Tendencias CTI

Ciberinteligencia de Amenazas

Segundo semestre 2025

Índice

Índice

1. Resumen ejecutivo

El **segundo semestre de 2025** (S2 2025) ha consolidado una evolución estructural del panorama de ciberamenazas, marcada por la convergencia entre tensiones geopolíticas, profesionalización del cibercrimen y madurez tecnológica de los actores de amenaza, más que por la aparición de técnicas radicalmente nuevas. El periodo se ha definido por un cambio profundo en la lógica operativa del atacante, orientado a la persistencia, el sigilo y la maximización del impacto económico, estratégico y reputacional.

El **ciberespacio se ha confirmado como un dominio central de confrontación híbrida**, integrado de forma estable en dinámicas geopolíticas globales. Conflictos prolongados y rivalidades estratégicas se han proyectado sobre infraestructuras digitales, cadenas de suministro y ecosistemas tecnológicos, generando efectos transversales que afectan tanto a gobiernos como a sectores críticos y organizaciones privadas. La fragmentación geoeconómica, la soberanía digital y la reconfiguración de alianzas tecnológicas han reforzado un entorno más volátil, menos cooperativo y con mayores dificultades de atribución y respuesta coordinada.

Desde el punto de vista operativo, el semestre ha evidenciado una reducción deliberada del ruido técnico. **Los atacantes han priorizado intrusiones de bajo perfil basadas en el abuso de identidades legítimas, servicios *cloud* y herramientas habituales** de las organizaciones, disminuyendo el uso de *malware* tradicional. Este enfoque incrementa el tiempo de permanencia en los entornos comprometidos y dificulta la detección temprana, desplazando el foco defensivo desde indicadores técnicos evidentes hacia señales débiles y distribuidas.

El ***ransomware* y la extorsión basada en datos han alcanzado un grado avanzado de industrialización**. La innovación ya no reside en el cifrado, sino en la orquestación integral de campañas: automatización, selección de información de alto valor, presión escalonada y explotación reputacional.

Este modelo reduce la dependencia del impacto operativo directo y permite monetizar intrusiones incluso sin interrumpir completamente los servicios de la víctima.

La **inteligencia artificial (IA) se ha consolidado como un multiplicador operativo**. Su uso se ha normalizado para acelerar tareas concretas, ingeniería social, reconocimiento, adaptación de herramientas; reduciendo costes y barreras de entrada, sin sustituir al operador humano. Por otro lado, se ha observado una aceleración sostenida en la **explotación de vulnerabilidades críticas** tras su divulgación pública, intensificando la asimetría entre capacidades ofensivas y defensivas.

Simultáneamente el **ecosistema criminal ha experimentado una fragmentación significativa**. La caída de grandes foros *underground* y *marketplaces* centralizados no reduce la actividad, ilícita, sino que la redistribuye hacia mercados especializados, *brokers* de acceso inicial y canales privados más opacos, dificultando la monitorización y la obtención de inteligencia temprana.

En paralelo, el semestre ha estado marcado por un **refuerzo del marco legal y regulatorio y por operaciones policiales internacionales de alto impacto,** así como por una **mejora progresiva de las capacidades defensivas** de las organizaciones. No obstante, la capacidad de adaptación de los actores maliciosos sigue superando estos avances, poniendo de manifiesto una brecha persistente entre el cumplimiento normativo y la resiliencia operativa real.

En conjunto, el segundo semestre de 2025 ha dibujado un escenario en el que la ciberseguridad deja de ser un problema exclusivamente tecnológico para convertirse en un reto sistémico, donde identidad, confianza, procesos organizativos y contexto geopolítico resultan tan determinantes como las capacidades técnicas. La gestión eficaz del riesgo exige una aproximación integral, orientada a la detección contextual, la resiliencia y la anticipación estratégica frente a amenazas persistentes y altamente adaptativas.

2. Introducción

2.1. 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 **segundo 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.

2.2. 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.

Nos encontramos en un 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, que **comprende de julio a diciembre de 2025**, resulta clave para anticipar posibles movimientos futuros y fortalecer las capacidades de respuesta ante un entorno cada vez más complejo.

3. Panorama global de amenazas

Durante el segundo semestre de 2025, el panorama global de amenazas ha evolucionado hacia un entorno **más volátil y fragmentado**, marcado por la convergencia de tensiones geopolíticas, disrupciones tecnológicas y dinámicas económicas adversas. Esta combinación ha incrementado de forma sostenida la superficie de exposición de gobiernos, empresas y ciudadanos, especialmente en sectores críticos y ecosistemas digitales interconectados.

Los riesgos digitales ya no se manifiestan de forma aislada, sino que interactúan y **se refuerzan mutuamente**, generando impactos sistémicos que afectan simultáneamente a múltiples sectores estratégicos (World Economic Forum, 2025). En este contexto, el ciberespacio se ha consolidado como un vector transversal que amplifica conflictos preexistentes y acelera dinámicas de confrontación más amplias.

La creciente dependencia de infraestructuras digitales críticas, junto con la fragmentación geoeconómica y regulatoria, ha complicado la cooperación internacional en materia de ciberseguridad. La coexistencia de distintos marcos normativos, modelos tecnológicos y enfoques de gobernanza incrementa la complejidad operativa y dificulta la respuesta coordinada ante incidentes transfronterizos.

Este apartado identifica los **factores estructurales del entorno global que, por su carácter sistémico, influyen de manera directa** en la evolución del riesgo cibernético y en la estabilidad de los ecosistemas digitales.

3.1 Geopolítica y Ciberseguridad

Durante la segunda mitad de 2025, la relación entre geopolítica y ciberseguridad se ha intensificado hasta consolidar el ciberespacio como un dominio central de competencia estratégica entre Estados. Las rivalidades tecnológicas, las tensiones económicas y la lucha por el control de recursos críticos ya no se limitan al plano diplomático o comercial, sino que se proyectan de forma sistemática sobre infraestructuras digitales, cadenas de suministro y ecosistemas tecnológicos globales.

Este periodo se ha desarrollado en un contexto de multipolaridad desequilibrada, caracterizado por la ausencia de un orden internacional estable y la coexistencia de múltiples centros de poder con capacidad suficiente para erosionar o desestabilizar el sistema sin imponer reglas comunes (Aznar Fernández-Montesinos, 2025). En este escenario, Estados Unidos, China y Rusia continúan marcando el ritmo de la confrontación estratégica, con efectos directos sobre la estabilidad del ciberespacio.

La competencia geopolítica se articula cada vez más mediante instrumentos geoeconómicos, sanciones, controles tecnológicos, *friendshoring* y presión regulatoria, que actúan como catalizadores indirectos de ciberoperaciones contra sectores estratégicos. Esta dinámica contribuye a redirigir las amenazas hacia ámbitos como energía, transporte, manufactura avanzada y servicios financieros, incrementando el impacto potencial de los incidentes cibernéticos.

Un elemento clave de esta evolución es la consolidación de modelos soberanos de Internet. Iniciativas como **RuNet** en Rusia reflejan un enfoque de control estatal del tráfico, los servicios y la gobernanza digital, apoyado en infraestructuras autónomas y marcos regulatorios propios. Estos modelos, potencialmente replicables en otros contextos, tienen implicaciones directas sobre la atribución, la visibilidad de los incidentes y la respuesta coordinada, reforzando la fragmentación del ciberespacio global (Hernández, 2025).

En paralelo, la **inteligencia artificial** se ha consolidado como un multiplicador estratégico. Su integración en operaciones de ciberespionaje, desinformación y automatización ofensiva reduce las barreras de entrada, acelera los ciclos de ataque y amplifica el alcance de las campañas híbridas, tanto por parte de Estados como de actores criminales avanzados

En este contexto, el ciberespacio se consolida como el entorno preferente para la **confrontación** por debajo del umbral del conflicto armado, permitiendo ejercer presión, disrupción y señalización estratégica con un riesgo político y militar limitado.

Friendshoring es una estrategia de reorganización de las cadenas de suministro mediante la cual los Estados o las empresas desplazan la producción, el abastecimiento o los servicios críticos hacia países considerados aliados, socios estratégicos o políticamente afines, con el objetivo de reducir riesgos geopolíticos, económicos y de seguridad.

3.2 Geopolítica y principales actores

Durante el segundo semestre de 2025, los principales conflictos internacionales no han experimentado transformaciones abruptas, pero sí una profundización de sus dimensiones híbridas, en las que el ciberespacio se integra de forma estructural con presiones económicas, maniobras diplomáticas y narrativas informativas.

- **Rusia – Ucrania: profundización de la dimensión híbrida del conflicto**

La guerra entre Rusia y Ucrania ha continuado sin grandes avances territoriales, pero con una intensificación sostenida de su dimensión híbrida. Durante este periodo, Rusia ha reforzado el uso del ciberespacio como complemento a la presión política, económica y diplomática, ampliando las operaciones no solo contra objetivos ucranianos, sino también contra instituciones y empresas europeas que prestan apoyo a Kiev.

El semestre ha estado marcado por un incremento de campañas de denegación de servicio, intentos de interrupción de servicios esenciales y operaciones de influencia destinadas a manipular percepciones públicas en la Unión Europea, dirigidas contra organismos públicos e infraestructuras digitales de países de la UE y la OTAN alineados con Ucrania. Paralelamente, se observa una mayor convergencia entre actores estatales y colectivos de *hacktivismo* prorruso, con una integración más estrecha entre desinformación, explotación de vulnerabilidades y ataques dirigidos a sectores críticos cuyo objetivo principal de estas campañas no ha sido la destrucción de sistemas, sino la disrupción operativa y el impacto mediático.

Un elemento relevante del periodo ha sido el avance hacia atribuciones públicas más explícitas por parte de gobiernos occidentales. Este giro refleja un cambio desde una actitud predominantemente prudente hacia una estrategia más orientada a la disuasión, que busca elevar el coste político de las operaciones maliciosas, reforzar la atribución colectiva y sentar precedentes normativos, aunque con el riesgo de escaladas controladas en el plano digital.

- **Oriente Medio: ciberespacio como escenario de confrontación indirecta**

El segundo semestre de 2025 ha estado marcado por una intensificación de las tensiones entre Irán e Israel, donde el ciberespacio actúa como **escenario de confrontación directa pero contenida**. Las operaciones observadas combinan intrusiones, filtraciones, sabotajes selectivos y campañas de manipulación informativa orientadas a degradar capacidades críticas sin desencadenar una escalada militar abierta.

Un riesgo especialmente relevante en este contexto es el *spill-over* regional. La elevada interdependencia tecnológica de infraestructuras energéticas, financieras y logísticas incrementa la probabilidad de impactos colaterales sobre terceros países y actores privados. A diferencia del plano militar, donde los altos el fuego pueden marcar puntos de inflexión claros, en el ciberespacio las dinámicas de confrontación tienden a mantenerse activas de forma autónoma, incluso cuando se reduce la violencia física.

- **China – Occidente: competencia sistémica y presión tecnológica**

La rivalidad entre China y las potencias occidentales no ha derivado en un conflicto abierto, pero sí ha experimentado una intensificación notable en el ámbito digital. Durante este semestre, los actores asociados a Pekín han incrementado sus campañas de ciberespionaje contra sectores estratégicos como semiconductores, telecomunicaciones, energía renovable, manufactura avanzada y servicios financieros, alineadas con objetivos de proyección industrial y tecnológica a largo plazo.

Un rasgo distintivo del periodo ha sido la reducción del tiempo entre la divulgación de vulnerabilidades críticas y su explotación operativa, reflejo de una estructura de inteligencia técnica altamente eficiente. Esta dinámica incrementa la presión sobre empresas occidentales y refuerza el uso del ciberespacio como herramienta para condicionar decisiones estratégicas, especialmente en el contexto del Indo-Pacífico y las tensiones en torno a Taiwán.

Spill-over regional: propagación indirecta del impacto de un conflicto hacia terceros actores o regiones interconectadas.

- **Corea del Norte y África: persistencia y entornos de oportunidad**

Corea del Norte mantiene una actividad sostenida centrada en la obtención de recursos financieros y el espionaje estratégico, con indicios crecientes de cooperación operativa con actores rusos. Esta convergencia amplía el alcance potencial de sus operaciones y añade complejidad a los procesos de atribución.

En paralelo, regiones como el Sahel continúan ofreciendo entornos propicios para la proliferación de actores híbridos. La combinación de debilidad institucional, fragmentación política y presencia de infraestructuras críticas facilita actividades oportunistas de sabotaje digital, espionaje y desinformación, incrementando la exposición de empresas europeas con presencia en la región.

En conjunto, el segundo semestre de 2025 confirma que la geopolítica, la tecnología y la ciberseguridad forman un **sistema interdependiente**, en el que las tensiones estratégicas se trasladan al ciberespacio con rapidez y efectos transversales. Estas dinámicas, aunque no siempre se materializan en conflictos abiertos, están redefiniendo el equilibrio digital global y condicionan de forma directa la seguridad de Estados, sectores estratégicos y organizaciones privadas.

3.3 Afectación de ciberataques a sectores específicos

Para concluir con el análisis del panorama de amenazas del segundo semestre de 2025, desde el **Departamento de Cyber Threat Intelligence de NTT DATA** resulta esencial examinar la evolución de los ciberataques por sectores y países más afectados. Los datos registrados entre julio y diciembre muestran que, pese a la persistencia de patrones consolidados en semestres anteriores, se observan variaciones relevantes asociadas a la intensificación de tensiones geopolíticas y al incremento del número de actores con capacidad disruptiva.

En comparación con el primer semestre de 2025 (S1 2025), la distribución sectorial presenta cambios significativos en la priorización de objetivos, así como una consolidación de ataques contra sectores estructurales para la administración pública y el funcionamiento económico global.

La distribución sectorial de los ataques vuelve a poner de manifiesto la clara preferencia de actores maliciosos, tanto estatales como no estatales, por sectores estratégicos que concentran información sensible, dependencias operativas críticas y un elevado impacto potencial en caso de disrupción. A diferencia del semestre anterior, en el que los ataques se concentraron en un número más reducido de sectores, en este periodo se observa un incremento generalizado del volumen de ataques, especialmente en el sector público, la educación y los servicios financieros.

- **Administración Pública y Gobiernos:**

El sector de la **Administración Pública** continúa ocupando la primera posición en número de incidentes, acumulando **un total de 3.343 ataques en los últimos seis meses.** Este dato supone un incremento significativo respecto al primer semestre y consolida la tendencia observada desde finales de 2024, marcada por campañas dirigidas a organismos públicos de todos los niveles. La constante exposición de los sistemas administrativos, junto con la criticidad de sus operaciones, los convierte en un objetivo prioritario para grupos que buscan obtener información estratégica, comprometer servicios esenciales o ejecutar acciones de presión política mediante *defacement* y filtraciones de datos.

El aumento de intrusiones asociadas a actores motivados políticamente, como las campañas atribuidas a grupos vinculados a México durante este periodo, evidencia que los organismos gubernamentales continúan siendo uno de los principales vectores de impacto en un contexto de creciente de cibertensión internacional.

En cuanto al **Gobierno y Sector Público**, se han registrado **590 ataques confirmados en los últimos seis meses**, una cifra significativamente inferior a la observada en el conjunto de la Administración Pública, pero que confirma que este ámbito sigue siendo un **objetivo recurrente** dentro del ecosistema de amenazas. Estos incidentes se concentran principalmente en organismos con alta visibilidad institucional y en entidades responsables de la prestación de servicios al ciudadano, donde el impacto reputacional y operativo continúa siendo un factor clave para los atacantes.

El término Sector Público engloba a todas las entidades controladas por el Estado, mientras que Administración Pública se refiere específicamente a los órganos y estructuras administrativas que ejecutan políticas públicas.

- **Educación:**

Con **1.460 ciberataques, el sector educativo se mantiene como uno de los más afectados.** Aunque la cifra es ligeramente inferior a la registrada durante el primer semestre, las instituciones educativas siguen siendo especialmente vulnerables debido a la heterogeneidad de sus sistemas, la gestión descentralizada de activos y la presencia de datos personales, académicos e investigativos de alto valor.

En este semestre se observa un cambio en el tipo de ataque predominante: junto al robo de credenciales y el compromiso de redes internas, aumenta la presencia de campañas de extorsión basadas en filtración de datos aprovechando la baja capacidad de respuesta de muchas instituciones regionales y privadas. Las universidades continúan destacando como uno de los focos principales de estas amenazas.

- **Servicios financieros:**

El sector financiero **registra 957 ataques en este periodo, manteniéndose entre los tres más afectados a nivel global.** Los incidentes continúan centrados en ataques de *ransomware*, accesos no autorizados y robo de información sensible. La creciente sofisticación de las técnicas empleadas por grupos criminales, junto con la presencia de actores estatales interesados en el espionaje económico, explica la persistencia de este sector como objetivo de alto valor.

Se observa asimismo un aumento del interés por compañías *fintech* y plataformas de pago digitales, cuyo crecimiento durante el último año ha ampliado la superficie de exposición y atraído campañas oportunistas basadas en explotación de vulnerabilidades críticas.

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

Los sectores de Servicios TI (**802 ataques**) y Telecomunicaciones (**614 ataques**) han vuelto a situarse entre los más presionados digitalmente. La mayoría de los incidentes registrados en este semestre están relacionados con la explotación de vulnerabilidades en sistemas de terceros, ataques dirigidos contra proveedores de servicios gestionados y compromisos de cadenas de suministro.

La naturaleza interconectada de estas industrias convierte cualquier intrusión en una potencial amenaza multiplicada, ya que los atacantes pueden escalar lateralmente hacia clientes y socios tecnológicamente dependientes. Este patrón se ha consolidado especialmente en los meses de septiembre y noviembre, coincidiendo con picos globales de actividad maliciosa.

- **Transporte, Logística y Comercio Electrónico:**

Con **592 ataques en Transporte y Logística y 532 en Comercio Electrónico, estos sectores continúan experimentando una presión elevada.** La interrupción de cadenas de suministro, las campañas de fraude digital y la manipulación de datos de clientes siguen siendo vectores habituales entre julio y diciembre.

En el caso concreto del comercio electrónico, el repunte de actividad coincide con la campaña comercial del último trimestre (con eventos como el *Black Friday*, el *Cyber Monday* o la época navideña), periodo en el que los atacantes buscan maximizar el impacto mediante operaciones de *carding*, *skimming* y compromisos de plataformas de venta.

- **Salud y Servicios Sanitarios:**

El sector sanitario acumula **526 incidentes,** una cifra que, aunque menor que en semestres anteriores, continúa situándolo entre los objetivos más críticos. Los ataques de *ransomware* siguen siendo la principal amenaza, dado su potencial para interrumpir servicios clínicos, comprometer datos médicos y generar impactos directos en la atención al paciente.

Este semestre destaca la concentración de incidentes en entidades de tamaño medio y proveedores privados, un indicio de que los atacantes buscan objetivos con menor capacidad de inversión en seguridad, pero igualmente relevantes operativamente.

En comparación con el primer semestre del año, se observa un cambio relevante en la composición del conjunto de sectores más afectados. Si bien la mayoría de los sectores mantienen una posición similar, destaca la salida del sector manufacturero, que hasta el semestre anterior figuraba entre los diez más atacados.

En su lugar, durante este segundo semestre irrumpe el sector de **Construcción (445 ataques),** que adquiere suficiente peso como para situarse entre los ámbitos con mayor volumen de incidentes. Este desplazamiento evidencia un reajuste en las prioridades de los actores maliciosos, con un mayor énfasis en sectores con alta rentabilidad económica.

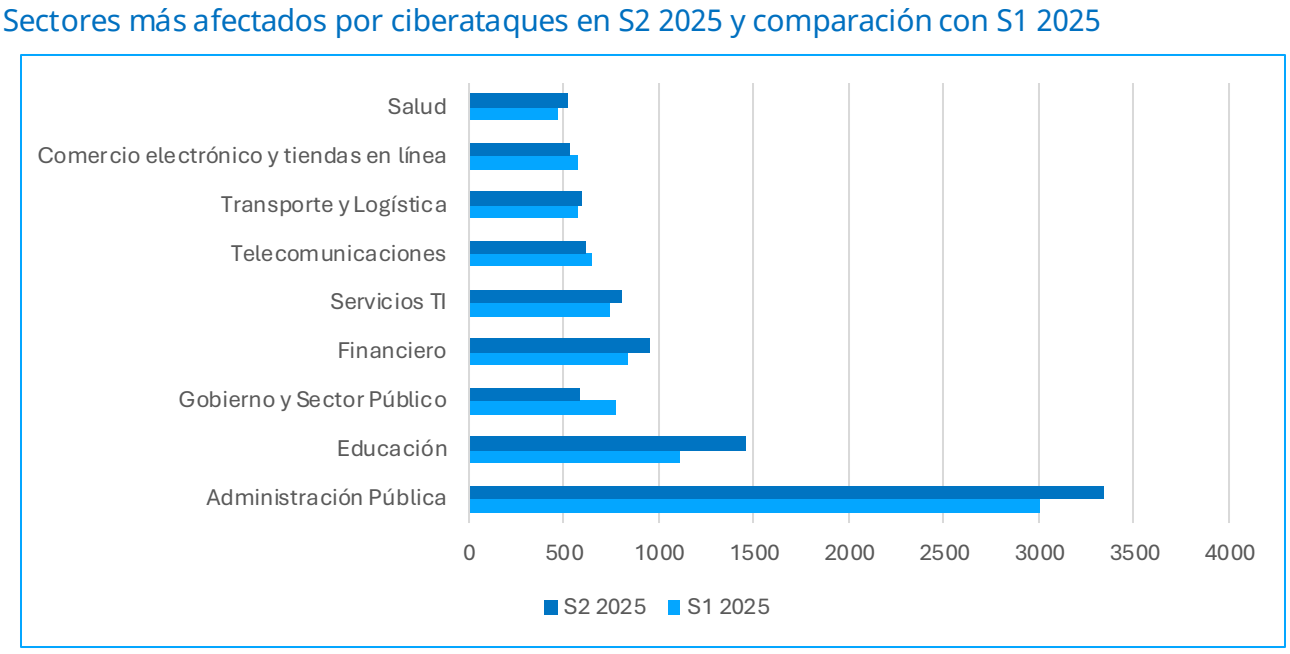


Figura 1 | Sectores más afectados por ciberataques en el segundo semestre de 2025.

