Threat Landscape Report 2025

Primer semestre

THALES

> Contenidos

INTRODUCCIÓN

Este informe analiza en profundidad la evolución del panorama de las ciberamenazas y subraya cómo las tensiones geopolíticas están influyendo cada vez más en la seguridad de gobiernos e infraestructuras críticas.

A lo largo del documento se presenta un repaso detallado de los incidentes más relevantes observados en el primer semestre de 2025, entre los que destacan las amenazas de ransomware, el incremento de sofisticación del malware, las campañas de phishing y los compromisos en la cadena de suministro. Asimismo, se presta especial atención al papel creciente de los grupos hacktivistas y de APTs —principalmente de Rusia, China, Irán y Corea del Norte—, así como las técnicas de ataque más utilizadas y la rápida explotación de vulnerabilidades zero-day por parte de grupos cibercriminales.

Más allá del análisis, este informe pretende servir como un recurso estratégico para profesionales de la ciberseguridad y responsables de la toma de decisiones, tanto en el ámbito público como en el privado. Al situar la intersección entre la geopolítica y las ciberamenazas, proporciona una visión integral de los riesgos actuales y emergentes, ayuda a las organizaciones a evaluar su nivel de exposición y priorizar sus activos a proteger. Del mismo modo, aporta elementos prácticos para fortalecer la ciberresiliencia, diseñar políticas de gestión de riesgos adaptadas a cada sector y fomentar la cooperación entre la industria y los organismos gubernamentales. Finalmente, constituye también una base de apoyo para la planificación de escenarios y los ejercicios de modelización de amenazas, facilitando la transición de posturas reactivas hacia enfoques proactivos de anticipación y mitigación.

Vulnerabilidades

Según los datos de la National Vulnerability Database (NIST), durante el primer semestre de 2025 se ha detectado ***un total de 27.498 vulnerabilidades****. Esto supone un notable aumento en la cantidad de vulnerabilidades descubiertas explotadas en entornos reales, a lo que se suma también un aumento de su complejidad. Esta tendencia al alza ya se venía consolidando desde años anteriores, pero en 2025 se ha intensificado, marcando un nuevo pico, tanto en volumen como en velocidad de explotación.*

Uno de los cambios más significativos es que los atacantes están aprovechando vulnerabilidades con una gran rapidez, lo cual implica que muchos de los fallos explotados son de tipo zero-day. Esto refleja no solo una mejora en la capacidad ofensiva de actores maliciosos, sino también una creciente brecha entre la detección y la mitigación efectiva de amenazas.

VULNERABILIDADES ZERO-DAY

Durante el primer semestre de 2025 se han identificado más **zero-day explotadas activamente en el entorno real**. Además, destaca que muchas de estas vulnerabilidades han sido utilizadas en ataques dirigidos por actores patrocinados por estados, especialmente en sectores gubernamentales, tecnológicos e infraestructuras críticas.

Algunas de las vulnerabilidades destacadas durante el primer semestre de 2025 han sido las siguientes:

Vulnerabilidades en hipervisores (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226)

Durante el primer semestre de 2025, un conjunto de vulnerabilidades afectó a productos clave de virtualización de software. Estas vulnerabilidades **comprometían por completo el principio de aislamiento** entre máquinas virtuales.

La criticidad de estas vulnerabilidades no se limita a su impacto técnico. Diversas fuentes, entre ellas la CISA, confirmaron que estas vulnerabilidades fueron explotadas activamente como zero-days, es decir, antes de que estuvieran disponibles parches oficiales.

Las vulnerabilidades se encadenaban para permitir el **acceso no autorizado** desde una máquina virtual hacia el sistema operativo anfitrión, con posibilidad de escalar privilegios hasta obtener control total del servidor físico.

A la fecha de su divulgación, se estimaba que más de 37.000 instancias expuestas seguían sin parchear, lo cual facilitó la propagación de campañas de explotación automatizada. Dado el nivel de acceso que esta vulnerabilidad otorga, atacantes pudieron utilizarla para exfiltrar información confidencial, desplegar malware, modificar imágenes de máquinas virtuales e, incluso, interferir con infraestructuras críticas.

Vulnerabilidad en un importante software de planificación de recursos empresariales (ERP) (CVE-2025-31324)

Este zero-day se origina por la **falta de una verificación de autorización** en el componente Metadata Uploader del Visual Composer, accesible a través del endpoint /developmentserver/metadatauploader. Un atacante no autenticado puede cargar archivos ejecutables arbitrarios, lo que puede resultar en **ejecución remota de código**.

La empresa emitió un parche de emergencia el 24 de abril de 2025 (Security Note 3594142). Debido a que este parche no resolvía completamente la causa raíz, se lanzó una segunda actualización de seguridad (Security Note 3604119), publicada el 13 de mayo, que abordó el problema subyacente de deserialización asociado con CVE-2025-42999. Ambas CVEs fueron añadidas al catálogo KEV de CISA el 29 de abril y el 15 de mayo.

VULNERABILIDADES EN ENTORNOS IOT

La seguridad de los dispositivos del Internet de las Cosas (IoT) ha continuado siendo una **preocupación clave** durante el primer semestre de 2025. La creciente adopción de estos dispositivos en entornos domésticos, empresariales e infraestructuras críticas ha traído consigo una expansión en la superficie de ataque y, con ello, un aumento en las vulnerabilidades detectadas.

A continuación, se destacan algunas vulnerabilidades relevantes descubiertas o ampliamente explotadas durante este período:

CVE-2025-45987

Una vulnerabilidad que afecta a múltiples modelos de routers Blink (BL-WR9000, BL-AC2100_AZ3, BL-X10_AC8, BL-LTE300, BL-F1200_AT1, BL-X26_AC8, BL-AC450M_AE4, BL-X26_DA3). El problema radica en una inyección de comandos a través de los parámetros dns1 y dns2 en la función bs_SetDNSInfo, lo que permite la ejecución de comandos arbitrarios mediante solicitudes manipuladas al panel de administración.

CVE-2025-29660

Una vulnerabilidad que afecta al Yi IOT XY-3820 v6.0.24.10, donde el proceso daemon expone un servicio TCP en el puerto 6789 sin validación de entrada adecuada, permitiendo la ejecución de scripts arbitrarios mediante solicitudes TCP especialmente diseñadas y técnicas de navegación de directorios.

CVE-2025-52471

Una vulnerabilidad que afecta al framework de desarrollo IoT ESP-IDF (versiones 5.4.1, 5.3.3, 5.2.5 y 5.1.6) en la implementación del protocolo ESP-NOW. Un subdesbordamiento de enteros en la función de recepción de paquetes del componente Wi-Fi ESP puede provocar accesos a memoria fuera de límites y escrituras arbitrarias, lo que en sistemas sin protección de memoria podría derivar en ejecución remota de código (RCE). Corregido en versiones posteriores con una validación más estricta de la longitud de los datos.

OTRAS VULNERABILIDADES

Por otro lado, es cada vez más común que la explotación de vulnerabilidades se combine con técnicas de ingeniería social, como el phishing, ya que los ciberdelincuentes buscan maximizar el impacto de sus campañas. La explotación de vulnerabilidades permite **automatizar el proceso de infección**, comprometer sistemas de forma rápida y facilitar el robo de credenciales o la instalación de malware.

Una vulnerabilidad que ha sido utilizada en este período en ataques de phishing es CVE-2025-21298, una vulnerabilidad zero-click que permite a los atacantes ejecutar código de forma remota simplemente enviando un correo electrónico especialmente manipulado. Esta vulnerabilidad no requiere que el usuario interactúe con el correo (como abrir adjuntos), ya que puede ejecutarse al visualizar o previsualizar el mensaje. En el primer semestre de 2025, se reportaron casos en los que correos maliciosos que suplantaban a organizaciones de confianza se utilizaron para entregar cargas maliciosas y **exfiltrar datos sensibles** de forma automática, permitiendo a los atacantes obtener acceso no autorizado e infiltrarse más profundamente en entornos corporativos.

Finalmente, cabe destacar las vulnerabilidades explotadas en herramientas y sistemas de gestión utilizados por empresas, tanto pequeñas como grandes multinacionales, que resultan especialmente atractivos para los ciberdelincuentes. Se trata de aplicaciones de uso cotidiano como herramientas de colaboración, correo electrónico y videoconferencia. Un ejemplo es CVE-2025-32711 (EchoLeak), una vulnerabilidad zero-click de inyección de prompt que puede extraer información corporativa sensible sin interacción del usuario. Este tipo de fallos en numerosas aplicaciones empresariales representan una amenaza crítica, ya que permiten a los atacantes acceder a información confidencial, interrumpir comunicaciones, filtrar datos o incluso desplegar malware dentro de las redes corporativas. La naturaleza interconectada de estas aplicaciones implica que **una sola vulnerabilidad pueda tener efectos en cascada**, comprometiendo no solo a un usuario, sino a toda la organización.

> En resumen, el primer semestre de 2025 ha estado marcado por **un aumento en el número y la sofisticación** de las vulnerabilidades y ciberataques, con ciberdelincuentes que se adaptan notablemente a las nuevas tecnologías y a plataformas impulsadas por inteligencia artificial. Esto subraya la necesidad de mantener una **vigilancia constante** y de implementar medidas de **seguridad proactivas** para proteger los sistemas y datos sensibles.

Ransomware

Según la telemetría recopilada, el escenario global de amenazas ransomware se ha recrudecido, registrando un total de ***3.775 ataques****.*

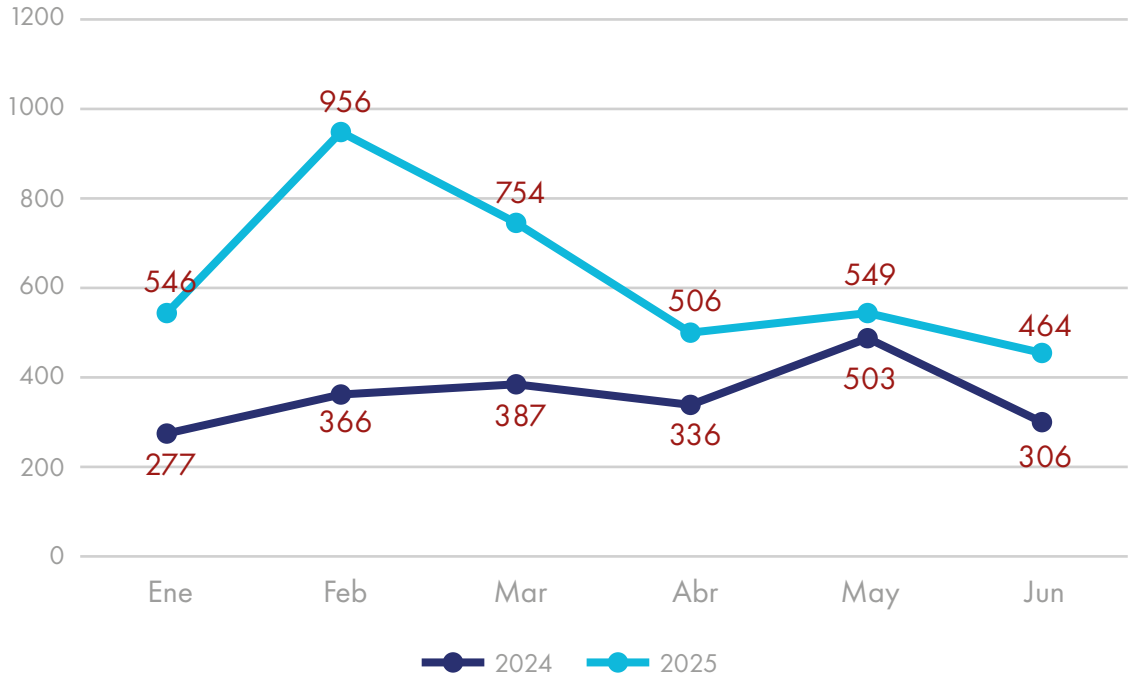
Durante la primera mitad de 2025, el equipo de Threat Intelligence de Thales ha continuado con la monitorización activa de la actividad por parte de grupos de ransomware en más de 80 blogs de la deep web.

Este primer semestre, los grupos de ransomware han mostrado un claro aumento en la sofisticación y frecuencia de los ataques, así como un continuo cambio y adaptación de las estrategias, métodos y modelos de trabajo.

Siguiendo el modo de operación de años anteriores, los grupos han continuado empleando el modelo de ransomware-as-a-service, aunque destaca una clara tendencia por ciertos grupos como Babuk, SecP0 y Silent Ransom Group a realizar únicamente el robo y extorsión de los datos sin cifrado, lo que parece marcar un cambio en el panorama del ransomware.

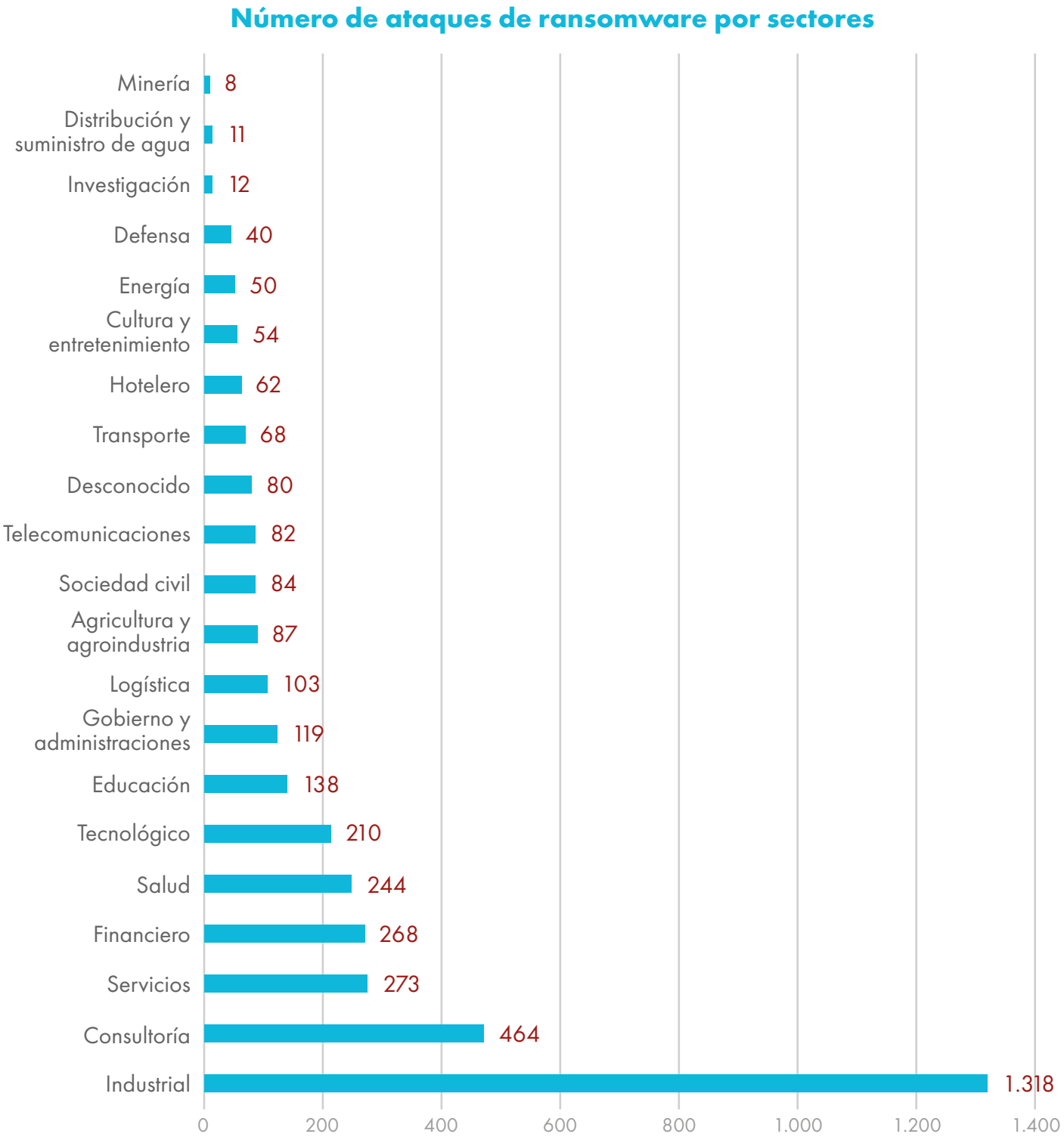
En el primer semestre de 2025 se registran 3.775 ataques, un **aumento del 74%** respecto al primer semestre de 2024.

Número de ataques de ransomware en el primer semestre de 2024 y 2025



SECTORES MÁS AFECTADOS

En cuanto a los sectores afectados, en primera posición se encuentra el sector **industrial** con 1.318 empresas afectadas, lo que supone un 34,9% del total, seguido por el sector de **consultoría** con 464 ataques (12,3%) y el sector **servicios** con 273 (7,2%). Otros sectores que destacan según la afectación de ataques son el sector **financiero** con 268 ataques (7%), el sector **salud** con 244 (6,5%) y el sector **tecnológico** con 210 (5,6%).



PAÍSES MÁS AFECTADOS

Siguiendo la tendencia de años anteriores, los grupos de ransomware se han dirigido principalmente a objetivos localizados en América del Norte, región que se corresponde con el 58% del total de ataques registrados. El país más afectado es **Estados Unidos**, con 1.923 entidades reivindicadas, seguido por **Canadá** con 218 ataques.

Según la afectación en el resto de las regiones, Europa aglutina el 22% del total, siendo **Alemania**, **Reino Unido** e **Italia** los países más afectados con 151, 141 y 92 ataques respectivamente.

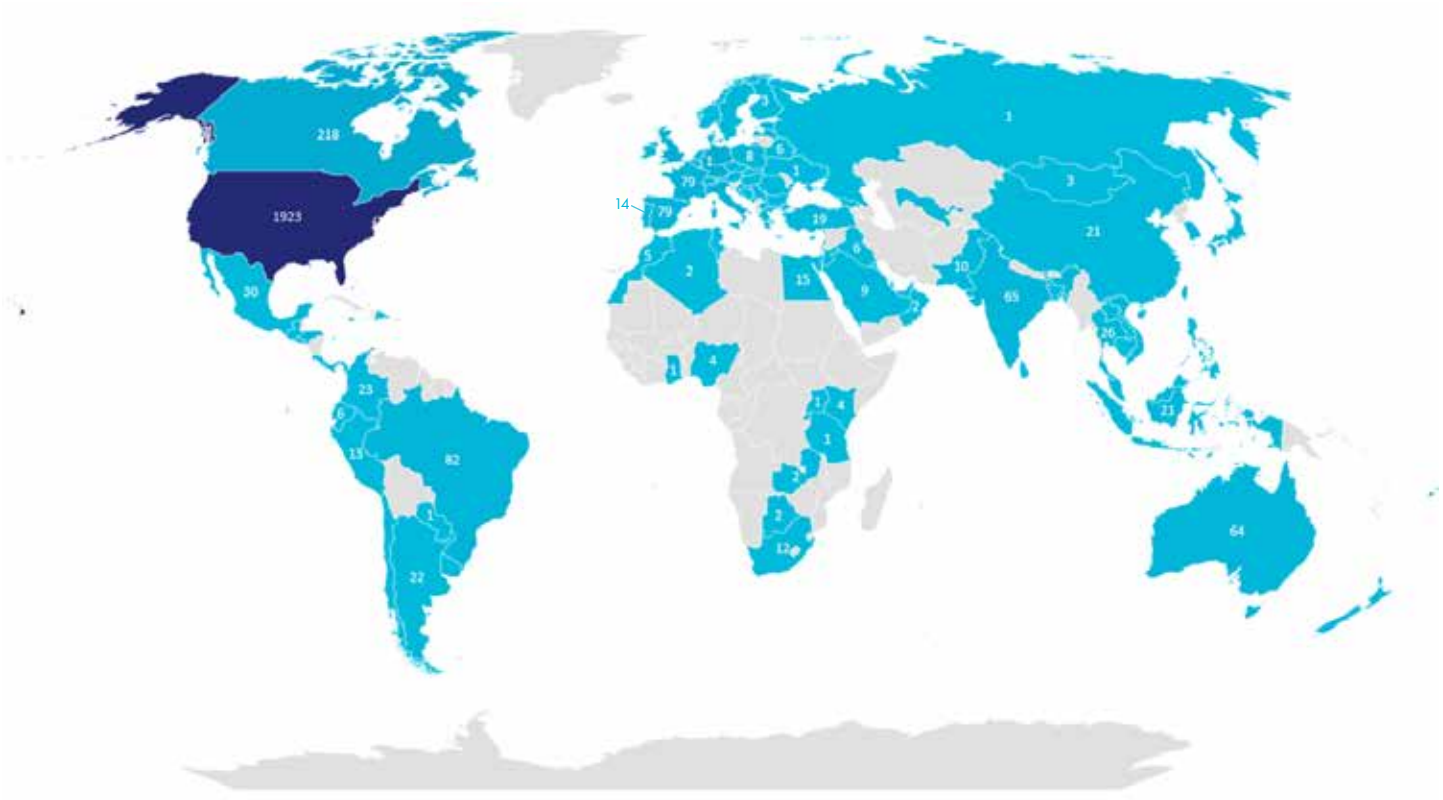
Tanto Francia y España se posicionan como el séptimo país más perjudicado por la amenaza ransomware en el primer semestre de 2025, con ambos registrando un total de 79 ataques.

Por un lado, **Francia muestra un aumento del 25%** respecto al primer semestre de 2024 en el que se reivindicaron 63 empresas francesas. En cuanto a las familias de ransomware más destacadas se encuentran Qilin con 11 ataques, 8Base y Cl0p ambos en segunda posición con 6 ataques cada uno y, en tercera posición, Lynx y Fog, con 5 ataques.

Respecto a **España**, durante el primer semestre de 2024 se documentaron 58 ataques, lo que supone un **incremento del 36%** entre el primer semestre de 2024 y 2025. Akira se posiciona como la amenaza más destacada con 15 ataques registrados, seguida por Qilin con 10 ataques y Fog con 5 ataques.

Finalmente, **Portugal** muestra una afectación de 14 organizaciones atacadas, **un aumento del 250%** respecto al primer semestre de 2024, en el que 4 entidades portuguesas sufrieron ataques de ransomware. En cuanto a las familias que se han dirigido hacia Portugal se encuentran Akira (la más prolífica con 3 ataques) y Nightspire, Nitrogen y Warlock con 2 ataques cada uno.

Asimismo, como anteriormente fue visto con la guerra entre Rusia y Ucrania, los conflictos geopolíticos han afectado de manera significativa a la victimología, con un aumento de los ataques a organizaciones gubernamentales y defensa, así como a entidades israelíes, entre otras.



GRUPOS NUEVOS

En 2025 continúa la tendencia a la proliferación de nuevas variantes que se suman a las amenazas de ransomware ya existentes.

En el primer semestre de 2025, se ha registrado un total de **32 nuevas operaciones de ransomware**, un aumento del 60% respecto al semestre anterior. Teniendo en cuenta los valores de años anteriores, el número de nuevas familias de ransomware ha ido incrementándose con gran celeridad, mostrando una tendencia creciente pronunciada, que junto al aumento de ataques generan una gran preocupación.

Entre los nuevos grupos se encuentran GDLockerSec, Babuk, Kraken, Linkc, Anubis, Run Some Wares, Skira, Weyhro, CrazyHunter, NightSpire, SecP0, VanHelsing, Frag, Arkana, RALord, Chaos, Bert, Devman, Crypto24, Silent, Gunra, IMN Crew, J Group, WorldLeaks, Silent Ransom Group, DataCarry, Dire Wolf, Global, WALocker, TeamXXX, Warlock y Kawa4096.

GRUPOS DE RANSOMWARE MÁS ACTIVOS

AKIRA

En el primer semestre de 2025, **Akira** se consolida como el grupo de ransomware más prolífico con **355 ataques registrados**, lo cual supone un 9% del total. Se ha dirigido principalmente a los sectores **industriales** con 160 ataques, **consultoría** con 56 y **finanzas** con 30. En cuanto a la afectación geográfica vemos una tendencia hacia Estados Unidos, al que se dirigió 193 veces, seguido por Italia con 17 y Alemania con 16.

El ransomware Akira, también conocido como **Redbike**, comienza a operar en marzo de 2023 dirigiéndose hacia sistemas Windows, Linux y máquinas virtuales. Las primeras versiones del malware están escritas en C++ y encriptan los archivos con la extensión .akira, aunque desde agosto de 2023, se detectaron ciertos ataques empleando la variante **Megazord** escrita en Rust con la extensión .powerranges. Las tácticas de acceso inicial de Akira incluyen el uso de credenciales robadas, la explotación de vulnerabilidades en software, campañas de phishing y ataques de fuerza bruta a RDP.

Durante el primer semestre de 2025 se detectó una campaña en la que el grupo explotó una vulnerabilidad en SimpleHelp RMM para obtener acceso no autorizado a redes corporativas. Su ataque se caracteriza por una rápida ejecución de tácticas post-compromiso, incluyendo el descubrimiento de redes y sistemas, la creación de una cuenta de administrador denominada sqladmin y el establecimiento de persistencia mediante la instalación de una backdoor llamada agent.exe.

También se descubrió un incidente de seguridad en el cual Akira logró cifrar la red de una empresa utilizando una webcam insegura, evitando así la detección por parte de las soluciones de seguridad Endpoint Detection and Response (EDR). Los atacantes accedieron a la red corporativa mediante credenciales robadas o ataques de fuerza bruta y, tras ser bloqueados por el EDR, identificaron una webcam vulnerable con un sistema basado en Linux, sin protección y con acceso remoto no autorizado. Aprovechando estas vulnerabilidades, los atacantes montaron las unidades de red de la empresa en la webcam y ejecutaron el cifrado desde allí, logrando evadir la detección. Este incidente resalta la necesidad de actualizar los dispositivos IoT y aislarlos de redes críticas para evitar brechas de seguridad.

Asimismo, a principios de año se descubrió la utilización del software AnyDesk, una herramienta legítima de gestión remota empleada por el grupo, para lograr persistencia en los sistemas comprometidos. El uso de AnyDesk permite a los atacantes conectarse a los dispositivos reduciendo la probabilidad de detección, pues no se emplean herramientas maliciosas tradicionales. Esta estrategia subraya la creciente sofisticación de los cibercriminales, que recurren a herramientas comunes para evadir la detección y mantener el control sobre los sistemas de sus víctimas.

CL0P

En segundo lugar, se posiciona el grupo de ransomware **Cl0p**, con **331 ataques** dirigidos principalmente hacia Estados Unidos (231 ataques) y Canadá (32 ataques) en los sectores **industrial** (173 ataques), de **logística** (37 ataques) y **tecnológico** (22 ataques).

El grupo fue observado por primera vez en 2019, realizando campañas e intentos de phishing, fuerza bruta y la explotación de vulnerabilidades conocidas. Desde entonces ha ido evolucionando en sofisticación, propagándose mediante enlaces maliciosos en correos electrónicos, páginas web y otros enlaces fraudulentos. Para cifrar los archivos, emplea el algoritmo AES-256 en combinación con AES, RSA y RC4. Además, cuenta con la capacidad de propagarse a través de redes, lo que le permite comprometer múltiples dispositivos simultáneamente. El grupo es conocido por la **explotación de servicios de transferencia de archivos**, lo cual les permitió llevar a cabo un ataque en masa a los usuarios del servicio Progress Software's MOVEit y GoAnywhere en 2023 que tuvo una gran afectación.

En febrero de 2025, el grupo cobra relevancia tras la reivindicación de 320 entidades en su página de la dark web. En ataques previos, Cl0p solía compartir detalles sobre las vulnerabilidades explotadas, pero en esta ocasión, su lista de reivindicaciones carecía de dicha información. No obstante, los analistas de seguridad sugieren que el grupo podría haber aprovechado las vulnerabilidades CVE-2024-50623 y CVE-2024-55956 del software de transferencia de datos de Cleo que afectan a Cleo Harmony (versiones anteriores a 5.8.0.21), VLTrader (antes de la versión 5.8.0.21) y LexiCom (antes de la versión 5.8.0.21). CVE-2024-50623 permite la subida de archivos maliciosos al servidor para posteriormente ejecutarlos de forma remota. Este problema surge de un manejo inadecuado del directorio Autorun, que puede ser explotado enviando solicitudes de recuperación o subida de archivos maliciosos. CVE-2024-55956 permite la ejecución remota de código mediante Autorun, permitiendo a usuarios no autenticados importar y ejecutar comandos en Bash o PowerShell en el host utilizando las configuraciones del directorio Autorun. Este fallo también permite al atacante emplear backdoors y realizar movimientos laterales. Sin embargo, cabe destacar que el grupo anteriormente ha llegado a exagerar el número de víctimas para ganar atención.

QILIN

Finalmente, el grupo **Qilin**, también conocido como **Agenda**, se ha dirigido a **324 organizaciones industriales** (con 114 ataques), de **consultoría** (44 ataques) y de **salud** (35 ataques) de Estados Unidos (186 ataques) y Canadá (26 ataques).

Qilin emergió en octubre de 2022 y desde entonces se ha convertido en uno de los grupos más prometedores en el ámbito del ransomware, destacando por su **infraestructura técnica avanzada** y su enfoque integral hacia el cibercrimen como servicio. Utiliza malware desarrollado en Rust y C, dotado de sofisticadas capacidades de evasión, y proporciona a sus afiliados herramientas como ejecución en modo seguro, propagación en red, limpieza de registros y negociación automatizada. Además, el grupo ofrece servicios complementarios como campañas de spam, almacenamiento de datos a escala petabyte y asesoría legal, posicionándose no solo como una operación de ransomware, sino como una **plataforma criminal completa**.

Su ascenso coincide con el colapso de otros grupos, lo que le ha permitido consolidarse como líder en un ecosistema cada vez más inestable. A principios de abril de este año, el grupo de ransomware Ransomhub cesó sus operaciones, lo que provocó una migración de sus afiliados hacia otros grupos, entre ellos Qilin, lo que ha incrementado de forma considerable el número de ataques reivindicados por ellos en los últimos meses.

Se ha detectado a afiliados de Qilin haciendo uso de una nueva técnica conocida como bring-your-own-vulnerable-driver (BYOVD), empleando un driver conocido como TPwSav.sys que les permite desactivar las medidas de seguridad de EDR. Este driver, se diseñó originalmente para guardar batería de portátiles, por lo que está firmado por Windows, haciéndolo una opción atractiva para evadir el EDR. También, se han descubierto a varios actores de amenazas relacionados con Qilin empleando los malware SmokeLoader y NETXLOADER en sus campañas.

Asimismo, se ha detectado un ataque a una empresa proveedora de servicios gestionados (MSP) mediante un correo de phishing que suplantaba una alerta de autenticación de la herramienta de monitoreo y gestión Screen Connect. Tras esto el grupo ganó acceso al sistema que aprovechó para dirigir ataques de ransomware a múltiples clientes de la empresa. Este ataque se asocia a un afiliado que en 2022 ya realizó ataques similares con la misma infraestructura, patrones de nombramiento de dominios, técnicas herramientas y prácticas.

Durante los meses de mayo y junio, Qilin ha explotado activamente las vulnerabilidades CVE-2024-55591 y CVE-2024-21762 en sus campañas. Cabe destacar que la primera fue utilizada como zero-day en noviembre de 2024 por grupos como LockBit, mientras que la segunda, a pesar de haber sido parcheada en febrero, aún afecta a aproximadamente 150.000 dispositivos vulnerables.

Conflictos internacionales

*En los últimos años se ha observado un **aumento** de conflictos de alta intensidad y gran alcance. Estos eventos han dominado los asuntos globales. El primer semestre de 2025 fue una continuación de las tensiones geopolíticas presentes en el año anterior.*

El panorama permanece como un campo de batalla en el que los conflictos internacionales se desarrollan mediante operaciones híbridas.

CONFLICTO ARMADO ENTRE RUSIA Y UCRANIA

El conflicto armado entre Rusia y Ucrania **sigue siendo el conflicto más grande en Europa** desde la Segunda Guerra Mundial. A mediados de 2025, Rusia controla alrededor del 20 por ciento de los territorios reconocidos internacionalmente como ucranianos. Los esfuerzos bélicos se habían trasladado al ámbito cibernético incluso antes de la invasión rusa en febrero de 2022. Ambos estados han utilizado ciberataques a su favor. En 2025, los objetivos observados han sido **infraestructuras críticas**, **instituciones gubernamentales**, **medios de comunicación** y organizaciones que trabajan en el sector de **defensa**.

Los atacantes, identificados principalmente como actores patrocinados por el Estado y hacktivistas, han empleado técnicas como ingeniería social, distribución de malware y ataques DDoS para desestabilizar la sociedad, socavar la confianza pública en el Estado y obtener datos mediante espionaje para ganar ventaja en el conflicto.

Ciberespionaje y Ciberataques

Una característica definitoria de la dimensión cibernética del conflicto son las **campañas de espionaje** de Rusia y Ucrania que buscan obtener ventaja mutua. En 2025, diversas campañas han sido reveladas por investigadores, como el caso de la campaña rusa llamada "Double-Tap" que tuvo como objetivo Kazajistán. Los ataques se enfocaron en las relaciones diplomáticas y económicas de Kazajistán con países occidentales y asiáticos, dado que el país se ha ido distanciando de Rusia y fortaleciendo sus vínculos con China y Europa.

Además de las campañas de espionaje, ambos países han escalado el conflicto con **ataques dirigidos a infraestructuras críticas**. En el primer semestre de 2025, se observó una mayor combinación entre grupos patrocinados por el Estado y ciberdelincuentes. Unidades cibernéticas rusas como APT44 y Sandworm desplegaron malware tradicionalmente asociado con cibercriminales para interrumpir la logística y el transporte en Ucrania. Ucrania también intensificó sus operaciones ofensivas contra la infraestructura digital rusa. Su inteligencia lanzó varios **ciberataques contra la logística civil e industrial**.

Desinformación e Influencia Estratégica

En el primer semestre de 2025, las campañas de desinformación siguen siendo un **pilar central en la estrategia** de Rusia, con un enfoque principal en países europeos. En Alemania y Polonia, las campañas tuvieron un enfoque político, con el objetivo de influir en elecciones. Las actividades rusas se centraron en atacar a políticos con noticias falsas e historias circulando en plataformas de redes sociales. En Austria, las campañas de influencia combinaron noticias falsas con grafitis y pegatinas manipuladoras para socavar a los ucranianos. Además, los esfuerzos de desinformación en el primer semestre de 2025 se extendieron más allá de Europa: en Sudáfrica se detectaron campañas pagadas en redes sociales destinadas a desacreditar al liderazgo ucraniano antes de conversaciones diplomáticas.

Actividades Hacktivistas

En este conflicto, los grupos hacktivistas son un elemento crucial. Estos grupos participan frecuentemente en **ataques de denegación de servicio distribuido (DDoS)** y filtraciones de datos. En 2025, los grupos hacktivistas pro-rusos son más prominentes que sus contrapartes pro-ucranianas. Su actividad puede interrumpir operaciones y causar un impacto serio en los objetivos afectados. En 2025, los hacktivistas rusos atacaron infraestructuras críticas en Noruega explotando protocolos de seguridad débiles en una presa.

CONFLICTO ISRAEL-PALESTINA

El conflicto, que comenzó en 2023, se extendió a 2025 con una **escalada de violencia** que a menudo involucró a más organizaciones internacionales. Aunque se acordó una tregua que luego fue descartada, la dimensión cibernética del conflicto permaneció igual: dominada por **grupos patrocinados por el Estado y hacktivistas**.

Respecto a la actividad estatal, a principios de 2025, investigadores descubrieron que la unidad de inteligencia militar israelí 8200 estaba desarrollando un potente LLM entrenado con un conjunto de datos de comunicaciones palestinas interceptadas. El modelo de IA está diseñado para **detectar amenazas y patrones potenciales**, siendo capaz de identificar y monitorear individuos, ayudando a las operaciones militares y de inteligencia en los territorios ocupados. Esta operación, junto con otras, demuestra el interés de Israel en la recolección de inteligencia y campañas de vigilancia en lugar de la interrupción de infraestructuras críticas mediante ciberataques.

Las operaciones cibernéticas palestinas son menos numerosas, debido a recursos limitados, pero las que existen reflejan un interés en la recopilación de inteligencia.

En cuanto a la actividad hacktivista, al igual que el año anterior, los grupos **hacktivistas pro-palestinos** destacan sobre los pro-israelíes. Al igual que en años previos, las operaciones hacktivistas **OpIsrael** y **OpJerusalem** se llevaron a cabo alrededor de marzo y abril, dirigidas contra Israel. A raíz de ambas campañas, actores no estatales incrementaron su actividad contra entidades israelíes, realizando ciberataques como *defacing* de sitios web, ataques de denegación de servicio distribuido (DDoS), distribución de ransomware y filtraciones de datos. Varios grupos hacktivistas participan en estas operaciones que, a lo largo de los años, han provocado ocasionalmente interrupciones temporales en sitios web del gobierno, militares y sector privado israelí. En el primer semestre de 2025, la campaña se extendió más allá de Israel, atacando también a aliados internacionales y entidades que apoyan las políticas israelíes, demostrando el efecto de desbordamiento del conflicto.

GUERRA ISRAEL-IRÁN

El primer semestre de 2025 incluyó una guerra de 12 días entre Israel e Irán. El conflicto comenzó cuando Israel lanzó una **gran ofensiva aérea** contra Irán, llamada Operación León Ascendente, el 13 de junio de 2025. La operación fue descrita como un ataque preventivo para eliminar la amenaza representada por el poder nuclear iraní. Aunque el conflicto físico ocurrió en 2025, el conflicto cibernético ha estado activo durante los años previos. Sin embargo, los analistas observaron un **aumento del 700% en ciberincidentes relacionados** con este conflicto después del ataque aéreo.

Los grupos **APT34** y **APT42** vinculados a Irán atacaron las industrias de energía, telecomunicaciones y transporte de Israel. Mientras que grupos hackers vinculados a Israel atacaron infraestructura iraní, principalmente en los sectores bancario y financiero. Además de las operaciones APT y grupos estatales de ambos lados, se detectaron campañas de desinformación en redes sociales.

La combinación de ciberincidentes refleja la intensidad de las operaciones físicas. Irán, en medio de crecientes ciberamenazas, implementó un apagón de internet a nivel nacional para reducir el impacto de posibles operaciones israelíes.

Los grupos hacktivistas han participado en el conflicto, siendo responsables de gran parte de los ataques y teniendo un rol prominente. La mayoría de los grupos identificados se declaran pro-Irán, muchos de ellos con agendas pro-palestinas y antioccidentales. Las operaciones hacktivistas impulsadas por una coalición de actores con agendas similares buscan atacar a Israel mediante ataques DDoS, accesos no autorizados, brechas de datos y ransomware. Los grupos también utilizan sus canales de comunicación para amplificar sus narrativas geopolíticas alineadas.

CONFLICTO INDIA-PAKISTÁN

En 2025, India y Pakistán escalaron sus tensiones a una **confrontación militar a gran escala** tras un ataque terrorista en territorio indio perpetrado por militantes pakistaníes. Mientras Pakistán negó su implicación, India acusó al Estado de apoyar el terrorismo transfronterizo. India suspendió el Tratado de Aguas del Indo, expulsó diplomáticos pakistaníes, cerró la frontera Attari-Wagah e impuso una prohibición de viaje a ciudadanos pakistaníes. En represalia, Pakistán calificó las medidas indias como un acto de guerra, cerró su espacio aéreo a aerolíneas indias y suspendió el comercio.

El 7 de mayo, India lanzó la **Operación Sindoor**, donde una serie de ataques con misiles apuntaron a infraestructuras militares en Pakistán. El Estado pakistaní respondió con la **Operación Bunyanun Marsoos**, realizando ataques con misiles contra entidades que identificó como promotoras del terrorismo en su territorio. Fue la primera vez que ambos países participaron en guerra con drones.

La rivalidad cibernética entre India y Pakistán ha sido un problema durante décadas, pero en el primer semestre de 2025 fue la primera vez que operaciones cibernéticas se desvelaron con una campaña militar activa. Tras el ataque terrorista que inició el conflicto, se detectó un **aumento de ciberataques** en India dirigidos a sectores críticos. Actores patrocinados por el Estado pakistaní, como **APT36**, realizaron campañas. El panorama cibernético también estuvo marcado por actores independientes que desplegaron ataques DDoS, accesos no autorizados, brechas de datos y ransomware. India también realizó ciberataques que afectaron sectores importantes y sitios web. Ambos países se enfocaron en campañas de influencia en redes sociales amplificando sus narrativas.

Aunque se alcanzó un acuerdo de alto el fuego, la relación entre ambos Estados sigue siendo propensa a crisis, con tensiones que probablemente escalen en severidad con el tiempo.

TENSIONES CHINA-TAIWÁN

En el primer semestre de 2025, China y Taiwán se acusaron mutuamente de **ciberguerra**. Ambos gobiernos han compartido públicamente acusaciones de operaciones cibernéticas sofisticadas contra el otro. Generalmente, los ataques tienen como objetivo las redes gubernamentales, militares y del sector privado. Las acusaciones fueron escaladas por China, que acusó a Taiwán de patrocinar una campaña que comprometió 1.000 redes militares, energéticas y gubernamentales, además de acusar al Estado de atacar sistemas de infraestructura de Beijing en ataques coordinados ocurridos en marzo de 2025.

Los analistas observaron una escalada en el conflicto cibernético, señalando un **fuerte aumento de incidentes** vinculados a China que tienen como objetivo a Taiwán. Los incidentes se centran especialmente en infiltraciones en infraestructuras gubernamentales y de telecomunicaciones. Taiwán también acusó a China de lanzar campañas de desinformación para socavar su reputación internacional.

ÁFRICA

Aunque no es un conflicto regional, es crucial reconocer el **aumento de las ciberamenazas en África**. Se ha confirmado que más del 30% de todos los crímenes registrados en África Occidental y Oriental son ciberdelitos, con dos tercios de los estados miembros africanos afirmando que los delitos relacionados con la cibernética representan un porcentaje medio a alto de todos los crímenes. Las ciberamenazas más reportadas incluyen estafas en línea (particularmente phishing), ransomware (los países más afectados son Sudáfrica y Egipto), compromiso de correos electrónicos comerciales (BEC) y sextorsión digital. Los incidentes cibernéticos observados atacan infraestructura crítica y el sector gubernamental.

SUDAMÉRICA

Aunque no es un conflicto regional, en el primer semestre de 2025 América Latina ha experimentado un aumento en incidentes cibernéticos, enfrentando una **tasa de ciberataques superior al promedio global.** Los estados más afectados son Perú, Colombia, México, Jamaica y Paraguay. Los incidentes en la región varían entre malware avanzado, operaciones vinculadas a gobiernos y vulnerabilidades, frecuentemente relacionadas con plataformas en la nube. En cuanto al riesgo industrial, los sectores que han enfrentado el mayor número de ataques incluyen gobierno, militar, salud y telecomunicaciones.

Malware

*En 2025, se ha observado una **sofisticación creciente** en las técnicas de distribución y evasión de malware. Las amenazas más destacadas incluyen infostealers como Lumma y FleshStealer, loaders como Necro y Meta, y RATs como NetSupport y SugarGh0st. Además, han emergido nuevas técnicas de distribución, como "ClickFix" y "FileFlix", que explotan la interacción humana para eludir las defensas automatizadas.*

CLICKFIX

Se trata de una nueva técnica de ingeniería social que combina el engaño visual con la manipulación del navegador para inducir al usuario a ejecutar código malicioso manualmente. El atacante envía correos electrónicos, mensajes o notificaciones falsas que simulan alertas legítimas de plataformas de videoconferencia o servicios populares.

Al hacer clic en el enlace, el usuario es redirigido a una página web que simula un error crítico o un CAPTCHA que debe ser resuelto para continuar. Para "arreglar" el supuesto error, el usuario debe hacer clic en botones que, en realidad, ejecutan comandos de consola o descargas ocultas. Por ejemplo, el sitio puede pedir que se copie y pegue un comando en la consola (CMD, PowerShell o Terminal), o que se ejecute un archivo descargado que parece un parche o un complemento oficial.

Dado que la ejecución del malware depende de una acción directa del usuario (clic, ejecución manual), las soluciones antivirus y los sistemas de detección basados en comportamiento automatizado tienen dificultades para identificar la amenaza, pues no hay un proceso malicioso ejecutándose sin intervención. Una vez que el usuario ejecuta el comando o el archivo, se instala un malware (por ejemplo, infostealers como StealC o RATs como NetSupport), que queda oculto y empieza a robar información o controlar el sistema.

FILEFIX

Es una técnica de ataque emergente que se basa en ingeniería social avanzada, donde los usuarios son engañados para ejecutar comandos maliciosos a través de la barra de direcciones del Explorador de Archivos de Windows. Filefix aprovecha una funcionalidad legítima poco conocida: la posibilidad de ejecutar comandos directamente desde la barra del explorador, incluyendo llamadas a binarios del sistema (LOLBins) o incluso rutas remotas mediante protocolos como Search-MS o UNC. Los atacantes inducen a los usuarios a copiar y pegar comandos disfrazados de rutas legítimas, ocultando el código dañino mediante grandes espacios y comentarios HTML para que el contenido visible parezca inofensivo. Al presionar "Enter", el usuario ejecuta involuntariamente el payload.

Lo que vuelve a FileFix más preocupante que sus predecesores es su capacidad de explotar funcionalidades integradas de Windows sin necesidad de explotar vulnerabilidades técnicas.

LOADERS

Un loader es un tipo de malware cuyo propósito principal no es causar daño directo o robar información, sino actuar como un instalador para otros tipos de malware más dañinos, como infostealers, ransomware, troyanos de acceso remoto (RATs), entre otros.

En esencia, el loader es la puerta de entrada que permite desplegar y ejecutar las cargas útiles maliciosas en un sistema víctima.

META LOADER

Meta Loader se ha consolidado como uno de los loaders más activos y sofisticados en el primer semestre de 2025, destacándose en múltiples campañas de malware dirigidas a sistemas Windows y, en menor medida, a plataformas Android. Técnicamente, Meta Loader se propaga principalmente a través de campañas de phishing.

Su diseño modular le permite integrarse fácilmente en cadenas de ataque complejas, donde actúa como punto inicial para descargar y ejecutar payloads secundarios, facilitando la distribución de infostealers, ransomware y RATs.

Desde un punto de vista técnico, Meta Loader emplea conexiones cifradas con sus servidores de comando y control (C2), utilizando protocolos como HTTPS y, en ocasiones, canales personalizados que dificultan su detección por sistemas de monitoreo de red.

Meta Loader aprovecha técnicas avanzadas de persistencia y evasión. Modifica entradas del registro, crea tareas programadas y utiliza métodos fileless para mantener su presencia en el sistema sin dejar rastros evidentes en el disco. Su capacidad para cargar y ejecutar malware directamente en memoria sin necesidad de archivos visibles lo convierte en una amenaza difícil de detectar mediante antivirus tradicionales, aumentando su eficacia en campañas prolongadas y coordinadas.

Finalmente, la gran flexibilidad de Meta Loader lo ha hecho una herramienta preferida en campañas multietapa durante el primer semestre de 2025. Su capacidad para descargar y activar diferentes tipos de malware según las instrucciones recibidas permite a los atacantes cambiar rápidamente sus objetivos y métodos de ataque sin necesidad de modificar el loader base. Esta adaptabilidad, sumada a su evasión robusta, explica por qué Meta Loader ha sido tan prevalente en ataques recientes.

INFOSTEALER MALWARE

Durante el primer semestre de 2025, los infostealers han consolidado su posición como una de las principales amenazas en el panorama de la ciberseguridad. Estos programas maliciosos, diseñados específicamente para robar información sensible como credenciales, cookies, datos financieros y archivos personales, han evolucionado tanto en sofisticación como en alcance.

LUMMA STEALER

Lumma Stealer, también conocido como LummaC2, es un malware del tipo infostealer ofrecido bajo un modelo de Malware-as-a-Service (MaaS). Surgió en 2022, desarrollado por un actor identificado como Shamel y promocionado en foros clandestinos y canales de Telegram. Está diseñado para robar información sensible de equipos con Windows, incluyendo credenciales almacenadas en navegadores, billeteras de criptomonedas, extensiones 2FA y archivos personales, que luego exfiltra hacia servidores de comando y control (C2). Entre sus técnicas avanzadas destacan el uso de syscalls directos, process hollowing, y técnicas de ofuscación.

Su distribución se ha basado en campañas de phishing, malvertising, páginas fraudulentas de CAPTCHA, cracks de software y supuestas utilidades legítimas como "Free VPN" o "Minecraft Skin Changer" alojadas en GitHub. Con frecuencia, estas amenazas se presentan en archivos comprimidos con contraseña y utilizan mecanismos como carga dinámica de DLLs, inyección en memoria, técnicas anti-sandbox y ejecución a través de binarios legítimos de Windows como mshta.exe o MSBuild.exe. Este enfoque dificulta la detección y permite a los atacantes evadir gran parte de las defensas tradicionales.

Entre el 16 de marzo y el 16 de mayo de 2025, Microsoft detectó más de 394.000 sistemas Windows comprometidos por Lumma Stealer en todo el mundo. Como respuesta, una operación internacional liderada por Microsoft DCU, el Departamento de Justicia de EE.UU., Europol y socios privados consiguió interrumpir parte de su infraestructura: se incautaron o bloquearon unos 2.300 dominios maliciosos, incluyendo paneles de control y canales de distribución, y se redirigió tráfico hacia sinkholes para cortar la comunicación con los equipos infectados. Esta acción representó uno de los mayores intentos coordinados para frenar el impacto de este tipo de malware en 2025.

Sin embargo, desde junio se ha observado un resurgimiento de Lumma Stealer, con campañas más discretas y un cambio de infraestructura hacia proveedores menos colaborativos con las fuerzas de seguridad. Sus operadores han retomado el uso de cracks falsos, repositorios públicos y malvertising más selectivo, manteniendo una actividad constante en canales privados.

Esta capacidad de adaptación refuerza la idea de que Lumma Stealer seguirá siendo una amenaza persistente, obligando a las organizaciones a mantener una estrategia defensiva proactiva basada en inteligencia de amenazas, actualizaciones continuas de detección y cooperación internacional.

REMOTE ACCESS TROJAN

En 2025, los RATs continúan evolucionando con características avanzadas de evasión, incluyendo detección de sandbox, uso de técnicas fileless, y capacidad de moverse lateralmente dentro de redes. Su modularidad y escalabilidad los hacen una herramienta favorita tanto para ciberdelincuentes comunes como para actores patrocinados por estados.

NETSUPPORT

NetSupport RAT es la versión maliciosa del software legítimo NetSupport Manager, creado originalmente para administración remota de sistemas. Los actores adversos lo han reutilizado como un poderoso troyano de acceso remoto (RAT), aprovechando su amplia gama de funcionalidades legítimas para monitorear y controlar dispositivos infectados de forma encubierta. Este abuso del software ha sido recurrente desde al menos 2017 y se ha observado su proliferación en campañas como la vinculada a la pandemia, facilitando su distribución masiva.

Las campañas de distribución de NetSupport RAT utilizan una variedad de técnicas de engaño, incluyendo actualizaciones falsas del navegador, páginas fraudulentas de Docusign o Gitcode, descargas de PowerShell en múltiples etapas y alertas falsas de verificación CAPTCHA.

Malware móvil

Continuando con una tendencia similar a la de los últimos años, durante la primera mitad de 2025 el malware dirigido a dispositivos móviles ha mantenido una ***presencia significativa*** *en el panorama de amenazas. La presencia constante tanto de móviles como tabletas en la vida cotidiana, profesional y educativa hace que este tipo de dispositivos se conviertan en objetivos prioritarios para los cibercriminales. Si bien cada sistema se ve afectado de manera diferente, tanto los dispositivos Android como iOS han visto la aparición o evolución de diversas familias de malware dirigidos contra ellos.*

MALWARE ANDROID

La gran mayoría de familias de malware encontradas en dispositivos móviles puede agruparse en dos categorías principales: troyanos bancarios y spyware. En el caso de dispositivos Android, se han identificado numerosas variantes nuevas, así como actualizaciones de otras ya conocidas que se enmarcan en esas dos categorías.

Troyanos bancarios

Este tipo de programa tiene como objetivo principal **robar las credenciales del usuario** para acceder a entidades financieras, interceptar comunicaciones con las mismas o manipular transacciones. Suelen hacerse pasar por aplicaciones legítimas tanto en tiendas oficiales, como Google Play, como en markets de terceros.

Durante el mes de marzo se descubrió un nuevo troyano de este tipo al que los investigadores han denominado **Crocodilus**. Durante dicha campaña se identificaron víctimas tanto en Europa como en Sudamérica, siendo distribuido a través de anuncios en redes sociales. Entre sus características más distintivas, al margen de las más comunes entre este tipo de troyanos bancarios, Crocodilus crea un nuevo contacto en el dispositivo de las víctimas. La especulación de los investigadores es que esto permitiría a los operadores realizar llamadas telefónicas al teléfono comprometido haciéndose pasar por el servicio de soporte o atención al cliente de su banco.

Otra familia de malware destacable es **Zanubis**, cuya evolución ha sido constante desde su aparición en 2022 hasta sus últimas campañas observadas a principios de 2025. Este troyano bancario se caracteriza por su victimología, ya que se centra principalmente en usuarios peruanos, haciéndose pasar por aplicaciones de instituciones del país, y robando credenciales de acceso a entidades financieras peruanas. En algunas de sus campañas más recientes, amplió sus objetivos a las tarjetas virtuales y las billeteras de criptomonedas.

En marzo de 2025 se descubrió un nuevo troyano bancario para Android al que los investigadores han denominado **TsarBot**. Este malware se dirige contra más de 750 aplicaciones en todo el mundo, principalmente del sector bancario, criptomonedas y comercio online, haciéndose pasar por una actualización. Además de robar credenciales, PINs e información de tarjetas de crédito, TsarBot puede grabar la pantalla del teléfono infectado, almacenar pulsaciones de teclado, interceptar SMS (incluyendo aquellos que contienen códigos de segundo factor de autenticación) además de controlar de forma remota el dispositivo.

Descrito por primera vez en abril de 2025, destaca también **PlayPraetor**, un troyano para Android distribuido a través de páginas fraudulentas en anuncios de plataformas de META (Facebook, Instagram, etc.) y de mensajes SMS. Según las primeras cifras de la investigación original, se habrían observado más de 16.000 instancias de estas páginas. Si bien su victimología parecía centrarse en países asiáticos en un principio, campañas más recientes ampliaron sus objetivos a usuarios de todo el mundo, con una mayor frecuencia en Estados Unidos y Brasil, dependiendo de la versión específica del malware.

Spyware

Este tipo de malware está diseñado para **recopilar y exfiltrar información sensible** del usuario sin su consentimiento. Una vez instalado, recoge información como mensajes SMS o de aplicaciones de mensajería, historial de llamadas, contraseñas, actividad en aplicaciones, etc. Su propósito principal es el robo de datos personales o corporativos con fines comerciales, de vigilancia o la extorsión.

Durante la primera mitad de 2025 destacó **SpyMax**, un spyware que opera como troyano de acceso remoto (RAT), distribuido a través de campañas de phishing en las que se hace pasar por aplicaciones legítimas de diversas temáticas, desde invitaciones de boda, hasta entidades gubernamentales. Su actividad más reciente se ha visto centrada en víctimas del continente asiático, en especial contra usuarios en China y la India. Esta familia de malware también ha sido vinculada con el compromiso de soldados y oficiales del ejército sirio a través de canales de Telegram.

En el mes de abril se identificó por primera vez un nuevo malware denominado **Gorilla**, especializado en la interceptación de mensajes SMS con claves de un solo uso (OTP), a las que categoriza por tipo, dependiendo del servicio para el que sean las credenciales (para acceder a la aplicación del banco, iniciar sesión en navegadores, etc.) Su análisis inicial parece indicar que se trata de un programa aún en desarrollo en sus etapas iniciales.

Un mes después se descubrió un nuevo spyware para Android llamado **GhostSpy**. Este malware explota los servicios de Accesibilidad de Android para cargarse en el dispositivo y otorgarse permisos de forma automática, sin intervención del usuario. Una vez ejecutado, tiene capacidad para registrar pulsaciones de teclas, capturar la pantalla incluso de aplicaciones protegidas, grabar audio, video y llamadas, interceptar SMS, rastrear la ubicación GPS e incluso ejecutar comandos de forma remota, como el borrado del dispositivo.

A pesar de haber sido descubierto en 2022, otra familia de spyware conocida como **KoSpy** también ha continuado sus operaciones durante 2025. Este malware, atribuido al grupo vinculado a Corea del Norte APT37 se hace pasar por aplicaciones de utilidades, tanto en plataformas legítimas como en markets de terceros, como ApkPure. Si bien su objetivo principal parecen ser usuarios de Corea del Sur, también tiene soporte para usuarios de habla inglesa.

Entre las técnicas empleadas el malware para Android durante el primer semestre de 2025, destacan **GhostTap** y **NFC Relay**. GhostTap permite a estas aplicaciones maliciosas ejecutar acciones sin que el usuario tenga visibilidad mientras la pantalla parece estar bloqueada o apagada. Los operadores de campañas que emplean esta técnica pueden simular toques en la pantalla y escribir información en segundo plano para realizar fraudes y modificar la configuración del dispositivo sin que el usuario lo note. Los ataques de tipo NFC Relay por su parte, permiten interceptar y transmitir señales entre una tarjeta y un terminal a distancia. De esta forma, un atacante puede realizar pagos con la tarjeta de la víctima estando cerca de la misma. En abril de 2025 se detecto una plataforma conocida como SuperCardX, especializada en la venta de malware-as-a-service para fraudes financieros mediante el método de NFC Relay.

MALWARE IOS

A diferencia de Android, donde el modelo Open Source permite a los atacantes distribuir malware mediante plataformas de terceros o archivos APK, los entornos iOS son más cerrados y cuentan con un mayor nivel de control. Sin embargo, esto no exime a estos dispositivos de este riesgo. Los dispositivos iOS han sido objetivo de ataques más dirigidos y de mayor sofisticación en casos asociados al espionaje estatal y la inteligencia.

Durante los primeros 6 meses de 2025 han destacado los casos del malware **SparkCat** y su variante **SparkKitty**. El primero fue descubierto a principios de año y se cree que su actividad se remonta a marzo de 2024. Se trata de un troyano especializado en el robo de criptomonedas, presente tanto para dispositivos Android como para dispositivos de Apple. Se caracteriza por utilizar el reconocimiento óptico de caracteres (OCR) para analizar las imágenes de la galería de la víctima en busca de patrones relacionados con frases de recuperación de billeteras criptográficas y otros datos confidenciales. El segundo, SparkKitty, fue descubierto en junio de 2025, e igualmente se cree que habría estado activo desde principios de 2024. Al igual que SparkCat afecta tanto a dispositivos iOS como Android y se propaga mediante aplicaciones falsas relacionadas con criptomonedas, apuestas o redes sociales. También comparte con este el uso de OCR para analizar las imágenes de la galería de las víctimas. Sus campañas parecen están focalizadas en usuarios chinos y del sudeste asiático.

Sector financiero

El sector financiero y bancario se ha tratado de uno de los principales objetivos para los cibercriminales durante el primer semestre de 2025. En este sector se ha podido observar la incidencia de ***malware cada vez más sofisticado****, esquemas de phishing y metodologías de fraude cada vez más novedosas.*

Las plataformas de trading, bancos y redes de pago han sido objetivos principales para hackers que explotan herramientas masivas de malware como servicio (MaaS), deepfakes y botnets a gran escala.

MALWARE

La proliferación de troyanos bancarios avanzados se ha intensificado, con atacantes innovando tanto en las capacidades del malware como en los métodos de entrega:

Godfather

Este **troyano** ha evolucionado significativamente, utilizando ahora técnicas de virtualización para secuestrar más de 500 aplicaciones bancarias, de criptomonedas y comercio en todo el mundo. En lugar de métodos tradicionales de superposición, **crea un entorno virtual tipo sandbox** en el dispositivo de la víctima, dentro del cual se lanzan las aplicaciones legítimas. Mientras el usuario ve e interactúa con la interfaz real de la aplicación, el malware captura credenciales de inicio de sesión, datos de transacciones y tokens de sesión en tiempo real. La capa de virtualización hace que esta técnica sea altamente evasiva, ya que no interfiere directamente con la interfaz de usuario, sino que observa silenciosamente desde dentro del contenedor. La comunicación con su servidor de comando y control está cifrada, usando algoritmos de generación de dominios (DGA) para evitar detección estática.

SuperCard X

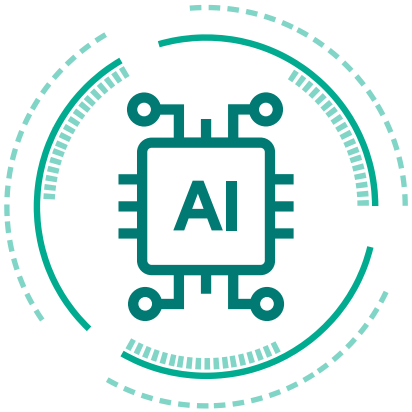
Se trata de una **Plataforma avanzada de Malware como Servicio** (MaaS). SuperCard X facilita el robo de dinero a través de **ataques de retransmisión NFC**. Las víctimas son típicamente atraídas mediante smishing o ingeniería social por voz, engañadas para instalar una aplicación maliciosa con privilegios elevados de NFC y accesibilidad. Una vez activa, el malware captura los datos de la tarjeta NFC cuando la víctima acerca una tarjeta de pago sin contacto al dispositivo comprometido. Los datos robados se transmiten instantáneamente a dispositivos controlados por los atacantes, capaces de suplantar la tarjeta de la víctima en terminales de punto de venta fraudulentos o incluso en cajeros automáticos. La naturaleza modular del malware, combinada con su bajo perfil de detección, representa una amenaza grave para las infraestructuras de pago modernas.

INGENIERÍA SOCIAL

En la primera mitad de 2025, la ingeniería social ha seguido siendo una de las tácticas más efectivas y peligrosas utilizadas por los ciberdelincuentes para comprometer la seguridad de organizaciones y usuarios. La combinación de técnicas tradicionales con tecnologías emergentes, como la inteligencia artificial y los deepfakes, ha elevado el nivel de sofisticación y la dificultad para detectar fraudes y ataques de phishing, poniendo en riesgo la integridad de datos sensibles y recursos financieros.

Campaña de Phishing CyberHeist

Reportada por CTM360, esta campaña internacional distribuyó más de 12.000 URLs de phishing que imitaban sitios web corporativos y de banca. Los atacantes utilizaron anuncios en navegadores combinados con filtrado en tiempo real para promover páginas de phishing personalizadas, diseñadas para capturar credenciales de acceso y códigos de autenticación multifactor (MFA), lo que les permitió obtener control total sobre las cuentas comprometidas.



Phishing asistido por IA

Los mensajes de phishing generados mediante inteligencia artificial han alcanzado tal nivel de realismo que ya no pueden distinguirse de comunicaciones genuinas. Gracias a chatbots que producen mensajes impecables, sin errores tipográficos y con el tono adecuado en cualquier idioma, junto con el uso de deepfakes en voz y video, el phishing por voz (vishing) y SMS (smishing) se han vuelto prácticamente indetectables, dificultando la diferenciación entre interacciones auténticas y fraudulentas.

Deep fakes

Grupos como CryptoCore han perfeccionado la combinación de ingeniería social con deepfakes para llevar a cabo estafas masivas. En enero de 2025, CryptoCore difundió videos falsos de Donald Trump y Elon Musk para promocionar falsas oportunidades en criptomonedas, logrando estafar aproximadamente 3.8 millones de dólares en 2.200 transacciones. Estas estafas se aprovechan de eventos mediáticos y figuras públicas para ganar credibilidad y engañar a un mayor número de víctimas.

DDOS

El sector también ha experimentado un aumento destacable en el número de ataques de DDoS.

DDoS a nivel de aplicación

En el segundo trimestre de 2025, los ataques DDoS a nivel de aplicación aumentaron un 74% en comparación con el año anterior. Las instituciones financieras representaron el 43,6% de los objetivos, enfrentando intentos de ataque que se hacían pasar por tráfico válido y, por lo tanto, resultaban muy difíciles de detectar y mitigar.

Botnets

Apareció una botnet gigantesca de 4.6 millones de unidades que pudo desatar una avalancha de más de cien millones de solicitudes contra servicios. El ataque más largo duró más de 65 horas, afectando operaciones financieras vitales así como el procesamiento de transacciones.

Sector energético

La industria energética en el primer semestre de 2025 sigue siendo un sector crítico en términos de actividad cibernética. Los ciberataques aumentaron en comparación con el primer semestre de 2024. Las agresiones cibernéticas al sector están motivadas por diversos factores, siendo los principales la obtención de ***ganancias financieras y asuntos políticos****. Los ciberdelincuentes suelen apuntar a empresas del sector energético debido a su percepción de* ***alta rentabilidad****, lo que las convierte en objetivos valiosos. Grupos patrocinados por estados y otros actores políticamente motivados, como los grupos hacktivistas, tienden a atacar el sector energético por sus vínculos directos con entidades gubernamentales. Además, dado que esta industria depende de infraestructuras críticas, un ataque puede causar una gran disrupción.*

El primer semestre de 2025 se ha caracterizado por ataques de ransomware, campañas de malware, amenazas persistentes avanzadas (APT), y vulnerabilidades.

GRUPOS DE RANSOMWARE

El ransomware es una de las **amenazas principales** para la industria energética, resultando principalmente en filtraciones de datos. Se estima que al menos 50 incidentes de ransomware dirigidos a organizaciones del sector energético fueron llevados a cabo y divulgados públicamente. Estados Unidos fue el país más atacado, seguido por Canadá. Los grupos responsables del mayor volumen de ataques contra la industria energética son Akira e INC Ransom.

Akira

Es uno de los **grupos de ransomware con mayor número de víctimas** en sectores industriales e infraestructuras críticas. Escrito en C++, apareció alrededor de marzo de 2023. Encripta archivos locales usando ChaCha20, añade la extensión ".akira" a los archivos cifrados y crea una nota de rescate en cada carpeta afectada. En muchos incidentes, la actividad inicial involucró a actores maliciosos que usaron credenciales válidas o accedieron a VPNs de las víctimas.

INC Ransom

También conocido como **Lynx**, es un **ransomware para Windows** escrito en C que cifra archivos en unidades locales, removibles y de red, agregando la extensión .INC. Usa un intercambio de claves Elliptic-curve Diffie–Hellman (ECDH) y SHA512 para generar una clave simétrica AES/128/CFB. Puede vaciar la papelera de reciclaje, eliminar copias sombra, detener procesos, cambiar el fondo de escritorio por una nota de rescate e imprimir esa nota mediante impresoras conectadas.

HACKTIVISMO

En el primer semestre de 2025, los grupos hacktivistas aumentaron su actividad contra compañías del sector energético. Tras la escalada de los conflictos Rusia-Ucrania e Israel-Hamas, múltiples grupos hacktivistas realizaron operaciones cibernéticas contra infraestructuras críticas del sector energético. Estas actividades incluyeron ataques de denegación de servicio distribuido (DDoS), *defacement* de sitios web y accesos no autorizados que derivaron en la exfiltración y publicación pública de datos sensibles de empresas eléctricas.

Algunos de los actores más destacados en el primer semestre de 2025 fueron **Noname057(16)** y **Z-Pentest**. Otros grupos que atacaron específicamente al sector energético fueron: **Dark Strom Team**, **TwoNet, Diplomata**, **SECT0R16**, **Ruski-Net**, **Arabian Ghosts**, **Golden Falcon**, **DieNet** y **Keymous+**.

MALWARE

Durante la primera mitad de 2025, se registró el despliegue de varios malwares dirigidos a empresas del sector energético.

PowerModul RAT

El grupo **Paper Werewolf** (GOFFEE) ha incrementado sus ataques a la infraestructura energética rusa, pasando del espionaje a la interrupción activa de sistemas. Sus ataques comienzan con correos phishing y despliegan PowerModul, un troyano de acceso remoto (RAT) basado en PowerShell, altamente persistente, que funciona incluso sin conexión a internet y se comunica mediante IDs únicos y scripts codificados. Su capacidad para operar en ambientes conectados y aislados lo convierte en una amenaza significativa para infraestructuras críticas.

Amethyst Stealer

En abril de 2025, el actor de amenazas **Sapphire Werewolf** lanzó una campaña sofisticada contra compañías energéticas con una versión mejorada del malware Amethyst Stealer. Distribuido vía correos phishing disfrazados de comunicaciones legítimas de RRHH, el malware corre completamente en memoria, evade detección mediante ofuscación .NET y roba credenciales de navegadores, apps de mensajería y VPNs. Los datos se exfiltran vía Telegram para mayor sigilo, resaltando el riesgo de infiltraciones prolongadas y robo de credenciales en infraestructuras críticas.

DarkWatchman RAT

Compañías energéticas rusas fueron objetivo de una campaña masiva de phishing que distribuyó DarkWatchman, un troyano de acceso remoto sin archivos, capaz de registrar teclas, recolectar datos y desplegar herramientas maliciosas adicionales. La campaña fue atribuida al grupo con motivación financiera **Hive0117**. Su diseño sigiloso y capacidades en evolución lo hacen una amenaza potente para infraestructura industrial y crítica, incluyendo operadores energéticos.

AMENAZAS PERSISTENTES AVANZADAS (APT)

En el primer semestre de 2025 se observaron campañas APT dirigidas al sector energético. Grupos vinculados a estados han pasado del espionaje a buscar activamente la interrupción de sistemas y la infiltración a largo plazo.

Campaña RevivalStone

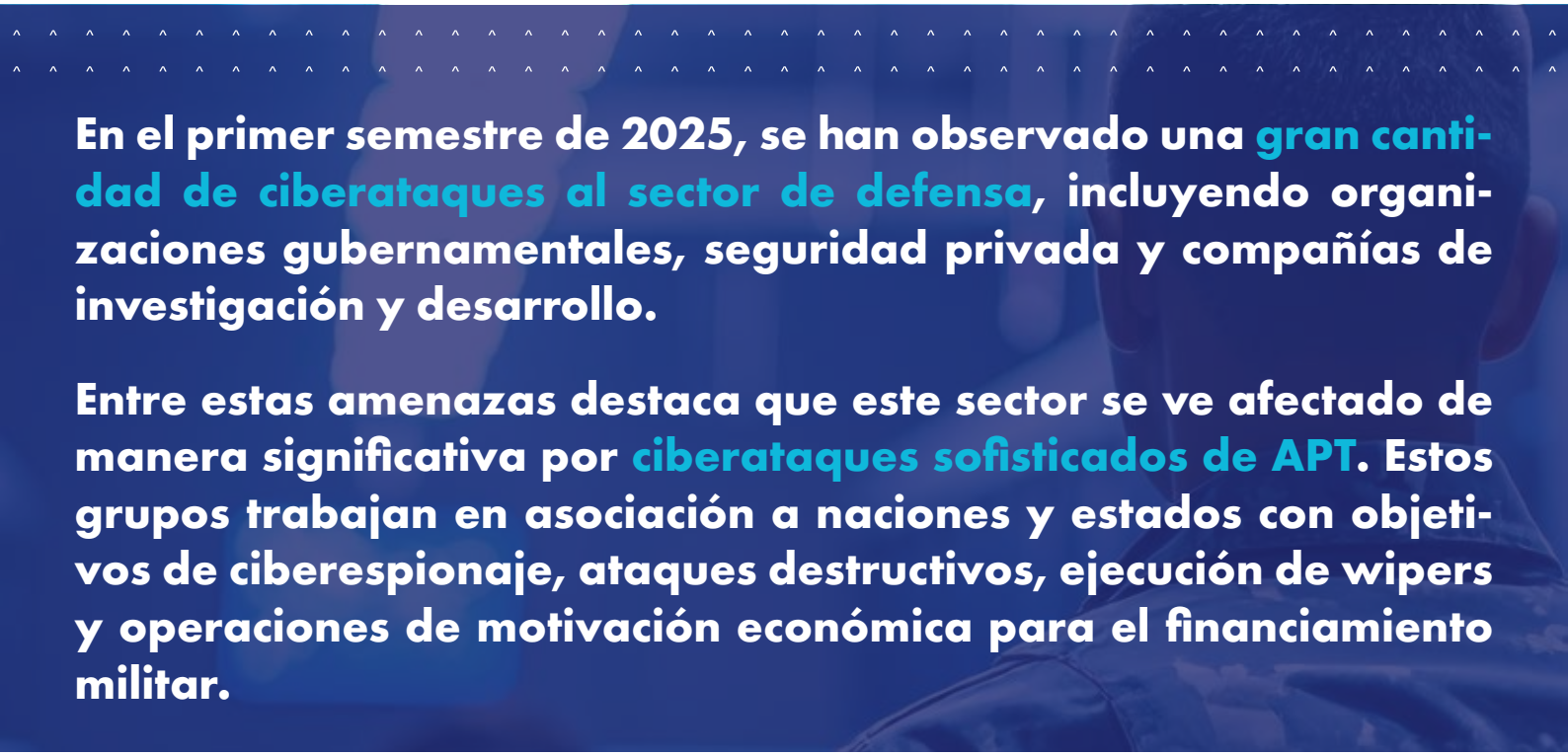
El actor vinculado a China, **Winnti**, un subconjunto de APT41, está relacionado con RevivalStone, una campaña dirigida a compañías energéticas japonesas. Winnti explota vulnerabilidades en aplicaciones para desplegar malware malicioso, incluyendo DEATHLOTUS, UNAPIMON, PRIVATELOG, CUNNINGPIGEON, WINDJAMMER y SHADOWGAZE.

Campaña OneClick

Investigadores descubrieron una campaña de ciberespionaje dirigida al sector energético y de petróleo y gas, denominada OneClick. El malware se entrega mediante phishing y explota la tecnología ClickOnce de Microsoft. El ataque usa un cargador .NET (OneClikNet) para desplegar un backdoor en Golang (RunnerBeacon), que se comunica a través de servicios legítimos de AWS. También secuestra procesos confiables vía AppDomainManager. Aunque la atribución es tentativa, la campaña muestra características de actores vinculados a China.

Sector defensa

*La industria de defensa es un sector clave que **maneja y protege información sensible**, como datos clasificados de operaciones militares y tecnología, así como **infraestructuras críticas**, ya sean cadenas de suministros, sistemas de comunicación, redes satelitales y sistemas de transporte entre otros. Una brecha de seguridad puede causar una pérdida o manipulación de datos, interrupción de operaciones y la revelación de información confidencial, lo que puede llegar a tener un gran impacto en la seguridad nacional, ventaja tecnológica y economía de los países afectados. Esto hace que estas empresas sean blancos atractivos para hackers y grupos de crimen organizado, que, con motivaciones financieras o políticas, llevan a cabo robo de propiedad intelectual, infiltración de redes de suministro, compromiso de equipamiento físico y ataques de malware.*



En el primer semestre de 2025, se han observado una gran cantidad de ciberataques al sector de defensa, incluyendo organizaciones gubernamentales, seguridad privada y compañías de investigación y desarrollo.

Entre estas amenazas destaca que este sector se ve afectado de manera significativa por ciberataques sofisticados de APT. Estos grupos trabajan en asociación a naciones y estados con objetivos de ciberespionaje, ataques destructivos, ejecución de wipers y operaciones de motivación económica para el financiamiento militar.

APT 36

APT36, también conocida como Transparent Tribe o Earth Karkaddan, es un grupo patrocinado por Pakistán operativo desde 2013. Se dirige principalmente hacia organizaciones gubernamentales, militares, de defensa, centros de investigación, diplomáticos e infraestructuras críticas de India.

El 7 de mayo de 2025, el grupo llevó a cabo una serie de campañas de phishing y robo de credenciales con el fin de mantener infiltraciones a largo plazo en las redes de defensa indias. Consistió en la diseminación de correos electrónicos con PDFs maliciosos diseñados para simular documentos gubernamentales del cuerpo policial de Jammu y Kashmir así como de la Fuerza Aérea de la India. Una vez abiertos, presentaban un botón con el inicio de sesión del National Informatics Centre (NIC) y tras pulsarlo, redirigía a las víctimas a una URL fraudulenta al mismo tiempo que se descargaba un archivo ZIP con el ejecutable malicioso Crimson RAT, disfrazado de una aplicación legítima.

T-APT-04

También llamado Sidewinder, es un es un grupo de cibercriminales vinculado a la India y activo desde 2012.

Durante este primer semestre, ha realizado múltiples campañas contra instituciones gubernamentales y militares de Sri Lanka, Bangladesh y Pakistán. Estos ataques se llevaron a cabo a través de correos de spear phishing que explotaban las vulnerabilidades CVE-2017-0199 y CVE-2017-11882 de documentos de Word y RTF para la ejecución remota de código.

Numerosas instituciones se han visto afectadas, entre las que destaca la División 55, una élite de infantería de la armada de Sri Lanka. Asimismo, otras organizaciones fueron atacadas y posteriormente empleadas en la ingeniería social de correos posteriores.

UNC4057

El grupo de amenazas ruso UNC4057 o COLDRIVER es conocido por el phishing de credenciales a trabajadores de los gobiernos de la OTAN, organizaciones no gubernamentales, diplomáticas y de inteligencia.

A partir de enero de 2025 el grupo ha llevado a cabo una serie de campañas contra consejeros de gobiernos occidentales, militares, periodistas, think tanks y ONGs, así como individuos conectados con Ucrania. Tras el robo de credenciales, se exfiltraron los correos y lista de contactos de las cuentas comprometidas, así como en ciertos casos también se llegó a ejecutar un nuevo malware conocido como LOSTKEYS de robo de archivos y datos mediante un CAPTCHA falso.

Earth Kasha (APT10)

Earth Kasha es un subgrupo dentro de la APT10 que conduce compañas de espionaje para China desde 2017.

En marzo de 2025 envió una serie de correos de spear-phishing con el droper ROAMINGMOUSE encargado de distribuir la backdoor ANEL. Se ha dirigido hacia empresas gubernamentales y sectores públicos de Japón y Taiwán.

TAG-110 (APT28)

TAG-110 es un actor de amenazas de alineación rusa relacionado con APT28, conocido por llevar a cabo operaciones de recolección de inteligencia contra Asia central desde 2021.

Entre enero y febrero se detectó una campaña de phishing contra los sectores de gobierno, defensa e infraestructuras públicas de Tayikistán en un momento clave de elecciones y actividad militar en el país. Se emplearon documentos gubernamentales aparentemente legítimos, entre los que se encuentran un informe de las fuerzas armadas para asegurar la seguridad ante radiaciones y la programación de las elecciones de Dushanbe.

Por otro lado, se observaron una serie de campañas no atribuibles a ninguna ATP:

Campaña contra el Ministerio de Defensa Británico

Un grupo de hackers de afiliación rusa se han hecho pasar por periodistas en un ataque dirigido al Ministerio de defensa británico en una operación de ciberespionaje. Sin embargo, esta fue descubierta y detenida tal y como establece el gobierno de Reino Unido en la página oficial del gobierno.

Campaña de denegación de servicio (DDos) contra Estados Unidos

Tras la intervención estadounidense en el conflicto Israel-Irán y el subsecuente bombardeo producido el 21 de junio, múltiples grupos hacktivistas alineados con Irán se dirigieron hacia Estados Unidos en sus ataques. Entre éstos, Mr. Hamza se ha dirigido a varios dominios de la Fuerza Aérea y compañías de los sectores de defensa y aeroespacial, los cuales el día 22 de junio mostraron una baja en sus páginas web durante un periodo de 10 horas.

Campaña de robo de credenciales ucranianas

El ataque fue llevado a cabo por UAC-0219, un grupo de operaciones de ciberespionaje conocido por dirigirse hacia los sectores críticos ucranianos. Esta campaña afectó al sector aeroespacial y defensa, empleando cuentas de correos electrónicos comprometidas para mandar correos de phishing. En éstos se establecía que el gobierno ucraniano iba a reducir salarios, incitando al receptor a pulsar un link para ver la lista de empleados afectados.

Campaña de DDoS, defacement y filtración de datos contra India

En relación al conflicto Pakistán-India, a principios de mayo de 2025 se coordinaron una serie de ataques de grupos hacktivistas pro-Pakistán a los sectores de gobierno, salud, defensa y sociedades civiles de India. En concreto, el grupo Electronic Army Special Forces, se atribuyó la responsabilidad de ataques a instituciones de defensa nacional, justicia y portales de ciberseguridad. Nation of Saviors por su parte, lanzó dos olas de ataques de DDoS, entre las que destacan la Central Bureau of Investigation, National Informatics Centre y la Fuerza Aérea India.

Finalmente se han observado distintos ataques de ransomware:

Durante el primer semestre de 2025, se han producido 40 ataques de ransomware, entre los que Babuk se ha consolidado como grupo más prolífico con 12 ataques de una amplia distribución geográfica. Además, Estados Unidos ha sido el país más afectado con 15 ataques, seguido por India y Bangladés, con 4 y 3 ataques respectivamente.

Entre las víctimas afectadas destacan los organismos de la marina y la armada de Bangladesh, la armada de Indonesia, el Departamento de Defensa de India, el Departamento de Empleados de la Comisión Militar de China, el Ministerio de Defensa de Vietnam, el Ministerio de Defensa de Corea del Sur, la Fuerza Aérea Griega y el Ejército de Perú.

Sector sanitario

Durante el primer semestre de 2025, la actividad cibernética ha revelado que el sector sanitario es un objetivo principal cuando se trata de ciberataques. El primer semestre de 2025 ha mostrado un ***aumento en los ciberataques al sector*** *en relación con el primer semestre de 2024.*

Este sector atrae a los ciberdelincuentes debido a su naturaleza crítica. La mayoría de los ciberataques están impulsados por la gran cantidad de datos personales sensibles que se manejan y por el impacto social que puede tener un ataque a este tipo de organizaciones.

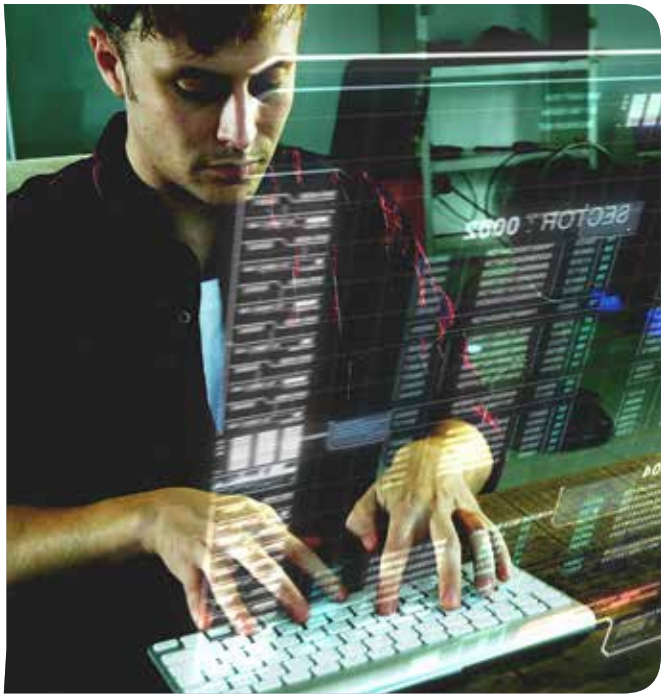
El primer semestre de 2025 ha estado marcado por ataques de ransomware, campañas de ingeniería social, brechas de datos, ataques a la cadena de suministro y vulnerabilidades en dispositivos médicos.

GRUPOS DE RANSOMWARE

El ransomware sigue siendo una de las **amenazas más significativas y disruptivas** para el sector de la salud. Se estima que al menos 243 incidentes de ransomware dirigidos a organizaciones del sector sanitario fueron llevados a cabo y hechos públicos. Estados Unidos sigue siendo el país más atacado, seguido por Australia y Canadá. Los grupos responsables del mayor volumen de ataques contra la industria de la salud son INC Ransom y Qilin.

INC Ransom

El ransomware INC Ransom, también conocido como Lynx, es un ransomware para Windows escrito en C que encripta archivos en unidades locales, extraíbles y de red, añadiendo la extensión .INC a los archivos. Utiliza una combinación de intercambio de claves de curva elíptica Diffie–Hellman (ECDH) y SHA512 para generar una clave simétrica AES/128/CFB para el cifrado del contenido de los archivos, con ECDH implementado usando Curve25519/Montgomery. El ransomware puede vaciar la Papelera de reciclaje, eliminar copias de volumen sombra, detener procesos, establecer el fondo de escritorio para mostrar una nota de rescate e imprimir la nota de rescate usando impresoras conectadas.



CAMPAÑAS DE INGENIERÍA SOCIAL

Las técnicas de ingeniería social son un **método fácil y con alto rendimiento** para que los ciberdelincuentes accedan a los sistemas sanitarios. Estas técnicas pueden usarse para diferentes ataques con diversos objetivos, desde fraude hasta robo de credenciales. En el primer semestre de 2025 se observaron campañas de phishing y vishing.

Campaña de phishing que imita al Servicio Nacional de Salud Italiano

Durante enero, en Italia, hubo una campaña activa de **phishing** que se hacía pasar por el Servicio Nacional de Salud y, en última instancia, por el Ministerio de Salud. El correo electrónico de phishing advertía que la víctima tenía un reembolso pendiente de recibir por un pago al Servicio Nacional de Salud. Los correos contenían un enlace que abría una página en nombre del Ministerio de Salud en la que se solicitaban datos personales para efectuar el pago, incluyendo nombre, apellido, residencia, teléfono y datos de tarjeta de crédito.

Campaña de ingeniería social contra proveedores de salud en EE. UU.

En junio de 2025 se descubrió una campaña de ingeniería social que apuntaba a proveedores sanitarios en Estados Unidos. Los atacantes se hacían pasar por doctores y llamaban a los servicios de asistencia de los hospitales solicitando restablecimientos de contraseña. Cuando se les pedía verificar su identidad, los interlocutores colgaban, un comportamiento consistente con ataques tempranos de **vishing** usados para obtener acceso no autorizado.

Sector industrial

En la primera mitad de 2025, el sector industrial se enfrentó a un panorama de amenazas caracterizado por los ataques ***ransomware****, un incremento de ataques* ***hacktivistas*** *y la explotación de* ***vulnerabilidades*** *en sistemas de control industrial. La cada vez mayor digitalización del sector aumenta la vulnerabilidad de este, la convergencia entre la tecnología operativa (OT) y la tecnología de la información (IT) ha ampliado considerablemente la superficie de ataque. Este apartado analiza las principales amenazas detectadas y sus implicaciones.*

El sector industrial continúa siendo uno de los sectores más afectados por los ciberataques. Por cuarto año consecutivo, encabeza la lista de industrias más atacadas.

Si bien el ransomware representa la amenaza más significativa, el factor humano sigue siendo un eslabón débil crucial. Según investigadores de ciberseguridad, el 22% de las filtraciones de datos en este sector se deben a técnicas de ingeniería social. Hay brechas de alta gravedad que no comienzan con errores técnicos, sino humanos. Ya sea por un correo de phishing, una contraseña débil o un fallo en los procedimientos.

Como se ha comentado, el ransomware sigue siendo la amenaza que más afecta al sector industrial. Desde 2023, ha sido la industria más afectada por este tipo de ataque. Durante ese período, el número de **filtraciones de datos confirmadas aumentó un 89,2%**.

Por otro lado, el sector industrial también se encuentra bajo una **creciente presión a través de sus cadenas de suministro**. La dependencia de múltiples proveedores externos para materias primas, logística y servicios especializados genera una superficie de ataque extensa que los ciberdelincuentes aprovechan con frecuencia.

El 47% de estas filtraciones de datos fueron causadas por ransomware.

Ciberataques iraníes contra los sectores de industria y transporte en Estados Unidos

Los grupos cibercriminales vinculados al Estado iraní han intensificado de forma considerable sus ataques contra infraestructuras críticas en Estados Unidos, con un aumento del 133% en la actividad maliciosa registrada durante los meses de mayo y junio de 2025. Esta escalada coincide con el repunte de las tensiones geopolíticas en torno al reciente conflicto con Irán, y forma parte de una campaña coordinada que, según analistas de ciberseguridad, está dirigida principalmente contra empresas estadounidenses de los sectores del transporte e industrial.

Durante este periodo de dos meses, se han documentado 28 incidentes, lo que supone un salto significativo respecto a los 12 ataques registrados en el trimestre anterior. Este incremento refleja un cambio claro en la estrategia de guerra cibernética iraní, que ahora se centra en comprometer entornos industriales mediante operaciones más sofisticadas y dirigidas. Como respuesta, tanto la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) como el Departamento de Seguridad Nacional de Estados Unidos han emitido advertencias urgentes, subrayando la necesidad inmediata de reforzar las medidas de ciberdefensa en sectores estratégicos.

Analistas de ciberseguridad han identificado a seis grupos iraníes de Amenaza Persistente Avanzada (APT) como responsables de los ataques: MuddyWater, APT33, OilRig, CyberAv3ngers, FoxKitten y Homeland Justice. Estos grupos han demostrado una notable persistencia y un alto nivel de sofisticación técnica, empleando tácticas y herramientas especialmente diseñadas para comprometer entornos de tecnología operativa (OT) y sistemas de control industrial.

Uno de los aspectos más preocupantes de esta campaña es la reutilización deliberada de infraestructuras de comando y control, como ha sido el caso del grupo CyberAv3ngers. Investigadores descubrieron que dicho grupo ha vuelto a emplear una dirección IP previamente utilizada en campañas anteriores, en las que se desplegó el malware OrpaCrab, también conocido como IOCONTROL. Este software malicioso, identificado por primera vez en diciembre de 2024, está diseñado específicamente para actuar sobre entornos industriales, con capacidad para manipular controladores lógicos programables y otros sistemas críticos.

Aumento de los ciberataques hacktivistas a la industria y sectores críticos en 2025

Durante 2025, se ha observado un incremento preocupante en los ataques cibernéticos perpetrados por grupos hacktivistas contra infraestructuras críticas a nivel global, con un foco creciente en sectores industriales clave. Estas acciones, anteriormente limitadas a ataques de denegación de servicio (DDoS) y desfiguraciones de páginas web, han evolucionado hacia operaciones mucho más sofisticadas que buscan comprometer directamente los sistemas de control industrial (ICS) y provocar disrupciones reales en entornos operativos.

Durante 2024 y el primer trimestre de 2025, se identificaron 29 actores de amenaza activos con foco específico en organizaciones industriales. De estos, un 79% fueron clasificados como grupos cibercriminales, y un 45% operaban con tácticas asociadas al ransomware. Esto representa un aumento del 71% en comparación con el año anterior, posicionando al sector industrial como el cuarto más atacado dentro de las infraestructuras críticas. Uno de los grupos más activos en este periodo ha sido responsable de ataques contra 78 organizaciones industriales a nivel global, destacándose no solo por el volumen de ataques, sino también por la magnitud de los robos de información. En dos incidentes, se exfiltraron 2 terabytes y 487 gigabytes de datos respectivamente, lo que pone de manifiesto el cambio de enfoque en las operaciones de ransomware, que ahora priorizan la recolección de información además del cifrado de sistemas.

Según investigadores de ciberseguridad, los ataques orientados a la manipulación de sistemas industriales, filtraciones de datos y accesos no autorizados representaron ya el 31% del total de las actividades hacktivistas en el segundo trimestre, frente al 29% del trimestre anterior. Este aumento evidencia una tendencia clara hacia la profesionalización técnica y el enfoque estratégico por parte de estos colectivos.

Los investigadores han detectado un aumento significativo en el tiempo de permanencia de los atacantes dentro de las redes comprometidas, lo que les permite llevar a cabo tareas de reconocimiento, identificar activos críticos y establecer mecanismos de persistencia antes de ejecutar sus objetivos principales. Esta permanencia prolongada complica la detección y remediación temprana por parte de los equipos de seguridad.

Una tendencia especialmente alarmante es la convergencia entre distintos tipos de actores de amenaza en torno a objetivos del sector industrial. Mientras que grupos patrocinados por Estados han intensificado su actividad en entornos OT e ICS, ciertos colectivos hacktivistas han adoptado técnicas propias del crimen organizado digital, incluyendo el uso de ransomware, con el fin de causar interrupciones mientras persiguen fines ideológicos o geopolíticos.

Sector telecomunicaciones

El sector de las telecomunicaciones está siendo cada vez más reconocido como un ***objetivo de alto riesgo*** *para los ciberataques. La industria desempeña un* ***papel crítico en la comunicación global*** *y el intercambio de datos. Las telecomunicaciones son la columna vertebral de la conectividad digital, con redes que transportan grandes cantidades de datos sensibles, desde información personal, datos corporativos hasta datos gubernamentales. Este papel crítico en la infraestructura digital hace que el sector sea atractivo para los ciberdelincuentes que buscan interceptar datos o interrumpir servicios.*

Además de lo anterior, la industria se basa en una infraestructura compleja que depende de proveedores externos y redes 5G; la complejidad de la infraestructura presenta múltiples vulnerabilidades que pueden ser explotadas.

En cuanto al impacto, un ataque exitoso puede tener consecuencias generalizadas, afectando a los usuarios y desestabilizando la economía. Las consecuencias de alto riesgo hacen que las empresas de telecomunicaciones sean un objetivo de alto valor tanto para ciberdelincuentes con motivaciones financieras como para actores de amenazas con motivaciones políticas.

BRECHAS DE DATOS

El sector de las telecomunicaciones ha estado experimentando un **número creciente de filtraciones de datos** en los últimos años. Estos ciberincidentes amenazan la integridad de la infraestructura crítica de comunicaciones y comprometen los datos de los clientes. Los ciberdelincuentes suelen explotar vulnerabilidades, redes mal configuradas, amenazas internas y proveedores externos débiles para atacar a grandes proveedores de servicios de telecomunicaciones.

Un importante operador de red móvil en Corea del Sur reveló un incidente que posteriormente resultó en una filtración de datos. Se detectó malware en las redes de la empresa, y los atacantes lograron infiltrarse en el Servidor de Suscriptores Doméstico (HSS), lo que permitió el acceso no autorizado a datos USIM, incluyendo claves de autenticación. Los ciberdelincuentes robaron información como IMSI, claves de autenticación USIM, datos de uso de red y SMS/contactos almacenados en la SIM. Dado que esta exposición incrementó el riesgo de ataques de intercambio de SIM (SIM-swapping), la empresa emitió reemplazos de SIM para todos sus clientes. Alrededor de 26.95 millones de usuarios fueron notificados de que sus datos sensibles fueron expuestos. Las investigaciones revelaron que la brecha inicial ocurrió en 2022 y pasó desapercibida durante casi tres años; en total, se comprometieron 23 servidores y se identificaron 25 tipos de malware.

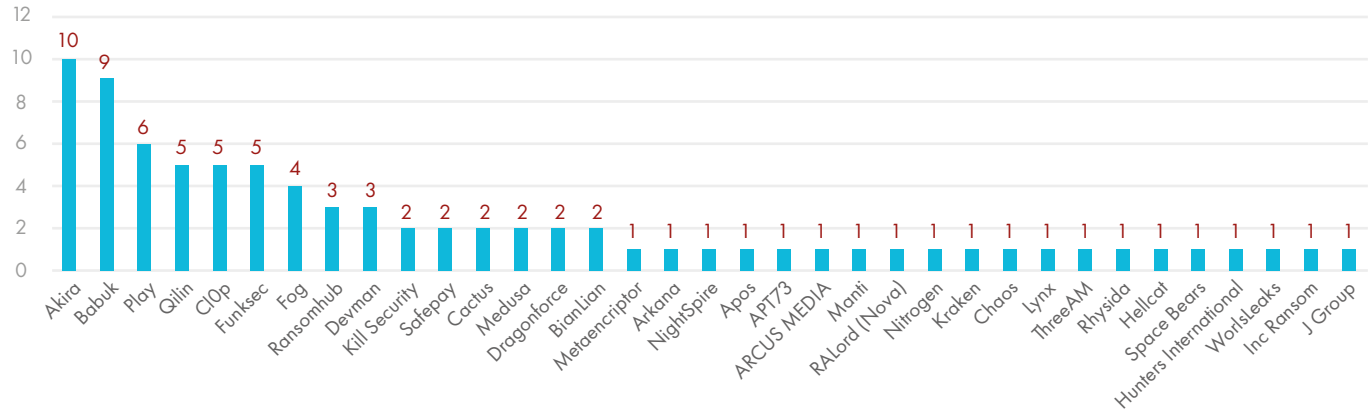
En abril, un importante proveedor de servicios de telecomunicaciones en África informó sobre un incidente que resultó en la filtración de información personal de sus clientes. La empresa ofrece servicios de banda ancha y redes móviles a aproximadamente 288 millones de usuarios en 18 mercados del continente. El incidente no afectó su red central, ni su infraestructura de facturación o servicios financieros, y las cuentas ni monederos de los clientes fueron comprometidos directamente.

En febrero, una gran empresa de telecomunicaciones japonesa reveló que un actor no autorizado accedió ilegalmente a sus sistemas informáticos internos, lo que provocó una filtración de datos que comprometió la información de cerca de 18.000 clientes corporativos. La investigación mostró que el actor de amenaza había accedido al "Sistema de Distribución de Información de Pedidos" y obtuvo datos pertenecientes a 17.891 clientes empresariales. Los datos comprometidos incluían el nombre del contrato registrado, el nombre del representante, número de contacto, número telefónico, dirección de correo electrónico, dirección física e información sobre el uso de los servicios.

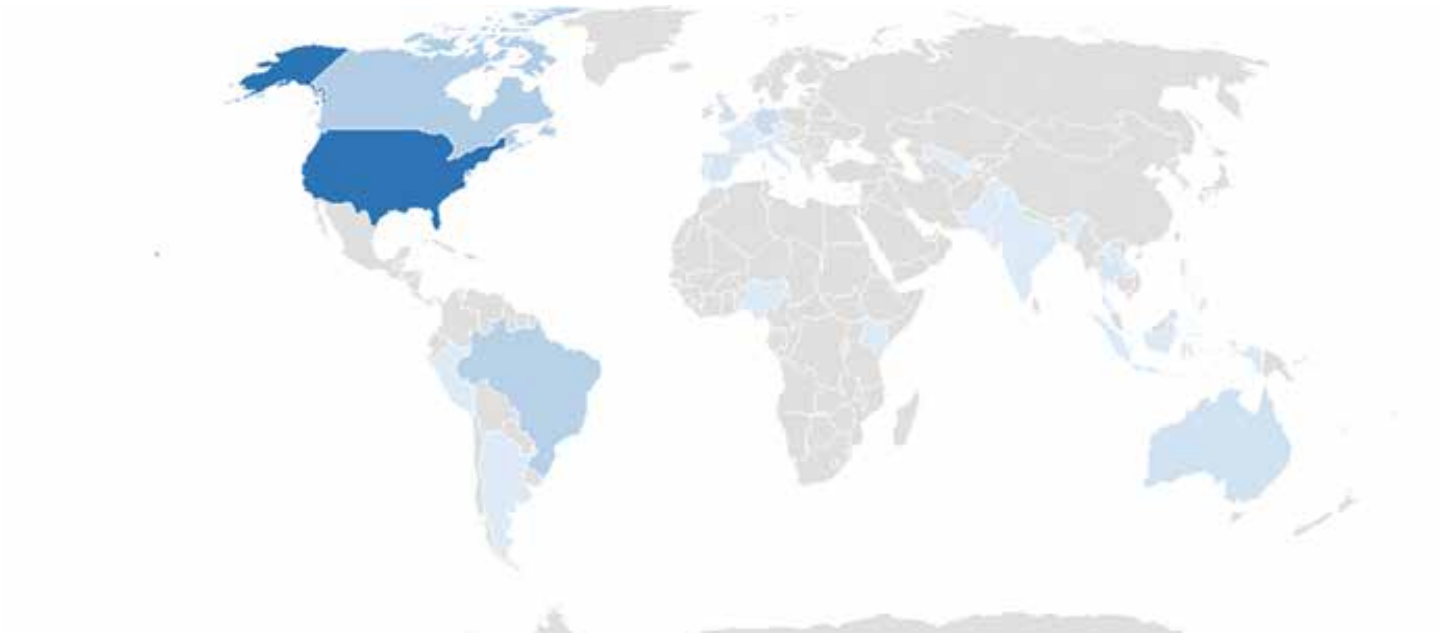
GRUPOS DE RANSOMWARE

En la primera mitad de 2025, se han producido **82 ataques de ransomware**, lo que supone un aumento del 86,36% en comparación con la primera mitad de 2024, lo que indica una escalada significativa de la actividad de amenazas en el sector de las telecomunicaciones. El grupo más activo que atacó al sector en el primer semestre de 2025 fue Akira, seguido de Babuk y Play.

Número de ataques de ransomware por actor



Estados Unidos, **Canadá** y **Brasil** fueron los países más afectados, con más de la mitad de los ataques de ransomware, siendo las empresas de medios de comunicación y los proveedores de servicios de Internet los principales objetivos.



APT

Las redes de telecomunicaciones siguen siendo **objetivos estratégicos** para los actores de ciberamenazas patrocinados por el Estado, que con frecuencia aprovechan a los proveedores de servicios de telecomunicaciones y la infraestructura de redes globales como vectores críticos para la recopilación de inteligencia extranjera.

Los ataques patrocinados por el Estado suelen formar parte de **campañas de inteligencia** amplias y prolongadas para recopilar información sobre objetivos de gran interés, como funcionarios gubernamentales. Estas operaciones suelen implicar la geolocalización y el seguimiento de personas, la vigilancia de las comunicaciones telefónicas y la interceptación de mensajes SMS.

> Salt Typhoon

En la primera mitad de 2025, el grupo de amenazas patrocinado por el Estado chino denominado Salt Typhoon continuó su campaña contra el sector de las telecomunicaciones. Según se informa, el grupo **comprometió a cinco proveedores** de telecomunicaciones en todo el mundo. La campaña se llevó a cabo entre diciembre de 2024 y enero de 2025 y tuvo como objetivo dispositivos periféricos Cisco sin parches. Se observó que el grupo de amenazas intentó comprometer más de 1.000 dispositivos de este tipo en todo el mundo durante la campaña. Además de las empresas de telecomunicaciones, la campaña también se dirigió a varias universidades, posiblemente para obtener acceso a investigaciones en el ámbito de las telecomunicaciones. Para el acceso inicial, Salt Typhoon explotó CVE-2023-20198, una vulnerabilidad de escalada de privilegios en la interfaz de usuario web del software Cisco IOS XE, y CVE-2023-20273, un fallo relacionado con la escalada de privilegios, para obtener acceso root.

> Earth Kurma

Earth Kurma es un APT recientemente descubierto que lleva activo al menos desde 2020. Esta APT, que aún no se ha atribuido a ningún Estado, fue descubierta llevando a cabo una **sofisticada campaña dirigida a varios países del sudeste asiático**, entre ellos Filipinas, Vietnam y Malasia. Las sofisticadas campañas tenían como objetivo entidades gubernamentales y de telecomunicaciones. Durante los ataques, el grupo de amenazas empleó malware avanzado, rootkits y servicios de almacenamiento en la nube como Dropbox y OneDrive para robar información confidencial y mantener un acceso prolongado a las redes.

Según los investigadores, entre sus herramientas se encuentran los rootkits MORIYA y KRNRAT, diseñados para **ocultar sus actividades** a nivel del núcleo del sistema. Aunque algunas técnicas se solapan con las de otros grupos conocidos, como ToddyCat y Operation TunnelSnake, Earth Kurma tiene características distintivas que justifican su clasificación como una nueva amenaza.

Sector aeronáutico

La ciberseguridad juega un papel fundamental en la industria aeroespacial. Este sector se ha convertido en un ***objetivo muy atractivo*** *para ciberdelincuentes debido a varios factores. Por un lado, la aviación es considerada* ***infraestructura crítica****, es decir que cualquier interrupción de los servicios vinculados con este sector puede tener consecuencias significativas en el transporte de mercancías, la seguridad nacional y la economía mundial. Además, las aerolíneas y fabricantes, en ocasiones, gestionan datos sensibles y de alto valor, desde información personal de viajeros hasta propiedad intelectual de tecnologías aeronáuticas, lo que resulta especialmente atractivo tanto para delincuentes financieros como para grupos de ciberespionaje patrocinados por estados.*

Por otro lado, la elevada complejidad e interconexión de los sistemas hacen que el sector aeroespacial sea particularmente vulnerable a ciberataques. Las operaciones aeronáuticas dependen de una extensa cadena de proveedores y equipos interconectados entre sí, de tal forma que una incidencia en un eslabón puede tener efectos en cascada sobre todo el sistema.

Durante la primera mitad de 2025 se produjo un aumento significativo de las ciberamenazas dirigidas a las industrias aeronáutica y aeroespacial.

Las principales amenazas que afectan al sector en este periodo incluyen grupos de ransomware que intentan interrumpir las operaciones para obtener beneficios económicos y APT, en particular grupos patrocinados por el Estado dedicados al ciberespionaje o a la destrucción de sistemas.

GRUPOS DE RANSOMWARE

Varios incidentes sonados este año evidencian cómo los grupos de ransomware están ampliando su foco hacia aerolíneas y fabricantes aeronáuticos.

Ransomware BASHE

A comienzos de 2025, una reconocida aerolínea con sede en Malasia fue víctima de un ataque perpetrado por el grupo de ransomware Bashe, un grupo identificado por primera vez en 2024 y motivada principalmente por fines económicos. Aunque se desconoce la magnitud exacta de los datos exfiltrados, los atacantes afirmaron en su sitio de extorsión haber accedido a **información confidencial** tanto de la compañía como de sus clientes.

Sin embargo, cabe destacar que la **credibilidad de este grupo de ransomware ha sido puesta en duda** en múltiples ocasiones, ya que se les ha acusado de publicar filtraciones falsas o de reutilizar datos obtenidos en brechas anteriores. En este caso particular, existen sospechas de que la información divulgada no sea auténtica, dado que coincide en gran medida con una filtración real ocurrida en 2019 a la misma compañía.

INC Ransomware

Uno de los grupos más activos contra el sector aeroespacial durante el año 2025 ha sido INC Ransomware, identificado por primera vez en junio de 2023 y conocido por emplear la **técnica de doble extorsión** y por operar bajo el modelo de **Ransomware-as-a-Service** (RaaS), lo que demuestra una clara motivación financiera.

En enero de 2025, INC Ransomware llevó a cabo un ataque contra un destacado fabricante estadounidense de misiles y sistemas de armamento aéreo. A través de su sitio de extorsión en la Dark Web, el grupo afirmó haber **exfiltrado alrededor de 4 terabytes de información** altamente sensible, incluyendo código fuente, planos de diseño, firmware de todos los UAV producidos y copias de pasaportes de los empleados. La gravedad del mensaje difundido por los atacantes evidencia la magnitud del incidente y subraya la importancia estratégica del sector aeroespacial en el actual panorama de ciberamenazas. Este caso resalta la necesidad de fortalecer las capacidades de ciberseguridad en las organizaciones vinculadas a esta industria.

Por otro lado, el 6 de mayo de 2025, una aerolínea sudafricana emitió un comunicado oficial confirmando que había sido víctima de un ciberataque ocurrido el 3 de mayo del mismo año. El incidente provocó la **interrupción temporal** del acceso a su sitio web, aplicación móvil y varios sistemas internos, aunque todos los servicios fueron restablecidos más tarde ese mismo día. Diez días después, el 16 de mayo, el grupo de ransomware INC se atribuyó la autoría del ataque a través de su sitio de extorsión en la Dark Web. En dicha publicación, difundieron una primera filtración de datos bajo el título "Part 1", lo que sugiere la posibilidad de nuevas divulgaciones si la aerolínea no atendía sus demandas de rescate. No obstante, hasta la fecha, no se tiene constancia de que INC haya publicado información adicional relacionada con este caso.

Scattered Spider

Uno de los ciberataques con mayor impacto fue el que sufrió una importante aerolínea australiana a finales de junio de 2025, cuando un actor malicioso conocido como 'Scattered Spider' logró acceder a una plataforma de atención al cliente de un tercero y **comprometer datos** de hasta 6 millones de pasajeros. El ataque se llevó a cabo mediante avanzadas técnicas de ingeniería social, incluyendo el uso de MFA push fatigue (bombardeo de notificaciones de autenticación) y vishing (llamadas telefónicas fraudulentas) para engañar al personal de IT. Este enfoque coincide con el modus operandi característico de Scattered Spider, lo que llevó a varios analistas a atribuir el incidente a este grupo especializado en ransomware, conocido por emplear precisamente estas tácticas para infiltrarse en sus objetivos.

Por otro lado, una aerolínea canadiense confirmó haber sufrido un ciberataque que afectó a varios de sus sistemas internos y dejó inoperativos su sitio web y aplicación móvil durante un tiempo. Lo mismo sucedió con una empresa de aviación hawaiana, que reveló que había detectado un incidente de ciberseguridad en algunos de sus sistemas informáticos. Las primeras investigaciones apuntaron nuevamente hacia Scattered Spider como posible responsable de estos ataques.

HACKTIVISMO

Durante el primer semestre de 2025 se han observado amenazas contra el sector aeroespacial ligadas al hacktivismo, es decir, ataques motivados por razones ideológicas o geopolíticas más que por lucro financiero.

> NoName057

En el contexto de la guerra en Ucrania, los grupos hacktivistas pro-rusos han continuado lanzando **campañas de denegación de servicio** (DDoS) de sitios web contra infraestructuras de transporte aéreo en países de la OTAN, buscando generar impacto político y mediático. Por ejemplo, en febrero de 2025, este grupo reivindicó una oleada de ciberataques contra sitios web institucionales en Italia, entre ellos las páginas de varios aeropuertos importantes del país.

Sin embargo, es importante señalar que este tipo de grupos hacktivistas no suelen concentrar sus ataques contra un sector específico. Su principal objetivo es ganar visibilidad en el panorama cibernético, impulsados por motivaciones de carácter político. Además, sus acciones rara vez provocan un impacto crítico en las organizaciones afectadas.

APT

El sector aeroespacial y de la aviación ha sido históricamente un objetivo prioritario de grupos APT. En 2025, esta tendencia continúa vigente con **campañas de ciberespionaje** altamente dirigidas contra empresas y organismos de aviación, muchas veces con fines de robo de información sensible (diseños, tecnologías, contratos) o sabotaje encubierto. Varias potencias estatales emplean parte de su infraestructura gubernamental para infiltrarse en este sector estratégico:

CHINA

Los grupos APTs de origen chino han sido históricamente una de las amenazas más activas contra el sector aeroespacial. Actores como Winnti o Salt Typhoon llevan años infiltrando redes de fabricantes aeronáuticos y sus proveedores para sustraer secretos comerciales y propiedad intelectual de aviones civiles y militares.

Winnti (APT41)

El 28 de febrero de 2025, se detectó que el grupo de amenazas chino Winnti (APT41) había estado llevando a cabo una campaña de ciberespionaje dirigida a empresas del sector industrial de todo el mundo. El actor de amenazas explotaba una vulnerabilidad de VPN en las puertas de enlace de seguridad de Check Point (CVE-2024-24919), lo que les permitía obtener acceso inicial a las redes de varias organizaciones de tecnología operativa (OT). Numerosas cadenas de suministro aeroespacial y de aviación, cruciales para la infraestructura espacial comercial, se encontraban entre los objetivos clave de esta campaña.

RUSIA

Desde el inicio del conflicto bélico entre Rusia y Ucrania en 2022, las campañas de ciberespionaje protagonizadas por grupos APT rusos han aumentado de forma considerable. En este escenario, la infraestructura crítica y los sectores estratégicos, como el aeroespacial, se han convertido en objetivos prioritarios, especialmente en países europeos y miembros de la OTAN.

Fancy Bear (APT28)

A comienzos de 2025, se identificó una campaña de ciberespionaje atribuida al grupo Fancy Bear (APT28) dirigida contra un organismo clave responsable del control del tráfico aéreo en Alemania. El ataque incluyó campañas de phishing y tentativas de comprometer los sistemas internos con el objetivo de acceder a información confidencial relacionada con la aviación. Aunque la entidad afectada aseguró que la seguridad operacional no se vio comprometida, el incidente generó serias preocupaciones sobre la protección de infraestructuras críticas nacionales. Este ataque se enmarca en un patrón de actividad observado en grupos APT rusos desde 2022, lo que sugiere que podría formar parte de una estrategia más amplia de ciberespionaje orientada a vigilar o comprometer la gestión del tráfico aéreo europeo en este contexto de elevada tensión geopolítica.

Sector transporte

El sector del transporte es un objetivo prioritario para los ciberdelincuentes debido a su impacto económico y social. ***Maneja información crítica****, incluidos datos logísticos, redes de transporte público, sistemas de control de tráfico terrestre, marítimo y ferroviario, así como operaciones de flotas comerciales y de carga.*

Estas infraestructuras son ***vitales para la conectividad****, el suministro de bienes esenciales y el buen funcionamiento de la economía, por lo que la ciberseguridad es una prioridad para evitar interrupciones o brechas de seguridad. Como pilar fundamental de la movilidad, la conectividad regional y mundial y la estabilidad económica, es esencial proteger las infraestructuras críticas del sector del transporte.*

CAMPAÑAS DE MALWARE

El sector del transporte se ha convertido en un objetivo atractivo para los ciberdelincuentes, que aprovechan su dependencia de los sistemas digitales para lanzar sofisticadas campañas de malware.

Sosano

Durante este semestre, se identificó una campaña avanzada de ciberataques dirigida contra infraestructuras críticas en los Emiratos Árabes Unidos, incluyendo sectores clave como la aviación, las comunicaciones satelitales y el transporte. Esta operación, denominada UNK_CraftyCamel, se basó en técnicas de ingeniería social altamente elaboradas y el uso de malware.

Los atacantes emplearon correos electrónicos fraudulentos enviados desde cuentas previamente comprometidas de empresas con relaciones legítimas con las víctimas. En particular, suplantaron a una empresa india del sector electrónico para dirigir a los objetivos a un dominio fraudulento en el que se descargaba un archivo comprimido que contenía el malware Sosano.

Sosano estaba oculto dentro de archivos aparentemente inofensivos, como hojas de cálculo y documentos PDF, lo que le permitía evadir muchas soluciones de seguridad tradicionales. Estos archivos incluían código malicioso que se interpretaba de manera distinta según el software utilizado, dificultando aún más su detección. Al ser abiertos, activaban la carga maliciosa que se comunicaba con un servidor de comando y control (C2) remoto.

Una vez dentro del sistema, Sosano habilitaba el acceso remoto, permitía la ejecución de comandos, el desplazamiento lateral por la red, la descarga de componentes maliciosos adicionales y la manipulación de archivos, comprometiendo así la integridad, confidencialidad y disponibilidad de los sistemas críticos afectados.

GRUPOS DE RANSOMWARE

Durante el primer semestre de 2025, una de las principales amenazas cibernéticas que afectó al sector del transporte son los grupos de ransomware. Estos atacantes buscan paralizar las operaciones de las empresas del sector con el fin de obtener un beneficio económico. Con respecto a los grupos de ransomware más activos que han atacado al sector transporte se incluyen: Qilin, Akira y Play.

Qilin

Qilin es un grupo de ransomware activo desde 2022, también conocido como Agenda, que opera bajo un modelo de Ransomware-as-a-Service. Se caracteriza por emplear tácticas de doble extorsión, cifrando y exfiltrando datos confidenciales con amenazas de divulgación si no se paga el rescate.

Se distribuye a través de phishing, explotación de vulnerabilidades conocidas (como la CVE-2023-27532) y accesos remotos comprometidos (por ejemplo, VPN). Además, los atacantes utilizan técnicas como inyección de procesos, modificación de claves de registro y tareas programadas para evadir defensas y mantener persistencia en los sistemas.

Qilin emplea herramientas como Cobalt Strike y PsExec para el movimiento lateral y el despliegue del ransomware, que está desarrollado en Go y Rust, y es compatible con sistemas Windows y Linux (incluidos sistemas virtualizados). El ataque a Parrish Leasing fue anunciado en Telegram, una plataforma habitual para sus comunicaciones. Este incidente refuerza el patrón del grupo de apuntar a infraestructuras críticas en países occidentales, utilizando afiliados que se benefician de un ecosistema de ataque cada vez más profesionalizado.

HACKTIVISMO

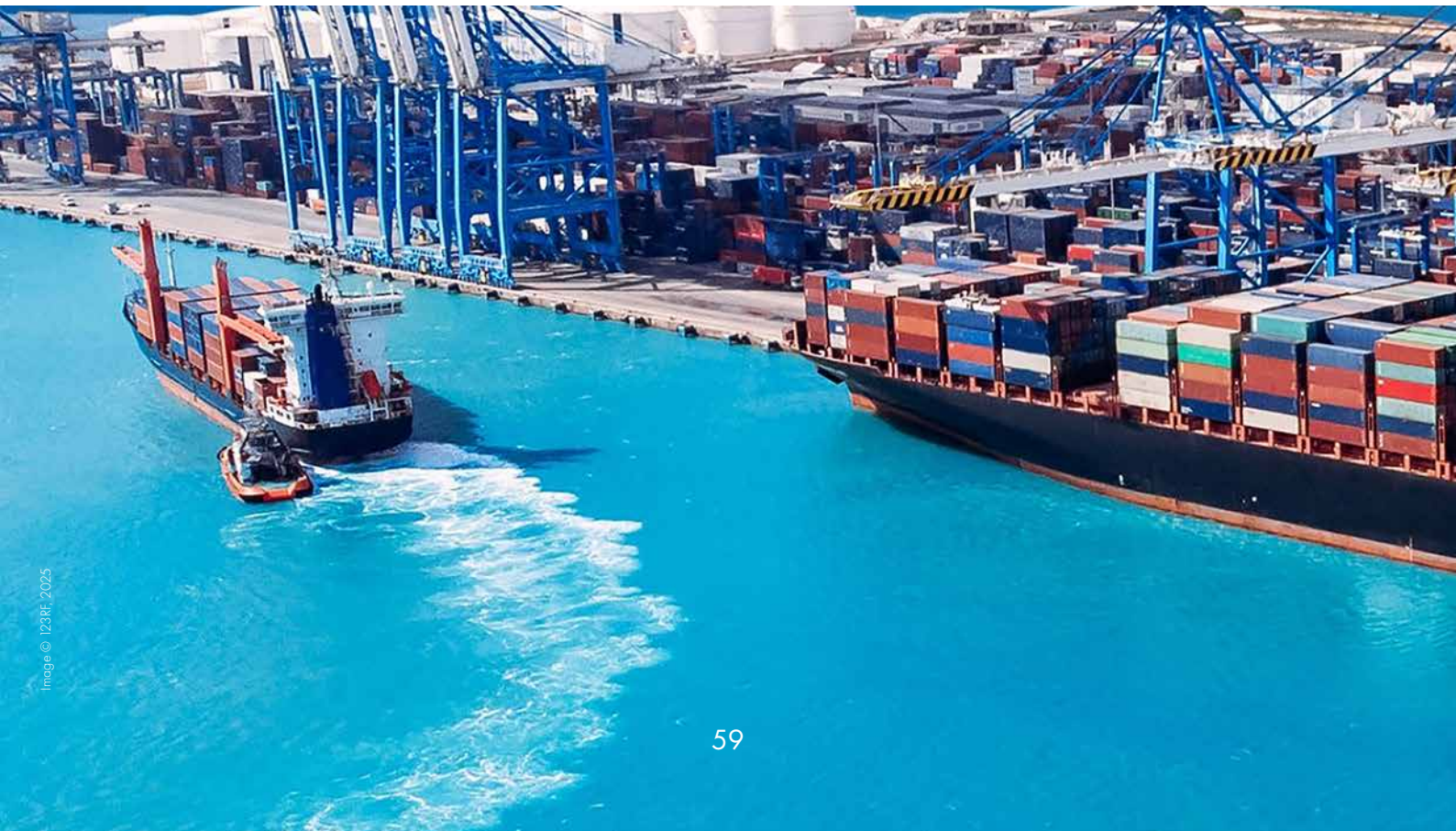
En el primer semestre de 2025, el sector del transporte se consolidó como uno de los principales objetivos de los grupos hacktivistas, que llevaron a cabo ataques cibernéticos dirigidos contra infraestructuras críticas en diversos países. Estas ofensivas, motivadas por agendas políticas y alineaciones ideológicas, pusieron en jaque la operatividad de servicios esenciales, generaron interrupciones significativas y expusieron vulnerabilidades en sistemas tecnológicos clave. Los ataques más frecuentes fueron campañas de denegación de servicio distribuido (DDoS), diseñadas para saturar las plataformas digitales y paralizar la operativa de organizaciones.

@DDOS_54 y la ofensiva contra Marruecos

El grupo @DDOS_54 se ha sumado recientemente al escenario del hacktivismo digital con un ciberataque que dejó fuera de servicio el sitio web oficial del Ministerio de Transporte y Logística del Gobierno de Marruecos. Este ataque, de tipo denegación de servicio distribuido (DDoS), colapsó el portal mediante un aluvión de solicitudes automatizadas, impidiendo el acceso a servicios esenciales como trámites administrativos o consulta de normativas. La acción, reivindicada públicamente a través de Telegram, evidencia cómo actores digitales pueden afectar la operatividad gubernamental con métodos relativamente simples, pero altamente disruptivos.

ServerKillers y la infraestructura estratégica polaca bajo ataque

Polonia también ha sido blanco de acciones ciberactivistas. El grupo ServerKillers reivindicó múltiples ataques contra plataformas digitales del gobierno polaco, como la Agencia de Desarrollo Empresarial y la Comisión de Supervisión Financiera. El motivo declarado fue el apoyo de Polonia a Ucrania en el conflicto con Rusia. Además, sectores críticos como el transporte ferroviario y el energético también fueron impactados, afectando páginas como la de la operadora nacional PKP. Estas acciones demuestran una intención clara de dañar tanto estructuras gubernamentales como servicios públicos esenciales, utilizando la ciberofensiva como herramienta de presión política.



Noname057(16) y las ofensivas coordinadas en Europa del Este

El grupo prorruso Noname057(16) ha mantenido una actividad constante con ataques dirigidos a infraestructuras críticas en países como Polonia y Lituania. En Polonia, la ofensiva afectó el Metro de Varsovia, operadores de autobuses y tranvías, así como plataformas administrativas digitales. En Lituania, el objetivo fue el sistema de transporte público de Klaipėda, el aeropuerto de Šiauliai y entidades bancarias, con el objetivo de desestabilizar y generar una sensación de vulnerabilidad institucional. Estos ataques se han justificado como respuesta a políticas consideradas antirrusas, y se inscriben dentro de una campaña más amplia de guerra híbrida digital.

España en la mira: "OpSpain" y la ofensiva contra el gasto militar

España tampoco ha sido ajena a esta tendencia. Los grupos Twonet y Diplomat lanzaron una campaña cibernética denominada "OpSpain", que tuvo como objetivo instituciones como la Dirección General de Tráfico (DGT), la red de metro de Madrid y empresas privadas relevantes. Estas acciones fueron presentadas como protesta contra el gasto militar español en el marco del apoyo a la OTAN.

Ataques globales: del Reino Unido a la India y Alemania

La expansión del hacktivismo se refleja también en ataques fuera del contexto ruso-ucraniano. En el Reino Unido, una plataforma de compra de billetes de tren sufrió una caída masiva tras un ataque del grupo DieNet v3, mientras que en la India, el colectivo Ripper-Sec llevó a cabo un ataque DDoS contra la página web de la Fábrica Integral de Coches del Ministerio de Ferrocarriles, afectando sistemas esenciales para la gestión del transporte ferroviario. En Alemania, múltiples operadores de transporte público regional fueron blanco de ciberataques que provocaron interrupciones en los servicios de información en tiempo real y sistemas de pago.

APT

Durante el primer semestre de 2025, los grupos de amenazas persistentes avanzadas (APT) han continuado siendo ***uno de los pilares más activos de la ciberdelincuencia*** *a nivel de global. Por norma general, este tipo de grupos están patrocinados o financiados por un Estado nación y suelen contar con un nivel de sofisticación y recursos muy alto, lo que los hace especialmente eficientes y precisos en sus operaciones. Su principal objetivo es obtener acceso prolongado a una red con el fin de robar información sensible para llevar a cabo fraudes financieros, actividades de ciberespionaje o causar daños estratégicos.*

Dependiendo de cada APT, las tácticas, técnicas y procedimientos (TTP) varían, aunque siempre incluyen recolección de credenciales, reconocimiento de la red y la capacidad para moverse por la organización sin ser detectados. El 90% de las APT utilizan phishing en cualquiera de sus variantes para obtener acceso inicial a equipos o infraestructuras, siendo una de las más importantes habilidades de los grupos APT la capacidad de conocer a sus objetivos.

A continuación, se presenta un análisis detallado, organizado por país de origen, sobre los grupos APT más relevantes que han estado operando a lo largo del año 2025.

CHINA

Se estima que ha habido un **incremento del 150%** en campañas de ciberespionaje llevadas a cabo por actores de amenazas de origen chino con respecto al año pasado. Los grupos más activos en 2025 son los siguientes:

MUSTANG PANDA
(RedDelta, Bronze President)

Mustang Panda es un grupo de ciberespionaje que se enfoca principalmente en objetivos gubernamentales e infraestructura crítica. Este actor de amenazas es conocido por emplear el malware PlugX (Korplug) en sus ataques y por utilizar técnicas de 'SpearPhishing' haciéndose pasar por entidades diplomáticas. Actualmente, Mustang Panda es considerado uno de los grupos más activos en Europa.

En cuanto a la actividad de este actor en 2025, se le ha observado involucrado en ataques a agencias gubernamentales europeas vinculadas con el transporte marítimo, afectando a países como Noruega, Reino Unido, Bulgaria, Grecia, Polonia o Países Bajos. En sus campañas recientes, se ha detectado a Mustang Panda haciendo uso de dispositivos USB para inyectar payloads de PlugX (Korplug) con el objetivo de desplegar Backdoors para generar persistencia en el sistema infectado. Las tácticas empleadas por este actor de amenazas podrían indicar una motivación de ciberespionaje orientada a la recolección de información valiosa para fines geoestratégicos.

VIXEN PANDA
(APT15, Ke3Chang)

Vixen Panda es un grupo APT que lleva activo al menos desde el año 2004, enfocado principalmente a organizaciones gubernamentales y sectores de alto valor. Durante los últimos 20 años, la actividad de este actor ha sido relativamente baja. Sin embargo, recientemente se ha observado un aumento significativo de operaciones llevadas a cabo por Vixen Panda. Las campañas activas en el año 2025 vinculadas con este grupo son las siguientes:

En primer lugar, se identificó la participación de Vixen Panda en la "Operación PurpleHace", una campaña de alto impacto en la que el grupo APT ejecutó una serie de ataques durante ocho meses, desde julio de 2024. Los objetivos de esta operación incluyeron entidades de alto valor, como un gobierno asiático, un medio de comunicación europeo y un destacado proveedor de ciberseguridad. Asimismo, cabe destacar que, durante la mencionada campaña, se ha observado la colaboración de Vixen Panda con un actor de amenazas, actualmente inidentificado, que algunos analistas de ciberseguridad monitorizan como UNC5174.

Por otro lado, durante el primer semestre de 2025, Vixen Panda ha estado involucrado en ataques hacia ministerios de asuntos exteriores en América del Norte y del Sur, así como contra comunidades de origen chino asentadas en el extranjero.

WINNTI GROUP
(Brass Typhoon, Wicked Panda, APT41)

Este grupo ha estado activo desde al menos 2010 y es conocido por su doble actividad de ciberespionaje patrocinado por China y operaciones financieras ilícitas. Utiliza frecuentemente el phishing como vector de entrada inicial, enviando correos electrónicos con enlaces o archivos adjuntos maliciosos. Una vez dentro, emplean malware avanzado para mantener un acceso persistente en las organizaciones objetivo.

A finales de 2024 se descubrió un sitio web gubernamental comprometido que alojaba malware, utilizado para atacar a otras entidades gubernamentales. Este ataque, llevado a cabo por el grupo Winnti, distribuyó un payload llamado TOUGHPROGRESS, que utilizaba la aplicación del Calendario como canal de comando y control (C2) para ocultar su actividad maliciosa.

VOLT TYPHOON
(Vanguard Panda)

Este actor de amenazas chino lleva activo desde al menos 2021 atacando principalmente a infraestructura crítica en Estados Unidos. Es un grupo especialista en operar con sigilo haciendo uso de web shells y tácticas living-off-the-land (aprovechar herramientas legítimas del sistema operativo objetivo para llevar a acabo el ataque de forma sigilosa).

En el año 2025 Vanguard Panda continúa operando de forma sigilosa, con especial énfasis en ciberespionaje estratégico con el objetivo de obtener ventajas en el ámbito geopolítico.

SALT TYPHOON
(GhostEmperor, FamousSparrow)

Este grupo APT de origen chino es considerado uno de los más sofisticados y peligrosos en la actualidad. Activo desde al menos 2019, se especializa en operaciones de ciberespionaje dirigidas principalmente contra entidades occidentales, con un enfoque particular en infraestructuras críticas, especialmente en los sectores de telecomunicaciones y proveedores de servicios de internet (ISPs). Salt Typhoon destaca por el uso de técnicas altamente avanzadas que le permiten evadir sistemas de seguridad de última generación y generar persistencia dentro de las redes comprometidas.

Continuando con su dinámica habitual, Salt Typhoon ha seguido con sus ataques dirigidos al sector de telecomunicaciones durante 2025. A comienzos de este año, una importante empresa estadounidense de comunicaciones por satélite detectó una intrusión en sus sistemas atribuida a este grupo. Esta compañía, con una presencia global significativa, ofrece servicios de banda ancha satelital a gobiernos, así como a clientes de sectores clave como aviación, defensa, energía, marítimo y corporativo. La sofisticación y el alcance de esta operación no solo evidencian la peligrosidad de Salt Typhoon, sino que también subrayan su enfoque estratégico en infraestructuras críticas que sostienen servicios esenciales a nivel mundial.

RUSIA

Con motivo del conflicto bélico que sucede entre Rusia y Ucrania desde el año 2022, los grupos APTs atribuidos a Rusia han intensificado sus ataques contra Ucrania y otros países europeos. Sus actividades combinan ciberespionaje, sabotaje destructivo y, en algunos casos, motivaciones financieras. Los actores de amenazas rusos más activos durante 2025 son los siguientes:

FANCY BEAR
(APT28, Sednit)

Fancy Bear es uno de los grupos APT más activos y peligrosos que hay actualmente. Este actor está atribuido al Departamento Central de Inteligencia (GRU) del gobierno ruso y se estima que lleva operando desde al menos el año 2004. Este actor de amenazas es conocido principalmente por sus actividades de ciberespionaje a gobiernos de la OTAN y por atacar al sector defensa e infraestructuras críticas. Desde principios de 2025 se ha observado una tendencia de este grupo centrada en sofisticar sus tácticas de explotación de vulnerabilidades web y de 'SpearPhishing' dirigidos.

La campaña más destacable desarrollada por Fancy Bear durante el primer semestre de 2025 es la operación "RoundPress", dirigida a servicios de webmail vinculados a organizaciones gubernamentales, especialmente en Ucrania. En este caso, el actor de amenazas explotó vulnerabilidades de Cross-Site-Scripting (XSS) que permitía la inyección de código JavaScript en la página del webmail. Esta campaña destacó notablemente por la explotación de la vulnerabilidad Zero-Day CVE-2024-11182, descubierta por Fancy Bear, que afectó a una importante empresa de servicio de webmail para comprometer las comunicaciones de numerosas organizaciones ucranianas.

Por otro lado, durante el primer semestre de 2025, se ha observado a este grupo llevando a cabo campañas de 'SpearPhishing' dirigidas a empresas del sector defensa en Ucrania y Bulgaria.

PRIMITIVE BEAR
(Gameredon)

La actividad atribuida a este actor de amenazas ruso está focalizada prácticamente de forma exclusiva a Ucrania. Se caracteriza principalmente por llevar a cabo ataques de phishing masivo y emplear malware sencillo pero efectivo, lo cuál indica un menor nivel de sofisticación técnica con respecto a otras APT de origen ruso. A pesar de ello, Primitive Bear sigue siendo uno de los grupos más activos del año 2025.

En primer lugar, este grupo intensificó significativamente sus campañas de 'SpearPhishing' contra instituciones gubernamentales y de seguridad ucranianas, introduciendo mejoras para evadir la detección. Por ejemplo, se han observado ataques en los que desplegó una nueva variante de su malware Pterodo llamada PteroBox, un 'Remote Access Trojan' (RAT) que emplea Dropbox para exfiltrar datos. Por otra parte, cabe destacar que Primitive Bear ha ampliado ligeramente su rango de objetivos a algunos países de la Unión Europea, posiblemente para obtener información relacionada con el apoyo occidental a Ucrania.

SANDWORM
(APT44, Voodoo Bear)

Este grupo APT de origen ruso es considerado uno de los más peligrosos. Está atribuido al Departamento Central de Inteligencia (GRU) del gobierno de Rusia y es conocido principalmente por sus ataques de carácter destructivo a infraestructura crítica, especialmente contra Ucrania. Tras un periodo de relativa inactividad, este actor de amenazas retomó sus operaciones ofensivas desde el año 2024.

A inicios del año 2025, Sandworm llevo a cabo una campaña que consistió en una oleada de ataques destructivos contra compañías energéticas ucranianas haciendo uso de un malware tipo wiper llamado 'Zerolot'. Esta operación supuso una interrupción significativa de la actividad del sector eléctrico de Ucrania, subrayando la amenaza constante a sectores de alto valor e infraestructura crítica en el contexto bélico que está sucediendo actualmente en torno a estos países.

ROMCOM
(Storm-0978, Void Rabisu)

RomCom es un actor de amenazas activo desde el año 2022, cuya naturaleza presenta características tanto de un grupo APT como de actores asociados al cibercrimen convencional. Aunque su atribución oficial no ha sido confirmada, se ha observado una fuerte vinculación con intereses del Estado ruso, especialmente por su enfoque reiterado en objetivos en Ucrania y Europa del Este. Este grupo ha sido asociado con el despliegue del ransomware Cuba, lo que sugiere una motivación financiera además de actividades de ciberespionaje. Si bien no se le considera una APT en el sentido estricto, se sospecha que opera con el consentimiento del gobierno ruso, probablemente en apoyo a objetivos geopolíticos.

Desde finales de 2024, se ha observado a RomCom explotando vulnerabilidades Zero-Day en campañas contra objetivos europeos. Específicamente, aprovechó las vulnerabilidades CVE-2024-9680 y CVE-2024-49039.

IRÁN

Los grupos APT iraníes han mantenido un alto nivel de actividad en 2025, enfocados principalmente en campañas de ciberespionaje en Asia y, ocasionalmente, en operaciones destructivas contra adversarios geopolíticos. Sus ataques suelen dirigirse contra entidades gubernamentales rivales o sectores industriales estratégicos. Los actores de amenazas de origen iraní más destacados durante 2025 son los siguientes:

STATIC KITTEN
(MuddyWater, APT34)

Este grupo APT es uno de los actores iraníes más activos y versátiles. Está vinculado al Ministerio de Inteligencia de Irán (MOIS) y se caracteriza principalmente por emplear la técnica de 'SpearPhishing' para desplegar malware personalizado. Sin embargo, recientemente se ha observado a este grupo implementando en sus ataques software legítimo de administración remota como 'ScreenConnect' o 'SimpleHelp'. De esta manera, consigue evadir sistemas de seguridad y generar persistencia en sus campañas. En un caso destacado, se observó colaboración entre Static Kitten y Lyceum, un subgrupo de otra APT iraní conocida como OilRig, lo cual demuestra su versatilidad y capacidad de adaptación con el fin de aumentar las probabilidades de éxito en sus campañas.

Durante el primer semestre de 2025, Static Kitten ha enfocado sus esfuerzos en atacar a ministerios de asuntos exteriores, empresas de telecomunicaciones y universidades en países como Turquía, Pakistán y Emiratos Árabes, con fines de espionaje. Sus correos de phishing a menudo se hacen pasar por agencias gubernamentales locales para ganar credibilidad.

BLADEDFELINE

BladedFeline es un actor de amenazas vinculado a Irán que, en abril de 2022, comprometió a una empresa de telecomunicaciones en Uzbekistán. En marzo de 2025 se detectó actividad sospechosa que coincidía con las tácticas, técnicas y procedimientos (TTP) característicos de este grupo APT, nuevamente dirigida contra la misma empresa. Este segundo ataque se produjo en un contexto de acercamientos diplomáticos entre Irán y Uzbekistán, lo que sugiere que su posible motivación era la obtención de inteligencia con fines de influencia política.

COREA DEL NORTE

Durante 2025, los grupos APT norcoreanos han mostrado una actividad especialmente intensa en campañas con fines económicos, destinadas a la financiación del régimen. No obstante, también continúan llevando a cabo operaciones de espionaje tradicional, centradas principalmente en Corea del Sur y otros objetivos internacionales. Aunque estos grupos operan bajo distintas estructuras del gobierno norcoreano, la mayoría de sus actividades se agrupan comúnmente bajo dos grandes entidades: Lazarus y Kimsuky. Las actividades más destacadas llevadas a cabo por Corea del Norte son la siguientes:

LAZARUS
(APT38)

Lazarus es uno de los grupos más activos y sofisticados atribuidos al gobierno de Corea del Norte, concretamente vinculado a la Oficina de Reconocimiento del gobierno norcoreano (RGB), la principal agencia de inteligencia del país. Este grupo ha estado operativo al menos desde 2009. Lazarus ha sido implicado en una amplia gama de operaciones cibernéticas que incluyen ciberespionaje, sabotaje, y cibercrimen con fines financieros. Las actuaciones recientes de este grupo se han destacado por dedicarse al robo de criptomonedas con el principal objetivo de financiar al régimen.

Una de las campañas más destacadas que ha involucrado al grupo Lazarus durante los últimos seis meses es la operación 'FakeJob'. En este caso, el actor de amenazas empleó ofertas de empleo falsas en empresas de criptomonedas o Blockchain como señuelo, enviando mensajes en LinkedIn y GitHub para atraer a profesionales del sector tecnológico. Al hacer clic, las víctimas descargaban el malware multiplataforma 'WeaselStore'. Esta operación pone de manifiesto el alto nivel de sofisticación en técnicas de ingeniería social empleadas por Lazarus, así como la considerable infraestructura y recursos operativos de los que dispone el grupo.

KIMSUKY
(Velvet Chollima)

Kimsuky es otro de los principales grupos APT atribuidos a Corea del Norte, particularmente a la Oficina de Reconocimiento del gobierno norcoreano (RGB). Se estima que este grupo ha estado activo desde al menos 2012, con un enfoque principal en operaciones de ciberespionaje. A diferencia de Lazarus, que combina espionaje con cibercrimen financiero, Kimsuky se especializa casi exclusivamente en actividades de inteligencia y ciberespionaje, con el objetivo de recopilar información estratégica que apoye los intereses políticos, diplomáticos y militares del régimen norcoreano.

Históricamente, las campañas de Kimsuky se han dirigido contra gobiernos, organismos de seguridad, medios de comunicación, instituciones académicas y organizaciones políticas, con un enfoque prioritario en Corea del Sur. Sin embargo, en los últimos años el grupo amplió su radio de acción, concentrando gran parte de su actividad en entidades occidentales, especialmente en Europa y Estados Unidos. Tras un breve periodo de menor actividad a finales de 2024, Kimsuky ha retomado recientemente sus operaciones, redirigiendo sus esfuerzos hacia objetivos gubernamentales y diplomáticos en Corea del Sur.

Operaciones de influencia

Las operaciones de influencia son un producto de actores estatales y no estatales, cuyo objetivo es la ***desinformación****, la* ***manipulación*** *de la opinión pública y la* ***interferencia*** *política. Las campañas se han convertido en armas poderosas, siendo una herramienta para la estrategia geopolítica, desafiando las dinámicas de poder. En la primera mitad de 2025 se han documentado numerosas operaciones de influencia a nivel global.*

Interferencia rusa: campaña de desinformación en redes sociales

Las redes sociales han sido otro escenario crucial para las operaciones de influencia rusas en 2025. Plataformas como Google, YouTube y otras compañías tecnológicas han desempeñado un papel clave en detectar y bloquear campañas masivas de desinformación.

En enero, Google anunció la eliminación de 1.263 canales de YouTube, vinculados a una consultora rusa, que difundían sistemáticamente contenido favorable al gobierno y mensajes contra Ucrania y Occidente. En febrero, se identificaron y bloquearon 177 dominios operados por Portal Kombat, en los que se alojaban noticias falsas adaptadas a distintos contextos.

Estas operaciones han sido particularmente versátiles y multilingües, alcanzando todo tipo de público a nivel internacional. En algunos casos, se ha documentado incluso la interferencia directa en procesos políticos nacionales, como una campaña diseñada para influir en el debate electoral alemán.

Interferencia rusa: campaña de desinformación a través de la red de Medios Estatales Rusos

Durante el primer semestre de 2025, Rusia intensificó sus operaciones de influencia global a través de medios estatales y plataformas encubiertas. Una denuncia formal del G7, el grupo de democracia más importante del mundo, en enero de este año señaló directamente al canal estatal RT (Russia Today) y a la Agencia de Diseño Social (SDA) como herramientas clave del gobierno para promover campañas de desinformación a gran escala.

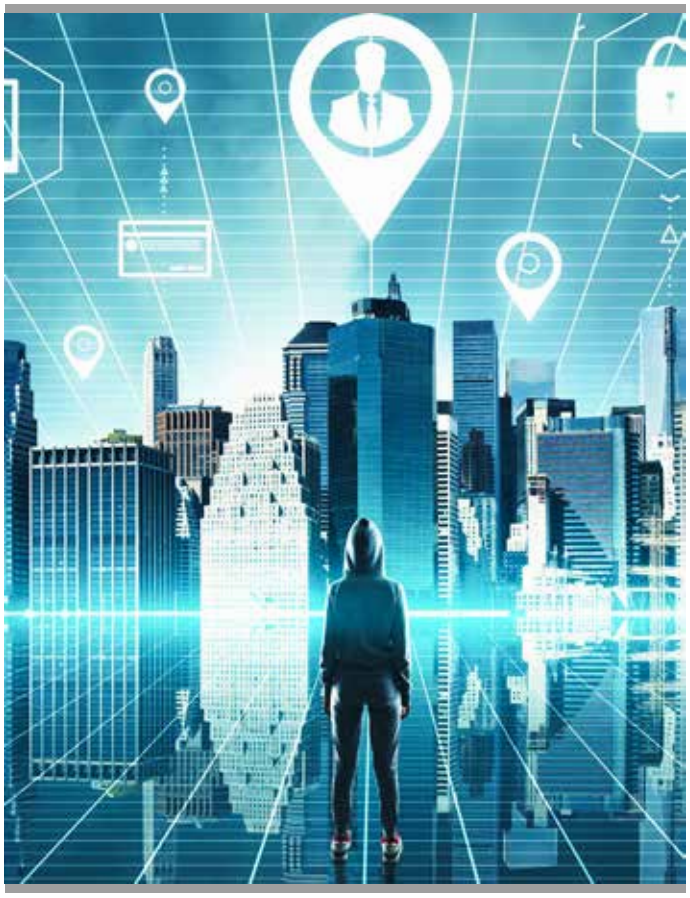
Según el Mecanismo de Respuesta Rápida del G7, estas plataformas son financiadas y dirigidas por Moscú con el objetivo de subvertir sociedades democráticas, explotando divisiones internas mediante la difusión masiva de contenidos manipulados. El contenido suele presentarse como noticias legítimas, pero está diseñado para reforzar intereses estratégicos rusos, debilitar gobiernos democráticos y generar confusión social. La capacidad multilingüe de estos medios les permite actuar simultáneamente en múltiples frentes informativos a nivel global.

Interferencia rusa: Portal Kombat, la red digital encubierta prorrusa

Una de las operaciones más sofisticadas del gobierno de Rusia durante el primer semestre de 2025 ha sido la expansión de una red conocida como "Portal Kombat" (también referida como la Pravda network), dedicada a difundir narrativas alineadas con la propaganda rusa en el espacio informativo mundial.

Esta red está compuesta por numerosos sitios web que simulan ser medios de comunicación locales o independientes, pero que en realidad forman parte de una infraestructura digital coordinada para difundir contenido prorruso. Para inicios de 2025, se estimaba que Portal Kombat ya contaba con más de 224 sitios activos, capaces de publicar hasta 10.000 artículos diarios en más de 50 idiomas.

Más allá de su alcance, lo más destacable de esta operación es su intención de influir en tecnologías emergentes: el principal objetivo de esta red es introducir estos contenidos en sistemas de entrenamiento de inteligencias artificiales con el fin de alterar las respuestas de chatbots o sistemas predictivos de búsqueda, alineándolos con la corriente ideológica prorrusa.



Interferencia china: propaganda digital de desinformación automatizada. Operación Spamouflage

Durante el primer semestre de 2025, China ha desplegado una estrategia de influencia internacional basada en la propaganda digital y la desinformación automatizada. El objetivo principal de estas campañas ha sido mejorar la imagen global de China y restar legitimidad a sus rivales, especialmente a Estados Unidos y sus aliados democráticos. A través de medios encubiertos, redes sociales, inteligencia artificial y técnicas de manipulación informativa, el aparato propagandístico chino ha intensificado sus esfuerzos por moldear la percepción internacional en favor de sus intereses estratégicos.

Una de las tácticas más destacadas ha sido el uso de perfiles falsos automatizados, creados con tecnologías de IA generativa, que simulan ser ciudadanos reales en redes sociales como X (antiguo Twitter), Facebook o YouTube. Esta técnica ha sido ampliamente documentada en una campaña conocida como "Spamouflage", que cuenta con una sólida estructura de desinformación y permite a China difundir de manera masiva mensajes alineados con la narrativa del gobierno. El uso de tecnología avanzada ha permitido aumentar el realismo y el volumen de los contenidos difundidos, haciendo más difícil su detección y aumentando su impacto e influencia en el panorama internacional.

Interferencia china: desmantelamiento de miles de canales de YouTube vinculados a la red Dragonbridge

A comienzos de 2025, las grandes plataformas tecnológicas, especialmente Google, actuaron para desmantelar redes masivas de influencia atribuidas a China. En uno de los operativos más significativos, Google eliminó 11.697 canales de YouTube vinculados al Partido Comunista Chino. Estas cuentas publicaban contenido en chino e inglés con una clara orientación propagandística.

Se estima que una parte de esta actividad estaba relacionada con la red conocida como "Dragonbridge", identificada desde años anteriores como una de las más prolíficas y organizadas. Los mensajes difundidos reproducían puntos de vista oficiales del gobierno chino sobre asuntos internacionales, justificaban sus reclamaciones territoriales, defendían la figura del presidente Xi Jinping y criticaban con dureza las políticas occidentales, especialmente las estadounidenses. El principal objetivo de esta estrategia es higienizar la imagen global del país tratando de restar relevancia a sus competidores occidentales.

Interferencia iraní: propaganda pro-palestina

Durante los primeros meses de 2025, Irán intensificó sus esfuerzos de desinformación, manteniendo su tradicional estrategia de propaganda pro-palestina y crítica hacia Israel y Estados Unidos. Aprovechando el conflicto entre Israel y Hamás iniciado en Gaza a finales de 2023, el aparato mediático iraní reforzó su posicionamiento como defensor de la causa palestina ante la población musulmana.

Diversas investigaciones revelaron redes de desinformación asociadas al régimen iraní, que operaban principalmente en árabe y farsi. Estas redes difundían mensajes que ensalzaban el gobierno iraní y los movimientos palestinos, a la vez que atacaban a Israel y a Occidente. Google desmanteló varias de estas estructuras a inicios de año, cerrando decenas de canales y sitios web que replicaban sistemáticamente esta narrativa. Los mensajes eran difundidos a través de redes sociales, medios digitales e incluso en colaboración con medios tradicionales, mostrando un alcance regional amplio y coordinado.

Interferencia iraní: conflicto con Israel

El estallido del conflicto militar directo entre Israel e Irán el 13 de julio de 2025 marcó un punto de inflexión en el panorama geopolítico internacional. Más allá del enfrentamiento convencional, ambos países intensificaron sus estrategias de comunicación y propaganda, desarrollando en paralelo una guerra informativa y cibernética de alta intensidad.

Irán desplegó tácticas de guerra psicológica dirigidas directamente a la población israelí, con el objetivo de generar miedo, caos y desconfianza en las autoridades. Durante los primeros días del conflicto, ciudadanos israelíes recibieron mensajes de texto falsos que simulaban provenir del Comando del Frente Interior. Estos mensajes advertían de emergencias inexistentes, como una supuesta escasez inminente de combustible o ataques terroristas ficticios, logrando en algunos casos sembrar confusión antes de ser desmentidos por las autoridades.

Operaciones policiales

Durante la primera mitad de 2025, se han sucedido más de una docena de operaciones policiales ***contra el ecosistema del cibercrimen****, tanto en el aspecto digital contra su infraestructura, como en el plano físico, con arrestos y detenciones. Este apartado analizará las 10 operaciones más relevantes de este semestre, además de las detenciones de personalidades conocidas de los foros underground. Fuera de este análisis quedan las operaciones llevadas a cabo contra plataformas de tráfico de armas y drogas, así como de la distribución de contenido sexual.*

Las siguientes figuras resumen los valores clave de estas 10 operaciones, incluyendo su cronología, detenciones, incautaciones y agencias involucradas.

OPERATION TALENT

Operación apoyada por Europol y liderada por autoridades alemanas en cooperación con ocho países y dirigida contra dos de los foros cibercriminales más relevantes. Las plataformas afectadas, conocidas como Nulled y Cracked, tenían en el momento de su retirada más de 10 millones de usuarios en total, y se empleaban como canal de comunicación sobre cibercrimen además de actuar como mercado de bienes ilegales, cibercrimen como servicio, o herramientas de hacking. Las acciones policiales llevaron a 2 detenciones y la incautación de 17 servidores y 50 dispositivos electrónicos.

PHOBOS AETOR

Operación internacional coordinada por Europol contra las actividades del grupo de ransomware 8Base, variante de Phobos Ransomware. La operación llevó a la detención de 4 ciudadanos de nacionalidad rusa y a la intervención de 27 servidores vinculados a la red criminal. Más de 400 organizaciones fueron avisadas del potencial riesgo de verse atacadas por este ransomware gracias a los resultados de esta investigación.

BULLETPROOF HOSTING SERVICES

Operación de la Policia de Amsterdam contra la infraestructura de servicios de hosting empleados por cibercriminales. Las plataformas afectadas fueron Zservers/XHost, de la cual se incautaron 127 servidores.

OPERATION RED CARD

Operación internacional coordinada por Interpol contra una red dedicada a la realización de fraudes bancarios y de inversión a través de medios cibernéticos. La operación se llevó a cabo en 7 países africanos y llevó a los arrestos de más de 300 personas y la intervención de más de 1.800 dispositivos. Según informaron las autoridades nigerianas, alguna de las personas trabajando en los centros fraudulentos podrían ser víctimas de tráfico de personas, forzadas o coaccionadas a llevar a cabo estas actividades criminales.

OPERATION SECURE

Operación internacional coordinada por Interpol en cooperación con agencias de 26 países durante los meses de enero a abril de 2025 contra la infraestructura criminal de varios information stealers. Los resultados de la operación fueron más de 20.000 dominios cerrados afectando a 69 variantes de infostealers, así como la incautación de más de 40 servidores y el arresto de 32 individuos. La información disponible acerca de esta operación no ofrece detalles sobre las familias de malware específicas que fueron investigadas.

OPERATION ENDGAME (II)

Siguiendo con las acciones de la Operación Endgame de mayo de 2024 contra múltiples droppers de malware, Europol informó en abril de 2025 de una serie de acciones coordinadas contra los clientes de la botnet Smokeloader, operada por un actor malicioso conocido como Superstar.

OPERATION ENDGAME (III)

Continuando con la Operación Endgame, Europol informó en mayo de 2025 de la incautación de 300 servidores y la ejecución de órdenes de arresto contra 20 individuos en un esfuerzo internacional contra el ecosistema de ransomware. Entre las familias de malware afectadas por la operación se encuentran Bumblebee, Latrodectus, Qakbot, Hijackloader, DanaBot, Trickbot y Warmcookie.

LUMMAC2

Operación coordinada entre diferentes agencias europeas, de Estados Unidos y Japón, además de la cooperación de Microsoft como parte del Advisory Group on Internet Security de Europol. Esta operación se centró en la infraestructura de uno de los infostealer más activos hadta la fecha, conocido como Lumma Stealer o LummaC2. Las agencias participantes cortaron la comunicación entre Lumma y sus víctimas, e incautaron más de 1.300 dominios relacionados.

AVCHECK

Operación internacional contra servicios empleados por cibercriminales para llevar a cabo sus actividades, incluyendo grupos de ransomware. El objetivo principal de la operación fue la plataforma AvCheck, empleada para probar si un programa malicioso sería detectado por diferentes programas y soluciones de seguridad, sirviendo de apoyo a los desarrolladores de malware para maximizar sus opciones de evadir la detección.

BIDENCASH DOMAINS

Operación contra el marketplace conocido como BidenChas, especializado en la compraventa de tarjetas de crédito e información personal desde 2022. La operación resultó en la incautación de más de 145 dominios, además de fondos en criptomonedas. Las estimaciones del Departamento de Justicia de Estados Unidos indican que la plataforma habría tenido más de 117.000 clientes, permitiendo el tráfico de más de 15 millones de tarjetas de pego, generando un beneficio de 17 millones de dólares.

SOBRE THALES

Thales, su socio de confianza para enfrentar y protegerse del cambiante panorama de las ciberamenazas.

Con el enfoque holístico de Thales, las organizaciones críticas pueden afrontar con confianza las complejidades del panorama de ciberamenazas, asegurándose de estar bien preparadas para detectar, responder y recuperarse de cualquier incidente. Respaldados por un equipo de 6.000 expertos en ciberseguridad, nuestros servicios gestionados incluyen una supervisión 24x7 de nuestros 8 Centros de Operaciones de Seguridad (SOC), tanto para las infraestructuras de IT como de OT, donde analistas expertos detectan, analizan y responden a los incidentes en tiempo real, asegurando una rápida contención y recuperación.

Junto con nuestros servicios globales de respuesta a incidentes, equipamos a las organizaciones con estrategias personalizadas para gestionar y remediar eficazmente los ciberincidentes. Estos servicios se ven reforzados por **nuestros equipos de Threat Intelligence** (CTI) y de protección contra riesgos digitales (DRPS), diseñados para mejorar el conocimiento de la situación, proporcionando información útil sobre las amenazas emergentes y mitigando los riesgos de forma proactiva, al tiempo que se protege la reputación de la marca y los datos sensibles. Además, nuestros servicios de gestión continua de la exposición a amenazas abarcan simulaciones de infracciones y ataques y gestión de vulnerabilidades, lo que permite a las organizaciones identificar de forma proactiva los puntos débiles y reforzar sus capacidades de seguridad.

Para más información, contáctanos en:

cds.thalesgroup.com

THALES
Building a future we can all trust

cds.thalesgroup.com/cyberthreat-hitmap