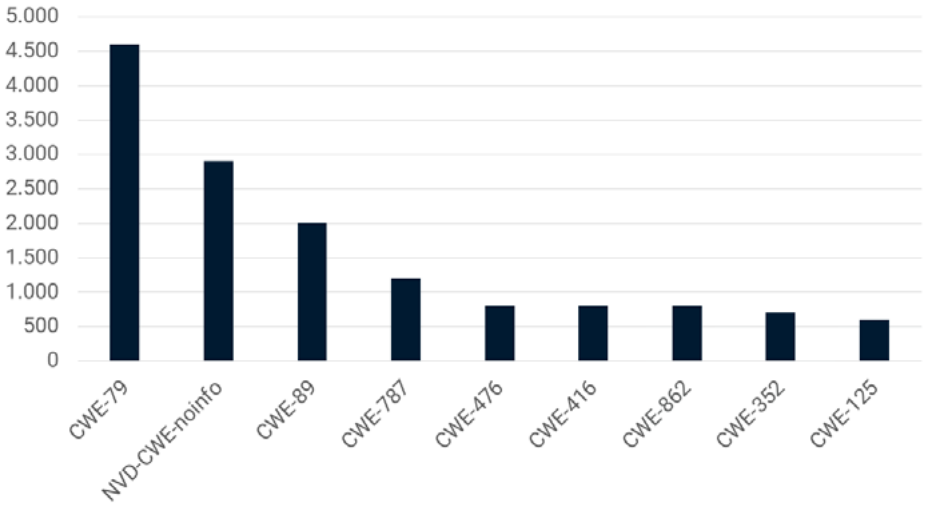


Ilustración 12: Clasificación de las vulnerabilidades por CWE

50. Taxonomía desarrollada por MITRE Corporation que clasifica las debilidades de software y los fallos de diseño

Esta misma clasificación, pero con las vulnerabilidades críticas presenta los siguientes resultados.

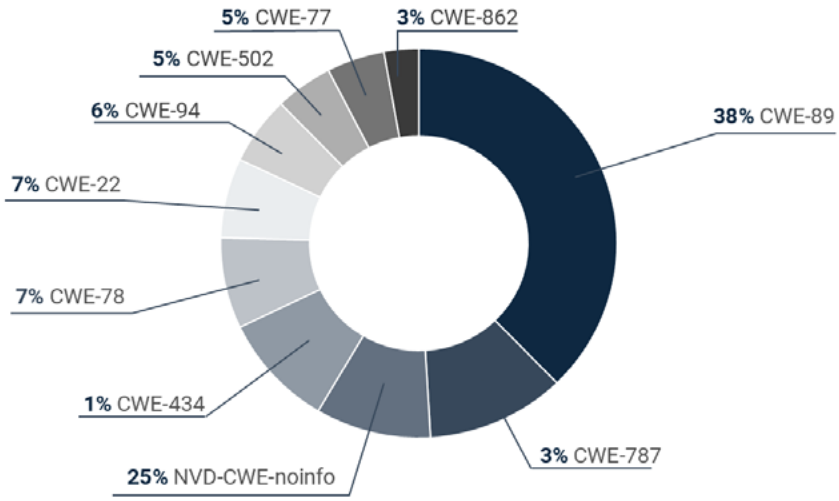


Ilustración 13: Clasificación de las vulnerabilidades críticas por CWE

Respecto al **uso de vulnerabilidades en campañas activas,** se ha identificado que la vulnerabilidad CVE-2017-11882, relacionada con el **componente EQNEDT32.exe de Microsoft Office,** sigue siendo la más explotada. También se destaca otra vulnerabilidad relacionada con la suite, el CVE-2017-0199. Todo apunta a que el uso todavía de vulnerabilidades de 2017 puede deberse a que aún existe una gran cuota de mercado de versiones antiguas de Office.

Otra vulnerabilidad también de 2017 y que sigue siendo explotada es el CVE-2017-17215, relacionada con **modelos de routers Huawei** e implementada por botnets IoT. El motivo de la explotación de vulnerabilidades tan antiguas, años después, es que la mayoría de sistemas IoT no fueron diseñados con la ciberseguridad en mente y no cuentan con ciclos de vida que garanticen actualizaciones más allá de unos pocos años.

Durante marzo de 2024, se detectó una modificación con código dañino de la **librería de compresión de datos XZ Utils,** utilizada en muchas distribuciones de Linux. La vulnerabilidad fue introducida de manera hostil por uno de los mantenedores del proyecto en las versiones 5.6.0 y 5.6.1 de la biblioteca liblzma, publicadas en febrero de 2024. Esta modificación permite a un atacante con una clave privada Ed448 específica ejecutar código de forma remota en sistemas Linux afectados, obteniendo acceso completo al sistema. La vulnerabilidad recibió una puntuación CVSS de 10.0.[51]

La vulnerabilidad fue descubierta el 29 de marzo de 2024. Aunque XZ Utils es ampliamente utilizado en las distribuciones de Linux, la puerta trasera afectaba principalmente a sistemas basados en arquitecturas x86-64 que utilizan los gestores de paquetes dpkg o rpm. En el momento del descubrimiento, la versión comprometida aún no se había desplegado ampliamente en entornos de producción, pero ya se encontraba en versiones en desarrollo de algunas de las principales distribuciones de Linux.

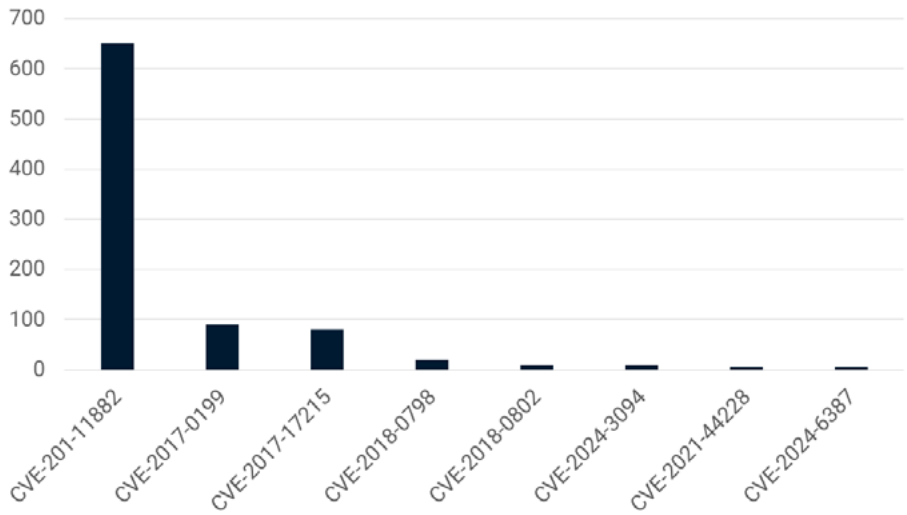


Ilustración 14: Vulnerabilidades utilizadas en campañas activas

El uso todavía de vulnerabilidades de 2017 puede deberse a que aún existe una gran cuota de mercado de versiones antiguas de Office.