Los datos del segundo semestre de 2025 confirman un patrón continuista en el impacto geográfico, con los ciberataques concentrándose en países altamente digitalizados y con peso geopolítico, en estrecha relación con el contexto político internacional.

- **Estados Unidos** vuelve a situarse como el país más afectado, **acumulando 3.963 ataques. Aunque se observa una ligera reducción respecto al semestre anterior, Estados Unidos mantiene el mayor volumen de ataques a nivel global**. Este volumen refleja tanto el liderato económico del país como su papel central en conflictos tecnológicos y geoestratégicos, especialmente su rivalidad con China y su implicación en la guerra de Ucrania.

- **Tailandia**, **con 1.341 ataques, entra por primera vez entre los cinco países más afectados en el periodo reciente**. El aumento del volumen de ciberataques se relaciona con la expansión de infraestructuras de pago digital, el crecimiento del comercio electrónico y la mayor exposición del país a campañas de *phishing* y *ransomware* desplegadas a gran escala en el sudeste asiático.

- En **India**, que registra **1.244 ataques, se observa una continuidad en la actividad maliciosa** vinculada tanto a tensiones regionales como a la digitalización del país. India se mantiene como objetivo prioritario para actores criminales y estatales debido a su volumen poblacional, el crecimiento de su sector tecnológico y su papel estratégico en el Indo-Pacífico.

- **Israel** ocupa la cuarta posición**, con 1.233 ataques**, un volumen coherente con la persistencia de la tensión regional, pese a registrar una reducción respecto al semestre anterior. La actividad cibernética dirigida a Israel combina operaciones ofensivas vinculadas a grupos estatales adversarios con campañas de *hacktivismo* motivadas por la situación en Oriente Medio.

- Por último, **Alemania registra 856 ataques,** manteniéndose como uno de los principales objetivos europeos. La actividad maliciosa se ha concentrado en sectores industriales, servicios gubernamentales y entidades financieras, en un contexto marcado por el impacto económico derivado de la guerra en Ucrania y su papel como principal potencia tecnológica de la Unión Europea.

Distribución de ciberataques por países en S2 2025

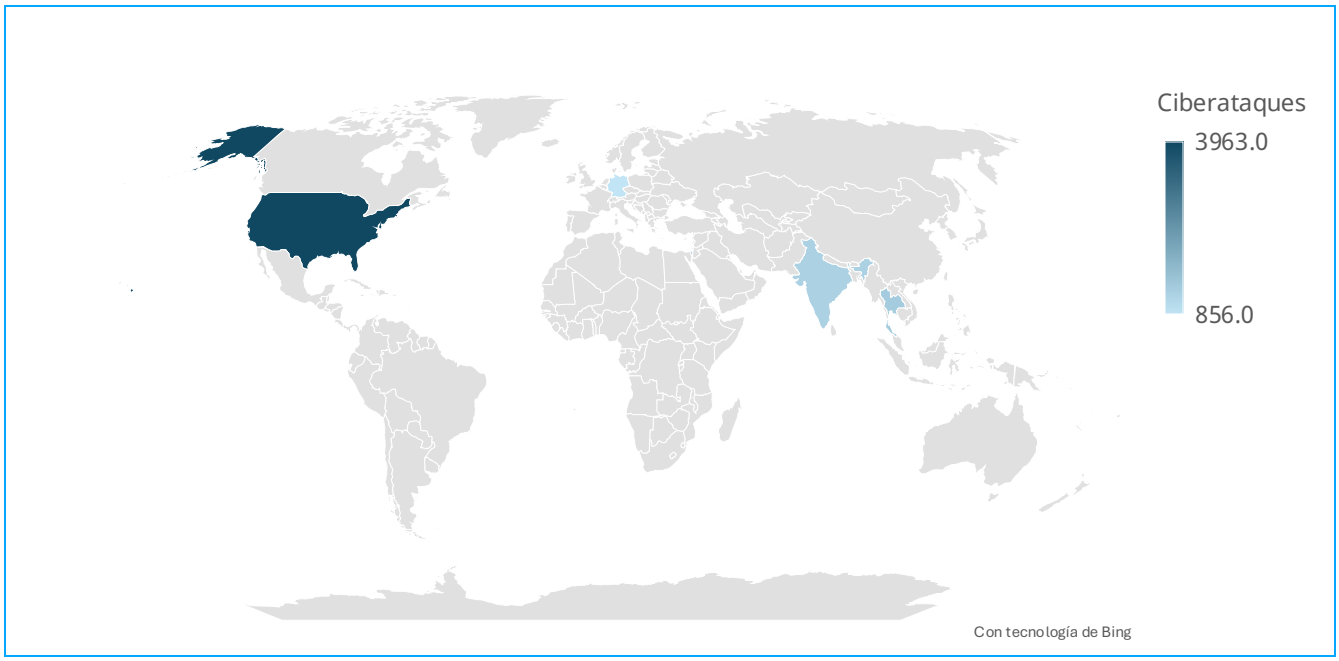


Figura 2 | Distribución geográfica del impacto de ciberataques en el segundo semestre de 2025.

3.4 Panorama en España

El segundo semestre de 2025 ha confirmado que España se ha consolidado como uno de los escenarios europeos más expuestos a la actividad de ciberamenazas. Con **alrededor de 605 incidentes significativos** registrados entre julio y diciembre, el país ha recibido una alta presión por parte de actores criminales especializados en *ransomware*, extorsión digital, filtración de datos y campañas de *phishing* avanzado. Este volumen de actividad ha situado a **España entre los países más atacados del continente**, en línea con análisis internacionales que ya en la primera mitad del año lo identificaban como uno de los países con mayor número de incidentes a escala global (Valdeomillos, 2025).

El patrón predominante ha seguido siendo la **motivación económica**. La mayor parte de los ataques registrados han respondido a campañas de *ransomware*, con o sin doble extorsión, y a operaciones centradas en la obtención ilícita de información para su venta o chantaje posterior. Esta tendencia se explica por el elevado grado de digitalización del país, la relevancia económica de determinados sectores y la presencia de un tejido empresarial compuesto mayoritariamente por pymes con niveles de protección desiguales.

- **Actores y sectores más afectados en España**

El impacto sectorial durante el periodo analizado ha mostrado un comportamiento diferenciado respecto al patrón global. Los **servicios profesionales y consultoría** se han situado como uno de los sectores más perjudicados. Firmas de ingeniería, asesoría o gestión documental han sido objetivo recurrente de grupos como **Qilin** e **INC Ransomware Group**, que han centrado su actividad en comprometer repositorios internos y extraer información sensible. Durante septiembre y octubre se registraron incidentes en los que los atacantes filtraron documentación técnica de proyectos con el objetivo de presionar a las víctimas, ilustrando el creciente peso de la extorsión como vector de presión.

El sector **manufacturero**, aunque ha perdido presencia entre los sectores más atacados a nivel internacional, **ha mantenido en España un protagonismo notable**. Varias empresas industriales experimentaron intrusiones contra sistemas *OT* y *SCADA* a lo largo de septiembre y octubre, con casos en los que se vieron obligadas a detener temporalmente líneas de producción para evitar la propagación del ataque. Este impacto directo sobre la continuidad operativa explica por qué la industria española continúa siendo uno de los focos prioritarios para los actores orientados al beneficio económico.

La **Administración Pública** continúa entre los sectores más afectados por la actividad de ciberamenazas, especialmente en el ámbito local. La combinación de infraestructuras heterogéneas, recursos limitados y una elevada dependencia de servicios digitales ha incrementado de forma notable la superficie de exposición. En diciembre, el **Ayuntamiento de Elche** sufrió un ataque informático que obligó a bloquear sistemas municipales y a interrumpir servicios internos y de atención ciudadana, activando protocolos de contingencia para contener el incidente (Pico, 2025). Este episodio vuelve a poner de relieve la vulnerabilidad estructural de las administraciones locales frente a ataques disruptivos y la dificultad de garantizar la continuidad operativa ante incidentes de este tipo.

El sector del **transporte y la logística** ha mantenido un nivel sostenido de ciberincidentes durante el segundo semestre del año, aunque la mayoría de ellos no han trascendido públicamente debido a las políticas de confidencialidad que caracterizan a este sector. Los datos agregados de plataformas especializadas han mostrado actividad significativa dirigida a operadores de movilidad, servicios auxiliares y sistemas de gestión asociados a cadenas de suministro, especialmente mediante campañas de *phishing* e intentos de acceso no autorizado a portales operativos.

El **sector sanitario** ha seguido estando entre los más afectados, con varios ataques de *ransomware* que obligaron a clínicas privadas y centros regionales a retrasar consultas y procedimientos médicos. La alta dependencia tecnológica del sector salud hace que cualquier interrupción tenga un impacto directo en la ciudadanía, lo que explica su atractivo para grupos criminales que buscan garantizar presión para el pago de rescates.

En el ámbito del **turismo**, **uno de los pilares de la economía española**, se registró en septiembre un ataque de doble extorsión contra un operador turístico nacional, afectando sus sistemas de reservas y comunicaciones internas. Este incidente es un ejemplo de la estacionalidad del riesgo en un sector que concentra su mayor actividad en verano y principios de otoño.

Finalmente, sectores como ***retail***, **comercio electrónico** y **alimentación** también han sufrido un incremento de incidentes durante el segundo semestre, especialmente vinculados a la interceptación de datos, accesos no autorizados a paneles administrativos y compromisos de servicios externos. Uno de los casos más relevantes del periodo se produjo en octubre de 2025, cuando la empresa textil Mango notificó un acceso no autorizado a datos personales de clientes a través de un **proveedor externo de servicios de marketing** (Macías, 2025).

- **Tendencias y tipologías de ataque en España**

El análisis temporal ha mostrado un pico de actividad en **octubre**, coincidiendo con la reactivación tras el periodo estival y el inicio del último trimestre del año. Durante este periodo, las técnicas más utilizadas han sido:

- ***Ransomware*** **y doble extorsión**, predominante en manufactura, administración pública, salud y servicios profesionales.
- **Exfiltración y chantaje**, especialmente relevante en consultoría, *retail* y *travel*.
- ***DDoS***, habitual en portales municipales y autonómicos.
- ***Phishing*** **dirigido**, especialmente activo contra banca, seguros y grandes empresas.
- **Compromiso de servicios *cloud***, frecuente en educación y servicios profesionales debido a configuraciones débiles o ausencia de *MFA*.

El panorama español durante el segundo semestre de 2025 ha revelado un ecosistema especialmente expuesto a ciberataques con motivación económica, en el que sectores como los servicios profesionales, la manufactura, la administración pública, el transporte, la salud y el turismo concentran la mayor parte de los incidentes.

Los ejemplos registrados en estos meses han evidenciado no solo la sofisticación creciente de los atacantes, sino también la necesidad de reforzar la resiliencia en áreas donde el impacto puede tener consecuencias operativas, económicas y sociales de gran alcance. España afronta así un escenario en el que la combinación de alta digitalización y madurez defensiva desigual convierte al país en un objetivo prioritario, subrayando la importancia de avanzar hacia un marco de ciberseguridad más robusto, cohesionado y preventivo.

4. Principales amenazas globales

Durante el segundo semestre de 2025, el panorama de amenazas globales ha estado marcado por una alta intensidad operativa, con campañas más coordinadas, mayor profesionalización de los actores y un impacto creciente sobre infraestructuras críticas, grandes organizaciones y cadenas de suministro.

Se ha consolidado la convergencia entre *ransomware*, espionaje y sabotaje digital, con actores que reutilizan técnicas y capacidades de distintos ecosistemas criminales y estatales. El periodo ha confirmado una evolución hacia ataques más persistentes, selectivos y difíciles de atribuir, reforzando el carácter estructural de la amenaza cibernética a nivel global.

4.1. Ciberincidentes destacados y grandes campañas

Los ciberincidentes más relevantes del semestre han reflejado una escalada en alcance y sofisticación, con campañas de alto impacto dirigidas a sectores estratégicos, servicios esenciales y grandes corporaciones. Predominan operaciones prolongadas en el tiempo, apoyadas en credenciales comprometidas, infraestructuras legítimas y técnicas de *Living-off-the-Land* (LotL), que dificultan la detección temprana. Las grandes campañas observadas evidencian una clara orientación a la exfiltración masiva de datos, extorsión múltiple y disrupción operativa, consolidando modelos de ataque más agresivos y eficaces.

Desde el **Departamento de Cyber Threat Intelligence de NTT DATA** hemos documentado algunos de los ciberincidentes más relevantes del segundo semestre de 2025, seleccionándolos por su valor representativo de las principales amenazas observadas en este periodo.

Víctimas	Sector	Atacante	País / región afectada	Origen del atacante	Fecha del incidente	URL
SonicWall	Ciberseguridad	Akira Ransomware Group	Global	Desconocido	22/07/2025	Fuente
Salesforce / Salesloft	Nube	UNC6395	Global	Desconocido	09/08/2025	Fuente
Jaguar Land Rover (JLR)	Automoción / Manufactura	Scattered Lapsus$ Hunters	Global	Desconocido	01/09/2025	Fuente
Stellantis	Automoción	ShinyHunters	Norte América	Desconocido	21/09/2025	Fuente
Claro Colombia	Telecomunicaciones	Crimson Collective	Colombia	Desconocido	25/09/2025	Fuente
Asahi Group Holdings	Bebidas y productos alimenticios	Qilin	Japón	Desconocido	29/09/2025	Fuente
Red Hat	*Software*	Crimson Collective	Global	Desconocido	01/10/2025	Fuente
Muji / Askul	Comercio minorista (*retail*)	Desconocido	Japón	Desconocido	19/10/2025	Fuente
Knownsec	Ciberseguridad	Desconocido	Global	Desconocido	02/11/2025	Fuente
Anthropic	Inteligencia artificial	Desconocido	Global	China	13/11/2025	Fuente
Logitech	Electrónica	Cl0p	Global	Desconocido	14/11/2025	Fuente
Pornhub	Entretenimiento	ShinyHunters	Global	Desconocido	16/12/2025	Fuente
Ministerio del Interior de Francia	Gobierno / Seguridad Pública	Desconocido	Francia	Desconocido	17/12/2025	Fuente
Agencia Espacial Europea (ESA)	Espacial	888	Europa	Desconocido	31/12/2025	Fuente

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

Por otro lado, como se adelantó en el anterior informe, el segundo semestre de 2025 ha mostrado un ecosistema de amenazas más automatizado, más sigiloso y con mayor especialización sectorial, impulsado por la convergencia de IA generativa, cadenas de suministro comprometidas y operaciones con fuerte componente geopolítico.

Campañas de ciberataques en S2 2025 agrupadas por objetivo

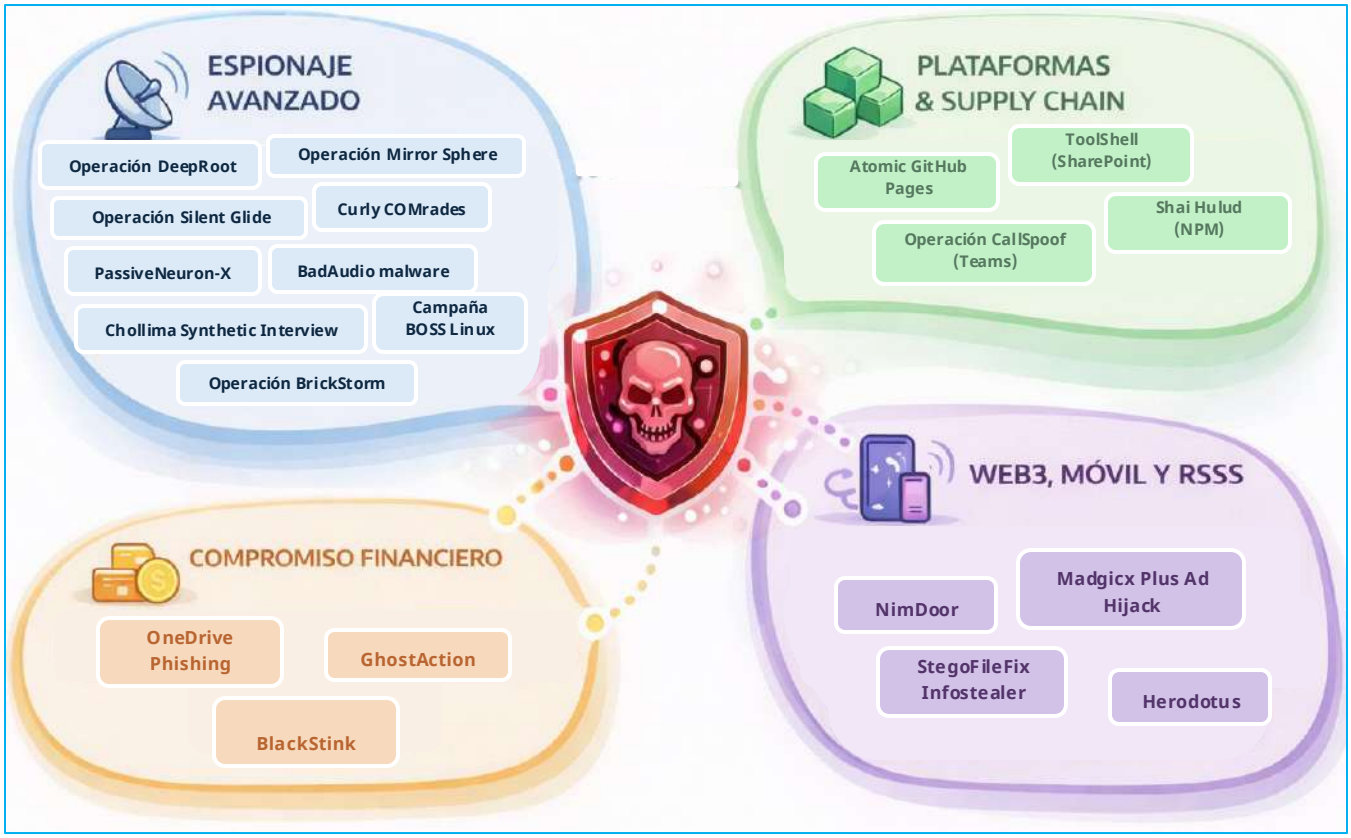


Figura 3 | Grandes campañas detectadas en el segundo semestre de 2025.

4.2 Tendencias emergentes de ataques

En el segundo semestre de 2025 se han afianzado tendencias que apuntan a un cambio estructural en los modelos de ataque, con mayor automatización, modularidad de herramientas y accesos iniciales de bajo perfil, confirmando un escenario que ya se preveía dinámico, donde priman la persistencia, la evasión y el impacto económico.

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

4.2.1 Ataques *low-noise* y *malware-free* apoyados en infraestructuras legítimas

Se ha consolidado el uso de técnicas *Living-off-the-Land* y un mayor abuso de servicios legítimos, especialmente *cloud* y SaaS, para persistir y moverse lateralmente sin dejar apenas artefactos, reduciendo la huella forense. Se ha observado el uso de OneDrive, Google Drive, Slack, GitHub, Discord o servicios OAuth como canales de mando y control encubierto; abuso de autenticaciones válidas y *tokens* legítimos en lugar de *malware* persistente; y el reemplazo de binarios maliciosos por *scripts* nativos, tareas programadas y abuso de utilidades del sistema (LOLBins).

4.2.2 Inteligencia artificial como multiplicador operativo

De nuevo la IA se ha observado como tendencia continuada, durante este periodo predomina su uso para acelerar fases concretas del ciclo operativo: automatizar reconocimiento, generación de *phishing* convincente, desarrollo de *payloads* polimórficos y automatización de campañas (*ransomware*, fraude, identidad sintética), todo esto adaptado de forma dinámica al perfil de la víctima.

4.2.3. Auge del compromiso de la cadena de suministro *software* y plataformas de desarrollo

Los ataques observados este semestre han mostrado un interés creciente en el compromiso herramientas y procesos de desarrollo: inyección de código malicioso en paquetes NPM, PyPI y repositorios GitHub (ejemplo del caso **Shai-Hulud 2.0** o **Glassworm** en extensiones de VS Code); manipulación de *pipelines* CI/CD con afectación en cascada a múltiples aplicaciones; y publicación de dependencias clonadas o con puertas traseras con propagación sin intervención activa una vez integradas.

