NTT DATA

Tendencias CTI

Inteligencia de ciberamenazas

Primer semestre 2026



Índice

1. **Resumen ejecutivo** 4

2. **Introducción** 6

2.1. Propósito del informe 6
2.2. Alcance geográfico y temporal del informe 6

3. **Panorama global de amenazas** 7

3.1. Geopolítica y Ciberseguridad 8
3.2. Geopolítica y principales actores 9
3.3. Afectación de ciberataques a regiones y sectores específicos 10
3.4. Panorama en España 13

4. **Principales amenazas globales** 15

4.1. Ciberincidentes destacados y grandes campañas 16
4.2. Tendencias emergentes de ataques 18
4.3. Estadísticas globales sobre incidentes de seguridad, tipos de ataques y actores de amenazas involucrados 19
4.4. Costes de los ciberataques para las empresas 21

5. **Marco legal y detenciones en Ciberseguridad** 22

5.1. Principales leyes en el ámbito de la ciberseguridad 23
5.2. Principales detenciones en el ámbito de la ciberseguridad 24

6. ***Dark Web Insights*** 28

6.1. Presión policial y reconfiguración del ecosistema *underground* 29
6.2. Foros *underground* activos 30
6.3. Mercados *underground* activos 31

7. **Actores de amenaza (*Threat Actors*)** 34

7.1. Nuevos actores identificados 35
7.2. *Ransomware* 36
7.3. Hacktivismo 41
7.4. APT 42

© 2026 NTT DATA, Inc.

Índice

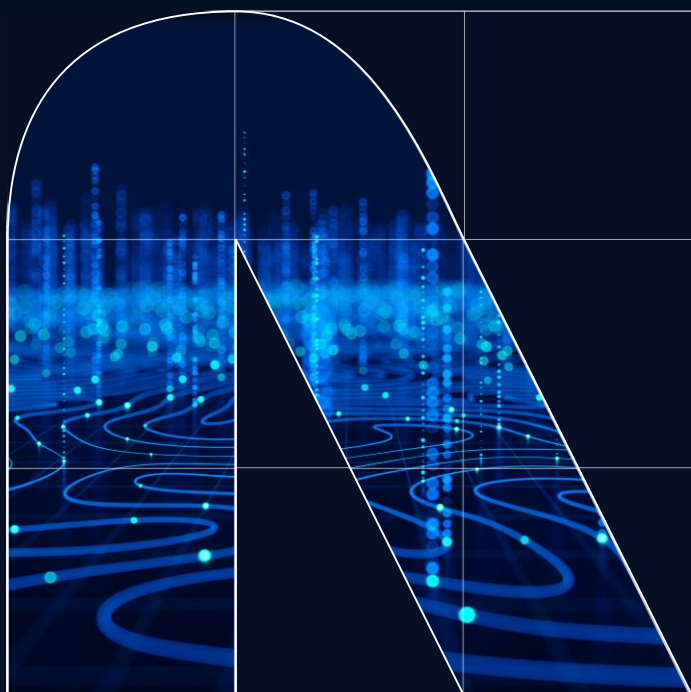
8. **Tácticas, Técnicas y Procedimientos** **45**

8.1. Descripción de las TTP más comunes utilizadas por los cibercriminales 46
8.2. Vectores de entrada más usuales 50
8.3. Innovación en ataques: nuevas técnicas y tácticas 51

9. **Vulnerabilidades** **53**

10. **Perspectiva futura** **58**

11. **Referencias** **60**



© 2026 NTT DATA, Inc.



1. Resumen ejecutivo

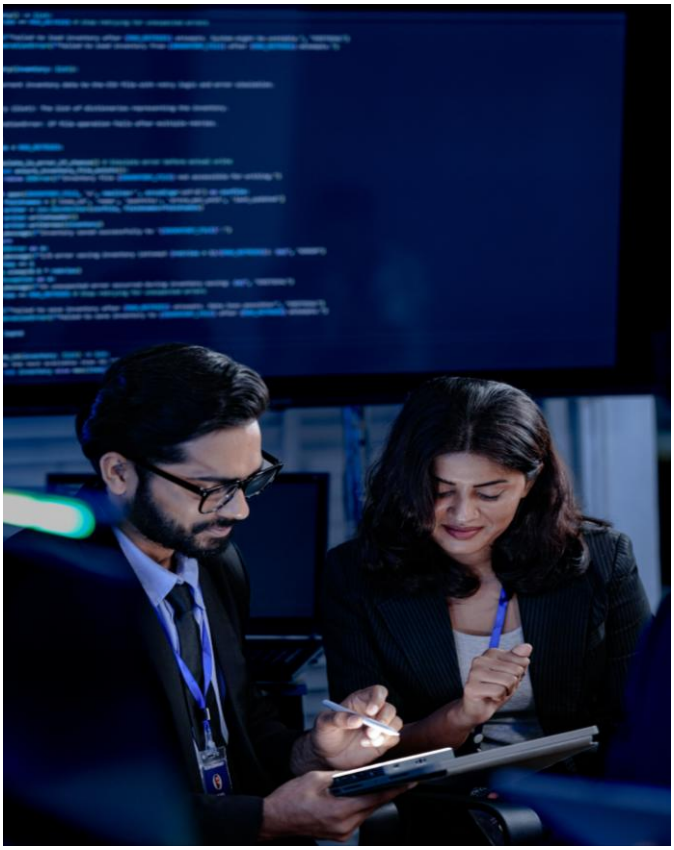
El primer semestre de 2026 ha estado definido por una **aceleración operativa del ciclo de ataque,** en un entorno donde la presión ciber se explica por la combinación de geopolítica, exposición digital, dependencia de terceros, explotación rápida de vulnerabilidades y monetización de identidades comprometidas.

La principal diferencia frente a periodos anteriores no ha sido la aparición de nuevas categorías de amenaza, sino la **capacidad de convertir vectores conocidos en campañas** más rápidas, escalables y difíciles de contener.

En el **plano geopolítico**, el ciberespacio se ha mantenido como un **dominio de presión estratégica**. La rivalidad entre potencias ha condicionado la selección de objetivos y la intensidad de las campañas. La actividad más visible se ha manifestado en DDoS, *defacement*, filtraciones y propaganda; sin embargo, el riesgo estratégico se concentra también en operaciones menos ruidosas: espionaje persistente, abuso de proveedores, explotación de infraestructuras expuestas y presencia encubierta en sectores críticos.

La **victimología global** confirma que la presión cibernética no responde solo al volumen de objetivos disponibles, sino a la combinación de exposición digital, criticidad operativa, valor económico, relevancia geopolítica y capacidad de generar impacto indirecto. **Estados Unidos** ha mantenido la mayor visibilidad y la **Administración pública** destaca por su visibilidad institucional y presión política.

Las **principales amenazas globales** han estado marcadas por la continuidad del *ransomware*, la explotación de vulnerabilidades, el uso de *infostealers*, la ingeniería social impulsada por IA, el abuso de *cloud*/SaaS y los ataques disruptivos contra infraestructuras críticas. **En Q1 2026 se registraron 2.122 víctimas publicadas en sitios de filtración**, la segunda cifra más elevada para un primer trimestre, mientras que **el *ransomware* estuvo presente en el 48% de las brechas analizadas**, destacando grupos como **Qilin, Akira o The Gentlemen**. Además, la explotación de vulnerabilidades ha superado al robo de credenciales como principal vía de acceso inicial, reflejando la rapidez con la que los actores operativizan fallos públicos.



© 2026 NTT DATA, Inc.



1. Resumen ejecutivo

El impacto económico mantiene una escala sistémica. **El coste global del cibercrimen ha superado los 12,5 billones de dólares anuales**, con un coste medio por brecha de 4,44 millones. Al mismo tiempo, la caída del precio medio del acceso corporativo comprometido, situado en torno a 439 USD frente a los 1.427 USD de hace tres años, evidencia una **deflación del acceso inicial** que amplía la base de actores capaces de monetizar intrusiones.

El **marco legal y la acción policial** han avanzado hacia una **respuesta más operativa**. El desarrollo del Cyber Resilience Act, el CMMC, nuevas guías NIST y reformas normativas en distintas regiones han reforzado la exigencia sobre seguridad de producto, protección de infraestructuras críticas, proveedores y reporte de incidentes. En paralelo, operaciones como **Endgame/SocGholish, Operation Saffron u Operation Ramz** muestran una mayor capacidad de disrupción contra infraestructuras criminales, aunque su impacto sigue siendo temporal frente a un ecosistema con alta capacidad de migración y reconstrucción.

El ecosistema *underground* ha mantenido un alto nivel de actividad pese a la presión policial. La actividad no ha desaparecido tras la caída o incautación de grandes foros, sino que **se ha redistribuido** hacia plataformas alternativas, mercados especializados, comunidades privadas y canales de acceso restringido.

Finalmente, la sección de vulnerabilidades confirma que la prioridad defensiva debe basarse en explotación activa, exposición real y criticidad operativa, no solo en severidad CVSS. Los casos analizados muestran que **el riesgo de una CVE reside en su capacidad para integrarse rápidamente en campañas automatizadas, silenciosas y orientadas a persistencia, robo de datos o impacto operacional.**

En **España**, el primer semestre de 2026 ha estado marcado por fraude masivo, exposición de datos, dependencia de terceros, *ransomware* y hacktivismo simbólico. Casos como los analizados en este informe reflejan el uso fraudulento de datos, el riesgo asociado a proveedores externos y la presión sobre servicios sensibles.

La ciberseguridad se consolida como un desafío sistémico donde tecnología, geopolítica y abuso de identidades legítimas convergen. La gestión del riesgo exige una aproximación integral: **detección contextual basada en comportamiento, resiliencia operativa y anticipación estratégica.**
La ventaja defensiva dependerá de anticipar, correlacionar y responder con rapidez.

De cara al segundo semestre de 2026, **el escenario apunta a más automatización ofensiva,** mayor explotación de servicios expuestos, presión sostenida sobre infraestructuras críticas y un ecosistema criminal más concentrado en operadores eficaces, pero más distribuido en canales y mercados.

© 2026 NTT DATA, Inc.



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 (CTI) durante el **primer semestre de 2026**. 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 enero a junio de 2026**, resulta clave para anticipar posibles movimientos futuros y fortalecer las capacidades de respuesta ante un entorno cada vez más complejo.

© 2026 NTT DATA, Inc.



3. Panorama global de amenazas

El panorama global de amenazas actual confirma la aceleración de tendencias ya consolidadas en periodos previos, donde se apreciaba una transición hacia amenazas más persistentes y menos ruidosas, dentro de un entorno más volátil y fragmentado.

La dinámica observada en 2026 refleja: más influencia geopolítica, más velocidad ofensiva, más abuso de confianza digital y mayor presión sobre sectores críticos.

Esta lectura encaja con el *World Economic Forum* (WEF), que sitúa la aceleración de la IA, la fragmentación geopolítica y la desigualdad de capacidades como factores que están reconfigurando el riesgo cibernético en 2026 (World Economic Forum, 2026).

Este apartado analiza los **principales factores del entorno global** que, por su alcance estructural, condicionan la evolución del riesgo cibernético y la estabilidad de los ecosistemas digitales.

Factores estructurales predominantes en el panorama global de amenazas S1 2026



Figura 1 | Factores de riesgo más influyentes en el panorama global de amenazas durante S1 2026.

3.1 Geopolítica y Ciberseguridad

La actividad cibernética del primer semestre de 2026 evidencia que el ciberespacio no acompaña al conflicto, sino que ya forma parte de él desde el diseño.

La **geopolítica** deja de ser un factor de contexto para convertirse en un elemento que condiciona la actividad ciber. Los conflictos abiertos, las rivalidades tecnológicas y la competencia entre bloques influyen en qué sectores se priorizan, qué narrativas se amplifican y qué objetivos adquieren valor estratégico.

El WEF también señala que el **64%** de las organizaciones ya incorpora ciberataques motivados geopolíticamente en sus estrategias de mitigación, y que el **91%** de las organizaciones más grandes ha modificado su estrategia de ciberseguridad por la volatilidad geopolítica.

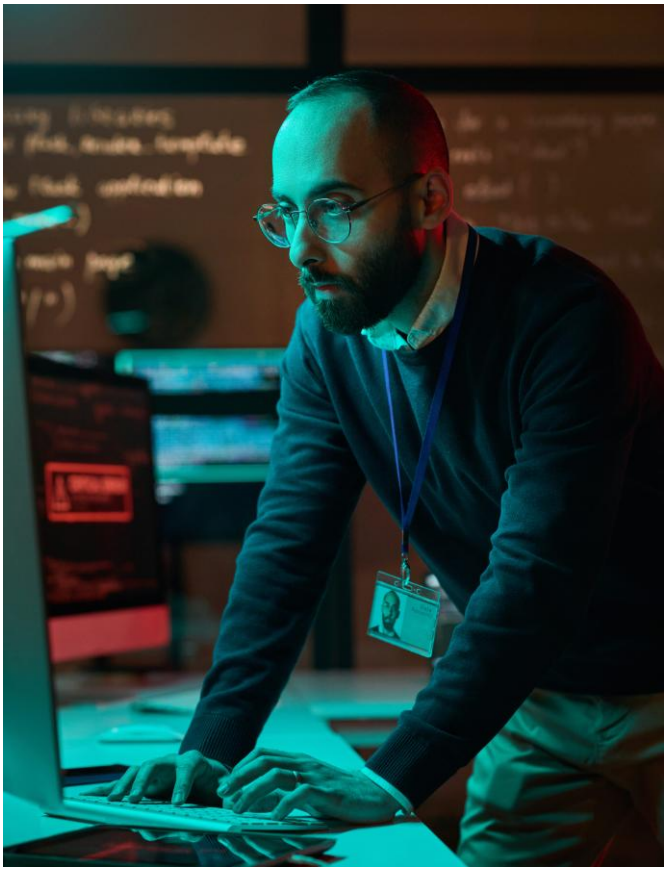
Por otro lado, la **IA y la automatización** actúan como aceleradores del ciclo ofensivo. Su relevancia no reside únicamente en la aparición de técnicas nuevas, sino en la capacidad de hacer más rápidos, convincentes y escalables ataques ya conocidos: *phishing*, fraude, reconocimiento, suplantación, generación de contenido y apoyo al desarrollo de herramientas. Durante el semestre se han visto familias de *malware* como **PROMPTFLUX** y **PROMPTSTEAL**, capaces de consultar modelos LLM durante su ejecución para adaptar comportamiento

© 2026 NTT DATA, Inc.

o evadir detección (Google Cloud, 2026). También se han incrementado las operaciones norcoreanas de suplantación de identidad por IA y *deepfakes*, conectando así geopolítica, inteligencia artificial y abuso de identidad, otro de los factores estructurales hacia los que se ha desplazado el riesgo durante el semestre.

El perímetro real de las organizaciones ya no se limita a su infraestructura propia, abarca una confianza digital distribuida entre usuarios y terceros, donde los **ataques a la cadena de suministro y el abuso de accesos legítimos** permiten a los atacantes operar con menor ruido técnico. Técnicas tipo *Adversary-in-the-Middle* (AitM), *sesión hijacking* o *MFA fatigue*, diseñadas para robar identidades, y campañas coordinadas de *supply chain*, como la de paquetes npm (Shai-Hulud y variantes), se convierten en vectores críticos de entrada a una superficie de ataque extendida.

Finalmente, como parte del panorama de amenazas global, la **explotación de vulnerabilidades** en activos expuestos se mantiene como factor de riesgo, así como el ***ransomware* y la extorsión** que siguen funcionando como motor económico del cibercrimen, con una lógica más madura.



3.2 Geopolítica y principales actores

Durante S1 2026, la relación entre geopolítica y ciberseguridad se mantiene como uno de los ejes estructurales del panorama global de amenazas.

La principal diferencia del semestre no es la aparición de un nuevo tipo de amenaza, sino la forma en que el contexto geopolítico condiciona la actividad ciber.

Los eventos políticos, militares o diplomáticos actúan como disparadores de campañas; las alianzas, sanciones o posicionamientos internacionales influyen en la selección de objetivos; y los sectores con valor estratégico adquieren mayor exposición por su capacidad de generar impacto operativo, reputacional o político.

En el eje **Irán-Israel/EE. UU. y Oriente Medio**, la actividad ciber refleja una combinación de campañas hacktivistas, actores afines a intereses estatales, operaciones de desinformación, DDoS, *defacement* y filtraciones. Los datos observados refuerzan esta lectura: Oriente Medio aparece como uno de los focos con mayor visibilidad en la muestra, especialmente por la concentración de actividad asociada a Israel-Irán y por la diversidad de tipologías observadas. Esta información debe interpretarse como señal de movilización y presión narrativa, no como medición absoluta del volumen real de ataques.

En paralelo, la rivalidad **Estados Unidos-China** mantiene un perfil menos visible, pero estratégicamente más relevante. En este caso, el riesgo no se manifiesta principalmente mediante campañas ruidosas, sino a través de espionaje persistente, targeting de telecomunicaciones, infraestructura militar, transporte, gobierno y proveedores tecnológicos.

Corea del Norte mantiene una lógica diferenciada, donde el ciberespacio opera simultáneamente como herramienta de espionaje y fuente de financiación estatal. Esta combinación de espionaje, robo financiero, abuso de identidad y acceso encubierto refuerza la idea de que el riesgo geopolítico no siempre adopta la forma de sabotaje o disrupción directa.

© 2026 NTT DATA, Inc.

En conjunto, S1 2026 confirma que la geopolítica no es solo contexto, sino un factor que activa campañas, orienta objetivos y amplifica impactos. La actividad más visible se materializa en DDoS, *defacement*, filtraciones y propaganda; sin embargo, el riesgo estratégico se encuentra también en operaciones menos ruidosas: espionaje, preposicionamiento, abuso de proveedores, explotación de infraestructuras expuestas y persistencia en sectores críticos. La consecuencia para las organizaciones es clara: la exposición cibernética debe analizarse no solo desde la superficie técnica, sino también desde su posición geográfica, sectorial, regulatoria y geopolítica.

Mapa global de presión ciber por contexto geopolítico en S1 2026

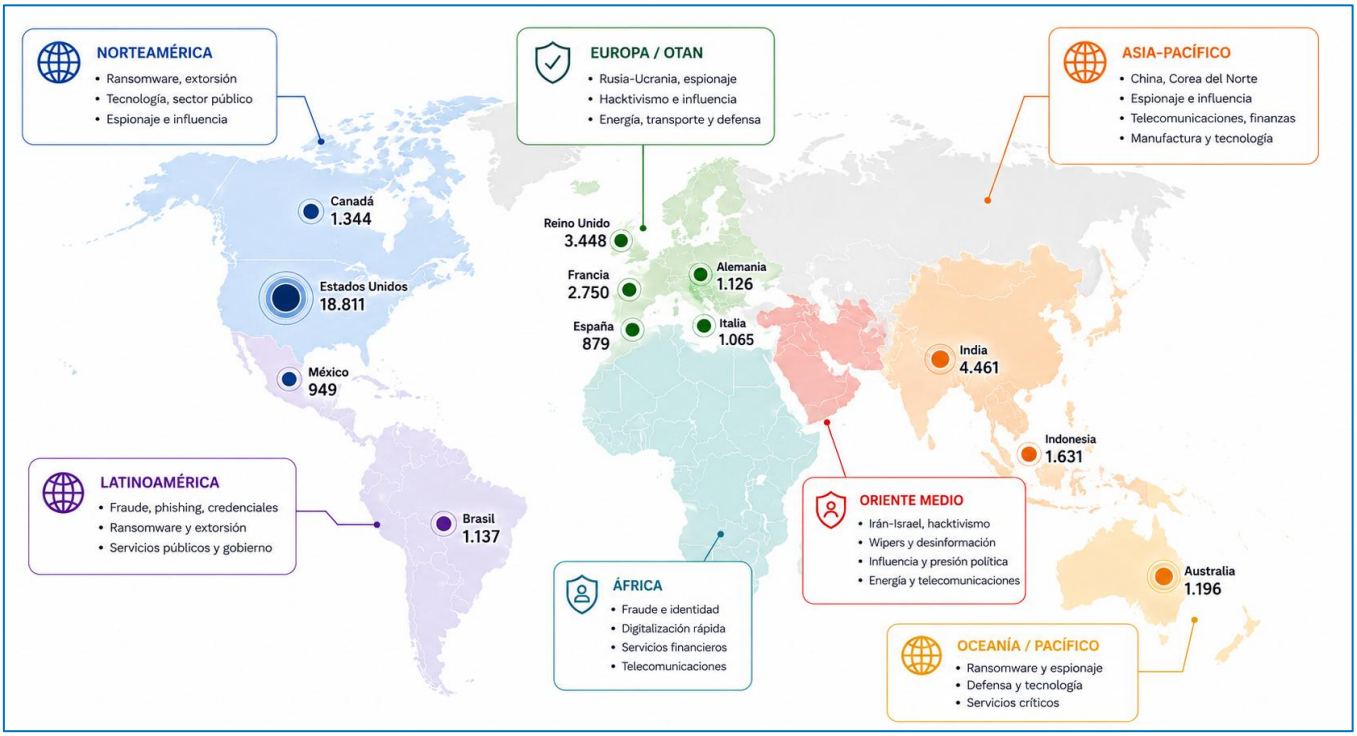


Figura 2 | Mapa global de presión ciber y contexto geopolítico durante el primer semestre de 2026.

3.3 Afectación de ciberataques a regiones y sectores específicos

Durante S1 2026, la **actividad maliciosa global** vuelve a evidenciar que la presión ciber no se distribuye únicamente en función del volumen de objetivos disponibles, sino de la combinación entre **exposición digital, criticidad operativa, valor económico, relevancia geopolítica y capacidad de generar impacto indirecto**. Los datos observados sitúan a **Estados Unidos** como el país con mayor visibilidad, seguido por economías altamente digitalizadas como **India, Reino Unido, Francia, Canadá, Australia, Brasil, Alemania, Italia, México y España**. Esta distribución debe interpretarse como una señal de exposición y actividad monitorizada, no como una medición absoluta del volumen global de ataques. A nivel geográfico, el patrón observado confirma que las economías con mayor dependencia de servicios digitales, ecosistemas empresariales amplios y presencia de sectores críticos concentran mayor presión. Estados Unidos mantiene una exposición destacada por su peso económico, tecnológico y geopolítico; India refleja el impacto de una digitalización acelerada y de su papel estratégico en el Indo-Pacífico; mientras que países europeos como Reino Unido, Francia, Alemania, Italia y España continúan expuestos por su integración en cadenas de suministro globales, su apoyo a Ucrania, su peso regulatorio y su dependencia de servicios públicos digitales. La presencia de Brasil y México refuerza además una tendencia relevante: Latinoamérica no debe considerarse un entorno periférico, ya que combina monetización de

© 2026 NTT DATA, Inc.

datos, *phishing, ransomware*, robo de credenciales y compraventa de accesos.

Desde el punto de vista sectorial, los atacantes priorizan sectores donde una interrupción, una filtración o un acceso indirecto puede generar impacto más allá de la entidad comprometida: servicios ciudadanos, producción industrial, datos financieros, continuidad logística, confianza del cliente o acceso a terceros.

La **Administración Pública** se mantiene como uno de los objetivos más presionados por su valor simbólico, su visibilidad institucional y su función en la prestación de servicios esenciales. El peso de **Manufactura** confirma la presión sostenida sobre sectores industriales y entornos con dependencia operativa. A diferencia de otros sectores donde el impacto se concentra en datos o reputación, en manufactura el riesgo puede trasladarse a producción, logística, OT y continuidad física.

Los sectores de **Educación, Servicios Profesionales, Información y Tecnología** mantienen una exposición elevada por motivos distintos pero conectados.
Educación combina superficies amplias, heterogeneidad tecnológica y alto valor de credenciales, datos académicos e investigación. Servicios profesionales, Información y Tecnología actúan además como nodos de confianza: consultoras, proveedores SaaS, integradores, plataformas *cloud* y empresas tecnológicas pueden convertirse en vías de acceso indirecto a terceros.