51. https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know

4.6. MOVILIDAD

Los dispositivos móviles se han convertido en uno de los objetivos más interesantes para los actores de amenazas debido al gran uso que le damos hoy en día y a la cantidad de información sensible que almacenan.

A lo largo del 2024, las soluciones de seguridad de esta compañía detectaron y bloquearon un total de 33.265.112 ataques, lo que equivale a un promedio de 2,8 millones de ataques mensuales. Estas amenazas incluyeron malware, adware y otras formas de software no deseado.

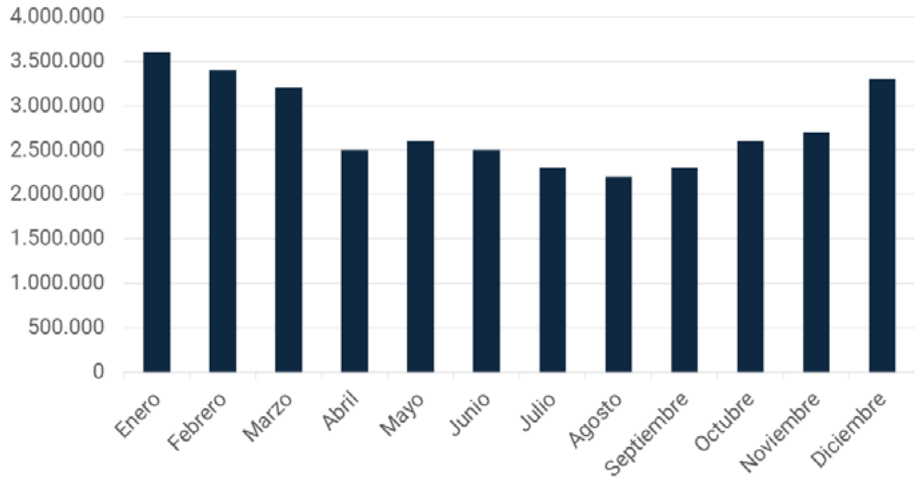


Ilustración 15: Número de ataques contra dispositivos móviles en 2024 [52]

A finales de 2024, se identificaron nuevos medios de distribución de código dañino dirigidas a usuarios de dispositivos Android del troyano bancario *Mamont*, especialmente en Rusia y otros países europeos. Este nuevo vector utilizaba ofertas falsas de productos con descuento que terminaban en enlaces para la instalación de aplicaciones con código dañino. Todo apunta a que el impacto en Rusia tenía una motivación financiera, debido al alto uso de mercados de aplicaciones no seguros, siendo más susceptibles de instalar aplicaciones no legítimas.

En otro caso, descubierto en la República Checa, los atacantes modificaban aplicaciones como NFCGate para engañar a los usuarios y extraer datos de tarjetas bancarias. Este método también se detectó en Rusia, usando aplicaciones falsas de banca o servicios gubernamentales, y en ocasiones el SpyNote RAT como vector de instalación.

52. https://securelist.lat/mobile-threat-report-2024/99586/

4.6.1. ESTADÍSTICAS DE MALWARE MÓVIL EN 2024

Las aplicaciones de tipo **adware y RiskTool** siguieron encabezando la lista de amenazas detectadas. Dentro del adware, las familias BrowserAd (22,8%), HiddenAd (20,3%) y Adlo (16%) representaron la mayor proporción. En cuanto a RiskTool, aumentó notablemente, principalmente debido al aumento de aplicaciones pornográficas de la familia Fakapp.

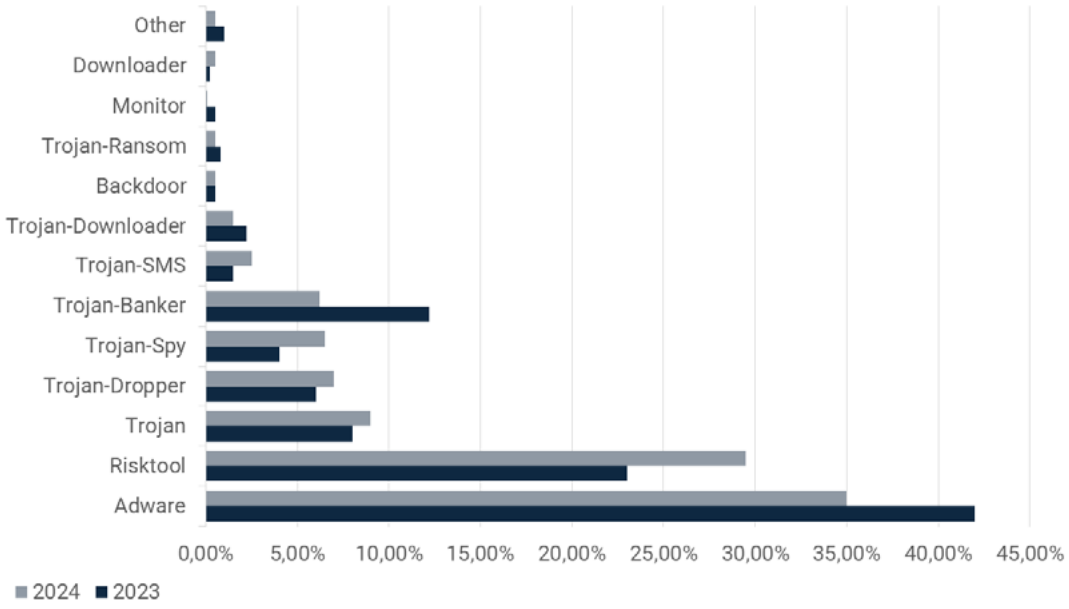


Ilustración 16: Comparativa de tipología de malware móvil detectado 2023 Vs 2024

5.
AMENAZAS

Durante el año 2024, en España, el principal objetivo de las ciberamenazas fue la **Administración pública**, con un 36,19% del total de los ataques recibidos; seguido por las **infraestructuras críticas** (tanto públicas como privadas) con el 23,7%; **empresas**, 18,12%; y **ciudadanía** con el 17,26%.