4.2.4 Consolidación del *cloud* y SaaS como superficie primaria de ataque

El incremento sostenido de intrusiones en entornos *cloud* y SaaS ha reflejado el desplazamiento de ataques desde *endpoints* clásicos a ecosistemas interconectados en la nube. Los actores de amenaza han priorizado la explotación de configuraciones inseguras en entornos *multi-tenant*, el uso de aplicaciones de autorización abierta (OAuth) para obtener acceso persistente sin necesidad de credenciales, y el movimiento lateral basado en sincronización entre servicios SaaS, aprovechando conexiones entre aplicaciones con permisos excesivos.

4.2.5 Espionaje avanzado con fuerte componente geopolítico

El espionaje observado este semestre ha presentado características técnicas recurrentes como mayor persistencia distribuida, donde los atacantes utilizan varios mecanismos redundantes sin concentrar riesgos en un solo punto; el uso de C2 fragmentado y encubierto dentro de tráfico legítimo; técnicas de *beaconing* irregular, evitando patrones detectables y ajustando la frecuencia según actividad del usuario.

4.2.6 *Toolkits* modulares reutilizables

La adopción de arquitecturas modulares ha permitido a los actores de amenaza cambiar su propósito sin rediseñar la operación.

Esta práctica está marcando la profesionalización de los grupos como una evolución natural del mercado clandestino, como se venía viendo al inicio del año. Han predominado los *frameworks* que combinan robo financiero, espionaje corporativo y exfiltración selectiva, la reutilización de implantaciones ligeras con activación selectiva, y la aparición de ecosistemas de acceso persistente como servicio, donde se facilita infraestructura a APTs.

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

Durante el segundo semestre de 2025, el panorama global de ciberseguridad ha estado marcado por la consolidación de amenazas maduras, especialmente el *ransomware*, y por la aceleración de vectores habilitadores como la ingeniería social avanzada y el uso de inteligencia artificial. Lejos de observarse una reducción de la actividad maliciosa tras el pico de principios de año, los datos indican una estabilización en niveles elevados, acompañada de una mayor sofisticación técnica y organizativa de los actores de amenazas.

4.3.1 Incidentes de seguridad

El ***ransomware*** se ha mantenido como el principal generador de incidentes de alto impacto. Durante el tercer trimestre de 2025 se contabilizaron **1.592 víctimas** publicadas en sitios de filtración de datos, lo que supone una media aproximada de **535** víctimas mensuales. Aunque esta cifra es inferior al pico observado en el primer trimestre de 2025 (**2.289** víctimas), confirma que el segundo semestre se ha caracterizado por una actividad sostenida en valores históricamente altos, descartando un escenario de contención real de la amenaza (Check Point Research, 2025).

A nivel agregado, se ha observado que **el *ransomware*** está implicado en aproximadamente el **44% de las brechas de seguridad** registradas en 2025, frente a cerca del **32%** en 2024, consolidándose como el principal vector de impacto operativo y económico.

4.3.2 Tipos de ataques y vectores predominantes

A la cola del *ransomware* se han situado los ataques a la **cadena de suministro** presentes en un **30%** de los incidentes de 2025, consolidándose como principal amplificador del riesgo; los ataques a través de ***malware*** no *ransomware* (troyanos, *spyware*, *infostealer*, etc.) representan cerca del **17%**. Este tipo de *malware* se utiliza, principalmente, como mecanismo de preparación del entorno y persistencia.; y los ataques **DDoS** con una presencia

más limitada del **5%**, manteniendo un rol táctico y complementario.

En cuanto a vectores de entrada, el ***phishing*** ha seguido siendo el más frecuente, presente en torno al **16% de las brechas**, respondiendo al bajo coste y adaptabilidad de las técnicas de ingeniería social; sin embargo, el **compromiso de terceros** como punto de acceso (**15%**) se ha observado casi al mismo nivel, confirmando el desplazamiento de vectores iniciales al perímetro organizativo más allá de la infraestructura propia; finalmente el **compromiso de credenciales** (**10%**) ha evidenciado el abuso de identidades legítimas, confirmando el patrón observado a lo largo del informe.

Desde la perspectiva de la evolución tecnológica, **alrededor del 16%** de los incidentes ya han incorporado algún uso de **inteligencia artificial** por parte de los atacantes, principalmente para la generación de contenidos de *phishing*, suplantaciones de identidad y automatización de campañas (Khalil, 2025). Aunque el uso de IA aún no sustituye a las técnicas tradicionales, sí incrementa su escala, credibilidad y eficacia, actuando como multiplicador del riesgo.

4.3.3 Actores de amenazas y dinámica del ecosistema

El ecosistema criminal en el segundo semestre de 2025 ha mostrado una fragmentación sin precedentes, especialmente en el ámbito del *ransomware*. En el tercer trimestre se han identificado al menos **85 grupos de *ransomware* activos**, la cifra más alta registrada hasta la fecha (Check Point Research, 2025). Este aumento no implica necesariamente más capacidad global, sino una mayor atomización del modelo *Ransomware-as-a-Service* (RaaS), con proliferación de marcas, afiliados y campañas de menor escala. Esta dinámica dificulta la atribución, reduce el efecto de las disrupciones puntuales y aumenta la volatilidad del ecosistema.

Asimismo, se ha observado una rotación constante de herramientas y servicios criminales.

La caída del **86%** en la actividad de **Lumma Stealer** en el segundo semestre respecto al primero (ESET Research, 2025) no indica una reducción del robo de credenciales, sino la rápida sustitución de herramientas tras acciones de desmantelamiento contra infraestructuras MaaS. Este patrón confirma que las operaciones policiales generan impacto, pero también aceleran la migración hacia nuevas familias de *malware*.

En conjunto, las estadísticas del segundo semestre de 2025 reflejan un ecosistema criminal más maduro, resiliente y adaptable, capaz de absorber disrupciones y reorganizarse rápidamente.

Estadísticas globales por tipo de ataque en 2025

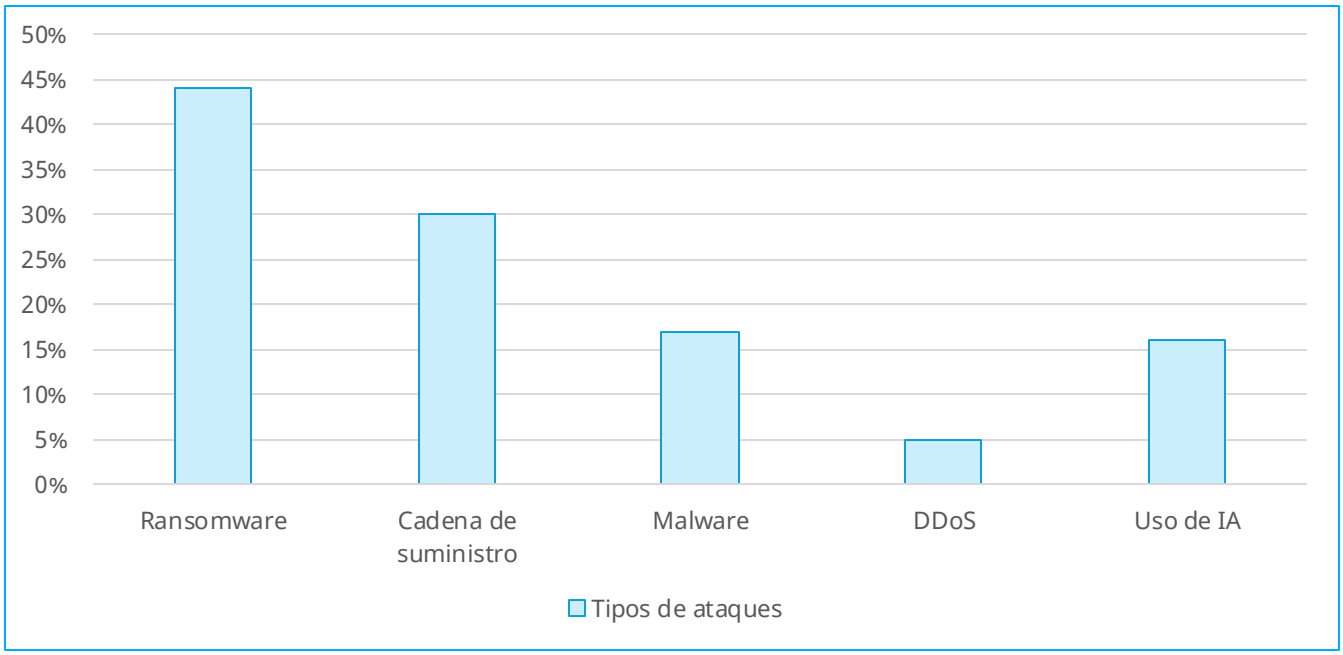


Figura 4 | Frecuencia de los ataques por tipo durante 2025.

4.4 Costes de los ciberataques para las empresas

En 2025, la estimación del impacto económico del cibercrimen se ha situado en el entorno de los **10,5 billones de USD** anuales, confirmando su carácter de riesgo sistémico para las organizaciones.

A nivel operativo, el incidente más frecuente ha sido el ***ransomware*** y, aunque la demanda media de rescate se ha situado en torno a los **115.000 USD**, el **64 %** de las organizaciones opta por no pagar, lo que desplaza el peso económico hacia costes indirectos como la **disrupción operativa**, la recuperación técnica y las consecuencias legales y reputacionales, promediándose un coste total por incidente de **5,08 millones de USD**, añadiendo los periodos de interrupción y recuperación.

A nivel mundial, el **coste medio de una brecha de datos ha alcanzado los 4,44 millones de USD**, un **9%** menor a la media de 2024. En el caso concreto de **Estados Unidos,** la cifra ha ascendido hasta los **10 millones de USD** en sectores regulados como el sanitario, el financiero o las infraestructuras críticas. **Oriente Medio** registra un coste medio por brecha de aproximadamente **7,3 millones de USD**, aunque con una reducción del **18%** respecto a 2024, atribuida a mayores inversiones en ciberseguridad y al uso de defensas basadas en IA. En contraste, Europa presenta un coste medio en torno a los **4 millones de USD**, influido por marcos regulatorios de protección de datos más consolidados y una mayor estandarización de los procesos de respuesta.

A nivel estructural, en 2025 se han identificado algunos factores clave que operan como multiplicador del impacto económico. Los **incidentes que afectan a terceros** son los que más incrementan el coste, con un sobrecoste medio de **227.000 USD**.

A estos les siguen las **arquitecturas de seguridad excesivamente complejas (+207.000 USD)** y el uso de **TI en la sombra (+200.000 USD)**, que dificultan la detección y la respuesta. Además, el **uso malicioso de la IA** o la **ausencia de un gobierno** adecuado de esta tecnología añade en torno a **193.000 USD** al coste medio de una brecha. Destaca especialmente el fenómeno de ***Shadow AI***, cuyo uso no supervisado puede incrementar el impacto económico en aproximadamente **670.000 USD** adicionales por incidente.

Por el contrario, las organizaciones que aplican medidas de seguridad integradas desde el diseño han conseguido reducir de forma significativa el impacto económico. La adopción de **DevSecOps** reduce el coste medio en **227.000 USD**, el uso de analítica de seguridad basada en **IA/ML** en **223.000 USD**, los programas sólidos de **inteligencia de amenazas** en **211.000 USD** y el **cifrado** extensivo de datos en **208.000 USD**. En conjunto, el uso de IA y automatización en la defensa permite una reducción media de costes del **34%**, poniendo de relieve una brecha cada vez mayor entre organizaciones con alta madurez en ciberseguridad y aquellas con enfoques más reactivos (Khalil, 2025).

Las estimaciones de mercado publicadas durante 2025 han situado el **gasto mundial** en seguridad de la información y gestión de riesgos en torno a los **213.000 millones de USD**, lo que representaría un crecimiento interanual cercano al **14%** (Stamford, 2025).

Este dato refleja una realidad clave del segundo semestre: el aumento sostenido de la inversión en seguridad como respuesta a la complejidad creciente del entorno de amenazas, sin que ello se traduzca aún en una reducción proporcional del impacto económico de los incidentes.

Aunque este informe se centra en las tendencias observadas durante el segundo semestre de 2025, las estadísticas utilizadas corresponden a datos agregados de todo el año. Estas cifras se emplean como referencia para contextualizar las dinámicas consolidadas a lo largo de 2025 y facilitar su interpretación en el cierre del ejercicio.

5. 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 segundo 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.

5.1 Principales leyes en el ámbito de la ciberseguridad

En el segundo semestre de 2025, el marco legal y normativo en materia de ciberseguridad ha experimentado una evolución significativa a escala global, impulsada por la necesidad de reforzar la resiliencia digital, mejorar la gobernanza tecnológica y armonizar las obligaciones regulatorias entre sectores y jurisdicciones. Durante este periodo, distintos organismos nacionales e internacionales han publicado o puesto en vigor nuevas leyes, estrategias nacionales y estándares técnicos que consolidan la transición desde un enfoque meramente preventivo hacia uno de cumplimiento verificable y supervisión activa.

Entre los avances más relevantes destacan la plena aplicación del **Reglamento DORA** en la Unión Europea, las reformas legislativas en Italia, Singapur y Brasil, y la actualización de marcos internacionales de referencia como **ISO/IEC 27001** y las guías del **NIST**, que establecen las bases de una convergencia regulatoria global en ciberseguridad.

Continente	Normativa	Institución	Referencias
América del Norte	**NIST SP 800-53 – Release 5.2.0** (27-ago-2025)	NIST / CSRC	Aviso y resumen de cambios del release 5.2.0.
	NIST SP 800-88 Rev.2 – Sanitización de soportes (IPD 21-jul-2025; publicación final sep-2025) **Obsoleto**	NIST / CSRC	NIST Computer Security Resource Center
	NIST SP 800-18 Rev.2 – System/Privacy/SCRM Plans (IPD, junio-jul 2025)	NIST / CSRC	NIST Computer Security Resource Center
América del Sur (Brasil)	**Decreto n.º 12.573/2025 – E-Ciber (Estrategia Nacional de Ciberseguridad)** (4-ago-2025)	Presidencia de Brasil (Planalto)	Diario oficial en Planalto
Asia	**Cybersecurity (Amendment) Act 2024 – Commencement Notification 2025** (entra en vigor 31-oct-2025 varias secciones)	Gov. de Singapur (AGC / Statutes Online)	Notificación S 677/2025 con detalle de secciones y fecha sso.agc.gov.sg
	Paquete de cibercrimen y asistencia mutua (tercera lectura aprobada; rumbo a Convenio de Budapest)	Gobierno de NZ	Nota oficial (Beehive) 24-jul-2025; contexto en Min. Justicia
Europa	**DORA – RTS Subcontratación TIC** (Regl. Delegado **(UE) 2025/532**, 2-jul-2025)	Comisión Europea / EUR-Lex	Texto en DOUE
	DORA – Guía de supervisión de Proveedores TIC Críticos (CTPPs) (15-jul-2025)	ESAs (EBA/EIOPA/ESMA)	Guía conjunta publicada por las ESAs
	DORA – Hoja de ruta para designación de CTPPs (jul-2025)	ESAs (EBA/EIOPA/ESMA)	Nota/roadmap oficial
	RED/EN 18031 (serie) – estándares de ciberseguridad armonizados (aplicables desde 1-ago-2025)	Comisión Europea / EUR-Lex	Decisión de Ejecución **(UE) 2025/138** que cita EN 18031-1/-2/-3 con restricciones
	Ley 132/2025 – IA (deepfakes, agravantes en cibercrimen, gobernanza) (en vigor 10-oct-2025)	República Italiana (Gazzetta Ufficiale)	Publicación oficial (GU n.º 223, 25-sep-2025)
Internacional	**ISO/IEC 27001:2022 – fin de transición** (**31-oct-2025**)	IAF / BSI (acreditación & certificación)	Línea temporal (BSI) y criterio de transición (IAF MD26)
	ISO/IEC 19790:2025 (módulos criptográficos) & **ISO/IEC 24759:2025** (ensayos)	ISO/IEC	Ficha oficial ISO 19790:2025 Ficha oficial ISO 24759:2025

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

Estas normas jurídicas y técnicas, tanto a nivel nacional como internacional, reflejan un avance significativo hacia la consolidación de un marco regulatorio global en ciberseguridad, centrado en la resiliencia operativa, la protección de infraestructuras críticas y la gestión de riesgos tecnológicos.

5.2 Principales detenciones en el ámbito de la ciberseguridad

Durante el segundo semestre de 2025, se ha mantenido un alto nivel de actividad en materia de cooperación policial y judicial internacional frente al cibercrimen. En este periodo, se han ejecutado múltiples operaciones orientadas a la neutralización de actores maliciosos y la desarticulación de infraestructuras criminales asociadas a *ransomware*, *crime-as-a-service*, *hacktivismo* y fraude financiero.

Estas acciones, coordinadas entre **Europol**, **INTERPOL**, **Eurojust**, el **Departamento de Justicia de EE. UU**. y diversos **cuerpos nacionales de seguridad**, reflejan una tendencia consolidada hacia el modelo de disrupción colaborativa, donde la inteligencia técnica y la cooperación transfronteriza resultan determinantes para impactar las capacidades operativas de los grupos criminales.

A continuación, se recoge una tabla resumen con las principales operaciones desarrolladas en el segundo semestre de 2025, destacando sus resultados y el papel de las distintas agencias implicadas:

Operación	Grupo de sector de amenazas	Fuerzas y cuerpos de seguridad	Resultados	Referencias
Eastwood	*Hacktivismo* pro-ruso (**NoName057(16)**)	Europol, Eurojust, autoridades de Alemania, Francia, España, Suecia, Suiza y EE. UU.	Desmantelamiento **>100** sistemas de infra; parte del "core" fuera de línea; **6** órdenes de arresto (DE).	Europol – Eastwood
Arresto admin XSS.is	Ecosistema *underground* / venta de accesos y *malware*	Policía Nacional de Francia, Fiscalía de París, SBU (Ucrania), Europol	Arresto del presunto admin; plataforma con **>50k** usuarios; ganancias **>€7M**.	Europol – Press Release
Checkmate (BlackSuit/Royal)	Raas / extorsión	Departamento de Justicia de EE. UU. (DOJ), FBI, socios internacionales	**4 servidores** y **9 dominios** incautados; **≈$1M** intervenido.	DOJ Press Release
Zeppelin Case	*Ransomware* / lavado de activos en cripto	DOJ (EE. UU.), FBI	Incautación **>USD 2,8M** en cripto, **USD 70k** en efectivo y un vehículo; imputación a Ianis A. Antropenko.	DOJ – Indictment Zeppelin
Contender 3.0	Fraude en línea / BEC / *phishing* masivo	INTERPOL + 25 países africanos	**260 arrestos**, **81** infra desmanteladas; **1.463** víctimas; pérdidas **≈USD 2,8M**.	INTERPOL Press Release

Tabla 3 | Principales operaciones de desmantelamiento de bandas de cibercriminales llevadas a cabo en S2 de 2025.

Operación	Grupo de sector de amenazas	Fuerzas y cuerpos de seguridad	Resultados	Referencias
Serengeti 2.0	Ciberdelincuencia transnacional (*ransomware*, fraude, BEC)	INTERPOL + 18 países africanos y Reino Unido	**1.209 arrestos**, **11.432** infra maliciosas desmanteladas; **USD 97,4M** recuperados.	INTERPOL Press Release
SIMCARTEL Takedown	*Crime-as-a-Service* (SIM-box / OTP bypass / telecom fraud)	Europol, Eurojust, policía de Letonia, Austria, Estonia, Finlandia	**7 arrestos**, **1.200** SIM-box, **40.000** SIMs, **5** servidores; pérdidas **≈€4,5M (AT)** y **€420k (LV)**; 2 webs intervenidas.	Europol SIMCARTEL
Arresto caso Collins Aerospace / Aeropuertos UE	Intrusión / Disrupción en infraestructura crítica	NCA (Reino Unido), colaboración con fuerzas europeas	1 arresto en UK; investigación en curso; incidente reportado el **19 sep**.	NCA Press Release
Eurojust–Europol Fraude Cripto	Fraude de inversión / lavado de dinero	Eurojust, Europol, autoridades de Francia, Bélgica, Chipre, Alemania y España	**9 detenidos**; red que defraudó **>€600M** vía "investment platforms" falsas.	Eurojust Case Release
Endgame – fase nov-2025	*Malware/Crime-as-a-Service* (ecosistema Rhadamanthys *infostealer*, VenomRAT RAT, Elysium *botnet*)	Europol, Eurojust y LEAs de 10 países (incl. EE. UU., Reino Unido, DE, FR, CA, AU, NL, GR)	**1.025 servidores** desmantelados/perturbados; **20 dominios incautados;** principal sospechoso de **VenomRAT arrestado en Grecia (03-nov-2025)**	Europol (oficial) BleepingComputer The Hacker News
Arresto en Phuket (Tailandia)	APT/Estado-patrocinado (espionaje) – presuntos vínculos con *Void Blizzard/ColdRiver* (prensa)	Cyber Crime Investigation Bureau (Tailandia) en coordinación con FBI (EE. UU.)	**1 detenido (06-nov-2025);** dispositivos incautados; inicio de **trámite de extradición a EE. UU.**	AP (NPR/AP syndication)
US DOJ – Account Takeover Fraud	Fraude financiero	Departamento de Justicia de EE. UU. (DOJ), FBI	Incautación de dominio e infraestructura; base de datos con credenciales robadas; pérdidas estimadas **≈USD 14,6M**; **más de 5.100 víctimas**.	DOJ Press Release
Sentinel	Fraude en línea / BEC / *ransomware*	INTERPOL + 19 países africanos	**574 arrestos**; **≈USD 3M recuperados**; desmantelamiento de redes criminales transnacionales y cierre de infra maliciosa.	INTERPOL Press Release

Tabla 3 | Principales operaciones de desmantelamiento de bandas de cibercriminales llevadas a cabo en S2 de 2025.

Caso destacado: Operación Eastwood — Desmantelamiento de la red *hacktivista* pro-rusa NoName057(16)

Durante el mes de julio de 2025, **Europol**, en colaboración con **Eurojust** y las autoridades policiales de Alemania, Francia, España, Suecia, Suiza y Estados Unidos, ejecutó la "**Operación Eastwood**", dirigida contra la red **NoName057(16)**, una de las organizaciones de *hacktivismo* pro-ruso más activas desde el inicio de la guerra en Ucrania (EUROPOL, 2025).

El grupo era responsable de miles de ataques DDoS coordinados contra infraestructuras críticas, entidades gubernamentales y medios de comunicación europeos, principalmente en países que apoyan a Ucrania.

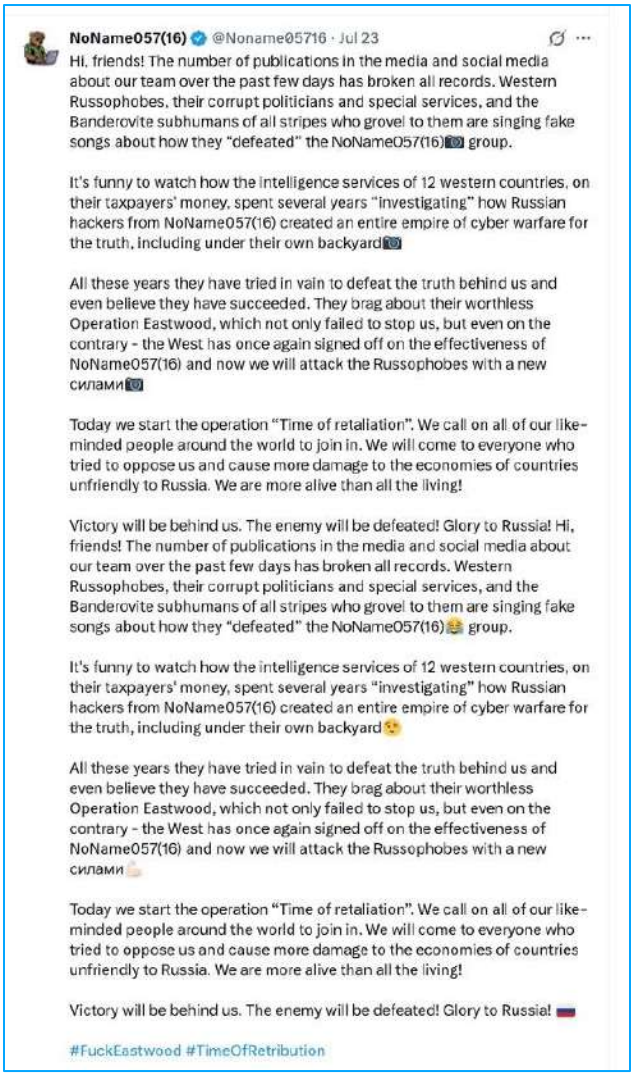
La operación permitió desmantelar una infraestructura distribuida compuesta por más de un centenar de servidores utilizados para coordinar ataques y gestionar la plataforma DDoSIA, empleada por el grupo para automatizar campañas de denegación de servicio mediante un modelo de "voluntariado gamificado".

Además, se emitieron siete órdenes internacionales de detención (seis de ellas en Alemania) contra individuos identificados como miembros clave del grupo, y se practicaron dos arrestos en territorio europeo (Francia y España).

Las investigaciones también permitieron identificar a más de un millar de usuarios activos en los canales de reclutamiento de Telegram, muchos de los cuales recibían incentivos económicos en criptomonedas por participar en las ofensivas.

La relevancia de la **Operación Eastwood** trasciende el plano técnico. Representa un hito en la cooperación internacional frente al *hacktivismo* coordinado, al ser la primera operación multinacional que logra neutralizar una red de este tipo mediante la combinación de capacidades judiciales, policiales y de ciberinteligencia.

El enfoque de las agencias participantes refleja una madurez operativa: se priorizó la neutralización de la infraestructura, la persecución de responsables y la desarticulación del modelo de financiación y reclutamiento digital que sostenía la campaña.



NoName057(16) @Noname05716 · Jul 23

Hi, friends! The number of publications in the media and social media about our team over the past few days has broken all records. Western Russophobes, their corrupt politicians and special services, and the Banderovite subhumans of all stripes who grovel to them are singing fake songs about how they "defeated" the NoName057(16) group.

It's funny to watch how the intelligence services of 12 western countries, on their taxpayers' money, spent several years "investigating" how Russian hackers from NoName057(16) created an entire empire of cyber warfare for the truth, including under their own backyard

All these years they have tried in vain to defeat the truth behind us and even believe they have succeeded. They brag about their worthless Operation Eastwood, which not only failed to stop us, but even on the contrary - the West has once again signed off on the effectiveness of NoName057(16) and now we will attack the Russophobes with a new силами

Today we start the operation "Time of retaliation". We call on all of our like-minded people around the world to join in. We will come to everyone who tried to oppose us and cause more damage to the economies of countries unfriendly to Russia. We are more alive than all the living!

Victory will be behind us. The enemy will be defeated! Glory to Russia! Hi, friends! The number of publications in the media and social media about our team over the past few days has broken all records. Western Russophobes, their corrupt politicians and special services, and the Banderovite subhumans of all stripes who grovel to them are singing fake songs about how they "defeated" the NoName057(16) group.

It's funny to watch how the intelligence services of 12 western countries, on their taxpayers' money, spent several years "investigating" how Russian hackers from NoName057(16) created an entire empire of cyber warfare for the truth, including under their own backyard

All these years they have tried in vain to defeat the truth behind us and even believe they have succeeded. They brag about their worthless Operation Eastwood, which not only failed to stop us, but even on the contrary - the West has once again signed off on the effectiveness of NoName057(16) and now we will attack the Russophobes with a new силами

Today we start the operation "Time of retaliation". We call on all of our like-minded people around the world to join in. We will come to everyone who tried to oppose us and cause more damage to the economies of countries unfriendly to Russia. We are more alive than all the living!

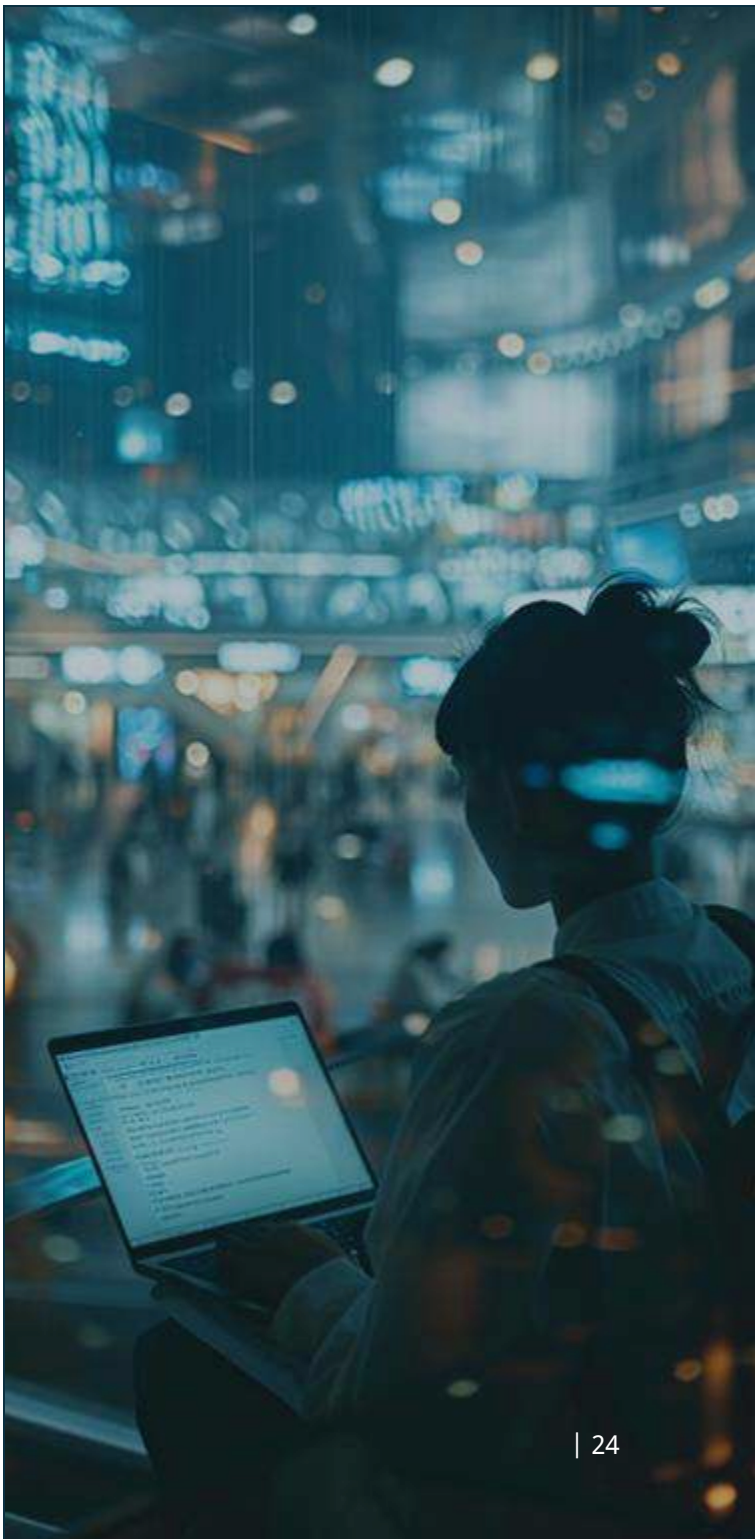
Victory will be behind us. The enemy will be defeated! Glory to Russia!

#FuckEastwood #TimeOfRetribution

Ilustración 1 | Declaración pública de intenciones de NoName057(16) y llamada a la acción contra la operación Eastwood.

En términos estratégicos, la **Operación Eastwood** demuestra la evolución del enfoque europeo frente al *hacktivismo* con motivación geopolítica, evidenciando cómo el uso de tácticas híbridas y la instrumentalización de "voluntarios digitales" se consideran ya una amenaza transnacional estructurada.

Este caso refuerza la tendencia hacia una colaboración más estrecha entre fuerzas de seguridad, organismos judiciales y socios del sector privado para responder de forma integrada a amenazas complejas que combinan motivaciones políticas, técnicas y financieras.



6. *Dark Web Insights*

Durante el segundo semestre de 2025, el ecosistema de foros *underground* ha experimentado una reconfiguración significativa impulsada por la presión sostenida de las fuerzas de seguridad, el desmantelamiento de infraestructuras críticas utilizadas por actores de alto perfil y la fragmentación de comunidades históricas.

Aunque los grandes *hubs* tradicionales continúan perdiendo tracción, emergen nuevas plataformas que absorben parte del flujo de actividad criminal, mientras que otras desaparecen o se transforman a causa de detenciones, incautaciones o conflictos internos.

Este periodo se caracteriza por tres dinámicas clave:

- **Disrupción continua de foros consolidados**, provocando migraciones masivas y pérdida de confianza entre los actores.
- **Aparición de espacios alternativos o resurgimiento de comunidades preexistentes**, que se posicionan como nuevos centros de actividad.
- **Incremento del uso de canales paralelos (Telegram, Tox, paneles privados)** ante la percepción creciente de riesgo en los foros públicos y semiprivados.

Este contexto obliga a adaptar la monitorización CTI a un entorno más distribuido y opaco, en el que el prestigio y la reputación digital se han convertido en factores críticos para acceder a inteligencia útil para la toma de decisiones.

6.1 La caída de DarkForums: el último gigante que se derrumbó

DarkForums, el heredero natural de **BreachForums** y uno de los centros neurálgicos del cibercrimen en 2025, colapsó durante el segundo semestre del año en un proceso tan acelerado como revelador.

Lo que había nacido como refugio de actores expulsados de otros foros terminó hundiéndose bajo su propio peso: creciente presión policial, conflictos internos y un deterioro técnico imposible de ocultar.

Primero llegaron los rumores de infiltración. Luego, los fallos en los sistemas de acceso, los cortes constantes y las acusaciones entre moderadores. Para septiembre, los miembros más veteranos ya recomendaban públicamente abandonar la plataforma. Para noviembre, la migración hacia Telegram, Tox y otros canales privados era masiva. **DarkForums** pasó en cuestión de semanas de ser "el nuevo **BreachForums**" a convertirse en un espacio fantasma, sin actividad ni credibilidad.

La caída de **DarkForums** no solo marca el final del último gran foro centralizado, sino que simboliza un cambio estructural en el ecosistema criminal. Los actores de amenazas, tradicionalmente activos en foros de la *deep* y *dark web*, muestran una pérdida de confianza incluso en estas infraestructuras relativamente estables y optan por entornos más fragmentados, efímeros y compartimentados, como canales privados, mercados temporales o plataformas cifradas, que resultan mucho más opacos y difíciles de monitorizar.

6.2 Foros *underground* activos

Durante el segundo semestre de 2025, el ecosistema de foros *underground* se mantiene activo a pesar de la caída de **DarkForums** y la presión policial constante sobre comunidades rusoparlantes y angloparlantes. La actividad se redistribuye hacia plataformas más fragmentadas, nichos técnicos y enclaves privados que sirven como puntos de encuentro para actores criminales de distintos niveles de sofisticación.

A continuación, se destacan los foros más relevantes y operativos en este periodo.

- **Exploit.in**: con más de 15 años de actividad, **Exploit.in** sigue siendo el epicentro del cibercrimen técnico rusoparlante. Es uno de los pocos foros con continuidad real después de múltiples caídas de otros espacios, y mantiene una comunidad altamente experimentada donde circulan *0-days*, *exploits* RCE, *kits* de intrusión y accesos iniciales de alto valor.
- **Dread: Dread** ha recuperado su actividad tras meses de inestabilidad por ataques *DDoS* y volvió a convertirse en el gran ***hub* social** del *darknet*. Actúa como un "Reddit clandestino" donde se discuten caídas de *markets*, reputación de *vendors*, análisis de operaciones policiales y alertas de *scams*.
- **Cracked.io:** tras resurgir con fuerza después de *Operation Talent*, **Cracked.io** sigue siendo uno de los foros con **mayor volumen de actividad** en el ecosistema angloparlante. Su contenido está dominado por credenciales expuestas, configuraciones para *stealers*, herramientas automatizadas, *leaks* y tutoriales de intrusión de bajo/medio nivel.
- **Nulled.to:** considerado históricamente uno de los mayores foros de *cracking* y filtraciones, **Nulled.to** mantiene una base sólida de usuarios dedicada a compartir bases de datos filtradas, manuales técnicos, *scripting* malicioso y herramientas de ataque de fácil adopción.
- **Sinister.ly:** combina estética de cultura *hacker* con contenidos técnicos orientados a *phishing*, *carding*, automatización ofensiva y desarrollo en Python. Esta mezcla lo hace popular entre perfiles jóvenes que comienzan a adentrarse en el ecosistema, sirviendo como una **"academia informal"** donde se comparten técnicas accesibles pero efectivas.
- **RAMP (*Ransomware Affiliate Market Place*):** aunque no es un foro tradicional, **RAMP** sigue siendo un punto crítico para la **comunidad de *ransomware* y programas RaaS**. Durante 2025 alberga anuncios de reclutamiento de afiliados, pruebas de paneles y venta de accesos utilizados para intrusiones asociadas a grupos de *ransomware*.
- **Ecosistema post-XSS: subforos fragmentados y clanes rusos:** tras la caída de **XSS.is**, surgieron varios foros fragmentados y comunidades sucesoras que intentan ocupar el espacio dejado por el que fue uno de los mayores foros criminales rusoparlantes.
- **RuTor / Ru.Tor:** no es un foro criminal en sentido estricto, pero su comunidad semiclandestina funciona como un entorno donde circulan *malware* ligero, herramientas de *carding*, servicios antifraude, métodos para *cashout* y *scripts* para automatización delictiva.
- **KernelForum / Kern3l:** un foro técnico avanzado centrado en *malware development*, *reversing*, *loaders*, *crypters* y OPSEC ofensivo. Aunque su tamaño es reducido, la calidad técnica de sus usuarios lo convierte en un espacio donde a menudo aparecen técnicas nuevas antes de que se utilicen en campañas reales.
- **Comunidades especializadas en *botnets* y *stealers* (R0 Crew, etc.):** existen foros pequeños dedicados específicamente a ***cracking* de paneles de *stealers***, intercambio de configuraciones para *botnets* populares (RedLine, Lumma, Raccoon, etc.) y venta de *logs*. Aunque modestos en volumen, son muy útiles para identificar nuevas variantes, patrones de distribución y evoluciones en el ecosistema de *malware* commoditizado.
- **KickAss Forum:** un foro emergente que ha ganado relevancia entre desarrolladores de *malware* por su enfoque en *loaders*, *crypters*, paneles personalizados y *malware* privado. Cada vez más utilizado por actores que buscan herramientas más "premium" sin exponerse en foros masivos.

Durante el segundo semestre de 2025 se observa un cambio en la actividad de la *dark web*, marcado por el aumento de la venta de *logs* y accesos comprometidos, impulsado por infecciones de *malware infostealer* y por la creciente demanda de credenciales robadas.

Principales publicaciones en el *dark web* en S2 2025

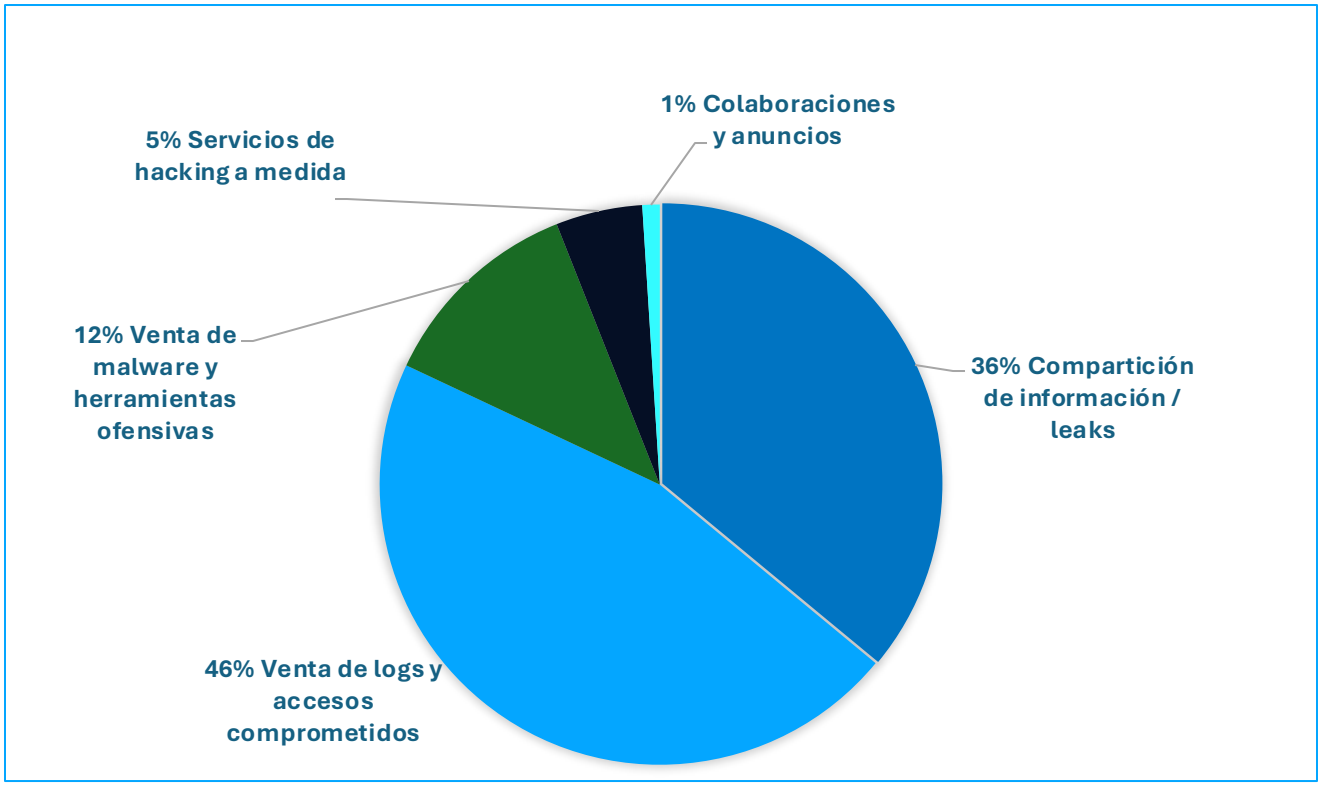


Figura 5 | Principales categorías de publicaciones en la *dark web* en el segundo semestre de 2025.

Los datos estimados evidencian un ecosistema criminal cada vez más orientado hacia la **monetización de accesos** y la explotación de credenciales, mientras que las filtraciones públicas pierden peso debido a la fragmentación de los foros tradicionales. A su vez, la actividad en ***malware* y herramientas ofensivas** continúa al alza, consolidando estas categorías como elementos clave del segundo semestre de 2025.

6.3 Mercados *underground* activos

Durante el segundo semestre de 2025, el ecosistema de mercados *underground* ha seguido mostrando una actividad sostenida, aunque con cambios estructurales relevantes respecto a periodos anteriores. Las disrupciones de *marketplaces* generalistas no han supuesto una reducción del volumen criminal, sino una **reconfiguración del ecosistema**, caracterizada por una mayor fragmentación, especialización funcional y una creciente dependencia de mercados orientados a datos, accesos y servicios asociados a intrusión.

Los ***logs* de *infostealers*** continúan siendo uno de los activos más demandados dentro del *underground*. Familias como **Lumma, RisePro** y **RedLine** siguen siendo recurrentes en este ecosistema, con grandes volúmenes de credenciales en circulación y una clara priorización de la actualización frecuente del inventario. Este modelo refuerza el papel de los mercados como proveedores directos de acceso inicial, estrechamente conectados con campañas de *ransomware* y fraude.

Mercados consolidados

- **Russian Market:** se mantiene como uno de los principales ***hubs* de credenciales robadas y *stealer logs***. Su modelo de actualización constante y su elevada rotación de inventario lo convierten en un actor clave dentro de la cadena de suministro criminal, especialmente para *Initial Access Brokers* (IAB) y operadores de *ransomware*.
- **Brian's Club:** continúa siendo un **referente histórico del *carding***, con un volumen relevante de tarjetas comprometidas. Aunque el *carding* pierde peso relativo frente a la venta de accesos y credenciales, sigue siendo un mercado estructural dentro del ecosistema de fraude financiero.
- **Exodus Market:** gana relevancia como mercado orientado a la **venta de accesos privilegiados, *exploits* y servicios asociados a intrusión**, con especial foco en entornos corporativos. Destaca por la implementación

de mecanismos de reputación y verificación más estrictos, indicativos de una profesionalización creciente.

Mercados en declive o caídos

- **Abacus Market:** tras su protagonismo durante el primer semestre de 2025, el mercado sufrió **disrupciones críticas en julio**, finalizando con su caída. Las señales observadas apuntan a un probable *exit scam,* reforzando la tendencia de inestabilidad de los DNMs generalistas y la pérdida de confianza en plataformas centralizadas.
- **Plataformas generalistas de corta vida:** durante el periodo analizado se han observado múltiples *marketplaces* de escasa duración, con ciclos de vida reducidos y bajo volumen, que no llegan a consolidarse como actores relevantes dentro del ecosistema.

Mercados emergentes y espacios alternativos

- **Exploit.in:** se consolida como uno de los principales foros orientados a la **venta de accesos iniciales** (RDP, VPN, credenciales corporativas y accesos persistentes). Durante el segundo semestre de 2025 se observa un incremento de ofertas relacionadas con entornos empresariales, reforzando su papel como espacio de referencia para IAB.
- **2easy Market:** *marketplace* especializado en ***logs*** **de** ***infostealers*** **y credenciales robadas**, con una fuerte presencia de accesos corporativos reutilizables. Su modelo operativo, centrado en la disponibilidad y búsqueda de credenciales recientes, incrementa su valor para actores que operan en fases tempranas de intrusión.
- **Styx Market:** mercado orientado a herramientas y servicios para campañas de *phishing*, *kits* y soporte operativo para la distribución de *malware*. Durante este periodo mantiene una actividad relevante como **plataforma de apoyo** a operaciones de intrusión.
- **B1ack's Stash:** identificado como un **mercado emergente de *carding***, orientado a la venta de tarjetas robadas y *dumps* recientes. Su aparición refleja la atomización del fraude financiero, con plataformas de vida corta, alta agresividad comercial y rápida monetización.
- **TorZon Market:** DNM generalista que ha absorbido parte del tráfico residual tras la caída de otros *marketplaces*, aunque sin alcanzar una posición dominante. Su actividad refleja el **desplazamiento parcial del tráfico** hacia alternativas menos consolidadas.
- **Otros mercados y espacios fragmentados:** incluye foros IAB de bajo perfil, servicios privados de búsqueda de *logs*, reventas de *datasets* derivados (incluidos modelos heredados de mercados desmantelados) y **canales cerrados accesibles por invitación**. Esta categoría refleja el elevado grado de fragmentación y descentralización observado en el segundo semestre.

Evolución del ecosistema de mercados *underground*

Durante este semestre se ha observado una **redistribución significativa de la actividad** respecto al primer semestre de 2025, marcada principalmente por la caída de *marketplaces* generalistas y el aumento del peso relativo de plataformas orientadas a accesos, credenciales y servicios de intrusión.

La desaparición previa de actores como **Abacus Market** y **Breach Forums** no ha supuesto una reducción del volumen criminal, sino un desplazamiento de la actividad hacia mercados especializados, foros IAB-*centric* y canales privados, así como hacia entornos menos visibles y más difíciles de monitorizar. En este contexto, plataformas como **Russian Market**, **Exploit.in** y mercados especializados como **Exodus Market** han incrementado su relevancia operativa.

Asimismo, se observa una **mayor fragmentación del ecosistema**, con la aparición de múltiples mercados de nicho, especialmente en ***carding*** y venta de accesos iniciales, caracterizados por ciclos de vida más cortos, menor visibilidad pública y una rápida rotación de inventario.

Durante el segundo semestre de 2025, varios de estos actores han estado frecuentemente asociados a campañas de intrusión y *ransomware*, actuando como proveedores de accesos iniciales, credenciales robadas y datos reutilizables. Este modelo refuerza el papel de **los mercados *underground* como infraestructura crítica dentro de la cadena de valor del cibercrimen**, más allá de su función tradicional como simples plataformas de compraventa.

En cuanto a la **comunicación operativa**, aunque **Telegram** continúa siendo una plataforma de referencia, se ha identificado un incremento sostenido en el uso de canales privados y aplicaciones cifradas *end-to-end* (como Signal, TOX y soluciones descentralizadas). Esta tendencia responde a una mayor percepción de riesgo por parte de los actores criminales y a la búsqueda de menor exposición a infiltraciones, incautaciones de infraestructura y monitorización OSINT.

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

Plataformas de venta *underground* en S2 2025

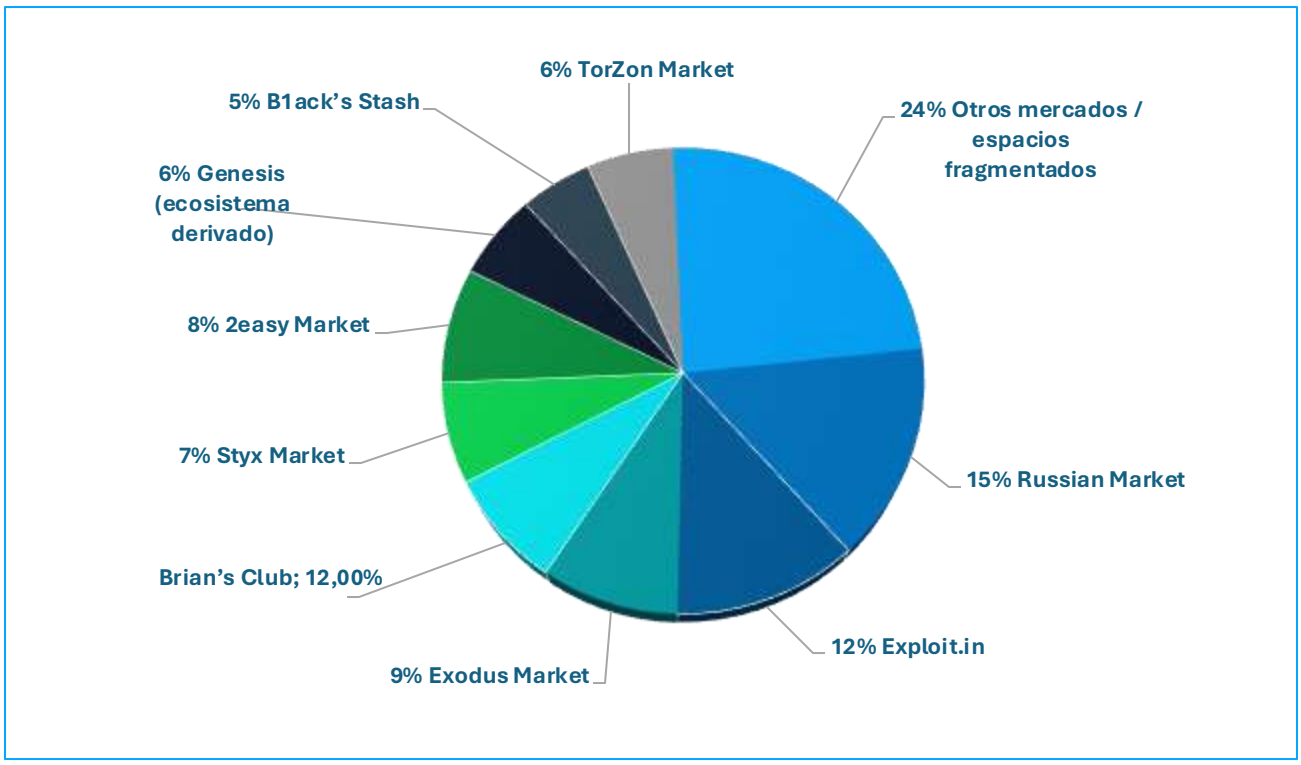


Figura 6 | Principales plataformas de venta *underground* identificadas en el segundo semestre de 2025.

7. Actores de amenaza *(Threat Actors)*

El semestre ha confirmado un ecosistema más híbrido y difícil de atribuir, donde cibercrimen, espionaje y *hacktivismo* convergen en técnicas, infraestructura y objetivos.

Con predominio de la exfiltración selectiva, la ingeniería social avanzada y el abuso de servicios legítimos, mientras han proliferado pequeños grupos ágiles y alianzas temporales que comparten TTPs y amplifican el impacto de sus operaciones.

7.1 Nuevos actores identificados

En el informe del semestre pasado se anticipó un aumento en la colaboración entre grupos criminales, así como una convergencia progresiva entre cibercrimen y ciberespionaje. Los nuevos actores identificados en este periodo han confirmado plenamente esa evolución: colectivos pequeños, altamente dinámicos y con estructuras flexibles que combinan técnicas de extorsión, intrusiones silenciosas y explotación de accesos legítimos. Su actividad ha dibujado un panorama más fragmentado, en el que la separación entre motivaciones financieras y operativas se ha difuminado y la exfiltración selectiva de datos se ha consolidado como el vector dominante.

FulcrumSec

Detectado en septiembre de 2025, **FulcrumSec** se distingue por centrarse exclusivamente en la extorsión mediante la exfiltración de datos, **sin desplegar *ransomware***, para, posteriormente publicarlos en su sitio de *leaks* (*clearnet* y *dark web*) o canal de Telegram, con la intención de vender la base a un solo comprador y maximizar beneficio. Su principal objetivo son empresas de alto perfil, hasta la fecha se han confirmado públicamente dos víctimas relevantes dentro del **sector tecnológico**, dedicadas a la distribución global de componentes y soluciones, aunque en su "muro de la fama" confirma haber obtenido acceso a datos altamente sensibles (PII) y secretos corporativos de, al menos, una decena de corporaciones globales multimillonarias, a través de *backends* públicamente expuestos. Sin embargo, su canal de Telegram y su sitio de la *dark web* están inactivos, aparentemente desde principios de noviembre, sin confirmación de su completa desaparición o parón temporal para la preparación de nuevos ataques (Shenouda, 2025).

NetMedved

Este actor fue identificado a mediados de octubre de 2025 como responsable de una campaña dirigida principalmente a empresas en Rusia. Su táctica incluye ***phishing*** con correos que contienen archivos ZIP con accesos engañosos (archivo *LNK* disfrazado de factura o petición comercial), con el fin de desplegar *malware* **NetSupportRAT** para espionaje o movimientos posteriores dentro de la red. Esa combinación de ingeniería social, abuso de herramientas legítimas como *scripts* de PowerShell, múltiples dominios de entrega y persistencia sugiere una evolución táctica más refinada, posiblemente heredada de campañas anteriores (Shenouda, 2025) (AlienVault, 2025).

Zestix

Zestix es un actor emergente en diciembre de 2025, centrado en la **exfiltración y venta directa de datos**, sin uso de *ransomware*. Su operación más destacada es el acceso a información legal y de clientes de Mercedes-Benz USA a través de la cadena de suministro, comprometiendo a terceros que gestionaban documentación sensible. El grupo demuestra reconocimiento previo, selección de archivos de alto valor (estrategias legales, reclamaciones, datos corporativos) y una monetización rápida mediante foros clandestinos. También se le han atribuido dos ventas de bases de datos con información de proyectos de una compañía turca de robótica y una industrial de mecánica y gas de Perú. Su actividad refleja una tendencia creciente: actores nuevos y poco estructurados que combinan técnicas clásicas de intrusión con una orientación casi de inteligencia corporativa, priorizando accesos indirectos y datos estratégicos sobre volúmenes masivos (Shenouda, 2025).

7.2 *Ransomware*

El *ransomware* ha evolucionado hacia modelos de extorsión basados en datos, mayor autonomía de afiliados y una expansión global sostenida. Las alianzas entre colectivos han reforzado la coordinación, la compartición de recursos y el aumento de campañas de presión pública, consolidando un ecosistema más profesionalizado y orientado a maximizar visibilidad y monetización.

7.2.1 Nuevos grupos

La distribución temporal ha mostrado un ecosistema en expansión, pero altamente volátil (DarkFeed, 2025). Julio y agosto concentraron el mayor volumen de nuevos grupos, reflejando una fase de entrada de actores oportunistas y de consolidación de modelos de extorsión basados en datos, con **SLH** como hito que acelera la

cooperación entre colectivos. Septiembre introdujo una capa de especialización, con grupos orientados a nichos (cripto, filtraciones selectivas, *branding* agresivo), señal de madurez y segmentación del mercado criminal. A partir de octubre, ha aumentado el ruido operativo con *rebrandings* y grupos efímeros, mientras que en noviembre disminuyó la cantidad, pero creció la definición técnica de los nuevos actores. En conjunto, el patrón ha confirmaso un semestre marcado por proliferación temprano-media, diversificación en el punto central y especialización hacia el cierre del periodo.

Figura 7 | Grupos de *ransomware* detectados en el segundo semestre de 2025.

Este semestre ha destacado el colectivo **Scattered LAPSUS$ Hunters (SLH)**, que representa una fusión operativa entre tres de los grupos criminales más notorios: **Scattered Spider, LAPSUS$ y ShinyHunters**. Emergió en agosto de 2025 como un modelo federado de extorsión y exfiltración de datos. Bajo este paraguas, han compartido canales en Telegram para coordinar operaciones, reclutar afiliados y amplificar campañas de presión pública, reflejando una estructura híbrida entre cibercrimen y estrategia de marca en el *underground*. SLH opera principalmente con **extorsión como servicio (*EaaS*)**, convocando a asociados para exigir pagos a cambio del uso de su reputación consolidada, y ha utilizado técnicas clásicas de ingeniería social, *spear-phishing*, SIM *swapping* y compromiso de plataformas como Salesforce para obtener accesos iniciales y exfiltrar datos sensibles. Esta alianza ha ilustrado una tendencia preocupante de colaboración más estrecha entre colectivos previamente independientes, con intercambio de tácticas y recursos que dificulta la atribución y eleva el impacto de las campañas de extorsión global (Lakshmanan, 2025).

7.2.2 Grupos más activos

La actividad de *ransomware* en el segundo semestre ha mantenido un nivel alto y estable, pero con un rasgo más marcado que en semestres anteriores: fragmentación operativa y movilidad de afiliados, reflejando un mercado RaaS más maduro, descentralizado y competitivo.

- **Qilin**: se ha consolidado como el principal polo de atracción de afiliados del semestre. Su crecimiento no ha respondido tanto a innovación técnica disruptiva como a su capacidad para capitalizar la desestabilización de otros RaaS, ofreciendo continuidad operativa, infraestructura estable y monetización fiable. Representa un modelo de *ransomware* industrializado y escalable, más cercano a una plataforma que a un grupo tradicional.
- **Akira**: ha mantenido una presencia constante en el *top* sin picos abruptos, lo que sugiere un núcleo de afiliados estable y campañas bien integradas en el mercado RaaS. Su persistencia refuerza la tendencia hacia operaciones sostenidas de bajo riesgo, priorizando continuidad y rentabilidad frente a visibilidad o expansión agresiva.
- **INC Ransomware**: ha destacado como ejemplo de crecimiento acelerado durante el semestre, con una orientación clara hacia objetivos de alto impacto operativo. Su evolución apunta a una estrategia de posicionamiento rápido mediante campañas más selectivas, lo que lo convierte en un actor relevante para explicar el desplazamiento del foco hacia sectores críticos y entornos con mayor presión temporal para la negociación.

- **Play**: ha reforzado su papel como actor de volumen constante, alineado con campañas menos sofisticadas pero sostenidas en el tiempo. Su comportamiento encaja con un ecosistema en el que la rentabilidad proviene de la repetición y la estandarización, más que de la innovación técnica o la especialización sectorial.
- **Safepay**: ha mostrado una evolución irregular, con una reducción progresiva de su actividad hasta noviembre, seguida de un repunte abrupto en diciembre. Este patrón sugiere una estrategia de reactivación selectiva coherente con un crecimiento controlado y una menor exposición operativa, centrada en organizaciones medianas y en la explotación de superficies de ataque menos saturadas por los grandes operadores RaaS.

Top grupos de *ransomware* del S2 2025

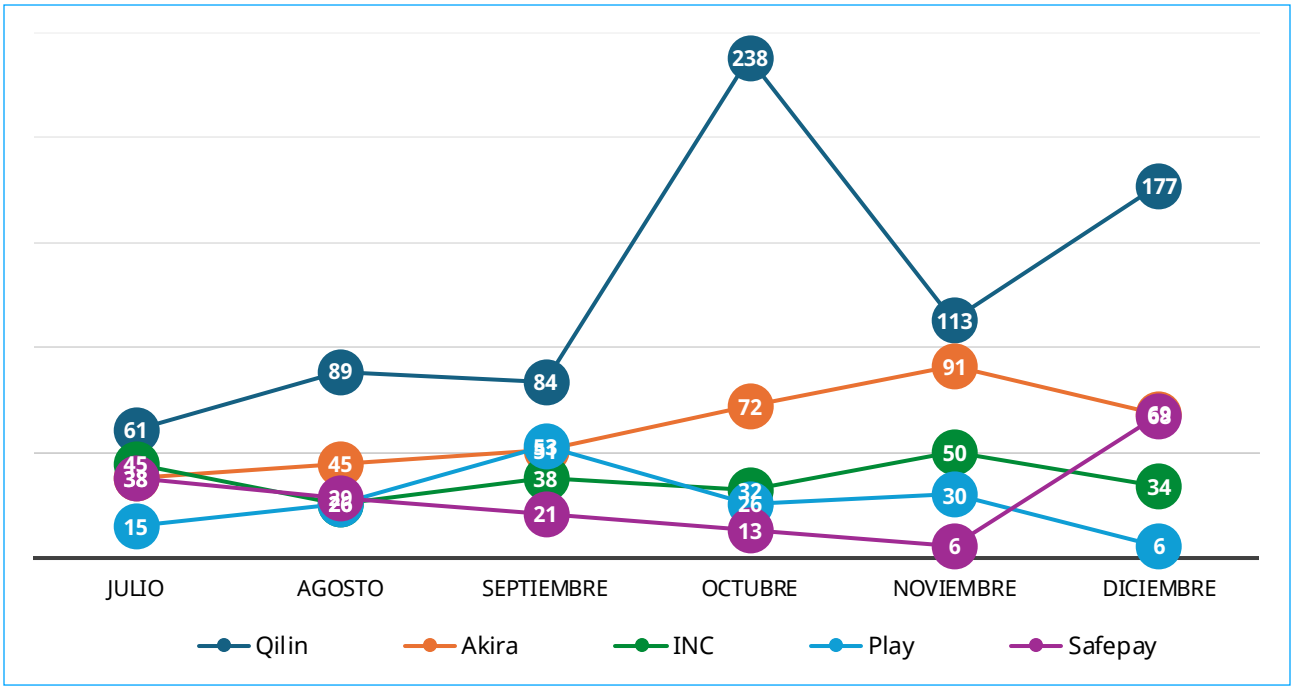


Figura 8 | Actividad de los grupos de *ransomware* más activos en el segundo semestre de 2025.

7.2.3 Afectación global

La distribución geográfica de las víctimas confirma que los grupos de *ransomware* han seguido concentrando su actividad en economías desarrolladas, con un claro epicentro en **Estados Unidos** y una expansión progresiva hacia Europa, Asia-Pacífico y, en menor medida, Oriente Medio. En los datos de julio a diciembre, Estados Unidos se mantuvo de forma constante como primer objetivo (de 280 a 461 incidentes mensuales)(DarkFeed, 2025), consolidándolo como "capital mundial del *ransomware*" por valor de los activos, madurez digital y capacidad de pago, más que por población o tamaño de mercado.

En segundo nivel se han situado un bloque de países occidentales con elevada exposición: **Reino Unido, Alemania, Francia, Canadá, España e Italia** han mostrado cifras sostenidas y, en algunos casos, un crecimiento notable en el trimestre (por ejemplo, Canadá y Francia triplicando sus cifras en octubre). Este patrón encaja con una victimización concentrada en Norteamérica y Europa, donde se combinan cadenas de suministro complejas, alta dependencia de servicios digitales y marcos regulatorios que obligan a notificar incidentes, lo que aumenta la visibilidad estadística.

A partir de septiembre se observó además una diversificación hacia Asia-Pacífico y otras regiones: aparecieron con más peso Corea del Sur, India, Tailandia, Japón y Australia, mientras que en octubre se registró también actividad significativa en Emiratos Árabes Unidos, señalando una extensión de las campañas hacia Oriente Medio.

En estas regiones el modelo RaaS y la fragmentación del ecosistema ha facilitado campañas simultáneas en múltiples geografías.

En conjunto, la tendencia del segundo semestre ha apuntado a un doble eje: concentración del volumen total en Estados Unidos y países occidentales, como se comentó en el anterior informe, pero con un foco de operaciones cada vez más globalizado, en el que los afiliados rotan infraestructuras y listas de víctimas entre regiones para maximizar presión, evitar saturar defensas locales y aprovechar ventanas regulatorias o de madurez de ciberseguridad desiguales entre países.

Países más afectados por *ransomware* del S2 2025

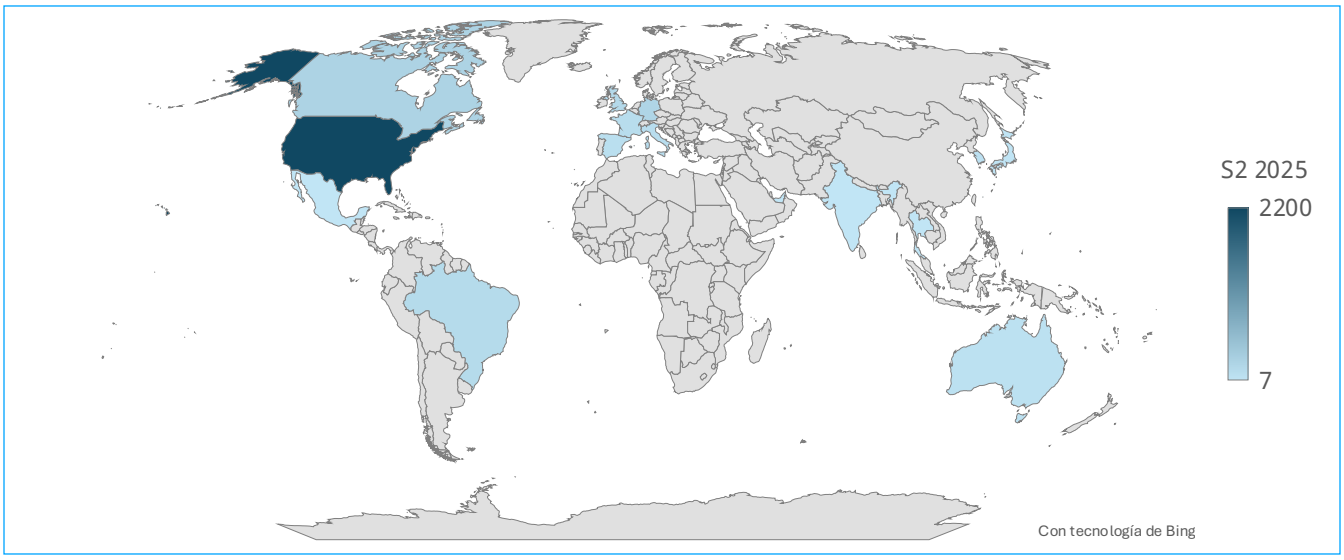


Figura 9 | Países más afectados por *ransomware* en el segundo semestre de 2025.

Por otro lado, el análisis sectorial del segundo semestre de 2025 ha confirmado una concentración sostenida del impacto del *ransomware* en sectores con alta dependencia operativa y baja tolerancia a la interrupción, más que en aquellos simplemente más digitalizados. **Consultoría** (servicios profesionales + legal) ha sido el principal sector agregado del semestre, con crecimiento claro a partir de octubre. **Manufactura** ha mantenido una presión constante y transversal, impulsada por la exposición de entornos híbridos IT/OT, la criticidad de sistemas industriales y el elevado coste asociado a paradas de producción. A este núcleo se han sumado ***retail*** y **consumo discrecional**, especialmente sensibles a la estacionalidad del segundo semestre, y **servicios IT y profesionales**, cuyo atractivo reside en su capacidad de generar impacto en cadena sobre múltiples organizaciones.

Desde una perspectiva estructural, el semestre ha evidenciado una madurez estratégica del ecosistema *ransomware*: los actores priorizan sectores donde la presión temporal, regulatoria o reputacional acelera la toma de decisiones por parte de la víctima. **Salud**, **administración pública** y **educación** han mantenido una afectación constante, no por volumen, sino por su valor coercitivo, mientras que el peso persistente del sector refuerza la tendencia hacia ataques orientados al impacto operativo más que a la mera explotación masiva. El aporte diferencial respecto a semestres anteriores no es un cambio de sectores objetivo, sino una optimización del *targeting*, con campañas mejor alineadas con ciclos de negocio y una presión más sostenida, anticipando una continuidad de este patrón de riesgo de cara a 2026.

Ataques de *ransomware* por sector en S2 2025

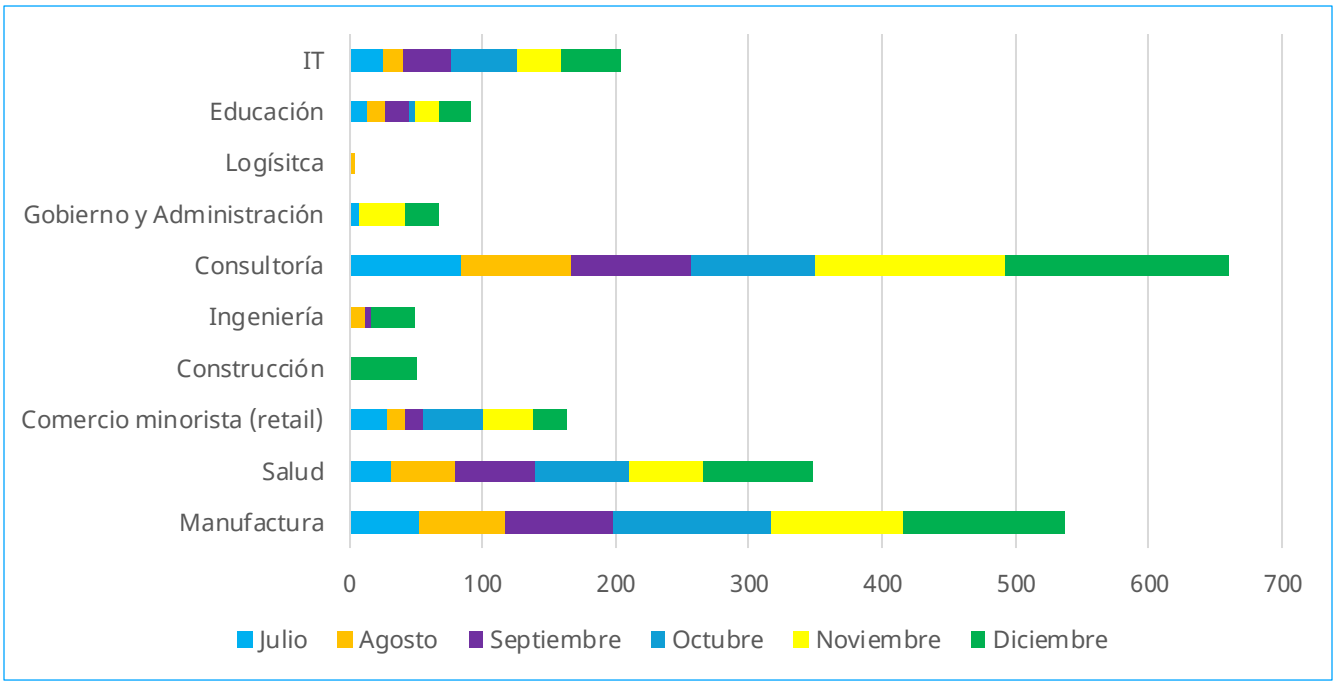


Figura 10 | Sectores más afectados por *ransomware* en el segundo semestre de 2025.

7.3 *Hacktivismo*

Durante el segundo semestre se ha observado una intensificación clara del fenómeno *hacktivista*, caracterizada no tanto por la aparición de nuevos actores, sino por la **consolidación de modelos de coordinación entre grupos** y una mayor alineación con agendas geopolíticas definidas (FalconFeeds.io, 2025).

El ecosistema se ha articulado en torno a bloques regionales y afinidades ideológicas, destacando, por un lado, el entorno prorruso, estructurado alrededor de colectivos como **NoName057(16)** y **Anonymous Russia**, que han operado como nodos de coordinación y agregación de capacidades. Estos grupos han actuado como vertebradores de campañas distribuidas, orientadas principalmente contra infraestructuras, instituciones y entidades asociadas a países de la OTAN y a Ucrania.

En paralelo, se ha consolidado un segundo bloque en el entorno Asia–Pacífico, especialmente activo en el sudeste asiático y articulado alrededor de **BD Anonymous, Nullsec Philippines y Cyber Team Indonesia**, donde múltiples colectivos han operado bajo una lógica federada, compartiendo recursos, narrativas y objetivos, y permitiendo la ejecución de campañas regionales de mayor alcance y persistencia, compensando capacidades técnicas limitadas mediante volumen, continuidad y coordinación en ventanas temporales concretas.

Un tercer eje lo han conformado actores alineados con la causa palestina y con otras corrientes ideológicas afines de carácter antioccidental y político-religioso, como **Al-Mujahideen Force 313, Red Eye of Palestine y Cyber Islamic Resistance** que han incrementado progresivamente su nivel de cooperación transregional. Estos grupos han mostrado una mayor interconexión con otros *clusters* geográficos, lo que amplifica su visibilidad y su impacto, especialmente en momentos de alta tensión geopolítica.

El análisis realizado permite identificar además varios **grupos conectores** que han actuado como nodos de alto grado y han facilitado la difusión de TTPs e infraestructura entre ecosistemas: **BD Anonymous** es el actor más repetido en las alianzas del periodo; **NoName057(16) y Dark Storm Team** con su rol como *hub* del entorno pro-ruso; **Keymous+** y **Clobelsec** enlazan de forma estable grupos de Bangladesh, Oriente Medio, Europa y Rusia; mientras que **Hezi Rash, Hider_Nex** o **LunarisSec** refuerzan el entramado técnico en la parte final del semestre.

La actividad observada ha confirmado un perfil orientado a la disrupción y la presión simbólica más que al espionaje profundo, con ataques DDoS, *defacements*, filtraciones selectivas y acciones de amplificación propagandística, con una fuerte reutilización de infraestructuras, herramientas conocidas y reivindicación cruzada entre grupos para maximizar visibilidad.

En conjunto, el segundo semestre ha confirmado la evolución del *hacktivismo* hacia un modelo más organizado, coordinado y persistente, basado en alianzas flexibles entre grupos **fuertemente reactivas al contexto geopolítico**, con capacidad para sostener campañas prolongadas y dirigir ataques contra objetivos de alto valor simbólico y operativo. Este patrón refuerza el riesgo de acciones sincronizadas y de mayor impacto contra infraestructuras críticas y entidades estratégicas en múltiples regiones.

Supernodos de grupos *hacktivistas*

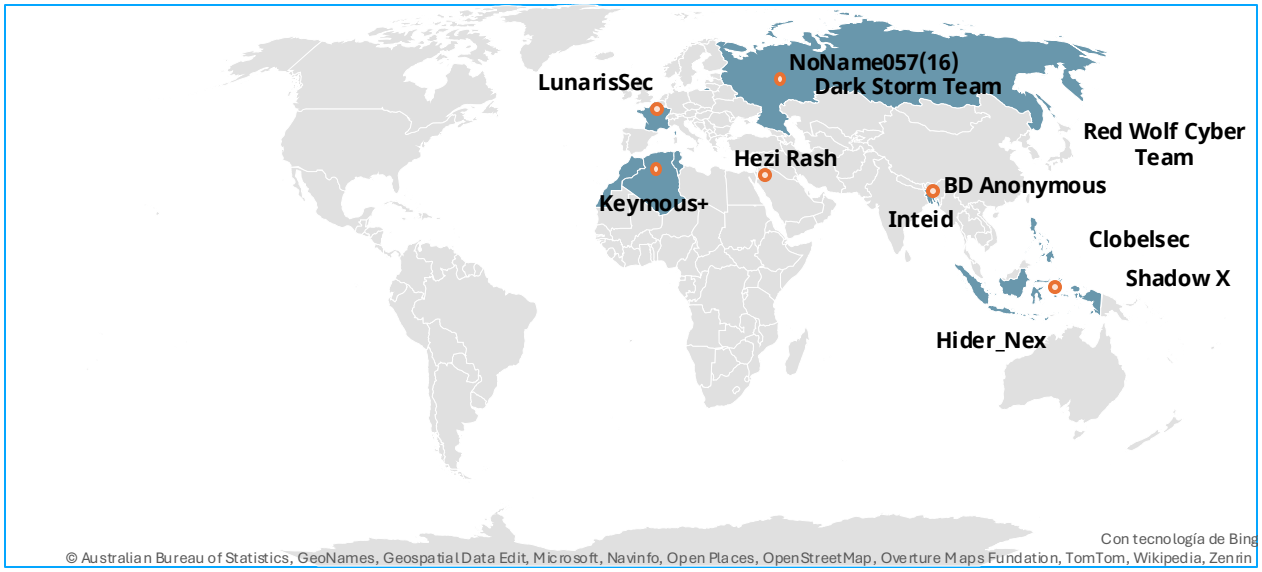


Figura 11 | Grupos conectores *hacktivistas* por ubicación geográfica.

7.4 APT

Entre julio y diciembre de 2025 se ha consolidado un patrón muy claro: mayor sofisticación técnica, ampliación geográfica de las campañas y un énfasis creciente en compromisos de largo plazo que aporten ventajas estratégicas, tanto geopolíticas como económicas (ESET Research, 2025).

- **APT rusos**

El segundo semestre ha reflejado una transición desde la agresividad abierta del primer semestre hacia una estrategia de infiltración prolongada con campañas activas centradas principalmente en Ucrania y estados europeos. Entre los actores destacados, **RomCom** explotó una vulnerabilidad *0-day* en **WinRAR (CVE-2025-8088)** para distribuir *malware* y establecer accesos persistentes, mientras que **Gamaredon** ha seguido siendo uno de los grupos con mayor volumen de actividad, caracterizado por campañas masivas de *spear-phishing*, el uso intensivo de *malware* personalizado y una elevada rotación de infraestructuras, orientadas al espionaje táctico y a la recopilación de inteligencia en entidades gubernamentales ucranianas y europeas. **Sandworm** ha mantenido su perfil de operaciones destructivas y de interrupción mediante el despliegue de *wipers* como **ZEROLOT** y **Sting** contra entidades gubernamentales, energéticas y logísticas. También se ha identificado la actividad del *cluster* **InedibleOchotense**, centrado en *spear-phishing* con *payloads* que combinan herramientas legítimas y *backdoors* propios. Finalmente, el ecosistema *hacktivista* ha mostrado una menor convergencia operativa que en el primer semestre: las campañas de DDoS y las filtraciones de información han seguido siendo frecuentes, pero se ha observado una reducción de las operaciones coordinadas a nivel técnico y una mayor fragmentación en la ejecución de las acciones.

- **APT chinos**

Las campañas identificadas durante el segundo semestre han mostrado una diversificación de objetivos, principalmente transporte, gobiernos, manufactura y educación. Ha aumentado la persistencia, más que la variedad de nuevas capacidades: se han priorizado operaciones de inteligencia política y estratégica con ciclos operativos largos. Se ha observado una actividad intensa de grupos como **Mustang Panda, Flax Typhoon, Speccom y FamousSparrow,** este último especialmente activo en América Latina con intrusiones en múltiples gobiernos. Ha destacado el incremento en el uso de técnicas *adversary-in-the-middle* (AitM) para el acceso inicial y movimiento lateral, así como la explotación de *routers*, actualizaciones y otros vectores de confianza para desplegar *backdoors*, observado en grupos como **SinisterEye** y **PlushDaemon**. En comparación con el primer semestre, no se ha detectado un equivalente a las grandes piezas de *malware* (como fue **NanoSlate**), sino una optimización incremental del arsenal existente.

- **APT iraníes**

El foco iraní se ha desplazado hacia la infiltración e ingeniería social con técnicas más creíbles y difíciles de detectar, reforzando la tendencia global de persistencia encubierta. **MuddyWater** ha destacado por intensificar sus campañas globales de *spear-phishing* mediante el uso de buzones internos comprometidos para enviar correos maliciosos, una técnica ya identificada en el primer semestre. Otros actores como **BladedFeline** (parte de **OilRig**) y **GalaxyGato** han evolucionado su arsenal, incorporando *DLL-search-order hijacking* y nuevas versiones de *backdoors* como **C5**, diseñados para el robo de credenciales, persistencia y evasión. Los objetivos principales han seguido siendo organismos gubernamentales y sectores estratégicos en Oriente Medio, aunque con expansión hacia Europa y Asia Central, consolidando una presencia más amplia y técnica en el ámbito del espionaje.

- **APT norcoreanos**

Los grupos vinculados a Corea del Norte han sostenido una actividad elevada, combinando espionaje y operaciones dirigidas a generar ingresos para el Estado, consolidando un modelo híbrido APT–crimen. Actores como **Lazarus, Kimsuky, DeceptiveDevelopment y Konni** mantienen campañas diversificadas, dirigidas a gobiernos, diplomacia, tecnología y especialmente al sector de criptomonedas.

Este semestre se ha observado una colaboración sin precedentes entre **Kimsuky** y **Lazarus**, que combinan capacidades de espionaje y explotación técnica en campañas coordinadas globales. **Kimsuky**, especializado en reconocimiento y exfiltración de inteligencia vía *spear-phishing* sofisticado,

inicia intrusiones con correos dirigidos (ej. invitaciones académicas con *malware* FPSpy y *keylogger*) para mapear redes y recolectar credenciales. Una vez comprometido el entorno, Lazarus aprovecha vulnerabilidades de día cero y distribuye paquetes maliciosos que consiguen privilegios SYSTEM y despliegan el *backdoor* InvisibleFerret, diseñado para evasión de EDR y exfiltración de activos de alto valor (incluyendo cripto).

Ambos grupos usan una infraestructura compartida para la coordinación, ejecución y limpieza de huellas y han apuntado a sectores críticos como defensa, finanzas, energía y *blockchain*. Esta alianza ha reforzado la tendencia hacia operaciones APT más integradas, donde la combinación de técnicas de espionaje y ciberdelito financiero incrementa la eficacia de las campañas (De Jong, 2025).

Según las estadísticas observadas (NSFOCUS, 2025), las claves que han marcado el periodo son:

Tendencias clave observadas en grupos APT en S2 2025

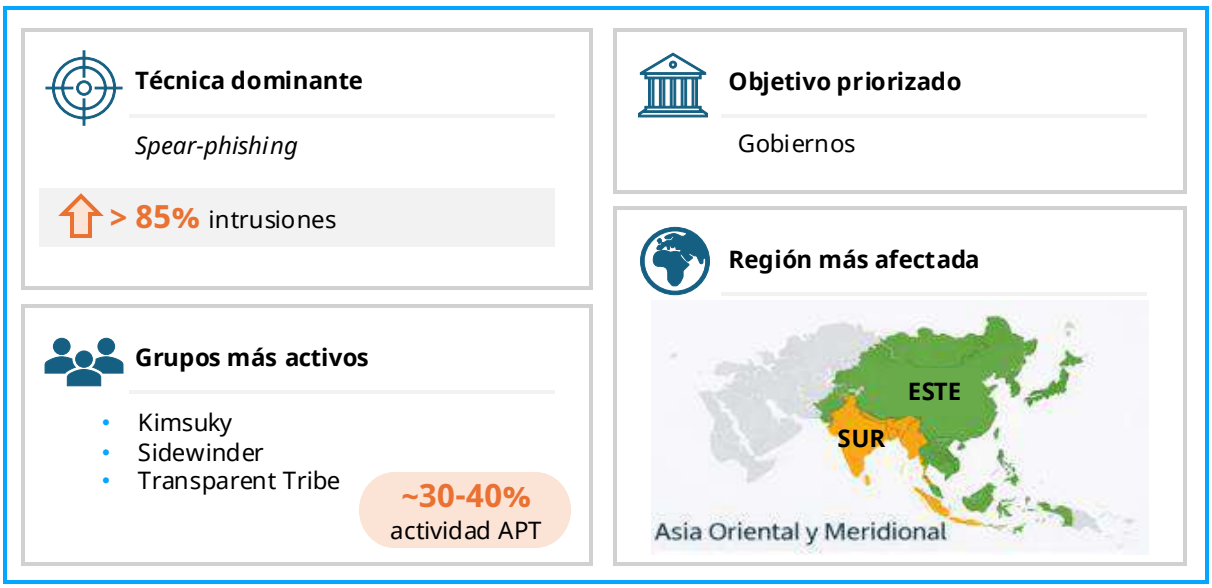


Figura 12 | Tendencias clave de grupos APT durante el segundo semestre de 2025.

El análisis del segundo semestre de 2025 ha confirmado un predominio de campañas de espionaje persistente por parte de las APT alineadas con China, Corea del Norte y los grupos del sur de Asia, frente a un mayor componente disruptivo y destructivo en actores vinculados a Rusia y, en menor medida, Irán. Esta diferenciación operativa, condicionada por el contexto geopolítico, permite identificar patrones claros por región y anticipar una evolución hacia intrusiones más prolongadas, sigilosas y orientadas a la obtención de ventajas estratégicas a medio y largo plazo.

8. Tácticas, Técnicas y Procedimientos (TTPs)

Durante el segundo semestre de 2025, el equipo **de Cyber Threat Intelligence de NTT DATA** ha analizado la evolución de las tácticas, técnicas y procedimientos (TTPs) empleadas por grupos cibercriminales y actores con motivaciones geopolíticas. El análisis confirma una tendencia clara: los atacantes no dependen mayoritariamente de técnicas radicalmente nuevas, sino de la combinación de TTPs conocidas ejecutadas con mayor velocidad, escala y automatización, apoyadas cada vez más por herramientas basadas en inteligencia artificial.

Los datos recopilados en informes de referencia del sector muestran que el cibercrimen con motivación económica continúa dominando el panorama global, representando más del **70%** de las intrusiones interactivas observadas en el último año (CrowdStrike, 2025). En este contexto, el *ransomware*, la extorsión múltiple, el abuso de identidades y la explotación de infraestructuras expuestas siguen siendo los pilares operativos de la mayoría de las campañas.

8.1 Descripción de las TTP más comunes utilizadas por los cibercriminales

En comparación con el primer semestre de 2025, las TTPs observadas durante el segundo semestre no introducen técnicas nuevas dentro del marco MITRE ATT&CK, pero sí muestran **un cambio en su uso y combinación**. Se observa un mayor peso de técnicas orientadas a **persistencia, acceso a credenciales y evasión de defensas**, frente a enfoques más directos y ruidosos del semestre anterior. Asimismo, aumenta la relevancia del **abuso de identidades válidas y servicios remotos**, especialmente en entornos *cloud*, y se consolida la **exfiltración de datos como paso previo al *ransomware***, reforzando los esquemas de doble extorsión.

En conjunto, el segundo semestre refleja una **mayor madurez operativa de los atacantes**, más centrada en mantener accesos y maximizar el impacto que en desplegar técnicas novedosas.

Táctica	MITRE ATT&CK ID	Descripción
Persistencia (TA0003)	T1098 – Manipulación de cuentas	Los atacantes modifican cuentas existentes (usuarios locales, cuentas *cloud* o de servicio) para mantener acceso persistente y dificultar la detección.
	T1136.001 – Crear cuenta: Cuenta local	Creación de cuentas locales adicionales para asegurar persistencia tras el acceso inicial.
	T1547.001 – Ejecución al inicio: Claves del Registro / Carpeta de inicio	Establecimiento de persistencia mediante claves de inicio automático en sistemas Windows.
	T1133 – Servicios remotos externos	Uso de servicios expuestos (RDP, VPN, aplicaciones web) para acceder o persistir en el entorno comprometido.
	T1098.004 – Manipulación de cuentas: Claves de nube adicionales	Adición de claves, *tokens* o credenciales en entornos *cloud* para mantener acceso persistente.
Escalada de privilegios (TA0004)	T1134 – Manipulación de *tokens* de acceso	Uso indebido de tokens para ejecutar acciones bajo un contexto de mayor privilegio.
	T1548 – Abuso de mecanismos de elevación de privilegios	Aprovechamiento de configuraciones débiles o controles inadecuados para elevar privilegios.

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

Táctica	MITRE ATT&CK ID	Descripción
Evasión de defensas (TA0005)	T1562.001 – Deshabilitar o modificar herramientas de seguridad	Desactivación de antivirus, EDR o mecanismos de protección para evitar la detección.
	T1562.004 – Modificar o deshabilitar *firewall* del sistema	Alteración de reglas de *firewall* para facilitar la comunicación del atacante.
	T1070.001 – Eliminación de indicadores: Borrado de registros	Eliminación de *logs* del sistema para ocultar rastros de la intrusión.
	T1564.008 – Ocultar artefactos: reglas de ocultación de correo electrónico	Uso de reglas de correo para ocultar comunicaciones maliciosas o exfiltración de datos.
Acceso a credenciales (TA0006)	T1003 – Volcado de credenciales del SO	Extracción de credenciales almacenadas en memoria o archivos del sistema.
	T1552 – Credenciales sin proteger	Obtención de credenciales almacenadas en texto claro, *scripts* o configuraciones.
	T1528 – Robo de *tokens* de acceso a aplicaciones	Robo de tokens válidos para acceder a aplicaciones y servicios remotos.
Descubrimiento (TA0007)	T1046 – Descubrimiento de servicios de red	Enumeración de servicios y puertos para identificar objetivos adicionales.
	T1082 – Descubrimiento de información del sistema	Obtención de detalles sobre sistema operativo y *hardware*.
	T1016 – Descubrimiento de configuración de red	Identificación de topología y conexiones de red mediante comandos nativos.
	T1057 – Descubrimiento de procesos	Enumeración de procesos activos para identificar *software* de seguridad u objetivos críticos.
	T1087.001 – Descubrimiento de cuentas: Cuenta local	Enumeración de cuentas de usuario locales para facilitar movimientos posteriores.
Movimiento lateral (TA0008)	T1021 – Servicios remotos	Uso de RDP, SMB u otros servicios para desplazarse lateralmente dentro de la red.
Exfiltración (TA0010)	T1041 – Exfiltración sobre canal de mando y control	Exfiltración de datos a través de canales ya establecidos con el atacante.
Impacto (TA0040)	T1486 – Cifrado de datos para impacto	Cifrado de sistemas y archivos como parte de campañas de *ransomware*.
	T1490 – Inhibición de recuperación del sistema	Eliminación o desactivación de copias de seguridad para impedir la recuperación.

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

8.2 Vectores de entrada más usuales

Durante el segundo semestre de 2025, los vectores de entrada empleados por los cibercriminales mantienen una clara continuidad con los observados en el primer semestre. No obstante, el análisis realizado por el equipo de **Cyber Threat Intelligence de NTT DATA** confirma que la relevancia de estos vectores no reside en su novedad técnica, sino en su **consolidación como mecanismos de acceso inicial silenciosos, persistentes y de baja visibilidad**.

A diferencia de periodos anteriores, el acceso inicial se apoya cada vez menos en la explotación directa de vulnerabilidades visibles y más en **identidades, credenciales legítimas, confianza organizativa y servicios correctamente configurados pero abusados**. Este desplazamiento dificulta la detección temprana y reduce la capacidad de diferenciar entre actividad legítima y maliciosa desde las primeras fases de la intrusión

Identidad como vector de acceso	**Ingeniería social orientada a identidad**	**Entornos *cloud* y APIs**
El abuso de identidades válidas se consolida como uno de los principales mecanismos de acceso inicial. Los atacantes utilizan credenciales robadas, *cookies* de sesión y *tokens* de acceso para operar sin desplegar *malware*, reduciendo significativamente la visibilidad y aumentando el tiempo de detección. Este vector favorece intrusiones prolongadas y facilita el movimiento lateral desde fases tempranas.	Uso de técnicas de ingeniería social dirigidas a obtener credenciales o consentimiento del usuario, incluyendo *vishing*, suplantación de soporte técnico, campañas BEC y abuso de flujos habituales de autenticación. Este vector explota la confianza en procesos cotidianos y permite el acceso inicial sin necesidad de explotación técnica directa.	Incremento de accesos iniciales mediante errores de configuración en entornos *cloud*, permisos excesivos, claves API expuestas y abuso de relaciones de confianza entre servicios. Este vector es especialmente relevante en arquitecturas híbridas y *multicloud*, donde la visibilidad y el control son más limitados.
***Infostealers* avanzados**	***Software* no autorizado / *shadow* IT**	**Abuso de servicios remotos legítimos**
Evolución del uso de *infostealers* como fase previa estructural a ataques de *ransomware*, fraude y accesos no autorizados. El robo automatizado de credenciales, *cookies* y datos del navegador posiciona este vector como uno de los más eficaces del semestre, tanto por su escalabilidad como por su bajo coste operativo.	Uso de herramientas profesionales y *software* descargado fuera de canales oficiales como puerta de entrada inicial. Este vector aprovecha la presión operativa y la confianza en aplicaciones aparentemente legítimas, introduciendo accesos persistentes y reduciendo la capacidad de detección y actualización de seguridad.	Uso de RDP, VPN y herramientas de administración remota con credenciales válidas como mecanismo de acceso inicial. Este vector permite a los atacantes operar mediante servicios legítimos, minimizando la huella técnica del acceso y complicando la detección temprana por parte de los equipos defensivos.

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

En conjunto, durante el segundo semestre de 2025 el acceso inicial deja de apoyarse principalmente en fallos técnicos evidentes y se orienta cada vez más hacia **identidades, confianza y uso legítimo de servicios**. Este enfoque incrementa la dificultad de detección temprana y eleva el impacto potencial de los ataques, al permitir a los adversarios establecer accesos iniciales que no generan alertas inmediatas ni comportamientos claramente anómalos.

Esta evolución refuerza la necesidad de abordar la seguridad del acceso inicial desde una perspectiva que combine **controles técnicos, gestión de identidades, visibilidad sobre entornos *cloud* y supervisión de procesos humanos**, sentando las bases para comprender la evolución operativa que se desarrolla en el apartado de innovación en ataques.

8.3 Innovación en ataques: nuevas técnicas y tácticas

Durante el segundo semestre de 2025, la innovación en las campañas de ciberataque no se ha manifestado en la aparición de técnicas radicalmente nuevas dentro del marco MITRE ATT&CK, sino en un **cambio estructural en la lógica operativa del atacante**. A diferencia de los enfoques más directos y oportunistas observados en el primer semestre, el segundo semestre consolida un modelo basado en **persistencia, automatización y explotación sistemática de la confianza**, donde el objetivo no es únicamente comprometer sistemas, sino **integrarse de forma prolongada en los procesos normales de la organización**.

Este cambio no se expresa en la fase de acceso inicial, descrita en el apartado de vectores de entrada, sino en la manera en que los atacantes **operan una vez dentro del entorno comprometido**, gestionan el tiempo, reducen señales de detección y maximizan el impacto final.

De ataques ruidosos a operaciones prolongadas y de bajo perfil

Una de las principales diferencias respecto al primer semestre es la **reducción deliberada del ruido técnico**.

Los atacantes priorizan cada vez más técnicas *hands-on-keyboard*, el uso de herramientas legítimas del sistema y la ejecución manual asistida, frente al despliegue masivo de malware persistente. Informes de *threat hunting* confirman que una proporción creciente de intrusiones interactivas se desarrolla sin implantar *malware* tradicional, lo que dificulta la detección temprana y alarga significativamente el tiempo de permanencia en los entornos comprometidos (CrowdStrike, 2025).

En este contexto, el **tiempo se convierte en un activo estratégico del atacante**. La permanencia prolongada permite comprender el entorno, identificar activos críticos, observar patrones operativos y preparar el impacto final con mayor precisión. Este enfoque marca una transición clara desde campañas oportunistas hacia **operaciones selectivas**, donde el valor no está en la velocidad inicial, sino en la capacidad de permanecer sin ser detectado y de fragmentar las señales defensivas entre múltiples dominios (identidad, *endpoint* y *cloud*).

Industrialización del *ransomware* y consolidación de la extorsión múltiple

Durante el segundo semestre, el *ransomware* deja de ser una técnica puntual de impacto para consolidarse como un **proceso empresarial altamente estructurado**. Los datos disponibles indican que los ingresos globales asociados a pagos por *ransomware* superan los 2.000 millones de dólares, lo que evidencia la madurez económica y organizativa del modelo (Financial Crimes Enforcement Network [FinCEN], 2025).

La innovación no reside en el cifrado en sí, sino en la **orquestación integral de la campaña**. Los atacantes automatizan la clasificación de la información robada, seleccionan de forma prioritaria los datos más sensibles y emplean filtraciones parciales y escalonadas como mecanismo de negociación. Este modelo refuerza los esquemas de doble y triple extorsión y reduce la dependencia del cifrado como único medio de presión, permitiendo obtener beneficios incluso sin interrumpir completamente la operación de la víctima.

La inteligencia artificial como acelerador táctico, no como sustituto

A diferencia del primer semestre, donde la inteligencia artificial aparecía principalmente como tendencia emergente, durante el segundo semestre de 2025 se observa su **integración práctica y sistemática en distintas fases del ataque**. La IA se utiliza para acelerar tareas concretas: generación de contenido de ingeniería social, adaptación lingüística y cultural, análisis de información previa sobre la víctima o apoyo al desarrollo y modificación de herramientas maliciosas (IBM Security, 2025).

En el ámbito del *malware*, se han documentado casos de herramientas desarrolladas o ajustadas con apoyo de IA para reducir errores de código, mejorar la ofuscación o adaptar *payloads* a distintos entornos operativos (ESET, 2025; Garaschenko, 2025). No obstante, estos desarrollos siguen requiriendo supervisión humana, lo que confirma que la IA **no sustituye al operador**, sino que **reduce el coste cognitivo y operativo del ataque**, permitiendo escalar campañas con menos esfuerzo y mayor rapidez.

Explotación de la confianza y de los procesos organizativos como vector operativo

Un elemento claramente diferencial del segundo semestre es la **instrumentalización de procesos organizativos legítimos como parte central de la táctica de ataque**. Más allá del acceso inicial, los atacantes utilizan procesos como la contratación, la colaboración técnica, el trabajo remoto o el uso cotidiano de herramientas profesionales para **normalizar su presencia dentro de la organización**.

Se han identificado campañas en las que actores maliciosos emplean identidades sintéticas y asistencia basada en IA para superar entrevistas técnicas, integrarse en equipos de trabajo y mantener accesos prolongados a sistemas internos. Este tipo de tácticas desplaza el foco desde la infraestructura tecnológica hacia la **confianza operativa y cultural**, ampliando de forma significativa la superficie de ataque y difuminando la frontera entre amenaza externa e interna (CrowdStrike, 2025).

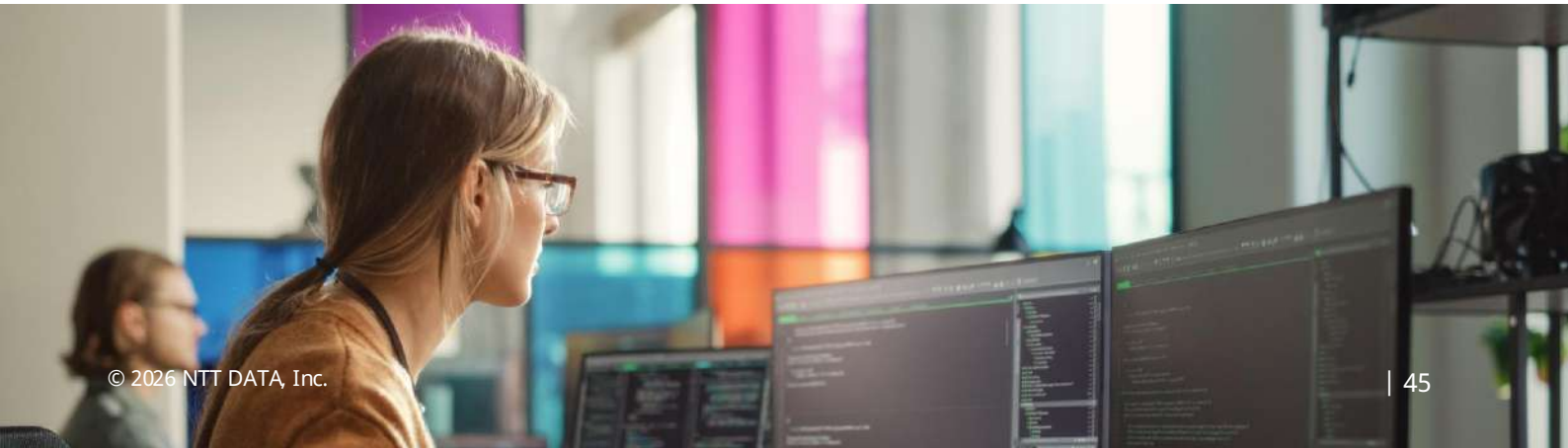
Velocidad de explotación y presión temporal sobre la defensa

El segundo semestre también consolida una **reducción drástica del margen de reacción defensiva**. La explotación de vulnerabilidades críticas se produce cada vez con mayor rapidez tras su divulgación pública, integrándose de forma casi inmediata en campañas automatizadas. Este comportamiento incrementa la presión sobre los equipos defensivos y penaliza especialmente a organizaciones con ciclos de parcheo lentos, visibilidad limitada o dependencia de procesos manuales (Arctic Wolf, 2025; Wright, 2025)

La combinación de automatización, inteligencia artificial y especialización criminal convierte la divulgación pública de una vulnerabilidad en una **carrera asimétrica**, donde los atacantes pueden reaccionar más rápido que muchas organizaciones defensivas.

En conjunto, el segundo semestre de 2025 marca una evolución cualitativa respecto al primero: **menos foco en el acceso inicial y más énfasis en cómo operar dentro de la organización sin ser detectado**. La innovación no se expresa en nuevas técnicas aisladas, sino en la combinación de persistencia, automatización, inteligencia artificial y abuso de la confianza para ejecutar ataques más selectivos, duraderos y rentables.

Esta dinámica refuerza la necesidad de abordar la ciberseguridad no solo desde la tecnología, sino desde una perspectiva integral que incluya **procesos, cultura organizativa y capacidades de detección contextual**, capaces de interpretar señales débiles y operaciones distribuidas en múltiples dominios.



9. Vulnerabilidades

El segundo semestre de 2025 consolidó a las vulnerabilidades críticas como uno de los principales vectores de compromiso inicial, con un patrón claro de explotación rápida, campañas dirigidas y uso recurrente de *0-days*. La actividad observada refleja una reducción sostenida del tiempo entre la divulgación, e incluso antes de ella, y la explotación activa, evidenciando una elevada madurez operativa de los actores de amenazas.

Durante este periodo la explotación no se limitó a ataques oportunistas, sino que se integró en **campañas estructuradas**, combinando acceso inicial, movimiento lateral y persistencia.

A continuación, se presenta un análisis mensual de las vulnerabilidades más destacadas del periodo, como base de orquestación de las grandes campañas detectadas.

- **Julio:**

La vulnerabilidad conocida como **SharePoint ToolShell Exploitation** hace referencia a una campaña de explotación dirigida contra servidores **Microsoft SharePoint** en entornos locales que no estaban correctamente parcheados. Esta campaña se basó en el aprovechamiento de fallos críticos de seguridad que permitían a un atacante ejecutar código de forma remota y realizar técnicas de suplantación, comprometiendo completamente el sistema afectado.

Inicialmente, la explotación se asoció a las vulnerabilidades identificadas como **CVE-2025-49706 y CVE-2025-49704**, que posteriormente fueron ampliadas y correlacionadas con los identificadores **CVE-2025-53770 y CVE-2025-53771**. Estas vulnerabilidades afectaban específicamente a instalaciones *on-premises* de **SharePoint**, lo que incrementaba el riesgo en organizaciones que no aplicaban las actualizaciones de seguridad de manera oportuna.

La campaña fue atribuida a varios actores de amenazas avanzadas. Entre ellos destaca **Storm-2603**, un actor de *ransomware* vinculado a China, así como el grupo **Threat Group-3390** y **ZIRCONIUM**, este último asociado principalmente a actividades de ciberespionaje. La diversidad de actores implicados evidencia el alto valor estratégico de estas vulnerabilidades y su uso tanto con fines económicos y de inteligencia.

La información y atribución de esta campaña se encuentra documentada por **MITRE ATT&CK**, donde se recoge como una campaña específica de explotación bajo el identificador correspondiente, sirviendo como referencia para el análisis y la mitigación de este tipo de amenazas (MITRE, 2025).

- **Agosto:**

La vulnerabilidad de **Directory Traversal** en **WinRAR** corresponde a un fallo crítico de seguridad identificado en la versión para Windows de este *software* de compresión. Esta debilidad permitía a un atacante manipular las rutas internas de archivos comprimidos para escribir o ejecutar ficheros fuera del directorio previsto, lo que abría la puerta a la ejecución de código arbitrario en el sistema de la víctima.

La vulnerabilidad fue registrada como **CVE-2025-8088** y se explotaba mediante archivos comprimidos especialmente diseñados. Al ser abiertos por el usuario, estos archivos permitían la instalación silenciosa de código malicioso sin necesidad de privilegios elevados ni interacción adicional, comprometiendo de forma directa la integridad del sistema afectado.

Este fallo fue explotado activamente a nivel global, destacando su uso por parte del grupo de amenazas **RomCom**, un actor alineado con intereses rusos. **RomCom** aprovechó esta vulnerabilidad como vector inicial de acceso para desplegar *malware* de tipo puerta trasera, facilitando el control remoto, la persistencia en los sistemas comprometidos y la posterior ejecución de actividades maliciosas.

La información técnica y el seguimiento de esta vulnerabilidad han sido documentados por diversas fuentes de inteligencia de amenazas, que alertaron sobre su explotación activa y la necesidad de actualizar WinRAR para mitigar el riesgo asociado a este vector de ataque (Strobes, 2025).

- **Septiembre:**

La vulnerabilidad de ejecución arbitraria de código en **Windows** hace referencia a un fallo de seguridad crítico que permitía a un atacante ejecutar código malicioso en sistemas afectados mediante la interacción del usuario. Comprometiendo directamente la confidencialidad, integridad y disponibilidad de los sistemas Windows vulnerables.

Esta vulnerabilidad podía ser utilizada como vector inicial de acceso, derivando en la ejecución de código y el compromiso del endpoint afectado, sin requerir necesariamente privilegios elevados.

Identificada como **CVE-2025-9491**, la vulnerabilidad fue explotada activamente antes de la publicación de un parche oficial. Su abuso afectaba a la confidencialidad, integridad y disponibilidad de los sistemas comprometidos.

La explotación de esta vulnerabilidad se atribuyó al actor de amenazas **UNC6384**, un grupo afiliado a China. Este actor dirigió sus ataques contra objetivos de alto valor, concretamente sistemas pertenecientes a diplomáticos europeos ubicados en Bélgica, Hungría y otros Estados miembros de la Unión Europea, lo que indica una clara motivación de ciberespionaje.

La información sobre esta vulnerabilidad y su explotación ha sido registrada, sirviendo como referencia para el seguimiento de la amenaza y la implementación de medidas de seguridad destinadas a prevenir este tipo de ataques en entornos Windows (Girnus, 2025).

- **Octubre:**

La vulnerabilidad **CVE-2025-41244** afectó a determinados componentes de **VMware**, incluyendo VMware Tools / VMware Aria Operations, y ha sido asociada principalmente a escenarios de elevación de privilegios locales en sistemas vulnerables. Diversos avisos de seguridad indicaron indicios de explotación en entornos reales, lo que reforzó la necesidad de aplicar con urgencia las actualizaciones y mitigaciones publicadas por el fabricante.

Si bien la vulnerabilidad no habilita por sí misma la ejecución remota de código ni los movimientos laterales, su explotación puede facilitar el fortalecimiento de la posición del atacante tras un acceso inicial previo, incrementando el impacto de una intrusión ya en curso dentro de infraestructuras corporativas.

En campañas reales observadas durante el periodo, una vez obtenido el acceso inicial por otros vectores, los atacantes emplearon herramientas de acceso remoto como **ScreenConnect** para la operación interactiva y persistencia, así como para la realización de movimientos laterales dentro de la red corporativa. Estas técnicas deben entenderse como TTPs post-compromiso, y no como mecanismos inherentes a la explotación directa de la vulnerabilidad **CVE-2025-41244.**

La actividad maliciosa relacionada con estas cadenas de ataque ha sido atribuida al grupo de amenazas **UNC5174**, un actor con capacidades avanzadas y experiencia en entornos empresariales complejos. Este caso pone de manifiesto el riesgo que supone la explotación de fallos en plataformas de virtualización ampliamente desplegadas y la importancia de mantener una adecuada estrategia de gestión de vulnerabilidades y detección post-explotación en entornos **VMware** (SOCRadar, 2025; SOCRadar Extended Threat Intelligence, 2025).

- **Noviembre:**

En noviembre de 2025 se identificó y explotó activamente un fallo crítico de deserialización en **Microsoft Windows Server Update Services (WSUS)**. Esta vulnerabilidad afectaba a servidores **WSUS** expuestos y permitía a un atacante ejecutar código de forma remota con privilegios de sistema, comprometiendo completamente el servidor afectado.

La vulnerabilidad fue registrada **como CVE-2025-59287** y se trató de un *0-day* durante el periodo inicial de explotación, hasta que **Microsoft** publicó el correspondiente parche de seguridad. Los atacantes aprovecharon este fallo como vector de acceso inicial, lo que les permitió tomar el control del servicio **WSUS** y utilizarlo como punto de entrada a la infraestructura interna de las organizaciones.

Tras la explotación, los actores de amenazas desplegaron el *backdoor* modular **ShadowPad**, una herramienta avanzada que proporciona control remoto persistente, capacidades de espionaje y ejecución de comandos. El uso de **ShadowPad** es especialmente relevante, ya que este *malware* se asocia habitualmente con grupos de ciberespionaje patrocinados por el Estado chino, lo que sugiere una motivación estratégica detrás de los ataques.

La información sobre esta vulnerabilidad y su explotación fue documentada en informes de inteligencia de amenazas que alertaron sobre la gravedad del impacto y la necesidad urgente de aplicar las actualizaciones de seguridad correspondientes para mitigar el riesgo asociado a **CVE-2025-59287** (Lakshmanan, 2025).

- **Diciembre:**

En diciembre de 2025 se identificó y explotó activamente un fallo crítico en **React Server Components**, conocido como **React2Shell,** que afectaba a aplicaciones web expuestas que utilizaban determinadas versiones del *framework* **React** en el lado servidor. Esta vulnerabilidad permitía a un atacante ejecutar código de forma remota en el servidor objetivo, comprometiendo la aplicación y el entorno subyacente sin necesidad de autenticación previa.

La vulnerabilidad fue registrada como **CVE-2025-55182** y recibió una puntuación CVSS de 10.0 debido a su impacto crítico. El fallo residía en el manejo inseguro del proceso de deserialización de datos enviados desde el navegador al servidor a través del protocolo **React Flight**. Mediante el envío de una única solicitud HTTP especialmente manipulada, un atacante podía interferir en la lógica interna de la aplicación y lograr la ejecución de código **JavaScript** arbitrario con los mismos privilegios que la aplicación afectada. Esta debilidad impactó directamente a *frameworks* basados en **React Server Components**, como **Next.js**, ampliando significativamente la superficie de ataque.

Tras la explotación inicial, se observaron múltiples actividades post-explotación en sistemas comprometidos, incluyendo la descarga y ejecución de *loaders* maliciosos, la instalación encubierta de **Node.js**, la creación de mecanismos de persistencia mediante **systemd, cron y rc.local**, así como comunicaciones con infraestructuras de comando y control alojadas en servicios *cloud* públicos. También se detectaron tareas de reconocimiento de red, exfiltración básica de información y el uso de *webhooks* y **Canarytokens** para confirmar el éxito de la intrusión.

Diversas investigaciones atribuyeron la explotación de esta vulnerabilidad a actores de amenazas avanzados, principalmente vinculados a China, incluyendo infraestructuras asociadas a grupos como **Earth Lumia y Jackpot Panda**. No obstante, la publicación de código de prueba de concepto incrementó rápidamente el riesgo de explotación por parte de actores oportunistas, ampliando el alcance del impacto más allá del espionaje estatal. Los informes de inteligencia de amenazas destacaron la necesidad urgente de aplicar los parches de seguridad publicados y revisar la exposición de aplicaciones **React** accesibles desde Internet para mitigar el riesgo asociado a **CVE-2025-55182** (Westman y Sophos, 2025).

Tendencias de explotación de estas vulnerabilidades

El segundo semestre de 2025 confirma y refuerza las tendencias ya observadas durante la primera mitad del año, en la que se anticipaba una **explotación cada vez más temprana y sistemática de vulnerabilidades críticas** como principal vector de acceso inicial. Lejos de estabilizarse, el ritmo de abuso de fallos de alto impacto se intensificó en S2, consolidando un escenario marcado por **ventanas de exposición cada vez más reducidas** entre la divulgación y la explotación activa.

Tal y como se preveía en S1 2025, los atacantes priorizaron vulnerabilidades en **tecnologías empresariales** ampliamente adoptadas, incluyendo plataformas Microsoft, infraestructuras de virtualización, *software* de uso masivo y componentes web modernos. La explotación observada en S2 no respondió únicamente a dinámicas oportunistas, sino que se integró de forma recurrente en **campañas estructuradas**, tanto en operaciones de ciberespionaje como en actividades con motivación económica.

El análisis mensual del periodo confirma además otra de las previsiones del primer semestre: **la exposición de servicios críticos, entornos híbridos y aplicaciones accesibles desde Internet** continúa amplificando el impacto de estas vulnerabilidades.

La persistencia de debilidades en la gestión de parches y la falta de priorización basada en explotación real siguen siendo factores determinantes, reforzando la necesidad de enfoques proactivos y continuos de gestión de vulnerabilidades para reducir el riesgo operativo en entornos reales.

10. Perspectiva futura

¿Qué nos espera en el 2026?

De cara a 2026, el panorama de ciberamenazas apunta a una consolidación y profundización de las dinámicas observadas durante 2025, más que a una disrupción radical del modelo de ataque. La cibercriminalidad continuará evolucionando hacia estructuras altamente especializadas, persistentes y orientadas a maximizar el impacto operativo y reputacional, apoyadas en una economía clandestina cada vez más fragmentada pero resiliente.

La progresiva profesionalización del *ransomware*, combinada con la reutilización de infraestructuras, afiliados y herramientas procedentes de grupos desmantelados o debilitados, favorecerá un ecosistema más distribuido y menos dependiente de marcas concretas. En paralelo, los actores estatales y los grupos ideológicamente alineados seguirán difuminando la frontera entre espionaje, sabotaje y criminalidad económica, utilizando el ciberespacio como un dominio estratégico de presión prolongada más que como un vector de ataques puntuales.

Durante 2026 se espera un aumento sostenido de campañas basadas en **persistencia silenciosa**, abuso de identidades y explotación de relaciones de confianza, tanto humanas como técnicas. El uso ofensivo de inteligencia artificial continuará expandiéndose, no tanto mediante técnicas disruptivas, sino como acelerador de procesos existentes: automatización del reconocimiento, personalización avanzada de ingeniería social, generación de contenidos sintéticos y optimización de la selección de objetivos. Esta evolución reducirá aún más las barreras de entrada al cibercrimen y ampliará la base de actores capaces de ejecutar ataques complejos.

Al mismo tiempo, la creciente fragmentación geopolítica y la desglobalización digital reforzarán la regionalización de las amenazas, con campañas alineadas a conflictos activos, intereses estratégicos nacionales y tensiones económicas. Sectores críticos, administraciones públicas, infraestructuras tecnológicas y cadenas de suministro seguirán concentrando gran parte del riesgo, actuando como amplificadores del impacto sistémico de los incidentes.

En este contexto, 2026 se perfila como un año marcado por **menos ataques visibles, pero más intrusiones prolongadas**, donde el valor no estará únicamente en la explotación inmediata, sino en la capacidad de los actores para mantenerse dentro de los entornos comprometidos, influir en decisiones, condicionar operaciones y monetizar el acceso de forma flexible a lo largo del tiempo.

11. Referencias

- AlienVault (2025, 26 de noviembre). *The 'Bear' attacks: what we learned about the phishing campaign targeting Russian organizations*. AlientVault. https://otx.alienvault.com/pulse/6926cae8043aabe58197d11e
- Arctic Wolf (2025). *2025 Arctic Wolf Threat Report*. Arctic Wolf. https://arcticwolf.com/resource/aw/arctic-wolf-threat-report-2025?lb-mode=overlay
- Aznar Fernández-Montesinos, F. (2025). *El gran reto geopolítico del siglo XXI: La multipolaridad desequilibrada (Documento de Análisis IEEE 06/2025)*. Instituto Español de Estudios Estratégicos – Ministerio de Defensa de España. https://www.ieee.es/Galerias/fichero/docs_analisis/2025/DIEEEA06_2025_FAFM_Multipolaridad.pdf
- Check Point Research (2025). *Threat Intelligence Reports*. Check Point. https://research.checkpoint.com/intelligence-reports/
- 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
- CrowdStrike (2025). *CrowdStrike 2025 Threat Hunting Report*. CrowdStrike. https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/
- DarkFeed (2025). *RANSOMWARE GROUPS: 2025 ACTIVITY*. [Publicaciones de X]. X. https://x.com/ido_cohen2/
- De Jong, L. (2025, 22 de noviembre). *Kimsuky and Lazarus join forces in coordinated attacks*. CYBERWARZONE. https://cyberwarzone.com/2025/11/22/kimsuky-and-lazarus-join-forces-in-coordinated-attacks/
- ESET (2025, 2 de septiembre). *ESET descubre el primer ransomware basado en IA*. ESET. https://www.eset.com/pa/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/eset-descubre-el-primer-ransomware-basado-en-ia/
- ESET Research (2025, 6 de noviembre). *ESET APT ACTIVITY REPORT Q2 2025–Q3 2025*. ESET. https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2025-q3-2025.pdf
- ESET Research (2025, 16 de diciembre). *ESET Threat Report H2 2025*. ESET. https://web-assets.eset.com/fileadmin/ESET/IT_2/Agenzia_Davide/H2-2025_Threat-Report.pdf
- EUROPOL (2025, 16 de julio). *Global operation targets NoName057(16) pro-Russian cybercrime network*. EUROPOL. https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network
- FALCONFEEDS.IO (2025). *ALERT: NEW HACKTIVIST ALLIANCE*. [Publicaciones De X]. X. https://x.com/FalconFeedsio
- Financial Crimes Enforcement Network [FinCEN] (2025, 4 de diciembre). FinCEN Issues Financial Trend Analysis on Ransomware. FinCEN. https://www.fincen.gov/news/news-releases/fincen-issues-financial-trend-analysis-ransomware
- Garaschenko, V. (2025, 14 de noviembre). *AI Malware and LLM Abuse: The Next Wave of Cyber Threats*. SOC Prime. https://socprime.com/blog/latest-threats/ai-malware-and-llm-abuse/

- Girnus, P. (2025, 18 de marzo). *(0Day) Microsoft Windows LNK File UI Misrepresentation Remote Code Execution Vulnerability*. Trend Micro Zero Day Initiative. https://www.zerodayinitiative.com/advisories/ZDI-CAN-25373/
- Hernández, A. (2025, 20 de noviembre). *Internet en la agenda de seguridad nacional rusa: RuNet y la soberanía digital*. UCM. https://doi.org/10.5209/geop.95098
- IBM Security (2025). *IBM X-Force 2025 Threat Intelligence Index*. IBM. https://www.ibm.com/reports/threat-intelligence
- Khalil, M. (2025, 29 de noviembre). *Cybersecurity Statistics 2025: Breach Costs, Ransomware & AI Threats*. DeepStrike. https://deepstrike.io/blog/cybersecurity-statistics-2025-threats-trends-challenges
- Lakshmanan, R. (2025, 4 de noviembre). *A CYBERCRIME MERGER LIKE NO OTHER — SCATTERED SPIDER, LAPSUS$, AND SHINYHUNTERS JOIN FORCES*. The Hacker News. https://thehackernews.com/2025/11/a-cybercrime-merger-like-no-other.html
- Lakshmanan, R. (2025, 24 de noviembre). *ShadowPad Malware Actively Exploits WSUS Vulnerability for Full System Access*. The Hacker News. https://thehackernews.com/2025/11/shadowpad-malware-actively-exploits.html
- Macías, E. (2025, 15 de octubre). *Mango sufre un ciberataque a través de su cadena de suministro*. COMPUTERWORLD. https://www.computerworld.es/article/4072830/mango-sufre-un-ciberataque-a-traves-de-su-cadena-de-suministro.html
- MITRE (2025, 15 de octubre). *SharePoint ToolShell Exploitation*. MITRE. https://attack.mitre.org/campaigns/C0058/
- NSFOCUS (2025, 25 de agosto). *NSFOCUS MONTHLY APT INSIGHTS – JULY 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-july-2025/
- NSFOCUS (2025, 18 de septiembre). *NSFOCUS MONTHLY APT INSIGHTS – AUGUST 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-august-2025/
- NSFOCUS (2025, 12 de noviembre). *NSFOCUS MONTHLY APT INSIGHTS – SEPTEMBER 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-september-2025/
- NSFOCUS (2025, 28 de noviembre). *NSFOCUS MONTHLY APT INSIGHTS – OCTOBER 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-october-2025/
- Pico, R. (2025, 28 de Agosto). Elche es el último ayuntamiento bloqueado por un ataque informático. COMPUTERWORLD. https://www.computerworld.es/article/4047504/elche-es-el-ultimo-ayuntamiento-bloqueado-por-un-ataque-informatico.html
- SHENOUDA, J. (2025, 29 de octubre). *NEW THREAT ACTOR: FULCRUMSEC*. SHENOUDA.NL. https://www.shenouda.nl/new-threat-actor-fulcrumsec/
- SHENOUDA, J. (2025, 29 de noviembre). *NEW THREAT ACTOR: NETMEDVED*. SHENOUDA.NL. https://www.shenouda.nl/new-threat-actor-netmedved/

- SHENOUDA, J. (2025, 2 DE DICIEMBRE). *NEW THREAT ACTOR: ZESTIX*. SHENOUDA.NL. HTTPS://WWW.SHENOUDA.NL/NEW-THREAT-ACTOR-ZESTIX/
- SOCRADAR (2025, 1 DE OCTUBRE). *VMWARE CVE-2025-41244 EXPLOITED: WHAT YOU NEED TO KNOW ABOUT THE LATEST FLAWS*. SOCRADAR. HTTPS://SOCRADAR.IO/BLOG/VMWARE-CVE-2025-41244-EXPLOITED/
- SOCRADAR EXTENDED THREAT INTELLIGENCE (2025, OCTUBRE). *VMWARE CVE-2025-41244 EXPLOITED BY UNC5174 APT GROUP*. LINKEDIN. HTTPS://WWW.LINKEDIN.COM/POSTS/SOCRADAR_VMWARE-CVE-2025-41244-EXPLOITED-WHAT-YOU-ACTIVITY-7379088943851536385-ZS75/
- STAMFORD, C. (2025, 29 DE JULIO). *GARTNER FORECASTS WORLDWIDE END-USER SPENDING ON INFORMATION SECURITY TO TOTAL $213 BILLION IN 2025*. GARTNER. HTTPS://WWW.GARTNER.COM/EN/NEWSROOM/PRESS-RELEASES/2025-07-29-GARTNER-FORECASTS-WORLDWIDE-END-USER-SPENDING-ON-INFORMATION-SECURITY-TO-TOTAL-213-BILLION-US-DOLLARS-IN-2025
- STROBES (2025, AGOSTO). *CVE-2025-8088*. HTTPS://VI.STROBES.CO/CVE/CVE-2025-8088
- VALDEOLMILLOS, C. (2025, 20 DE OCTUBRE). *ESPAÑA ES EL QUINTO PAÍS QUE MÁS CIBERATAQUES HA SUFRIDO EN LA PRIMERA MITAD DE 2025, SEGÚN MICROSOFT*. MCPRO. HTTPS://WWW.MUYCOMPUTERPRO.COM/2025/10/20/ESPANA-QUINTO-PAIS-CIBERATAQUES-PRIMERA-MITAD-2025-MICROSOFT
- WORLD ECONOMIC FORUM. (2025, 13 DE ENERO). *GLOBAL CYBERSECURITY OUTLOOK 2025*. WORLD ECONOMIC FORUM. HTTPS://WWW.WEFORUM.ORG/REPORTS/GLOBAL-CYBERSECURITY-OUTLOOK-2025
- WESTMAN, R. Y SOPHOS COUNTER THREAT UNIT RESEARCH TEAM (2025, 11 DE DICIEMBRE). *REACT2SHELL FLAW (CVE-2025-55182) EXPLOITED FOR REMOTE CODE EXECUTION*. SOPHOS. HTTPS://WWW.SOPHOS.COM/EN-US/BLOG/REACT2SHELL-FLAW-CVE-2025-55182-EXPLOITED-FOR-REMOTE-CODE-EXECUTION
- WRIGHT, R. (2025, 31 DE MARZO). CISA WARNS NEW MALWARE TARGETING IVANTI ZERO-DAY VULNERABILITY. CYBERSECURITY DIVE. HTTPS://WWW.CYBERSECURITYDIVE.COM/NEWS/CISA-WARNS-MALWARE-TARGETING-IVANTI-ZERO-DAY/743967/


NTT DATA