En **Finanzas, *Retail* y Salud**, la motivación combina monetización directa, fraude, datos sensibles y presión reputacional. Finanzas sigue siendo un objetivo natural por el valor económico de sus activos y la confianza que sostiene el servicio; *Retail* y comercio digital concentran exposición a fraude, credenciales y disponibilidad web; y Salud mantiene una criticidad diferencial por la sensibilidad de los datos y la baja tolerancia a interrupciones.

En conjunto, la victimología de S1 2026 muestra un cambio relevante: la víctima ya no debe analizarse únicamente como organización atacada, sino como parte de un ecosistema de dependencias. El impacto puede extenderse a terceros y sectores conectados. Por ello, los países y sectores más visibles en el panorama no solo representan mayor volumen de actividad, sino mayor concentración de valor estratégico, económico y operativo.



© 2026 NTT DATA, Inc.

Sectores con mayor exposición e impacto ciber en S1 2026

Sector	Ataques obs.	Exposición	Impacto	Lectura CTI
Administración pública	**9.454**	**Muy alta**	**Alta**	Alta visibilidad institucional, servicios ciudadanos y presión política; objetivo recurrente para DDoS, hacktivismo, espionaje y filtraciones.
Manufactura	**5.478**	**Alta**	**Muy alta**	Dependencia OT/IT, continuidad operativa y cadenas de suministro; impacto elevado ante interrupciones o extorsión.
Educación	**5.271**	**Alta**	**Media-alta**	Superficie amplia, credenciales reutilizables y menor madurez defensiva; atractivo para robo de datos y accesos.
Finanzas y seguros	**5.154**	**Alta**	**Muy alta**	Monetización directa, fraude, datos sensibles y confianza del cliente; alto valor para extorsión y abuso de identidad.
Servicios prof. y técnicos	**5.123**	**Alta**	**Alta**	Acceso indirecto a clientes, consultoría, integradores y proveedores críticos; vector relevante de cadena de suministro.
Información / tecnología	**5.097**	**Muy alta**	**Muy alta**	SaaS, *cloud,* APIs, tokens y capacidad de amplificación hacia terceros; exposición e impacto muy altos.
Retail	**3.773**	**Media-alta**	**Media-alta**	Pagos, credenciales, fraude, disponibilidad web y datos de clientes; alta exposición por volumen transaccional.
Salud y asistencia social	**2.959**	**Media-alta**	**Muy alta**	Datos sensibles, urgencia operativa y baja tolerancia a interrupciones; impacto crítico en continuidad asistencial.
Transporte y logística	**2.078**	**Media**	**Alta**	Movilidad, comercio y continuidad física; impacto relevante en crisis o disrupciones regionales.
Construcción	**1.284**	**Media**	**Media-alta**	Proyectos, contratistas, documentación sensible y dependencia de terceros; riesgo creciente por cadena de suministro.

Tabla 1 | Sectores con mayor exposición, impacto y actividad ciber observada durante el primer semestre de 2026.



© 2026 NTT DATA, Inc.



3.4 Panorama en España

Durante el primer semestre de 2026, España mantiene la línea observada en el cierre de 2025: una presión ciber sostenida, predominantemente económica, en la que **el fraude, la extorsión, el abuso de identidad y la exposición de terceros actúan como vectores conectados, no como fenómenos aislados.** El Balance de Criminalidad del primer trimestre confirma el peso estructural del riesgo digital: la cibercriminalidad representa ya el **20,6%** de la criminalidad registrada en España, y las estafas informáticas concentran el **90,2%** de toda la cibercriminalidad del periodo (Ministerio del Interior, 2026). Esta lectura da continuidad al patrón identificado en el semestre anterior, en el que España ya aparecía como un escenario europeo especialmente expues-to a *ransomware*, extorsión digital, filtración de datos y *phishing*.

20,6%
de la criminalidad total registrada en España corresponde a la cibercriminalidad, según el Balance de Criminalidad (2026).

90,2%
de la cibercriminalidad se concentra en estafas informáticas durante el primer trimestre de 2026.

La primera idea clave del semestre es que el **fraude digital** se consolida como el hilo conductor del panorama español. El incidente notificado por Endesa refleja bien esta dinámica: el valor del acceso no autorizado no reside únicamente en la exposición inicial de datos, sino en su posible reutilización para suplantación, *phishing*, *spam* o intentos de fraude contra clientes (INCIBE, 2026). Este patrón se refuerza en el ámbito turístico, especialmente relevante para España. La AEPD alertó en mayo de un aumento de brechas vinculadas a establecimientos hoteleros y encargados de tratamiento, generalmente plataformas de gestión de reservas, cuyos datos estaban siendo utilizados para contactar con clientes y reclamar pagos fraudulentos (AEPD, 2026). El caso Booking, con acceso no autorizado a datos de reservas y riesgo posterior de campañas de *phishing*, confirma que los datos contextuales (reserva, fecha, alojamiento, contacto) elevan la credibilidad del fraude y aumentan su probabilidad de éxito (INCIBE-CERT, 2026a).

La segunda tendencia diferencial es el desplazamiento del perímetro efectivo hacia **proveedores, plataformas externas y encargados de tratamiento.** En marzo, la AEPD destacó que un único incidente en un encargado puede generar brechas en múltiples responsables, multiplicando el impacto regulatorio y operativo (AEPD, 2026). En la misma línea, INCIBE-CERT vinculó el incidente de Inditex / Zara a una plataforma de terceros que almacenaba

© 2026 NTT DATA, Inc.

información, sin que la intrusión se produjera en los sistemas internos de Zara ni constase compromiso de contraseñas o medios de pago (INCIBE-CERT, 2026c). Desde una perspectiva CTI, esto confirma que la cadena de suministro digital ya no es un riesgo periférico: es una extensión real de la superficie de ataque.

La tercera línea de presión se concentra en ***ransomware*** y extorsión contra servicios con baja tolerancia a la interrupción. El ataque al Puerto de Vigo mostró un impacto relevante sobre servidores, servicios digitales y gestión logística, aunque la operativa física pudo mantenerse parcialmente mediante procedimientos manuales (GaliciaPress, 2026). En la Administración Local, el caso Valdemoro ilustra un impacto aún más visible para la ciudadanía: la afectación de servidores municipales impidió trámites y consultas, obligó a desconectar sistemas y derivó en la suspensión de plazos administrativos por afectación general a sistemas informáticos, sede electrónica, correo corporativo, aplicaciones de gestión y atención electrónica (Ayuntamiento de Valdemoro, 2026).

Finalmente, el semestre también evidencia que el **hacktivismo** mantiene capacidad de presión simbólica y operativa en España. La detención de integrantes de Anonymous Fénix por ataques DDoS contra ministerios, partidos e instituciones públicas muestra que este tipo de actor busca visibilidad, interrupción temporal y desgaste institucional más que una intrusión prolongada (Guardia Civil, 2026).

En conjunto, **España afronta S1 2026 con un riesgo ciber marcado por la convergencia entre fraude masivo, exposición de datos, dependencia de terceros y ataques disruptivos contra servicios públicos y sectores estratégicos.**

El reto defensivo no se limita a reforzar tecnología: **exige mejorar la gobernanza de proveedores, la gestión de identidad, la autenticación fuerte, la resiliencia operativa y la detección temprana de accesos anómalos** antes de que el incidente se convierta en fraude, extorsión o interrupción de servicio.



Fraude digital

- Reutilización de datos
- *Phishing* y suplantación
- Mayor impacto en turismo

Terceros

- Proveedores críticos
- Impacto en cadena





Ransomware

- Servicios esenciales

Hacktivismo

- Ataques DDoS
- Desgaste institucional



© 2026 NTT DATA, Inc.



4. Principales amenazas globales

Durante el primer semestre de 2026, el panorama global de amenazas ha estado marcado por una actividad intensa y, a la vez, sostenida. El nivel de coordinación de las campañas es más elevado y los actores de amenazas son aún más capaces de combinar técnicas de espionaje, *ransomware* y de disrupción en operaciones de largo alcance.

Este periodo ha confirmado una tendencia hacia ataques más costosos y difíciles de detectar, impulsada en gran parte por la integración de inteligencia artificial en el ciclo de vida del ataque. La geopolítica se afianza una vez más como un factor estructural del riesgo, siendo capaz de condicionar tanto la naturaleza de las amenazas como la capacidad coordinada de respuesta a nivel internacional.

4.1. Ciberincidentes destacados y grandes campañas

El primer semestre de 2026 ha dejado un conjunto de incidentes de alto impacto que confirman la madurez operativa de los actores de amenazas actuales. Las campañas más significativas han apuntado a sectores de valor estratégico, como el sanitario, el industrial y el gubernamental, combinando técnicas de intrusión sigilosa, exfiltración masiva de datos y extorsión como método principal de presión. La convergencia entre los actores estatales y los grupos de cibercrimen organizado se ha hecho más evidente, dificultando en la mayoría de las ocasiones tanto la atribución como la respuesta coordinada.

Desde el **Departamento de Cyber Threat Intelligence de NTT DATA** hemos documentado algunos de los ciberincidentes más relevantes del primer semestre de 2026, 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
Red Eléctrica de Polonia	Energía e Infraestructuras críticas	Electrum	Polonia	Rusia	Enero 2026	Fuente
Entidades gubernamentales y militares (CEE)	Gobierno y Defensa	APT28 GRU Unidad 26165	Europa Central y del Este	Rusia	Enero 2026	Fuente
Instituciones gubernamentales Indias	Gobierno y Defensa	APT36 Transparent Tribe	India	Pakistán	Enero 2026	Fuente
Ministerio de Economía de Francia	Gobierno y Finanzas	Desconocido	Francia	Desconocido	Febrero 2026	Fuente
Operadoras de telecomunicaciones de Singapur	Telecomunicaciones	UNC3886	Singapur	China	Febrero 2026	Fuente
Telus	Telecomunicaciones	ShinyHunters	Canadá	Global	Marzo 2026	Fuente
Stryker	Tecnología y Sanidad	Handala	Global	Irán	Marzo 2026	Fuente
Comisión Europea	Gobierno	TeamPCP	Unión Europea	Europa del Este	Marzo 2026	Fuente
FBI	Gobierno y Seguridad	Desconocido	Estados Unidos	China	Abril 2026	Fuente

© 2026 NTT DATA, Inc.

Víctimas	Sector	Atacante	País / región afectada	Origen del atacante	Fecha del incidente	URL
Booking	Turismo	Desconocido	Global	Desconocido	Abril 2026	Fuente
Medtronic	Tecnología y Medicina	Desconocido	Global	Desconocido	Abril 2026	Fuente
Foxconn – Fábricas norteamericanas	Industria	Nitrogen Ransomware Gang	Estados Unidos Global	Desconocido	Mayo 2026	Fuente
Trellix	Ciberseguridad	RansomHouse	Global	Rusia	Mayo 2026	Fuente
Instructure (Canvas)	Educación	ShinyHunters	Global	Global	Mayo/Junio 2026	Fuente

Tabla 2 | Grandes ciberincidentes de seguridad en el primer semestre de 2026.

Por otro lado, el primer semestre de 2026 ha mostrado un ecosistema de amenazas más fragmentado y especializado. Cada vez un mayor número de actores combina la automatización y la explotación de entornos de desarrollo con motivaciones híbridas (principalmente geopolíticas y financieras) para operar con mayor alcance, persis-tencia e impunidad.

Campañas de ciberataques en S1 2026 agrupadas por objetivo

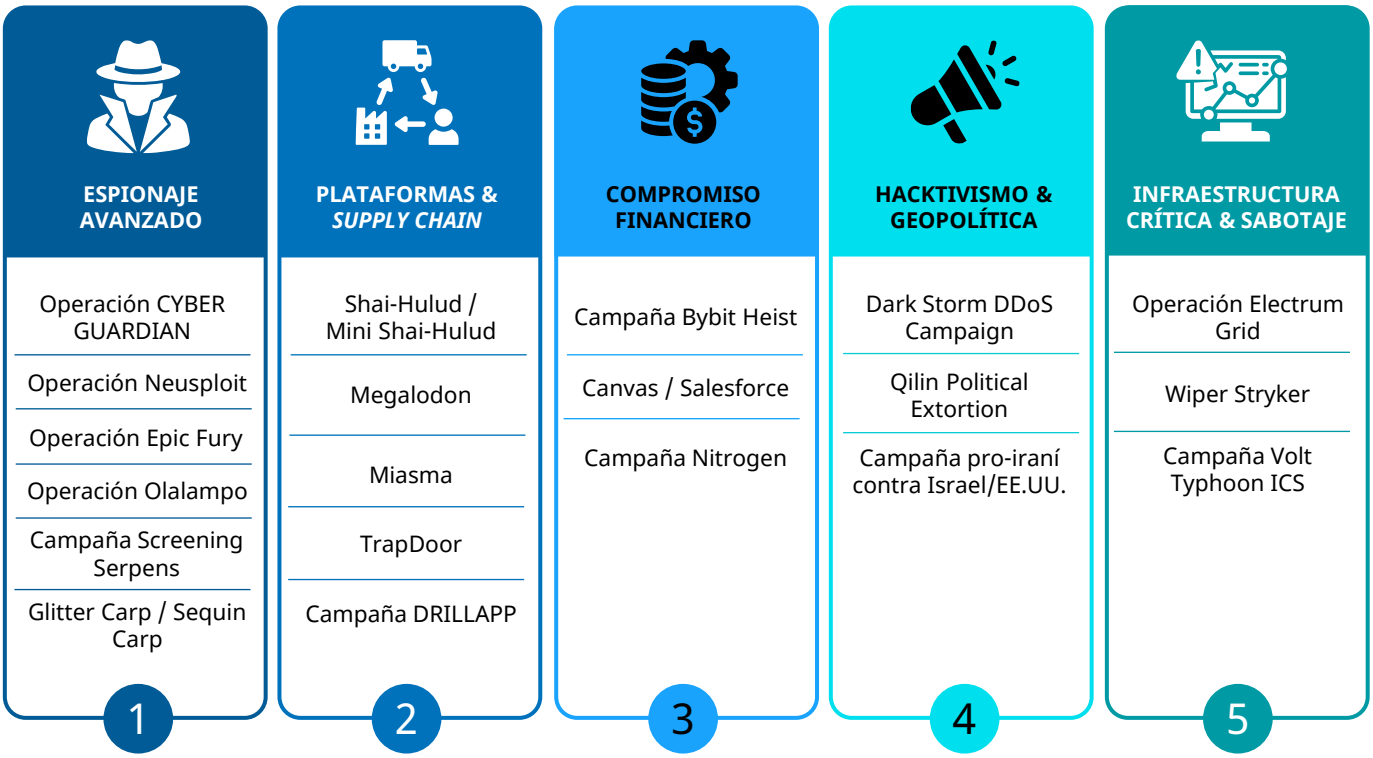


Figura 3 | Grandes campañas detectadas en el primer semestre de 2026.

© 2026 NTT DATA, Inc.

4.2 Tendencias emergentes de ataques

Durante el primer semestre de 2026, se ha observado una evolución continuada de las capacidades ofensivas de los actores de amenazas, marcada por una reducción de los tiempos de compromiso, una mayor dependencia en la obtención y uso de identidades legítimas y el aprovechamiento de las capacidades de la inteligencia artificial.

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

4.2.1 Compromiso de credenciales como vector principal de acceso

Aunque la explotación de vulnerabilidades ha pasado a ocupar el primer lugar como vía de acceso inicial en 2026, el abuso de credenciales comprometidas, sesiones autenticadas y *tokens* válidos sigue siendo un mecanismo central para consolidar acceso, moverse lateralmente y mantener persistencia. Los actores han reducido la necesidad de explotar vulnerabilidades en todas las fases de la intrusión, pero continúan apoyándose en identidades legítimas mediante técnicas como *Adversary-in-the-Middle*, *phishing* avanzado, secuestro de sesiones, robo de *tokens* o abuso de OAuth.

Esta tendencia ha derivado en intrusiones de bajo perfil difícilmente detectables mediante los controles habituales.

4.2.2 Ingeniería social impulsada por IA

La inteligencia artificial ha continuado actuando como principal facilitador operativo, destacando especialmente en la generación de campañas de ingeniería social altamente personalizadas a cada objetivo. Además, ha tenido una gran adopción la automatización de correos fraudulentos, la elaboración de señuelos, la falsificación de comunicación corporativa y la generación de contenidos multilenguaje. La efectividad de estas operaciones se ha visto incrementada significativamente gracias a su escalabilidad y capacidad de personalización.

4.2.3. Explotación de vulnerabilidades aún más acelerada

El tiempo transcurrido desde la divulgación de vulnerabilidades hasta su explotación activa ha continuado reduciéndose. Los actores de amenazas han demostrado una creciente capacidad de identificación automática de sistemas vulnerables y despliegue de campañas masivas en cuestión de horas. Entre los principales activos afectados se encuentran los dispositivos perimetrales, componentes de terceros y aplicaciones expuestas a Internet.

4.2.4 Foco en entornos *cloud* y SaaS

Los entornos *cloud* y SaaS mantienen su posición como superficie prioritaria de ataque. La tendencia de las intrusiones observadas se ha orientado hacia el abuso de cuentas con privilegios, sincronizaciones entre servicios y configuraciones inseguras.

El incremento de uso de canales legítimos para la exfiltración de información continúa dificultando la labor de diferenciación entre actividades legítimas y maliciosas.

4.2.5 Ciberespionaje sobre innovación tecnológica

La actividad de ciberespionaje ha mostrado un interés creciente por sectores tecnológicos, propiedad intelectual, información estratégica e inteligencia artificial. Se han observado campañas con accesos prolongados y mecanismos de persistencia avanzados con la finalidad principal de recopilar información de manera discreta. Esta tendencia refleja la importancia que cobra la ventaja tecnológica y económica desde un punto de vista geopolítico.

4.2.6 Ataques disruptivos sobre infraestructuras críticas

La generación de impacto operativo sobre infraestructuras críticas y sus servicios mantiene su estatus creciente.

Para ello, se combinan capacidades técnicas con objetivos de presión económica, política o reputacional. Se han observado campañas dirigidas que hacen uso de *ransomware*, *wipers* y técnicas DDoS con el fin de generar efectos en cadena. Esta tendencia refleja una evolución desde modelos centrados en la obtención de información hacia operaciones híbridas con mayor potencial disruptivo.

© 2026 NTT DATA, Inc.

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

Durante el primer semestre de 2026, la actividad asociada al *ransomware* se ha mantenido entre las principales amenazas del panorama global de ciberseguridad, en un contexto marcado por la evolución y reorganización del ecosistema criminal. Los datos observados reflejan una actividad sostenida en niveles históricamente altos acompañada de una consolidación operativa entre los grupos más activos.

4.3.1 Incidentes de seguridad

El ***ransomware*** se ha mantenido como el principal generador de incidentes de alto impacto. Durante el primer trimestre de 2026 se contabilizaron **2.122 víctimas** publicadas en sitios de filtración de datos, la segunda cifra más elevada registrada para un primer trimestre. Aunque supone un **descenso del 12,2%** respecto al máximo histórico alcanzado en el cuarto trimestre de 2025 (Check Point Research, 2026), los datos continúan reflejando una actividad sostenida en niveles aún muy elevados.

Esta evolución confirma la consolidación del *ransomware* como una de las amenazas más persistentes y disruptivas del panorama actual de amenazas.

4.3.2 Tipos de ataques y vectores predominantes

El ***ransomware*** ha estado presente en el **48%** de las brechas analizadas a nivel global durante 2026 (Verizon, 2026), frente al 44% del periodo anterior, consolidándose como el vector de mayor impacto operativo y económico. Los *infostealers* se han posicionado como la variante de *malware* más activa, con más de **155.000 detecciones registradas** a comienzos de 2026 (SentinelOne, 2026), utilizándose principalmente como mecanismo de preparación del entorno y robo de credenciales. Por su parte, los **ataques DDoS** han mantenido una presencia relevante sobre el sector tecnológico, con una cuota del **45%** a nivel de capa de red (Radware/GlobeNewswire, 2026), manteniendo un rol táctico y complementario en operaciones de disrupción.

En cuanto a vectores de entrada, la explotación de vulnerabilidades ha superado al robo de credenciales como principal vía de acceso inicial, estando presente en un **31%** de las brechas. Este hecho supone una respuesta a la rapidez con la que los atacantes operativizan vulnerabilidades de carácter público. El hecho de que el **número de víctimas** de *ransomware* confirmadas haya **aumentado** un **53%** (Check Point Software / StockTitan, 2026) confirma el patrón de profesionalización e intensificación de la actividad.



Incidentes de seguridad

2.122

víctimas publicadas en sitios de filtración de datos durante el primer trimestre de 2026.

-12,2%

variación respecto al máximo histórico del cuarto trimestre de 2025.



Tipos de ataques y vectores predominantes

48%

de las brechas analizadas a nivel global están relacionadas con *ransomware* durante el primer trimestre de 2026.

+155.000

detecciones de *infostealers* registradas a comienzos de 2026.

45%

de los ataques a nivel de capa de red corresponden a DDoS en el sector tecnológico.

© 2026 NTT DATA, Inc.

Desde la perspectiva de la evolución tecnológica, los **archivos de configuración de inteligencia artificial** se han consolidado como un nuevo riesgo de cadena de suministro, requiriendo el mismo nivel de escrutinio que las dependencias de código de terceros. Además, las credenciales de acceso a modelos de inteligencia artificial también están siendo recolectadas activamente a escala. Este vector confirma que la **adopción de inteligencia artificial** por parte de las organizaciones está ampliando la superficie de exposición tan rápido como se despliega, sin que ello suponga un avance de los controles de seguridad asociados al mismo ritmo.

4.3.3 Actores de amenazas y dinámica del ecosistema

El ecosistema criminal ha mostrado un giro relevante respecto a la fragmentación observada en el semestre anterior, especialmente en el ámbito del *ransomware*. Tras un par de años de crecimiento sostenido la tendencia se ha revertido: los **diez grupos de *ransomware*** más activos han concentrado el **71,1%** de las víctimas publicadas (Check Point Research, 2026).

Esta consolidación no implica una reducción de actividad a nivel global sino una **reorganización del modelo RaaS** hacia operadores más capaces que absorben más afiliados.

Asimismo, se ha observado notable **resiliencia del mercado de robo de credenciales** pese a las acciones de desmantelamiento.
A pesar de las disrupciones realizadas contra los principales operadores, el ecosistema fue capaz de seguir creciendo. Los *infostealers* exfiltraron más de **1.800 millones de credenciales** (Shattered.io / DeepStrike, 2026) incluyendo, por parejas, cuentas de correo tanto personales como corporativas y sus respectivas contraseñas. Este patrón confirma que las disrupciones generan impactos puntuales, pero no son capaces de frenar la **capacidad de adaptación** de los mercados clandestinos, que recurren a nuevas familias de *malware*.

En conjunto, las estadísticas del primer semestre de 2026 reflejan un ecosistema criminal más concentrado en el *ransomware*, más resiliente en el robo de credenciales y más capaz de reorganizarse con rapidez en torno a actores de mayor capacidad operativa.

Estadísticas globales por tipo de ataque en 2026

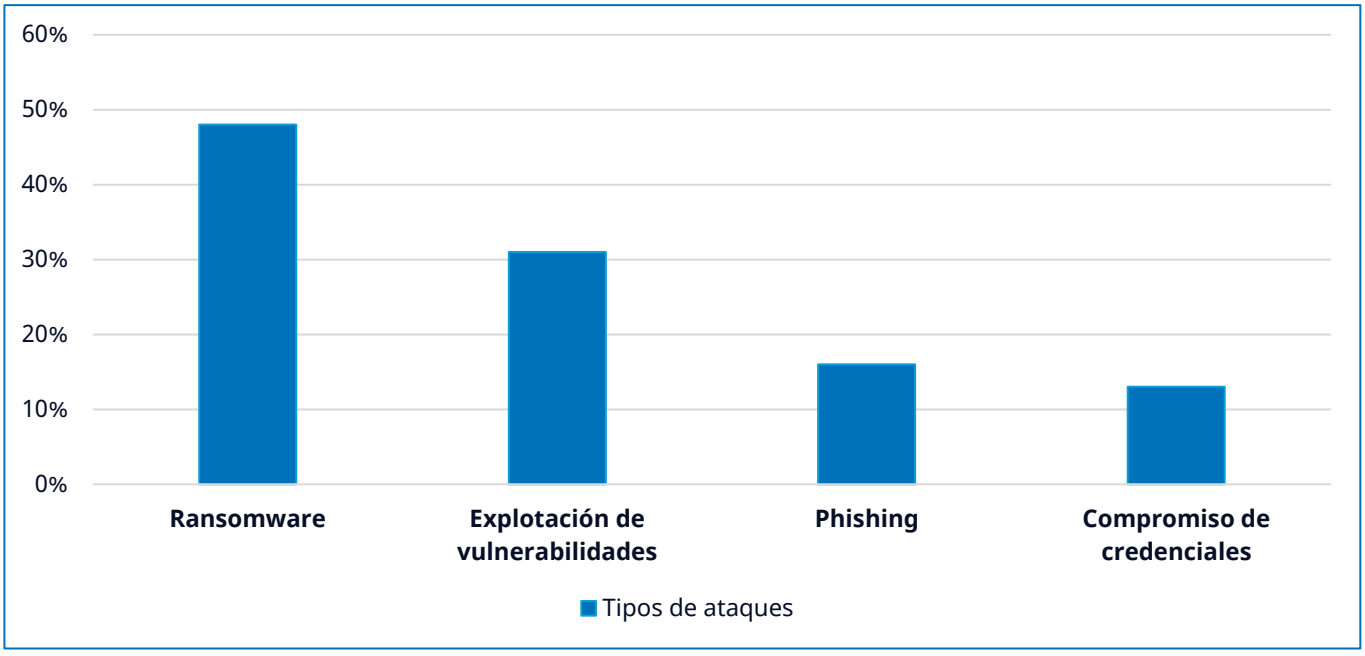


Figura 4 | Frecuencia de los ataques por tipo durante 2026 (Verizon, 2026)

© 2026 NTT DATA, Inc.

4.4 Costes de los ciberataques para las empresas

El primer semestre de 2026 ha confirmado que el cibercrimen opera ya como una economía paralela de escala comparable a la de grandes potencias industriales, con un impacto global que supera los **12,5 billones de USD anuales** (Aftra, 2026). Esta cifra situaría a cualquier país entre las mayores economías del planeta, muy por delante de la mayoría de los PIB nacionales.

Durante el periodo, la dinámica de pago de rescates ha mostrado un patrón contradictorio: **mientras el volumen de ataques aumenta, el comportamiento de las víctimas se vuelve más resistente**. El porcentaje de organizaciones afectadas que han accedido a realizar el pago se sitúa únicamente entre un 20% y un 28%. Estas cifras suponen las más bajas registradas hasta la fecha, frente a tasas que, hace apenas un par de años, superaban el 60-70% (SOSRansomware, 2026). Aun así, el dinero sigue fluyendo hacia los atacantes. En el caso de *blockchain,* los pagos rastreados han alcanzado los **820 millones de USD** a nivel global, repartidos entre un número mucho mayor de incidentes, pero de menor cuantía individual. Esta tendencia confirma un desplazamiento claro del modelo de negocio criminal hacia el volumen frente a la cantidad. A pesar de que los grupos de *ransomware* continúen reclamando importes muy elevados, el pago efectivo medio se sitúa en **592.000 USD** y una mediana de **325.000 USD** (SecurityToday, 2026), cifras muy por debajo de las cantidades que suelen recibir mayor atención mediática.

El verdadero coste rara vez coincide con el rescate exigido. Por ello, los **gastos derivados** de la disrupción operativa, la recuperación de sistemas, las obligaciones legales, las notificaciones regulatorias y el daño reputacional han seguido teniendo un peso mayor que la cantidad pagada por rescate.

En este sentido, la geografía sigue marcando diferencias notables. Estados Unidos encabeza el ranking mundial con **10,22 millones de USD** de coste medio por brecha (StationX, 2026). Esto supone la cifra más alta jamás registrada para el país, impulsada por unas sanciones regulatorias y unos litigios cada vez más costosos. Por su parte, en segunda posición, se mantiene Oriente Medio, como una de las regiones con mayor exposición económica a nivel global, con **7,29 millones de USD** por incidente (StationX, 2026). El promedio mundial del coste por brecha se ha situado en **4,44 millones de USD** (StationX, 2026), una cifra notablemente inferior a la estadounidense, con Europa manteniéndose por debajo de esa media gracias a marcos regulatorios más maduros y procesos de respuesta a incidentes más estandarizados entre sus organizaciones. Esta brecha geográfica refleja tanto diferencias normativas como distintos niveles de madurez en las capacidades de detección y contención de cada región.

Por último, la economía subterránea que sostiene todo este ecosistema se ha abaratado de forma drástica durante el semestre. El acceso a una red corporativa comprometida ha sufrido una **caída de precio** cercana al **70%**. En la actualidad, cuesta una media de **439 USD**, frente a los 1.427 USD que costaba hace apenas tres años (Crypto-Economy, 2026).

Esta deflación viene impulsada por la automatización, el uso de herramientas asistidas por inteligencia artificial en las fases de reconocimiento, y la sobreoferta de credenciales robadas mediante *infostealers*. El acceso al cibercrimen se está democratizando y se está ampliando considerablemente la base de actores capaces de monetizar una intrusión, incluso con escasas capacidades técnicas.



© 2026 NTT DATA, Inc.



5. Marco legal y detenciones en Ciberseguridad

Desde el **Departamento de Cyber Threat Intelligence de NTT DATA**, se considera esencial analizar las leyes aprobadas en materia de ciberseguridad y las operaciones realizadas por los cuerpos de seguridad a nivel global durante el primer semestre de 2026.
Este análisis permite evaluar el compromiso de los países en la regulación de tecnologías actuales y emergentes, así como el esfuerzo conjunto de organismos legislativos, judiciales y policiales para reforzar la resiliencia digital y combatir actividades ilícitas en el ciberespacio.

5.1 Principales leyes en el ámbito de la ciberseguridad

En el primer semestre de 2026, el marco legal y normativo en materia de ciberseguridad continuó **avanzando hacia un enfoque basado en la resiliencia operativa, la seguridad de producto, la protección de infraestructuras críticas, la obligación de reporte y la supervisión de proveedores tecnológicos**.

Entre los avances más relevantes destacan el desarrollo normativo del *Cyber Resilience Act* en la Unión Europea, la actualización del régimen europeo de sanciones frente a ciberataques, la aplicación progresiva del CMMC en Estados Unidos, la publicación de nuevas guías NIST y CERT-In, la entrada en vigor de la reforma de la *Cybersecurity Law* de China y la aplicación en Australia de obligaciones sobre dispositivos inteligentes y reporte de pagos por *ransomware*.

Continente	Normativa	Institución	Referencia
Europa	**Reglamento Delegado (UE) 2026/881**. Desarrollo del *Cyber Resilience Act*.	Comisión Europea / EUR-Lex	EUR-Lex - Reglamento Delegado (UE) 2026/881
Oceanía	***Smart Devices Rules* 2025**. Requisitos mínimos para dispositivos inteligentes.	Department of Home Affairs / Gobierno de Australia	Australian Department of Home Affairs - Security Standards for Smart Devices
Canadá	**Bill C-8 / *An Act Respecting Cyber Security***. Protección de sistemas cibernéticos críticos.	Gobierno de Canadá / Public Safety Canada	Public Safety Canada - Royal Assent of Bill C-8
América del Norte	**CMMC Phase 1**. Madurez de ciberseguridad en proveedores del DoD.	U.S. Department of Defense / DoD CIO	DoD CIO - Cybersecurity Maturity Model Certification
	NIST SP 800-172 Rev. 3 / 172A Rev. 3. Protección reforzada de información sensible.	NIST / CSRC	NIST CSRC - SP 800-172 Rev. 3; NIST CSRC - SP 800-172A Rev. 3
Asia	**Reforma de la *Cybersecurity Law* de China**. Actualización del régimen de cumplimiento y sanciones.	National People's Congress / Gobierno de China	Library of Congress - China: Amended Cybersecurity Law Takes Effect
América Latina	**Decreto 941/2025 y Disposición 1/2026**. Gobernanza nacional de ciberseguridad en Argentina.	Poder Ejecutivo Nacional / Centro Nacional de Ciberseguridad / Boletín Oficial de Argentina	Boletín Oficial - Decreto 941/2025; Boletín Oficial - CNC Disposición 1/2026

Tabla 3 | Leyes aprobadas o de aplicación en el primer semestre del 2026.

© 2026 NTT DATA, Inc.

Estos desarrollos refuerzan la conexión entre regulación y amenaza real. Las nuevas obligaciones se orientan a reducir superficies de ataque explotables, mejorar la visibilidad sobre incidentes y elevar los requisitos de seguridad en proveedores, productos digitales e infraestructuras críticas. Esto confirma una tendencia hacia marcos más operativos, en los que el cumplimiento se vincula cada vez más con la capacidad de prevención, detección, respuesta y recuperación frente a actores avanzados.



5.2 Principales detenciones en el ámbito de la ciberseguridad

Durante el primer semestre de 2026, la cooperación policial y judicial internacional frente al cibercrimen mantuvo un alto nivel de actividad. Las operaciones más relevantes se centraron en la neutralización de infraestructuras criminales utilizadas para *phishing*, *malware*, *ransomware*, *DDoS*, fraude financiero, servicios VPN criminales, *botnets* y redes de *proxies* residenciales.

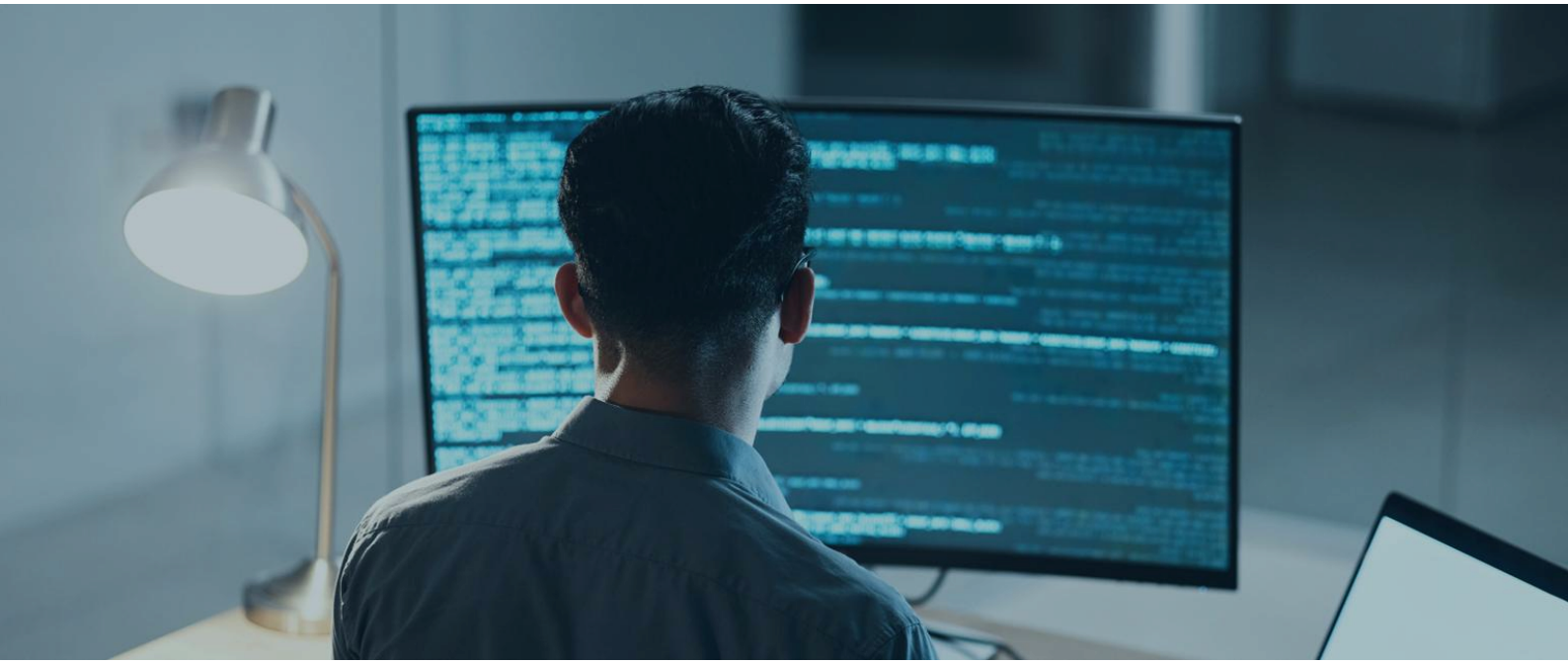
Estas acciones, coordinadas por organismos como INTERPOL, Europol, Eurojust, el Departamento de Justicia de EE. UU., cuerpos policiales nacionales y centros nacionales de ciberseguridad, reflejan una tendencia consolidada hacia modelos de disrupción operativa, en los que la inteligencia técnica, la cooperación transfronteriza y la incautación de infraestructura resultan clave para reducir la capacidad de actuación de los grupos criminales.

© 2026 NTT DATA, Inc.

Operación	Grupo o sector de amenazas	Fuerzas y cuerpos de seguridad	Resultados	Referencias
Operation Ramz	*Phishing, malware* y fraude online	INTERPOL y autoridades de 13 países de MENA	**201 arrestos**, 382 sospechosos identificados, 3.867 víctimas localizadas y **53 servidores incautados**.	INTERPOL Press Release
First VPN / Operation Saffron	VPN criminal usada por *ransomware*, intrusiones y ocultación de actividad	Europol, Eurojust, autoridades de Francia, Países Bajos, Ucrania y otros países	**33 servidores desmantelados** y búsqueda/interrogatorio de un sospechoso en Ucrania.	Europol / Eurojust
KimWolf Botnet	*DDoS-for-hire* / botnet IoT	DOJ, FBI, DCIS, autoridades canadienses y socios internacionales	Arresto en Canadá del presunto administrador; KimWolf habría infectado **más de un millón de dispositivos**.	DOJ Press Release
Botnet de proxies residenciales	Botnet / residential proxies	Policía de Países Bajos y NCSC-NL	Desmantelamiento de una botnet de al menos **17 millones de dispositivos infectados** y unos **200 servidores** en Países Bajos.	NCSC-NL / Politie.nl
FIOD hosting takedown	Infraestructura de *hosting* vinculada a ciberataques y evasión de sanciones	FIOD, autoridades neerlandesas	**2 detenidos** y más de **800 servidores incautados** en una investigación sobre apoyo a entidades sancionadas.	FIOD
CaaS bancario España-Francia	*Phishing, smishing* y fraude bancario bajo modelo Crime-as-a-Service	Policía Nacional, Europol, policía de Hannover y autoridades francesas	**3 detenidos,** 1,5 millones de euros en criptoactivos localizados y más de 4 millones de euros de perjuicio acreditado.	Ministerio del Interior
Operation KRATOS 2	Streaming ilegal y crimen organizado digital	Europol y autoridades europeas	**29 arrestos**, nueve grupos criminales desmantelados y más de **27.000 URLs ilegales** retiradas.	Europol
Operation Endgame / SocGholish	*Malware, Initial Access Broker, ransomware enablement*	Policía de Países Bajos, Canadá, EE. UU., Alemania, Europol y Eurojust	Limpieza de **14.971 sitios WordPress infectados**, desactivación de infraestructura asociada a SocGholish y acción contra una red vinculada a Evil Corp.	Politie.nl; Operation Endgame

Tabla 4 | Principales operaciones de desmantelamiento de bandas de cibercriminales llevadas a cabo en S1 de 2026.

© 2026 NTT DATA, Inc.



Caso destacado: Operation Endgame y la ofensiva contra SocGholish

En junio de 2026, una nueva fase de **Operation Endgame** se dirigió contra la infraestructura de **SocGholish**, también conocido como **FakeUpdates**, una operación de *malware* utilizada para comprometer sitios web legítimos y facilitar infecciones posteriores.
La acción fue coordinada por autoridades de Países Bajos, Canadá, Estados Unidos, Alemania y otros socios internacionales, con apoyo de Europol y Eurojust.

La operación permitió limpiar **14.971 sitios WordPress infectados** y desactivar **106 servidores y dominios** vinculados a la infraestructura criminal. Este volumen convierte el caso en una de las acciones más relevantes del semestre contra *malware* distribuido a través de sitios web legítimos comprometidos.
La relevancia del caso no reside únicamente en el volumen de infraestructura intervenida, sino en el papel de SocGholish como facilitador de accesos iniciales. Este tipo de *malware* permite comprometer usuarios mediante falsas actualizaciones del navegador y puede servir como puerta de entrada para robo de credenciales, despliegue de herramientas posteriores o campañas asociadas a *ransomware*.

Además, el caso conecta con actores de alto perfil. La Policía neerlandesa vincula SocGholish con **Evil Corp**, grupo históricamente asociado a *malware*, fraude financiero y operaciones de *ransomware*.

Esto refuerza el valor de la operación como acción contra una infraestructura habilitadora del cibercrimen, no solo contra un *malware* concreto.
En términos estratégicos, Operation Endgame muestra la evolución de las operaciones policiales hacia acciones de limpieza y disrupción a gran escala.



Al remediar miles de sitios web comprometidos y desactivar infraestructura asociada, **las autoridades reducen la superficie de infección disponible para los operadores, dificultan la continuidad de campañas activas** y obligan a los actores a reconstruir parte de su ecosistema técnico.

© 2026 NTT DATA, Inc.

Caso complementario: Operation Saffron y el desmantelamiento de First VPN

Otra operación relevante del semestre fue **Operation Saffron**, dirigida contra **First VPN**, un servicio promocionado en foros rusoparlantes de cibercrimen como herramienta para mantener el anonimato y evitar la cooperación con autoridades. Europol indicó que este servicio aparecía en prácticamente todas las grandes investigaciones de cibercrimen apoyadas por la agencia en los últimos años.
La operación permitió intervenir 33 servidores distribuidos en varios países y realizar una búsqueda e interrogatorio de un sospechoso en Ucrania. El caso destaca porque First VPN era utilizado por actores vinculados a *ransomware*, robo de datos, escaneo malicioso y ataques *DDoS*, por lo que su desmantelamiento afectó a una capa transversal de anonimización del ecosistema criminal.

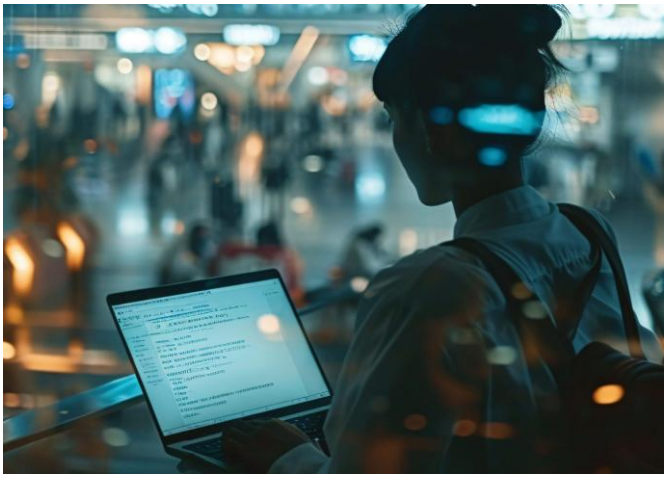
Regulación, disrupción e impacto operativo

El primer semestre de 2026 confirma una evolución relevante en la forma en que los Estados y organismos internacionales abordan el cibercrimen. El marco legal avanza hacia obligaciones más técnicas y verificables, mientras que las operaciones policiales muestran una mayor capacidad para actuar contra infraestructuras criminales complejas y distribuidas. Esta doble tendencia refleja un cambio de enfoque: la respuesta institucional ya no se limita a perseguir ataques concretos, sino que busca reducir la capacidad estructural de los actores para operar, escalar y monetizar sus campañas.
Las nuevas normas analizadas durante el semestre refuerzan áreas directamente relacionadas con las principales amenazas observadas en los últimos años: seguridad de producto, protección de infraestructuras críticas, control de proveedores, respuesta ante incidentes, protección de información sensible y reducción de vulnerabilidades explotables. Este enfoque resulta especialmente relevante en un contexto en el que los grupos criminales dependen cada vez más de cadenas de suministro, servicios legítimos comprometidos, dispositivos expuestos, credenciales robadas e infraestructuras de terceros para sostener sus operaciones.
En paralelo, las operaciones policiales del semestre muestran una mayor madurez en la disrupción del ecosistema criminal. Casos como **Operation Endgame / SocGholish**, vinculada a infraestructura utilizada para comprometer miles de sitios web y asociada a actores como **Evil Corp**, evidencian que las autoridades están priorizando servicios habilitadores del cibercrimen.

> La limpieza de sitios comprometidos, la incautación de servidores, el desmantelamiento de servicios VPN criminales, la neutralización de *botnets* y la identificación de operadores permiten afectar simultáneamente a múltiples campañas, en lugar de limitarse a una única víctima o incidente.

Esta evolución es significativa porque muchas operaciones criminales dependen de servicios compartidos: infraestructura de anonimización, *malware*, accesos iniciales, *hosting*, *botnets* y redes de fraude. Cuando una operación policial impacta sobre una de estas piezas, el efecto puede extenderse a varias campañas y obligar a los actores a migrar, reconstruir infraestructura o modificar sus procedimientos.
Aunque estas acciones no eliminan la amenaza, sí elevan el coste operativo del cibercrimen y reducen temporalmente su capacidad. Además, la información obtenida durante los desmantelamientos puede alimentar nuevas investigaciones y mejorar la visibilidad sobre relaciones entre actores, servicios e infraestructuras.

En conjunto, el semestre muestra una convergencia creciente entre regulación, inteligencia técnica y acción policial, consolidando una respuesta más coordinada frente a un ecosistema criminal cada vez más distribuido y profesionalizado.



© 2026 NTT DATA, Inc.



6. *Dark Web Insights*

Durante el primer semestre de 2026, el ecosistema *underground* mantuvo un alto nivel de actividad, pero bajo una presión policial y operativa creciente. La incautación de foros, el cierre de servicios utilizados por actores criminales y las operaciones contra infraestructuras habilitadoras no redujeron la demanda de datos robados, credenciales, accesos comprometidos o herramientas ofensivas, pero sí aceleraron la fragmentación del ecosistema (SOCRadar, 2026a; U.S. Department of Justice, 2026).

El periodo estuvo marcado por una mayor desconfianza hacia los grandes *hubs* centralizados. Actores, vendedores y afiliados continuaron migrando hacia foros alternativos, canales privados, Telegram, comunidades por invitación y mercados especializados en *logs*, credenciales, accesos iniciales y servicios de fraude. En este contexto, la reputación, la verificación entre actores y la capacidad de operar en espacios menos visibles se consolidaron como elementos clave para sostener la actividad criminal (SOCRadar, 2026).

También se observó una **mayor presencia de la inteligencia artificial en conversaciones y ofertas dentro de comunidades *underground***. Su uso aparece vinculado principalmente a automatización, generación de contenido para *phishing*, ingeniería social, análisis de datos robados y soporte al desarrollo de herramientas, aunque todavía conviven capacidades reales, experimentación y reclamos comerciales exagerados (Sophos, 2026).

6.1 Presión policial y reconfiguración del ecosistema *underground*

El primer semestre de 2026 estuvo marcado por nuevas acciones contra plataformas utilizadas para el comercio de datos robados y servicios criminales. El caso más relevante fue el desmantelamiento de **LeakBase**, una operación liderada por Estados Unidos y coordinada internacionalmente que afectó a uno de los mayores foros de compraventa de información robada.

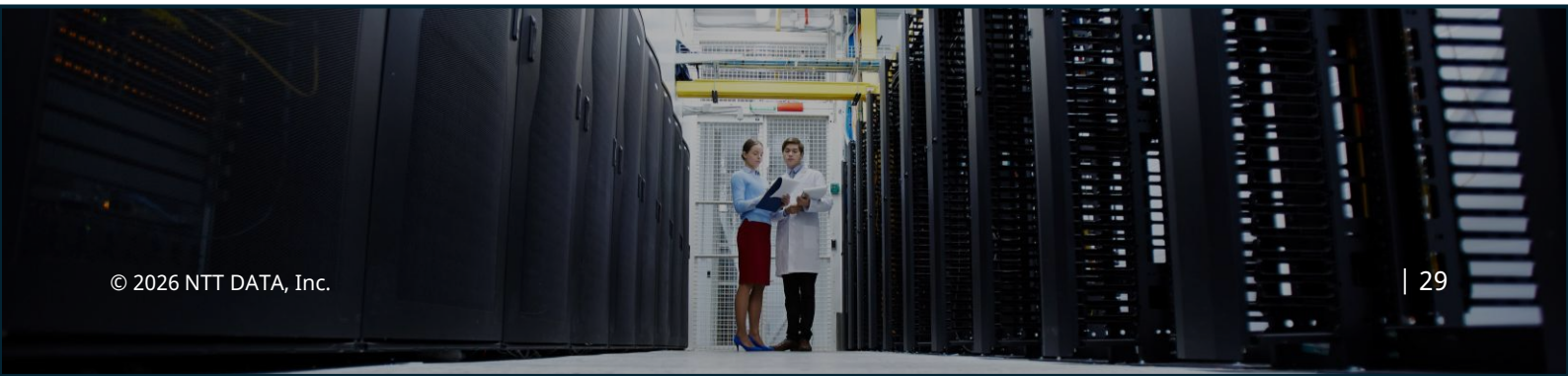
Según el Departamento de Justicia de EE. UU., LeakBase contaba con más de **142.000 miembros** y más de **215.000 mensajes privados**, y permitía a sus usuarios vender información procedente de bases de datos robadas, credenciales y otros datos ilícitos (U.S. Department of Justice, 2026).

La operación permitió incautar dominios, datos del foro, cuentas, publicaciones, mensajes privados y registros técnicos, lo que incrementa el riesgo para usuarios y vendedores que habían utilizado la plataforma. Más allá del cierre del foro, el impacto principal reside en la pérdida de confianza: cuando una plataforma centralizada queda bajo control policial, la información interna puede alimentar investigaciones posteriores y exponer relaciones entre actores, compradores, vendedores e infraestructuras (U.S. Department of Justice, 2026).

En paralelo, la incautación de **RAMP**, foro asociado históricamente a *ransomware* y servicios relacionados, reforzó la percepción de que incluso espacios especializados y de alto valor operativo pueden ser alcanzados. SOCRadar señala que entre 2025 y principios de 2026 varios foros dominantes fueron interrumpidos, incluyendo LeakBase, RAMP y BreachForums, lo que refleja una reconfiguración del ecosistema hacia plataformas más segmentadas y canales privados (SOCRadar, 2026a).

El resultado no es la desaparición de la actividad criminal, sino su redistribución. La presión sobre los grandes foros acelera el desplazamiento hacia espacios alternativos, reduce la confianza en administradores y vendedores, y obliga a los actores a diversificar canales de comunicación, venta y reclutamiento.

> Para la monitorización CTI, esto implica un entorno más disperso, menos visible y más dependiente de reputación, acceso privado y seguimiento continuo de migraciones.



© 2026 NTT DATA, Inc.

6.2 Foros *underground* activos

Durante el primer semestre de 2026, la actividad en foros *underground* se mantuvo activa, aunque más distribuida que en periodos anteriores. Tras la disrupción de plataformas consolidadas, parte de la actividad se desplazó hacia foros técnicos rusoparlantes, comunidades de *leaks*, espacios de discusión sobre mercados y canales privados utilizados para compraventa de accesos, credenciales, herramientas y servicios criminales (SOCRadar, 2026).

Los foros más relevantes durante el periodo pueden agruparse en tres grandes categorías:

- **Foros técnicos rusoparlantes**

Plataformas como **Exploit.in** y **XSS** siguieron siendo espacios relevantes para actores con mayor especialización técnica, especialmente en torno a *exploits*, accesos iniciales, *malware*, servicios ofensivos y compraventa de información comprometida. Ambos foros se sitúan entre los principales espacios monitorizados en 2026, junto con otros entornos como **BHF** y **DamageLib** (SOCRadar, 2026a).

- **Comunidades de discusión, reputación y mercados**

Dread mantuvo su papel como uno de los principales espacios de discusión del ecosistema *darknet*, con funciones similares a un foro social donde se debaten mercados, reputación de vendedores, alertas de estafas, caídas de plataformas y cambios operativos. Este tipo de comunidades no solo concentran actividad criminal, sino que también actúan como mecanismo de confianza y validación entre actores (SOCRadar, 2026).

- **Foros angloparlantes de *leaks*, *cracking* y credenciales**

Foros como **Cracked**, **DarkForums**, **CryptBB** y **Altenen** continuaron apareciendo en investigaciones y seguimiento de actividad relacionada con credenciales filtradas, *combo lists*, configuraciones de *stealers*, herramientas automatizadas, bases de datos expuestas y servicios de fraude. Estos espacios suelen atraer perfiles de distinto nivel técnico y funcionan como puntos de entrada para actores menos sofisticados, pero también como canales de distribución de datos útiles para campañas posteriores (SOCRadar, 2026a; CloudSEK, 2026).

En conjunto, el semestre confirma que la actividad no desaparece tras la caída o incautación de grandes foros, sino que se redistribuye hacia plataformas alternativas y comunidades con distintos niveles de acceso.

Esta reconfiguración, iniciada a finales de 2025 y consolidada durante el primer semestre de 2026, reduce la visibilidad directa sobre determinadas operaciones y aumenta la importancia de monitorizar espacios secundarios, canales privados y comunidades especializadas.

> Tras la disrupción de plataformas consolidadas, parte de la actividad se desplazó hacia foros técnicos, comunidades de *leaks*, y canales para compraventa de servicios criminales.

Foros y espacios *underground* activos en S1 2026



Figura 5 | Principales tipos de foros y espacios *underground* activos durante el primer semestre de 2026.

© 2026 NTT DATA, Inc.

Principales publicaciones en la *dark web* en S1 2026

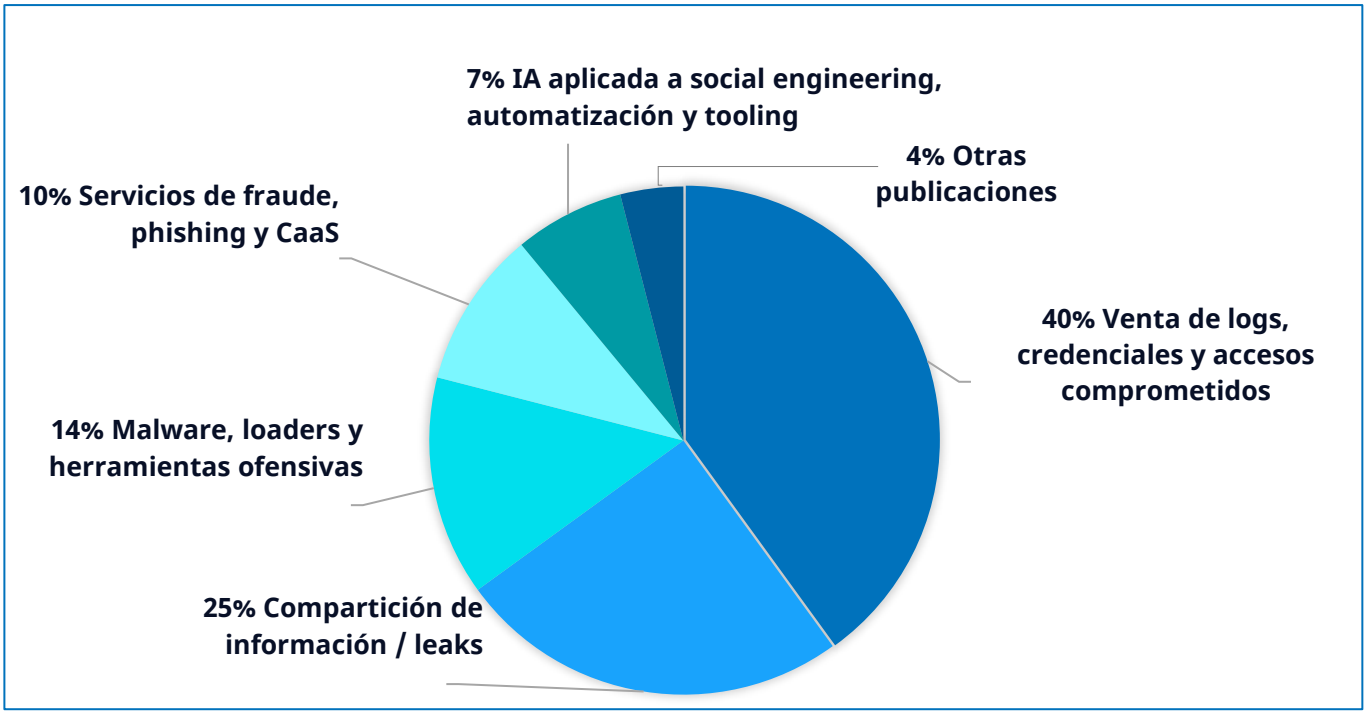


Figura 6 | Principales categorías de publicaciones en la *dark web* en el primer semestre de 2026.

Los datos estimados muestran un ecosistema *underground* cada vez más orientado a la monetización de credenciales, *logs* de *infostealers* y accesos comprometidos. Aunque la compartición de información y las filtraciones siguen siendo relevantes, pierden peso relativo frente a mercados más especializados en acceso inicial, fraude, herramientas ofensivas y servicios criminales.
Durante el primer semestre de 2026, también se observa una presencia creciente de publicaciones vinculadas a inteligencia artificial, especialmente en automatización, generación de contenido para *phishing*, ingeniería social y soporte al desarrollo de herramientas, aunque su adopción real sigue combinando capacidades efectivas, experimentación y reclamos comerciales exagerados (SOCRadar, 2026b; Sophos, 2026).

6.3 Mercados *underground* activos

Durante el primer semestre de 2026, el ecosistema de mercados *underground* se mantuvo activo, aunque con una estructura más fragmentada y especializada.
Las disrupciones policiales, los cierres de foros y la inestabilidad de algunos mercados no redujeron la actividad criminal, sino que favorecieron una redistribución hacia plataformas centradas en credenciales, *infostealer logs*, accesos iniciales, datos de pago y servicios de fraude (SOCRadar, 2026b; BreachSense, 2026).

Los mercados orientados a credenciales y *logs* continuaron siendo especialmente relevantes. Plataformas como **Russian Market** mantienen un papel central en la compraventa de credenciales robadas, *cookies*, datos de navegador, accesos corporativos y registros procedentes de *infostealers*. Este modelo refuerza la conexión entre mercados *underground*, intermediarios de acceso inicial y campañas posteriores de fraude, intrusión o *ransomware* (SOCRadar, 2026b; BreachSense, 2026).
En paralelo, los mercados de *carding* y fraude financiero conservaron un papel relevante dentro del ecosistema. **BriansClub** continuó apareciendo como una referencia histórica en la compraventa de tarjetas comprometidas, mientras que mercados como **STYX Market** mantuvieron actividad vinculada a fraude, *phishing*, servicios financieros ilícitos y herramientas de soporte operativo.

© 2026 NTT DATA, Inc.

Aunque el *carding* ha perdido parte de su protagonismo frente a los *stealer logs* y los accesos corporativos, sigue siendo una categoría estructural dentro de la economía criminal digital (SOCRadar, 2026b).

También se observó la consolidación de mercados con una orientación más amplia o especializada en servicios de intrusión. Plataformas como **TorZon Market**, **Exodus Marketplace**, **Vortex Marketplace**, **Anubis Market**, **FreshTools** y **WeTheNorth Market** aparecen en fuentes de inteligencia como espacios relevantes para el seguimiento de datos robados, herramientas, accesos, servicios fraudulentos y actividad criminal distribuida. Su relevancia varía según el momento, pero reflejan un ecosistema en el que los vendedores migran rápidamente cuando un mercado cae, pierde confianza o se vuelve menos operativo (SOCRadar, 2026b; DeepStrike, 2026).

La tendencia principal del semestre es la especialización funcional. Los mercados ya no actúan únicamente como plataformas generalistas de compraventa, sino como **nodos dentro de una cadena criminal más amplia**: unos facilitan credenciales, otros proporcionan accesos iniciales, otros concentran tarjetas comprometidas y otros ofrecen servicios de fraude o herramientas ofensivas. Esta división permite que actores con distintos niveles de sofisticación accedan a recursos criminales bajo modelos cada vez más profesionalizados.

A nivel operativo, esta fragmentación obliga a ampliar la monitorización más allá de los mercados dominantes. Los actores alternan entre *marketplaces*, foros, canales privados y servicios cerrados para reducir exposición, mantener reputación y asegurar continuidad comercial. Por ello, el seguimiento de mercados *underground* en 2026 debe centrarse no solo en plataformas concretas, **sino también en los flujos de datos, vendedores, categorías de producto y migraciones entre espacios.**

Función de los *marketplaces underground* en S1 2026

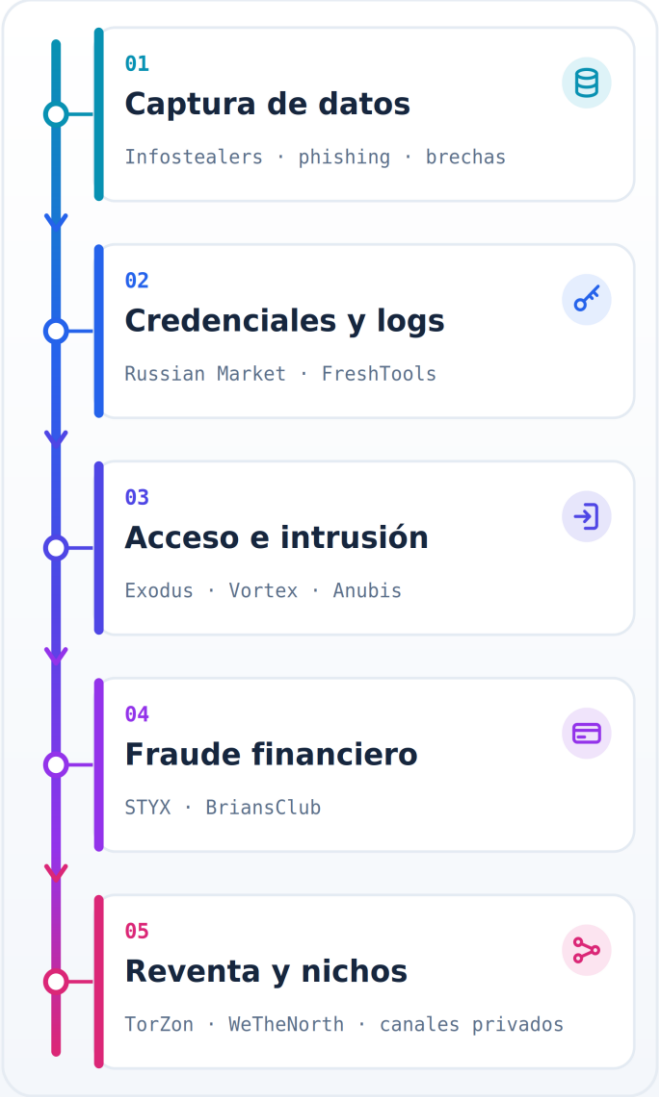


Figura 7 | Función de los principales *marketplaces underground* dentro de la cadena criminal durante el primer semestre de 2026.

Aunque el *carding* ha perdido parte de su protagonismo frente a los *stealer logs* y los accesos corporativos, sigue siendo una categoría estructural dentro de la economía criminal digital.

© 2026 NTT DATA, Inc.

A continuación, se muestra la distribución estimada de las principales plataformas de venta *underground* activas durante el primer semestre de 2026, en función de su volumen de actividad observada, especialización criminal y relevancia dentro del ecosistema.

Plataformas de venta *underground* en S1 2026

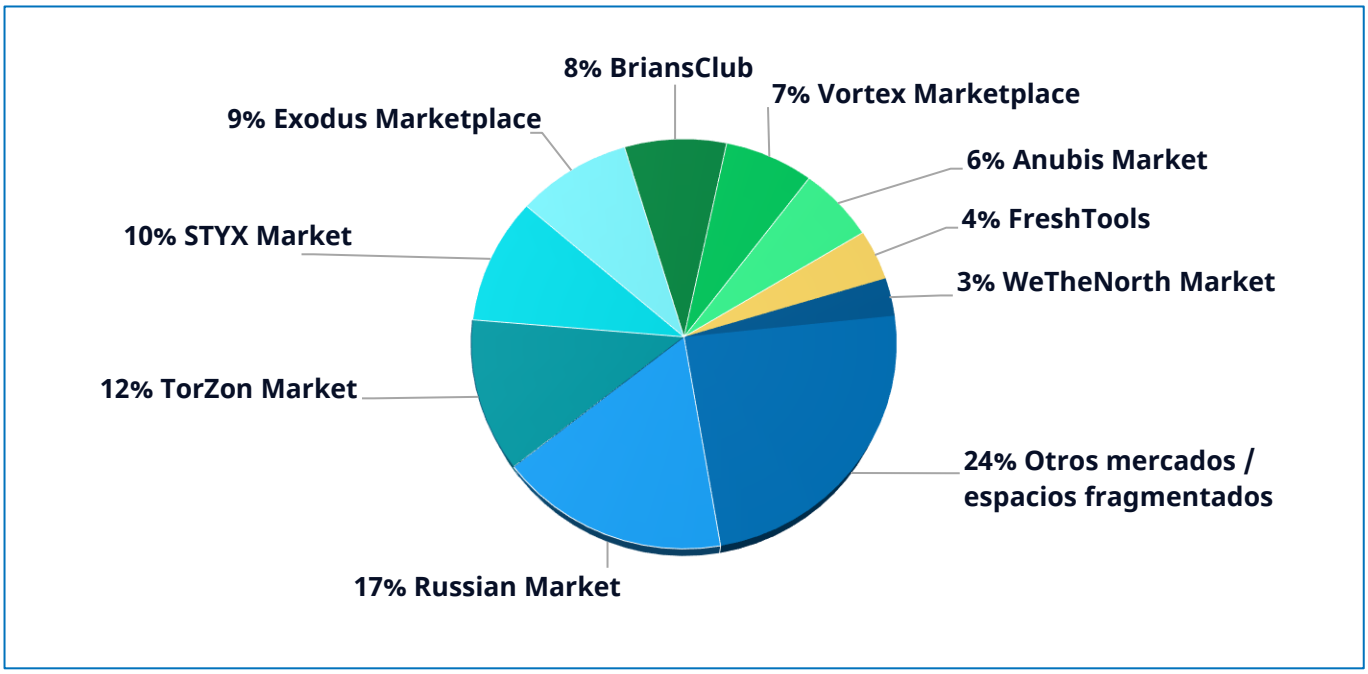
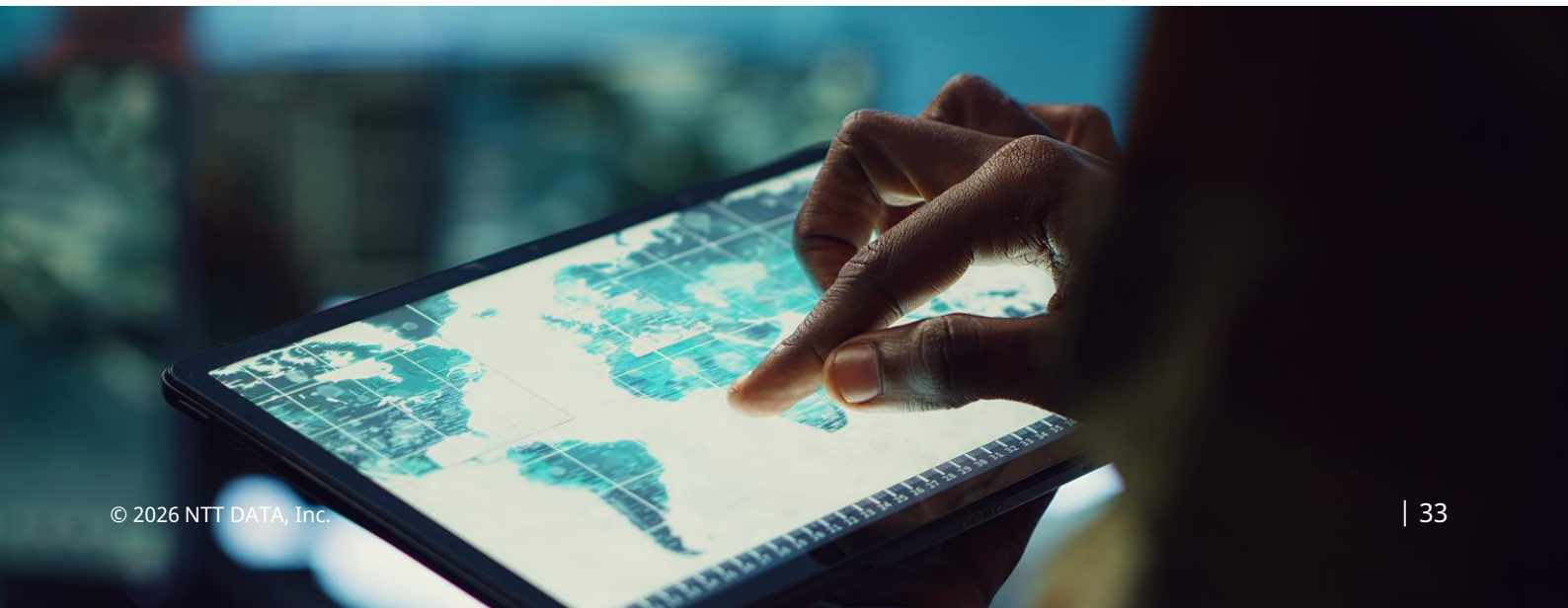


Figura 8 | Principales plataformas de venta *underground* identificadas en el primer semestre de 2026.

La distribución estimada refleja un ecosistema de mercados *underground* más fragmentado y funcionalmente especializado. **Russian Market** mantiene un peso destacado por su orientación a credenciales, *stealer logs*, *cookies* y accesos corporativos, mientras que **STYX Market**, **Exodus Marketplace** y **TorZon Market** concentran actividad relacionada con fraude, accesos, herramientas y servicios criminales.
El peso de "otros mercados / espacios fragmentados" evidencia la pérdida de centralidad de los grandes *marketplaces* y el desplazamiento hacia plataformas de nicho, canales privados y servicios de ciclo de vida más corto.



© 2026 NTT DATA, Inc.



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.**

Han predominado 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 señaló la creciente **diversificación** del ecosistema de amenazas y la aparición de actores cada vez más especializados. Los nuevos grupos identificados durante este periodo reflejan esa evolución mediante perfiles operativos diferenciados que abarcan tanto actividades de **ciberespionaje** estratégico como campañas **de robo de información orientadas al fraude**. Su actividad evidencia un panorama más **fragmentado**, en el que actores emergentes desarrollan capacidades específicas para alcanzar objetivos concretos, ya sea la obtención de inteligencia sensible o la monetización ilícita de datos comprometidos. Asimismo, la **recopilación y exfiltración de información** continúa consolidándose como uno de los principales objetivos operativos, independientemente de la motivación final de los actores implicados.

Diaoyu

Detectado en febrero de 2026, **Diaoyu** es un actor de amenazas vinculado a actividades de **ciberespionaje** y presuntamente alineado con intereses estatales **chinos**. El grupo ha llevado a cabo campañas dirigidas contra organismos gubernamentales, entidades de investigación y organizaciones estratégicas en al menos 37 países, comprometiendo más de 70 instituciones mediante el uso de *malware* personalizado y técnicas avanzadas de persistencia y evasión. Su actividad se caracteriza por operaciones de larga duración orientadas a la obtención de inteligencia sensible, aprovechando infraestructuras encubiertas y herramientas desarrolladas específicamente para evitar su detección. Aunque la atribución definitiva sigue siendo limitada, diversos indicios técnicos apuntan a una operación altamente sofisticada y con importantes recursos, lo que refuerza la hipótesis de un respaldo estatal. A pesar de la reciente exposición pública de sus actividades, no existen evidencias de que el grupo haya cesado sus operaciones, por lo que continúa siendo considerado una amenaza activa para organismos gubernamentales y sectores estratégicos a nivel global (Shenouda, 2026).



© 2026 NTT DATA, Inc.