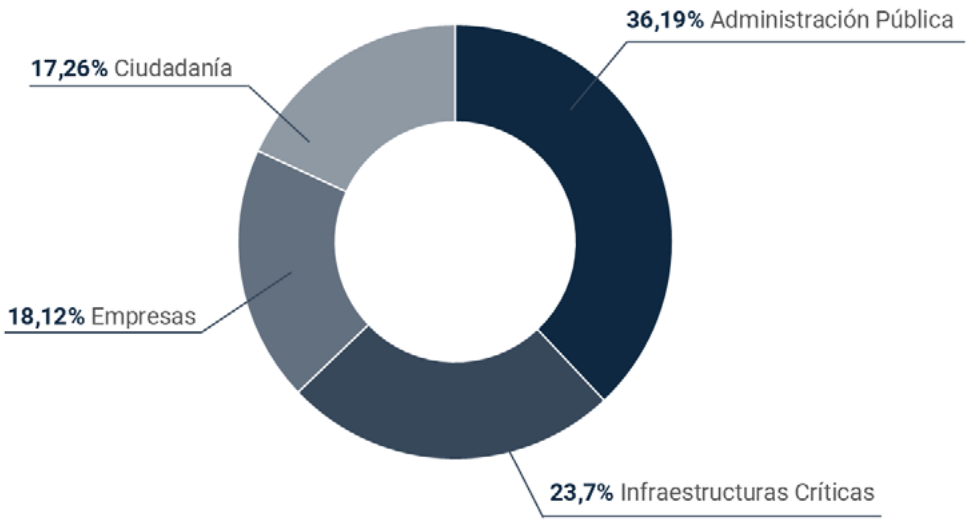


Ilustración 17: Principales objetivos de las amenazas durante 2024

5.1. ADMINISTRACIÓN PÚBLICA

Tal y como se puede observar, la Administración pública es el principal objetivo del año. Indagando en la motivación de dichas campañas, se puede llegar a la conclusión de que han sido las **acciones de hacktivismo** las que han tenido mayor recurrencia, suponiendo un total del 67,4% del total, especialmente las del actor pro ruso NoName057. Estas acciones están enmarcadas en la **Denegación de Servicio** y, aunque el principal objetivo de éstas es privar de servicios públicos a la ciudadanía, también existe un componente reputacional y propagandístico, publicitándose en sus canales de difusión.

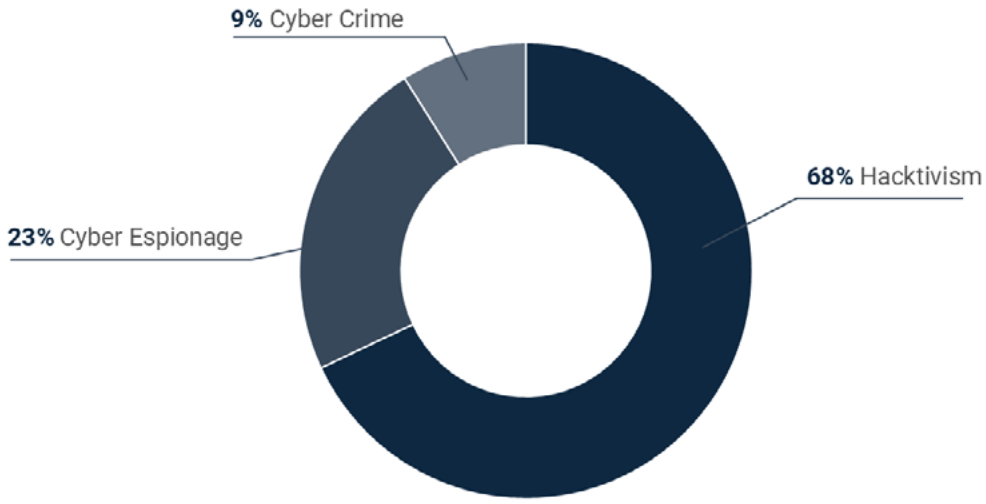


Ilustración 18: Motivación de las campañas contra la Administración pública

Tras el hacktivismo, la segunda motivación para realizar campañas contra las Administraciones públicas es el **ciberespionaje de los actores estatales.**

Por último, el **cibercrimen** ocupa la tercera causa de los ataques cuyo objetivo es el sector público. En este caso, los actores se centraron en explotar servicios web para realizar robos masivos de datos de carácter personal y buscar posteriormente su monetización. Esto lo hicieron a través de publicaciones en foros de la darkweb o la deepweb.

5.2. INFRAESTRUCTURAS CRÍTICAS Y EMPRESAS ESTRATÉGICAS

Tal y como se han mencionado en el apartado de Actores Hostiles, amenazas de muy alta sofisticación están teniendo como objetivo infraestructuras críticas de países pertenecientes a la OTAN, especialmente aquellos que proporcionan un servicio esencial. Amenazas como Volt Typhoon, de origen chino, o Sandworm, de origen ruso son algunas de estas amenazas.

Este tipo de campañas no solo tienen como objetivo información de carácter estratégico, sino también posicionar un artefacto con capacidades de disrupción y/o destrucción para un impacto a nivel físico en caso de un conflicto bélico.

Un ejemplo de esta fase temprana para la preparación de un conflicto posterior pudo verse en los años anteriores al inicio de la guerra ruso-ucraniana. Desde 2013 existen registros de campañas de origen ruso contra las infraestructuras críticas ucranianas, destacando la Operación Armagedón (2013), BlackEnergy (2015) o la parálisis de la Tesorería Estatal de Ucrania (2016).

5.3. RESTO DE EMPRESAS

Respecto a las empresas, la principal amenaza que han sufrido durante el periodo analizado han sido los actores del **cibercrimen**. Esto se debe a que, las organizaciones no consideradas dentro de infraestructura crítica no suponen un interés especial para los actores estado, quedando al margen de asuntos geopolíticos, resultando lo económico como su principal motivación.

En lo relativo al ransomware, tal y como se ha detallado anteriormente, RansomHub y Lockbit3.0 han sido los actores con mayor afectación durante el periodo. Sin embargo, el factor humano sigue siendo uno de los principales riesgos en las empresas, reportándose que el 70% de los ataques identificados son clasificados como phishing, evidenciándose la necesidad de seguir reforzando la concienciación y formación en el ámbito de la ciberseguridad en los empleados.[53]

5.4. CIUDADANOS

Respecto a las amenazas contra la ciudadanía, se puede observar cómo el abanico de amenazas es mucho más diverso que en otras tipologías, pues las diez amenazas de mayor impacto en 2024 apenas suponen el 30% del total de las amenazas totales.

