Tendencias CTI

Ciberinteligencia de Amenazas

Primer semestre 2025

Índice

Índice

Introducción

1.1. Propósito del informe

El presente informe tiene como objetivo proporcionar un análisis detallado de las tendencias, incidentes y acontecimientos relevantes en el ámbito de la Inteligencia de Ciberamenazas durante el primer semestre del 2025. El informe aborda las amenazas emergentes que están redefiniendo el panorama de la ciberseguridad, los actores maliciosos con una actividad destacada, las campañas cibernéticas más significativas y las vulnerabilidades críticas detectadas en este período. Asimismo, se identifican patrones recurrentes y se esbozan posibles escenarios futuros que podrían influir en las estrategias de gestión y mitigación del riesgo.

1.2. Alcance geográfico y temporal del informe

El análisis presentado adopta una perspectiva global, lo que permite comprender cómo las amenazas evolucionan de forma interconectada en distintos contextos geográficos. Esta visión amplia facilita la identificación de dinámicas comunes y particularidades regionales que enriquecen la comprensión del entorno cibernético actual.

Entorno marcado por cambios relevantes en el comportamiento de las amenazas y por eventos que han tenido un impacto significativo en el ecosistema digital. Este intervalo temporal resulta clave para anticipar posibles movimientos futuros y fortalecer las capacidades de respuesta ante un entorno cada vez más complejo.

Panorama Global de Amenazas

2. Panorama global de amenazas

En 2025, el mundo enfrenta un entorno de riesgos cada vez más interconectado y complejo, donde las amenazas físicas y del ciberespacio convergen y se amplifican mutuamente. Los conflictos armados, los fenómenos meteorológicos extremos y los ciberataques a infraestructuras críticas figuran entre los cinco riesgos más urgentes del año (World Economic Forum, 2025), propiciando un panorama cada vez más incierto.

Esta combinación de amenazas refleja una tendencia clara: los riesgos ya no se presentan de forma aislada, sino que se retroalimentan en un contexto de creciente fragmentación geopolítica, polarización social y aceleración tecnológica. En este escenario, la colaboración internacional y la resiliencia organizacional se han convertido en pilares fundamentales para hacer frente a un panorama de amenazas que evoluciona con rapidez y que exige respuestas coordinadas, adaptativas y basadas en la inteligencia de amenazas.

2.1 Geopolítica y Ciberseguridad

Dentro del panorama global actual los riesgos geopolíticos y tecnológicos conforman la mayor preocupación a corto plazo. Por un lado, la digitalización masiva, junto con la expansión de la IA, ha incrementado la superficie de ataque y facilitado la aparición de nuevas formas de ciberdelincuencia, espionaje y desinformación. Por otro lado, el aumento de las tensiones geopolíticas, que impulsa una creciente desglobalización, empuja a los Estados y organizaciones a desenvolverse en un entorno cada vez más hostil, caracterizado por ataques descentralizados y por la dificultad de imponer marcos legales o normativos eficaces para regular estas amenazas, lo que complica aún más las estrategias de ciberseguridad.

Entre enero y junio de 2025, se han observado las siguientes tendencias clave que intensifican la relación entre la ciberseguridad y la situación geopolítica global (Group-IB, 2025; CrowdStrike, 2025):

- **Auge de los actores estatales y el ciberespionaje geopolítico:**

Se ha observado un aumento de la actividad en el ciberespacio atribuida a actores patrocinados por Estados, destacando las operaciones vinculadas a entidades de la República Popular China, que han multiplicado sus operaciones de ciberespionaje en sectores estratégicos como finanzas, manufactura y medios. **Corea del Norte** e **Irán** también han intensificado sus operaciones, combinando espionaje, generación de ingresos ilícitos y campañas de desinformación con fines políticos. Además, las APTs (Amenazas Persistentes Avanzadas) se han vuelto más especializadas y difíciles de rastrear, actuando con mayor OPSEC (Seguridad Operacional) y compartiendo herramientas entre grupos.

- **Uso de IA generativa en campañas de desinformación y espionaje:**

Como adelantábamos en el informe del semestre pasado, la IA generativa se ha consolidado como una herramienta clave para los adversarios. Permite crear campañas de ingeniería social más sofisticadas, perfiles falsos, deepfakes y desinformación electoral a gran escala, obligando a los gobiernos a crear unidades de detección especializadas (Federal Ministry of the Interior, 2025). Esta tecnología ha reducido las barreras de entrada para actores maliciosos, facilitando la automatización de ataques y el desarrollo de scripts maliciosos con mayor rapidez y eficacia, principalmente para explotar vulnerabilidades y automatizar campañas de phishing.

- **Ransomware como herramienta de presión geopolítica:**

Tanto el modelo de Ransomware-as-a-Service (RaaS) como el número de ataques de ransomware registrados en publicaciones de sitios de filtración siguen en alza. Algunos ataques han tenido un impacto geopolítico directo en infraestructuras críticas, sobre todo en redes gubernamentales e industrias manufactureras, lo que evidencia su potencial desestabilizador. Por otra parte, la aparición de nuevos grupos de ransomware en lo que va de año revela una tendencia emergente hacia la profesionalización del cibercrimen, algunos

con iniciativas de autopromoción que imitan estrategias empresariales.

- **Fragmentación digital y obstáculos normativos:**

La desglobalización digital y el aumento de tensiones políticas dificultan la cooperación internacional en materia de ciberseguridad. Las barreras jurisdiccionales y la falta de marcos legales comunes complican la persecución de actores transnacionales, lo que ha sido aprovechado por grupos criminales y estatales para operar desde regiones con baja cooperación legal.

Así pues, la ciberseguridad se ha consolidado como un instrumento estratégico en el contexto geopolítico global, clave para anticipar amenazas tecnológicas que trascienden lo digital y se proyectan sobre el mundo físico.

2.2 Geopolítica y principales actores

La evolución del panorama de ciberseguridad durante el primer semestre de 2025 ha estado profundamente influenciada por los conflictos armados, las tensiones diplomáticas y las rivalidades estratégicas entre potencias. En este contexto, los actores de amenazas vinculados a Estados-nación han intensificado sus operaciones, utilizando herramientas digitales para el espionaje, el sabotaje y la desinformación.

Este apartado analiza los principales focos de conflicto geopolítico y los grupos cibernéticos más activos, destacando cómo sus acciones han impactado la estabilidad regional y global a través de campañas dirigidas y persistentes.

- **Ciberguerra en la sombra: Rusia y Ucrania en el frente digital**

En el conflicto entre Rusia y Ucrania las operaciones digitales han desempeñado un papel central en las **estrategias de desgaste y control de la información,** extendiéndose también a terceros países con interés geopolítico, especialmente en la Unión Europea.

Las campañas atribuidas a actores rusos han evidenciado una doble dimensión: por un lado, el ciberespionaje y la desinformación como instrumentos de presión diplomática y manipulación narrativa; por otro, las operaciones de interrupción y sabotaje digital dirigidas a infraestructuras críticas, especialmente contra Ucrania. Esta táctica híbrida combina persistencia técnica con objetivos políticos, amplificando el alcance del conflicto más allá de sus fronteras físicas. El análisis técnico detallado de estas operaciones, junto con los actores responsables, se desarrolla en el apartado “6.4. APT” dedicado a este tipo de amenaza, donde se examina en profundidad la evolución de campañas específicas, herramientas utilizadas y su impacto regional.

- **Oriente Medio: escalada regional y amenazas transnacionales**

Durante el primer semestre de 2025, Oriente Medio ha experimentado una intensificación de sus tensiones geopolíticas, con consecuencias directas en el ciberespacio. El 13 de junio Israel lanzó una importante ofensiva aérea contra Irán y los ciberataques contra Israel aumentaron un 700% en los dos días posteriores. El número de grupos iraníes o proiraníes parece ser mucho mayor. Si bien
la cultura activista sigue siendo fuerte en los países occidentales, la escena hacktivista está dominada en gran medida por actores del hemisferio oriental, donde Irán goza de un mayor apoyo.

Diferentes fuentes han llegado a identificar 65 grupos proiraníes, 11 antiiraníes y 6 proisraelíes, un total de 82 grupos. Se espera que la cifra aumente a medida que el conflicto continúa.

Los actores de amenazas alineados con Irán se mantuvieron muy activos, liderados por MuddyWater, que frecuentemente utilizaba herramientas RMM en ataques de phishing. Asimismo, BladedFeline volvió a atacar a una víctima anterior, una empresa de telecomunicaciones en Uzbekistán, coincidiendo con el acercamiento diplomático de Irán. Otros como CyberToufan llevaron a cabo operaciones destructivas, desplegando un ataque de borrado de datos contra múltiples organizaciones en Israel.

- **Estados Unidos contra China: batalla digital entre superpotencias**

El conflicto geopolítico entre Estados Unidos y China en 2025 ha trascendido el plano diplomático y económico para consolidarse como una ciberguerra de alta intensidad por el dominio tecnológico, la soberanía informativa y el control del comercio y las infraestructuras críticas, con una creciente fragmentación de las cadenas de suministro globales.
Por un lado, Volt Typhoon, un grupo APT vinculado al gobierno chino, ha sido protagonista de campañas de infiltración en redes estadounidenses y de Taiwán, especialmente en sectores como telecomunicaciones, energía y defensa. Su enfoque se basa en el sigilo y la persistencia, utilizando técnicas Living off the Land (LotL), para evitar ser detectado. Las maniobras militares y los ciberataques en torno a Taiwán también se han intensificado recientemente.

Por otro lado, Equation Group y TAO, ambos asociados a la NSA, representan la respuesta cibernética de EE.UU., con capacidades ofensivas altamente sofisticadas. Estos grupos han sido acusados de realizar operaciones de espionaje y sabotaje digital en infraestructuras extranjeras, incluyendo objetivos chinos.

- **Conflicto en la península coreana: una guerra sin disparos**

Los actores de amenazas alineados con Corea del Norte estuvieron particularmente activos en campañas con fines financieros.
El grupo **DeceptiveDevelopment** amplió significativamente sus objetivos, utilizando ofertas de trabajo falsas, principalmente en los sectores de criptomonedas, *blockchain* y finanzas. Empleando técnicas de ingeniería social, como ataques **ClickFix** y publicaciones falsas utilizadas para distribuir el *malware* multiplataforma **WeaselStore.**

Por otro lado, el robo de criptomonedas de **Bybit,** atribuido por el FBI a **TraderTraitor,** implicó una vulneración de la cadena de suministro de *Safe,* que causó pérdidas de aproximadamente 1.500 millones de dólares.

Mientras tanto, otros grupos alineados con Corea del Norte experimentaron fluctuaciones en su ritmo operativo: a principios de 2025, **Kimsuky y Konni** volvieron a sus niveles habituales de actividad tras un notable descenso a finales de 2024, y centraron sus ataques principalmente en entidades y personal diplomático surcoreanos. El grupo de amenazas **Andariel** resurgió, tras un año de inactividad, con un sofisticado ataque contra una empresa surcoreana de software industrial.

- **Otros frentes abiertos en el Indo-Pacífico**

La situación actual en Myanmar ha propiciado un entorno en el que el **ciberespionaje interno y la represión digital** ejercida por el régimen militar convergen con operaciones criminales transnacionales de **ciberfraude a gran escala.** Estafas como el pig butchering, las apuestas ilegales y los fraudes con criptomonedas han evolucionado mediante el uso de deepfakes, IA generativa y tecnologías blockchain, lo que ha otorgado a los grupos delictivos un mayor nivel de anonimato, eficiencia y sofisticación operativa.

Paralelamente, el 22 de abril se intensificó la tensión entre India y Pakistán tras un atentado terrorista en territorio indio (región de Jammu y Cachemira), que disparó la tensión política entre ambos países, desencadenando una serie de enfrentamientos militares entre ambos bandos hasta el “alto al fuego” tras la mediación de EE.UU. el 10 de mayo. Estos episodios originaron una intensa campaña de desinformación en redes sociales y medios digitales, caracterizada por **videos manipulados, narrativas fabricadas y la amplificación de contenidos polarizantes** mediante redes de cuentas falsas. Además, los servicios gubernamentales indios han sido blanco de múltiples ciberataques atribuidos a actores como **AnonSec, Sylhet Gang (SG) y DieNet,** enmarcados en una guerra de información que involucra tanto a grupos estatales como no estatales en un contexto de ciberconflicto creciente.

que involucra tanto a grupos estatales como no estatales en un contexto de ciberconflicto creciente.

En conjunto, el año 2025 consolida al ciberespionaje como una herramienta central en la competencia geopolítica global. El spear phishing se mantiene como la técnica predilecta entre las APTs de múltiples regiones, mientras que las operaciones disruptivas, particularmente desde Oriente Medio, y las campañas de desinformación adquieren una relevancia creciente, marcando el rumbo del conflicto digital contemporáneo.

2.3 Afectación de ciberataques a sectores específicos

Para concluir con el apartado de amenazas globales, desde el **Departamento de Cyber Threat Intelligence de NTT DATA** consideramos relevante incluir la evolución de ciberataques en los sectores y países más afectados en el primer semestre de 2025, con leves variaciones estructurales respecto la disposición del último semestre de 2024.

La distribución de los ataques refleja de nuevo la fuerte influencia de las tensiones geopolíticas, dirigidos principalmente a sectores estratégicos y países de alta relevancia económica o en conflicto. El impacto de estos ataques no ha sido uniforme, aunque las diferencias entre sectores se han reducido de forma significativa. En En comparación con el segundo semestre de 2024, la variabilidad del grado de afectación sectorial ha disminuido cerca de un 8%.

- **Administración Pública y Gobiernos:**

Este sector prevalece en primera posición con el mayor número de ciberataques registrados en el primer semestre de 2025, con **3.005 ataques dirigidos** a las administraciones públicas y **779 hacia el Gobierno y Sector Público,** conformando un total de 3.784 ciberataques, con un **aumento del 41,30%** en comparación con los ataques registrados a este sector en el informe anterior. De nuevo, las tensiones constantes entre naciones motivan nuevas amenazas contra estas entidades, buscando información sensible que pueda ofrecer ventajas estratégicas o acciones *hacktivistas.*

- **Educación:**

El número de ciberataques registrados contra las instituciones educativas se ha visto **reducido cerca de un 23% desde el año pasado**, con un **total de 1.110**. Pese al descenso de la cifra de ataques en este sector, los centros educativos, en particular las universidades, siguen siendo un blanco de ataque atractivo por su propiedad intelectual, sus datos personales y sus vulnerabilidades operativas.

- **Servicios financieros:**

Por su parte, el sector financiero se ha visto un **26,9% más afectado que en 2024, con 835 ciberataques registrados,** manteniéndose dentro de los tres sectores más atacados. Se observa una tendencia de cómo la situación geopolítica está redistribuyendo los ataques, decantándose los actores de amenazas por objetivos gubernamentales y aumentando sus objetivos financieros.

- **Tecnologías de la Información y Telecomunicaciones:**

Con 739 y 652 ciberataques registrados respectivamente, los recursos tecnológicos son un objetivo interesante que explotar. Los ataques más comunes son el robo de datos y el compromiso de sistemas, con el fin de obtener beneficios económicos, causar la interrupción de los servicios y operaciones e, incluso, causar daños físicos.

El ransomware sigue siendo el ciberataque por excelencia. Aunque su tendencia se ha reducido en el último trimestre (abril a junio de 2025), entre enero y febrero se registraron los mayores picos de actividad. En estos tres meses recientes, los sectores más afectados han sido el de la construcción y el manufacturero, que concentran el 12% del total de ataques. Geográficamente, los países más atacados han sido EE.UU. (664), Canadá (77) y Alemania (69).

Este tipo de ataque se detalla en profundidad en el apartado “6.2. Grupos de *ransomware*”.

Sectores más afectados por ciberataques de enero a junio de 2025 y comparación con S2 2024

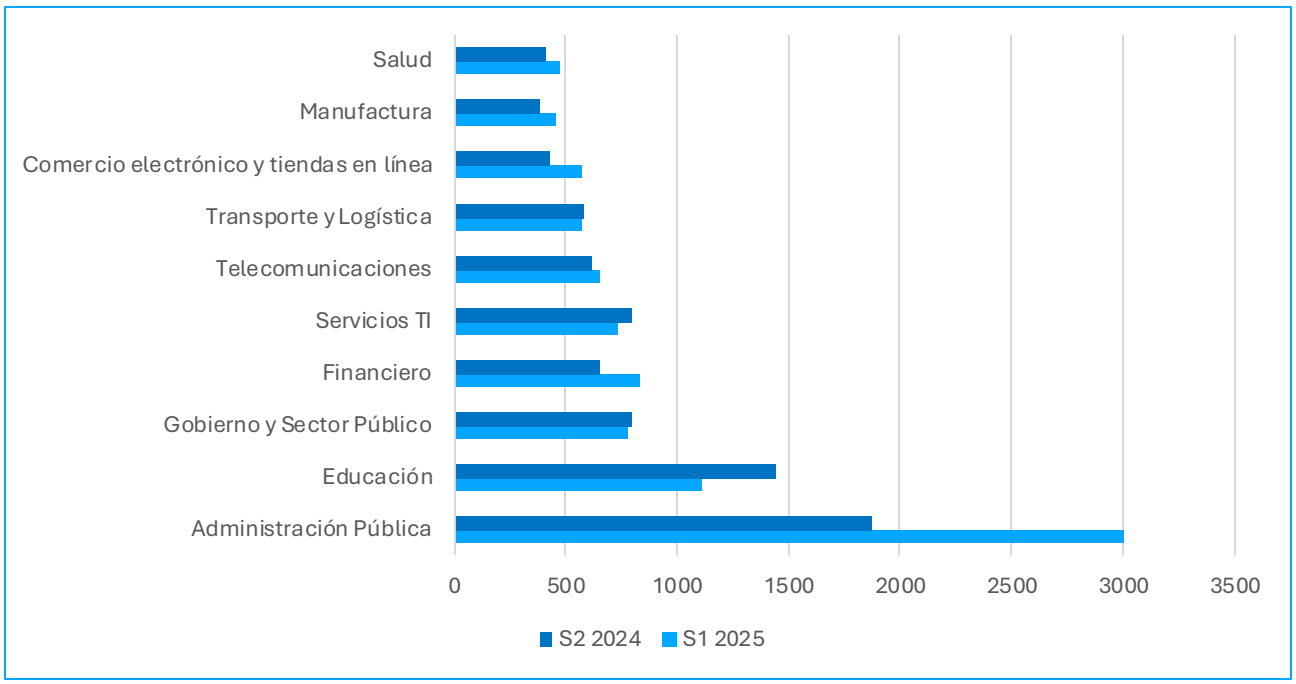


Figura 1 | Sectores más afectados por ciberataques en el primer semestre de 2025.

Por otro lado, la distribución temporal de ciberataques totales registrados marcó un aumento uniforme durante el último trimestre de 2024, manteniéndose en su mayoría constante durante el primer trimestre de 2025 y descendiendo casi a la mitad en abril de este mismo año. La tendencia sigue una evolución constante desde mayo pero se espera que vuelvan a incrementar los valores a lo largo del año.

Evolución temporal de ciberataques

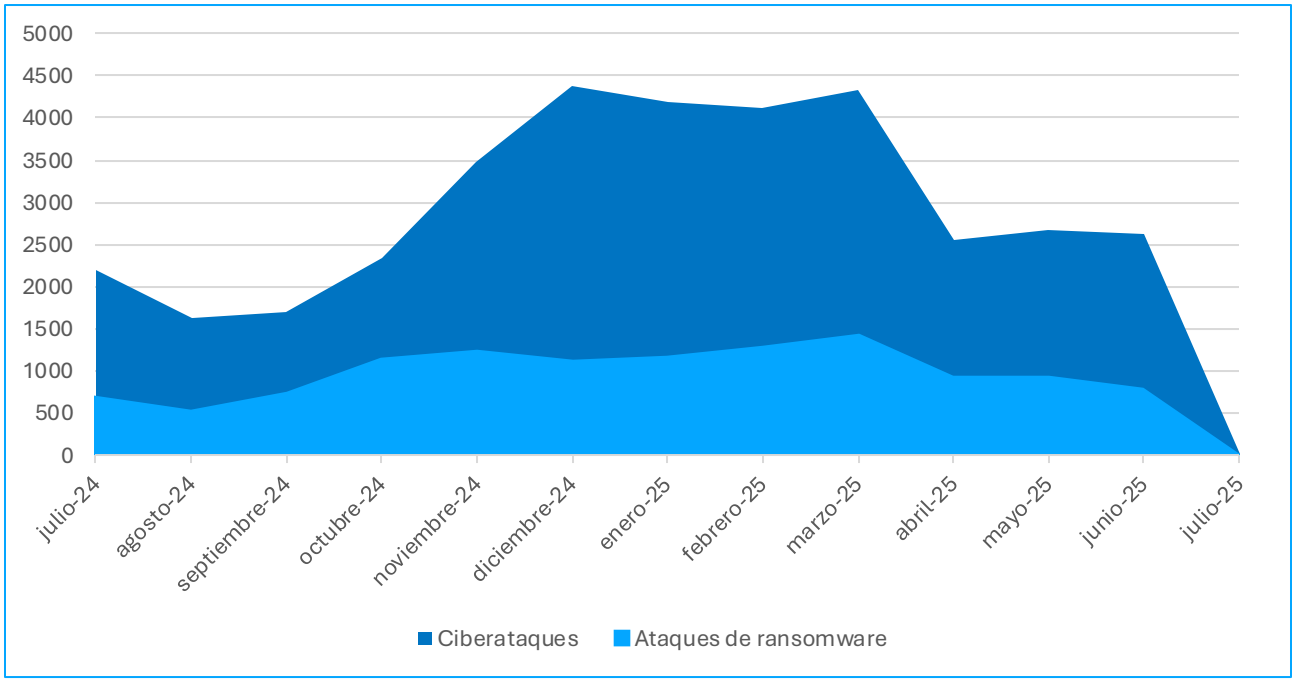


Figura 2 | distribución temporal de los CIBERATAQUES registrados del s2 2024 hasta 2025.

Continuando con la distribución del impacto, no solamente se observa una clara variación entre sectores, sino que se puede identificar una tendencia marcada en ciertos países que han sufrido un mayor volumen de ciberataques en este primer semestre del año:

- **Estados Unidos:** Con **4.046 ataques,** lidera la lista de países más afectados, lo que refleja su importancia estratégica y económica, con **un aumento del 35,6% desde 2024.**
- **India:** Involucrada en conflictos armados, y aun siendo recientemente blanco de diferentes actores de amenazas, ha registrado **1.644 ataques,** casi un 21% menos que en el último semestre del año pasado.
- **Israel:** La guerra con Palestina lo posiciona en contra de muchas potencias, con un registro de **1.637 ciberataques** en 2025 Israel es el **tercer país más afectado a nivel mundial.**
- **Francia:** Con un **4% de la distribución, 921 ataques,** Francia se prepara para la ciberguerra con simulacros de defensa ante simulaciones de ataques reales inspirados por el conflicto Rusia-Ucrania.
- **Ucrania:** Con **768 ataques,** sigue enfrentando amenazas vinculadas a los conflictos regionales, entre las que se incluyen el ciberespionaje y el sabotaje de infraestructuras críticas. Si bien, parece que las estrategias de defensa y contraataque están siendo efectivas, ya que la cifra actual de ciberataques se sitúa en un **36% menos que el semestre pasado.**

Distribución de ciberataques por países de Enero a Junio 2025

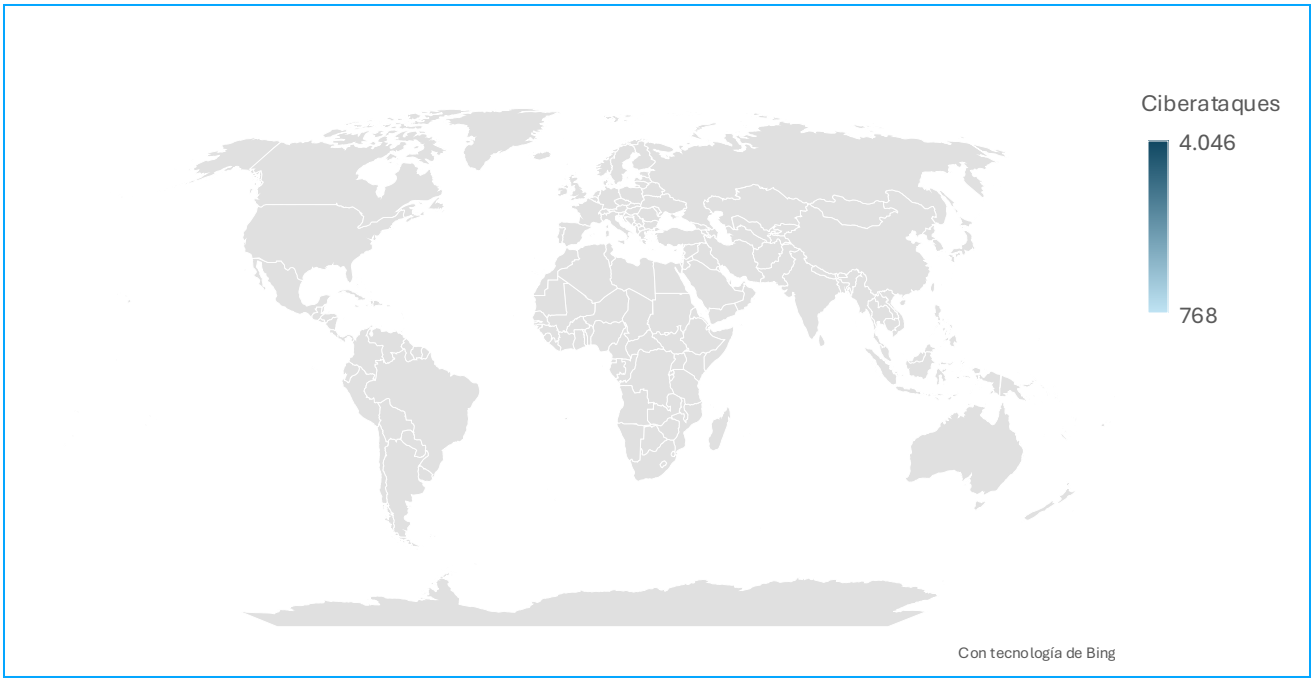


Figura 3 | Distribución geográfica del impacto de ciberataques en el primer semestre de 2025.

La distribución geográfica de los ciberataques marca como principal foco a Estados Unidos, involucrado en el conflicto con China por la guerra comercial, tecnológica y territorial, también en constante rivalidad con Rusia, quien históricamente cuenta con grupos APT muy avanzados. A su vez, el resto de potencias afectadas seguirán siendo foco de amenazas mientras se mantengan los conflictos actuales, dependiendo la distribución geográfica de la situación geopolítica extendida al ciberespacio.

Principales Amenazas Globales

3. Principales amenazas globales

El primer semestre de 2025 ha mantenido un panorama de ciberamenazas en constante evolución, marcado por un alto grado de sofisticación y una creciente orientación hacia la explotación de vulnerabilidades críticas. Aunque muchas tácticas observadas en 2024 siguen vigentes, se ha consolidado una mayor especialización por parte de los actores maliciosos.

Los ciberincidentes con impacto global, el auge de nuevas técnicas de acceso y persistencia, y la profesionalización de modelos como el RaaS reflejan una amenaza que no solo persiste, sino que se adapta con rapidez. Al mismo tiempo, el mercado clandestino continúa activo, aunque con una menor visibilidad pública debido al traslado hacia canales más privados.

3.1 Grandes ciberincidentes y/o campañas

En los primeros seis meses de 2025, el mundo ha presenciado una serie de ciberincidentes de gran escala que han comprometido infraestructuras críticas, servicios esenciales y la privacidad de millones de personas. Estos eventos no solo han evidenciado vulnerabilidades técnicas, sino también déficits en la gestión del riesgo, la respuesta a incidentes y la preparación frente a amenazas complejas.

Desde el **Departamento de Cyber Threat Intelligence de NTT DATA** hemos documentado algunos de los ciberincidentes más relevantes del primer semestre de 2025, seleccionándolos por su valor representativo de las principales amenazas observadas en este periodo. Nuestra lista incluye casos confirmados de *ransomware*, fugas de datos, campañas de phishing, ataques DDoS, *malware* y ciberataques destructivos, con el objetivo de ilustrar la diversidad de sectores afectado y la evolución de las tácticas empleadas por los actores maliciosos.

Víctimas	Tecnología / Sector	Atacante	País afectado	País del atacante	Fecha del incidente	URL
United Health	Salud / Datos personales	Desconocido	EE.UU.	Desconocido	01/01/2025	Fuente
Plataforma e-commerce Japón	Infraestructura Web	Desconocido	Japón	Desconocido	01/01/2025	Fuente
Cloudflare	Red / Infraestructura	Desconocido	Global	Desconocido	02/02/2025	Fuente
Insight Partners	Servicios financieros	Desconocido	EE.UU.	Desconocido	19/02/2025	Fuente
Marks & spencer	Retail	Scattered Spider	Reino Unido	Desconocido	27/04/2025	Fuente
Synnovis	Salud pública	Qilin	Reino Unido	Desconocido	20/05/2025	Fuente
Condado de Cobb	Gobierno local	Qilin	EE.UU.	Desconocido	20/05/2025	Fuente
Varias plataformas	Servicios online/ contraseñas	Malware / Infostealer	Global	Desconocido	28/05/2025	Fuente
GLS (Phishing)	Logistica	Desconocido	España	Desconocido	31/05/2025	Fuente
Victoria´s Secret	Retail / e-commerce	Desconocido	EE.UU.	Desconocido	02/06/2025	Fuente
Coinbase	Tecnología/ BPO	Insider/ Amenaza interna	India	Desconocido	02/06/2025	Fuente
Telefónica	Telecomunicaciones	Dedale	Perú	Desconocido	03/06/2025	Fuente
SVT / Bank-id	Televisión/ sistemas de identificación	Desconocido	Suecia	Desconocido	11/06/2025	Fuente

Tabla 1 | Grandes ciberincidentes de seguridad en el primer semestre de 2025.

3.2 Tendencias emergentes de ataques

Durante el primer semestre de 2025, el panorama de amenazas ha mostrado una clara aceleración. La madurez operativa de los grupos de ransomware, la adopción de IA ofensiva, la industrialización de los accesos iniciales y la explotación sistemática de vulnerabilidades han dado lugar a un ecosistema más ágil, opaco y difícil de anticipar.

En este contexto, se destacan las siguientes tendencias técnicas y operativas que marcan la actividad en el ciberespacio durante este primer semestre:

3.2.1 Uso masivo de brokers de acceso e IA ofensiva

Los *Initial Access Brokers* (IABs) han consolidado su rol como facilitadores clave para operaciones de *ransomware* y exfiltración. Sus catálogos han crecido un 15%, destacando accesos a tecnologías como Ivanti *Connect Secure*, Fortinet FortiOS y *appliances* de Palo Alto (Group-IB, 2025).

Estos accesos se venden por precios que oscilan entre los 300 y 5.000 USD. Paralelamente, herramientas de IA están siendo utilizadas para el reconocimiento automatizado de superficies de ataque expuestas, alimentado a brokers y APTs con información actualizada sobre activos vulnerables.

3.2.2 Profesionalizando el ransomware: alianzas, reagrupaciones y especializaciones

El modelo Raas ha alcanzado una madurez operativa sin precedentes. Grupos como Cl0p, Akira, Qilin y RansomHub han protagonizado la mayoría de campañas, sumando más de 1.200 ataques en el semestre. Destaca el uso extendido de herramientas legítimas antes del cifrado, conocido como *Living off the Land,* donde los atacantes priorizan estas herramientas para obtener persistencia y evitar ser detectados por antivirus tradicionales.

Además, estamos presenciando un fenómeno sin precedentes en el ecosistema del ransomware: la absorción de afiliados y la reutilización de infraestructuras por parte de grupos emergentes, que aprovechan los restos operativos y técnicos de colectivos disueltos como LockBit o Alphv. Este reciclaje se apoya en la inteligencia recopilada desde foros y canales de Telegram filtrados.

Paralelamente, se están consolidando alianzas entre actores de distintas especialidades, incluso de regiones geopolíticamente opuestas. Estos acuerdos permiten repartir beneficios, subcontratar fases del ataque y optimizar recursos como si se tratara de estructuras empresariales.

También se dan situaciones contrarias de enfrentamientos entre grupos, como el caso del cese de operaciones de Black Basta en abril de 2025 tras filtraciones internas, mientras en plataformas como X se han visto disputas públicas entre actores maliciosos por apropiaciones de víctimas de fugas de información, evidenciando un entorno cada vez más competitivo y fragmentado (Group-IB, 2025).

3.2.3 Automatización del fraude con IA: Suplantaciones y ataques dirigidos

En el primer semestre de 2025 se ha consolidado el uso de IA en campañas de fraude, suplantación e ingeniería social, impulsando ataques más personalizados, creíbles y automatizados. La IA se emplea para generar identidades falsas, voces sintéticas y correos de spear phishing basados en datos filtrados o perfiles públicos, así como para automatizar fases completas de ataques en sectores financieros y gubernamentales (Hitachi Cyber, 2025; KrakenLabs, 2025).

Paralelamente, se ha documentado un ecosistema emergente de herramientas ofensivas basadas en IA que abaratan y simplifican el cibercrimen. Entre ellas destacan generadores de texto como FraudGPT y WormGPT para redactar comunicaciones fraudulentas; herramientas de clonación de voz (ElevenLabs, Voicemy.ai) y vídeo (DeepFaceLab, Faceswap) usadas para eludir verificaciones de identidad y kits como EvilProxy o Robin Banks, que automatizan páginas de phishing con capacidades Adversary-in-the-Middle (AITM) para robar credenciales con MFA. Asimismo, se ha detectado el uso de bots sociales con IA en Telegram y otras plataformas, que simulan conversaciones de soporte técnico para obtener datos sensibles.

Estas capacidades están reduciendo la barrera técnica de entrada al cibercrimen, permitiendo que actores sin experiencia previa desplieguen campañas complejas y dirigidas, lo que agrava la amenaza para las empresas y gobiernos.

3.2.4 Malware como servicio: auge de infostealers como Lumma y RedLine

El mercado MaaS (Malware-as-a-Service) ha tenido como protagonistas a Lumma Stealer y RedLine, con registros de más de 3 millones de credenciales robadas por día (MTI, MDC & MSE, 2025). Lumma ha sido relacionado con múltiples campañas de robo masivo de información, incluyendo cookies de sesión, wallets, contraseñas de navegador y configuraciones de VPN.

Aunque su infraestructura fue interrumpida en mayo por Europol y Microsoft, se observó un resurgimiento casi inmediato a través de forks y rebranding de su C2. Además, los atacantes han *trasladado su distribución a canales privados como Discord y Telegram, dificultando su detección y atribución.*

3.2.4 Selección de objetivos y explotación sectorial

Los actores maliciosos están afinando sus campañas según la industria objetivo. Sectores como el financiero, educación y administración pública han concentrado la mayoría de los ataques debido a su bajo umbral de seguridad, alta dependencia digital y potencial impacto reputacional (CERT-EU, 2025). Esta segmentación no solo mejora las tasas de éxito, sino que también permite maximizar la presión extorsiva adaptando el lenguaje, la documentación robada y las técnicas de comunicación.

3.3 Estadísticas globales sobre incidentes de seguridad, tipos de ataques y actores de amenazas involucrados

Desde el Departamento de Cyber Threat Intelligence se ha podido establecer que, durante el primer semestre de 2025, los ciberataques no solo han mantenido un ritmo sostenido, sino que han mostrado una evolución en cuanto a su enfoque, complejidad técnica y segmentación sectorial.

A continuación, se resumen las principales estadísticas y tendencias observadas en este periodo:

- **Ransomware:** Se mantiene como la principal amenaza global. El número de ataques **aumentó en torno al 32% respecto al semestre anterior.** Más de 1.200 incidentes se han atribuido a grupos como Akira, Cl0p y RansomHub, destacando por su segmentación sectorial y uso sistemático de técnicas de doble extorsión y herramientas legítimas previas al cifrado (CrowdStrike, 2025; KrakenLabs, 2025).
- **Phishing y vishing:** Se ha observado un crecimiento marcado del vishing asistido por IA, con un aumento de ataques desde finales de 2024. Las campañas se han vuelto más realistas, aprovechando tecnologías de clonación de voz y perfiles sintéticos para ejecutar fraudes dirigidos, especialmente en entornos financieros y de recursos humanos (Group-IB, 2025; Hitachi Cyber, 2025).
- **Filtraciones de datos:** En lo que va de año, se han reportado más de 1.000 brechas relevantes, muchas con impacto en organizaciones del sector financiero, retail y administración pública. La tendencia al alza de 2024 se mantiene, con actores que emplean herramientas más complejas para la exfiltración y monetización de la información (World Economic Forum, 2025; CyberArk, 2025).
- **Ataques DDoS:** Aunque el volumen global de ataques ha descendido ligeramente, se ha incrementado su sofisticación y uso combinado con tácticas de extorsión. Las campañas selectivas contra infraestructuras críticas y plataformas de pago se han consolidado como una herramienta de presión recurrente (CERT-EU, 2025).
- **Ataques impulsados por IA:** El uso ofensivo de inteligencia artificial se ha convertido en una táctica transversal. Se aplica a múltiples fases del ataque: desde la automatización del reconocimiento hasta la generación de correos maliciosos o identidades falsas. Esto ha potenciado campañas de phishing, suplantación y ataques multivector más creíbles y masivos (KrakenLabs, 2025; CrowdStrike, 2025).

Incremento porcentual estimado de ataques por categoría para el primer semestre de 2025.

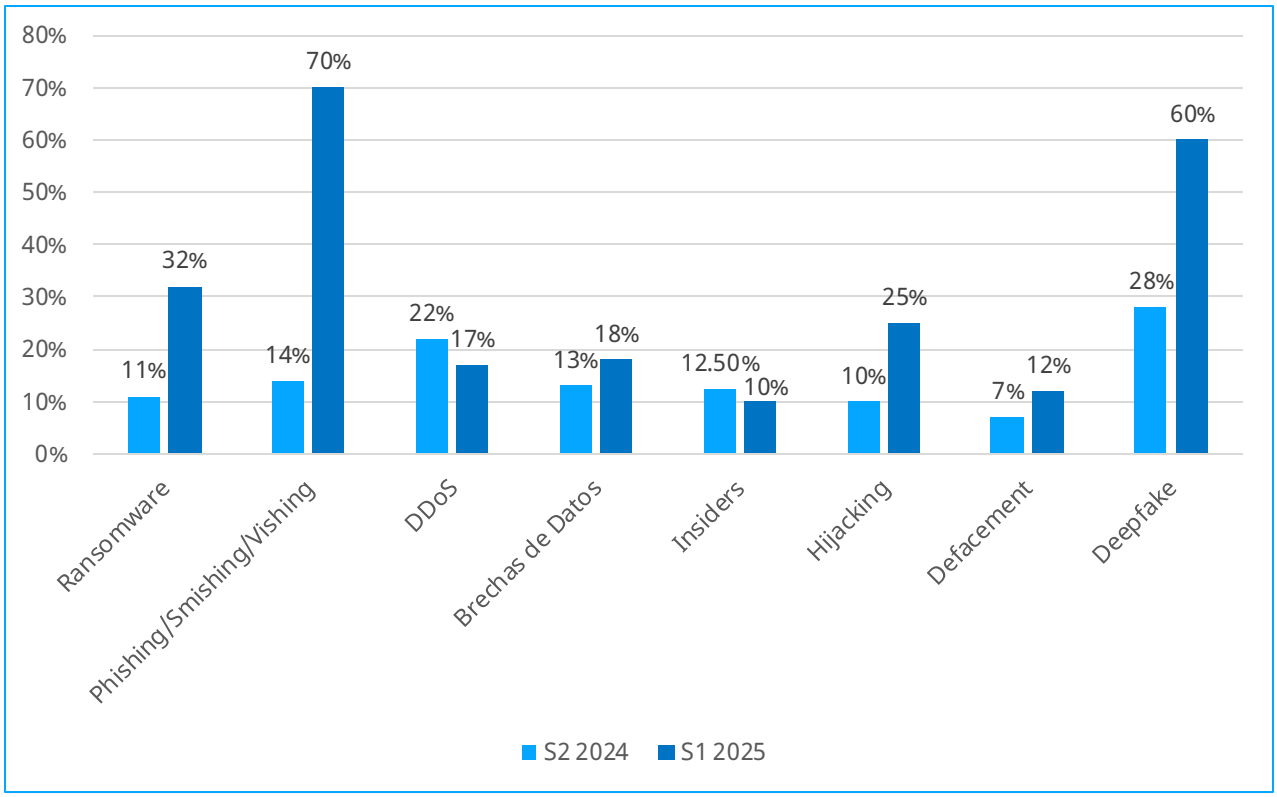


Figura 4 | Porcentaje de incremento en el número de ataques por categoría en comparación con el segundo semestre de 2024.

A pesar de que algunas categorías como el *phishing*, el *smishing* o los *deepfakes* presentan un mayor incremento porcentual respecto al semestre anterior, esto no implica que hayan superado en volumen absoluto a amenazas consolidadas como el *ransomware*.

Estos datos reflejan la evolución dinámica del panorama de amenazas, donde técnicas emergentes están creciendo con rapidez, aun así, **el *ransomware* continúa liderando en cuanto a impacto operativo, frecuencia global y rentabilidad para los actores maliciosos.**

3.4 Costes de los ciberataques para las empresas

Durante el primer semestre de 2025, los costes derivados de los ciberataques han seguido una trayectoria ascendente, impulsados tanto por la frecuencia y sofisticación de los incidentes como por el impacto operativo que generan. Las estimaciones más recientes sitúan el **coste global del cibercrimen en una cifra récord de 10,5 billones de dólares anuales**, con una proyección de crecimiento sostenido que **podría alcanzar los 12 a 15 billones hacia finales de año** si se mantienen los niveles actuales de actividad maliciosa (Cybersecurity Ventures, 2025).

En términos específicos, los gastos más relevantes para las organizaciones durante este semestre han sido:

- **Disrupciones de negocio,** que encabezan el impacto económico con una **media estimada de 13,2 billones de USD,** debido a interrupciones en cadenas de suministro, plataformas de pago y servicios críticos.
- **Los costes de "ciberrefuerzo",** incluyendo inversiones en detección, respuesta y formación, han ascendido hasta los **10,8 billones USD,** presionados por la rápida adopción de tecnologías basada en IA y entornos *multicloud.*
- Los **rescates pagados** a grupos de *ransomware* han alcanzado los **6,3 billones USD**, con un aumento notable en las demandas superiores a los 5 millones por incidente, especialmente en los sectores salud, manufactura y transporte.

- Las **sanciones económicas y legales derivadas de incidentes y filtraciones de datos** han **superado los 7,14 billones USD**, en parte debido al endurecimiento normativo en regiones como la UE, Reino Unido y Asia-Pacífico (Gov.UK, 2025; Stamford, 2024).

Comparado con el cierre de 2024, se observa un **crecimiento estimado del 15% en los costes globales de ciberseguridad**, concentrado especialmente en sectores como infraestructuras críticas o procesos altamente interconectados. Las campañas dirigidas durante fechas clave también han contribuido a la escalada de estos costes, con picos de hasta un 40% adicional en gastos de contención en empresas afectadas en diciembre y enero. (Stamford, 2024; Tamzid, 2025).

Evolución anual de los costes estimados en ciberseguridad desde 2020 hasta 2025.

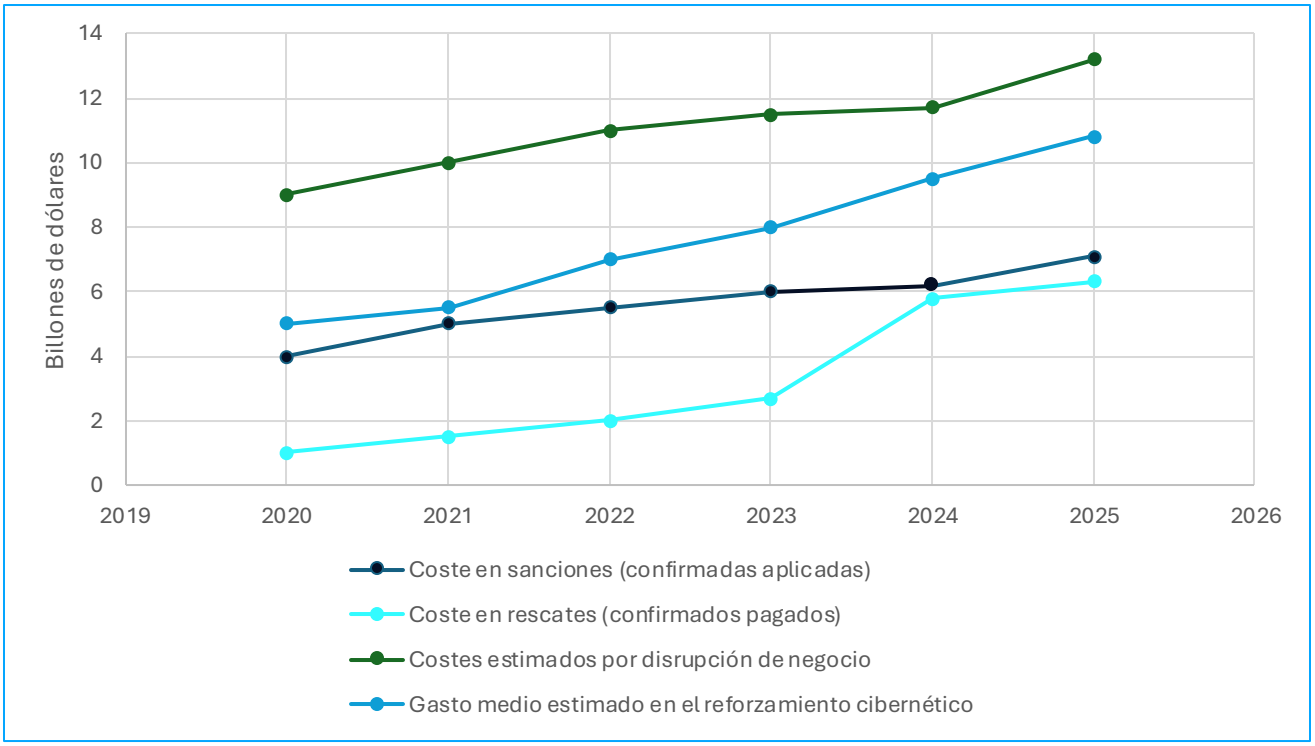
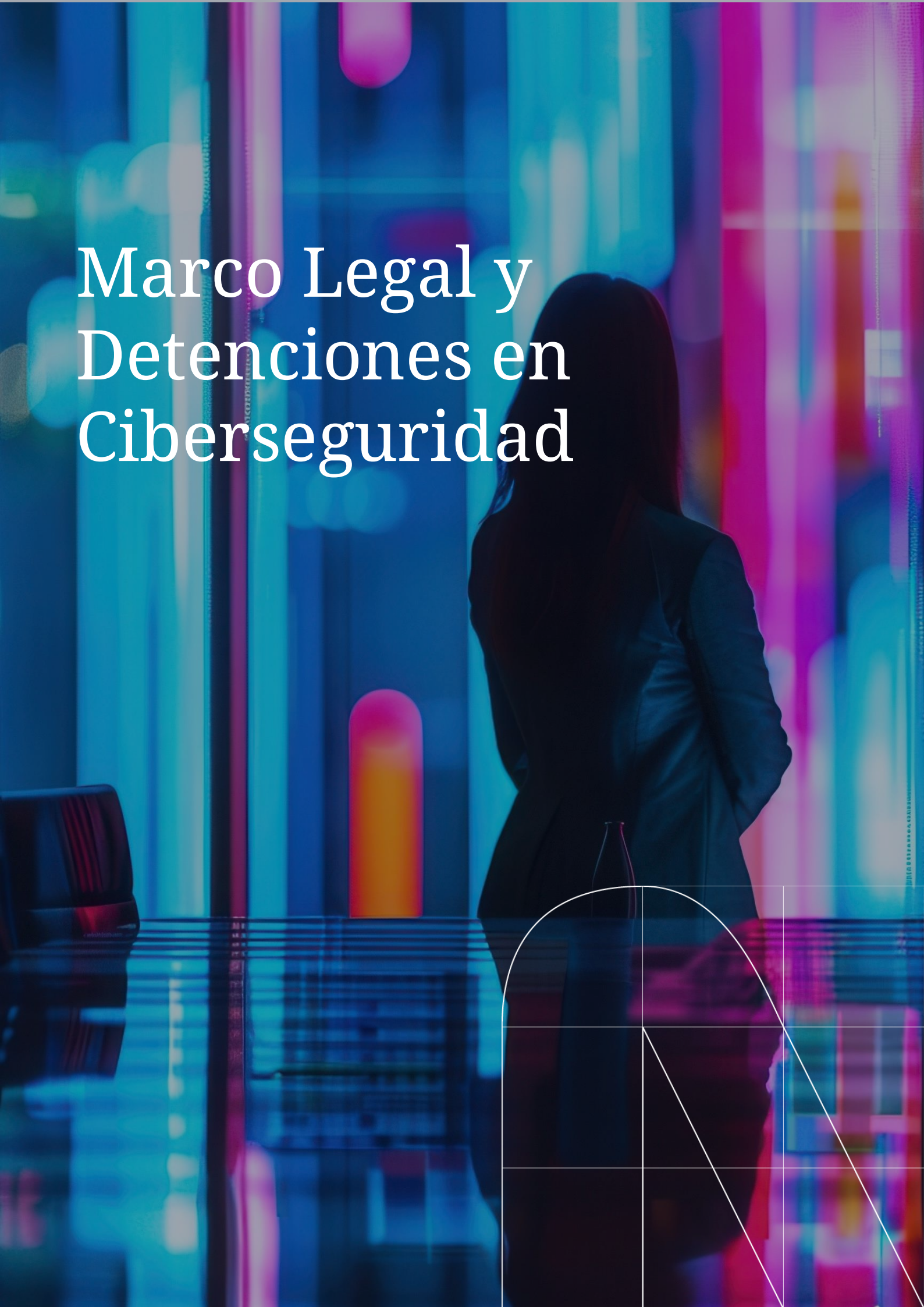


Figura 5 | Evolución anual comparativa de los costes estimados en ciberseguridad (2020-2025) desglosados en sanciones, rescates, disrupciones de negocio y refuerzo cibernético.

La gráfica incluida en este apartado ha sido actualizada para reflejar los datos consolidados del segundo semestre de 2024 y del primer semestre de 2025, basados en fuentes oficiales y publicaciones de proveedores internacionales. Durante la elaboración del informe anterior, las cifras de 2024 fueron estimadas en un contexto de cierre parcial del año y con información todavía sujeta a revisión. Con la publicación en 2025 de métricas estandarizadas y fiables sobre el coste económico del cibercrimen, se han corregido las discrepancias iniciales y se presenta una fotografía más precisa del impacto real.



Marco Legal y Detenciones en Ciberseguridad

4. Marco legal y detenciones en ciberseguridad

Desde el **Departamento de Cyber Threat Intelligence** de **NTT DATA**, se considera esencial analizar las medidas de seguridad implementadas, las leyes aprobadas en el ámbito de la ciberseguridad y las detenciones realizadas por los cuerpos de seguridad a nivel global en este primer semestre de 2025.

Con este análisis se evalúa el compromiso de los países en la regulación y control de tecnologías actuales y emergentes, así como su aplicación responsable. Además, se refleja el esfuerzo conjunto de los órganos legislativos, judiciales y de defensa para enfrentar las brechas de seguridad corporativa y combatir las actividades ilícitas en el ciberespacio.

4.1 Principales leyes en el ámbito de la ciberseguridad

En el primer semestre de 2025, el marco legal y normativo en materia de ciberseguridad ha seguido evolucionando a nivel global y nacional. A pesar de que algunos documentos aún se encuentran en fase de implementación o revisión, ya se observan importantes avances en cuanto a la armonización legislativa en el ciberespacio. Entre los principales desarrollos destacan:

Continente	Normativa	Institución	Referencias
África	The Cyber Security Act, 2025 The Cyber Crime Act, 2025	Parlamento de Zambia	National Assembly of Zambia
América del Norte	Insure Cybersecurity Act of 2025	U.S. National Telecommunications and Information Administration	USA Government
	HIPAA Privacy Rule (Actualizaciones 2025)	U.S. Department of Health & Human Services	Access Partnership
América del Sur	Ley Marco de Ciberseguridad N° 21.663	Ministerio del Interior y Seguridad Pública de Chile	Biblioteca del Congreso Nacional de Chile
	Plan Federal de Prevención de Ciberdelitos y Gestión Estratégica de la Ciberseguridad (2025 - 2027)	Ministerio de Seguridad Nacional de Argentina	Boletín Oficial de la República Argentina
Asia	Reglamento sobre la Gestión de la Seguridad de los Datos en Red (Nuevo proyecto de enmiendas)	Consejo de Estado de la República Popular China	China Briefing
	Ley de Tecnología Digital (DTI Law – Aprobada en junio)	Ministerio de Ciencia y Tecnología de Vietnam	Vietnam Briefing
	Proyecto de Ley de Protección de Infraestructuras Críticas (Sistemas Informáticos)	Consejo Legislativo de Hong Kong	Consejo Legislativo de Hong Kong
	Proyecto de ley de protección contra estafas	Parlamento de Singapur	Singapore Government
	Ley de Ciberdefensa Activa (ACD – Aprobada en mayo)	Parlamento Nacional de Japón	The House of Representatives, Japan
Europa	Reglamento de Ciberresiliencia (Cyber Resilience Act (CRA))	Comisión Europea	Comisión Europea
	Reglamento de Inteligencia Artificial	Unión Europea	Consejo Europeo
	Reglamento (UE) 2025/37	Unión Europea	Unión Europea
	Reglamento de Cibersolidaridad (Cyber Solidarity Act)	Unión Europea	Unión Europea
	NIS2 Directive	Unión Europea	NIS2 Directive
	Reglamento de Resiliencia Operativa Digital (DORA)	Comisión Europea / Autoridades Financieras Unión Europea	Field Fisher
	EU Cybersecurity Act (en revisión con nuevos esquemas de certificación)	Agencia de Ciberseguridad de la UE (ENISA)	Field Fisher
	Ley española de Coordinación y Gobernanza de la Ciberseguridad	Gobierno de España / INCIBE España	Ministerio del Interior
Oceanía	Cyber Security (Ransomware Payment Reporting) Rules 2025	Gobierno de Australia	Federal Register of Legislation

Tabla 2 | Leyes aprobadas o de aplicación en el primer semestre del 2025.

Estas normas jurídicas, tanto a nivel nacional como europeo, buscan mejorar la resiliencia frente a los riesgos digitales, fortalecer la protección de datos e infraestructura crítica, y establecer un marco de evaluación de riesgos más robusto. En particular, la Directiva NIS2 y el Reglamento DORA representan un paso hacia la homogeneización de las normas de seguridad digital entre los países miembros de la Unión Europea.

4.2 Principales detenciones en el ámbito de la ciberseguridad

Durante el primer semestre de 2025, se han llevado a cabo numerosas operaciones internacionales orientadas al desmantelamiento de redes cibercriminales y la neutralización de grupos de ransomware, actores de desinformación y APT. Estas actuaciones impulsadas en muchos casos por colaboraciones entre cuerpos de policía, agencias gubernamentales y entidades privadas han permitido interrumpir la actividad de actores altamente organizados y con presencia transnacional.

A continuación, se presenta una tabla resumen con las principales operaciones desarrolladas en este semestre:

Operación	Grupo de sector de amenazas	Fuerzas y cuerpos de seguridad	Referencias
Operación contra *Lumma Stealer*	Numerosos dominios	Departamento de Justicia de EE.UU. Europol *Microsoft's Digital Crimes Unit* (DCU)	Justice Government
Phobos	Phobos Ransomware	Europol Interpol Agencias locales de varios países	United States Attorney's Office
Phobos Aetor	*8Base Ransomware*	Europol Police Lieutenant General Trairong Phiwphan Agencias policiales locales	Dark Web Informer
Sindoor	*AnonSec* y actores relacionados con desinformación y terrorismo	Gobierno de India Inteligencia militar	Clarion India
Raptor	Vendedores de la d*ark web*	Europol Agencias policiales de Austria, Brasil, Alemania y otros países	Europol
Operation secure	Ataque a infraestructuras maliciosas que albergan *infostealers*	Interpol Agencias locales de varios países	Interpol
Operation Deep sentinel	*Archetyp Market*	Autoridades policiales de Alemania Europol Eurojust	Europol
Operación contra BreachForuns	Cúpula de *BreachForums*	Brigada de Ciberdelincuencia (BL2C) (París) FBI	USA Attorney's Office Le Parisien

Tabla 3 | Principales operaciones de desmantelamiento de bandas de cibercriminales llevadas a cabo en 2025.

Además de estas operaciones llevadas a cabo por agencias policiales reconocidas a nivel global, se ha observado una intensificación de las **campañas de filtraciones internas y desenmascaramientos** de grupos conocidos de ransomware por otros grupos de dudosa reputación. Una muestra destacada de este fenómeno es la aparición del canal de Telegram ***"GangExposed",*** gestionado por el grupo ***CactusPulse,*** que ha ganado notoriedad por su labor de recopilación, verificación y publicación de inteligencia operativa sobre miembros de grupos altamente destructivos como **Conti, Trickbot y Black Basta.**

Durante los meses de abril y mayo, *GangExposed* publicó imágenes y perfiles de 15 miembros del grupo *Conti*, entre ellos su supuesto negociador principal, Arkady Valentinovich Bondarenko. Además, se reveló la identidad de un actor apodado "8G", considerado como uno de los coordinadores centrales de *Black Basta*, responsable de operaciones de despliegue, evasión de antivirus, sección de objetivos y pagos en criptomonedas.

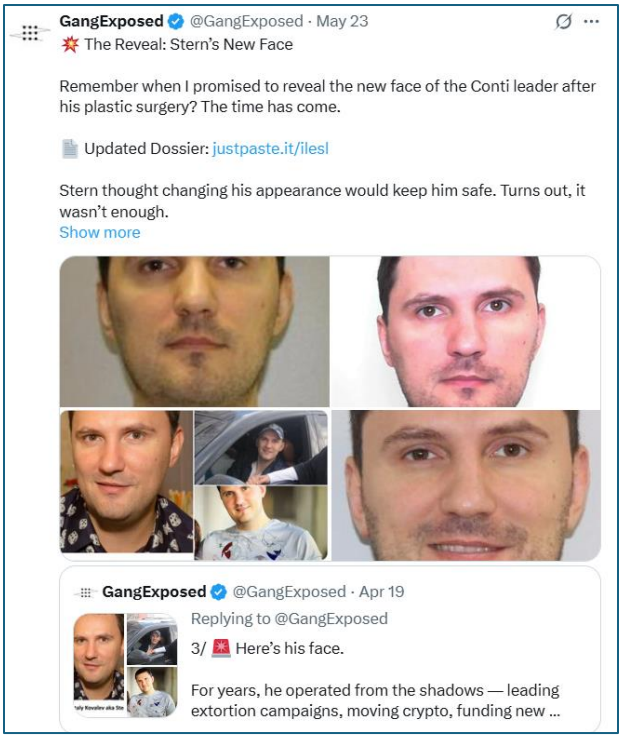


Ilustración 1 | Exposición en la plataforma X realizada por el grupo *GangExposed.*

Las publicaciones de este canal han incluido chats internos filtrados, evidencias sobre pagos, estrategias de ingeniería social utilizadas para contactar con víctimas, y manuales de procedimiento para operaciones maliciosas. Esta actividad representa un tipo de guerra de inteligencia no vista hasta ahora en el panorama cibercriminal, donde algunos grupos o individuos, posiblemente motivados por represalias, recompensas gubernamentales o rupturas internas, optan por filtrar datos confidenciales y estructuras jerárquicas de sus antiguos aliados.

Este fenómeno no solo está ayudando a las fuerzas del orden a identificar y perseguir a líderes de alto nivel dentro del cibercrimen organizado, sino que también está desestabilizando estructuras delictivas que hasta ahora se creían protegidas por el anonimato y la descentralización.

Dark Web Insights

5. Dark Web Insights

En el primer semestre de 2025, la dark web ha seguido funcionando como uno de los principales ecosistemas para la actividad cibercriminal, especialmente en lo referente a la compraventa de datos robados, accesos ilícitos a sistemas, credenciales, herramientas de malware y servicios de hacking bajo modelos CaaS (Crime-as-a-Service). Este periodo ha estado marcado por una reconfiguración profunda tanto en los mercados como en los foros underground, principalmente a raíz de la pérdida de Breach Forums.

5.1 La caída de BreachForums: impacto y consecuencias

El cierre de *BreachForums* en abril de 2025 , la posterior puesta en venta del foro por parte de uno de sus administradores en junio y las detenciones de sus administradores más famosos, como *IntelBroker*, supuso un punto de inflexión.

El foro era una de las principales plataformas de intercambio de bases de datos robadas, accesos comprometidos, *logs* de *infostealers* y herramientas ofensivas. Su desaparición dejó un vacío logístico y simbólico en el ecosistema cibercriminal. Este colapso ha forzado una **migración de usuarios** hacia foros privados y canales cifrados, pero también hacia *marketplaces* ya consolidados. La consecuencia directa ha sido una mayor descentralización de la actividad maliciosa y un crecimiento de plataformas especializadas.

5.2 Foros *underground* activos en 2025

- En ausencia de *BreachForums*, otros foros han retomado protagonismo:
- ***Dread***: Foro similar a *Reddit* en la *dark web*, utilizado para *doxing*, filtraciones y discusión técnica.
- **XSS.is**: Considerado el "foro élite" para actores rusoparlantes, algunos participantes fueron vinculados a incidentes contra infraestructuras críticas en Europa del Este.
- ***Dark Forums***: Cuenta con **más de 12.767 usuarios registrados en abril de 2025**, obteniendo a la mayoría gracias a la desaparición de *Breach Forums*. Se caracteriza por una comunidad muy activa en *malware*, *infostealers* y *cracking* de cuentas. Es uno de los pocos que mantiene una sección educativa con guías detalladas de *scripting* malicioso.
- ***Exploit.in***: Fundado hace más de 15 años, es el foro con mayor permanencia histórica. A menudo se publican vulnerabilidades antes de que tengan CVE asignado. En **febrero de 2025, se reveló ahí un *0-day* contra *Palo Alto Networks*.**
- ***Nulled***: Enfocado en la compartición de credenciales, herramientas *cracking* y *leaks* masivos.
- ***Sinister.ly*:** Mezcla contenido técnico con foros sociales o de cultura *hacker*, lo que lo hace atractivo para perfiles más jóvenes. Es una de las plataformas donde más se discuten herramientas basadas en *Python* para automatizar *phishing*.
- ***Cracked.io*:** Portal híbrido entre foro y *market*, especializado en cuentas de servicios en línea.
- ***KickAss***: Aunque más reciente, ha ganado fama por ser un punto de encuentro para desarrolladores de *malware* modular. También ofrece servicios de desarrollo personalizado para grupos APT.

Estos foros permiten el intercambio libre de herramientas, tutoriales, vulnerabilidades y dumps de bases de datos, así como servicios a medida.

Principales publicaciones en el *Dark Web*

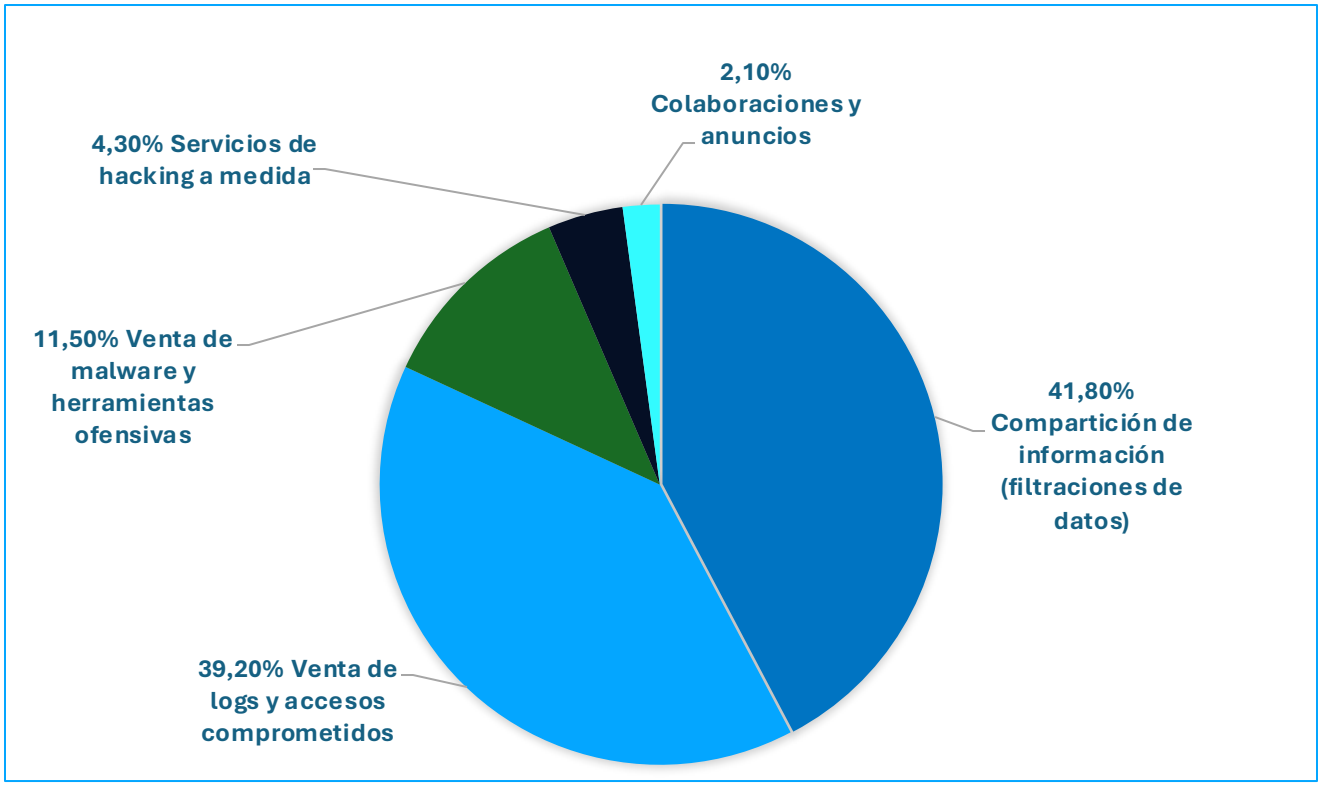


Figura 6 | Categorías principales de publicaciones en la Dark Web en el primer semestre de 2025.

Los *logs* de *infostealers* como ***Lumma***, ***RisePro*** y ***RedLine*** han tenido una presencia dominante, superando los **7,7 millones de conjuntos de credenciales listados** solo en los primeros cinco meses de 2025. A su vez, los *dumps* de tarjetas comprometidas alcanzaron los **14,4 millones, con un 80% de tarjetas estadounidenses**, vendidas entre 5 y 30 dólares.

5.3 Mercados underground activos en 2025

- ***Abacus Market*:** Con una interfaz simple, es conocido por la venta de tarjetas SIM anónimas y *kits* de robo de identidad. Gana relevancia en 2025 por el número creciente de vendedores especializados en *deepfakes* personalizados, aunque a finales de junio se ha podido observar **una serie de disrupciones en su servicio habitual**, lo cual puede indicar que posteriormente a este informe el mercado sea detenido.
- ***Russian Market*:** Acepta múltiples criptomonedas y ofrece **más de 150.000 credenciales robadas diarias**. Es particularmente conocido por su servicio de "actualización" de *logs* cada 24 horas, que garantiza la frescura de las credenciales.
- ***Brian's Club*:** Después de haber sido *hackeado* en 2019, resurgió y en 2025 vuelve a estar **entre los tres primeros en volumen de tarjetas**. Se estima que gestiona más de 10 millones de registros únicos activos.
- **Exodus Market:** Su punto fuerte son los exploits zero-day y el acceso privilegiado a servidores empresariales en regiones como LATAM y Asia-Pacífico. Tiene un sistema de reputación de triple verificación para los vendedores.
- **Styx Market:** Se especializa en herramientas para ataques de phishing multicanal. En marzo de 2025 fue vinculado a varias campañas de distribución de Lumma y RisePro a través de macros de Excel maliciosos.
- **BidenCash:** Se hizo popular por publicar gratuitamente más de 2 millones de tarjetas robadas en campañas de marketing criminal en 2022 y manteniendo su actividad con ventas de credenciales a mayores, hasta su desmantelamiento en la Operación RapTor.

A continuación se muestra la **distribución estimada** de las principales plataformas de venta *underground* activas durante el primer semestre de 2025, en función de su volumen de actividad y relevancia dentro del ecosistema cibercriminal:

Plataformas de venta underground

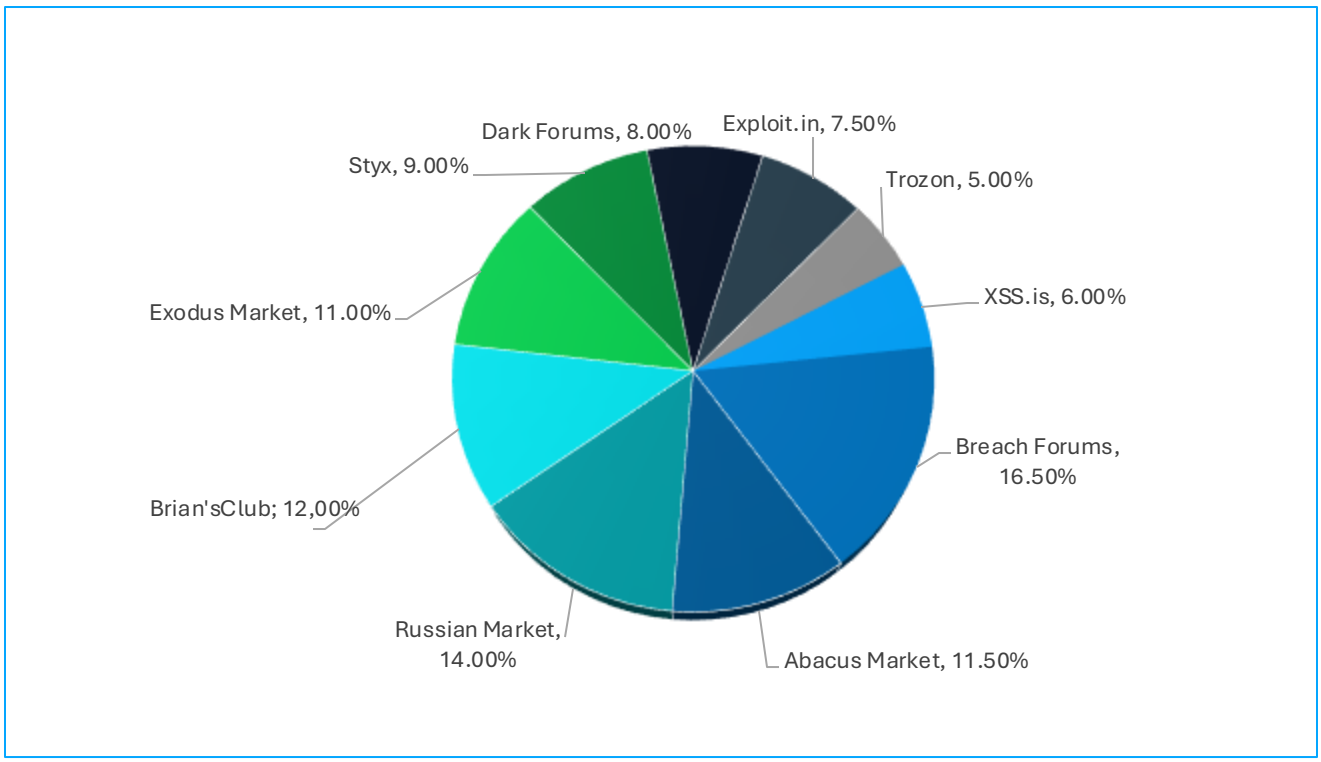


Figura 7 | Principales plataformas de venta underground identificadas en el primer semestre de 2025.

Durante este semestre, ha destacado la actividad del grupo ***RansomHub***, quien no solo ha absorbido a antiguos afiliados de otros grupos, sino que ha diversificado sus operaciones hacia foros y *markets* como ***Styx*** y ***Brian'sClub***. También se ha detectado un crecimiento operativo de **colectivos como *Storm-0953*** y afiliados asociados a herramientas de *infostealing*. Entre los **15 actores más prolíficos durante el segundo semestre de 2024 y el primer semestre 2025**, **9 estuvieron vinculados de alguna forma a *Breach Forums***.

Estos actores han protagonizado algunos de los ciberataques más relevantes de exfiltración de usuarios y ataques a grandes instituciones financieras de Asia (SOCRadar, 2025). En cuanto a la comunicación operativa, si bien Telegram sigue siendo una de las plataformas de referencia, se ha identificado un incremento significativo en el uso de **TOX, SimpleX y Signal,** todas aplicaciones descentralizadas y con fuerte cifrado *end-to-end*. Estas plataformas están ganando adeptos por ofrecer mayor privacidad, menor vigilancia y menor exposición a ataques de infiltración policial o toma de servidores.

Actores Maliciosos *(Threat Actors)*

6. Actores de Amenazas (Threat Actors)

En el primer semestre de 2025 el panorama de amenazas cibernéticas ha seguido evolucionando, marcado por la aparición de nuevos actores maliciosos, la adaptación y crecimiento de los grupos de ransomware, la actividad cada vez más organizada de los hacktivistas, y las tendencias y patrones emergentes de las APT.

6.1 Nuevos actores identificados

La continua diversificación de los actores de amenazas durante la primera mitad de 2025 no solo viene dada por la aparición de nuevos grupos cibercriminales, sino también por la consolidación de actores emergentes. Estos actores no hacen sino que reflejar, como ya adelantábamos, una profesionalización progresiva del ecosistema de amenazas.

Sector 16 / S16

Grupo activo desde enero de 2025 con una posible atribución rusa. Asociado con otros actores de amenazas como la alianza ***Z-Pentest*** o el grupo *hacktivista* ***OverFlame***, consolidando ataques contra infraestructuras críticas, particularmente hacia el sector petrolero y del gas y sistemas de tratamiento de agua. Con el uso de **técnicas de acceso inicial no autorizado a sistemas de control industrial y manipulación de parámetros operacionales** ha llevado ataques a organizaciones de diferentes partes del mundo: sistema SCADA de bombas de petróleo y tanques de almacenamiento en Texas (EE.UU.), una empresa italiana de bombas de agua industriales, y un par de empresas españolas, una de tratamiento de aguas y a un sistema APCS de una planta de dióxido de carbono (Orange Cyberdefense, 2025).

LazurGroup

Este colectivo de origen francés surgido en enero de 2025 ha centrado su actividad en Europa Occidental, especialmente en Francia y Bélgica. Sus operaciones combinan técnicas avanzadas de spear phishing, uso de herramientas de acceso remoto como *Cobalt Strike, y malware* personalizado. Además, gestionan canales de distribución y coordinación interna mediante Telegram. Su organización y grado de sofisticación ha llevado a expertos a considerarlo una potencial amenaza híbrida, con fines tanto criminales como ideológicos.

BianLian

Activo desde 2022, este grupo de *ransomware* ha evolucionado hacia un **modelo de extorsión sin cifrado**, basado exclusivamente en la filtración de datos. En 2025, tanto la CISA como el FBI alertaron sobre una oleada de campañas fraudulentas en las que actores independientes se hacen pasar por *BianLian* para extorsionar a ejecutivos mediante correo electrónico. Estas suplantaciones dificultan la atribución precisa, pero confirman el rol central del grupo en el panorama de amenazas contemporáneo (CISA, 2025; FBI, 2025).

Rhysida

Este RaaS fue identificado en 2023 y ha intensificado su actividad en 2025. La CISA, el FBI y el MS-ISAC actualizaron sus indicadores de compromiso y TTPs, tras varios ataques dirigidos a instituciones educativas, sanitarias y gubernamentales. Su estructura descentralizada y su enfoque multivectorial representan un desafío para la defensa (CISA, 2025).

Void Blizzard

También denominado *Laundry Bear*, es un grupo con afiliación rusa operativo desde abril de 2024 cuyas actividades pasadas se le han atribuido en mayo de 2025. Principalmente usa técnicas de *spear phishing*, exfiltración de datos y robo de credenciales y ha dirigido ataques contra infraestructuras críticas de Ucrania y sus aliados (miembros de la OTAN), y gobiernos y fuerzas especiales de Europa y EE.UU, por motivación geopolítica (Microsoft Threat Intelligence, 2025; Bleeing Computer, 2025).

Se observa una tendencia hacia una **diversificación de tácticas**, con un aumento en el uso de **herramientas LotL**. A lo largo del año, se espera un incremento en la **colaboración entre grupos**, así como una mayor convergencia entre el cibercrimen y el ciberespionaje, fusionando objetivos económicos y estratégicos que compliquen la atribución de ataques.

6.2 Grupos de ransomware

En 2025, el panorama de ciberamenazas ha sido marcado por la aparición de nuevos grupos de *ransomware* que han demostrado una rápida capacidad de adaptación y una creciente agresividad en sus tácticas. Paralelamente, los grupos ya consolidados han elevado su nivel de sofisticación, perfeccionando sus técnicas de evasión, cifrado y extorsión. Esta evolución ha intensificado la presión sobre organizaciones de todos los sectores, consolidando al *ransomware* como una de las amenazas más persistentes y disruptivas del ecosistema digital actual.

6.2.1 Nuevos grupos

Durante los primeros meses del año, especialmente en enero y febrero, se registró un volumen elevado de actividades atribuidas a campañas de *ransomware*, muchas de ellas vinculadas a actores ya conocidos.

En consecuencia, a partir de marzo y abril se ha observado un aumento en la detección de nuevos grupos, algunos de los cuales han surgido como escisiones de colectivos previamente desmantelados; una renovación constante del ecosistema criminal, donde la fragmentación y la reconfiguración de actores juegan un papel clave en la resiliencia del modelo de *ransomware* como servicio (RaaS) (DarkFeed, 2025).

Figura 8 | Grupos de *Ransomware* detectados en el primer semestre de 2025.

6.2.2 Grupos más activos

La actividad criminal en este ámbito ha seguido adaptándose a los cambios tecnológicos, las medidas defensivas y las oportunidades que ofrece el modelo RaaS. Esta dinámica ha dado lugar a un entorno altamente cambiante, donde la innovación técnica, la diversificación de objetivos y la descentralización operativa son elementos clave para entender las amenazas actuales.

A continuación, se presenta una gráfica que muestra los grupos de *Ransomware* más activos durante este periodo, ilustrando su distribución y evolución a lo largo de los primeros meses de 2025 (DarkFeed, 2025).

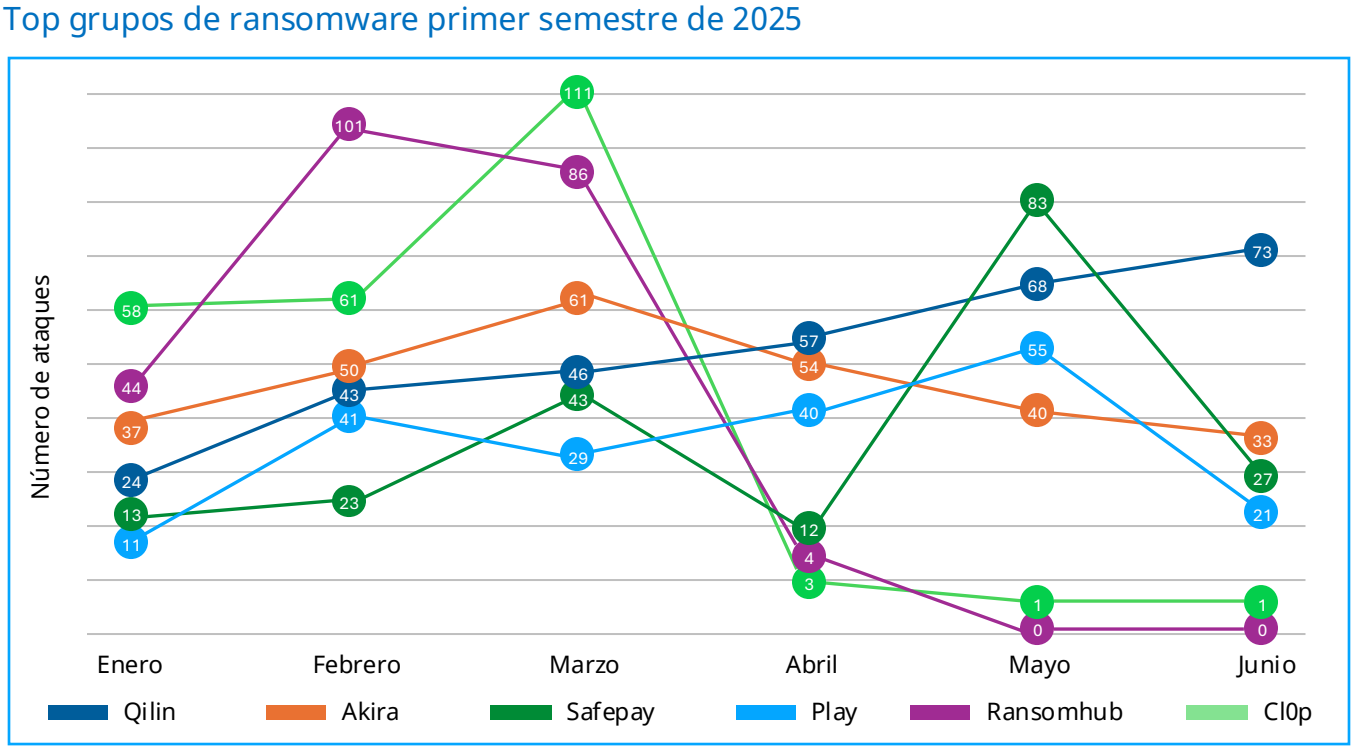


Figura 9 | Actividad de los grupos de *Ransomware* más activos en el primer semestre de 2025.

- ***RansomHub* y *Cl0p*:** Ambos con una distribución de los ataques muy similar, *Cl0p* recientemente entrado en la clasificación, con el mayor número de ataques de *ransomware* registrados en marzo (111); mientras que *RansomHub*, que se consolidó como uno de los grupos más activos de 2024, tuvo una caída drástica en su actividad en abril y desapareció por completo en mayo y junio.
- ***Qilin* y *Akira*:** Encabezando la lista con el mayor volumen de ataque. *Qilin* se ha posicionado como uno de los grupos dominantes de 2025, con un crecimiento acelerado atribuible en parte a la migración de afiliados desde *RansomHub*, y a su infraestructura técnica que le permite operar de forma eficiente, escalable y profesional. Por su parte, Akira, con una presencia constante y sofisticada, se consolida como un grupo persistente, con una infraestructura técnica madura.
- ***Play y Safepay:*** El grupo Play también se mantiene en el panorama de amenazas más activas durante este semestre, aunque no lidera en volumen de ataques ha seguido evolucionando hacia operaciones más dirigidas y técnicas, lo que sugiere una profesionalización de sus campañas. Mientras que Safepay, dirigiendo sus ataques a pymes y sectores menos protegidos aprovechando vulnerabilidades comunes, ha tenido un crecimiento gradual que le posiciona como grupo a observar en el segundo semestre de 2025, esperando que aumente su notoriedad a lo largo del año.

6.2.3 Afectación global

La actividad de los grupos de ransomware durante 2025 ha tenido un impacto global, afectando a organizaciones de todos los tamaños y sectores en múltiples regiones del mundo. Aunque la distribución geográfica de los ataques varía según el grupo y sus objetivos estratégicos, se observa una clara concentración en países con alta digitalización, predominando Estados Unidos, y sectores críticos como salud, educación, manufactura y servicios financieros.

En el análisis de los sectores más afectados por ataques de ransomware durante los últimos seis meses, que se presenta en este apartado, indica que el sector de manufactura continúa liderando como el principal objetivo de los ciberdelincuentes a nivel mundial.

Esta tendencia, que se ha mantenido constante en los últimos años, refleja una combinación de factores estructurales que hacen de este sector un objetivo especialmente atractivo. Su alta dependencia de sistemas operativos industriales, la conectividad creciente de entornos OT con redes IT, y la presión por mantener la continuidad de las cadenas de suministro globales, convierten a la manufactura en un entorno donde incluso una breve interrupción puede traducirse en pérdidas millonarias.

En 2025, los atacantes han perfeccionado sus técnicas, apuntando a sistemas SCADA, hipervisores y entornos de producción virtualizados, lo que ha elevado tanto la sofisticación como el impacto de los ataques. La siguiente gráfica ilustra los sectores más afectados por ransomware en la primera mitad de 2025, destacando la prominencia sostenida del sector de manufactura:

Ataques de Ransomware por sector en el primer semestre de 2025

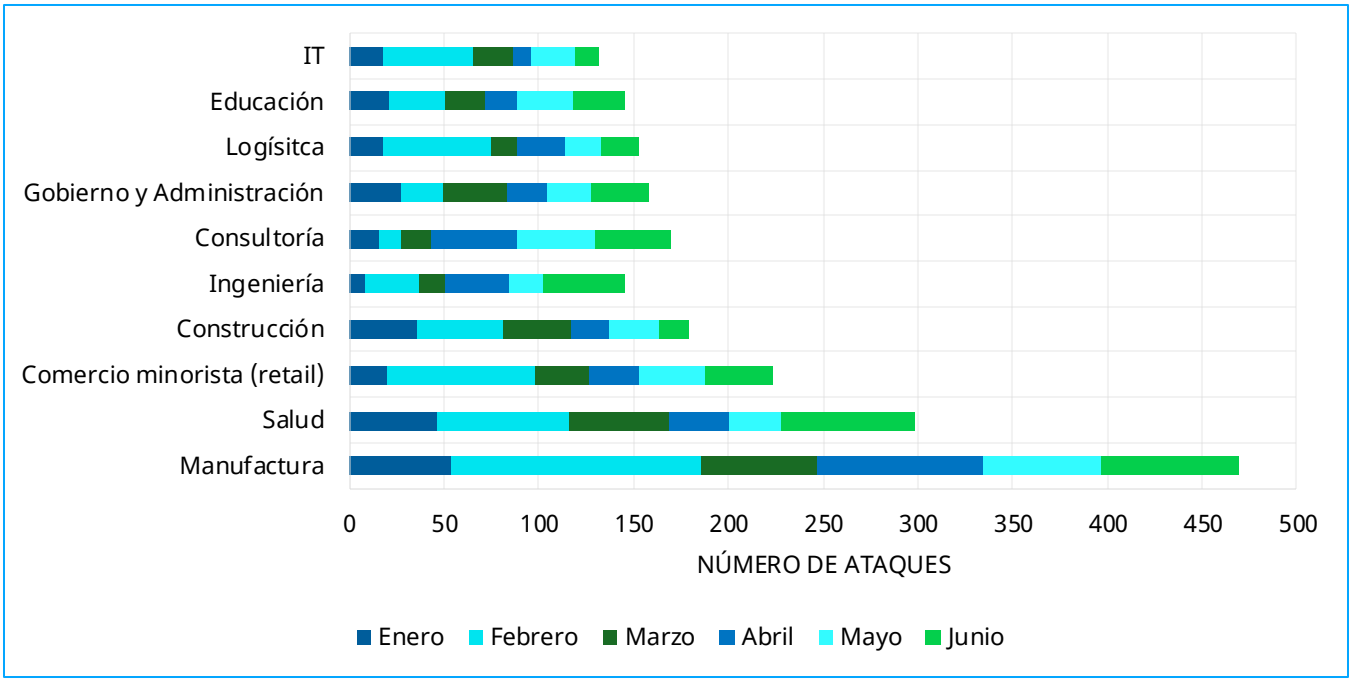


Figura 10 | Sectores más afectados por *Ransomware* en el primer semestre de 2025.

Por otro lado, se muestra la distribución geográfica de los países afectados por este tipo de ataque durante el mismo periodo:

Países más afectados por Ransomware de Enero a Junio 2025

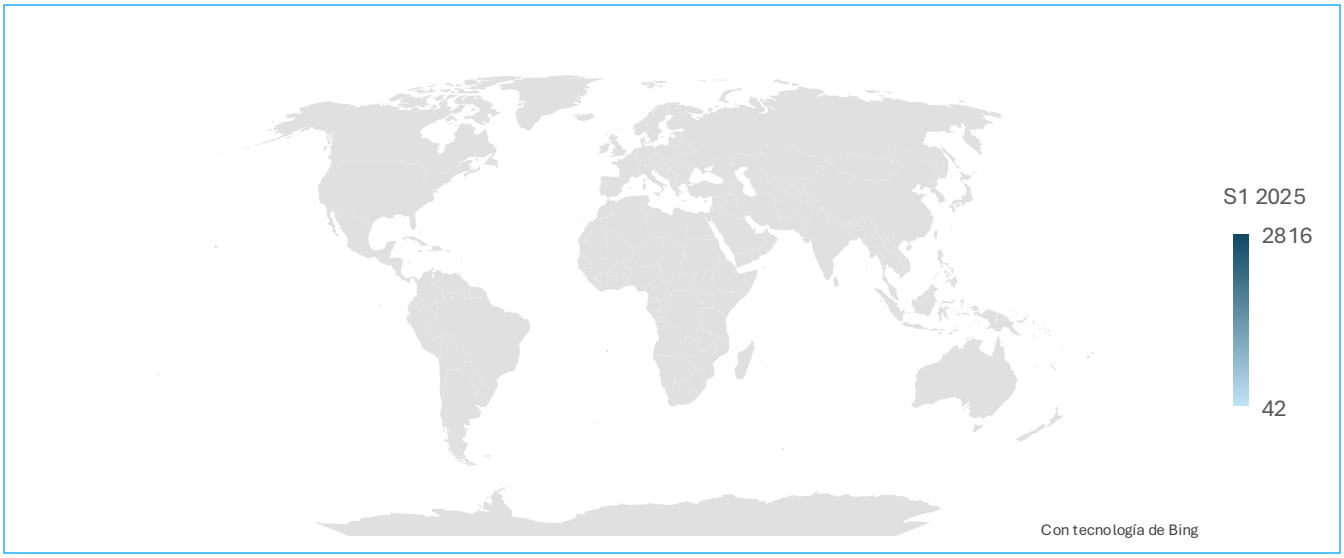


Figura 11 | Países más afectados por Ransomware en el primer semestre de 2025.

Como adelantábamos en este apartado, **Estados Unidos** encabeza la lista como el país más atacado, especialmente en infraestructuras críticas, sistemas financieros y redes gubernamentales. Le siguen países como **India** con gran exposición geopolítica, o países como **Reino Unido** y **Alemania**, donde la alta digitalización de sectores industriales y financieros ha incrementado su vulnerabilidad.

Por otra parte, los **crecientes ataques a Sudamérica** podrían estar reflejando una tendencia de expansión hacia economías emergentes, donde los niveles de digitalización aumentan más rápido que las capacidades de ciberdefensa. En este contexto, Brasil se posiciona como el países más afectados de la región, concentrando una parte significativa de los ataques, particularmente sobre sectores clave como la educación, salud, logística e incluso servicios digitales.

De forma paralela, en Centroamérica, México presenta actividad destacada por parte de grupos como Cl0p, LockBit y Akira, cuyas operaciones, motivadas principalmente por el beneficio económico, han impactado sectores como el financiero, la administración pública y la manufactura, situando a México como un nuevo objetivo prioritario para campañas de ransomware más sofisticadas y persistentes que en el resto de la región.

Esta distribución geográfica evidencia una tendencia clara: los actores de ransomware están priorizando países con alta dependencia tecnológica, infraestructuras críticas interconectadas y, en muchos casos, con brechas en sus capacidades de respuesta y resiliencia cibernética.

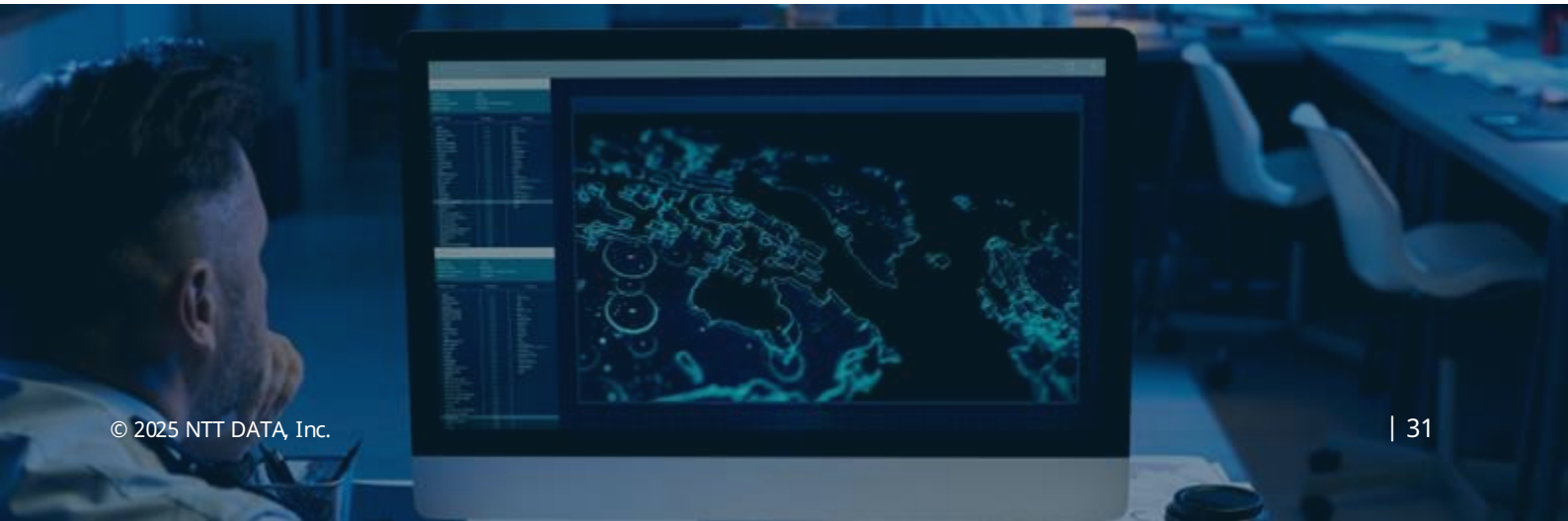
6.3 Hacktivistas

En 2025, el hacktivismo ha experimentado un notable resurgimiento, impulsado tanto por conflictos geopolíticos como por causas sociales globales. Este fenómeno ha evolucionado más allá de las acciones individuales o de pequeños colectivos, dando lugar a alianzas transnacionales de grupos hacktivistas que operan con una coordinación sin precedentes. En muchos casos, estos grupos reciben apoyo tácito o encubierto por parte de ciertos estados, que ven en ellos una herramienta útil para ejercer presión política sin recurrir a enfrentamientos militares directos.

Actualmente, el panorama hacktivista global se ha intensificado con la formación de alianzas entre grupos que operan en conflictos geopolíticos. **AnonSec,** tradicionalmente vinculado a campañas de filtración de datos, ha coordinado ataques descentralizados a infraestructuras críticas y campañas de desinformación, consolidando una red de colaboración con grupos pro-palestinos como **Mr. Hamza, Ghosts of Gaza, Handala Hack, Sylhet Gang-SG o Moses Staff,** todos con una fuerte orientación antioccidental, especialmente contra Estados Unidos, Israel y, recientemente, India, quien opera con su grupo nacionalista **Indian Cyber Force** contra países como Pakistán y China.

Por otro lado, **DieNet y DragonForce Malaysia** también han intensificado sus operaciones contra intereses estadounidenses, alineándose con causas islámicas y antiimperialistas. En el frente prorruso, **NoName057(16)** ha sido el grupo más activo, liderando campañas DDoS contra Ucrania y sus aliados, en colaboración con **Killnet y Anonymous Sudan,** atacando sitios gubernamentales, financieros y de transporte en Europa.

La creciente cooperación entre estos grupos refleja una tendencia hacia la profesionalización del hacktivismo, con estructuras más organizadas y objetivos estratégicos definidos.



Alianzas entre grupos hacktivistas

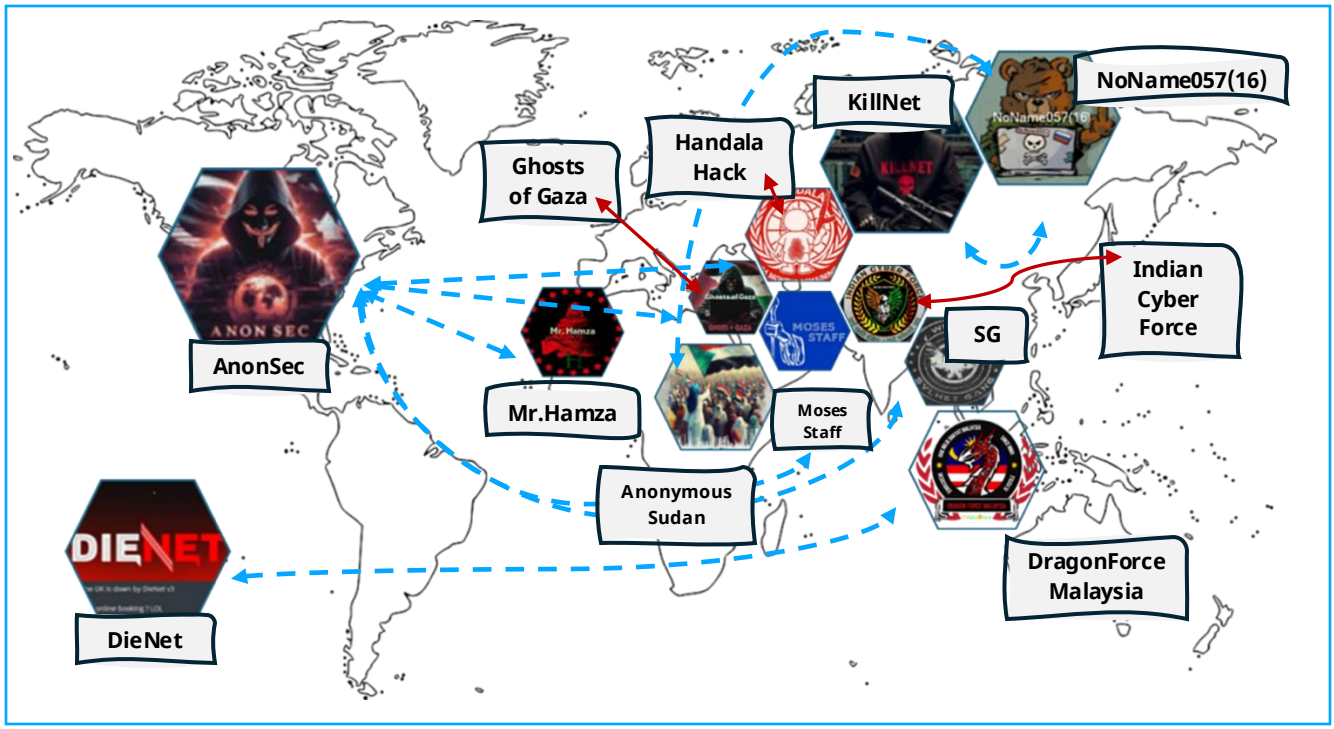
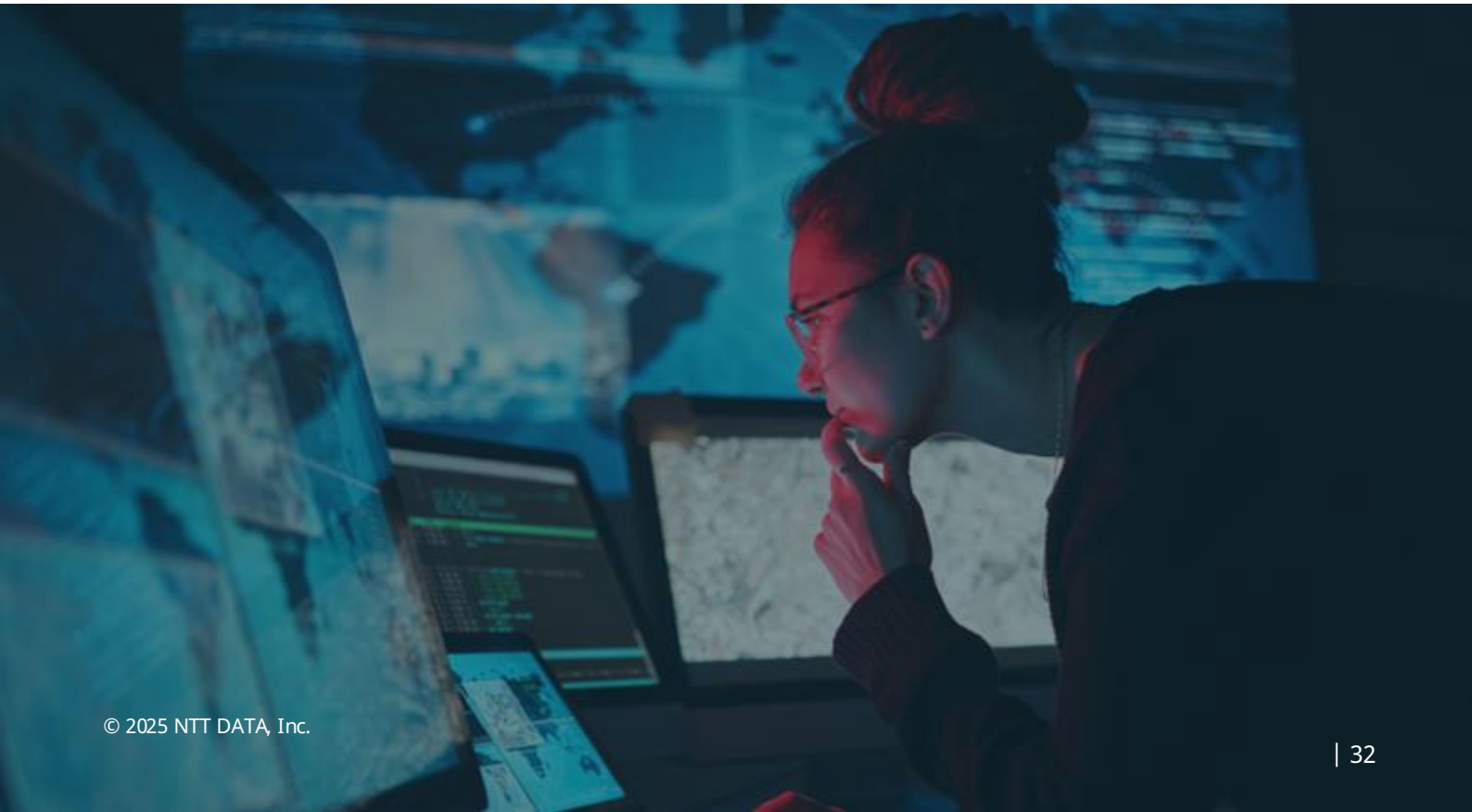


Figura 12 | Alianzas entre grupos hacktivistas por principales conflictos geopolíticos.

Inicialmente, el *hacktivismo* se limitaba a manifestaciones simbólicas o protestas digitales de bajo impacto. Sin embargo, en la actualidad ha evolucionado hacia una **herramienta estratégica en el ámbito geopolítico**, con operaciones meticulosamente orquestadas y objetivos que responden a intereses estatales o ideológicos. Esta evolución complica el panorama de la ciberseguridad global, al desdibujar las fronteras entre el activismo digital, las operaciones de inteligencia y los conflictos cibernéticos de carácter estatal.



6.4 APT

Durante el primer semestre de 2025, las APT globales han intensificado sus actividades sofisticando sus campañas tanto en técnica como en persistencia. A continuación, se detallan las tendencias clave observadas por región y actor estatal:

- **Las APT rusas,** como adelantábamos al inicio de este informe, han mantenido una estrategia agresiva centrada en 3 frentes: ciberespionaje diplomático, interrupción de servicios críticos y desinformación.

  - Sandworm con el despliegue en Ucrania del nuevo wiper "ZEROLOT", con el objetivo de interrumpir operaciones de operadores energéticos, distribuyéndose mediante políticas de grupo en Active Directory y herramientas RMM.

  - Otros como ***Sednit*** **(APT28)** que amplió su ya conocida ***Operación RoundPress*** (dirigida originalmente a *Roundcube*) para afectar también plataformas de correo como *Horde*, *Zimbra* y *MDaemon*, explotando vulnerabilidades XSS y *zero-day*. Una de las más relevantes fue **CVE-2024-11182**, aprovechada contra entidades ucranianas. Además, se identificó la explotación de fallos de día cero como **CVE-2024-9680** en *Mozilla Firefox* **y CVE-2024-49039** en *Microsoft Windows*, reforzando su perfil técnico ofensivo.

  - *Gamaredon*, con foco exclusivo en Ucrania, mantuvo una alta cadencia de ataques, actualizando constantemente sus implantes y técnicas de ofuscación. Introdujo PteroBox, un ladrón de archivos que abusa del servicio Dropbox como canal de exfiltración no convencional.

  - Por otro lado, grupos *hacktivistas* prorrusos como ***NoName057(16), Cyber Army of Russia Reborn*** y ***Solntsepyok*** continuaron con campañas DDoS y filtración de datos contra medios y gobiernos europeos. En algunos casos se identificó una convergencia operativa con campañas APT, reutilizando vulnerabilidades como las mencionadas anteriormente para acceso inicial, lo que refleja una creciente profesionalización en el ecosistema *hacktivista*.

- En **China las APT** han intensificado su enfoque hacia infraestructura crítica y redes gubernamentales, especialmente en Europa y Asia. Se detecta una consolidación del *tooling* compartido entre grupos estatales y su integración con nuevas puertas traseras y técnicas evasivas.

  - APT41 y ***Earth Baku*** mantuvieron campañas dirigidas a infraestructuras OT y dispositivos de red, empleando *ShadowPad* y nuevas variantes como "*VELVETSHELL*".

  - *DigitalRecyclers* utilizó el *backdoor HydroRShell* junto a *tunneling* con KMA VPN para comprometer entidades europeas.

  - *PerplexGoblin* lanzó "*NanoSlate*", un *malware* avanzado en C++, empleado contra instituciones gubernamentales centroeuropeas.

  - Estas APT destacaron por el uso coordinado de *exploits* contra *routers*, conmutadores *Cisco Nexus* y *proxies* empresariales para establecer persistencia invisible.

- Las **APT iraníes** han mostrado una dualidad clara entre ciberespionaje y campañas contra Israel.

  - *MuddyWater* y ***Lyceum*** emplearon *software* legítimo de administración remota para acceso inicial en campañas de *spear phishing* dirigidas a manufacturas e infraestructura en Israel.

  - En una acción coordinada, se observó a ***BledEdFeline*** colaborando con *MuddyWater* compartiendo artefactos de persistencia.

  - *CyberToufan*, actor emergente vinculado a actividades *hacktivistas*, combinó filtraciones de datos, borrado de sistemas y manipulación mediática.

- Finalmente, las **APT norcoreanas** continúan centradas en espionaje diplomático y robo masivo de criptomonedas para financiar al régimen.

  - *DeceptiveDevelopment* expandió su uso de *job lures* y plataformas como *WeaselStore*, logrando infecciones dirigidas a desarrolladores de *blockchain* y profesionales de IT.

  - El grupo ***TraderTraitor*** fue vinculado al ataque a la *wallet Safe{Wallet}*, comprometiendo su cadena de suministro y resultando en el robo de más de 1.500 millones de dólares en activos digitales.

  - Se ha registrado el retorno de ***Kimsuky*** y ***Andariel***, con campañas contra objetivos surcoreanos y diplomáticos de Asia-Pacífico.

Desde el **Departamento de Cyber Threat Intelligence de NTT DATA**, se ha elaborado una estimación basada en informes públicos y el análisis de fuentes de inteligencia abiertas, para clasificar las campañas APT del semestre según su motivación predominante.

Actividad APT clasificada por motivación en cada región en el primer semestre de 2025

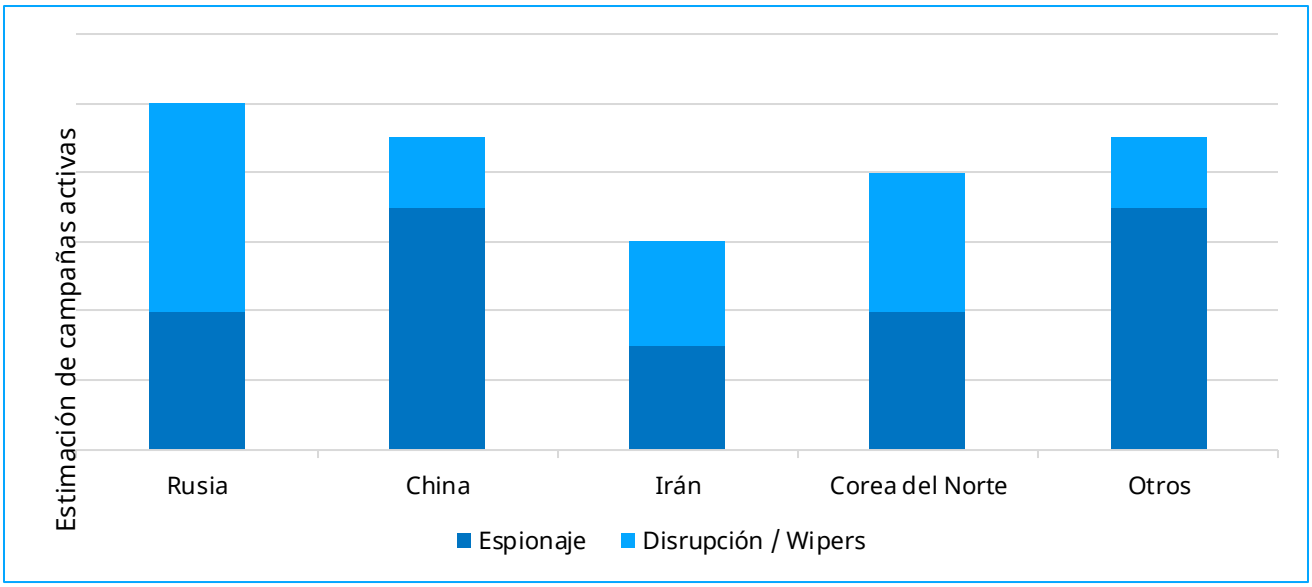


Figura 13 | Actividad de grupos APT en cada región clasificada por su motivación durante el primer semestre de 2025.

El análisis refleja una tendencia destructiva más acentuada en actores como Rusia e Irán, frente a enfoques más centrado en el espionaje por parte de China, Corea del Norte y grupos del sur de Asia. Esta segmentación permite identificar patrones operativos diferenciados por región y anticipar posibles líneas de evolución táctica en función del contexto geopolítico.

Tácticas, Técnicas y Procedimientos (TTPs)

7. Tácticas, Técnicas y Procedimientos

Las Tácticas, Técnicas y Procedimientos (TTPs) constituyen un enfoque fundamental para comprender las estrategias empleadas por actores maliciosos en el panorama cibernético. Identificar estos patrones no solo permite fortalecer la postura defensiva de las organizaciones, sino también anticipar y mitigar posibles riesgos de manera proactiva.

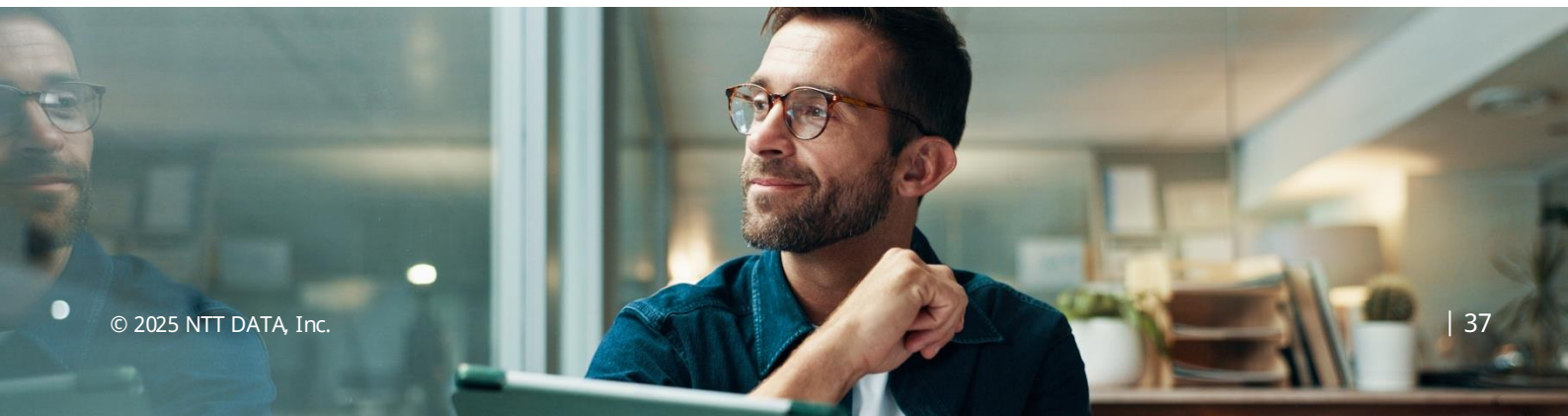
7.1 Descripción de las TTP más comunes utilizadas por los cibercriminales

Durante el primer semestre de 2025, el *phishing* fue la principal técnica de acceso inicial, con actores que utilizaron *vishing*, enlaces y archivos adjuntos maliciosos y ataques BEC (*Business Email Compromise*). Asimismo, se ha observado que los actores maliciosos utilizaron una mayor variedad de herramientas de acceso remoto comerciales y de código abierto, como ***SplashTop***, **Atera**, ***TeamViewer***, ***AnyDesk***, ***LogMeIn***, ***ScreenConnect***, ***QuickAssist***, ***TightVNC*** y la plataforma **RMM de Level**.

La siguiente tabla representa las técnicas de MITRE ATT&CK más observadas en el primer semestre de 2025:

Táctica	MITRE ATT&CK ID	Descripción
Reconocimiento (TA0043)	T1590 – Recopilar información de la red de víctimas	Los adversarios pueden recopilar información sobre las redes de la víctima que puede utilizarse para atacar. Esta información puede incluir diversos detalles, como datos administrativos, así como detalles sobre su topología y operaciones.
	T1595.002 – Escaneo Activo: Escaneo de Vulnerabilidades	Los atacantes pueden ejecutar escaneos de vulnerabilidades en la infraestructura pública de una organización para identificar posibles vulnerabilidades que puedan explotarse.
Acceso inicial (TA0001)	T1598.004 – Phishing de información: Spearphishing de Voz	En una campaña observada, los usuarios recibieron llamadas del adversario haciéndose pasar por soporte de TI y se les solicitó iniciar una sesión de QuickAssist.
	T1598.003 – Phishing para obtener información: Enlace de phishing selectivo	Los atacantes pueden enviar mensajes de phishing selectivo con un enlace malicioso para obtener información confidencial que pueda utilizarse durante el ataque.
	T1598 – Phishing de información: Archivo adjunto de phishing selectivo	Los atacantes pueden enviar mensajes de phishing selectivo con un archivo adjunto malicioso para obtener información confidencial que pueda utilizarse en ataques dirigidos.
	Explotación T1190 en una aplicación pública	Los atacantes pueden explotar una vulnerabilidad para acceder al sistema objetivo.
	T1078 – Cuentas Válidas	Los atacantes podrían usar credenciales comprometidas para acceder a cuentas válidas durante su ataque.
Ejecución (TA0002)	T1059.001 – Intérprete de comandos y scripts: PowerShell	Los atacantes pueden abusar de PowerShell para ejecutar comandos o scripts durante su ataque.
	T1047 – Instrumental de administración de Windows	Los atacantes pueden usar el Instrumental de Administración de Windows (WMI) para ejecutar comandos maliciosos durante el ataque.
	T1053 – Tarea/Trabajo programado	Los atacantes pueden abusar de la programación de tareas para facilitar la ejecución inicial o recurrente de código malicioso.

Táctica	MITRE ATT&CK ID	Descripción
Persistencia (TA0003)	T1098 – Manipulación de Cuentas	Los atacantes pueden manipular cuentas para mantener o aumentar el acceso a los sistemas de las víctimas.
	T1136.001 – Crear Cuenta: Cuenta Local	Los atacantes pueden crear una cuenta local para mantener el acceso a los sistemas de las víctimas.
	T1547.001 – Persistencia: Ejecución de inicio automático al iniciar sesión o arrancar: Claves de ejecución del Registro/Carpeta de Inicio	Los atacantes establecieron la persistencia mediante la incrustación de direcciones IP en la clave de registro de TitanPlus.
	T1133 – Servicios Remotos Externos	Los atacantes pueden aprovechar servicios remotos externos para acceder inicialmente o persistir en una red.
	T1546.008 – Ejecución Activada por Eventos: Funciones de Accesibilidad	Los atacantes pueden establecer la persistencia o aumentar los privilegios mediante la ejecución de contenido malicioso activado por funciones de accesibilidad.
Escalada de privilegios (TA0002)	T1134 – Manipulación de *tokens* de acceso	Los atacantes pueden modificar los *tokens* de acceso para que operen bajo un contexto de seguridad de usuario o sistema diferente, realizando acciones y evadiendo los controles de acceso.
Evasión de defensas (TA0005)	T1562.001 – Debilitar Defensas: Deshabilitar o Modificar Herramientas	Los atacantes pueden deshabilitar o desinstalar herramientas de seguridad para evitar ser detectados.
	T1562.004 – Debilitar Defensas: Deshabilitar o Modificar el *Firewall* del Sistema	Los atacantes pueden deshabilitar o modificar los *firewalls* del sistema para eludir los controles que limitan el uso de la red.
	T1564.008 – Ocultar Artefactos: Reglas de Ocultación de Correo Electrónico	Los atacantes pueden usar reglas de correo electrónico para ocultar correos electrónicos entrantes o salientes en el buzón de un usuario comprometido.
	T1070.001 – Eliminación de Indicadores: Borrar Registros de Eventos de Windows	Los atacantes pueden borrar los registros de eventos de Windows para ocultar sus rastros y dificultar el análisis forense.
	T1112 – Modificar el Registro	El atacante utilizó algunas modificaciones del registro para obtener una escalada de privilegios.
Acceso a Credenciales (TA0006)	T1003 – Volcado de Credenciales del SO	Los atacantes pueden volcar credenciales de diversas fuentes para facilitar el acceso lateral.
	T1528 – Robo de *Token* de Acceso a Aplicaciones	Los atacantes pueden robar *tokens* de acceso a aplicaciones para obtener credenciales y acceder a sistemas y recursos remotos.
Descubrimiento (TA0007)	T1046 – Descubrimiento de servicios de red	Los atacantes pueden usar herramientas como el escáner de puertos avanzado para escanear la red.
	T1057 – Descubrimiento de Procesos	Los adversarios pueden intentar obtener información sobre los procesos en ejecución en un sistema.
	T1018 – Descubrimiento de sistemas remotos	Los atacantes pueden intentar descubrir información sobre sistemas remotos con comandos como "*net view*".
	T1082 – Descubrimiento de información del sistema	Un atacante podría intentar obtener información detallada sobre el sistema operativo y el *hardware*.
	T1016 – Descubrimiento de la configuración de red del sistema	Los atacantes pueden usar comandos como "*ifconfig*" y "*net use*" para identificar conexiones de red.
	T1087.001 – Descubrimiento de cuentas: Cuenta local	Enumerar las cuentas de usuario en el sistema.



Táctica	MITRE ATT&CK ID	Descripción
Movimiento Lateral (TA0008)	T1021.001 – Servicios Remotos: Protocolo de Escritorio Remoto	Los adversarios pueden abusar de cuentas válidas mediante RDP para moverse lateralmente en un entorno objetivo.
	T1021.006 – Servicios Remotos: Administración Remota de Windows	Los adversarios pueden usar Cuentas Válidas para interactuar con sistemas remotos mediante Administración Remota de Windows (WinRM).
Comando y Control (TA0011)	T1219 – *Software* de Acceso Remoto	Un adversario puede usar *software* legítimo de soporte de escritorio y acceso remoto para establecer un canal interactivo de comando y control hacia sistemas objetivo dentro de las redes.
	T1105 – Transferencia de herramientas de entrada	Los atacantes pueden transferir herramientas desde un sistema externo a un sistema comprometido.
	T1572 – Tunelización de protocolos	Los atacantes pueden tunelizar las comunicaciones de red hacia y desde un sistema víctima mediante un protocolo independiente, como SMB, para evitar la detección o permitir el acceso.
Exfiltración (TA0010)	T1048 – Exfiltración mediante un protocolo alternativo	Los atacantes pueden robar datos exfiltrándolos mediante un protocolo diferente al del canal de comando y control existente, como WinSCP.
Impacto (TA0040)	T1486 – Datos cifrados para impacto.	Los atacantes pueden usar *ransomware* para cifrar datos en un sistema objetivo
	T1490 – Inhibir la recuperación del sistema	Los atacantes pueden deshabilitar funciones de recuperación del sistema, como las instantáneas de volumen.
	T1489 – Detención del servicio	Los atacantes pueden detener o deshabilitar servicios en un sistema para que no estén disponibles para usuarios legítimos.

Tabla 4 | TTP más comunes durante el primer semestre de 2025.

Basándonos en la evolución de estas TTPs y las tendencias actuales, **para el segundo semestre de 2025, se espera:** un aumento del **abuso de herramientas legítimas**, mayor **sofisticación en técnicas de evasión**, incremento en el uso de ***scritps* automatizados y basados en IA** y, **mayor persistencia** en entornos híbridos, donde hay más puntos de entrada expuestos.

La relación con el marco MITRE ATT&CK no solo permite comprender estas amenazas, sino que también proporciona un enfoque práctico para mitigarlas.

7.2 Vectores de entrada más usuales

En este contexto, y considerando que el *ransomware* continúa siendo una de las amenazas más persistentes y rentables, las tendencias actuales en vectores de entrada se pueden resumir de la siguiente manera (Check Point Research, 2025):

Edge devices	***Infostealers***	**Entornos *cloud***
El incremento en el uso de dispositivos IoT, *wereables* y *hardware* para trabajar a distancia facilita la entrada de nuevos ataques por ser objetivos menos protegidos y más fáciles de monitorear.	Este tipo de *malware* para robar información confidencial está a la orden del día, situándose como una de las amenazas más activas. Su **facilidad de acceso** por el auge del **MaaS** y su **creativa distribución**, ha incrementado su uso en fase inicial para ataques posteriores de *ransomware* o APTs. (*Lumma Stealer* – *PupkinStealer* *FormBook*)	La adopción de soluciones basadas en infraestructuras de **nube híbrida y multinube** es cada vez más frecuente y enfrenta retos como la **gestión de configuraciones** y la **seguridad de las API** que posiciona estos entornos como un vector de entrada de fácil acceso.
Business email compromise	**Denegación de servicio**	***Man-in-the-middle* (MitM)**
Aumento de ataques BEC perfeccionados con IA generativa. Con motivaciones económicas es una de las amenazas emergentes que más daño financiero inflige. Tácticas en constante evolución y mayor focalización en sectores críticos. (Cartier, 2025)	Patrones de **ataque automatizados y adaptados** en tiempo real para evasión de defensas. Coordinación de ***botnets* IoT** más eficiente. Uso de ataques DoS/DDoS como **táctica de distracción** para cubrir otros ataques. Aumento de ataques a **infraestructuras críticas**. Mayor accesibilidad por emersión del **DDoS-as-a-Service**. (*Cloudflare* – *X*)	**Explotación de vulnerabilidades en redes de nueva generación**, interceptando el tráfico cifrado en redes 5G y WiFi 6E. Aumento de ataques a **sistemas SCADA y dispositivos IoT industriales.** Incremento em ataques MitM a través de **aplicaciones móviles.** Sofisticación de técnicas y combinación con otros ataques al vincularse con campañas **APT**.

Tabla 5 | Vectores de entrada más usuales empleados en el primer semestre de 2025.

En definitiva, aunque surgen constantemente nuevas técnicas de intrusión, los vectores de entrada más tradicionales siguen demostrando una eficacia preocupante. El ***phishing*** continúa siendo el método más utilizado para engañar a los usuarios y obtener acceso inicial, mientras que los **ataques remotos**, el uso de **credenciales comprometidas** y la **explotación de vulnerabilidades**, incluidas las de tipo *zero-day*, mantienen su protagonismo como puertas de entrada clave, adaptándose y perfeccionándose continuamente.

7.3 Innovación en ataques : Nuevas técnicas y tácticas

A continuación se describen algunas de las técnicas más disruptivas observadas analizando sus mecanismos, campañas asociadas, y el motivo por el que representan una novedad frente a tácticas anteriores.

Instaladores de herramientas de IA como vector de distribución de *malware*

Esta técnica se basa en camuflar *malware* dentro de instaladores falsos de herramientas de IA. Los ejecutables maliciosos simulan estos *software* populares, incluyendo asistentes de productividad y generadores de texto o imagen, explotando así el crecimiento de la IA generativa.

- Ha sido observada en campañas reales distribuyendo *ransomware* (*CyberLock*), *malware* de control remoto (*Lucky_Gh0st*) y la **nueva amenaza identificada como *Numero***
(Cisco Talos Intelligence, 2025).
- Lo innovador de esta táctica radica en su aprovechamiento del interés masivo por la IA, combinando ingeniería social con técnicas de empaquetado avanzado.
- A diferencia de campañas previas basadas en archivos adjuntos o *scripts*, estas muestras incluyen interfaces falsas de instalación para legitimar la descarga.

Bypass* de MFA mediante *proxies* inversos y manipulación *OAuth

Esta técnica permite a los atacantes interceptar *tokens* de autenticación y tomar control de sesiones protegidas por MFA. Se basa en la creación de sitios falsos que replican el flujo de *login* real, redirigiendo el tráfico a través de *proxies* inversos como *Evilginx2* (Google Cloud, 2025)

- Utilizado en campañas reales por el grupo APT *ColdRiver*, dirigido contra ONGs, periodistas y entidades gubernamentales occidentales.
- Lo que hace a esta táctica especialmente peligrosa es su capacidad de **suplantar completamente el flujo de autenticación sin necesidad de *malware* local**, y su capacidad de extraer tanto credenciales como *tokens* válidos en tiempo real.
- Frente a ataques anteriores que requerían infecciones en el *endpoint*, esta técnica es 100% remota, más difícil de rastrear, y altamente efectiva en contextos con MFA.

Extensiones de navegador con funcionalidad doble: útil y maliciosa

Las extensiones afectadas proporcionan funciones legítimas (como edición de documentos o análisis web) mientras realizan actividades encubiertas como exfiltración de *cookies*, *keylogging* o conexión a comandos remotos.

- *DomainTools* identificó más de 30 extensiones en la Chrome Web Store activamente utilizadas en campañas reales (DomainTools, 2025)
- Esta técnica es innovadora por el uso de herramientas útiles como caballo de Troya, generando confianza real en el usuario. Además, al distribuirse desde tiendas oficiales, supera controles de seguridad comunes.
- Frente a extensiones clásicamente maliciosas, estas funcionan perfectamente, lo que prolonga su ciclo de vida y reduce el índice de desinstalación.

"Crime-as-a-Service"

- Plataformas clandestinas han comenzado a ofrecer *hacking* a demanda y *bomber services* (SOCRadar, 2025) que permiten realizar campañas de DDoS, *flooding* de SMS o *spam* masivo con solo registrarse, con *dashboards* tipo SaaS, soporte técnico y segmentación por país.
- Detectado en mercados de habla rusa en mayo, se destacan por su facilidad de uso y despliegue inmediato, incluyendo incluso tutoriales para atacantes sin experiencia (SOCRadar, 2025).
- La novedad está en el nivel de madurez operativa: estos servicios permiten a actores de bajo nivel realizar operaciones antes reservadas a APTs o grupos con infraestructura.
- Frente a foros como *Genesis Market*, esta nueva generación de plataformas ofrece automatización total, sin necesidad de contacto directo entre partes.

Chaos RAT

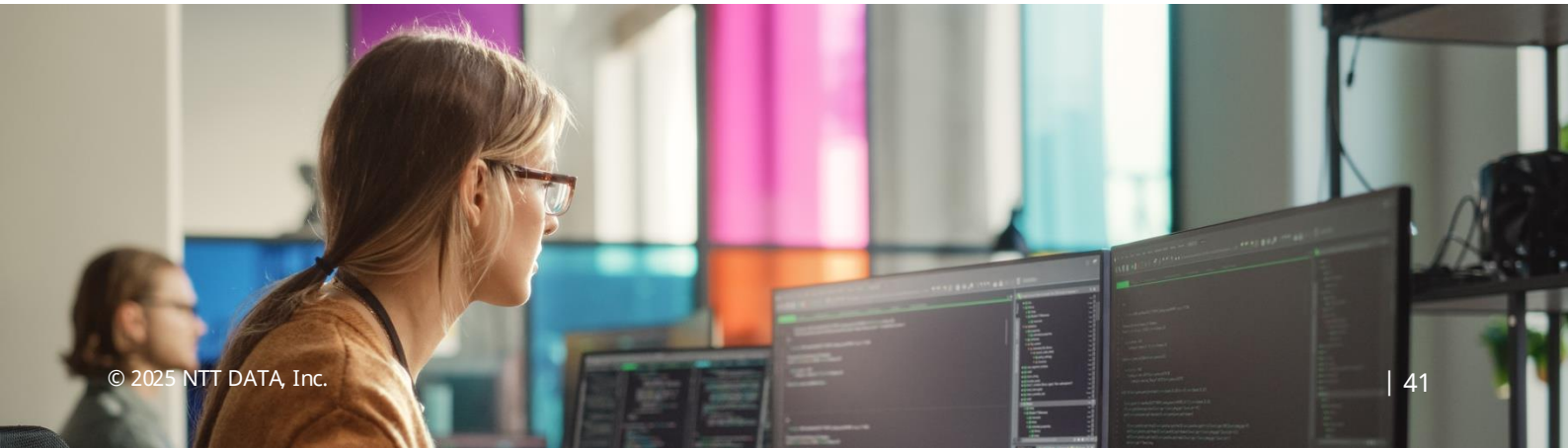
Esta nueva versión del troyano *Chaos RAT* presenta una arquitectura modular, cifrado personalizado en canal C2, instalación sigilosa y persistencia en entornos Windows, Linux e incluso dispositivos IoT (Acronis, 2025).

- Observado en mayo en campañas aún no atribuidas, su diseño le permite operar como plataforma ofensiva completa, con despliegue de *payloads* a demanda y ejecución remota de comandos en redes comprometidas.
- Destaca por su capacidad de operar sin detección durante semanas, y su resistencia a técnicas comunes de contención como listas blancas de procesos.
- Frente a *RATs* tradicionales como *njRAT* o *Quasar*, *Chaos* se comporta como un *framework ofensivo*, con control total del entorno objetivo.

Además de todas las técnicas descritas en este apartado, desde el **Departamento de Cyber Threat Intelligence** hemos observado una tendencia emergente en el uso de *malware* multicomponente, una táctica que, si bien no es nueva, está **ganando presencia en campañas recientes**. Este tipo de *malware* se caracteriza por estar dividido en múltiples fragmentos, entregados secuencialmente a través de canales de mensajería cifrados. Cada fragmento es inofensivo por separado, pero al ensamblarse en el equipo destino, forman la carga maliciosa completa.

Su resurgimiento apunta al uso de canales de distribución alternativos, incluyendo servicios de mensajería cifrada como Telegram o Signal. El principal riesgo reside en su capacidad de evasión y persistencia encubierta, lo que exige una mejora en los sistemas de detección basada en comportamiento y análisis contextual.

Esta evolución técnica refuerza la necesidad de adaptar continuamente las capacidades defensivas a TTPs cada vez más segmentadas, modulares y difíciles de correlacionar en tiempo real.



Vulnerabilidades

8. Vulnerabilidades

El primer semestre de 2025 ha confirmado la continuidad de una amenaza persistente y sofisticada en torno a las vulnerabilidades críticas, que siguen siendo una de las principales puertas de entrada para ciberataques a escala global. A lo largo de estos seis meses se ha observado una alta actividad en cuanto a identificación y explotación activa de fallos críticos, con una tendencia marcada hacia entornos empresariales, infraestructuras industriales y dispositivos móviles.

Entre enero y junio desde el **Departamento de Cyber Threat Intelligence de NTT DATA** se han monitorizado alrededor de 7.664 vulnerabilidades con CVE publicado, de las cuales 285 fueron clasificadas como críticas y al menos 105 fueron explotadas activamente *in the wild* . Esta cifra demuestra la agilidad de los atacantes para aprovechar fallos recientemente divulgados y la necesidad urgente de mejorar los tiempos de aplicación de parches y la supervisión continua.

A continuación se presenta un análisis mensual de las vulnerabilidades críticas **más destacadas del periodo**, según su impacto técnico, explotación en escenarios reales o su afectación a sectores críticos.

- **Enero:**

En enero de 2025, se identificaron **517 vulnerabilidades** , de las cuales **22 son de severidad crítica** y **20 fueron explotadas activamente**. Estas vulnerabilidades marcaron un inicio de año centrado en plataformas de red y entornos Linux, destacando por su facilidad de explotación y su integración en herramientas de ataque automatizadas.

Me basé en las totales de mes en GTIP, echade un ojo por si me pase ya que en el informe anterior las cifras eran bastante más pequeñas... así que àra la grafica he hecho comparativa de criticas vs explotacion y zero days.

Vulnerabilidades clave destacadas:

- **CVE-2024-12084 (rsync):** Heap overflow ampliamente explotable en entornos Linux.
- **CVE-2025-0060 / 0061 (SAP BusinessObjects):** RCE en plataformas BI corporativas.
- **CVE-2024-40891 / 40890 (Zyxel):** Inyecciones en dispositivos de red, utilizadas por botnets.

Impactos principales:

- Compromiso de infraestructuras de red.
- Robo de datos y acceso no autorizado a sistemas empresariales clave.
- El predominio de ataques automatizados y la velocidad de adopción en *kits* de explotación refuerzan la necesidad de segmentación de red y monitorización continua.

- **Febrero:**

En febrero de 2025, se identificaron **1.558 vulnerabilidades**, de las cuales **33 son de severidad crítica** y **16 fueron explotadas activamente**, marcando un aumento significativo en comparación con el mes anterior. Estas vulnerabilidades se dirigieron principalmente a infraestructuras de red y entornos *cloud-native*, reflejando un desplazamiento hacia objetivos más dinámicos y difíciles de proteger.

Vulnerabilidades clave destacadas:

- **CVE-2024-11218 (*containers* / *Red Hat*):** Escape de contenedor, explotado activamente.
- **CVE-2025-0890 (Zyxel):** Nuevo fallo en *router* ampliamente distribuido.
- **CVE-2025-21198 (Microsoft *Exchange*):** Fallo crítico en correo empresarial con *exploit* activo.
- **CVE-2024-45569 (Qualcomm):** Vulnerabilidad en *chipsets* Exynos, explotada en móviles.
- **Impactos principales:**
- Acceso remoto a sistemas corporativos, control de dispositivos IoT y fuga de información confidencial desde entornos de usuario final. La explotación activa de múltiples fallos en infraestructuras ampliamente desplegadas subraya el desafío de mantener una postura de seguridad consistente.

• Marzo:

En marzo de 2025, se identificaron **1.032 vulnerabilidades**, de las cuales **43 son de severidad crítica** y **24 fueron explotadas activamente**. El mes marcó un aumento en la explotación de fallos en productos de uso generalizado en empresas, incluidos sistemas de transferencia de archivos y herramientas de desarrollo *web*, con publicación de PoC casi inmediatas, aumentando el riesgo.

Vulnerabilidades clave destacadas:

- **CVE-2023-13124 (SAP NetWeaver Visual Composer):** Vulnerabilidad que permite la carga no autorizada de binarios maliciosos en entornos SAP a través del componente *Metadata Uploader*. Su explotación ha sido documentada en campañas dirigidas a entornos empresariales con alta dependencia de esta plataforma, comprometiendo integridad y disponibilidad.
- **CVE-2023-3161 (CrushFTP):** Bypass de autenticación en versiones <11.3.1, explotado activamente. Permite el acceso no autenticado a través de un fallo en la validación de HMAC, facilitando el control total del sistema. Ha sido vinculado a campañas de *ransomware* en entornos financieros y servicios gestionados.
- **CVE-2025-0603 (Aviatrix Controller):** Ejecución remota de comandos a través de la manipulación de parámetros API (*cloud_type*). La explotación activa de esta vulnerabilidad representa un riesgo elevado en entornos *multicloud* y plataformas híbridas utilizadas en operaciones críticas.

Impactos principales:

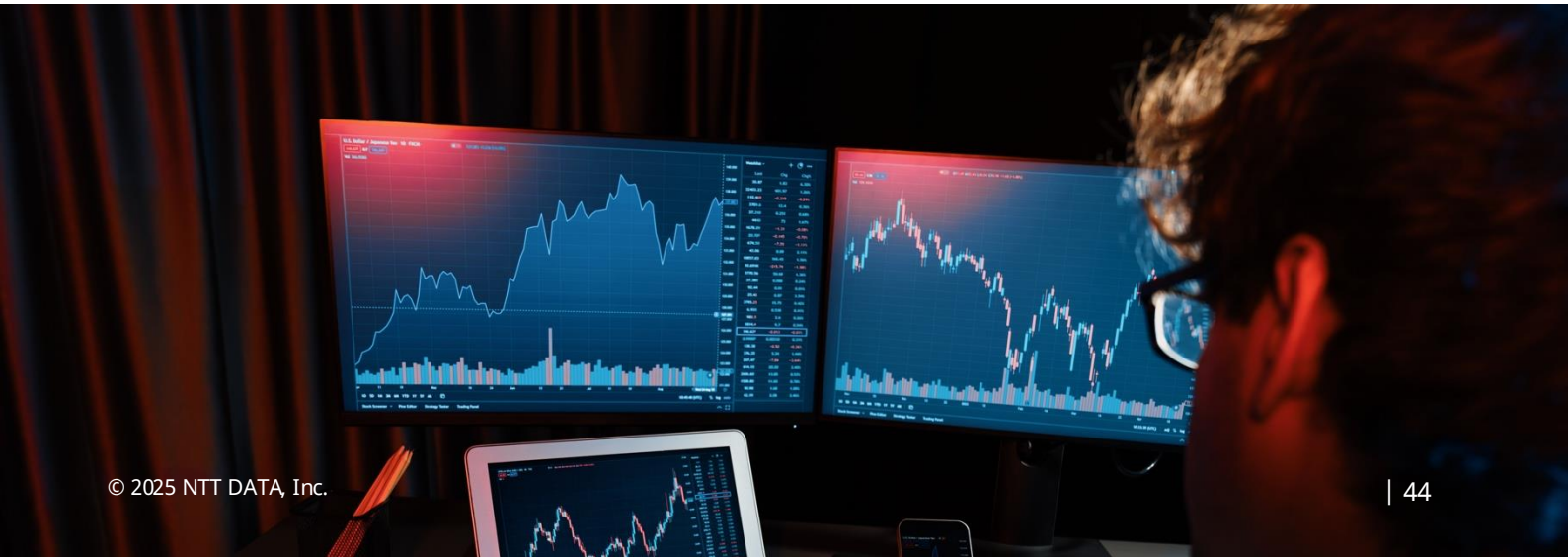
- Compromiso de servidores expuestos.
- Persistencia en sistemas y escalada de privilegios.

• Abril:

En abril se identificaron **1.381 vulnerabilidades**, **57 críticas y 13 con explotación activa**. Este mes destacó por la diversidad de productos afectados y por la explotación dirigida a dispositivos en el perímetro de la red y entornos de microservicios.

Vulnerabilidades clave destacadas:

- **CVE-2025-22457 (Ivanti EPMM):** Acceso remoto no autenticado en plataformas móviles.
- **CVE-2025-30215 (NATS.io):** RCE en *middleware* de microservicios.
- **CVE-2024-51138 / 51139 (DrayTek):** Vulnerabilidad en *routers* ampliamente utilizados.



- ## Mayo:

- En mayo de 2025, se identificaron **1.549 vulnerabilidades**, de las cuales **44 son de severidad crítica** y **17 fueron explotadas activamente.** Las vulnerabilidades destacadas estuvieron centradas en productos clave de seguridad y plataformas móviles, consolidando una tendencia hacia ataques altamente dirigidos y persistentes.

Vulnerabilidades clave destacadas:

- **CVE-2025-40595 (SonicWall):** *Exploit* activo contra *firewall* y dispositivos perimetrales.
- **CVE-2025-22252 (Fortinet):** RCE sin autenticación en soluciones ampliamente desplegadas.
- **CVE-2025-31219 (Apple):** *Zero-day* en sistemas Apple.
- **CVE-2025-0203 (Ivanti Connect Secure / Policy Secure):** Desbordamiento de búfer en *gateways* ZTA ampliamente utilizados, permite ejecución de código arbitrario sin autenticación. Su explotación está siendo vinculada a grupos de *ransomware* con objetivos en sectores gubernamentales y telecomunicaciones, debido al carácter crítico del acceso que proporciona.

Impactos principales:

- Acceso inicial.
- Persistencia en redes corporativas.
- Exposición de datos de usuarios móviles.

- ## Junio:

Se han identificado **1.426 vulnerabilidades, con 81 críticas y al menos 17 explotadas activamente**. Junio ha mostrado una actividad significativa en dispositivos VoIP, servidores Linux y dispositivos móviles, marcando una continuidad en la orientación de los ataques hacia entornos críticos y con alta superficie de exposición.

Vulnerabilidades clave destacadas:

- **CVE-2025-30507 (CyberData SIP):** RCE en dispositivos VoIP industriales.
- **CVE-2025-49087 (Red Hat / Perl-FCGI):** RCE en entornos *web* Linux.
- **CVE-2025-23107 (Samsung Exynos):** Explotada en ataques a dispositivos móviles.

Impactos principales:

- Amenazas a infraestructura crítica de voz, servidores *web* y ecosistemas Android/iOS. Se refuerza la necesidad de una visibilidad total sobre dispositivos conectados, donde la mayoría de usuarios desconocen la existencia de estas vulnerabilidades y los potenciales riesgos asociados.

Tendencias de vulnerabilidades y su explotación (S2 2024 - S1 2025)

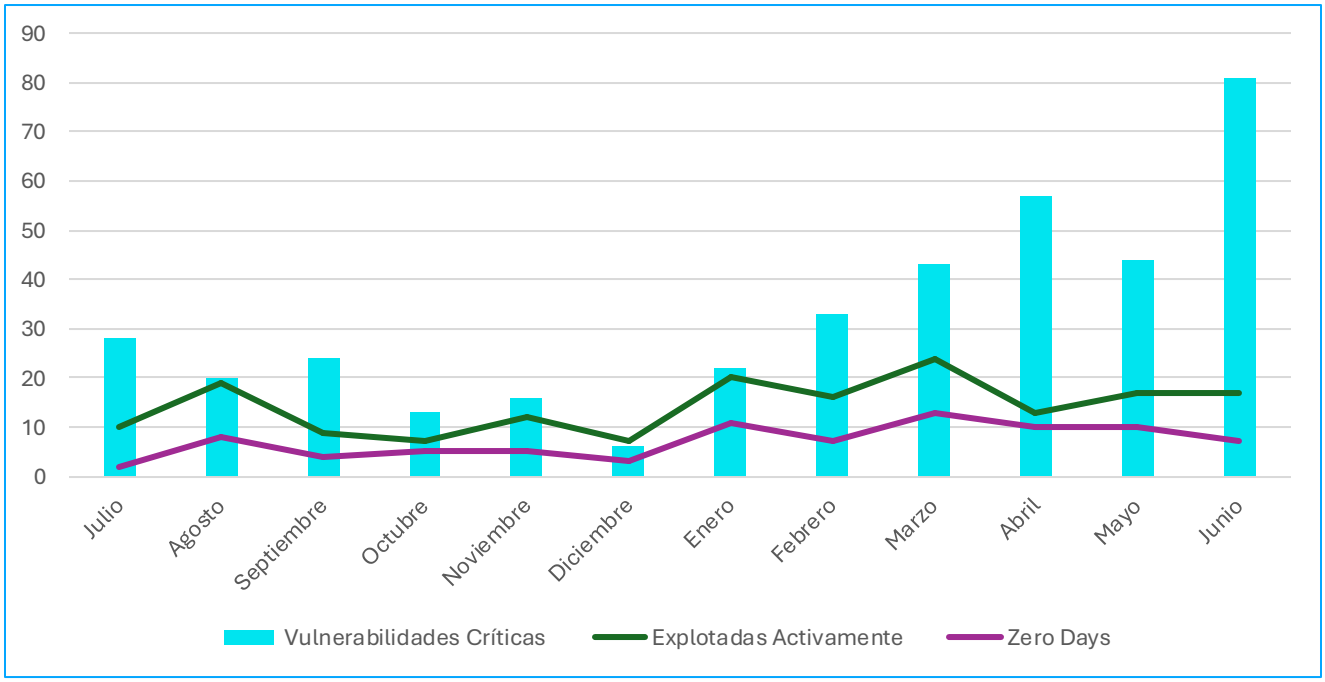


Figura 14 | Comparativa entre la explotación y presencia de vulnerabilidades críticas en el segundo semestre de 2024 con respecto al primer semestre de 2025.

Tendencias de explotación de estas vulnerabilidades:

- Durante el primer semestre de 2025, se ha consolidado una **estrategia por parte de los actores maliciosos** basada en la **explotación inmediata de vulnerabilidades críticas tras su divulgación**, especialmente aquellas con PoC públicos. A diferencia del segundo semestre de 2024, se ha observado un incremento considerable en la tasa de explotación activa frente al número total de fallos críticos publicados.

La preferencia operativa de los atacantes se ha centrado en:

- Sistemas expuestos de red y **dispositivos perimetrales** como *routers*, *firewalls* y soluciones de acceso remoto.
- **Entornos OT y dispositivos industriales**, donde los fallos tienen un impacto más disruptivo y crítico para operaciones continuas.
- **Infraestructura *cloud-native* y contenedores**, donde se aprovecha la complejidad de gestión para escalar privilegios y mantener persistencia.
- **Plataformas móviles y *chipsets*** populares, como los Exynos o Apple SoC, cada vez más dirigidos por su rol en la gestión de identidades y acceso a datos.

Además, se refuerza la hipótesis de una **mayor sofisticación en los grupos de *ransomware* y APT**, que alinean sus campañas con el calendario de divulgación de vulnerabilidades, reduciendo su tiempo de preparación técnica gracias a herramientas automatizadas de explotación.

Este cambio táctico evidencia una necesidad crítica de acortar el tiempo medio de parcheo, desplegar medidas de mitigación rápida (como listas de control de acceso o segmentación de red) y reforzar la inteligencia proactiva sobre amenazas, especialmente en sectores industriales, telecomunicaciones y servicios críticos.

Perspectiva Futura

9. ¿Qué nos espera el segundo semestre de 2025?

El segundo semestre de 2025 se proyecta como una continuación lógica, y probablemente intensificada, de los fenómenos observados durante la primera mitad del año. A lo largo del primer semestre, el ecosistema de amenazas ha estado marcado por un volumen elevado de vulnerabilidades (muchas de ellas *zero-days*) y por su explotación activa por parte de actores maliciosos en campañas reales, lo que indica una aceleración en la ventana entre la divulgación y el uso ofensivo de estos fallos.

En el plano de los actores de amenazas, el semestre ha estado marcado por una alta actividad de los grupos ***RansomHub*** y ***Cl0p***, líderes indiscutibles del *ransomware* en 2025 hasta el momento. Aunque algunos colectivos como ***LockBit*** han reducido su visibilidad, otros como ***Akira*** y ***Qilin*** se han mantenido firmemente en el *top* 5 en cuanto a campañas reportadas, consolidando un modelo de negocio altamente profesionalizado. Se espera que estos grupos, o nuevas escisiones derivadas de ellos, continúen activos e **incrementen su volumen operativo a medida que se acerquen los periodos de mayor presión fiscal y presupuestaria en entornos corporativos.**

En paralelo, el primer semestre también ha estado marcado por un fenómeno emergente: la **fragmentación del ecosistema cibercriminal**. Han surgido nuevas coaliciones entre grupos de *hacktivismo*, muchas veces formadas de forma oportunista o ideológica, enmarcadas dentro de la creciente polarización geopolítica, especialmente **en torno al conflicto de Israel y Gaza**. Esta polarización está convirtiendo a organismos gubernamentales occidentales, infraestructuras críticas de países OTAN y entidades vinculadas a intereses israelíes en **objetivos prioritarios**. Esta tendencia se mantendrá e incluso podría agravarse en el segundo semestre.

Por otro lado, el mundo *underground* también está viviendo una transformación significativa. Las detenciones recientes, la **pérdida de *BreachForums***, así como la **caída del mayor mercado de drogas de la *dark web***, *Archetype*, han provocado una situación de inestabilidad que está reconfigurando el equilibrio de poder entre actores y plataformas. Se observa un **efecto rebote**, en el que los **impactos en las capas profundas del cibercrimen están comenzando a tener reflejo en la superficie**: el surgimiento de grupos dedicados a extorsionar a otros colectivos, delatar a antiguos socios o interferir en campañas rivales podría generar un incremento de filtraciones internas, campañas de *doxing* o conflictos de visibilidad en foros clandestinos.

A todo esto, se suma una progresiva profesionalización del cibercrimen. La disponibilidad de herramientas accesibles, entornos de colaboración técnica, y una economía sumergida que ve en el delito digital una vía de sustento, están haciendo que el número de nuevos grupos operativos crezca cada mes. Esto, sumado al hecho de que muchos actores ahora operan bajo lógicas empresariales, permite anticipar un **incremento del volumen y calidad técnica de los ataques en el segundo semestre.**

En este contexto, se hace imprescindible reforzar los mecanismos de detección temprana de vulnerabilidades y aplicar modelos de priorización adaptativa, que permitan reducir el tiempo entre la identificación del fallo y su mitigación efectiva. También será clave monitorizar el entorno de amenazas no solo en sus expresiones técnicas (TTPs), sino también en su dimensión social y geopolítica, para anticipar la evolución de campañas impulsadas por polarización ideológica o conflictos entre colectivos criminales.

El seguimiento constante del mundo *underground* y la evolución de su ecosistema será igualmente crucial: lo que ocurra en estas capas durante los próximos meses puede ser la antesala de nuevas campañas, herramientas o filtraciones masivas que impacten directamente en el tejido empresarial y gubernamental global.

Referencias

- Cartier, M. (2025, 3 de marzo). *Business Email Compromise Statistics 2025*. Hoxhunt. https://hoxhunt.com/blog/business-email-compromise-statistics
- CERT-EU. (2025). *Threat Landscape Q1 & Q2 2025 Reports*[RG1] [SS2] . https://cert.europa.eu/publications/threat-intelligence/2025
- Check Point Research. (2025, 14 de enero). *5 Key Cyber Security Trends for 2025*. Check Point. https://blog.checkpoint.com/research/5-key-cyber-security-trends-for-2025
- CISA. (2024, 20 de noviembre). *#StopRansomware: BianLian Ransomware Group.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a
- CISA. (2025, 30 de abril). *#StopRansomware: Rhysida Ransomware*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
- Cloudforce One. (2025, 21 de mayo). *Cloudflare participates in global operation to disrupt Lumma Stealer*. Cloudflare. https://www.cloudflare.com/es-es/threat-intelligence/research/report/cloudflare-participates-in-joint-operation-to-disrupt-lumma-stealer/
- CrowdStrike. (2025). *CrowdStrike Global Threat Report 2025*. https://www.crowdstrike.com/global-threat-report/
- Cyber News Centre Team. (2025, 4 de julio). *The State of APAC Cybersecurity: CNC Intelligence Overwatch Report - July 2025*. Cyber News Centre. https://www.cybernewscentre.com/the-state-of-apac-cybersecurity-cnc-intelligence-overwatch-report-july-2025/
- Cybersecurity Ventures. (2025). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybersecurity Ventures. https://cybersecurityventures.com/cyberwarfare-report-intrusion/[RG3]
- CYFIRMA. (2025, 9 de mayo). *PupkinStealer : A .NET-Based Info-Stealer*. CYFIRMA. https://www.cyfirma.com/research/pupkinstealer-a-net-based-info-stealer/
- DarkFeed. (2025). *Here's a look at the most active ransomware groups of 2025* [Publicaciones de X]. X. https://x.com/ido_cohen2
- DarkFeed. (2025). *New Ransomware Group* [Publicaciones de X]. X. https://x.com/ido_cohen2
- Department for Science, Innovation and Technology, Home Office and Feryal Clark MP. (2025, 10 de abril). *Cyber Security Breaches Survey 2025*. Gov.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/
- Yoachimik, O. y Pacheco, J. (2025, 27 de abril). *Targeted by 20.5 million DDoS attacks, up 358% year-over-year: Cloudflare's 2025 Q1 DDoS Threat Report.* Cloudflare. https://blog.cloudflare.com/es-la/ddos-threat-report-for-2025-q1/

- FBI. (2025, 6 de marzo). *Mail Scam Targeting Corporate Executives Claims Ties to Ransomware.* Internet Crime Complaint Center. https://www.ic3.gov/psa/2025/psa250306-2#:~:text=March%206%2C%202025-,Mail%20Scam%20Targeting%20Corporate%20Executives%20Claims%20Ties%20to%20Ransomware,come%20from%20a%20ransomware%20group.
- Federal Ministry of the Interior. (2025). *Protecting the 2025 Bundestag elections from hybrid threats and disinformation*. Federal Ministry of the Interior. https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation-election/disinformation-election-artikel.html
- Fox, J. (2024, 23 de diciembre). *Top Cybersecurity Statistics 2025*. Cobalt. https://www.cobalt.io/blog/top-cybersecurity-statistics-2025/
- Franceschi-Bicchierai, L. (2025, 23 de mayo). *Mysterious hacking group Careto was run by the Spanish government, sources say*. TechCrunch. https://techcrunch.com/2025/05/23/mysterious-hacking-group-careto-was-run-by-the-spanish-government-sources-say/
- Fry, C. (2025). *The Cost of a Cyber Attack in 2025 on SMEs*. Robinson https://www.robison.co.uk/cost-of-a-cyber-attack-2025/
- Gatlan, S. (2025, mayo 27). *Russian Laundry Bear cyberspies linked to Dutch Police hack*. BleepingComputer. https://www.bleepingcomputer.com/news/security/russian-void-blizzard-cyberspies-linked-to-dutch-police-breach/
- Group-IB. (2025). *Hi-Tech Crime Trends Report 2025*. https://www.group-ib.com/landing/high-tech-crime-trends-2025/
- Hitachi Cyber. (2025, 17 de enero). *Cyber Threat Landscape in 2025: Trends and Challenges*. Hitachi. https://hitachicyber.com/cyber-threat-landscape-in-2025-trends-and-challenges/
- Identity Defined Security Alliance. (2025). *2025 Identity Security Landscape Report*. https://www.idsalliance.org
- KrakenLabs. (2025). *Threat Context Monthly Reports (January–May 2025)*. Outpost24. https://outpost24.com/blog
- Márquez, J. (2025, 24 de mayo). *El misterioso grupo de hackers Careto se encontraba detrás de un agente inesperado: el Gobierno de España*. Xataka. https://www.xataka.com/seguridad/misterioso-grupo-hackers-careto-se-encontraba-agente-inesperado-gobierno-espana-techcrunch
- Zang X. (2025, 22 de abril). Infostealer Malware FormBook Spread via Phishing Campaign – Part I. Fortinet. https://www.fortinet.com/blog/threat-research/infostealer-malware-formbook-spread-via-phishing-campaign-part-i

- Microsoft Threat Intelligence. (2025, 27 de mayo). *New Russia-affiliated actor Void Blizzard targets critical sectors for espionage*. Microsoft. https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/

- Microsoft Threat Intelligence, Microsoft Digital Crimes Unit and Microsoft Security Experts [MTI, MDC & MSE]. (2025, 21 de mayo). *Lumma Stealer: Breaking down the delivery techniques and capabilities of a prolific infostealer*. Microsoft. https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/

- Miliefsky, G. (2025, 13 de marzo). *The true cost of cybercrime: Why global damages could reach $1.2 to $1.5 trillion by end of 2025*. Cyber Defense Magazine. https://www.cyberdefensemagazine.com

- Newman, L.H. (2025, 11 de marzo). *What Really Happened With the DDoS Attacks That Took Down X*. Wired. https://www.wired.com/story/x-ddos-attack-march-2025/

- Orange Cyberdefense. (2025). *Sector 16 Group*. Orange. https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/Sector16/Sector16Group.pdf

- Stamford, C. (2024, 28 de agosto). *Gartner Forecasts Global Information Security Spending to Grow 15% in 2025*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

- SOCRadar. (2025, 22 de mayo). *Top 10 Deep Web and Dark Web Forums*. https://socradar.io/top-10-deep-web-and-dark-web-forums/

- Tamzid, A. (2025, 23 de mayo). *Cybercrime statistics and financial impact*. Bright Defense. https://www.brightdefense.com/resources/cybercrime-statistics/

- Toulas, B. (2025, 1 de mayo). *Pro-Russia hacktivists bombard Dutch public orgs with DDoS attacks*. BleepingComputer. https://www.bleepingcomputer.com/news/security/pro-russia-hacktivists-bombard-dutch-public-orgs-with-ddos-attacks/

- World Economic Forum. (2025, 13 de enero). *Global Cybersecurity Outlook 2025*. https://www.weforum.org/reports/global-cybersecurity-outlook-2025

- Yilmaz, E. y Yildirim, E. (2025, 10 de mayo). *Cyber threats to cost $10.5T by 2025 as cybersecurity investments surge*. AA News. https://www.aa.com.tr/en/science-technology/cyber-threats-to-cost-105t-by-2025-as-cybersecurity-investments-surge/3563268


NTT DATA