Insomnio

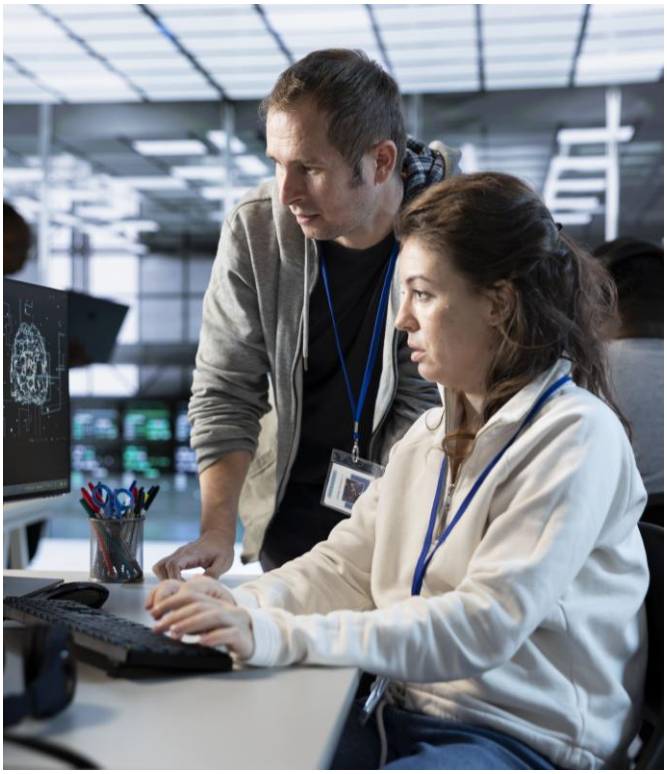
Identificado públicamente también en febrero de 2026, **Insomnio** es un actor de amenazas especializado en la **distribución de *malware* para Android** mediante campañas de **ingeniería social** dirigidas a usuarios de dispositivos móviles. Su actividad se centra en la suplantación de aplicaciones legítimas y el uso de sitios web fraudulentos para inducir a las víctimas a instalar aplicaciones maliciosas capaces de recopilar credenciales, información financiera y otros datos sensibles. El grupo destaca por el uso de infraestructuras de distribución adaptables y por la rápida rotación de dominios y recursos maliciosos para dificultar su detección y bloqueo. Aunque su actividad conocida se ha centrado principalmente en el robo de información, las capacidades observadas sugieren una evolución hacia operaciones más amplias de fraude móvil y compromiso de cuentas. Su aparición refuerza la tendencia creciente de actores emergentes que explotan el ecosistema Android como vector principal de acceso a información sensible y monetización ilícita (Shenouda, 2026).

7.2 *Ransomware*

La actividad de *ransomware* durante el primer semestre de 2026 ha confirmado la consolidación de un ecosistema altamente **competitivo**, caracterizado por la madurez del modelo **R*ansomware-as-a-Service* (RaaS**), la **movilidad de afiliados** y una **creciente capacidad de adaptación** por parte de los principales operadores. La persistencia de campañas a escala global, la aparición de nuevos actores con capacidad para ganar relevancia rápidamente y la continuidad de estrategias basadas en la doble extorsión reflejan un panorama cada vez más **profesionalizado**. En este contexto, los grupos de *ransomware* han mantenido su enfoque en organizaciones y sectores donde la interrupción operativa, la presión reputacional y el valor de la información comprometida maximizan las oportunidades de monetización (DarkFeed, 2026).

7.2.1 Nuevos grupos

La distribución temporal de los nuevos actores observados durante el primer semestre de 2026 ha reflejado un ecosistema especialmente dinámico y fragmentado, con una incorporación constante de grupos a lo largo de todo el periodo. Los primeros meses del año estuvieron marcados por la aparición de múltiples actores de perfil todavía limitado o emergente, lo que sugiere una baja barrera de entrada y una elevada rotación dentro del panorama criminal. Marzo y, especialmente, abril concentraron el mayor número de nuevos grupos identificados, evidenciando una fase de fuerte proliferación y diversificación operativa, con la coexistencia de actores vinculados a campañas de acceso inicial y operaciones de intrusión más especializadas. A partir de mayo se observa una reducción del volumen de nuevas incorporaciones, aunque los grupos detectados presentan una identidad operativa más definida y una mayor orientación hacia modelos de extorsión y monetización ya consolidados.
En conjunto, el semestre confirma la continuidad de una tendencia caracterizada por la atomización del ecosistema de amenazas, la rápida aparición de nuevos actores y la consolidación de estructuras cada vez más flexibles y adaptables, donde la permanencia de los grupos resulta menos relevante que su capacidad para integrarse en redes criminales más amplias y aprovechar herramientas y modelos operativos previamente establecidos.



© 2026 NTT DATA, Inc.

Nuevos grupos de *ransomware* del S1 2026

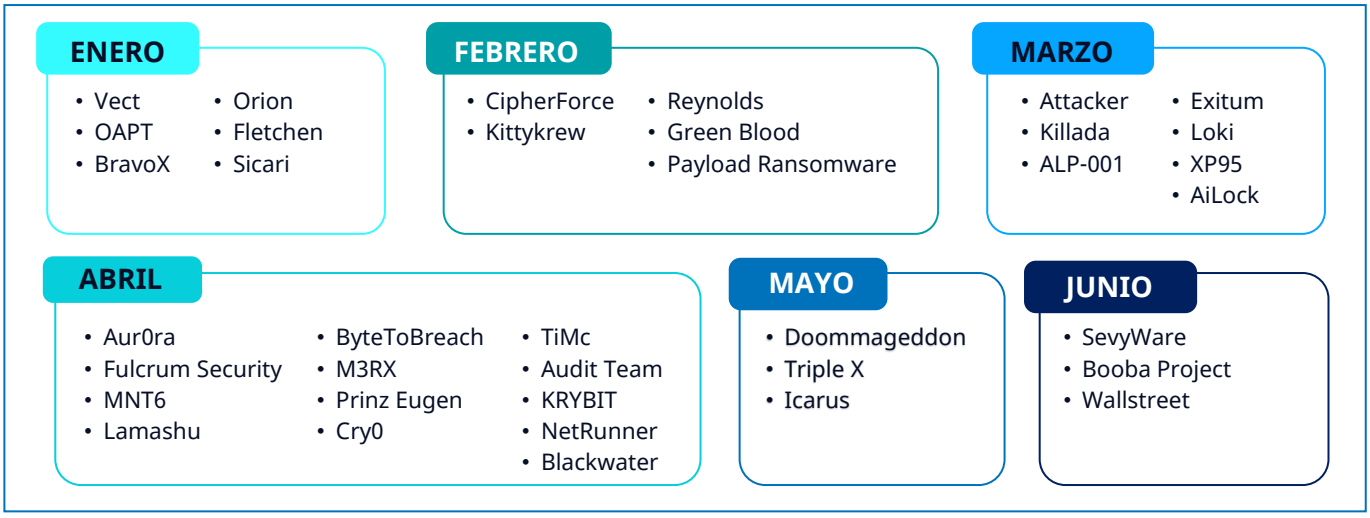


Figura 9 | Grupos de *ransomware* detectados en el primer semestre de 2026.

Este semestre destaca **CipherForce**, uno de los nuevos grupos de *ransomware* que emergieron durante febrero de 2026. A pesar de su reciente aparición, el colectivo logró posicionarse rápidamente dentro del ecosistema criminal mediante la publicación de múltiples víctimas en sus plataformas de filtración. Su evolución pone de manifiesto la creciente facilidad con la que nuevos actores pueden incorporarse al panorama *ransomware* aprovechando herramientas, infraestructuras y servicios criminales ya disponibles en el mercado clandestino. Más que representar una innovación técnica, **CipherForce** ejemplifica la continua renovación del ecosistema de extorsión digital, donde grupos emergentes pueden alcanzar visibilidad operativa en plazos cada vez más reducidos gracias a la reutilización de capacidades previamente desarrolladas por otros colectivos.



7.2.2 Grupos más activos

La actividad de *ransomware* durante el primer semestre de 2026 ha mostrado un ecosistema altamente dinámico, caracterizado por cambios frecuentes en el liderazgo operativo y una creciente competencia entre grupos por atraer afiliados y mantener visibilidad. A diferencia de periodos anteriores, ningún actor ha logrado monopolizar la actividad durante todo el semestre, observándose continuos movimientos de ascenso, descenso y sustitución entre los principales operadores. Esta volatilidad refleja un mercado RaaS cada vez más maduro, donde la capacidad de adaptación resulta tan importante como la sofisticación técnica.

- **Qilin:** ha mantenido el liderazgo global durante gran parte del semestre y continúa siendo uno de los actores más relevantes del ecosistema de *ransomware*. Sin embargo, tras alcanzar su máximo nivel de actividad en marzo, experimentó una reducción progresiva de operaciones durante los meses posteriores. Su posición confirma la fortaleza de su modelo operativo, aunque la pérdida gradual de actividad sugiere una competencia creciente por parte de grupos emergentes.

- **The Gentlemen:** ha protagonizado la evolución más consistente del semestre. Tras iniciar el periodo con niveles moderados de actividad, registró un crecimiento sostenido hasta convertirse en el grupo más activo en junio.

© 2026 NTT DATA, Inc.

Esta trayectoria refleja una expansión progresiva de capacidades y una consolidación operativa que lo sitúa entre los actores emergentes más relevantes del panorama actual. Ha sobresalido como representante de una generación de operadores más pequeños, pero altamente activos. Su presencia refuerza la tendencia hacia una mayor fragmentación del panorama del *ransomware*, donde grupos emergentes aprovechan espacios dejados por actores tradicionales para ganar relevancia y ampliar sus operaciones.

- **DragonForce**: ha destacado por experimentar uno de los crecimientos más rápidos observados durante el semestre. Su actividad aumentó de forma continuada hasta mayo, alcanzando niveles comparables a los principales operadores del ecosistema. Su actividad ilustra la creciente profesionalización del cibercrimen organizado y la tendencia hacia estructuras criminales capaces de integrar afiliados, recursos e infraestructuras bajo modelos cada vez más flexibles.
- **Akira**: ha mantenido una presencia relevante durante todo el semestre, aunque con una tendencia descendente tras alcanzar su punto máximo en marzo. La reducción progresiva de su actividad sugiere una pérdida relativa de protagonismo frente a operadores más dinámicos, manteniéndose no obstante como uno de los grupos con mayor continuidad dentro del ecosistema *ransomware*.
- **LockBit**: ha mostrado una evolución irregular, caracterizada por una actividad limitada al inicio del semestre y una recuperación gradual durante los últimos meses. Su repunte en junio evidencia que, pese a las presiones policiales y operativas sufridas en periodos anteriores, la marca continúa conservando capacidad de influencia y presencia dentro del panorama *ransomware* global (DarkFeed, 2026).

Top grupos de *ransomware* del S1 2026

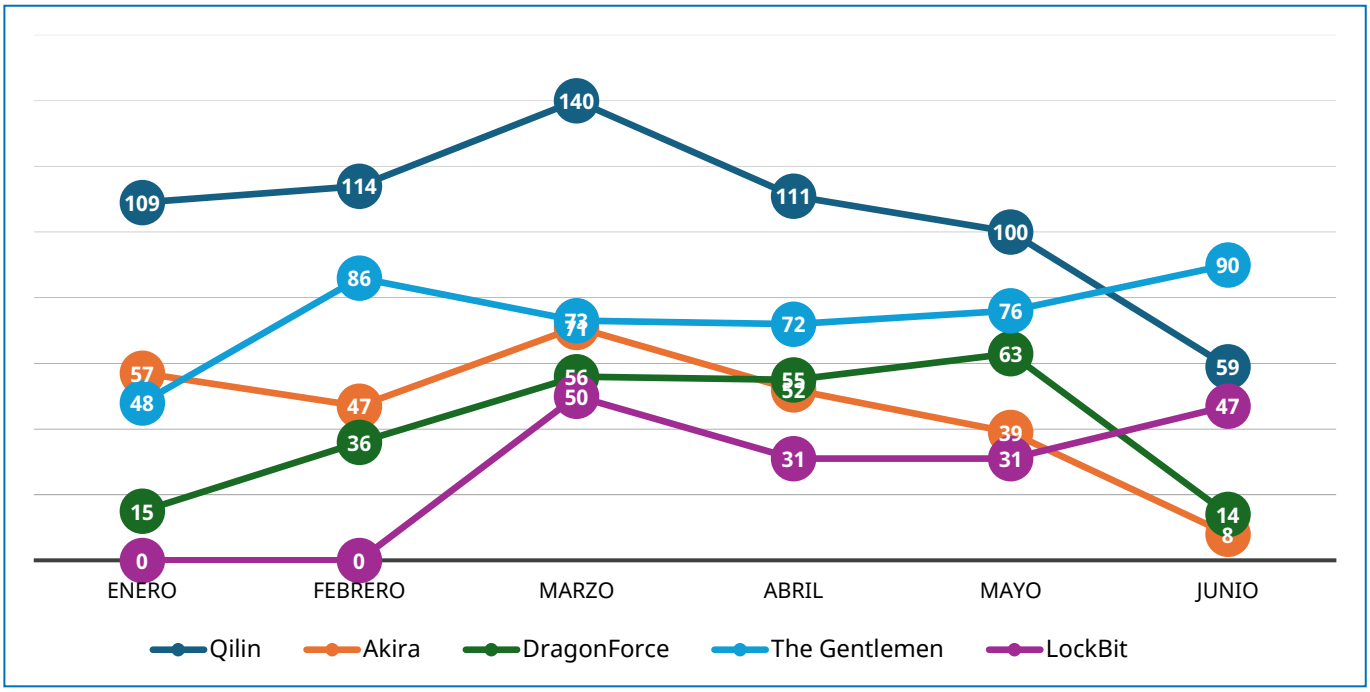


Figura 10 | Actividad de los grupos de *ransomware* más activos en el primer semestre de 2026.

© 2026 NTT DATA, Inc.

7.2.3 Afectación global

La distribución geográfica de las víctimas durante el primer semestre de 2026 confirma la continuidad de una tendencia ya observada en periodos anteriores: la actividad de *ransomware* sigue concentrándose principalmente en economías desarrolladas, con un claro predominio de **Estados Unidos** y una presencia sostenida en **Europa Occidental**. Estados Unidos se mantuvo como principal objetivo durante todo el semestre, acumulando 1.838 víctimas y registrando cifras muy superiores al resto de países, consolidándose como el principal foco global de actividad *ransomware.* En un segundo nivel se sitúan **Reino Unido, Canadá, Alemania e Italia**, que han mantenido una presencia constante entre los países más afectados. España y Francia también registraron una actividad relevante, confirmando que Europa Occidental continúa siendo una de las regiones más expuestas a este tipo de amenazas debido a su elevada digitalización y concentración de organizaciones de alto valor.

Los datos muestran además una diversificación progresiva hacia otras regiones. India, Tailandia, Japón y Australia aparecen de forma recurrente entre los países más afectados, mientras que Brasil mantiene una presencia destacada en América Latina. Aunque los volúmenes son inferiores a los observados en Norteamérica y Europa, su recurrencia evidencia un alcance cada vez más global de las campañas.

En conjunto, la tendencia del semestre mantiene un doble patrón: una fuerte concentración de víctimas en Estados Unidos y las principales economías occidentales, junto con una expansión sostenida hacia nuevas regiones favorecida por la madurez del modelo RaaS y la capacidad de los operadores para ejecutar campañas simultáneas a escala internacional (DarkFeed, 2026).

Países más afectados por *ransomware* del S1 2026

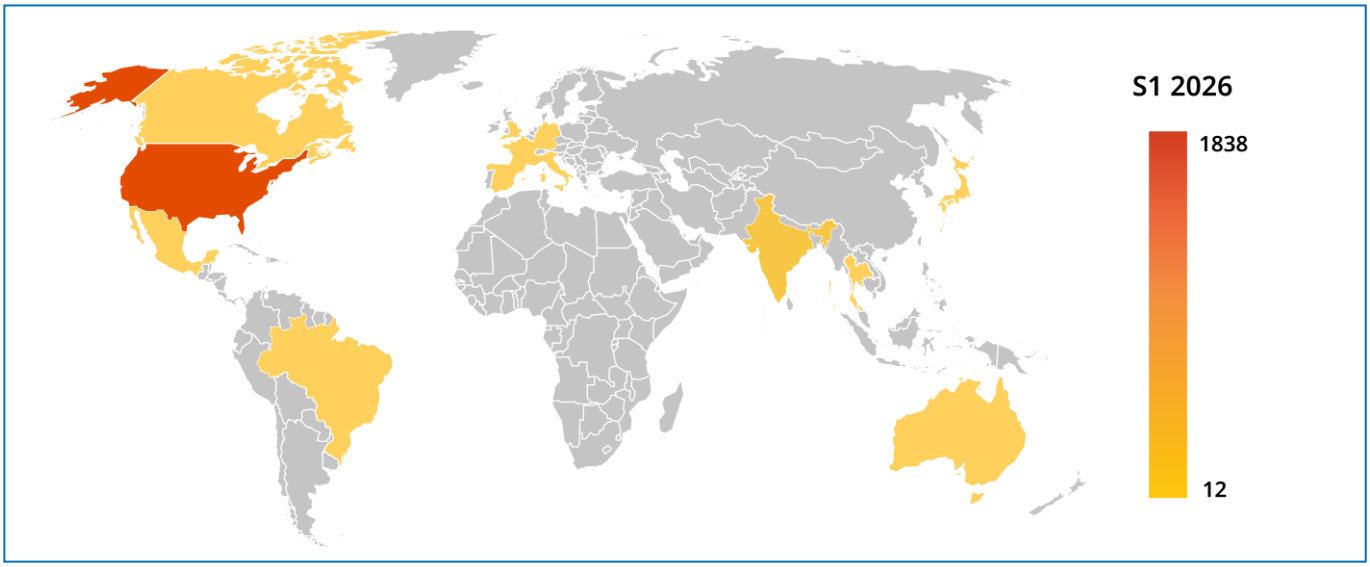


Figura 11 | Países más afectados por *ransomware* en el primer semestre de 2026.



© 2026 NTT DATA, Inc.

Por otro lado, el **análisis sectorial** del primer semestre de 2026 confirma la continuidad de una tendencia ya observada en periodos anteriores: los grupos de *ransomware* siguen concentrando sus esfuerzos en sectores donde la interrupción operativa genera un impacto económico inmediato y aumenta la presión para negociar. **Consultoría** se mantuvo como el sector más afectado durante todo el semestre, registrando los mayores volúmenes de víctimas de forma constante. Su atractivo radica en el acceso a información sensible, la gestión de servicios para terceros y el potencial efecto multiplicador que una intrusión puede generar sobre múltiples organizaciones.

Manufactura, salud y construcción conformaron un segundo bloque de sectores especialmente afectados. La manufactura mantuvo una presión sostenida a lo largo de todo el periodo, reforzando la tendencia observada hacia el *targeting* de entornos industriales y cadenas de producción críticas. El sector **sanitario** también registró una actividad elevada y constante, especialmente durante la parte central del semestre, reflejando el elevado valor coercitivo asociado a organizaciones con una baja tolerancia a la interrupción de sus servicios. De forma similar, la **construcción** continuó siendo un objetivo recurrente, impulsada por una creciente digitalización y por la dependencia de proyectos con plazos operativos ajustados.

Los **servicios IT** mantuvieron igualmente una presencia estable entre los sectores más afectados, mientras que comercio **minorista (*retail*), financiero y educación** registraron picos de actividad más localizados. Aunque su volumen global fue inferior al de los sectores líderes, su presencia recurrente evidencia que los operadores continúan buscando organizaciones capaces de generar impacto económico, acceso a terceros o presión reputacional.

Desde una perspectiva estructural, el semestre muestra una consolidación de las estrategias de selección de objetivos observadas en años anteriores. Más que ampliar significativamente el abanico de sectores afectados, los operadores han continuado priorizando aquellos donde los costes de interrupción, la sensibilidad de la información o la presión temporal incrementan la probabilidad de pago. En este sentido, la evolución del semestre refuerza la tendencia hacia campañas cada vez más selectivas y orientadas al impacto operativo, anticipando la continuidad de este patrón durante el resto de 2026.

Ataques de *ransomware* por sector en S1 2026

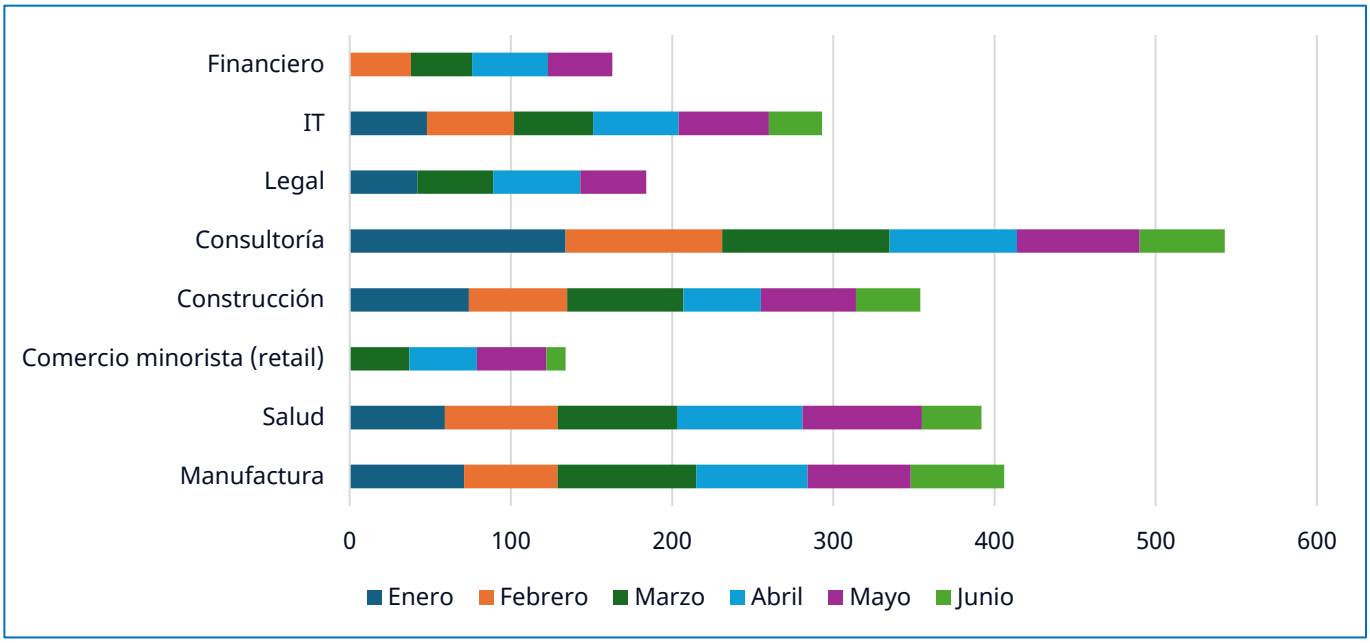


Figura 12 | Sectores más afectados por *ransomware* en el primer semestre de 2026.

© 2026 NTT DATA, Inc.

7.3 Hacktivismo

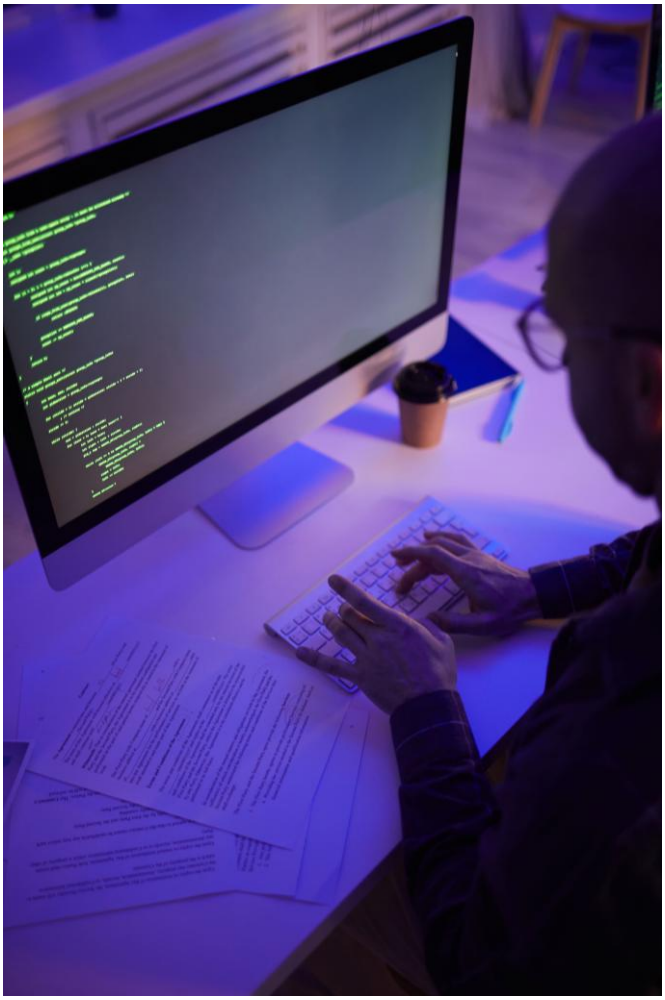
Durante el primer semestre de 2026 se ha observado una consolidación del fenómeno hacktivista como herramienta de presión geopolítica, caracterizada por una mayor coordinación entre colectivos, una rápida capacidad de movilización y una creciente orientación hacia la interrupción operativa y el impacto reputacional más que hacia operaciones de espionaje prolongadas. La actividad registrada confirma que el hacktivismo continúa evolucionando hacia modelos más organizados y visibles, capaces de reaccionar con rapidez ante acontecimientos internacionales y amplificar su impacto mediante campañas coordinadas (Orange Cyberdefense, 2026).

El ecosistema ha seguido articulándose en torno a bloques regionales e ideológicos definidos. El entorno prorruso ha mantenido un papel central, liderado por colectivos como **NoName057(16**) y respaldado por actores como **DieNet**, que han continuado dirigiendo campañas contra organismos gubernamentales, infraestructuras críticas y entidades vinculadas a países occidentales y de la OTAN. Paralelamente, los grupos alineados con la causa palestina y otras corrientes político-religiosas, entre ellos **Handala, Cyber Islamic Resistance, Nation of Saviors, Liwaa Mohammad, Team Fearless y 313 Team**, han incrementado su visibilidad aprovechando los principales focos de tensión en Oriente Medio y reforzando la dimensión ideológica del hacktivismo contemporáneo.

Por otro lado, se ha consolidado un eje de actividad en Asia-Pacífico y el norte de África, donde colectivos como **RipperSec, Sylhet Gang-SG, Keymous Plus y Moroccan Black Cyber Army** han participado en campañas de alcance internacional. Asimismo, grupos como **DarkStorm** han actuado como elementos conectores entre distintos ecosistemas regionales, facilitando la difusión de narrativas, reivindicaciones y objetivos comunes, y reforzando un modelo de cooperación flexible que permite aumentar el alcance de las operaciones sin necesidad de estructuras centralizadas (SOCRadar, 2026c).

La actividad observada durante el semestre ha confirmado un perfil orientado principalmente a la **disrupción** y la **presión simbólica**, con un predominio de **ataques DDoS, *defacements*, filtraciones de datos, *doxing* y campañas de presión psicológica y reputacional**. La rápida ejecución de estas acciones y su elevada visibilidad pública han convertido la interrupción temporal de servicios y el impacto mediático en los principales indicadores de éxito para estos colectivos, por encima de la persistencia técnica o la obtención de acceso prolongado a las redes comprometidas (Fortinet, 2026).

En conjunto, se ha confirmado la evolución del hacktivismo hacia un ecosistema más **coordinado, globalizado y estrechamente vinculado al contexto geopolítico internacional**. La creciente colaboración entre colectivos y su capacidad para sincronizar campañas contra infraestructuras críticas, organismos públicos y entidades estratégicas refuerzan el riesgo de acciones de mayor alcance e impacto, especialmente en escenarios de elevada tensión política o militar (PowerDMARC, 2026).



© 2026 NTT DATA, Inc.

Supernodos de grupos hacktivistas

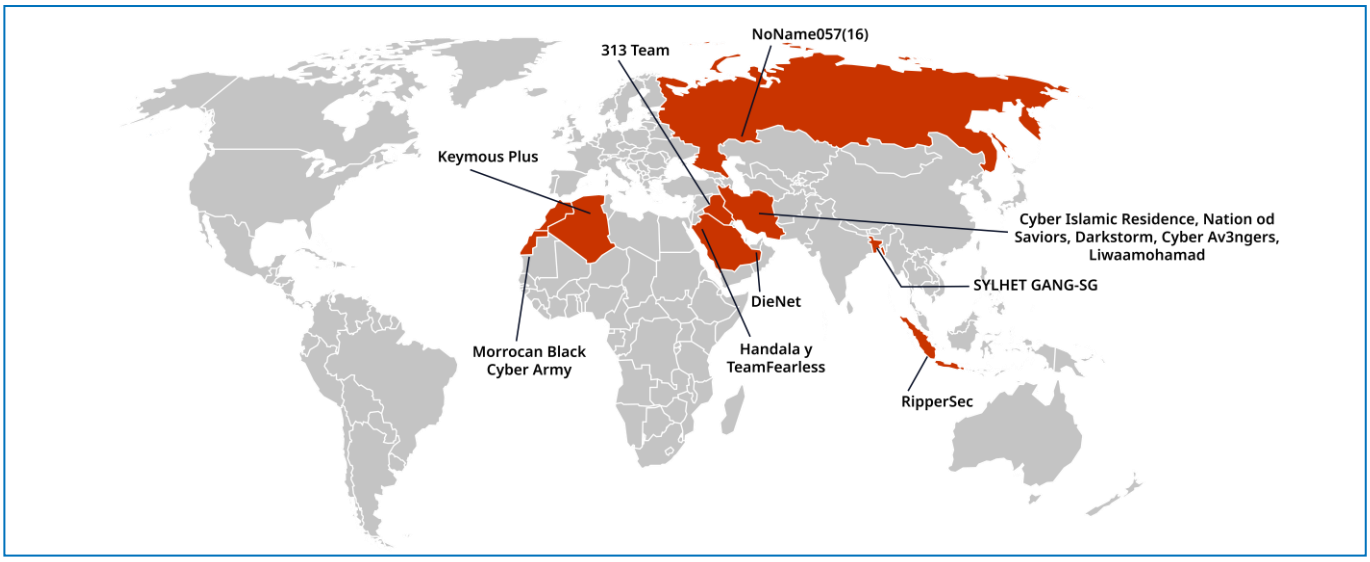


Figura 13 | Grupos conectores hacktivistas por ubicación geográfica.

7.4 APT

Durante el primer semestre de 2026 se ha profundizado y confirmado el patrón identificado en el período anterior: se han alineado las agendas geopolíticas y estatales y la selección de objetivos de los grupos APT. Además, cabe destacar también la reducción progresiva de la ventana de explotación de las vulnerabilidades *N-day* y la incorporación de inteligencia artificial en el desarrollo de herramientas ofensivas. (ESET, 2026)

- **APT rusos**

El primer semestre ha reflejado la continuidad de la presión rusa sobre Ucrania y los estados europeos, con una extensión inédita de carácter destructivo hacia infraestructura crítica de la OTAN. **Sandworm** protagonizó el primer episodio más relevante del período al desplegar el *wiper* **DynoWiper** contra una empresa energética polaca, suponiendo este caso el primer despliegue confirmado de *malware* destructivo de un actor alineado con Rusia contra un estado miembro de la Unión Europea. Posteriormente, amplió su actividad contra entidades gubernamentales, energéticas y logísticas en Ucrania con las nuevas familias de *malware* como **ZeroRays** y **NaughtyWipe**. Por su parte, **Sednit (APT28/Fancy Bear)** explotó la vulnerabilidad CVE-2026-21509 en menos de 24 horas desde su divulgación. Se trató de una campaña multietapa dirigida contra organismos gubernamentales ucranianos, instituciones de la UE y entidades marítimas y de transporte en Polonia, Eslovenia, Turquía, Grecia y Emiratos Árabes. Otro de los grupos APT con mayor presencia este semestre ha sido **Gamaredon**. Su actividad ha estado caracterizada por campañas masivas de *spear phishing*, uso intensivo de *malware* personalizado e incorporación de nuevos *stealers* y servicios de tunelización orientados al espionaje táctico. En paralelo a los actores estatales, el ecosistema hacktivista pro-ruso ha continuado activo con campañas DDoS y filtraciones de información marcadas por una menor convergencia operativa y una mayor fragmentación en la ejecución que en periodos anteriores.

- **APT chinos**

Las campañas identificadas durante el primer semestre han mostrado una diversificación de objetivos determinada directamente por la agenda geopolítica de Pekín, han priorizado operaciones económicas y de inteligencia política. Los principales grupos con mayor actividad observada han sido: **Mustang Panda (Twill Typhoon)**, **Salt Typhoon, FamousSparrow** y **NegativeGlimmer**. La actividad de FamousSparrow ha estado relacionada con recursos marítimos y energéticos en toda Latinoamérica y, en particular, en Venezuela. NegativeGlimmer comprometió una empresa de IA y robótica en Corea del Sur, alineada con las

© 2026 NTT DATA, Inc.

prioridades de *Made in China 2025*. El ecosistema APT chino ha estado marcado por el incremento de técnicas AitM, y la explotación de dispositivos *Edge* y cadenas de suministro de software para lograr accesos iniciales y operaciones de bajo perfil.

- **APT iraníes**

Durante el primer semestre de 2026, la actividad de los APT iraníes ha combinado operaciones de espionaje con capacidades destructivas dirigidas principalmente contra organizaciones israelíes. Los tres grupos más destacados son: **Rusty Boots**, **MoKhargosh** y **MOØN Badr**. Rusty Boots es un grupo de reciente adición que empleó un *bootkit wiper* para inutilizar por completo dispositivos israelíes. MoKhargosh se centra en operaciones de ciberespionaje utilizando **GoKhargosh** como *backdoor* principal y algunas de sus variantes que poseen también funcionalidades destructivas. MOØN Badr es otro de los grupos responsables de campañas de *spear phishing* con contenido adjunto malicioso para la distribución de su propio *backdoor* denominado **MOØN Agent**. En conjunto, estas operaciones reflejan un mayor énfasis en la persistencia, manteniendo como principales objetivos sectores estratégicos y organismos gubernamentales de Oriente Medio.

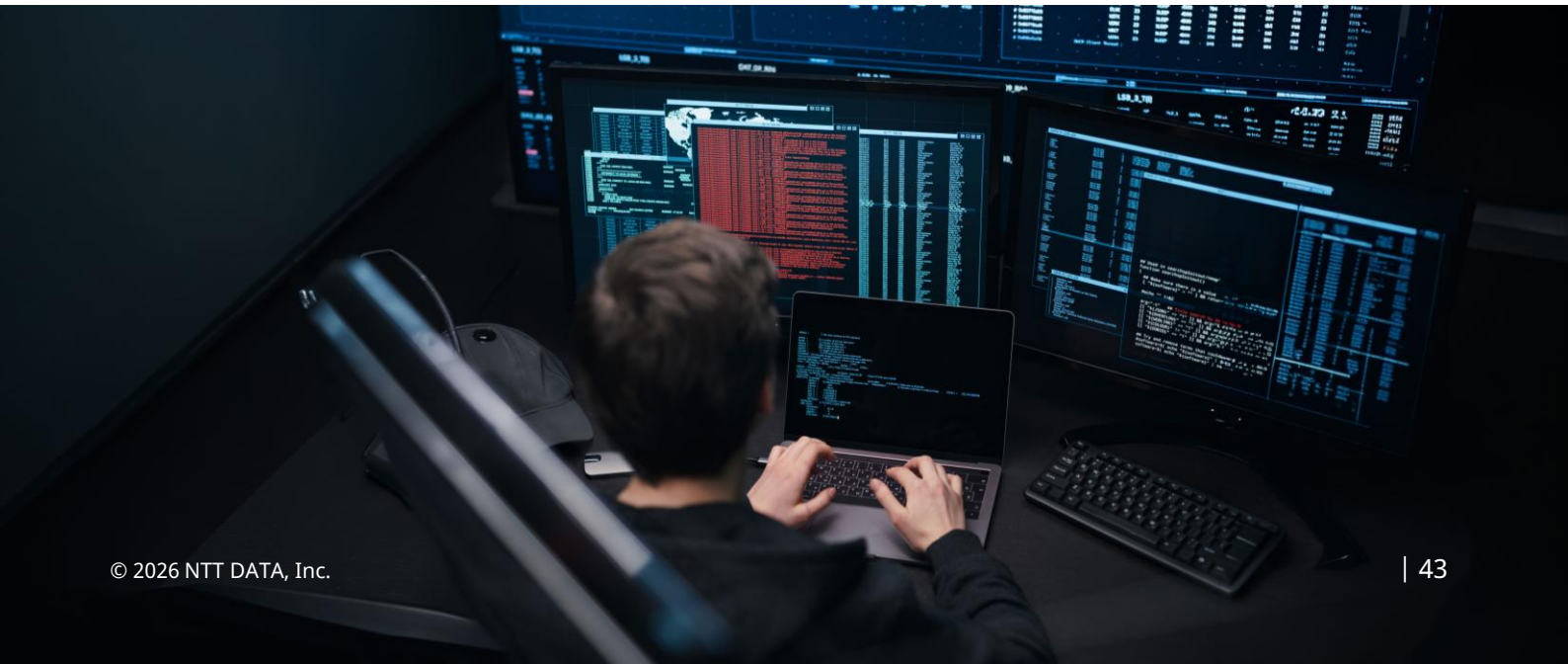
- **APT norcoreanos**

Los grupos vinculados a Corea del Norte han mantenido una actividad elevada, combinando espionaje y operaciones financieras. Actores como **Kimsuky**, **Lazarus** y **Golden Chollima** han centrado sus campañas en los gobiernos, la diplomacia, la tecnología y especialmente en el sector de las criptomonedas.

Kimsuky ha realizado intrusiones mediante el envío de correos dirigidos adjuntando, tanto el conocido *malware* **FPSpy**, como el *keylogger* **KLogEXE** con la finalidad principal de mapear redes y recopilar credenciales.

Por su parte, **Lazarus** ha centrado sus esfuerzos en la explotación de vulnerabilidades *zero day* y en el compromiso de cadenas de suministro de software (como el paquete axios npm en la **Operación DangerousPassword** o la **Operación Dreamjob**) para obtener privilegios, desplegar *backdoors* y exfiltrar activos de alto valor (ej: criptoactivos). El grupo **Golden Chollima** fue capaz de llevar a cabo una operación de seis meses de ingeniería social para ejecutar, en el mes de abril de 2026, el robo de 285 millones de dólares a la plataforma DeFi Drift.

En conjunto, estos actores han continuado perfeccionando sus capacidades mediante el uso de herramientas compartidas, cadenas de infección más sofisticadas y campañas mejor coordinadas. **Esta evolución consolida un modelo operativo que combina ciberespionaje, sabotaje y actividades de financiación ilícita** con el doble objetivo de dificultar la detección y atribución y, al mismo tiempo, aumentar el impacto de sus operaciones.



© 2026 NTT DATA, Inc.

A continuación, se presentan las claves que han marcado el periodo:

Tendencias clave observadas en grupos APT en S1 2026

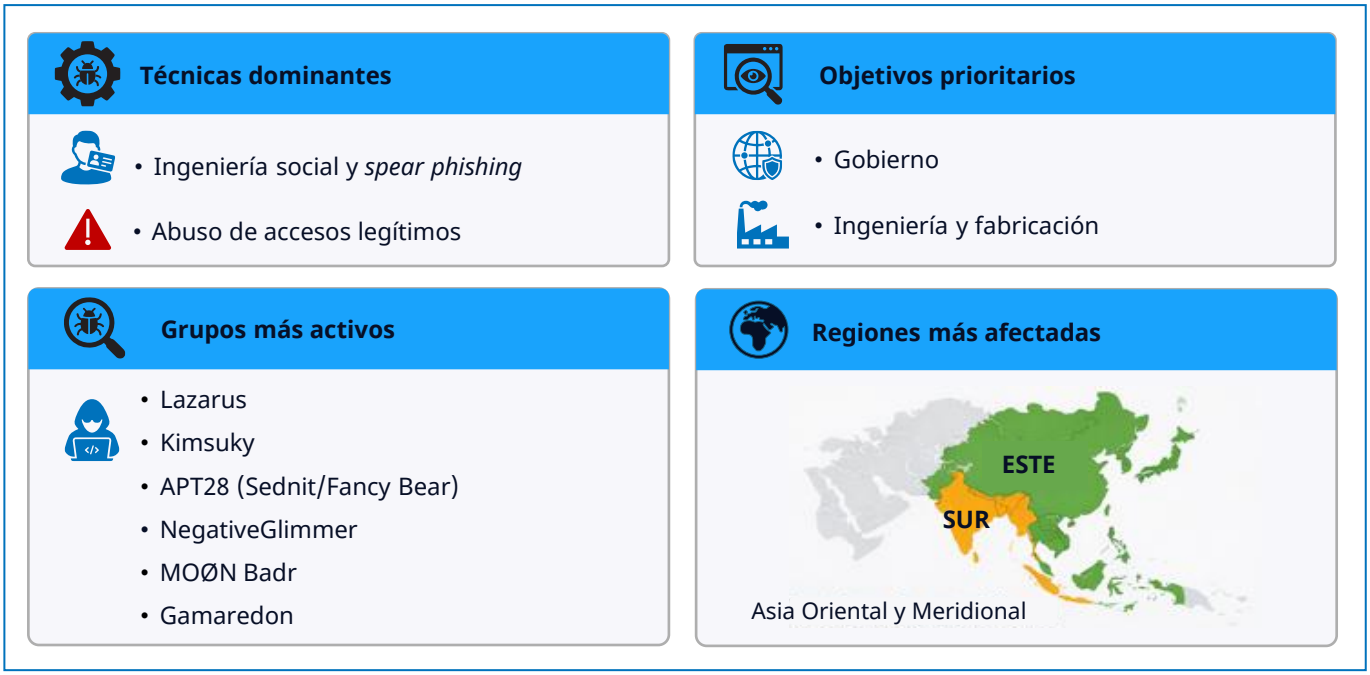


Figura 14 | Tendencias clave de grupos APT durante el primer semestre de 2026.

El análisis del primer semestre de 2026 refleja la continuidad de campañas de espionaje persistente por parte de los grupos APT relacionados principalmente con China, Corea del Norte y los grupos del sudeste asiático. En contraposición, destaca también un mayor componente disruptivo y destructivo en grupos de actores vinculados principalmente a Rusia y, en menor medida, a Irán.
Esta diferenciación operativa, condicionada por el contexto geopolítico, permite **identificar patrones por cada región y anticipar una evolución hacia intrusiones más prolongadas y sigilosas orientadas a la obtención de ventajas estratégicas a medio y largo plazo.**



© 2026 NTT DATA, Inc.



8. Tácticas, Técnicas y Procedimientos (TTPs)



Durante el primer semestre de 2026, el equipo de Cyber Threat Intelligence de NTT DATA ha seguido la evolución de las tácticas, técnicas y procedimientos (TTPs) empleadas por la actividad cibercriminal con ánimo de lucro y por actores con motivaciones geopolíticas. La conclusión es de continuidad pero con un matiz: el repertorio técnico apenas suma elementos inéditos, pero su forma de empleo cambia de manera apreciable. Lo decisivo ya no es qué técnica se usa, sino la rapidez, la escala y la automatización con que se encadenan TTPs conocidas, una orquestación que la IA empieza a sostener de forma rutinaria.

El cibercrimen de motivación económica mantiene su hegemonía y concentra más del **70%** de las intrusiones interactivas globales. Sobre esa base, el *ransomware*, la extorsión múltiple, el abuso de identidades legítimas y el aprovechamiento de infraestructura expuesta siguen vertebrando la mayoría de las campañas.

Se han observado dos fenómenos, que se refuerzan entre sí y singularizan este semestre frente a 2025: una **compresión temporal sin precedentes** del acceso a la exfiltración en minutos u horas, no en días, y la **conversión del acceso inicial en mercancía** suministrada por intermediarios especializados (Mandiant, 2026; Check Point Research, 2026).

8.1 Descripción de las TTP más comunes utilizadas por los cibercriminales

Frente al cierre de 2025, el catálogo de TTPs sigue dentro de los límites conocidos de MITRE ATT&CK; lo que cambia es el peso relativo de cada técnica y la lógica de su combinación. Sobre más de un millón de muestras de *malware*, **ocho de cada diez** de las técnicas más prevalentes buscan pasar inadvertidas, evadir defensas, sostener la persistencia o mantener un canal de control discreto (Picus Security, 2026): un tránsito del ataque "depredador", rápido y ruidoso, a la infección "parasitaria", de bajo perfil y vocación de permanencia.

© 2026 NTT DATA, Inc.

Tres desplazamientos concentran el cambio:

1

La inyección de procesos (T1055) **encabeza el ranking por primera vez (30%)** y entran entre las dominantes la evasión de *sandbox* (T1497) y el enmascaramiento (T1036), señal de que el antianálisis gana terreno.

2

El robo de credenciales deja de ser un trámite previo para volverse fin en sí mismo: **la sustracción desde navegadores y gestores (T1555) ya aparece en una de cada cuatro muestras (23%).**

3

El cifrado para impacto (T1486) cae del 21% al 12,94% un **–38%** relativo, confirmando el giro del *ransomware* de "cifrar" a "robar y extorsionar" (Picus Security, 2026). Se suman el peso creciente de identidades válidas y servicios remotos, sobre todo en la nube, y la exfiltración consolidada como antesala del *ransomware*, que apuntala la doble extorsión.

En síntesis, el semestre dibuja a un adversario más maduro, cuya prioridad es **conservar el acceso, esquivar la detección y rentabilizar el impacto** antes que exhibir técnicas novedosas.

Top técnicas MITRE ATT&CK observadas en S1 2026

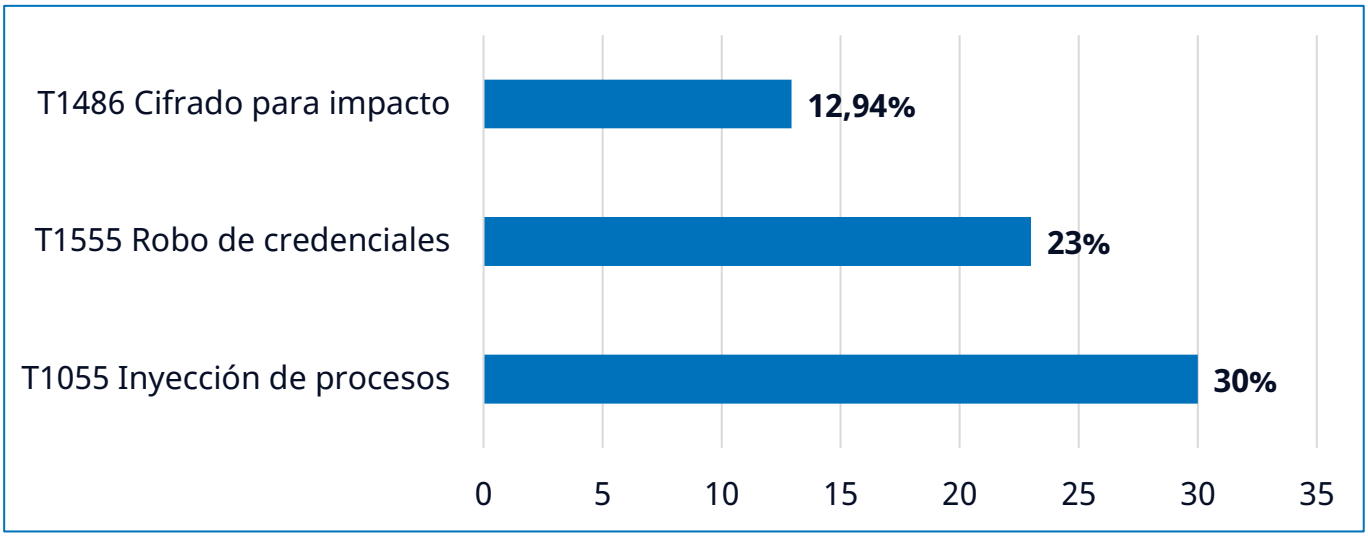


Figura 15 | Técnicas MITRE ATT&CK más prevalentes observadas en el primer semestre de 2026.

© 2026 NTT DATA, Inc.

Táctica	MITRE ATT&CK ID	Descripción
Ejecución (TA0002)	T1059 – Intérprete de comandos y *scripts*	PowerShell, *scripts* y binarios nativos para ejecutar en memoria y minimizar el rastro en disco; segunda técnica más observada del semestre.
	T1059.001 – PowerShell	Recurso preferente en operaciones manuales (*hands-on-keyboard*) y planteamientos *Living-off-the-Land*.
	T1047 – Instrumental de administración de Windows (WMI)	Ejecución remota y persistencia apoyadas en un servicio de gestión legítimo de Windows.
Persistencia (TA0003)	T1098 – Manipulación de cuentas	Alteración de cuentas existentes: locales, de servicio o de nube, para perpetuar el acceso sin levantar sospechas.
	T1098.004 – Claves de nube adicionales	Alta de claves, *tokens* o credenciales en plataformas *cloud* para sostener el acceso; en auge en intrusiones SaaS e híbridas.
	T1136.001 – Crear cuenta: cuenta local	Creación de cuentas locales de respaldo para asegurar la permanencia tras el acceso inicial.
	T1547.001 – Ejecución al inicio: claves del Registro / carpeta de inicio	Anclaje en el arranque automático de Windows para resistir reinicios.
	T1133 – Servicios remotos externos	Uso de servicios publicados (RDP, VPN, aplicaciones web) como punto de entrada y permanencia discreta.
Escalada de privilegios (TA0004)	T1134 – Manipulación de tokens de acceso	Apropiación y suplantación de *tokens* para actuar con mayor privilegio.
	T1548 – Abuso de mecanismos de elevación de privilegios	Explotación de configuraciones laxas o controles deficientes para escalar privilegios.
Evasión de defensas (TA0005)	T1055 – Inyección de procesos	Inserción de código en procesos de confianza para burlar el EDR; **técnica más prevalente del semestre** (30%).
	T1497 – Evasión de virtualización / *sandbox*	Detección de entornos de análisis para abortar la detonación; irrumpe entre las técnicas líderes.
	T1036 – Enmascaramiento (*Masquerading*)	Camuflaje de procesos y ficheros como legítimos; debut en la franja alta de prevalencia.
	T1562.001 – Deshabilitar o modificar herramientas de seguridad	Neutralización de antivirus y EDR (*EDR killers* y abuso de drivers vulnerables, BYOVD).
	T1562.004 – Modificar o deshabilitar *firewall* del sistema	Reescritura de reglas de cortafuegos para abrir paso a las comunicaciones del atacante.
	T1070.001 – Eliminación de indicadores: borrado de registros	Borrado de *logs*, a veces con purga periódica, para difuminar la traza de la intrusión.
	T1564.008 – Ocultar artefactos: reglas de ocultación de correo	Reglas de buzón para ocultar comunicaciones o exfiltración (BEC y abuso de SaaS).

Tabla 5 | Principales TTPs del primer semestre de 2026 - 1

© 2026 NTT DATA, Inc.

Táctica	MITRE ATT&CK ID	Descripción
Acceso a credenciales (TA0006)	T1555 – Credenciales de almacenes de contraseñas	Extracción desde navegadores y gestores; presente en **~1 de cada 4** muestras y elevada a objetivo en sí misma.
	T1003 – Volcado de credenciales del SO	Volcado de credenciales desde memoria o ficheros del sistema (SAM/NTDS).
	T1552 – Credenciales sin proteger	Recolección de secretos en texto claro en *scripts* o configuraciones (p. ej. con TruffleHog).
	T1528 – Robo de *tokens* de acceso a aplicaciones	Captura de *tokens* válidos para acceder a aplicaciones y servicios, en especial cloud.
Descubrimiento (TA0007)	T1046 – Descubrimiento de servicios de red	Barrido de servicios y puertos para localizar nuevos objetivos.
	T1082 – Descubrimiento de información del sistema	Recolección de datos del sistema operativo y el *hardware*.
	T1016 – Descubrimiento de configuración de red	Reconstrucción de topología y conexiones con comandos nativos.
	T1057 – Descubrimiento de procesos	Inventario de procesos activos para detectar seguridad o activos de interés.
	T1087.001 – Descubrimiento de cuentas: cuenta local	Enumeración de usuarios locales para preparar el avance posterior.
Movimiento lateral (TA0008)	T1021 – Servicios remotos	Desplazamiento por RDP, SMB u otros servicios con credenciales válidas; **Akira** llega a iniciarlo en seis minutos.
	T1570 – Transferencia lateral de herramientas	Distribución del instrumental del atacante por la red comprometida.
Comando y control (TA0011)	T1071 – Protocolo de capa de aplicación	C2 sobre protocolos web y servicios legítimos, incluida infraestructura *cloud* de terceros (APIs de IA y de proveedores *cloud*).
	T1219 – Herramientas de acceso remoto	Abuso de soluciones RMM legítimas (*ScreenConnect* y afines) como canal de mando; nueva entrada en el top.
Exfiltración (TA0010)	T1041 – Exfiltración sobre canal de mando y control	Extracción de datos por el canal C2 ya establecido.
	T1567.002 – Exfiltración a almacenamiento en la nube	Robo masivo de datos vía APIs y servicios cloud legítimos, antesala de la extorsión.
Impacto (TA0040)	T1486 – Cifrado de datos para impacto	Cifrado de sistemas en campañas de *ransomware*; **relevante, pero en claro retroceso** (del 21% al 12,94%), reflejo del giro a la extorsión sin cifrado.
	T1490 – Inhibición de la recuperación del sistema	Borrado o desactivación de copias e instantáneas para impedir la restauración.

Tabla 6 | Principales TTPs del primer semestre de 2026 - 2

© 2026 NTT DATA, Inc.

8.2 Vectores de entrada más usuales

Los vectores de entrada de 2026 han mantenido continuidad con el periodo anterior, pero con un giro de calado: junto a la consolidación del abuso de identidades, **la explotación de vulnerabilidades ha recuperado el primer plano como vía de acceso inicial**. Por primera vez en diecinueve años ha superado al robo de credenciales como mecanismo de acceso más frecuente en las brechas analizadas (Verizon, 2026); en la nube, la explotación de *software* de terceros salta del 2,9% al **44,5%**, desbancando al abuso de credenciales (Google Cloud, 2026). Y las vulnerabilidades de severidad alta y crítica explotadas se duplicaron en el año (+105%) (Rapid7, 2026).

El repunte no desmiente la tendencia de fondo, la matiza: el valor de los vectores no reside en su novedad técnica, sino en su **afianzamiento como accesos silenciosos, persistentes y de baja visibilidad** y en su **industrialización**. Cada vez más, el acceso inicial llega empaquetado por los *Initial Access Brokers* (IAB), que venden accesos RDP, VPN y RDWeb en *Access-as-a-Service* y atesoran inventarios de dispositivos y credenciales comprometidos **antes** de la operación final. Así, el adversario combina la explotación de servicios expuestos con identidades y credenciales válidas, enturbiando la distinción entre actividad legítima y maliciosa desde las primeras fases.

Abuso de identidades válidas	**Explotación de vulnerabilidades y dispositivos perimetrales**	**Ingeniería social orientada a identidad**
Las identidades legítimas se afianzan como una de las principales puertas de entrada. **Con credenciales robadas, *cookies* de sesión y *tokens*, el atacante opera sin *malware*, rebajando su visibilidad y dilatando la detección.** Las cuentas sin MFA o con MFA mal configurado encabezan los accesos más recurrentes del periodo.	Reactivación de la explotación de vulnerabilidades, concentrada en perímetro y aplicaciones publicadas (FortiGate, Cisco FMC, SharePoint, F5, ShareFile). **La ventana divulgación-explotación se estrecha hasta el *zero-day* y enlaza directamente con las cadenas de *ransomware*.**	Maniobras para arrancar credenciales o el consentimiento del usuario: *vishing*, suplantación de *help desk*, fraude del CEO/BEC y abuso de flujos de autenticación. **El *vishing* sube al segundo vector de acceso, presente en el 11% de las investigaciones** (Mandiant, 2026).
***Infostealers* avanzados**	**Abuso de servicios remotos legítimos**	**Entornos *cloud* y APIs**
Los *infostealers* se consolidan como fase previa al *ransomware* y al fraude. La captura automatizada de credenciales, *cookies* y datos del navegador alimenta a los IAB y es tan eficaz como barata: la mitad de las víctimas de *ransomware* con credenciales filtradas fueron atacadas en menos de 95 días.	RDP, VPN y RDWeb con credenciales válidas como acceso inicial, con interés creciente de los IAB por el RDWeb. **Al apoyarse en servicios legítimos, el adversario reduce su huella técnica y dificulta la detección temprana.**	Accesos por configuraciones erróneas en la nube, permisos excesivos, claves de API expuestas y abuso de relaciones de confianza entre servicios. **Se agudiza en entornos híbridos y multicloud, con menor visibilidad;** la explotación de *software* de terceros es ya el primer vector en *cloud* (Google Cloud, 2026; ReliaQuest, 2026).

Tabla 7 | Vectores de entrada más usuales empleados en el primer semestre de 2026.



© 2026 NTT DATA, Inc.

En definitiva, el acceso inicial de 2026 descansa sobre **dos pilares que se retroalimentan**: la explotación de infraestructura expuesta acelerada por la armamentización rápida y el acceso preposicionado y el abuso de identidades, confianza y uso legítimo de los servicios. Ambos confluyen en el mercado de los IAB, que convierte la entrada en un bien de consumo. El resultado: detección más difícil e impacto potencial mayor, pues son accesos que no disparan alertas inmediatas ni comportamientos claramente anómalos. Afrontarlo exige integrar gestión de vulnerabilidades y parcheo ágil con gobierno de identidades, visibilidad en la nube y vigilancia de los procesos humanos: el terreno de la innovación que se aborda a continuación.



8.3 Innovación en ataques: nuevas técnicas y tácticas

La innovación de 2026 no viene de técnicas inéditas en MITRE ATT&CK, sino de una **transformación en la lógica operativa del adversario**. El modelo que se afianza combina persistencia, automatización, compresión del ciclo de ataque y aprovechamiento metódico de la confianza; su meta no es solo comprometer sistemas, sino fundirse con la operativa ordinaria de la organización y precipitar el impacto en cuanto es rentable. El cambio se nota menos en cómo se entra y más en **cómo se actúa una vez dentro**: gestión del tiempo, reducción de señales y forma de materializar el daño.

De operaciones ruidosas a intrusiones sigilosas, automatizadas y de ciclo comprimido

La primera línea evolutiva combina una rebaja deliberada del ruido técnico con una **aceleración drástica del ciclo de ataque**. El adversario prioriza el trabajo manual (*hands-on-keyboard*), las herramientas nativas (*Living-off-the-Land*) y la ejecución asistida frente al *malware* persistente, hasta el punto de que una fracción creciente de las intrusiones interactivas transcurre sin *malware* tradicional. Esa convergencia diluye las fronteras entre actores: grupos estado-nación y bandas de *ransomware* como **Volt Typhoon, APT28, Black Basta o FIN7** usan un repertorio nativo casi idéntico: PowerShell, WMI, RDP, *ntdsutil* y *netsh* (SentinelOne, 2026).

Y, a la vez, el tiempo se ha vuelto un arma. El intervalo mediano entre acceso inicial y traspaso a un operador se ha desplomado a **22 segundos,** frente a más de ocho horas en 2022, **Akira** inicia el movimiento lateral en **6 minutos** y las campañas más veloces van del acceso a la exfiltración en unos **72 minutos** (Mandiant, 2026; ReliaQuest, 2026; Unit 42, 2026). Este bajo perfil a alta velocidad es posible por el **acceso preposicionado**: ya no hace falta explotar en tiempo real, basta con activar inventarios previos, lo que además reparte las señales defensivas entre varios dominios: identidad, *endpoint* y nube, y dificulta su correlación.

Industrialización del *ransomware* y consolidación de la extorsión múltiple

El ecosistema vive una **reconsolidación**: el top 10 ha acaparado el 71% de las víctimas publicadas en los *data leak sites* y solo cuatro operadores: **Qilin, Akira, The Gentlemen y LockBit**, suman el **41%**, mientras los grupos activos caen de 85 a 71 en pocos trimestres: "menos adversarios, pero más capaces" (Check Point Research, 2026).
La novedad no ha estado en el cifrado, sino en la **orquestación integral de la campaña**. **The Gentlemen** ejemplifica la industrialización del acceso: estrenó su operación con unos **14.700 FortiGate** comprometidos y **969 credenciales VPN** obtenidas por fuerza bruta (CVE-2024-55591), acumulados antes de existir como marca. A la par se ha afianzado el giro del cifrado hacia el **robo de datos y la extorsión sin cifrado**: el retroceso del 38% en la técnica de cifrado (Picus Security, 2026), la generalización de los *EDR killers* y la extorsión *encryptionless* y casos como **ShinyHunters** han generado daño desproporcionado con intrusiones *identity-first* y robo de datos nativo en SaaS, sin un solo cifrador, miden la madurez de la doble y triple extorsión (ReliaQuest, 2026).

© 2026 NTT DATA, Inc.

La inteligencia artificial como acelerador táctico, no como sustituto

Durante el primer semestre de 2026, la **inteligencia artificial se ha consolidado como un acelerador táctico dentro de la cadena de ataque**. Su impacto no se refleja tanto en la aparición de técnicas completamente nuevas dentro de MITRE ATT&CK, sino en la reducción del tiempo necesario para preparar, adaptar y ejecutar fases ya conocidas del ciclo ofensivo. Google Threat Intelligence Group observa una transición desde usos incipientes de IA hacia una aplicación más industrializada de modelos generativos en flujos adversarios, incluyendo investigación de vulnerabilidades, desarrollo de *exploits*, *malware*, reconocimiento, ingeniería social y operaciones de influencia (Google Threat Intelligence Group, 2026).

Los usos más relevantes se han concentrado en tareas de apoyo: generación de señuelos de *phishing* más creíbles, adaptación lingüística y cultural de mensajes, automatización de reconocimiento, clasificación de grandes volúmenes de datos robados, asistencia en *scripting*, modificación de herramientas y creación de contenido sintético. Sophos también identifica la IA como un tema cada vez más presente en comunidades *underground*, donde los actores debaten su potencial, afirman emplearla para *malware* o desarrollo de herramientas y, al mismo tiempo, muestran dudas sobre la veracidad, utilidad y seguridad operacional de algunas ofertas (Sophos, 2026).

Este matiz es clave: la IA no elimina la necesidad de supervisión humana. Los actores siguen dependiendo de operadores para seleccionar objetivos, validar accesos, decidir movimientos laterales, interpretar el contexto de la víctima y monetizar el compromiso. Sin embargo, reduce la carga cognitiva de tareas repetitivas y permite a perfiles menos sofisticados acceder a capacidades que antes requerían mayor experiencia técnica. En ese sentido, la IA actúa como un multiplicador de productividad criminal más que como un sustituto autónomo del atacante.

En campañas de ingeniería social, el impacto es especialmente relevante. Verizon señala que diferentes técnicas de ataque están siendo reforzadas por IA generativa y que los actores la emplean para acelerar fases que van desde la identificación de brechas hasta la escritura de *malware* (Verizon, 2026). Esto facilita la personalización de señuelos, la producción de contenido multilingüe, el uso de identidades sintéticas y la ejecución de campañas de *phishing*, *smishing*, *vishing* o BEC con menor coste operativo.
También han empezado a observarse usos más técnicos. Google Threat Intelligence Group indicó en mayo de 2026 que identificó, por primera vez, un actor criminal que habría empleado IA para desarrollar un *exploit zero-day* previsto para una operación de explotación masiva. El mismo informe describe casos de desarrollo asistido de *malware*, lógica de evasión, uso de IA para comandos autónomos y ataques contra entornos y dependencias de software de IA como vector de acceso inicial (Google Threat Intelligence Group, 2026).

En conjunto, la IA debe entenderse como un acelerador transversal de TTPs ya conocidas. No sustituye al atacante, pero permite preparar campañas con mayor rapidez, adaptar mensajes a más víctimas, automatizar fases repetitivas y reducir barreras de entrada. Para la defensa, esto implica que no basta con buscar “ataques con IA”; es necesario reforzar controles sobre identidad, correo, comportamiento anómalo, abuso de herramientas legítimas, exposición de datos y velocidad de respuesta.



© 2026 NTT DATA, Inc.

9. Vulnerabilidades



Durante el primer semestre de 2026, la explotación de vulnerabilidades ha consolidado su papel como vector prioritario de acceso inicial, impulsada por la rápida operacionalización de fallos críticos en servicios expuestos, *appliances perimetrales*, plataformas de administración, soluciones de seguridad y componentes ampliamente desplegados. Los casos observados muestran una transición hacia campañas más automatizadas y orientadas a post-explotación, donde el valor del CVE no depende solo de su severidad, sino de su exposición real, explotación activa y capacidad para facilitar persistencia, escalada de privilegios, robo de credenciales o impacto operativo.

• Enero:

El inicio del semestre estuvo marcado por la explotación de vulnerabilidades en tecnologías de red y administración centralizada. La **CVE-2026-24858**, asociada a **Fortinet** (Fortinet Security Advisory, 2026), representa un patrón especialmente relevante: el **abuso de relaciones de confianza y autenticación federada en ecosistemas perimetrales**. Su explotación permitió a actores de acceso inicial operar sobre dispositivos registrados, automatizar cambios en *firewall*, crear usuarios, habilitar VPN y extraer configuraciones. Desde una perspectiva CTI, el caso refleja cómo los atacantes ya no buscan únicamente comprometer un dispositivo expuesto, sino transformar ese acceso en control operativo inmediato sobre la infraestructura de red.
En paralelo, la explotación activa de la **CVE-2024-37079** en **VMware vCenter Server** (Broadcom/VMware Security Bulletin, 2026) ilustra el valor estratégico de las plataformas de virtualización como plano de control corporativo. La explotación de vCenter no debe analizarse solo como una ejecución remota de código, sino como una vía potencial hacia la administración de cargas virtualizadas, inventario de sistemas, privilegios elevados y movimiento lateral en infraestructuras críticas. Este caso confirma que los **sistemas de administración centralizada se han convertido en objetivos de alto valor** para campañas orientadas a persistencia y expansión interna.

Se observa una **consolidación de la automatización post-explotación.** Los actores de amenazas no solo se limitan a obtener acceso inicial a través de vulnerabilidades en servicios expuestos, sino que **integran flujos de trabajo automatizados para la configuración de infraestructuras maliciosas** de manera inmediata tras el compromiso.

• Febrero:

Durante febrero se observó una diversificación significativa de los vectores de ataque, combinando explotación masiva de sistemas expuestos con campañas más dirigidas contra infraestructuras críticas de red y aplicaciones empresariales. La vulnerabilidad de fallo de inyección SQL en el componente GUI de **FortiClient EMS** identificada como **CVE-2026-21643** (Fortinet, 2026), representa el patrón de **armamentización rápida de servicios publicados en Internet**: escaneo masivo, uso de PoC públicos y explotación por múltiples direcciones IP atacantes. Su relevancia no reside solo en la ejecución de comandos, sino en que afecta a una plataforma utilizada para gestión corporativa de *endpoints*, lo que amplifica el impacto en entornos empresariales.

Por otro lado, la vulnerabilidad de omisión de autenticación registrada como **CVE-2026-20127** en **Cisco Catalyst SD-WAN** (Cisco Security Advisory, 2026) refleja otro patrón relevante: el **abuso de confianza interna entre componentes de infraestructura**. La actividad asociada a **UAT-8616**, incluyendo degradación de versión, explotación de una vulnerabilidad previa (**CVE-2022-20775**) y restauración posterior del *software*, evidencia un enfoque más sofisticado y sigiloso. Este comportamiento apunta a actores que buscan mantener acceso privilegiado reduciendo la visibilidad de la intrusión.
Finalmente, la **CVE-2026-21513**, asociada a **Microsoft MSHTML** (Microsoft, 2026) y a la campaña **Operación Neusploit** atribuida a **APT28 (Fancy Bear / Forest Blizzard)**, refuerza la **convergencia entre explotación técnica e ingeniería social**.

© 2026 NTT DATA, Inc.

Esta campaña de explotación *zero-day* basada en el uso de *spear phishing* con archivos LNK y documentos RTF maliciosos (que instalaban *malware* avanzado en memoria como **NotDoor, MiniDoor y CovenantGrunt** para exfiltrar información confidencial) confirma que las vulnerabilidades en componentes de uso extendido siguen siendo un recurso eficaz para operaciones de ciberespionaje contra gobierno, diplomacia y política exterior. El patrón observado combina explotación de cliente, evasión de controles de seguridad y abuso de servicios legítimos para C2 y exfiltración.

Se observa una mayor orientación hacia el **compromiso de aplicaciones de negocio críticas**. Los actores aprovecharon vulnerabilidades de autenticación y ejecución remota de código para **acceder a plataformas que almacenan información corporativa** sensible y procesos operativos esenciales.

- **Marzo:**

Marzo introdujo un punto de inflexión con la campaña **Zero-click Copilot Theft**, asociada a la **CVE-2026-26144** en **Excel** (Microsoft Security Response Center, 2026). El caso es relevante porque desplaza el foco desde la explotación clásica de aplicaciones ofimáticas hacia el **abuso de agentes de inteligencia artificial integrados en flujos de productividad**. La explotación permitió exfiltrar información corporativa sin interacción directa del usuario, aprovechando capacidades del modo agente y conexiones salientes no autorizadas.
Desde una perspectiva CTI, este caso representa la aparición de un nuevo patrón: el "*IA-Agent Hijacking*". La superficie de ataque ya no se limita al docu-mento, la macro o el *endpoint*; se extiende a los agentes que procesan, interpretan y conectan datos internos. La tendencia apunta a ataques dirigidos al núcleo de la productividad corporativa, donde la información sensible puede ser extraída mediante canales aparentemente legítimos y difíciles de distinguir de la actividad normal.

Marzo marca un punto de inflexión significativo en el panorama de amenazas al **introducir ataques de "*IA-Agent Hijacking*".** La capacidad de exfiltrar datos de forma silenciosa a través de agentes internos indica una evolución hacia ataques dirigidos al *core* de la productividad y los datos confidenciales de las organizaciones.

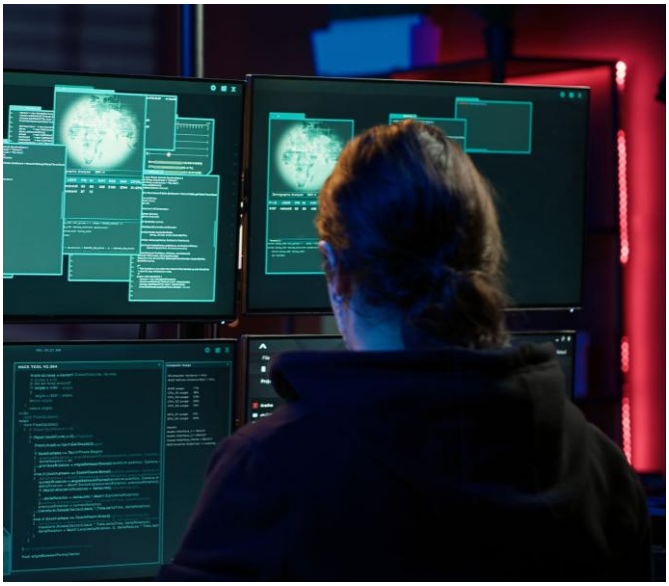


© 2026 NTT DATA, Inc.

• Abril:

El mes de abril estuvo marcado por campañas de ***ransomware*** que aprovecharon herramientas de administración remota y plataformas internas de gestión para maximizar su impacto. Destacaron las vulnerabilidades identificadas como **CVE-2024-1708** y **CVE-2024-1709** en **ConnectWise ScreenConnect** (ahora **ConnectWise Access**) (NIST, 2026) que representan un patrón recurrente: los atacantes priorizan herramientas RMM porque proporcionan acceso administrativo, persistencia y capacidad de movimiento interno **sin necesidad de desplegar *malware* complejo**. Su explotación por grupos como **Black Basta, Bl00dy y LockBit**, vinculados a Corea del Norte y China, confirma que las plataformas de soporte remoto siguen siendo un punto de entrada de alto valor para operaciones de extorsión.

Asimismo, las **CVE-2023-27350** y **CVE-2023-27351** en **PaperCut NG/MF** (PaperCut Security Bulletin, 2026) refuerzan una segunda lectura: la **explotación persistente de vulnerabilidades *N-day*** en servicios internos que permanecen expuestos o sin parchear. Aunque no se trata de vulnerabilidades nuevas, su uso por grupos como **Cl0p, Bl00dy, Mint Sandstorm, Mango Sandstorm y Lace Tempest** demuestra que el ciclo de riesgo de una CVE no termina con la publicación del parche. Los actores siguen explotando fallos antiguos cuando estos ofrecen acceso administrativo rápido, información sensible o capacidad de pivotar hacia otros sistemas corporativos.



Los grupos de *ransomware* están priorizando el compromiso de estas plataformas debido a que otorgan un acceso de nivel administrativo casi inmediato, **eliminando la necesidad de desarrollar herramientas maliciosas personalizadas para la persistencia.**

• Mayo:

Mayo reflejó una marcada transición hacia técnicas de post-explotación centradas en escalada de privilegios, evasión de defensas y consolidación silenciosa del acceso. La cadena de vulnerabilidades **CVE-2026-31431 (Copy Fail), CVE-2026-43500** y **CVE-2026-43284 (Dirty Frag) y CVE-2026-46300 (Fragnesia)** en **Linux Kernel**, representan el uso de vulnerabilidades LPE como fase posterior al compro-miso inicial. Su valor operativo reside en permitir elevar privilegios a *root*, reforzar persistencia y dificultar la detección al operar sobre memoria en lugar de modificar artefactos evidentes en disco (INCIBE-CERT, 2026b).

En paralelo, las **CVE-2026-41091** y **CVE-2026-45498** en **Microsoft Defender** (Microsoft Security Response Center, 2026) mostraron un patrón complementario: atacar los propios controles de seguridad. Su explotación para elevar privilegios a SYSTEM o interrumpir la plataforma *antimalware* confirma que **las soluciones defensivas también forman parte de la superficie de ataque**. Esta tendencia obliga a tratar los motores de seguridad, EDR y componentes *antimalware* como activos críticos que deben actualizarse y monitorizarse con el mismo rigor que los servicios expuestos.

El cambio estratégico de técnicas de intrusión masiva a operaciones “bajo el radar” busca consolidar el control total de los activos críticos sin dejar evidencias persistentes en disco, lo que supone un **reto directo para los sistemas de detección tradicionales y subraya la necesidad crítica de implementar seguridad basada en el comportamiento** (EDR/XDR).

© 2026 NTT DATA, Inc.

• Junio:

Para finalizar el semestre, **junio ha confirmado la presión sobre plataformas empresariales ampliamente desplegadas y servicios expuestos a Internet**. En primer lugar, la explotación de las vulnerabilidades **CVE-2026-50751** y **CVE-2026-50752** en **Check Point VPN** (CheckPoint, 2026), de omisión de autenticación, evidencian el interés sostenido por soluciones VPN y acceso remoto. Su explotación, relacionada parcialmente con una filial de **Qilin**, permitía establecer conexiones sin credenciales válidas, lo que encaja con una de las tendencias más relevantes del semestre: el perímetro de acceso remoto continúa siendo una puerta de entrada prioritaria para *ransomware*, *brokers* de acceso inicial y actores orientados a espionaje.
En segundo lugar, la **CVE-2026-28318** en **SolarWinds Serv-U** (SolarWinds, 2026) representa un patrón distinto, centrado en disponibilidad. Al tratarse de una vulnerabilidad de denegación de servicio (DoS), su impacto debe vincularse principalmente a la interrupción o degradación de servicios de transferencia de archivos expuestos, no a acceso inicial, persistencia o movimiento lateral salvo que exista una cadena de explotación adicional documentada. Su relevancia reside en que los servicios corporativos de intercambio de información pueden convertirse en puntos de presión operativa, especialmente cuando soportan procesos críticos o flujos de negocio sensibles.

> Los atacantes están explotando la vulnerabilidad de seguridad sin requerir privilegios mediante **ataques de baja complejidad que no requieren interacción del usuario.**
> Su explotación puede tener un alto impacto en la confidencialidad, la integridad y la disponibilidad del sistema afectado.

Tendencias de explotación de estas vulnerabilidades

En conjunto, el primer semestre de 2026 ha confirmado cuatro patrones principales.

- Los atacantes han **priorizado vulnerabilidades en tecnologías empresariales ampliamente desplegadas que concentran privilegios, conectividad o administración centralizada**: servicios expuestos a Internet como *firewalls* y VPN, plataformas de administración, acceso remoto, virtualización e impresión, herramientas ofimáticas y soluciones de seguridad.
- Se ha **consolidado la automatización post-explotación**. Los actores ya no se limitan a explotar un fallo y esperar una segunda fase manual, sino que integran flujos de trabajo para crear usuarios, habilitar VPN, modificar configuraciones, extraer credenciales o preparar movimiento lateral casi de forma inmediata tras el compromiso.
- Se ha observado una **convergencia creciente entre explotación técnica, identidad e ingeniería social**. Las campañas ya no dependen de un único vector: combinan documentos maliciosos, *spear phishing*, técnicas de ClickFix, abuso de servicios legítimos, credenciales válidas, agentes de IA y explotación de servicios expuestos.
- El **riesgo de una CVE** depende cada vez menos de su severidad teórica y más de su exposición real, explotación activa, criticidad del activo afectado y **capacidad para integrarse en campañas** de *ransomware*, espionaje o disrupción, factores en los que debe basarse la priorización defensiva.

Así pues, el semestre demuestra que las vulnerabilidades más relevantes no son necesariamente las más novedosas, sino aquellas que permiten a los atacantes acceder rápido, operar con bajo ruido, consolidar privilegios y transformar el compromiso inicial en impacto real sobre la organización.



© 2026 NTT DATA, Inc.



10. Perspectiva futura



¿Qué nos espera en el segundo semestre de 2026?

De cara al segundo semestre de 2026, el panorama de ciberamenazas apunta a una **consolidación de las dinámicas observadas durante la primera mitad del año.** No se espera una ruptura radical del modelo de ataque, sino una evolución hacia operaciones más rápidas, silenciosas y apoyadas en la automatización, el abuso de identidades legítimas, la explotación de servicios expuestos y el uso de inteligencia artificial como acelerador operativo.

El cibercrimen continuará avanzando hacia modelos más especializados y distribuidos. La presión policial sobre foros, mercados e infraestructuras criminales no elimina la demanda de credenciales, accesos iniciales, *logs* de *infostealers* o servicios criminales, pero sí empuja la actividad hacia comunidades privadas, canales cerrados y mercados más fragmentados. La confianza entre actores, la reputación y la capacidad de migrar rápidamente seguirán siendo elementos clave del ecosistema *underground*.

La inteligencia artificial seguirá ganando peso como herramienta de apoyo en fases repetitivas y escalables: generación de señuelos de *phishing*, adaptación lingüística y cultural, automatización del reconocimiento, asistencia en *scripting*, clasificación de datos robados y creación de contenido sintético. Su impacto no estará tanto en sustituir al atacante como en reducir tiempos, ampliar escala y permitir campañas más creíbles y personalizadas.

La identidad seguirá siendo uno de los principales campos de batalla. El abuso de credenciales válidas, *tokens*, sesiones, aplicaciones SaaS, servicios remotos y permisos excesivos continuará dificultando la detección temprana, especialmente en intrusiones que simulan actividad legítima durante sus primeras fases.
En paralelo, el *ransomware* y la extorsión mantendrán su relevancia, con mayor peso del robo de datos, la presión reputacional y la monetización flexible del acceso.

En el plano geopolítico, el ciberespacio continuará funcionando como un entorno de presión estratégica. **Las tensiones entre bloques, los conflictos activos, la competencia tecnológica y la protección de cadenas de suministro críticas seguirán impulsando operaciones de espionaje, influencia, sabotaje limitado y hacktivismo alineado con narrativas estatales.** Sectores como defensa, energía, telecomunicaciones, transporte, servicios financieros, tecnología y proveedores estratégicos seguirán concentrando buena parte del riesgo.

En conjunto, **el segundo semestre de 2026 se perfila como un periodo en el que la ventaja defensiva dependerá de la capacidad de anticipar, correlacionar y responder con rapidez.** Más que prepararse para amenazas completamente nuevas, las organizaciones deberán prepararse para adversarios más rápidos, más adaptativos y mejor coordinados.

© 2026 NTT DATA, Inc.



11. Referencias

- Australian Department of Home Affairs. (2026). Cyber security act. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-security-act
- Australian Department of Home Affairs. (2026). Security standards for smart devices. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/security-standards-for-smart-devices
- Council of the European Union. (2026). Council implementing regulation (EU) 2026/589 implementing regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the union or its member states. https://eur-lex.europa.eu/eli/reg_impl/2026/589/oj/eng
- Council of the European Union. (2026). Council implementing regulation (EU) 2026/1078 implementing regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the union or its member states. https://eur-lex.europa.eu/eli/reg_impl/2026/1078/oj/eng
- European Commission. (2026). Commission delegated regulation (EU) 2026/881 supplementing regulation (EU) 2024/2847. https://eur-lex.europa.eu/eli/reg_del/2026/881/oj/eng
- Government of Canada. (2026). Government of Canada strengthens cyber security and critical infrastructure with royal assent of bill C-8. https://www.canada.ca/en/public-safety-canada/news/2026/06/government-of-canada-strengthens-cyber-security-and-critical-infrastructure-with-royal-assent-of-bill-c8.html
- Indian Computer Emergency Response Team. (2026). CERT-In security guidelines CISG-2026-01: cyber security framework and guidelines for space including satellite communication. https://www.cert-in.org.in/s2cmainservlet?pageid=guidlnview02&refcode=cisg-2026-01
- Indian Computer Emergency Response Team. (2026). CERT-In security guidelines CISG-2026-02: blueprint for reducing exposure and defending against ai-assisted vulnerabilities exploitation in digital infrastructure. https://www.cert-in.org.in/s2cmainservlet?pageid=guidlnview02&refcode=cisg-2026-02
- Indian Computer Emergency Response Team. (2026). CERT-In security guidelines. https://www.cert-in.org.in/s2cmainservlet?pageid=guidlnview01
- Library of Congress. (2026, january 8). China: amended cybersecurity law takes effect. https://www.loc.gov/item/global-legal-monitor/2026-01-08/china-amended-cybersecurity-law-takes-effect/
- National Institute of Standards and Technology. (2026). SP 800-172 rev. 3: enhanced security requirements for protecting controlled unclassified information. https://csrc.nist.gov/pubs/sp/800/172/r3/final
- National Institute of Standards and Technology. (2026). SP 800-172A rev. 3: assessing enhanced security requirements for protecting controlled unclassified information. https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
- U.S. Department of Defense Chief Information Officer. (2026). Cybersecurity maturity model certification. https://dodcio.defense.gov/cmmc/
- Boletín Oficial de la República Argentina. (2026). Decreto 941/2025. https://www.boletinoficial.gob.ar/detalleaviso/primera/337032/20260102
- Boletín Oficial de la República Argentina. (2026). Disposición 1/2026 del Centro Nacional de Ciberseguridad. https://www.boletinoficial.gob.ar/detalleaviso/primera/341893/20260513
- Europol. (2026). 29 arrested: law enforcement strikes criminal networks behind illegal streaming. https://www.europol.europa.eu/media-press/newsroom/news/29-arrested-law-enforcement-strikes-criminal-networks-behind-illegal-streaming
- Europol. (2026). Cybercriminal VPN used by ransomware actors dismantled in global crackdown. https://www.europol.europa.eu/media-press/newsroom/news/cybercriminal-vpn-used-ransomware-actors-dismantled-in-global-crackdown

© 2026 NTT DATA, Inc.

- Eurojust. (2026). Eurojust coordinated investigation shuts down criminal VPN network. https://www.eurojust.europa.eu/news/eurojust-coordinated-investigation-shuts-down-criminal-vpn-network
- Fiscal Information and Investigation Service. (2026). FIOD houdt twee verdachten aan wegens overtreding sanctiewetgeving. https://www.fiod.nl/fiod-houdt-twee-verdachten-aan-wegens-overtreding-sanctiewetgeving/
- Interpol. (2026). 201 arrests in first-of-its-kind cybercrime operation in MENA region. https://www.interpol.int/news-and-events/news/2026/201-arrests-in-first-of-its-kind-cybercrime-operation-in-mena-region
- Ministerio del Interior. (2026). Desarticulada una organización criminal que creaba herramientas informáticas para cometer ciberestafas bancarias. https://www.interior.gob.es/opencms/es/detalle/articulo/desarticulada-una-organizacion-criminal-que-creaba-herramientas-informaticas-para-cometer-ciberestafas-bancarias/
- National Cyber Security Centre. (2026). Joint operation by police and NCSC takes down major botnet. https://www.ncsc.nl/en/news/joint-operation-by-police-and-ncsc-takes-down-major-botnet
- Politie. (2026). International law enforcement initiate hunt on malware group socgholish. https://www.politie.nl/en/news/2026/juni/18/11-international-law-enforcement-initiate-hunt-on-malware-group-socgholish.html
- U.S. Department of Justice. (2026). Canadian man arrested by international authorities and charged with administrating kimwolf ddos botnet. https://www.justice.gov/usao-ak/pr/canadian-man-arrested-international-authorities-charged-administrating-kimwolf-ddos
- Escudo digital. (2026). Desmantelan una red que había infectado 15.000 páginas webs hechas con wordpress. https://www.escudodigital.com/ciberseguridad/desmantelan-red-operacion-endgame-webs-infectadas.html
- Operation Endgame. (2026). Operation Endgame. https://www.operation-endgame.com/
- Breachsense. (2026). Top 7 dark web markets in 2026: what gets sold and how to monitor them. https://www.breachsense.com/blog/dark-web-markets/
- Cloudsek. (2026). Dark web forums and deep web communities. https://www.cloudsek.com/knowledge-base/dark-web-forums-and-deep-web-communities
- Deepstrike. (2026). Top dark web marketplaces. https://deepstrike.io/blog/top-dark-web-marketplaces
- Rapid7. (2025). Inside russian market: uncovering the botnet empire. https://www.rapid7.com/blog/post/tr-inside-russian-market-uncovering-the-botnet-empire/
- SOCRadar. (2026a). Top 10 deep web and dark web forums in 2026. https://socradar.io/blog/top-10-deep-web-and-dark-web-forums/
- SOCRadar. (2026b). Top 10 dark web markets in 2026: list & threat analysis. https://socradar.io/blog/top-10-dark-web-markets/
- SOCRadar. (2026c). Iran-Israel Cyber Conflict Dashboard. https://socradar.io/iran-israel-cyber-conflict-dashboard/
- Sophos. (2026). AI in the underground: curiosity, claims, and concerns. https://www.sophos.com/en-us/blog/ai-in-the-underground-curiosity-claims-and-concerns
- U.S. Department of Justice. (2026, march 4). United states leads dismantlement of one of the world’s largest hacker forums. https://www.justice.gov/opa/pr/united-states-leads-dismantlement-one-worlds-largest-hacker-forums

© 2026 NTT DATA, Inc.

- CrowdStrike. (2026). 2026 global threat report. https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-global-threat-report-findings/
- Google Cloud. (2026). Cybersecurity forecast 2026. https://cloud.google.com/security/resources/cybersecurity-forecast
- Google Threat Intelligence Group. (2026). ai-assisted vulnerability exploitation and initial access. https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access/
- Mandiant. (2026). M-Trends 2026. https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026/
- Microsoft. (2025). Microsoft Digital Defense Report 2025. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/
- World Economic Forum. (2026). Global Cybersecurity Outlook 2026. https://www.weforum.org/publications/global-cybersecurity-outlook-2026/digest/
- Biblioteca del Congreso Nacional de Chile. (2024). Ley 21.663: ley marco de ciberseguridad. https://www.bcn.cl/leychile/navegar?i=1202434
- Gabinete de Segurança Institucional. (2026). Plano nacional de cibersegurança. https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/plano-nacional-de-ciberseguranca-p-ciber
- Presidencia de Colombia. (2026). Ley 2573 de 2026. https://dapre.presidencia.gov.co/normativa/normativa/ley%20no.%202573%20del%2019%20de%20mayo%20de%202026.pdf
- Aftra. (2026). The growing economic impact of cybercrime threats. https://aftra.io/blog/economic-impact-of-increasing-cybercrime
- Axonius. (2026). Verizon DBIR 2026: back to the fundamentals. https://www.axonius.com/blog/verizon-dbir-2026-fundamentals-beyond-cves
- Center for Strategic and International Studies. (2026). Significant cyber incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
- CERT-EU. (2026). European commission cloud breach: A supply-chain compromise. https://cert.europa.eu/blog/european-commission-cloud-breach-trivy-supply-chain
- Check Point Research. (2026, 16 febrero). 16th february threat intelligence report. https://research.checkpoint.com/2026/16th-february-threat-intelligence-report/
- Check Point Research. (2026, 16 marzo). 16th march threat intelligence report. https://research.checkpoint.com/2026/16th-march-threat-intelligence-report/
- Check Point Research. (2026, 13 abril). 13th april threat intelligence report. https://research.checkpoint.com/2026/13th-april-threat-intelligence-report/
- Check Point Research. (2026, 18 mayo). 18th may threat intelligence report. https://research.checkpoint.com/2026/18th-may-threat-intelligence-report/
- Check Point Research. (2026, 8 junio). 8th june threat intelligence report. https://research.checkpoint.com/2026/8th-june-threat-intelligence-report/
- Check Point Research. (2026). The state of ransomware Q1 2026. https://research.checkpoint.com/2026/the-state-of-ransomware-q1-2026/

© 2026 NTT DATA, Inc.

- Check Point. (2026). Security Advisory – Action Required – Active Exploitation of Check Point VPN Authentication Bypass (CVE-2026-50751). https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/

- Check Point Software Technologies. (2026). 2026 cyber security report. Stocktitan. https://www.stocktitan.net/news/chkp/check-point-software-s-2026-cyber-security-report-shows-global-0aw8ddde6fjb.html

- Cyber Insurance News. (2026). Verizon 2026 DBIR: vulnerability exploitation now the #1 breach vector. https://cyberinsurancenews.org/verizon-2026-dbir-data-breach-report/

- Cyber Security Agency Of Singapore. (2026, febrero). Largest multi-agency cyber operation mounted to counter threat. https://www.csa.gov.sg/news-events/press-releases/largest-multi-agency-cyber-operation-mounted-to-counter-threat

- Cybersecurity Dive. (2026, 16 marzo). Telus digital confirms hack as shinyhunters claims credit for massive data theft. https://www.cybersecuritydive.com/news/telus-digital-cyberattack-shinyhunters/814817/

- Deepstrike. (2026, 14 junio). Infostealers stole 1.8B credentials. Shattered.io. https://shattered.io/infostealer-malware-1-8b-credentials/

- Federal Student Aid. (2026, 12 mayo). Technology security announcement. https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2026-05-12/technology-security-announcement

- Group-IB. (2026, 13 marzo). Six supply chain attack groups to watch out for in 2026. https://www.group-ib.com/blog/supply-chain-attack-groups-2026/

- INCIBE. (2026, 13 de enero). Endesa notifica a sus clientes una filtración de datos personales. https://www.incibe.es/ciudadania/avisos/endesa-notifica-sus-clientes-una-filtracion-de-datos-personales

- INCIBE-CERT. (2026a, 5 de mayo). Detección de un acceso no autorizado a datos de usuarios de Booking. https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/deteccion-de-un-acceso-no-autorizado-datos-de-usuarios-de-booking

- INCIBE-CERT. (2026b, 11 de mayo). Escalada local de privilegios en el kernel de Linux, Dirty Frag. https://www.incibe.es/incibe-cert/alerta-temprana/avisos/escalada-local-de-privilegios-en-el-kernel-de-linux-dirty-frag

- INCIBE-CERT. (2026c, 21 de mayo). Incidente de seguridad en Inditex vinculado a infraestructura externa de un proveedor. https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/incidente-de-seguridad-en-inditex-vinculado-infraestructura-externa-de

- Industrial Cyber. (2026, 24 marzo). M-Trends 2026 reveals threat landscape shaped by faster, coordinated and industrialized cyberattacks. https://industrialcyber.co/reports/m-trends-2026-reveals-threat-landscape-shaped-by-faster-coordinated-and-industrialized-cyberattacks/

- Le Monde. (2026, 18 febrero). Hacker accessed data from 1.2 million bank accounts. https://www.lemonde.fr/en/economy/article/2026/02/18/hacker-accessed-data-from-1-2-million-bank-accounts-french-economy-ministry-says_6750628_19.html

- Medtronic. (2026, 24 abril). Medtronic statement on unauthorized system access. https://news.medtronic.com/medtronic-statement-on-unauthorized-system-access

© 2026 NTT DATA, Inc.

- Radware. (2026, 19 febrero). 2026 global threat report shows ddos attacks jump 168% as cyber threats escalate across networks and applications. Globenewswire. https://www.globenewswire.com/news-release/2026/02/19/3240861/0/en/radware-2026-global-threat-report-shows-ddos-attacks-jump-168-as-cyber-threats-escalate-across-networks-and-applications.html

- SecurityToday. (2026, 6 abril). Ransomware 2026: pay or not pay. https://www.securitytoday.de/en/2026/04/06/ransomware-2026-companies-pay-ransom-payment/

- Securityweek. (2026, 19 mayo). Verizon DBIR 2026: vulnerability exploitation overtakes credential theft as top breach vector. https://www.securityweek.com/verizon-dbir-2026-vulnerability-exploitation-overtakes-credential-theft-as-top-breach-vector/

- SentinelOne. (2026, 7 mayo). 55 estadísticas más recientes de malware para 2026. https://www.sentinelone.com/cybersecurity-101/cybersecurity/malware-statistics/

- SOSransomware. (2026, 28 febrero). Ransomware in 2026: fewer victims paying but higher ransoms. https://sosransomware.com/en/ransomware-en/ransomware-payments-in-2025-fewer-victims-paying-but-higher-ransoms/

- StationX. (2026, junio). Cyber security breach statistics 2026: key facts & data. https://app.stationx.net/articles/cyber-security-breach-statistics

- Stryker. (2026, abril). Customer updates: stryker networks disruption. https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html

- TechRepublic. (2026, 3 abril). FBI declares surveillance system breach a ‘major incident’. https://www.techrepublic.com/article/news-china-linked-fbi-surveillance-breach-major-incident/

- TechRepublic. (2026, 20 abril). 2026’s breach list so far. https://www.techrepublic.com/article/news-top-cyberattacks-2026-so-far/

- The Cyber Express. (2026, 12 marzo). Cyber Warfare 2026: nation-state attacks. https://thecyberexpress.com/cyber-warfare-2026-nation-state-attacks/

- The Hacker News. (2026, 17 enero). Experts detect pakistan-linked cyber campaigns aimed at indian government entities. https://thehackernews.com/2026/01/experts-detect-pakistan-linked-cyber.html

- The Hacker News. (2026, 2 mayo). Trellix confirms source code breach with unauthorized repository access. https://thehackernews.com/2026/05/trellix-confirms-source-code-breach.html

- Verizon. (2026). 2026 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

- World Economic Forum. (2026, 12 enero). Cyber Risk in 2026: what execs need to know as global cyber risk. https://www.weforum.org/stories/2026/01/geopolitics-ai-fraud-global-cyber-cybersecurity-2026/

- Zscaler. (2026, 2 febrero). APT28 leverages CVE-2026-21509 in operation neusploit. https://www.zscaler.com/blogs/security-research/apt28-leverages-cve-2026-21509-operation-neusploit

- ESET. (2026). APT Activity Report. https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2025-q1-2026.pdf

© 2026 NTT DATA, Inc.


NTT DATA