53. https://www.esedsl.com/blog/resumen-2024-informe-sobre-ciberataques-de-esed

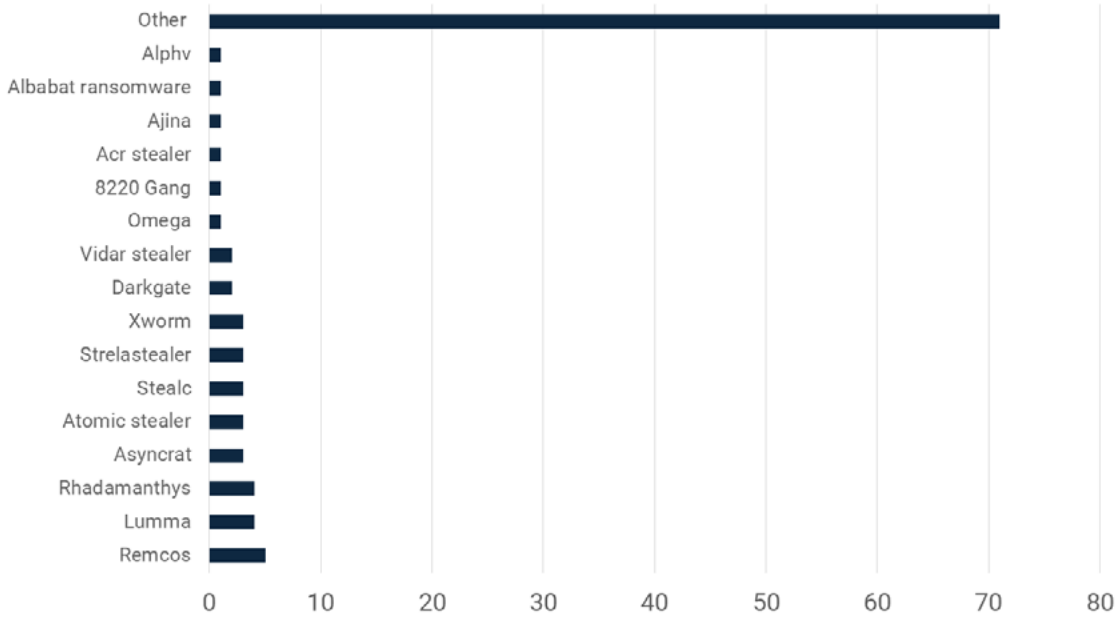


Ilustración 19: Clasificación de actores de la amenaza contra la ciudadanía

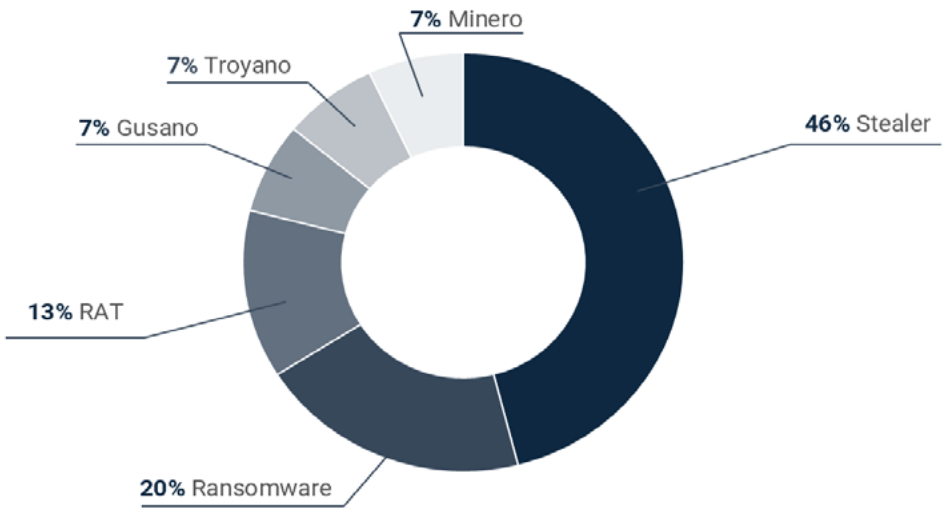


Ilustración 20: Tipología de malware utilizado contra la ciudadanía

Indagando en la tipología de malware, se han identificado una gran variedad de familias de *stealers*. A pesar de que existen campañas que han actuado para un posterior compromiso de la organización a la que pertenecen, la mayoría de las campañas tienen como objetivo final el **robo**, especialmente de **monederos de criptomoneda.**

Esto puede observarse en las técnicas de colección de información de los dispositivos víctima utilizados por los *stealers*. Credenciales asociadas a las plataformas como Exodus, Metamask, Wazirx, Lunoapp o Cryptonotify han sido objetivo de robo por parte de malware orientado a criptomoneda.

6. TENDENCIAS

6.1. ACTORES ESTADO

Se ha podido observar que la principal tendencia por parte de los actores estado es la explotación de **vulnerabilidades de día 0**, disposición ya observada en años anteriores, tal y como se puede observar en campañas de RomCom[54], Lazarus[55] o Void Banshee. Además, también se ha observado un uso oportunista de las vulnerabilidades de día 1 o día N, es decir, aquellas de muy reciente publicación, explotando especialmente aquellas que permiten un acceso inicial a la organización.

También los **ataques contra la cadena de suministro** siguen siendo tendencia, creciendo a un ritmo del 1.900% desde el año 2018.[56] Este tipo de ataques son de gran atractivo para los actores de la amenaza debido a que pueden acceder a organizaciones con una gran madurez en ciberseguridad a través a la relación de confianza con sus proveedores. Además, la explotación de vulnerabilidades en la cadena de suministro de software permite acceder a un gran abanico de potenciales víctimas. Un ejemplo es la campaña de PlushDaemon[57] contra un proveedor de servicios VPN, modificando el instalador de software para incluir un implante con código dañino.

Según se ha podido registrar, el país con mayor número de ataques recibidos en 2024 fue Ucrania. Este país ha sido un objetivo constante por parte de los grupos asociados a Rusia, tanto en acciones de CNE como de CNA. Corea del Sur también ha sido objeto de múltiples campañas, ocupando la segunda posición, especialmente debido a la gran actividad de los actores de Corea del Norte. La tercera posición la ocupa Estados Unidos. Su posición como potencia global le ha puesto en el punto de mira en las campañas de ciberespionaje de actores estatales, especialmente asociados a China, Rusia, Irán y Corea del Norte.

Los ataques contra la cadena de suministro siguen siendo tendencia, creciendo a un ritmo del 1.900% desde el año 2018.

---

54. https://www.infosecurity-magazine.com/news/romcom-apt-zeroday-flaws-firefox/

55. https://www.kaspersky.com/about/press-releases/lazarus-apt-exploited-zero-day-vulnerability-in-chrome-to-steal-cryptocurrency

56. https://www.exiger.com/perspectives/evolving-threats-and-regulations-in-software-supply-chain-security/

57. https://www.eset.com/us/about/newsroom/press-releases/eset-discovers-new-china-aligned-apt-group-plushdaemon-and-its-supply-chain-attack-on-south-korean-vpn-service/

6.2. CIBERDELITO

El cibercrimen ha alcanzado un nuevo hito en 2024, y es que se ha convertido en la tercera economía mundial, solo por detrás de Estados Unidos y China[58]. Concretamente, España experimentó un aumento de ataques de cibercrimen del 72% con respecto al año anterior. Estados Unidos fue el país con mayor número de ataques de ransomware, mientras que Suecia experimentó un aumento del 350% entre abril de 2023 y abril de 2024[59].

Los grupos más activos a nivel global han sido Ransomhub y Lockbit, con más de 500 ataques cada uno. RansomHub y LockBit son grupos de ransomware que operan bajo el modelo de Ransomware-as-a-Service (RaaS), donde los desarrolladores del malware lo alquilan a afiliados que lo usan para atacar víctimas. **LockBit** surgió en 2019 y ha sido uno de los grupos más activos y sofisticados, con raíces en foros de habla rusa y una estructura organizativa bien definida. Es de destacar que se encuentre en segunda posición en cuanto a actividad en 2024 se refiere, pues en febrero de 2024 el grupo fue desmantelado en la Operación Cronos, una operación conjunta entre más de once países[60], como ya se ha referido anteriormente.

RansomHub, en cambio, es un grupo más reciente, activo desde 2024, que ha ganado notoriedad al acoger exafiliados de otros grupos caídos como ALPHV/BlackCat, posicionándose rápidamente como una amenaza prominente tras el declive de varios actores históricos en el ecosistema del ransomware.

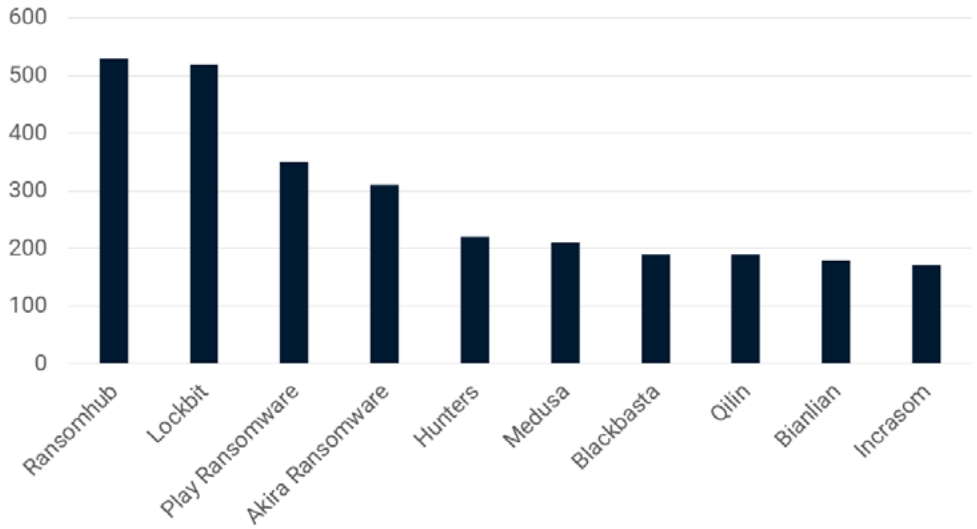


Ilustración 21: Grupos más activos de ciberdelincuentes

58. https://english.elpais.com/technology/2024-12-31/cybercrime-hits-record-levels-in-2024-as-ai-makes-attacks-more-targeted.html

59. https://www.zscaler.com/es/resources/industry-reports/threatlabz-ransomware-report.pdf

60. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

Los **sectores más atacados** a nivel mundial fueron el de **manufacturas y salud,** debido probablemente a que son industrias altamente dependientes de la continuidad operativa y el acceso inmediato a datos críticos, por lo que, además de información sensible y de carácter personal, pone en riesgo la vida de los pacientes. En manufactura, una interrupción puede detener líneas de producción completas, generando pérdidas económicas por cada hora de inactividad.[61]

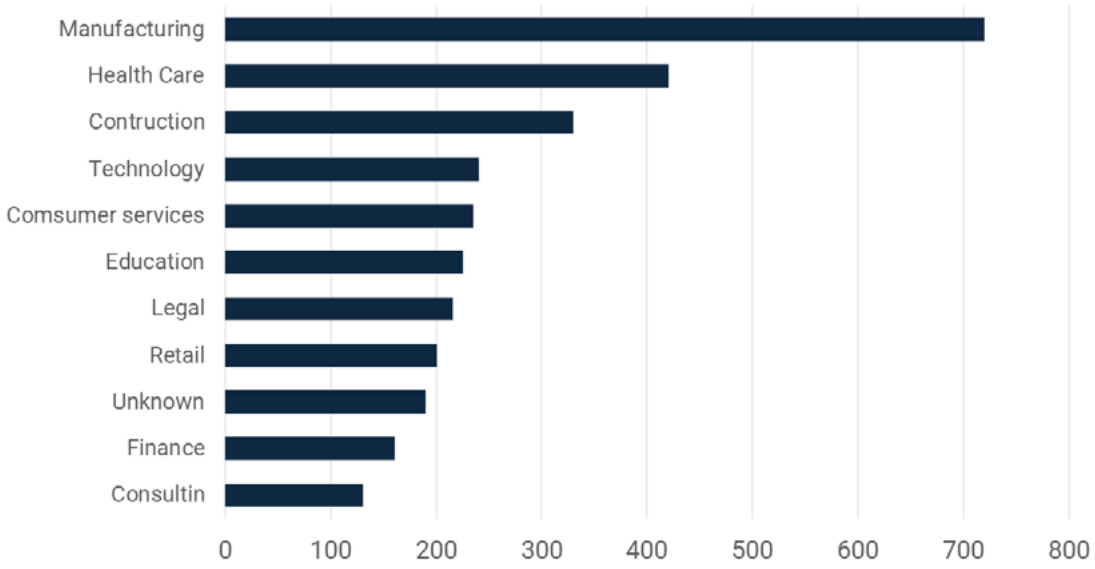


Ilustración 22: Sectores más atacados en 2024

El Malware as a Service (MaaS) sigue siendo una de las principales amenazas, representando hasta el 57% de las amenazas detectadas durante el segundo semestre de 2024, un 17% más con respecto a los primeros seis meses del año[62].

61. Datos extraídos de sondas privadas

62. https://www.darktrace.com/news/darktraces-2024-annual-threat-report-reveals-continued-rise-in-maas-threats-and-growing-use-of-evasion-tactics

6.3. HACKTIVISMO

Durante 2024 el hacktivismo ha terminado de consolidar una tendencia creciente iniciada en 2022 y ha incrementado la cantidad de ciberataques y la sofisticación de los mismos. Este fenómeno, impulsado por motivaciones ideológicas, geopolíticas y sociales, ha tenido un impacto relevante sobre gobiernos, infraestructuras críticas, medios de comunicación y organizaciones privadas.

De entre los más de 5.200 ataques de DDoS registrados durante 2024 por parte de varios de los grupos hacktivistas más influyentes, **NoName057(16) ha sido el más activo,** seguido por CyberArmyofRussia. Mientras que otros actores hostiles atacan cada cierto tiempo, estos dos grupos llevan lanzando ataques de DDoS todos los días desde hace varios años sin falta.

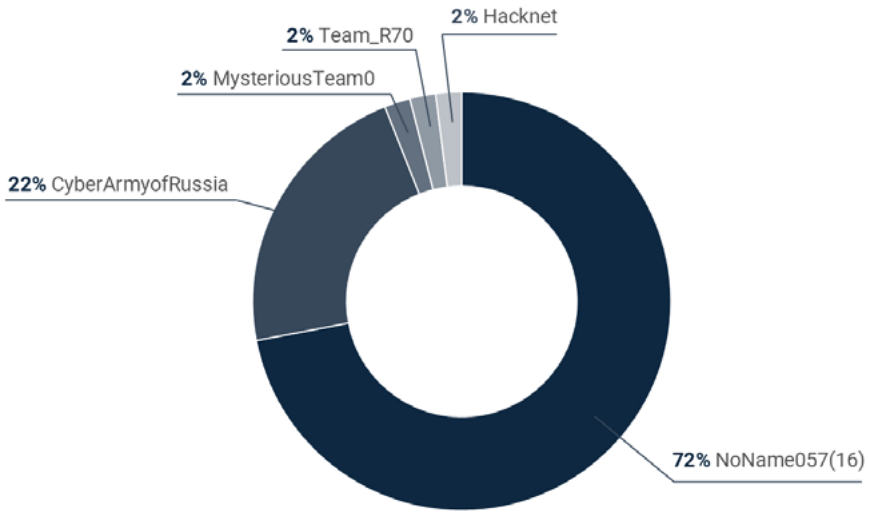


Ilustración 23: Porcentaje de ataques de DDoS por grupos registrados en 2024

En 2024, el hacktivismo estuvo profundamente influenciado por los **conflictos geopolíticos más relevantes,** especialmente la guerra entre **Rusia y Ucrania,** y el **conflicto palestino-israelí.** Puede observarse cómo las acciones hacktivistas son una respuesta inmediata a acciones o declaraciones políticas, suponiendo una acción intimidatoria para los actores geopolíticos. Como resultado, los países más atacados han sido precisamente aquellos directamente implicados en estos escenarios. Sin embargo, España ha escalado inesperadamente hasta ocupar el tercer puesto entre los países más afectados por actividades hacktivistas.

España ha escalado inesperadamente hasta ocupar el tercer puesto entre los países más afectados por actividades hacktivistas.

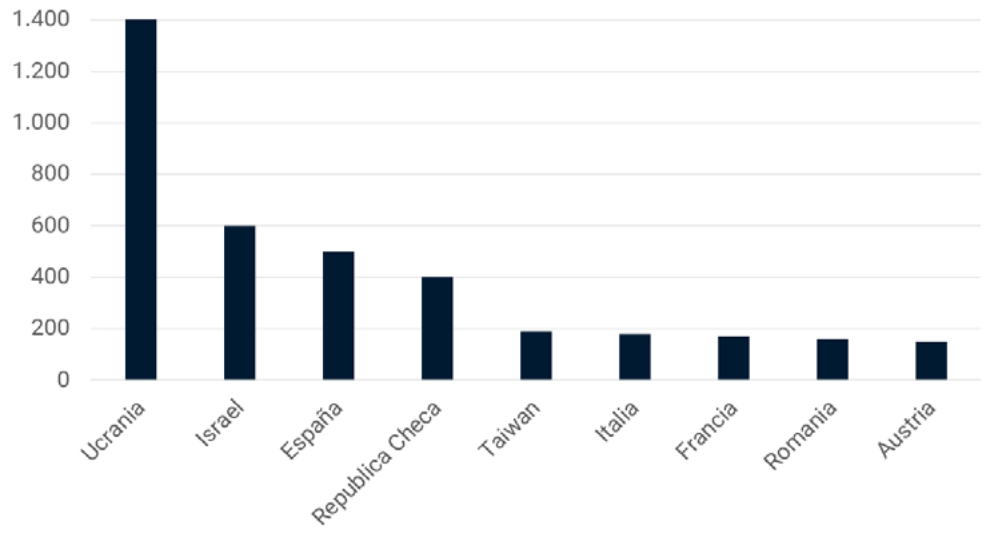


Ilustración 24: Países más afectados por actividades hacktivistas

Teniendo en cuenta el modus operandi y el comportamiento observado en los grupos hacktivistas más activos, resulta plausible pensar que detrás de muchas de estas campañas exista una estructura más compleja. Es probable que organizaciones militares o gubernamentales podrían estar coordinando estas operaciones encubiertas, utilizando el hacktivismo como fachada. Esta estrategia no solo les permite ejecutar ciberataques con cierto grado de impunidad, sino también revestirlos de una narrativa ideológica que atrae y moviliza a voluntarios o simpatizantes. Al disfrazar intereses estatales como causas ciudadanas, podrían buscar alinear emocional y políticamente a la opinión pública con sus objetivos geoestratégicos.

Tras analizar los sectores de las entidades atacadas, se concluye que los más afectados por este orden han sido el gubernamental,[63] seguido por el del financiero, el del transporte, el de las telecomunicaciones, el banquero y el energético.

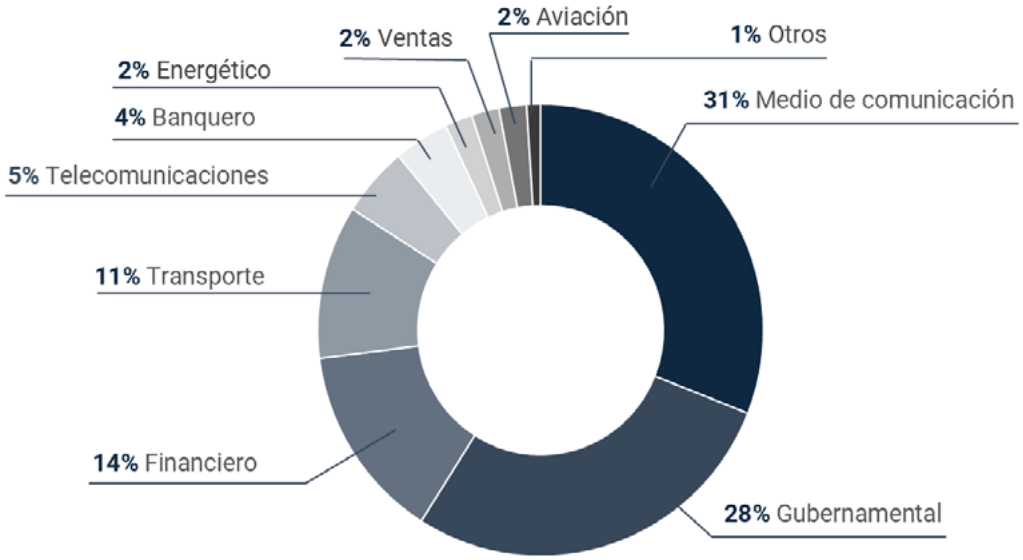


Ilustración 25: Sectores más afectados por actividades hacktivistas

63. Considerando también dentro de gubernamental el sector de defensa

Sectores más afectados

Durante años anteriores, la mayor parte de actividad hacktivista consistía en **ataques de denegación de servicios distribuidos (DDoS)**. No obstante, la investigación llevada a cabo durante 2024 muestra que además de los DDoS, se han observado una mayor cantidad relativa y absoluta de ataques más complejos, incluyendo el **robo de datos, defacement y filtraciones de información** con la intención de causar daños reputacionales.

Ilustración 26: Filtraciones publicadas por grupos hacktivistas

Filtraciones publicadas por grupos hacktivistas

También destaca la tendencia creciente de ataques contra **sistemas industriales e infraestructuras críticas.**

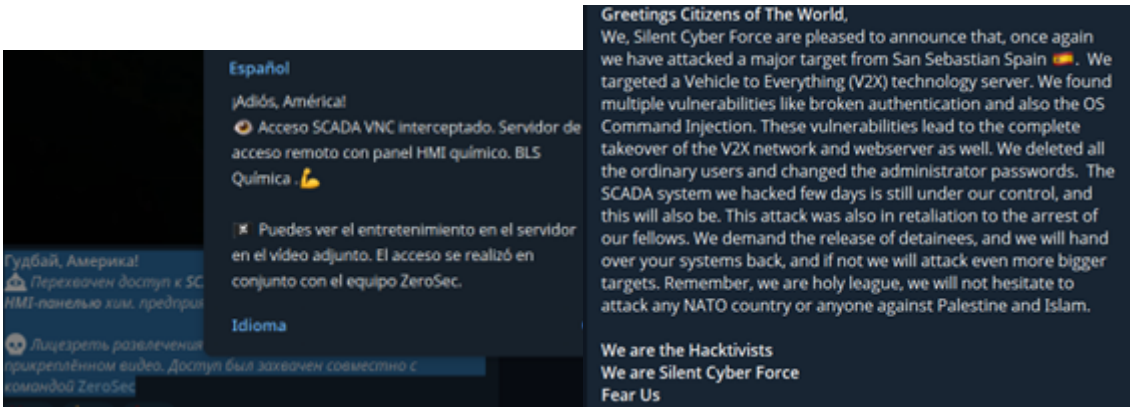


Ilustración 27: Publicaciones relativas a sistemas SCADA comprometidos durante 2024

Mientras que en 2023 el panorama del hacktivismo estuvo dominado por una red de grupos encabezados por KillNet, en 2024 cobra protagonismo un nuevo conglomerado de actores hostiles autodenominado **"Holy League".** Surgido poco después del incidente del 7 de octubre de 2023, este actor ha crecido rápidamente a través de la agrupación de diferentes grupos, hasta llegar a cerca de 40 células hacktivistas. A lo largo del periodo analizado, la "Holy League" ha estado detrás de la mayoría de los incidentes registrados, consolidándose como el principal actor del escenario cibernético actual.

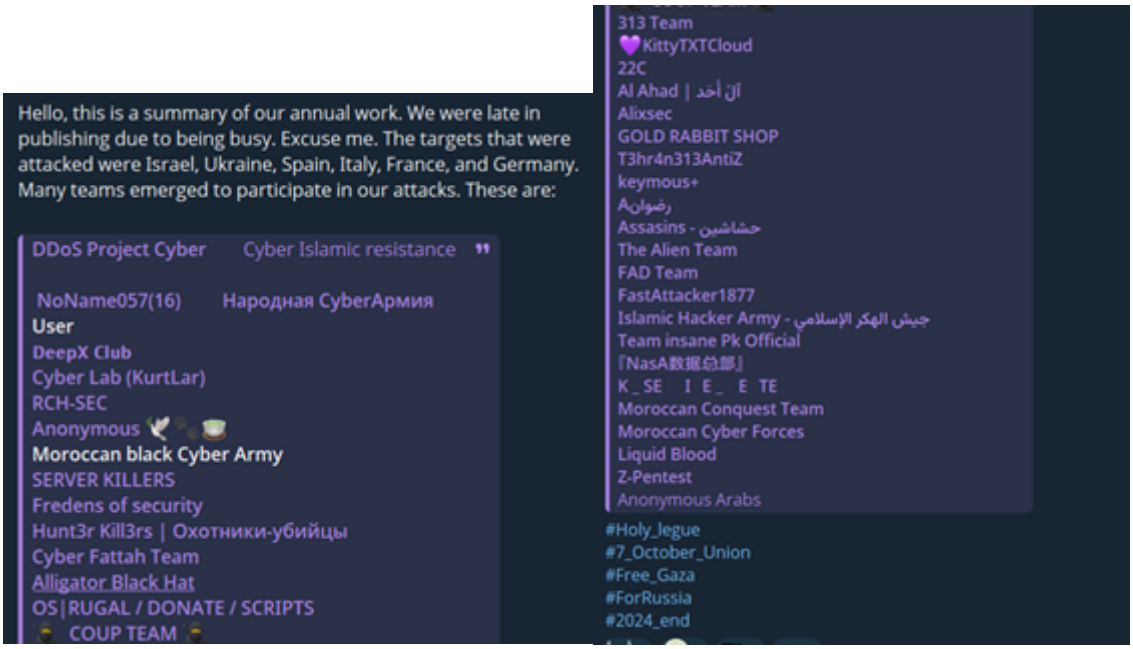


Ilustración 28: Publicación de Holy League donde se mencionan todos los grupos hacktivistas participantes

La investigación llevada a cabo durante 2024 muestra que además de los DDoS, se ha observado una mayor cantidad de ataques más complejos, incluyendo el robo de datos, defacement y filtraciones de información con la intención de causar daños reputacionales.

6.4. SISTEMAS INDUSTRIALES

La digitalización en los sectores industriales ha impulsado una integración más estrecha entre los sistemas de Tecnología Operacional (OT) y los entornos de Tecnología de la Información (IT). De esta manera, grupos criminales organizados y actores respaldados por Estados han empezado a enfocar sus esfuerzos en los sistemas OT, atraídos por el alto impacto que podría provocar la interrupción de sus operaciones.

La integración de los sistemas industriales de OT e IT está siendo potenciada por tecnologías como la inteligencia artificial o el *edge computing*[64] lo que permite una respuesta más rápida ante cualquier tipo de incidente. En el tercer trimestre de 2024, el panorama de amenazas para los Sistemas de Automatización Industrial (ICS) mostró una ligera mejora global, con una disminución del 1,5% en los equipos afectados respecto al trimestre anterior, situándose en un 22%[65].

64. https://cthings.co/blog/edge-computing-for-integrating-it-and-ot

65. https://ics-cert.kaspersky.com/publications/reports/2024/12/25/threat-landscape-for-industrial-automation-systems-q3-2024/

7.
CONCLUSIONES

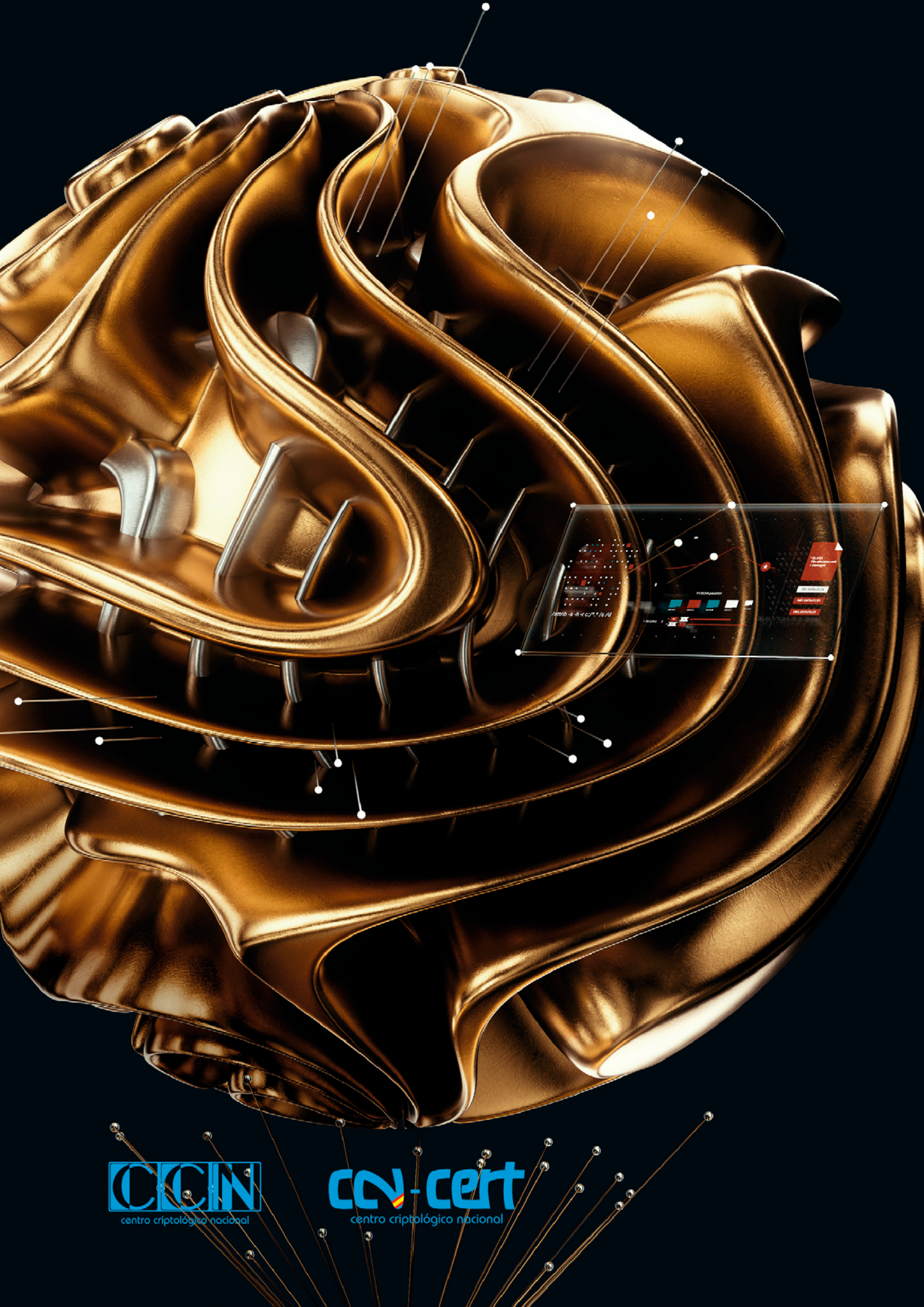
2024 ha sido un año donde el número de amenazas ha supuesto un aumento significativo, observándose una continuidad en la progresión de los últimos años.

Los **ciberataques asociados a actores estado** han seguido en aumento, especialmente motivados por el creciente clima geopolítico, observándose cada vez mayor número de campañas contra infraestructuras críticas, tanto de ciberespionaje como con objetivos de denegación, disrupción, degradación o destrucción. También el **hacktivismo** se ha consolidado como una amenaza continua, tanto en lo referente al conflicto entre Rusia y Ucrania como en el conflicto entre Israel y Hamás, impactando no sólo de manera directa en sus objetivos sino también a nivel reputacional, realizando continuas acciones propagandísticas.

Los **modelos de negocio de RaaS y MaaS** han provocado que un mayor número de actores hostiles puedan crear y distribuir campañas sin necesidad de un alto nivel técnico, aumentando así su frecuencia e impacto en las organizaciones.

En cuanto a la **Inteligencia Artificial**, se ha observado la consolidación en la integración de modelos de IA generativa los procesos de los actores hostiles, lo que anticipa una mayor automatización tanto en la ejecución de campañas como en el descubrimiento de vulnerabilidades, desarrollo de código dañino y selección de objetivos, suponiendo un mayor número y sofisticación en las futuras campañas. Esto ha podido ser observado en la creciente actividad del periodo respecto a 2023, apuntando a esta misma tendencia en el futuro.

En consecuencia, es necesario que las organizaciones integren también este mismo tipo de capacidades en las tareas de prevención, detección y bloqueo de amenazas, especialmente en la protección del acceso a la organización y la infraestructura en la nube.



CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional