CTI-TEND-2024

NTT DATA

Tendencias CTI

Ciberinteligencia de Amenazas

Segundo semestre 2024

Índice

1. **Introducción** **4**

1.1. Alcance del informe 4
1.2. Alcance geográfico y temporal del informe 4

2. **Panorama global de amenazas** **5**

2.1. Geopolítica y Ciberseguridad 6
2.2. Geopolítica y principales actores 6
2.3. Afectación a sectores específicos 7

3. **Principales amenazas globales** **10**

3.1. Grandes ciberincidentes y/o campañas 11
3.2. Tendencias emergentes de ataques 12
3.3. Estadísticas globales sobre incidentes de seguridad, tipos de ataques y Actores Maliciosos involucrados 14
3.4. Costes de los ciberataques para las empresas 15

4. **Marco legal y detenciones en ciberseguridad** **17**

4.1. Principales leyes en el ámbito de la ciberseguridad 18
4.2. Principales detenciones en el ámbito de la ciberseguridad 19

5. ***Dark Web Insights*** **22**

6. **Actores Maliciosos (*Threat Actors*)** **25**

6.1. Nuevos Actores Maliciosos 27
6.2. Grupos de *Ransomware* 29
6.3. *Hacktivistas* 31
6.4. APT 33

Índice

7. **Tácticas, Técnicas y Procedimientos** **34**

7.1. Descripción de las TTP más comunes utilizadas por los cibercriminales 35
7.2. Vectores de entrada más usuales 37
7.3. Innovación en ataques: Nuevas técnicas y tácticas desconocidas 37

8. **Tendencias de vulnerabilidades** **40**

9. **¿Qué nos espera en 2025?** **46**

10. **Referencias** **48**

Introducción

1.1. Alcance del informe

El presente informe tiene como objetivo proporcionar una visión detallada e integral de las tendencias, incidencias y acontecimientos relevantes en el ámbito de la Inteligencia de Amenazas durante el segundo semestre del 2024. Se analizarán las amenazas emergentes que están redefiniendo el panorama de la ciberseguridad, los Actores Maliciosos que han demostrado una actividad significativa, las campañas cibernéticas más destacadas, así como las vulnerabilidades críticas identificadas en este período. También, se analizarán patrones recurrentes y tendencias a futuro que podrían influir en la estrategia de mitigación de riesgos.

1.2. Alcance geográfico y temporal del informe

El alcance de este documento pone foco en las tendencias de Ciberinteligencia de Amenazas en un ámbito geográfico global, permitiendo a los lectores entender cómo las amenazas evolucionan de manera interconectada a lo largo de diferentes contextos geográficos y temporales.
Se analizan los eventos y dinámicas observadas en el ecosistema de las ciberamenazas en el segundo semestre del año 2024, de julio a diciembre. Un intervalo crítico en el que se han identificado eventos significativos y cambios en el comportamiento de las amenazas.

Panorama Global de Amenazas

2. Panorama global de amenazas

2.1 Geopolítica y Ciberseguridad

Desde el **Departamento de Cyber Threat Intelligence** de **NTT DATA,** examinamos la intensificación de la relación entre la geopolítica y la ciberseguridad durante el segundo semestre del 2024, evidenciando un mundo cada vez más interconectado y susceptible a las dinámicas globales. El ciberespacio se ha transformado en un ámbito estratégico en el que las tensiones a nivel mundial, conflictos regionales y la rivalidad entre potencias se expresan mediante ciber-ataques, espionaje digital y campañas de influencia.

Durante este periodo, tanto actores estatales como los no estatales han intensificado sus operaciones, impactando tanto en infraestructuras críticas como en sectores estratégicos esenciales. Este reporte ofrece un estudio minucioso de tres elementos clave: las amenazas globales originadas por las tensiones geopolíticas, los actores principales en estas operaciones y el efecto de estas acciones en sectores determinados.

Las innovaciones tecnológicas también han revolucionado este escenario, instrumentos como **la Inteligencia Artificial (IA)** y el **Internet de las Cosas (IoT)** han aumentado la complejidad de los ataques en el ciberespacio, facilitado la creación de *malware* flexible y *phishing* a medida.

En cambio, las **amenazas persistentes avanzadas (APTs)** han cobrado relevancia como instrumentos esenciales para el espionaje y el sabotaje. Con el objetivo de infiltrarse en sistemas esenciales, eludiendo las estrategias de seguridad convencionales. Simultáneamente, los **ataques a la cadena de suministro digital** han demostrado ser particularmente eficaces al poner en riesgo a los proveedores y propagar *malware* en actualizaciones de *software* auténticas, impactando sectores completos convirtiéndose en una amenaza clave en 2024 (Xygeni, 2024).

Es fundamental entender esta convergencia entre geopolítica y ciberseguridad para prever peligros y robustecer las tácticas de defensa.

2.2 Geopolítica y principales actores

La situación mundial en este segundo semestre de 2024 y su proyección para 2025 están estrechamente vinculadas a la geopolítica. En el panorama global de ciberamenazas, es crucial examinar cómo estas tensiones geopolíticas se materializan en conflictos específicos. De esta forma, se presenta una agrupación de los conflictos geopolíticos más relevantes y sus implicaciones en el ciberespacio.

- **Rusia y Ucrania: La guerra en el ciberespacio como prolongación del conflicto armado**

El conflicto entre Rusia y Ucrania continúa siendo el escenario predominante de **guerra híbrida**, en la que el ciberespacio potencia las operaciones bélicas convencionales.

Rusia, destaca por su uso del ciberespacio como un complemento a sus operaciones, movilizando agrupaciones maliciosas como ***Sandworm*** y ***Fancy Bear***, que han llevado a cabo ataques contra la infraestructura de energía y transporte de Ucrania usando tecnologías de vanguardia. Lo cual ha tenido impacto no solo en Ucrania, sino también en compañías y gobiernos europeos (ENISA, 2024; CrowdStrike, 2024 y Google Threat Analysis Group, 2024) .

Además, Ucrania ha potenciado sus habilidades de ofensiva con el respaldo de aliados internacionales. Grupos maliciosos como ***IT Army of Ukraine*** han llevado a cabo ataques distribuidos contra sistemas rusos. Esto ha demostrado que el ciberespacio se transforma en un multiplicador de fuerza en enfrentamientos actuales.

- **Irán y Arabia Saudita: Ciberataques en el Golfo**

En el Golfo Pérsico, Irán ha empleado *malware* para infiltrarse en instalaciones de energía de Arabia Saudita, impactando operaciones vitales en la industria del petróleo y el gas. Estos ataques se distinguen por su potencial dañino, dirigidos tanto a sistemas operativos como a datos esenciales, y evidencian el empleo estratégico del ciberespacio como un avance del conflicto político y militar en la zona (CrowdStrike, 2024).

En cuanto a Arabia Saudita, ha fortalecido su infraestructura de ciberseguridad a través de la cooperación con aliados a nivel global y el incremento de habilidades internas. Este esfuerzo tiene como objetivo salvaguardar

sectores críticos ante ciberamenazas sofisticadas que impactan tanto en la estabilidad energética como en la reputación mundial del país como proveedor fiable de recursos (International Telecommunication Union, 2024).

Este conflicto subraya la manera en que el ciberespacio incrementa las tensiones a nivel regional y posee la capacidad de desestabilizar mercados fundamentales como el energético.

- **Corea del Norte y Corea del Sur: Finanzas y espionaje**

Corea del Norte mantiene vínculos estratégicos con China para sustentar su régimen a través de ciberataques. Éstos incluyen operaciones del grupo malicioso ***Lazarus***, que ha sido asociado a ataques contra intercambios de criptomonedas y bancos a nivel mundial, sustrayendo grandes cantidades a través de métodos sofisticados como la implementación de puertas traseras en *software* y ataques orientados a redes financieras a nivel mundial (JPCERT, 2024).

Por su parte, Corea del Sur ha aumentado su inversión en ciberseguridad, centrándose en tecnologías de **Inteligencia Artificial** para la identificación y reducción precoz de amenazas. Estas tácticas han contemplado la aplicación de instrumentos de vigilancia avanzados y la cooperación con aliados a nivel global para enfrentar amenazas que trascienden fronteras (LISA Institute, 2024).

- **Israel y Gaza: Operaciones de ciberseguridad en un conflicto asimétrico**

La disputa entre estos dos países ha agudizado la utilización de ciberataques. Organizaciones apoyadas por Irán, como el grupo malicioso **APT33**, han llevado a cabo campañas de desinformación y sabotaje contra entidades financieras y gubernamentales de Israel (MITRE ATT&CK, 2024). Estas campañas tienen como objetivo debilitar la estabilidad interna de Israel a través del cese de servicios críticos y la difusión de propaganda. Aun así, las habilidades defensivas de Israel, han facilitado tanto la protección de su infraestructura como la ejecución de ataques para contrarrestar amenazas de estos actores. Estas operaciones resaltan la evolución de los ciberataques hasta transformarse en instrumentos esenciales en los conflictos. Con impactos tanto en la economía como en la percepción pública a nivel mundial.

- **EEUU y China: Imperio digital y ciberespionaje**

Este conflicto simboliza la lucha entre el dominio tecnológico del G20, encabezado por EEUU, y el avance de China, un miembro clave del BRICS que ha intensificado sus operaciones de ciberespionaje con agrupaciones maliciosas como **APT41**, orientadas al hurto de derechos de autor y a la infiltración en redes de telecomunicaciones de EEUU (CISA, 2024; Mandiant, 2024). Como reacción, EEUU ha establecido capacidades de ciberdefensa avanzadas, penalizando a compañías chinas y cooperando con aliados para contrarrestar estas amenazas, además, entidades como la CISA y la NSA han encabezado iniciativas para detectar y minimizar riesgos como, campañas de *phishing* y otros ataques (CrowdStrike, 2024; ENISA, 2024).

2.3 Afectación a sectores específicos

Desde el **Departamento de Cyber Threat Intelligence de NTT DATA** se ha identificado una evolución en los sectores más afectados en el segundo semestre de 2024.

Durante el segundo semestre de del 2024, los sectores más atacados incluyeron servicios profesionales, gobierno y finanzas. Sin embargo, según el análisis reciente de amenazas globales (ENISA, 2024; Verizon DBIR, 2024; CrowdStrike, 2024), se revela un cambio significativo en la distribución de los ataques.

Esta nueva distribución de ataques refleja la fuerte influencia de las tensiones geopolíticas, dirigidos principalmente a sectores estratégicos y países de alta relevancia económica o en conflicto. Aunque el impacto no se distribuyó uniformemente, ya que algunos sectores se vieron más afectados que otros:

- **Adminisración pública y Gobiernos**

Con 1.876 ataques registrados, los organismos gubernamentales y las entidades del sector público se enfrentan a amenazas constantes, a menudo procedentes de agentes del Estado-nación que buscan ventajas estratégicas o de *hacktivistas* con motivaciones ideológicas. El enorme volumen de datos de los ciudadanos y de infraestructuras críticas gestionadas por estas organizaciones las convierte en objetivos prioritarios.

- **Educación**

Con 1.440 ataques, las instituciones educativas, en particular las universidades, son cada vez más el blanco de ataques por su propiedad intelectual, sus datos personales y sus vulnerabilidades operativas. Los atacantes a menudo pretenden interrumpir las operaciones o monetizar los datos robados en la *dark web*.

- **Servicios financieros**

El sector de los servicios financieros, con 658 ataques, figura sistemáticamente entre las industrias más atacadas debido a su acceso a fondos y datos confidenciales de los clientes. En 2024, los ciberdelincuentes han adoptado tácticas sofisticadas y explotado múltiples vulnerabilidades internas.

- **Tecnología de la información**

Destaca con 795 ataques que buscan explotar recursos tecnológicos. El 22% de las brechas de datos globales en estas industrias estuvieron vinculadas a *malware* y *phishing*.

- **Energía**

Los ataques a este sector se centraron en APTs dirigidas a redes eléctricas y sistemas petroleros, reflejando un enfoque estratégico motivado por las tensiones geopolíticas globales.

Sectores más afectados de Julio a Diciembre 2024

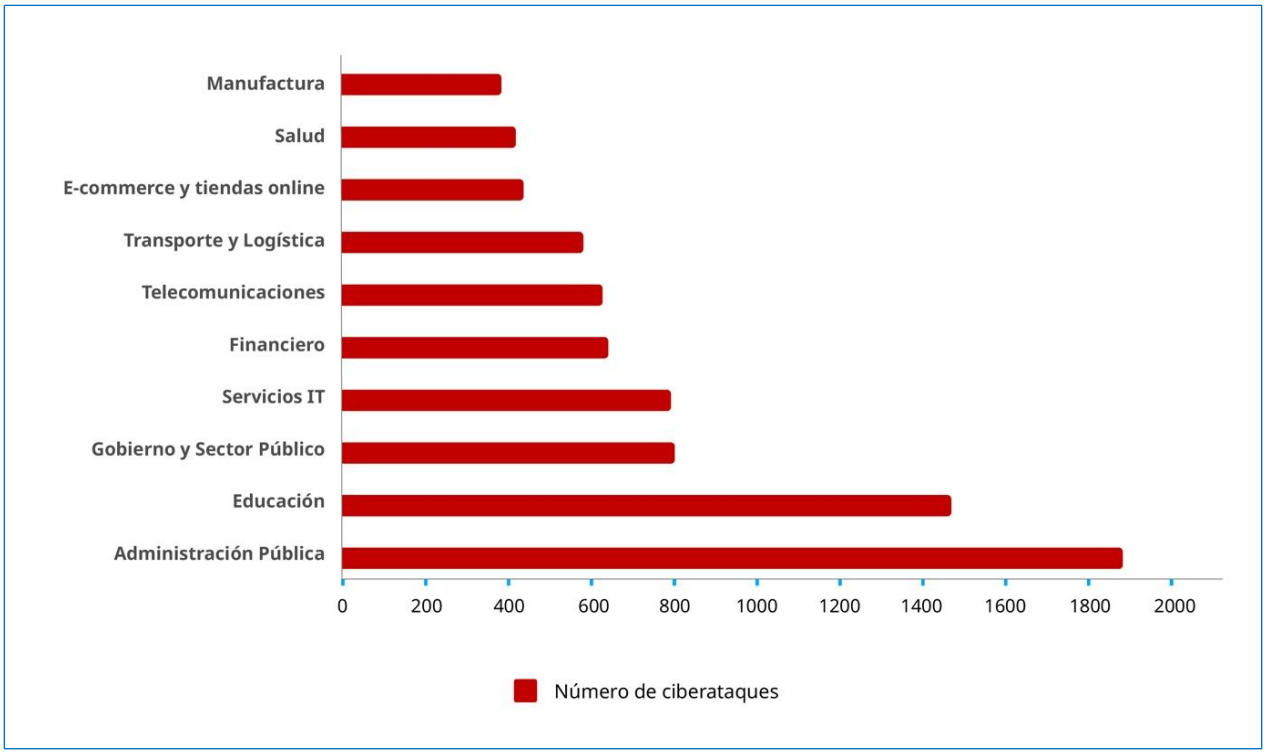


Tabla 1 | Sectores más afectados por ciberataques en el segundo semestre de 2024.

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

- **Estados Unidos**

Con 2.984 ataques, lidera la lista de países más afectados, lo que refleja su importancia estratégica y económica.

- **India**

Registró 2.069 ataques, impulsados por su acelerada digitalización y expansión tecnológica, siendo así el IoT y 5G sus puntos críticos de vulnerabilidad.

- **Israel y Ucrania**

Con 1.465 y 1.201 ataques respectivamente, enfrentaron amenazas vinculadas a los conflictos regionales, entre las que se incluyen el ciberespionaje y el sabotaje de infraestructuras.

- **Indonesia**

De entre los 763 ataques registrados, sufrió un ataque significativo contra su centro de datos nacional, destacando las vulnerabilidades en economías emergentes.

Distribución de ciberataques por países de Julio a Diciembre 2024

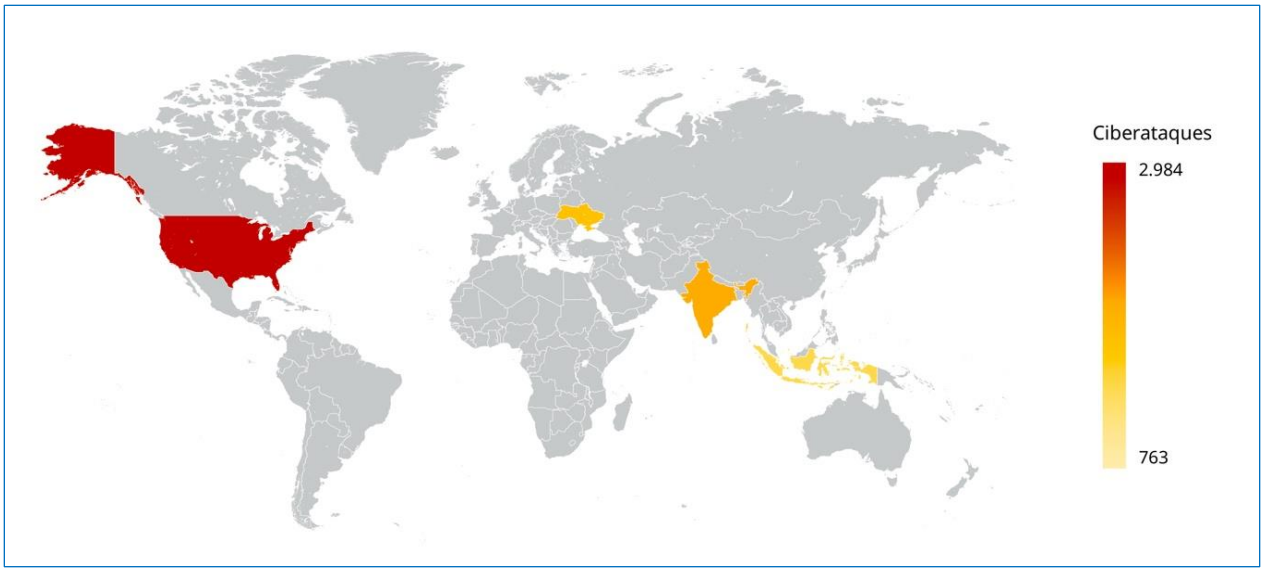


Figura 1 | Distribución por países del impacto de ciberataques en el segundo semestre de 2024.

Principales Amenazas Globales

3. Principales amenazas globales

Las ciberamenazas del segundo semestre de 2024 reflejan un panorama en constante evolución, caracterizado por una creciente sofisticación y la interconexión de riesgos en distintos ámbitos. Los avances tecnológicos, las vulnerabilidades en infraestructuras críticas y los desafíos asociados a la confianza digital y las identidades han generado un entorno de amenaza diversificado y más difícil de gestionar.

Desde el **Departamento de Cyber Threat Intelligence de NTT DATA**, hemos analizado estas amenazas para identificar patrones clave, los cuales han sido organizados en **cinco clústeres temáticos**: **Tecnología**, **Infraestructura**, **Identidad y Confianza**, **APTs** y **Amenazas Emergentes**. Esta categorización no solo facilita una comprensión más profunda de los riesgos actuales, sino que también ofrece una perspectiva estratégica para anticipar las tendencias que marcarán el panorama cibernético en 2025.

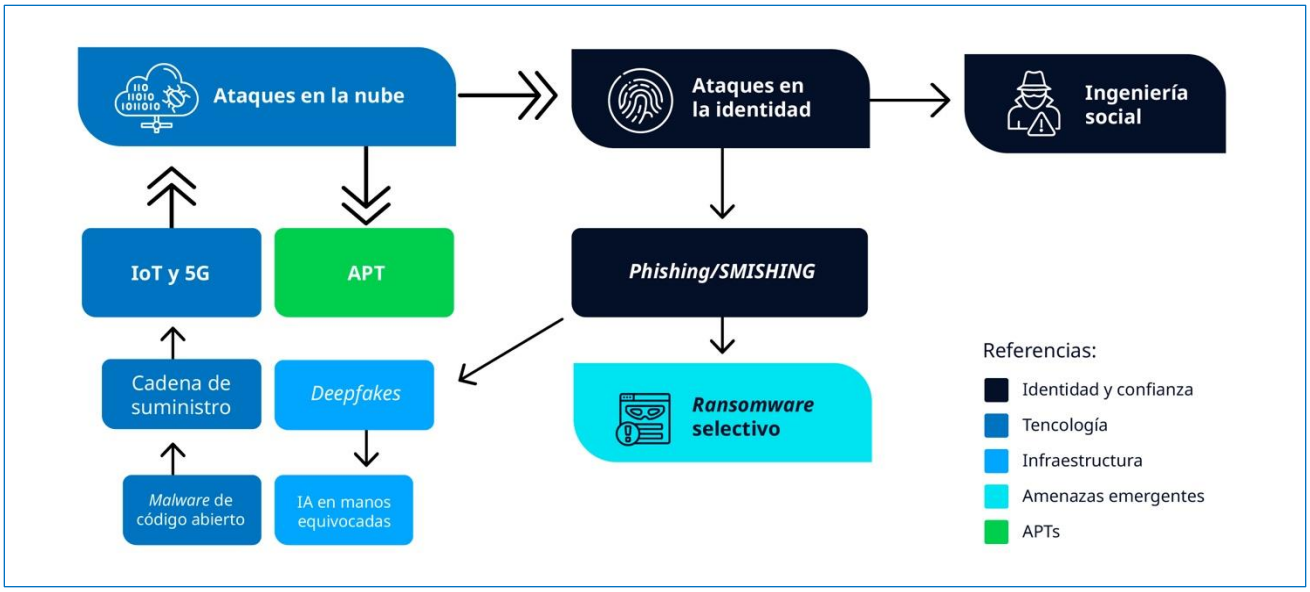


Figura 2| Diagrama que muestra las conexiones entre las principales amenazas cibernéticas de 2024 y su organización en clústeres temáticos: tecnología, infraestructura, identidad y confianza, apts y amenazas emergentes.

El segundo semestre de 2024 consolidó la convergencia de amenazas en torno a tecnologías avanzadas, como la IA y el IoT, con un aumento en el uso de estrategias de ingeniería social y vulnerabilidades en la cadena de suministro. Este análisis refuerza que, para 2025, el enfoque en la interconexión de estas amenazas será esencial para gestionar un ciberespacio cada vez más complejo.

3.1 Grandes ciberincidentes y/o campañas

El segundo semestre de 2024 marcó un incremento significativo en el número y la escala de ciberincidentes a nivel global, superando los registros del primer semestre del año. Este periodo estuvo caracterizado por un aumento en la sofisticación de los ataques, la aparición de nuevas tácticas y herramientas maliciosas, y el impacto generalizado sobre sectores clave, desde infraestructuras críticas hasta empresas privadas y usuarios individuales.

Estos eventos se presentan a continuación, organizados cronológicamente para resaltar su evolución e impacto a lo largo del periodo:

Empresa, Tecnología y/o Gobierno afectado	Atacante	País afectado	País del atacante	Fecha del incidente	URL
Prudential Financial	Alphy Ransomware	EEUU	Desconocido	01/07/2024	Fuente
Crowstrike	Desconocido	Mundial	Desconocido	19/07/2024	Fuente
Infraestructuras Críticas, Gobierno, Universidades, Empresas de TI y Hospitales	Earth Baku	Mundial	China	13/08/2024	Fuente
Ataque a Internet Archive	Hacktivistas pro-palestinos	Mundial	Desconocido	04/09/2024	Fuente
American Water	Desconocido	EEUU	Desconocido	07/10/2024	Fuente
Scheider Electric	Hellcat	Mundial	Desconocido	03/11/2024	Fuente
Nokia	IntelBroker	Mundial	Desconocido	04/11/2024	Fuente
Empresas de Telecomunicaciones Estadounidenses (Verizon y AT&T)	Salt Typhoon	EEUU	China	10/11/2024	Fuente
Equinox	LockBit	EEUU	Rusia	20/11/2024	Fuente
Refinadora Costarricense de Petróleo (RECOPE)	Desconocido	Costa Rica	Presuntamente Rusia	02/12/2024	Fuente
Administración Pública e Infraestructuras Críticas	Storm-2077	EEUU	Presuntamente China	06/12/2024	Fuente

Tabla 2 | Grandes ciberincidentes de seguridad en el segundo semestre de 2024.

3.2 Tendencias emergentes de ataques

A medida que nos acercamos a 2025, el panorama de la ciberseguridad se vuelve más complejo y dinámico, impulsado por la rápida evolución tecnológica. Las capacidades de los atacantes crecen a un ritmo sin precedentes, lo que amplía las amenazas y desafía a las organizaciones a anticiparse y adaptarse a este entorno en constante cambio.

3.2.1 Ataques generados con inteligencia artificial

El próximo año, se prevé que los ciberdelincuentes continúen adoptando rápidamente herramientas basadas en IA para potenciar y facilitar sus operaciones en línea a lo largo de las diferentes fases del ciclo de vida de los ataques. Se espera un uso continuado de la IA y de grandes modelos de lenguaje (LLM) para desarrollar y ampliar ataques de *phishing*, *vishing*, SMS y otros tipos de ingeniería social más sofisticados y persuasivos. Asimismo, se anticipa que actores de amenaza seguirán aprovechando *deepfakes* para el robo de identidad, el fraude y la elusión de los requisitos de seguridad de conocimiento del cliente (KYC - Know Your Customer).

Por otro lado, prevemos un incremento en la demanda de *LLM* sin barreras de seguridad en foros clandestinos, lo que permitirá a los actores maliciosos explorar temas ilícitos sin restricciones éticas. A medida que las capacidades de la IA se expandan y popularicen a lo largo de 2025, las empresas enfrentarán mayores dificultades para defenderse de estos ataques más frecuentes y eficaces.

3.2.2 Ataques de tipo *Ransomware:* Automatización y objetivos estratégicos

El *ransomware* y la extorsión por robo de datos son, y seguirán siendo en 2025, las formas de

ciberdelincuencia más disruptivas a nivel mundial. Su impacto no solo se mide por el volumen de ataques, sino también por los daños potenciales que cada ataque puede desencadenar. Estas operaciones se caracterizan por su capacidad de amplificar el daño mucho más allá de la víctima inicial, creando efectos dominó en comunidades y sectores enteros.

En 2024 se produjeron importantes ataques de *ransomware* en el sector sanitario que afectaron negativamente a la atención de los pacientes en los hospitales, impidiendo a los pacientes acceder a prescripciones médicas y dificultando a los médicos realizar pruebas de laboratorio vitales, o facturar a empresas de seguros.

Las operaciones de *ransomware* y extorsión en 2024 han afectado a más de 100 países y a todos los sectores. El número de sitios dedicados a la filtración de datos (DLS – Dedicated Leak Sites) se duplicó en 2024 con respecto a 2023, y la nueva aparición de múltiples ofertas de *ransomware* como servicio (RaaS), ilustran la próspera y prolífica naturaleza del panorama de amenazas de *ransomware* y la extorsión.

3.2.3 Ataques de tipo infostealers: Una puerta de acceso a las filtraciones de datos de alto impacto

Los *infostealers*, aunque no representan una amenaza nueva, han evolucionado hasta convertirse en una herramienta cada vez más sofisticada y eficaz dentro del arsenal de los actores maliciosos. Durante 2024, estas herramientas fueron utilizadas para recopilar credenciales robadas a gran escala, lo que permitió infiltraciones en organizaciones y causó intrusiones de alto impacto. Lo más alarmante es la facilidad con la que estas credenciales son accesibles en mercados clandestinos, permitiendo incluso a actores poco cualificados ejecutar ataques efectivos, lo que amplifica significativamente su potencial disruptivo.

Se prevé que esta tendencia continúe en 2025, con los *infostealers* manteniéndose como el principal vector para la obtención de credenciales robadas. Su impacto será especialmente pronunciado en entornos donde aún no se implemente la autenticación de dos factores, dejando a muchas organizaciones vulnerables a graves filtraciones de datos.

Además, la sofisticación del *malware infostealer* ha aumentado en los últimos años, incorporando técnicas de anti evasión y capacidades para eludir la detección y respuesta de puntos finales (EDR - Endpoint Detection Response), lo que los convierte en retos aún más complejos en el panorama de las ciberamenazas.

3.2.4 Democratización de las herramientas de ataque

En 2025, las organizaciones seguirán enfrentándose a un panorama de amenazas donde las barreras de entrada para los actores estatales y ciberdelincuentes menos sofisticados seguirán reduciéndose. La proliferación de herramientas, kits de *phishing* y recursos *«as-a-service»* con capacidades avanzadas, permitirá a actores maliciosos con poca experiencia, así como a nuevos participantes, ejecutar operaciones de manera más eficaz y con mayor destreza.

Esta profesionalización de los servicios cibercriminales ampliará las amenazas y complicará las respuestas necesarias para mitigarlas. Además, el uso de Inteligencia Artificial generativa en distintas fases de los ataques aumentará la eficiencia y adaptabilidad de los actores maliciosos frente a las defensas actuales.

3.3 Estadísticas globales sobre incidentes de seguridad, tipos de ataques y Actores Maliciosos involucrados

Desde el **Departamento de Cyber Threat Intelligence** de **NTT DATA** se pudo establecer que, durante el primer semestre de 2024, los ciberataques crecieron tanto en volumen como en alcance, con un incremento significativo del *ransomware*. Aunque **las defensas han mejorado en la contención de ciertos pagos**, el número de rescates confirmados continúa aumentando, impulsado por el incremento en el volumen y alcance de los ciberataques. Esto ha generado una presión adicional en los costos globales de ciberseguridad y ha mantenido el impacto económico y operativo en niveles críticos. **(Informe de Tendencias de CTI del primer semestre de 2024 - NTT Data, 2024).**

En el segundo semestre, la proliferación de servicios ***Ransomware-as-a-Service*** **(RaaS)** y ataques dirigidos a la **cadena de suministro** provocó un aumento del **39%** en los ataques reportados. Sectores como **salud, educación, gobiernos, PYMEs y finanzas** fueron los más afectados. (Acronis, 2024; IOCTA - Europol; 2024; ENISA, 2024).

Entre las principales estadísticas y tendencias del segundo semestre de 2024 podemos observar:

- **Actividad en la *Dark Web***

En el segundo semestre del 2024, 2.126 actores maliciosos estuvieron activos en la *Dark Web*, realizando colectivamente 18.537 publicaciones aproximadamente. Estas actividades se centraron principalmente en la venta de datos comprometidos y credenciales de acceso no autorizadas, lo que subraya el creciente panorama de amenazas en los foros clandestinos.

- ***Ransomware***

Estados Unidos fue el principal objetivo de los ataques de *ransomware*, con el 54,12% de todos los ataques registrados a nivel mundial. Durante el segundo semestre, los ataques de *ransomware* aumentaron un 15% en julio y un 18% adicional en septiembre, consolidándose como la amenaza principal, además el sector de la manufactura

- **Principales grupos de *ransomware***

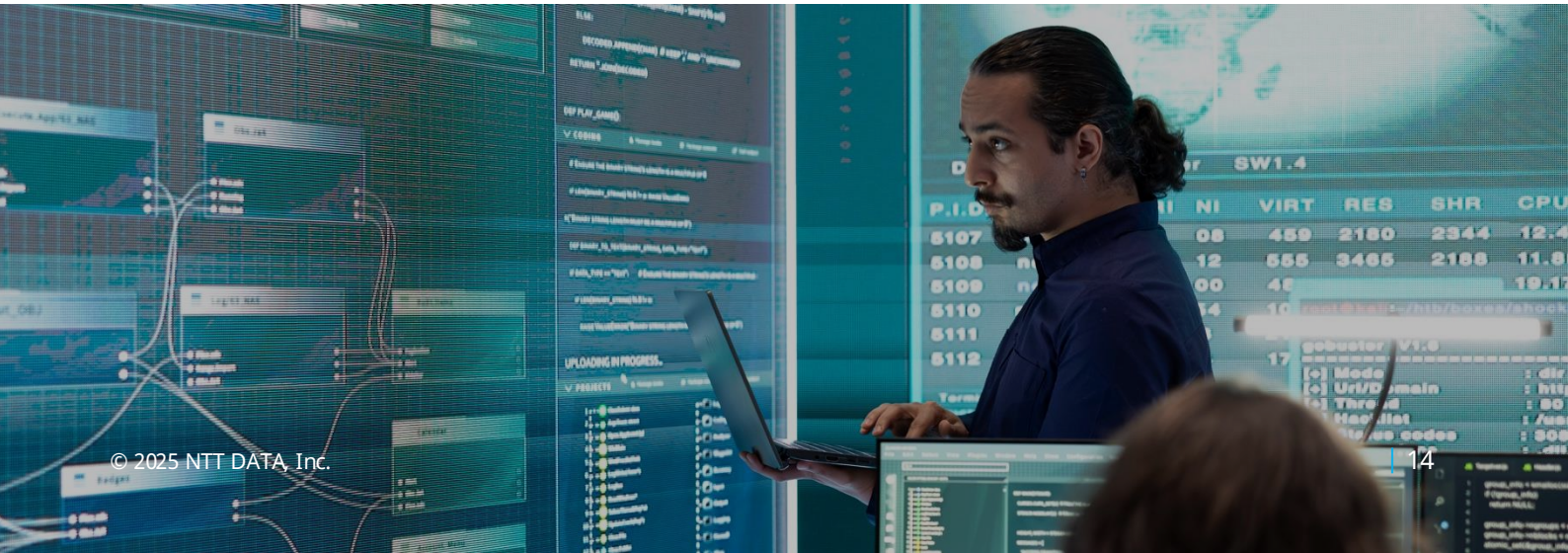
Los grupos maliciosos clave de *ransomware* que dominaron el panorama de 2024, fueron **RansomHub** (9,45%), **Play Ransomware Group** (6,91%) y **LockBit** (5,96%). Estos grupos maliciosos explotaron vulnerabilidades en sectores críticos, causando daños generalizados.

- **Ataques de *phishing***

Estados Unidos experimentó la mayor proporción de ataques de *phishing* a nivel mundial, con un 34,89%, seguido de Singapur (15,89%) y el Reino Unido (3,06%). Estas estadísticas revelan la concentración regional de las campañas de *phishing*. Se vieron incrementados un 12% en agosto, pero se estabilizaron en octubre, especialmente en sectores bancarios y de salud.

- **Denegación de servicios (DoS)**

Incrementaron un 20% entre septiembre y octubre, afectando particularmente a administraciones públicas.



Incremento porcentual estimado de ataques por categoría para el segundo semestre de 2024.

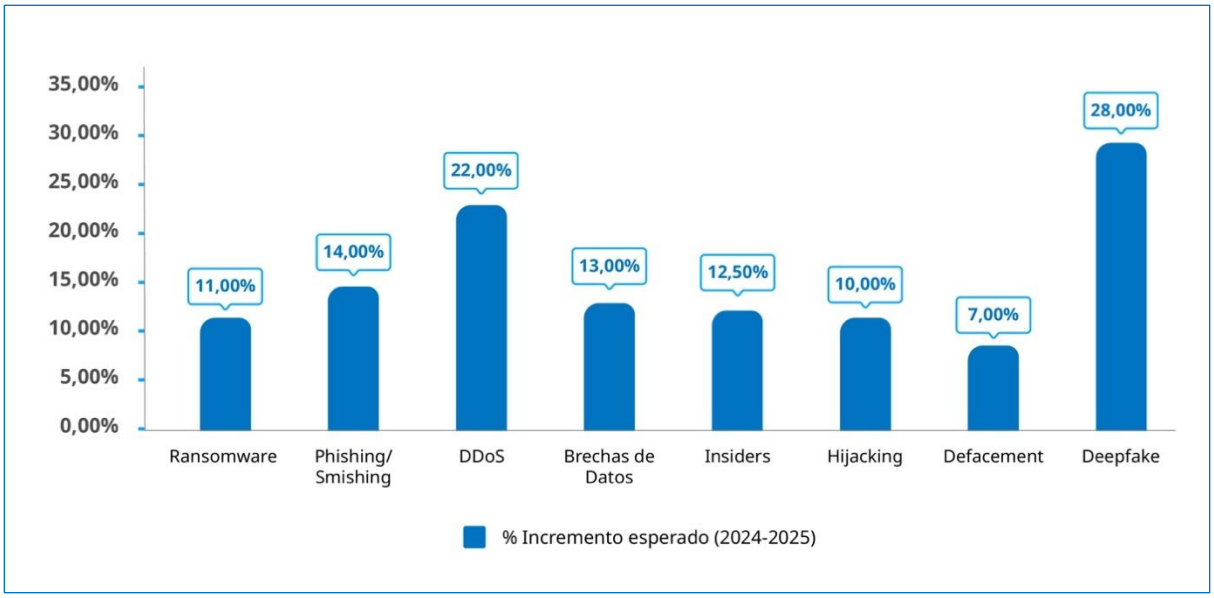


Figura 3 | Porcentaje de incremento en el número de ataques por categoría en comparación con el primer semestre de 2024.

- El aumento porcentual durante el segundo semestre de 2024 evidencia una intensificación operativa de los actores maliciosos y la variedad de sus metas.
- El incremento en *ransomware*, *phishing* y *deepfakes* indica un mayor enfoque en métodos que fusionan alcance masivo con impacto económico directo.
- Por otro lado, el aumento en ataques como el **DoS** y las **brechas de datos** demuestra un enfoque sistemático en la interrupción de servicios críticos y en el compromiso de información delicada.
- Los sectores más impactados son la salud, la manufactura y los servicios financieros, donde las debilidades estructurales y la necesidad de aparatos interconectados potencian la repercusión de estos sucesos.
- El incremento en la frecuencia y complejidad de ciberataques plantea retos significativos en costes de mitigación. Este escenario presiona a las organizaciones a invertir en soluciones más robustas de ciberseguridad, lo que se estima que podría **incrementar los presupuestos dedicados entre un 20% y un 30% anual para 2025.** (Revista Ciberseguridad, 2024; Kaspersky, 2024; Silicon Week, 2024; T21, 2024).

3.4 Costes de los ciberataques para las empresas

Desde inicios de 2024, los costes relativos en ciberseguridad han registrado un **aumento estimado del 35%** con proyecciones de **alcanzar hasta un 40%** durante campañas críticas como las de Navidad**.** Este incremento refleja no solo el mayor volumen de ciberataques, sino también el impacto financiero que supone la resiliencia ante nuevos vectores de ataque. Por ejemplo, la adopción de tecnologías emergentes en entornos empresariales, como el **Metaverso** y la integración de sistemas **OT e IoT**, ha incrementado los **costes de contención un 40%** en empresas que implementan estas herramientas, comparado con aquellas que no. (Gartner, 2024; IT User Cybersecurity, 2024; WEForum, 2024).

En este contexto, el impacto económico de los ciberataques sigue un patrón de crecimiento sostenido, acumulando además los efectos de eventos globales como la aceleración digital

durante la pandemia, el auge de nuevas tecnologías y la evolución de las amenazas cibernéticas. Es por ello que, al analizar el crecimiento desde 2020 hasta el último semestre de 2024, podemos comprender cómo ciertos eventos y tecnologías han generado un incremento gradual en sanciones, rescates, interrupciones de negocio y esfuerzos de reforzamiento cibernético.

Esta perspectiva histórica no solo nos permite visualizar tendencias claras, sino que también establece una base sólida para evaluar los retos de 2024, un año marcado por la consolidación de vectores de ataque emergentes y el creciente impacto financiero asociado.

Evolución anual de los costes estimados en ciberseguridad desde 2020 hasta 2024.

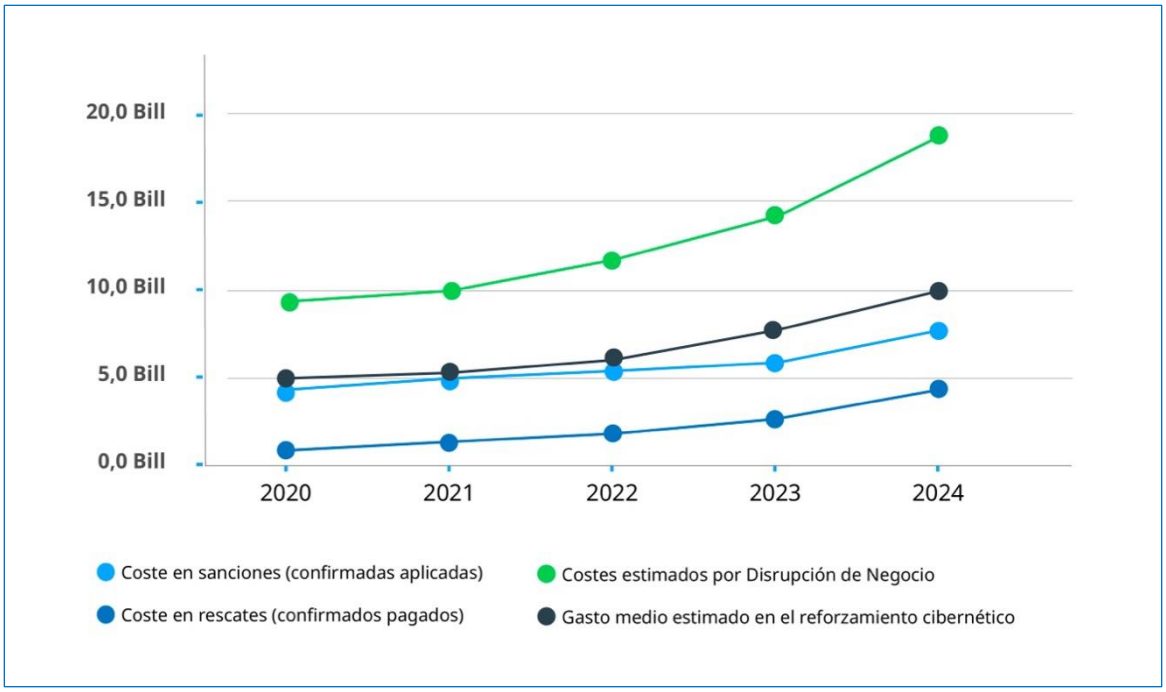


Figura 4 | Evolución anual comparativa de los costes estimados en ciberseguridad (2020 - 2024) desglosado en sanciones, rescates, disrupciones de negocio y refuerzo cibernético.

Marco legal y detenciones en ciberseguridad

4. Marco legal y detenciones en ciberseguridad

Desde el **Departamento de Cyber Threat Intelligence** de **NTT DATA**, se considera esencial analizar las medidas de seguridad implementadas, las leyes aprobadas en el ámbito de la ciberseguridad y las detenciones realizadas por los cuerpos de seguridad a nivel global en este segundo semestre de 2024.

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

4.1 Principales leyes en el ámbito de la ciberseguridad

En lo que respecta a la **Legislación Aplicable en Materia de Ciberseguridad**, a nivel mundial se ha presenciado una escalada en la generación de leyes, normativas, directivas y legislatura aplicable, principalmente centrada en la regulación de tecnologías de actualidad**,** con algún principio de interés en la regulación del uso de otras que están ganando una presencia significativa en el mercado.

En este contexto, resulta evidente la creciente necesidad de legislar en torno a la ciberseguridad y las tecnologías emergentes. Esto se refleja en el aumento constante del número de documentos legales que se han aprobado a nivel mundial desde 2020, con una tendencia al alza (ITU, 2024; WE Forum, 2024; Enisa, 2024):

Evolución anual del total de leyes aprobadas en materia de ciberseguridad (2020 - 2024).

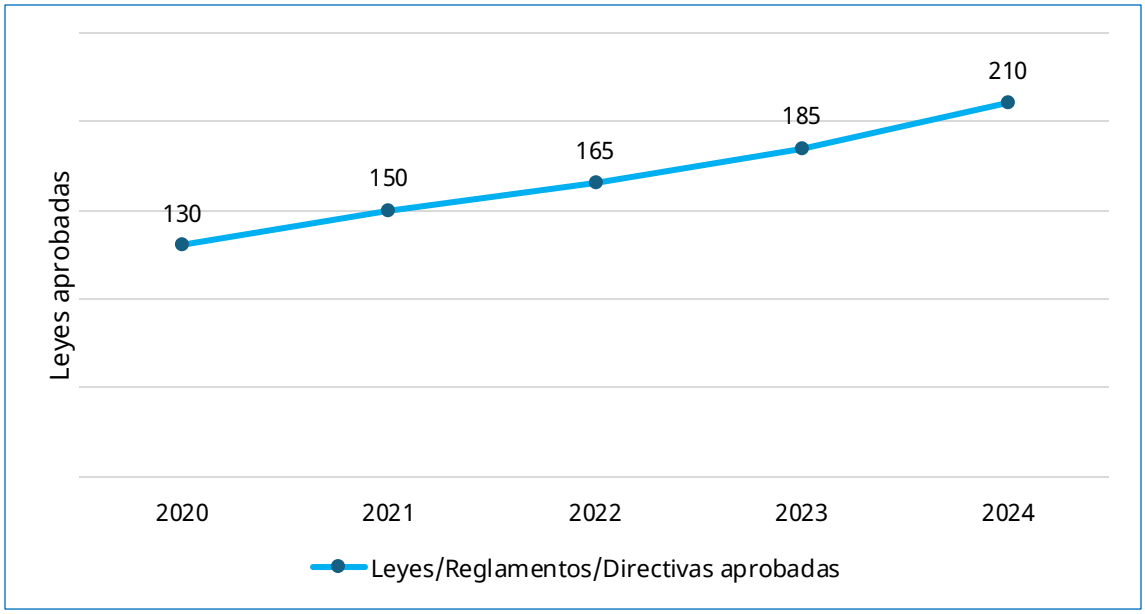


Figura 5 | Tendencia de aprobación de leyes desde 2020 y estimación para 2025.

En lo que respecta a la aprobación de legislación en el segundo semestre de 2024, podemos los siguientes documentos legales aprobados, entre los cuales se encuentran:

Continente	Ley	Institución	Referencias
Asia	Plan Director de Ciberseguridad de la Tecnología Operativa	Gobierno de Singapur	CSA
Europa*	Directiva de seguridad de la información y redes 2 (NIS2)	Unión Europea	Parlamento Europeo
	Reglamento de Resiliencia Operativa Digital (DORA)	Unión Europea	EIOPA
Oceanía	Cyber Security Bill	Gobierno de Australia	Parlamento de Australia

En el ámbito de la legislación europea, es importante destacar dos aspectos clave: por un lado, la **Directiva NIS2 ha comenzado a aplicarse directamente tras superarse el plazo de transposición, incluso en países como España que no han completado este proceso. Por otro lado, aunque el **Reglamento DORA** aún no ha sido aplicable durante el segundo semestre de 2024, entró en vigor el 17 de enero de 2025, con un impacto significativo no solo para las entidades financieras, sino también para los proveedores de servicios IT que les ofrezcan soporte.*

Tabla 3 | Leyes aprobadas en el segundo semestre de 2024.

4.2 Principales detenciones en el ámbito de la ciberseguridad

El segundo semestre de 2024 ha sido un periodo de actividad tanto para las organizaciones de cibercriminales como para los cuerpos y fuerzas de seguridad a nivel global. Este periodo se ha caracterizado por algunas de las detenciones y desmantelamientos de bandas cibercriminales, más activas y peligrosas, responsables de una alta incidencia de ataques en meses previos. Según datos recopilados, las intervenciones policiales internacionales han mostrado un incremento significativo en frecuencia y alcance (Europol, 2024; Interpol, 2024).

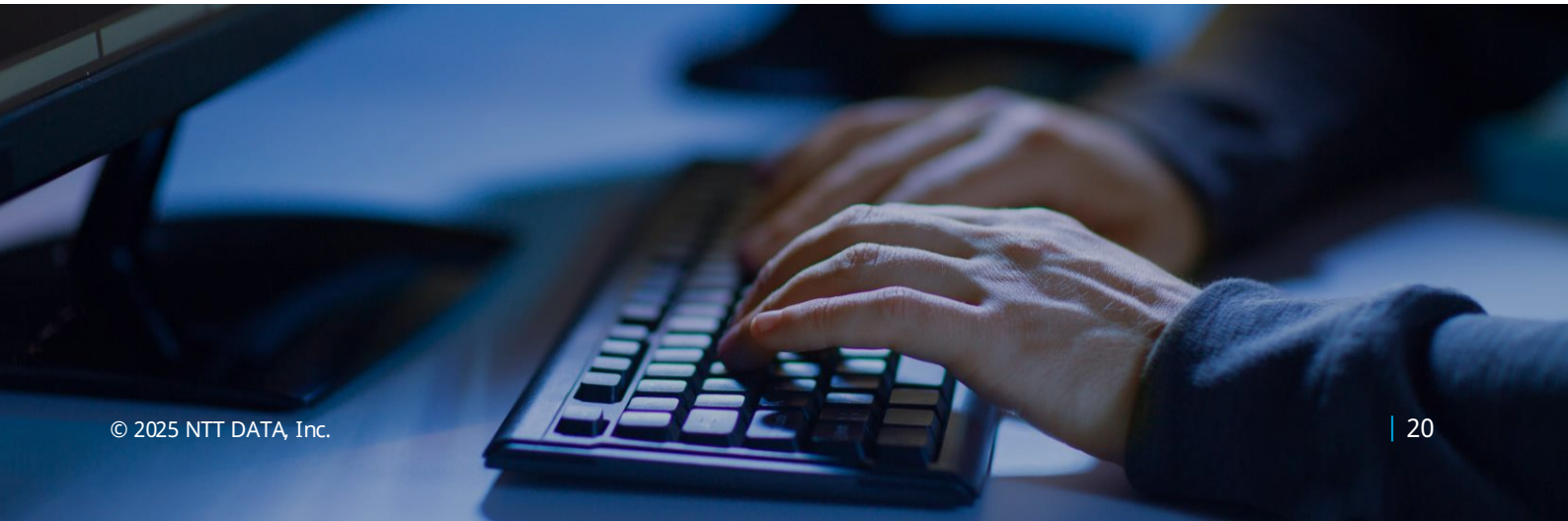
En el caso de **LockBit**, la **Operación Cronos**, liderada por la *National Crime Agency* (NCA) del Reino Unido en colaboración con el FBI, Europol y la Guardia Civil española, desarticuló gran parte de la infraestructura del grupo mediante detenciones clave, incluyendo la captura de un operador principal en España. Esta operación, cuya última fase se llevó a cabo en octubre de 2024, debilitó significativamente los ataques globales de *ransomware*. (Ministerio del Interior, 2024).

Operación	Grupo de actores maliciosos	Fuerzas y cuerpos de seguridad	Referencias
CRONOS	LockBit	NCA (Reino Unido) FBI (EE.UU.) Europol Guardia Civil Eurojust Agencias locales de Polonia y Ucrania	Europol Cybercrime Operations Interpol Europol Europol Europol
Operación Synergia II	Varios (Europa, Sudán del Sur y Zimbaue)	Europol Interpol Agencias locales de varios países	Interpol
Sin nombre	NoName057(16)	Guardia Civil Interpol Europol	INCIBE

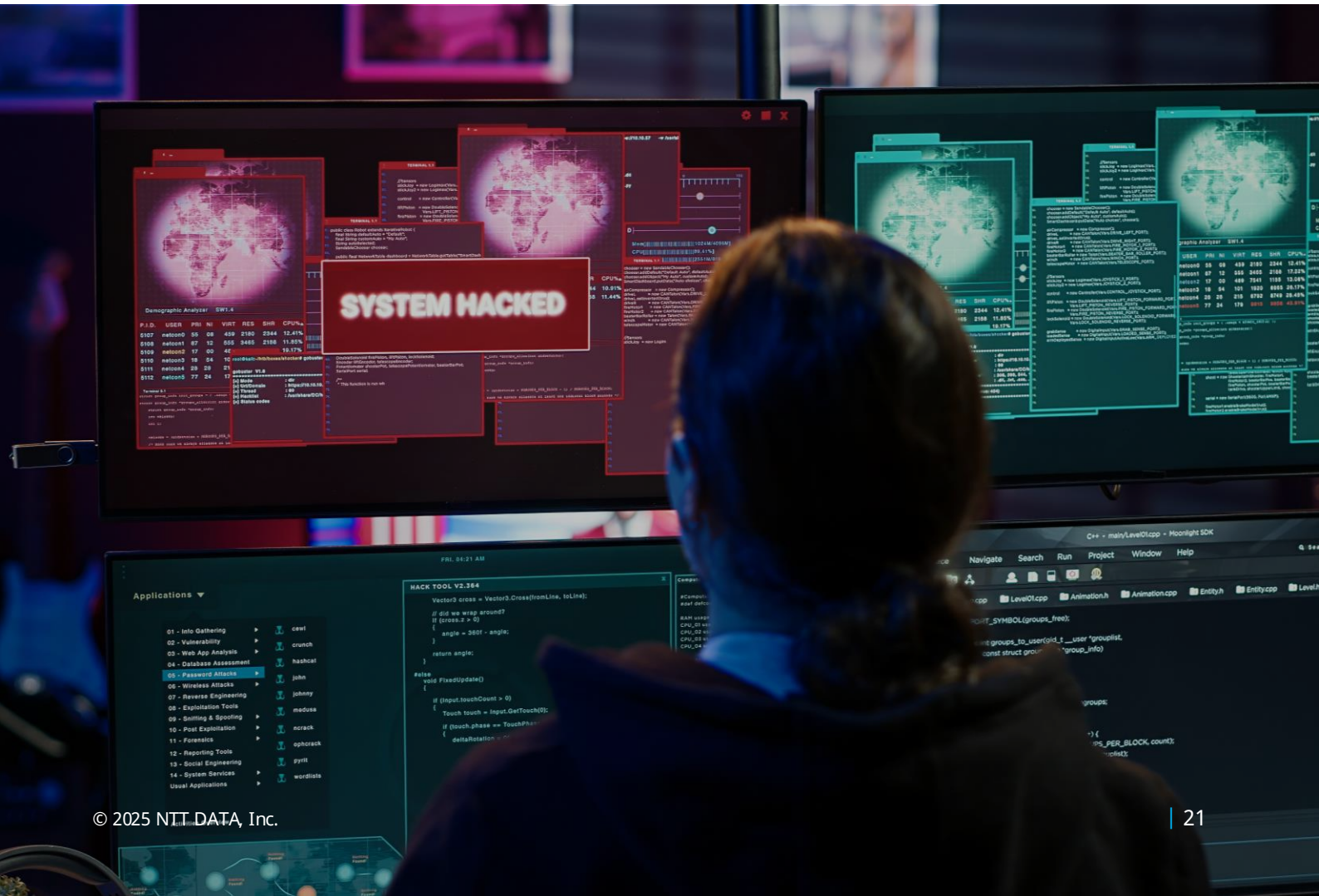
Tabla 4 | Principales operaciones de desmantelamiento de bandas cibercriminales llevadas a cabo en 2024.

A pesar de estos logros, existe una "cara B" en estas intervenciones. Un ejemplo claro es la reacción tras la detención de los tres miembros del grupo *hacktivista* ruso **Noname057(16)** en España, como parte de una operación conjunta de la Guardia Civil, Interpol y Europol. Aunque esta acción debilitó parcialmente sus actividades, el grupo emitió amenazas públicas a través de su canal de **Telegram** y, poco después, lanzó ataques DDoS dirigidos a páginas web de administraciones públicas y servicios críticos en España, causando interrupciones significativas.

Estas represalias evidencian cómo las detenciones pueden, en algunos casos, provocar una escalada de actividades cibercriminales. Esto subraya la importancia de no solo realizar estas operaciones con éxito, sino también preparar defensas cibernéticas robustas para mitigar las posibles consecuencias.



Ilustraciones 1 y 2 | Mensajes del canal de Telegram del grupo NONAME057(16) sobre sus ataques exitosos a webs españolas.




Dark Web Insights

5. *Dark Web Insights*

En la segunda mitad de 2024 se produjeron numerosas actividades en la *Dark Web*, lo que pone de relieve su papel como centro de actividad para los ciberdelincuentes. En total, el ´´**Departamento de Cyber Threat Intelligence de NTT DATA** ha detectado más de **10.352 incidentes en la *Dark Web***, que van desde filtraciones de datos a gran escala hasta la venta de información.

En el transcurso del último semestre del 2024, tras las revelaciones relacionadas con filtraciones de datos (44,59%), se ha identificado que la segunda categoría de publicaciones más recurrente en la *Dark Web*, según el análisis realizado por **NTT DATA**, está compuesta por anuncios relacionados con la venta (41,15%), promoción y distribución de *malware*. Este entorno muestra una constante aparición de nuevas cepas de *malware*, las cuales pueden ser comercializadas a precios fijos, subastadas al mejor postor o distribuidas de forma gratuita como herramientas de código abierto, disponibles para cualquier actor malintencionado.

Adicionalmente, se ha registrado que la tercera categoría más prominente de publicaciones en la *Dark Web*, según **NTT DATA**, se refiere a anuncios de acceso a servicios (12,62%). Este tipo de contenido abarca la venta o el intercambio directo de acceso a sistemas, redes o bases de datos comprometidas, permitiendo su aprovechamiento por otros actores maliciosos. La presencia de tales publicaciones es especialmente alarmante, dado su potencial para intensificar las amenazas cibernéticas y facilitar aún más la ejecución de actividades maliciosas.

A la cola de la lista se encuentran las publicaciones de nuevas asociaciones o cooperación entre actores maliciosos (1,17%), las de compra de información (0,41%) y en las que se difunde el objetivo de ataque (0,06%).

Principales publicaciones en la *Dark Web*

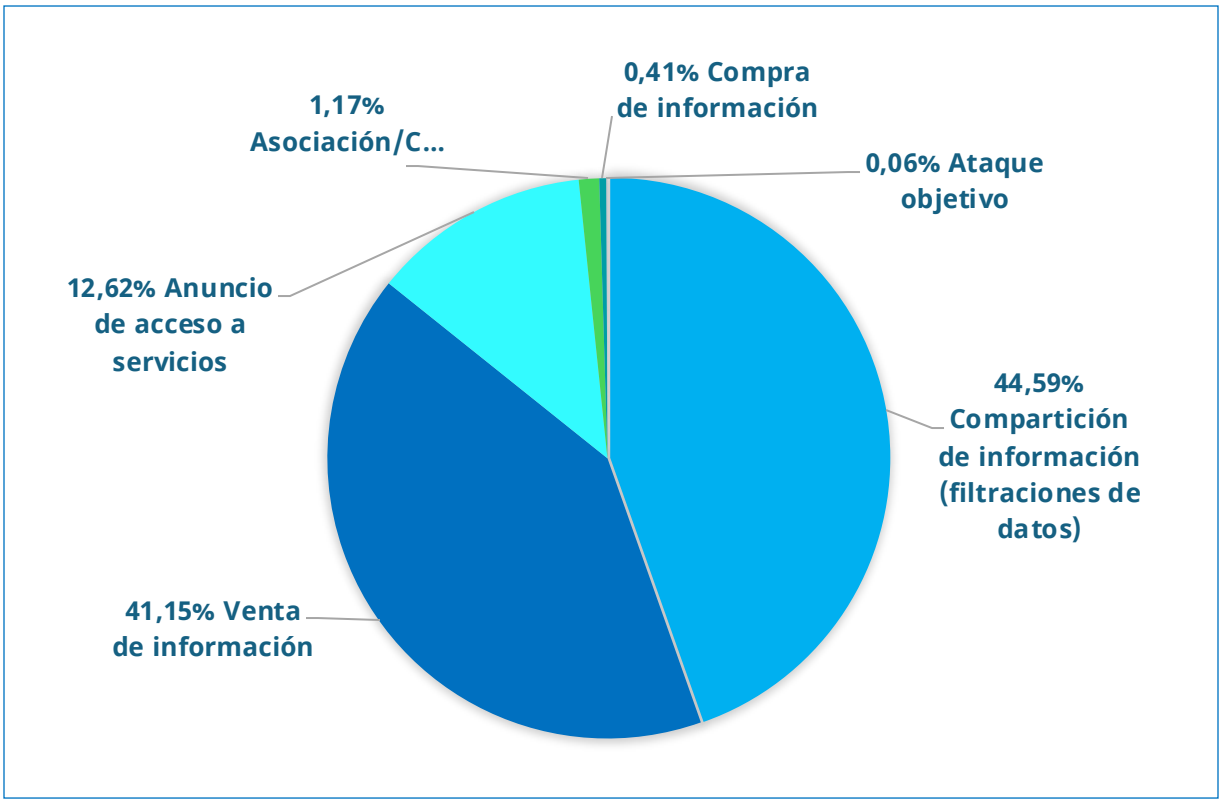


Figura 6 | Categorías principales de publicaciones en la *dark web* en el segundo semestre de 2024.

Durante el semestre que se evalúa, los foros clandestinos han continuado desempeñando un papel crítico como centros de operaciones para ciberdelincuentes, facilitando la compra, venta y coordinación de recursos destinados a ciberataques. En este contexto, ***Breach Forums*** se destacó notablemente, registrando más de 2.000 incidentes asociados. Le siguen ***Exploit Forum***, con 500 incidentes, y ***Xss Forum***, con 300 incidentes.

Estas plataformas no solo proporcionan credenciales de acceso, sino que también ofrecen una variedad de herramientas y servicios necesarios para llevar a cabo ciberataques efectivos. Este entorno ha dado lugar a un mercado floreciente que facilita la ciberdelincuencia de manera coordinada, lo que representa un desafío significativo para la seguridad cibernética.

Plataforma de venta *underground*

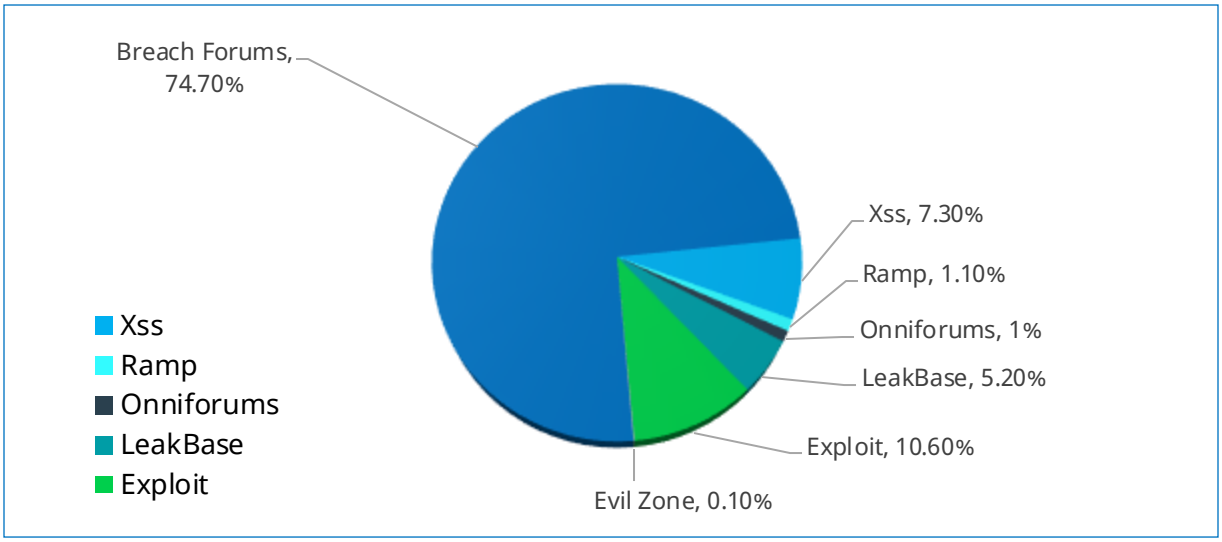


Figura 7 | Principales plataformas de venta *underground* identificadas en el segundo semestre de 2024.

Los actores maliciosos suelen iniciar sus operaciones infiltrándose en los sistemas de proveedores externos, ganando así acceso a la infraestructura y a los datos sensibles de la organización objetivo. Ejemplos notables de esta táctica incluyen filtraciones de datos significativas ocurridas durante el 2024, como el caso en el que los atacantes accedieron a la cuenta en la nube de **Snowflake de Ticketmaster** a través de contratistas externos.

Otro actor malicioso destacado durante este periodo fue **IntelBroker**, que ha utilizado metodologías similares para infiltrarse en importantes entidades corporativas, incluyendo a **Nokia, Ford** y múltiples clientes de **Cisco**, entre los cuales se encuentra **Microsoft**.

Por otro lado, durante 2024 se ha registrado un aumento notable en las actividades cibercriminales en la plataforma **Telegram**. Sin embargo, se proyecta que la comunidad clandestina podría volver a migrar hacia los foros de la *Dark Web*, en parte debido a las estrictas prohibiciones impuestas en **Telegram** por sus administradores. Esta migración proba-blemente intensificará la competencia entre los foros de la *Dark Web*. Para atraer nuevos usuarios y diferenciarse, es posible que los operadores de foros implementen innovaciones como servicios automatizados de custodia, pro-cesos más eficientes para la resolución de disputas y mejoras en seguridad y anonimato, estableciendo un nuevo estándar en el mercado *Underground*.

La vigilancia continua de estos foros es fundamental para que las organizaciones mantengan una postura proactiva frente a las amenazas emergentes. Esta monitorización activa es crucial para la prevención de incidentes antes de que ocurran, fortaleciendo así las estrategias de defensa y mitigación de riesgos en el ámbito cibernético.

Actores Maliciosos *(Threat Actors)*

Actores Maliciosos

(Threat Actors)

Durante 2024, el panorama cibernético ha estado marcado por una compleja red de actores maliciosos que han destacado tanto por el volumen de sus ataques como por sus tácticas innovadoras y su impacto global. Este informe identifica a los principales actores del año, ofreciendo una visión estratégica de sus métodos, motivaciones y ataques recientes para ayudar a las organizaciones a fortalecer sus defensas frente a estas amenazas.

El equipo de **Cyber Threat Intelligence de NTT DATA** analizó incidentes, informes del sector y actividades en la *Dark Web* para identificar a los nuevos grupos maliciosos y los más críticos.

6.1 Nuevos Actores Maliciosos

• Mad Liberator Blog

Mad Liberator Blog es un blog de extorsión de la *Dark Web*, clasificado como un sitio *«name-and-shame»*, operado presuntamente por el grupo **Mad Liberator Ransomware Group**. Reportado por primera vez el 12 de julio de 2024 en fuentes abiertas, el blog ya ha listado nueve víctimas de diversas industrias a nivel global. El sitio, escrito íntegramente en inglés, es accesible únicamente a través del navegador Tor.

Según la información publicada por los actores maliciosos, el grupo está compuesto por *hackers* de diversas partes del mundo y no se identifica como una APT ni como un grupo *hacktivista* con motivaciones políticas. Su estrategia de extorsión es directa: amenazan a las empresas con incluir su nombre en el blog si no responden en un día. Posteriormente, les otorgan un plazo de siete días antes de publicar los archivos robados, y si no se paga el rescate dentro de cinco días, prometen divulgar toda la información de la empresa.

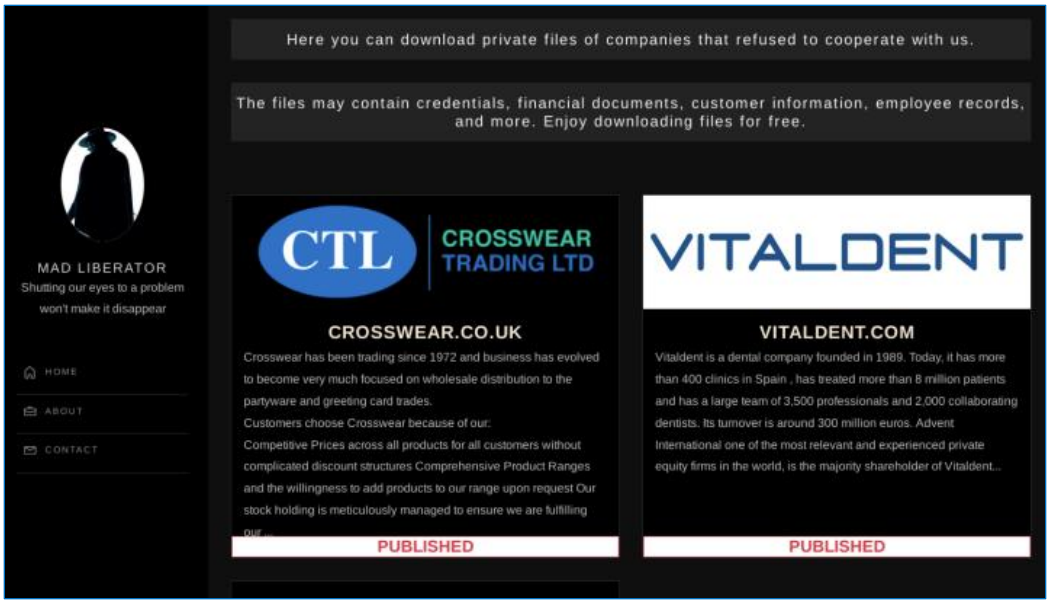


Ilustración 3 | Publicación del blog Mad Liberator.

• Helldown Blog

En agosto de 2024, se lanzó el ***Helldown Blog***, un sitio web de extorsión accesible a través de Tor, presuntamente operado por el grupo malicioso ***Helldown Ransomware Group***. Este blog se convirtió en una herramienta clave para sus actividades de *ransomware*, centradas en la extorsión y publicación de datos robados.

Entre el 5 y el 22 de agosto, el grupo malicioso publicó información de 22 víctimas, distribuidas en países como Estados Unidos, Reino Unido, Polonia, Italia, Austria, Suiza y Líbano. Las empresas afectadas pertenecían a sectores como tecnología de la información (TI), construcción, manufactura, bienes raíces y logística.

Los operadores de *Helldown Ransomware* emplearon **Tox**, una plataforma de comunicación cifrada, para coordinar las negociaciones y gestionar sus actividades ilícitas, subrayando su enfoque sofisticado en la anonimización y la evasión de rastros digitales.

• Valencia Blog

En septiembre de 2024, ***Insikt Group*** observó un nuevo sitio web de extorsión supuestamente operado por ***Valencia Ransomware Group***. El sitio web de extorsión estuvo activo durante un breve periodo de tiempo a finales de septiembre de 2024 y actualmente ya no existe. Los actores maliciosos indicaron en el blog de extorsión su Tox ID como principal método de comunicación.

Antes de desconectarse, el blog de extorsión enumeraba cuatro víctimas:

- **Grupo Cortefiel**: Empresa española que opera en los sectores minorista y textil.
- **Duopharma Biotech**: Una empresa de Malasia que opera en las industrias manufacturera y farmacéutica.
- **Satia Industries Ltd**: Empresa de la India que opera en la industria manufacturera.
- **Globe Pharmaceuticals Ltd**: Una empresa de Bangladesh que opera en el sector sanitario.

El grupo de ransomware utilizó una cuenta de redes sociales ya desaparecida en la plataforma X (@valenciaLeaks72).

• HellCat Blog (HellCat Ransomware)

HellCat Blog es un blog de extorsión de la *Dark Web* escrito en inglés y operado por ***Hellcat Ransomware Group***, que lleva activo desde octubre de 2024. En el momento de escribir este artículo, el blog de extorsión tenía tres víctimas:

- **College of Business Education (cbe[.]ac[.]tz):** Institución de educación superior dedicada a proporcionar educación en negocios, contabilidad, compras y campos relacionados en Tanzania.
- **Ministerio de Educación de Jordania (moe[.]gov[.]jo):** Autoridad gubernamental responsable de supervisar y gestionar el sistema educativo en Jordania.
- **Schneider Electric (se[.]com):** Empresa multinacional con sede en Francia especializada en soluciones de gestión de la energía y automatización.

6.2 Grupos de *ransomware*

Desde el **Departamento de Cyber Threat Intelligence de NTT DATA**, se realizó un análisis exhaustivo de las actividades de *ransomware* en el segundo semestre de 2024, destacando el marcado aumento de estos ataques liderados por grupos como **LockBit** y **RansomHub**. Este análisis también examina los impactos por sectores, como educación, gobierno, y energía mostrando notables aumentos de ataques.

Además, se analiza la evolución de grupos maliciosos clave de *ransomware*, como **Black Basta**, **Play** y amenazas emergentes como **Valencia Ransomware**, y **MAD LIBERATOR**, destacando la creciente complejidad y alcance de las operaciones de *ransomware* a nivel mundial.

A continuación, se presenta una gráfica que muestra los 6 grupos de *ransomware* más activos durante este periodo, ilustrando su distribución y destacando la preeminencia de RansomHub en el panorama de amenazas.

Top grupos de *ransomware*

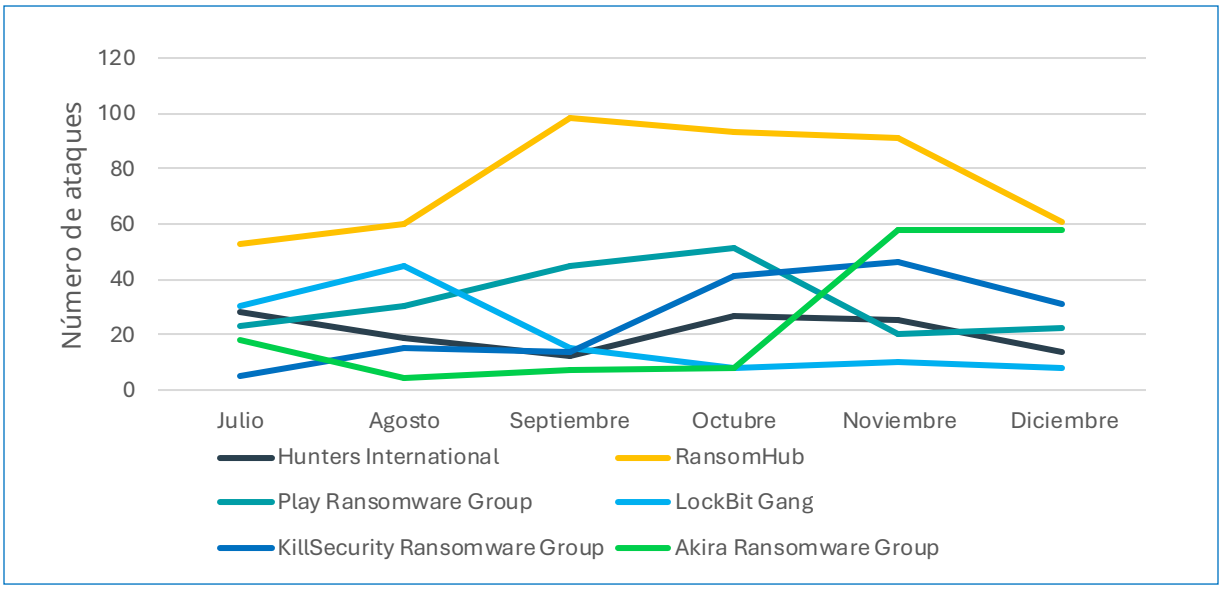


Figura 8 | Actividad del segundo semestre 2024 por parte de los 6 grupos de *ransomware* más activos.

- **RansomHub**

Detectado por primera vez en febrero de 2024, **RansomHub** ha alcanzado rápidamente la prominencia en el panorama del *ransomware*, aprovechando la interrupción de los principales actores como ALPHV y LockBit. Con sus raíces probablemente en Rusia y conexiones con antiguos afiliados de ALPHV, el grupo se ha establecido como una fuerza formidable aprovechando su modelo *Ransomware-as-a-Service* (RaaS), que ofrece atractivas condiciones de *profit-sharing* a los afiliados. Este enfoque ha provocado un aumento de los ataques, especialmente en agosto y septiembre de 2024, cuando se produjeron más de la mitad de sus ataques. Otro dato interesante es que **el recuento de ataques de esos dos meses representa más del 10% de todos los ataques de *ransomware* que hemos analizado este semestre**.

- **PLAY *Ransomware***

El *ransomware* PLAY ha sido responsable de numerosos ataques destructivos contra importantes municipios estadounidenses y ha ejecutado supuestamente más de 560 ataques con éxito desde junio de 2022. Múltiples investigadores han descubierto una variante Linux del *ransomware Play* que solo cifra archivos cuando se ejecuta en un entorno VMWare ESXi, lo que les ayuda a ampliar sus operaciones. Finalmente, Play **ha batido su propio récord de víctimas anuales en 2024 con 364 víctimas totales.**

- **Akira**

Activo desde marzo de 2023, Akira se ha hecho famoso por su adaptabilidad técnica, siendo el tercer mayor contribuyente reivindicando la **autoría de 153 víctimas durante el último semestre del 2024**. Durante los meses de noviembre y diciembre, este grupo alcanzó un pico operativo significativo, registrando un total de víctimas que supera más del triple del promedio mensual habitual. Este incremento no solo subraya el crecimiento de su actividad, sino que también consolida la posición de Akira como uno de los actores de *ransomware* más activos en la actualidad.

Durante los últimos seis meses, los ataques de *ransomware* han afectado a organizaciones en todo el mundo, pero algunos países han sufrido un impacto desproporcionado. **Estados Unidos** encabeza la lista de países más afectados con una diferencia abismal en comparación con otros, consolidándose como el principal objetivo de los actores de *ransomware*.

Esta tendencia puede atribuirse a la alta concentración de empresas tecnológicamente avanzadas, infraestructuras críticas y sistemas con datos altamente valiosos que atraen a los ciberdelincuentes. En la siguiente gráfica, se muestra la distribución de los países más afectados por este tipo de ataque durante el segundo semestre de 2024:

Países más afectados por *ransomware* de Julio a Diciembre 2024.

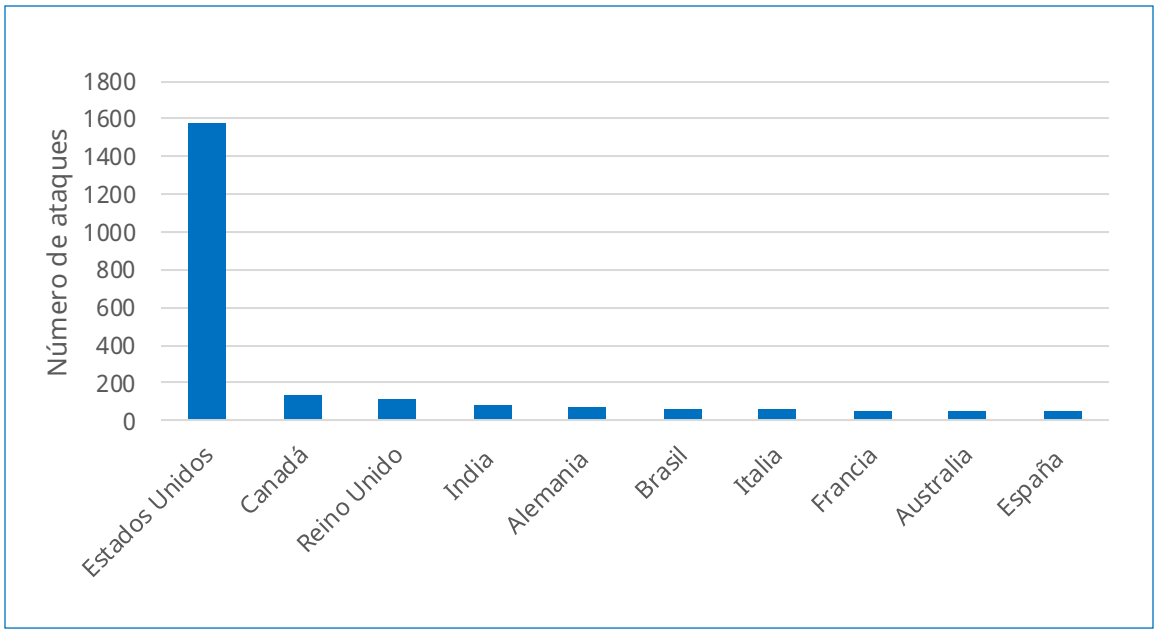


Figura 9 | Países más afectados por *ransomware* en el segundo semestre de 2024.

En el análisis de los sectores más afectados por ataques de *ransomware* durante los últimos seis meses, el **sector de manufactura se posiciona como el principal objetivo de los ciberdelincuentes**. Este sector ha experimentado un volumen significativamente mayor de ataques en comparación con otros, lo que refleja su vulnerabilidad debido a la alta dependencia de sistemas operativos críticos y la posible interrupción en cadenas de suministro globales.

Los actores de *ransomware* parecen priorizar este sector debido al impacto financiero y operativo que pueden generar sus ataques, lo que aumenta la presión sobre las organizaciones para cumplir con sus demandas. La siguiente gráfica ilustra los sectores más afectados, destacando la prominencia del sector de manufactura en este periodo:

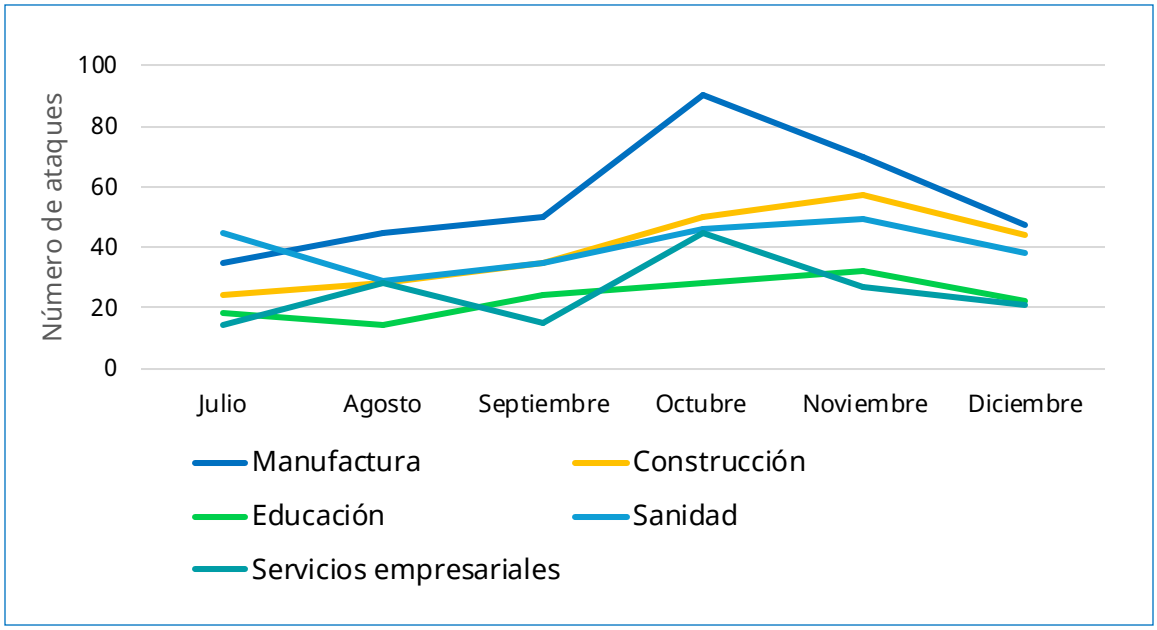


Figura 10 | Sectores más afectados por *ransomware* en el segundo semestre de 2024.

6.3 Hacktivistas

En el último semestre del 2024, los grupos *hacktivistas* siguieron influyendo en los acontecimientos mundiales, siendo motivados por agendas políticas, sociales e ideológicas. Estos grupos desplegaron diversas tácticas, como ataques de denegación de servicio distribuido (DDoS), desfiguración de sitios web (*defacement)* y violación de datos, para impulsar sus causas. A medida que seguimos de cerca este fenómeno, está claro que el *hacktivismo* va en aumento, alimentado por la creciente polarización política. Entre los grupos más destacados se encuentran:

- **NoName057(16);**

Este grupo, es un grupo de amenazas, presuntamente con base en Rusia, especializado en ataques de **DDoS**, *defacement* y filtración de datos. En agosto de 2024, **NoName057(16)** lanzó la operación **#OP404**, una campaña que comenzó en agosto con el objetivo de interrumpir el acceso a sitios web de gobiernos y medios en Ucrania y en países aliados, incluidos miembros de la OTAN. Los ataques, centrados en generar el error «404 página no encontrada», reflejan el propósito simbólico de desconectar y desestabilizar estos sitios web.

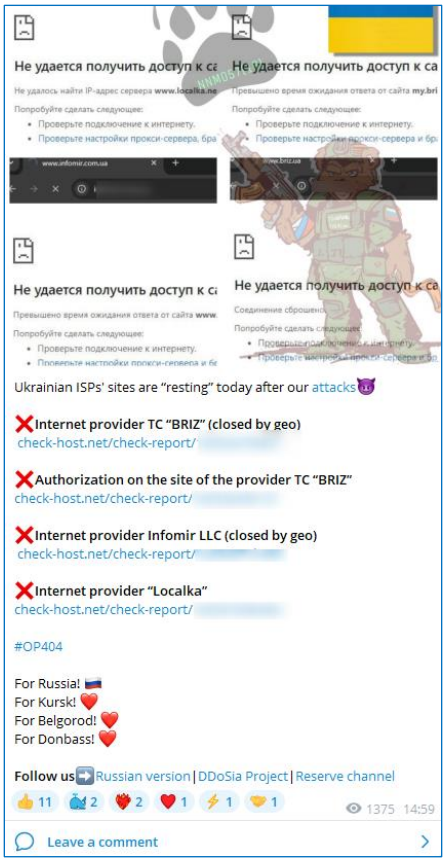


Ilustración 4 | Publicación en Telegram del grupo noname057(16).

- **Cyber Army of Russia Reborn**

Ha resurgido en 2024 como un actor clave en el ámbito del *cibeRhacktivismo*, impulsado por fuertes motivos nacionalistas. En julio de 2024, el grupo participó activamente en la campaña ***#OpSpain,*** siendo esta una cibercampaña lanzada por grupos *hacktivistas* prorrusos, contra sitios web y medios de comunicación del Gobierno Español. La operación incluye ataques DDoS y *defacements*, con el objetivo de interrumpir servicios y difundir propaganda prorrusa. La campaña es una represalia contra el apoyo de España a Ucrania y su alineación estratégica con la OTAN.

- **Indian Cyber Force**

Este grupo *hacktivista* indio, colabora con otros equipos pro-India como **TeamUCC**, **Team-Network-Nine** y **BlackDragonSec**. Es un grupo pro-Israel, conocido por reivindicar ciberataques a infraestructuras críticas en múltiples naciones, incluyendo Bangladesh, China, Pakistán e Indonesia. En agosto del 2024, el grupo ha lanzado recientemente ciberataques en Bangladesh, publicando vídeos en los que afirma haber pirateado el panel de control de la red de **Grameenphone Telecom** y otros proveedores de servicios de Internet, así como el sistema nacional de correo electrónico del Gobierno de Bangladesh.

- **UserSec**

Es un grupo prorruso conocido por llevar a cabo ataques de denegación de servicio distribuidos (DDoS) y publicar filtraciones de datos, dirigidos principalmente a entidades que apoyan a Ucrania. Tras la detención del CEO de Telegram, Pavel Durov, varios grupos prorrusos, entre ellos UserSec, lanzaron ataques contra entidades francesas bajo el hashtag de campaña *#FreeDurov*. En una reciente operación conjunta, UserSec y el **Ciberejército de Rusia Renacida** lograron inhabilitar los sitios web de la Audiencia Nacional de Francia y del Tribunal de París.

6.4 APT

- **APT iraníes**

Las **APT iraníes** ampliaron su alcance regional durante este semestre, con grupos como **MuddyWater** y **APT34** desplegando *malware* personalizado, como **BugSleep**, y aplicando tácticas avanzadas de ingeniería social. Estas campañas se dirigieron principalmente a gobiernos e infraestructuras críticas en todo Oriente Próximo, con **Israel** como principal objetivo, evidenciando una intensificación significativa en sus actividades de espionaje.

- **APT rusas**

Por su parte, las **APT rusas** aprovecharon vulnerabilidades de día cero para llevar a cabo ataques estratégicos. Grupos como ***APT29*** y ***APT28*** se enfocaron en vulnerabilidades de iOS y Chrome, empleando técnicas *de* ***watering hole*** y *malware* modular para infiltrarse en redes diplomáticas y gubernamentales, fortaleciendo así sus capacidades de espionaje. En **Ucrania**, los grupos alineados con Rusia mantuvieron una alta actividad, atacando entidades gubernamentales, el sector de defensa y servicios esenciales como energía, agua y calefacción.

- **APT chinas**

Las **APT chinas** adoptaron un enfoque renovado hacia infraestructuras de red críticas. Grupos como ***APT41*** y **Earth Baku** utilizaron *malware* avanzado, como **ShadowPad** y **VELVETSHELL**, para comprometer dispositivos de red, incluidos conmutadores Nexus de Cisco, afectando de manera notable la seguridad de estas infraestructuras.

- **APT norcoreanas**

Finalmente, las **APT norcoreanas** intensificaron sus esfuerzos de ciberespionaje, con grupos como **Kimsuky** y **Lazarus Group** atacando al sector educativo. Sus campañas se enfocaron en investigadores y académicos relacionados con la península de Corea y el sudeste asiático, utilizando técnicas de ***spear-phishing*** y *malware* avanzado, como **MoonPeak** y **FPSpy**, para lograr sus objetivos.

Tácticas, Técnicas y Procedimientos (TTPs)

7. Tácticas, Técnicas y Procedimientos

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

A continuación, se abordarán las TTPs destacados del segundo semestre de 2024 basadas en las tendencias identificadas.

7.1 Descripción de las TTP más comunes utilizadas por los cibercriminales

En el segundo semestre de 2024, los cibercriminales han demostrado una notable evolución en sus TTPs, adaptándose continua-mente a los nuevos entornos tecnológicos y a las medidas defensivas implementadas.

Este apartado presenta un resumen de las TTPs más utilizadas durante este periodo, analizando su relación con el marco MITRE ATT&CK, y proporcionando tanto una visión general de su impacto como recomendaciones clave para su mitigación.

Figura 11 | Evolución de las técnicas más comunes utilizadas durante 2024.

Técnica	MITRE ATT&CK ID	Descripción	Mitigaciones	Referencias
Phishing	T1078 - Cuentas válidas	Obtención de credenciales mediante phishing, utilizadas para acceso inicial o persistencia.	- Implementar MFA en todas las cuentas. - Sensibilizar a los empleados para identificar correos maliciosos.	T1078
	T1059 - Intérprete de comandos y scripts	Uso de comandos maliciosos tras comprometer cuentas para ejecutar cargas útiles o scripts.	- Habilitar reglas de reducción de superficie de ataque. - Limitar la ejecución de scripts no firmados.	T1059
Exploits de Vulnerabilidades	T1583 - Adquisición de infraestructura	Preparación de servidores y redes bot para lanzar ataques DDoS o explotar vulnerabilidades en sistemas críticos.	- Monitorizar actividades inusuales en la red. - Implementar soluciones DDoS en servicios críticos.	T1583
	T1547 - Ejecución de arranque o inicio automático	Persistencia en sistemas comprometidos mediante configuraciones que se ejecutan automáticamente al iniciar el sistema.	- Monitorizar cambios en programas de inicio. - Limitar privilegios administrativos.	T1547
Ransomware	T1547 - Ejecución de arranque o inicio automático	Uso de configuraciones automáticas para persistencia tras infectar el sistema.	- Limitar permisos administrativos. - Auditar los programas configurados para ejecutarse durante el arranque.	T1547
	T1078 - Cuentas válidas	Utilización de credenciales comprometidas para mover ransomware dentro de la red.	- Cambiar contraseñas predeterminadas. - Auditar cuentas regularmente para detectar actividades anómalas.	T1078

Tabla 5 | TTP más comunes durante el segundo semestre de 2024.

El segundo semestre de 2024 se caracterizó por la sofisticación y escalabilidad de las TTPs utilizadas por los cibercriminales, que han priorizado técnicas de acceso inicial y persistencia para maximizar su impacto. La relación con el marco MITRE ATT&CK no solo permite comprender estas amenazas, sino que también proporciona un enfoque práctico para mitigarlas.

7.2 Vectores de entrada más usuales

Ahora bien, para poder acceder a los sistemas y llevar a cabo los ataques, los actores maliciosos utilizan una amplia variedad de vectores de entrada o acceso inicial. Siguiendo el hilo de las técnicas más usadas este semestre, y teniendo en cuenta que el *ransomware* se ha posicionado como la amenaza principal, las tendencias de los vectores de entrada más comunes se resumen de la siguiente manera:

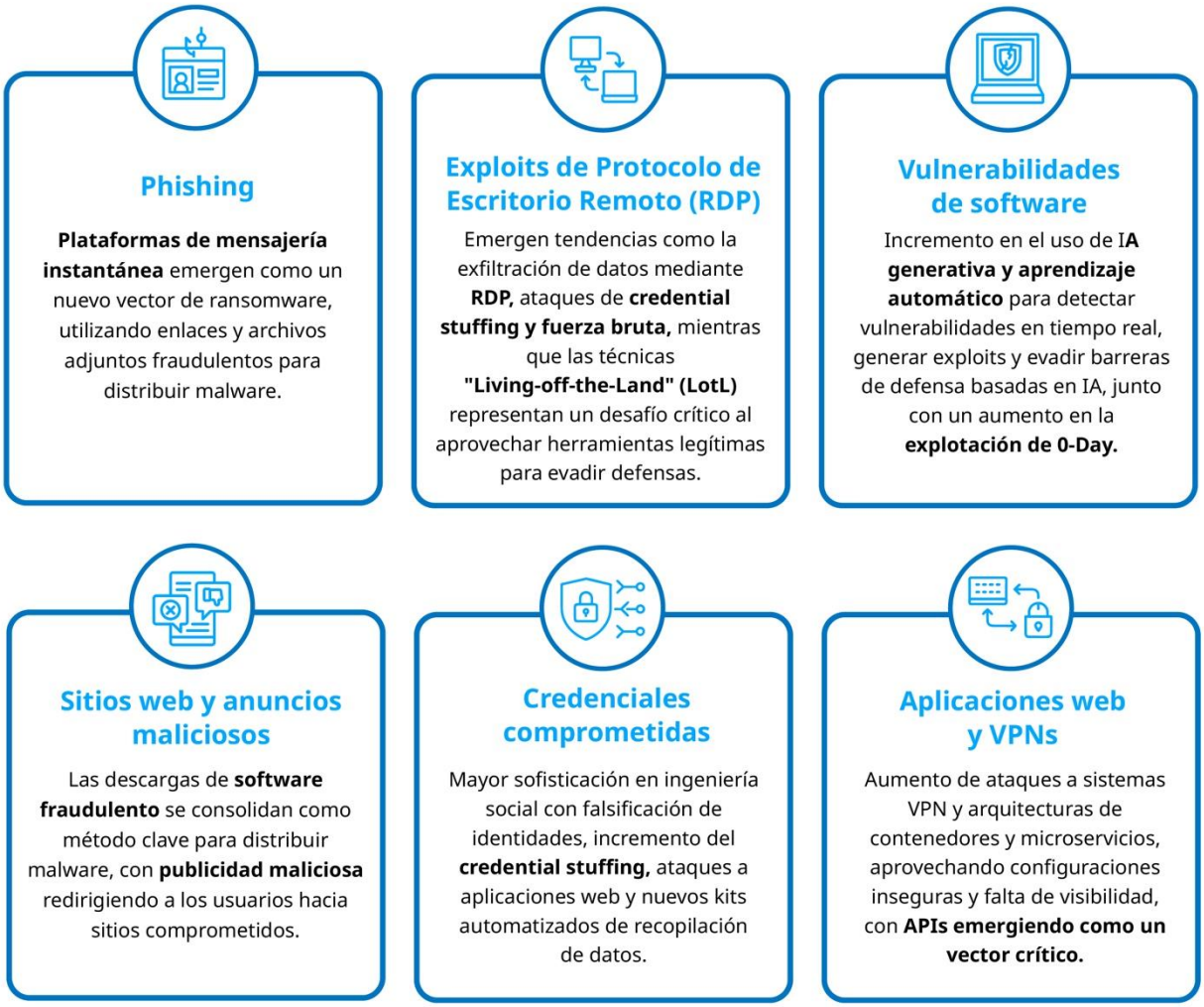


Tabla 6 | Vectores de entrada más usuales empleados en el segundo semestre de 2024.

7.3 Innovación en ataques: Nuevas técnicas y tácticas desconocidas

• Blast Radius

Descripción: Vulnerabilidad que explota el protocolo **RADIUS** (*Remote Authentication Dial In User Service*) con **MITM (*Man in the middle*)** y un ataque de **colisión**, para comprometer un dispositivo inicial falsificando una respuesta válida tras una autenticación fallida, sin necesidad de conocer las credenciales de usuario. La falta de autenticación y cifrado en el protocolo facilita el acceso no autorizado y la exposición de datos sensibles (Ars Technica, 2024; Blast-RADIUS, 2024).

Impacto: Afecta a todas las implementaciones RADIUS que utilizan métodos de autenticación no EAP sobre UDP.

Mitigaciones/Recomendaciones:

- Realizar auditorías de red para identificar dispositivos en uso.
- Actualizar los protocolos obsoletos e inseguros.
- Implementar segmentación de redes para limitar el movimiento lateral.
- Establecer un monitoreo continuo para detectar actividad sospechosa.
- Capacitar a empleados en ciberseguridad.

Este ataque subraya la importancia de modernizar las infraestructuras de red y adoptar medidas proactivas para minimizar riesgos.

• RustyAttr

Descripción: El grupo Lazarus (Corea del Norte) ha desarrollado ***RustyAttr***, un troyano para macOS que utiliza atributos extendidos para ocultar código malicioso y eludir antivirus. Empleando el marco **Tauri**, oculta *scripts* maliciosos en archivos que simulan ser documentos legítimos, como PDFs. Esta técnica no tiene precedentes en el marco MITRE ATT&CK, marcando un avance en evasión de seguridad (The Hacker News, 2024).

Impacto: *RustyAttr* representa un riesgo elevado para organizaciones que dependen de medidas tradicionales de seguridad en macOS, como Gatekeeper, comprometiendo sistemas con técnicas de camuflaje innovadoras.

Mitigaciones/Recomendaciones:

- Mantener políticas estrictas de Gatekeeper para bloquear aplicaciones no autorizadas.
- Realizar auditorías regulares del estado de seguridad de macOS.
- Establecer un monitoreo continuo para detectar actividad sospechosa.
- Formar al personal en identificación de tácticas de ingeniería social.

• *Quishing* - Suplantación de identidad mediante código QR

Descripción: Utiliza **códigos QR como vector de ataque**, redirigiendo a los usuarios a sitios maliciosos tras el escaneo. Estos sitios pueden instalar *malware*, robar credenciales u ofrecer contenido fraudulento. La técnica explota la confianza y familiaridad que los usuarios tienen con los códigos QR, evadiendo las defensas cibernéticas convencionales (ITWeb, 2024).

Impacto: Este método puede comprometer cualquier dispositivo con el que se lea el código QR, infectándolo con *malware*, robando información personal o propagando ataques en redes organizacionales. El impacto social recae en la confianza del usuario sobre la tecnología QR.

Mitigaciones/Recomendaciones:

- Implementar herramientas de navegación segura y detección de *malware* para verificar URLs antes del acceso.
- Configurar controles de red para bloquear sitios no autorizados o sospechosos.
- Capacitar a usuarios y empleados sobre los riesgos de los códigos QR y cómo identificar enlaces fraudulentos.
- Promover prácticas de verificación segura al escanear códigos QR.

• RDPWrap y Tailscale

Descripción: La combinación de **RDPWrap**, que habilita múltiples sesiones RDP en Windows, y **Tailscale**, una herramienta de red privada, permite a los atacantes establecer accesos remotos encubiertos a sistemas infectados. Estos accesos han sido utilizados para manipular y robar criptomonedas u otros activos digitales, así como exfiltrar información sensibles, sin modificar visiblemente el sistema (The Cyber Express, 2024).

Impacto: Este ataque afecta principalmente a usuarios del mercado de criptomonedas, comprometiendo la confidencialidad, integridad y disponibilidad de sus cuentas digitales. Los atacantes pueden acceder de manera no autorizada a sistemas Windows 10 y Windows Server que soportan RDPWrap, y a *routers*, *firewalls* y dispositivos IoT presentes durante la comunicación.

Mitigaciones/Recomendaciones:

- Restringir el uso de RDP y deshabilitarlo en sistemas donde no sea necesario.
- Implementar autenticación multifactor (MFA) para proteger accesos remotos.
- Usar herramientas de monitoreo para registrar y alertar sobre accesos inusuales.
- Realizar revisiones periódicas de registros de acceso para detectar intrusiones.
- Mantener sistemas actualizados con parches y políticas de control de acceso que limiten conexiones entrantes innecesarias.
- Capacitar a empleados sobre los riesgos de herramientas como RDPWrap y el uso de *software* no autorizado.

• OtterCookie

Descripción: *OtterCookie* es un ataque basado en ***credential stuffing*** (uso de credenciales filtradas de otras plataformas) sobre aplicaciones web con seguridad débil que automatiza el **envío masivo** de combinaciones de usuario y contraseña para acceder a cuentas vulnerables. Está diseñado en **JavaScript** para ejecutar cargas útiles adicionales, incluyendo exfiltración de datos, acceso a credenciales, y la implementación de *spam* a través de servicios SMTP o kits de *phishing* (Bleeping Computer, 2024; The Hacker News, 2024) .

Impacto: Este ataque afecta principalmente a sistemas en Japón y Corea del Norte, comprometiendo la confidencialidad, integridad y disponibilidad de las cuentas y datos. Además, los accesos obtenidos pueden ser utilizados para desplegar *ransomware*, realizar suplantaciones de identidad o comprometer la red interna de las organizaciones.

Mitigaciones/Recomendaciones:

- Implementar autenticación multifactor (MFA) en todas las cuentas críticas.
- Obligar el uso de contraseñas fuertes y únicas, fomentando prácticas como el uso de gestores de contraseñas.
- Monitorizar intentos de acceso fallidos y establecer alertas para múltiples fallos consecutivos.
- Realizar auditorías regulares en aplicaciones web y reforzar su seguridad.
- Capacitar a los usuarios para evitar la reutilización de contraseñas y detectar intentos de *phishing*.

• Nueva plataforma Raas de KillSec

Descripción: El grupo *hacktivista* ***KillSecurity*** ha lanzado una nueva plataforma de *ransomware* como servicio (**RaaS**) disponible a través de Telegram y accesible mediante Tor. Desarrollada en **C++,** permite a los atacantes personalizar *ransomware*, rastrear estadísticas de campañas y comunicarse con las víctimas a través de chat. Próximas funciones incluirán ataques **DDoS**, llamadas automáticas para presionar el pago de rescates, y herramientas de exfiltración de datos (RedHotCyber, 2024).

Impacto: Afecta tanto a usuarios individuales como a organizaciones. Compromete cuentas personales y empresariales, expone datos sensibles y provoca pérdidas financieras significativas por robo de activos y la interrupción operativa.

Mitigaciones/Recomendaciones:

- Realizar programas de formación continua para empleados, incluyendo simulaciones de ataques de *phishing* y tácticas de ingeniería social.
- Implementar autenticación multifactor (MFA) para proteger el acceso a sistemas críticos.
- Revisar y fortalecer las políticas de seguridad informática.
- Desplegar soluciones de monitoreo en tiempo real que detecten intentos de acceso desde ubicaciones desconocidas o patrones de descarga inusuales.

Tendencias de vulnerabilidades

8. Vulnerabilidades

El segundo semestre de 2024 ha puesto de relieve la amenaza persistente y cambiante de las **vulnerabilidades críticas** en los sistemas de *software* y *hardware*. Estas vulnerabilidades, a menudo explotadas por actores maliciosos, plantean riesgos significativos para organizaciones de diversos sectores. Pueden provocar filtraciones de datos críticos, pérdida de datos confidenciales e interrupción de servicios esenciales.

Para priorizar y abordar eficazmente estas vulnerabilidades, es crucial evaluar no sólo su gravedad técnica, sino también su posible impacto en el mundo real, por ello a continuación se analiza cómo evolucionaron las vulnerabilidades críticas mes a mes durante el segundo semestre de 2024.

• Julio

En julio de 2024, se identificaron **104 vulnerabilidades**, de las cuales **28 son de severidad crítica** y **10 fueron explotadas activamente**. Estas vulnerabilidades destacaron por su impacto en plataformas críticas utilizadas en entornos empresariales y por su capacidad para comprometer datos confidenciales y flujos de trabajo esenciales.

Vulnerabilidades clave destacadas:

- **ServiceNow (CVE-2024-4879 y CVE-2024-5217):** Permitieron el acceso no autorizado a datos críticos y la exfiltración de información sensible mediante la explotación de flujos de trabajo en esta plataforma basada en la nube.

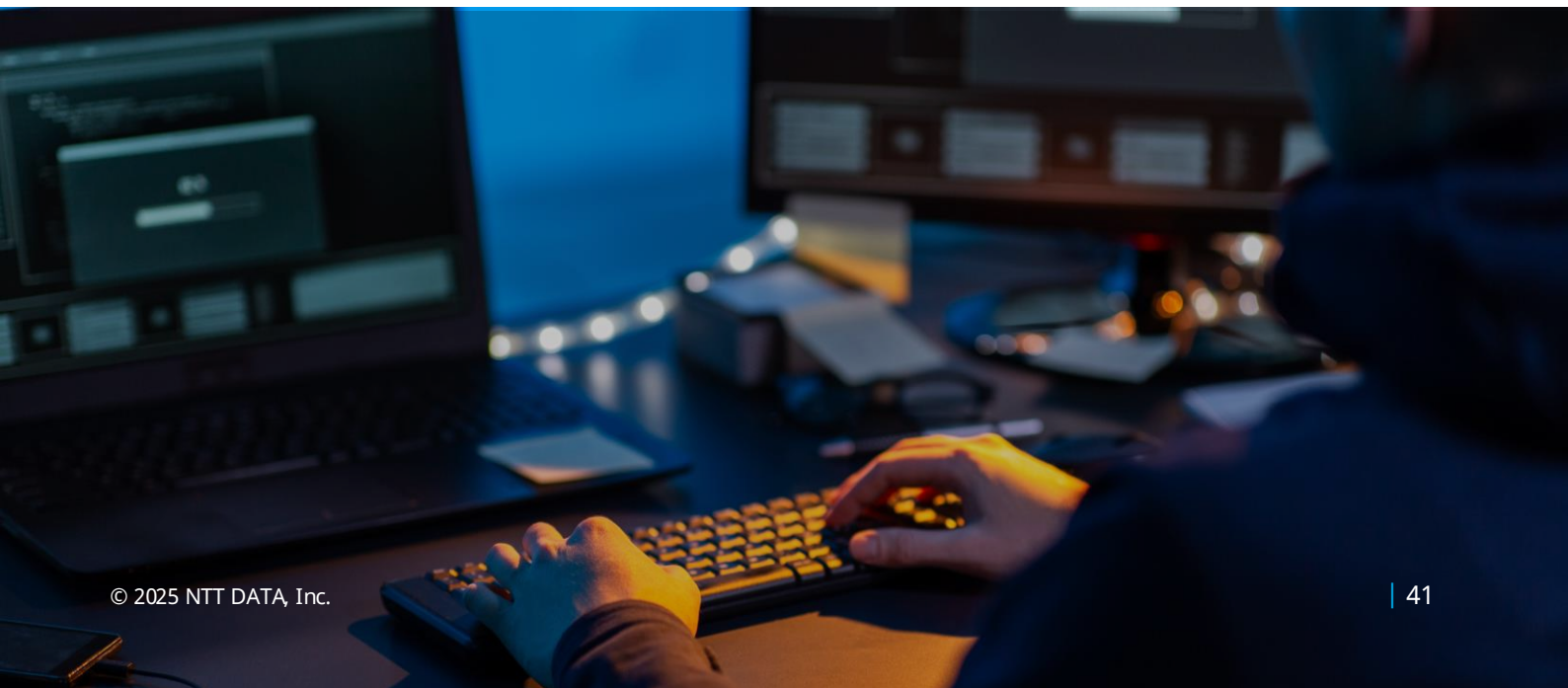
- **OpenSSH (CVE-2024-6387 - "regreSSHion"):** Una vulnerabilidad grave en el protocolo Secure Shell (SSH) que permitía la ejecución de código arbitrario como *root*, afectando a más de 200 productos.

- **GeoServer (CVE-2024-36401):** Vulnerabilidad en la evaluación de nombres de propiedades como expresiones XPath, que permitió a los atacantes ejecutar comandos arbitrarios en sistemas desactualizados.

Impactos principales:

- Acceso no autorizado a infraestructuras críticas y datos confidenciales.
- Compromiso de redes seguras mediante la ejecución de código arbitrario.
- Riesgos significativos en plataformas de gestión de datos geoespaciales.

La actividad de este mes refuerza la necesidad de una gestión proactiva de parches, especialmente en plataformas críticas como **ServiceNow** y **OpenSSH**. También destaca la importancia de auditorías de seguridad regulares para mitigar riesgos asociados con vulnerabilidades conocidas.



• Agosto

En agosto de 2024, se identificaron **118 vulnerabilidades**, de las cuales **20 son de severidad crítica** y **19 fueron explotadas activamente**, marcando un aumento significativo en comparación con el mes anterior. Estas vulnerabilidades fueron dirigidas principalmente a plataformas amplias y de uso generalizado.

Vulnerabilidades clave destacadas:

- **Windows SmartScreen (CVE-2024-38213 - "Copy2Pwn"):** Permite a los atacantes eludir protecciones mediante recursos compartidos WebDAV maliciosos. Fue vinculada a operadores de *malware* como DarkGate.
- **Microsoft Project y Windows Kernel (CVE-2024-38107, CVE-2024-38189):** Estas vulnerabilidades críticas facilitaron la elevación de privilegios y la ejecución remota de código.
- **Google Chrome (CVE-2024-7965):** Un fallo en el motor V8 que permitió corrupción de *heap*, explotado activamente en navegadores.
- **SolarWinds Web Help Desk (CVE-2024-28986):** Una vulnerabilidad de deserialización de Java, explotada rápidamente tras su revelación.

Impactos principales:

- Elevación de privilegios en sistemas operativos y navegadores web.
- Riesgos elevados en navegadores y herramientas de colaboración ampliamente utilizadas.
- Explotación dirigida al sector de criptodivisas por grupos como Citrine Sleet.

• Septiembre

En septiembre de 2024, se identificaron **96 vulnerabilidades**, de las cuales **24 son de severidad crítica** y **9 fueron explotadas activamente**. Este mes destacó por el predominio de vulnerabilidades en productos de Microsoft, reflejando su ubicuidad en entornos empresariales y personales.

Vulnerabilidades clave destacadas:

- **CVE-2024-38226 (Microsoft Publisher):** Utilizada para eludir controles de seguridad y facilitar ataques de ingeniería social.
- **CVE-2024-38217 (Windows Mark-of-the-Web):** Permitió la ejecución de archivos maliciosos al eludir funciones de seguridad.
- **Ivanti (CVE-2024-819) y Veeam (CVE-2024-40711):** Escalaron privilegios y eludieron funciones de seguridad para distribuir *malware*.

Impactos principales:

- Ataques de ingeniería social que dependieron de la interacción del usuario.
- Distribución de *malware* mediante productos clave de gestión empresarial.
- Riesgo elevado debido a días cero explotados activamente.

• Octubre

Octubre marcó un pico en el número de vulnerabilidades, con **153 identificadas**, de las cuales **13 son de severidad crítica** y **7 fueron explotadas activamente**. La gran diversidad de productos afectados en este mes subraya la necesidad de estrategias de defensa más amplias y una colaboración efectiva entre equipos de seguridad.

Vulnerabilidades clave destacadas:

- Diversidad de productos afectados: Microsoft Windows, Zimbra, Mozilla Firefox, Qualcomm, Samsung Exynos, Cisco, Ivanti, ScienceLogic y Grafana.
- **Microsoft Windows Kernel (CVE-2024-43640):** Explotada activamente para la elevación de privilegios.
- **Zimbra y Mozilla Firefox:** Vulnerabilidades críticas que comprometieron datos y accesos en herramientas ampliamente utilizadas.

Impactos principales:

- Diversificación de objetivos para maximizar el impacto de los ataques.
- Riesgos elevados en dispositivos móviles, herramientas de colaboración y navegadores.
- Mayor exposición debido a la publicación de *exploits* de prueba de concepto (PoC).

• Noviembre

En noviembre de 2024, identificaron **98 vulnerabilidades**, de las cuales **16 son de severidad crítica** y **12 fueron explotadas activamente.** La actividad de noviembre refuerza la necesidad de proteger sistemas móviles y plataformas empresariales críticas mediante parches oportunos y monitoreo constante.

Vulnerabilidades clave destacadas:

- **Oracle Agile Product Lifecycle Management (CVE-2024-21287):** Explotada para comprometer plataformas de productividad empresarial.
- **Apple iOS y GeoVision GVLX Mobile Video Recorder (CVE-2024-11120):** Ataques dirigidos a sistemas móviles y dispositivos de seguridad física.
- **Needrestart (Linux):** Una utilidad para gestionar procesos, comprometida para la elevación de privilegios.

Impactos principales:

- Ejecución de código arbitrario y accesos remotos.
- Afectación de infraestructuras críticas y dispositivos móviles.
- Riesgo elevado en *software* de gestión empresarial y SCADA.

• Diciembre

Diciembre cerró el año con un aumento significativo, alcanzando **65 vulnerabilidades de alto riesgo**, de las cuales **6 son de severidad crítica** y **7 fueron explotadas activamente**. De estas vulnerabilidades críticas, destacaron la actividad en plataformas de transferencia de archivos y sistemas operativos. El aumento en vulnerabilidades críticas durante diciembre subraya la importancia de estrategias de ciberseguridad sólidas para mitigar riesgos durante periodos de alta actividad maliciosa.

Vulnerabilidades clave destacadas:

- **CVE-2024-50623 y CVE-2024-55956 (Cleo MFT):** Explotadas por el grupo CL0P, afectando productos de transferencia de archivos.
- **CVE-2024-49138 (Microsoft Windows Common Log File System Driver):** Vulnerabilidad de día cero que permitió desbordamiento de búfer.

Impactos principales:

- Explotación de días cero en sistemas clave.
- Riesgos elevados en productos ampliamente utilizados para transferencia de datos.
- Incremento de vulnerabilidades críticas no explotadas pero con PoC publicados.

Tendencias

Tras analizar las vulnerabilidades del segundo semestre de 2024, se observa una evolución mensual que destaca tanto **el volumen de fallos críticos como su explotación activa**. Los atacantes han demostrado una creciente capacidad para **aprovechar vulnerabilidades de alto impacto**, especialmente **días cero**, antes de que se apliquen los parches correspondientes.

En julio y agosto, aunque el volumen de vulnerabilidades fue moderado, un alto porcentaje fue explotado activamente, reflejando el enfoque en sistemas desactualizados y sectores clave. A partir de septiembre, el número de vulnerabilidades aumentó significativamente, alcanzando su punto máximo en octubre, lo que ofreció más oportunidades a los atacantes para explotar fallos no parcheados.

En noviembre y diciembre, se observó un incremento en la explotación de días cero, evidenciando un cambio táctico hacia vulnerabilidades recién descubiertas.

Países más afectados por *ransomware* de julio a diciembre (Julio / Diciembre 2024)

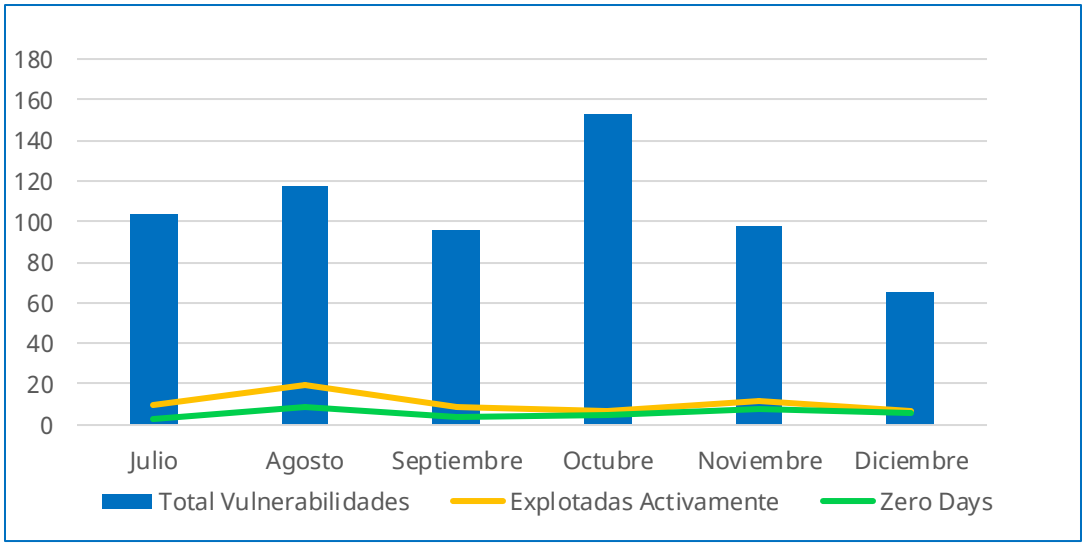


Figura 12 | Comparativa mensual de vulnerabilidades críticas identificadas, vulnerabilidades explotadas activamente y días cero durante el segundo semestre de 2024.

La evolución mensual de las vulnerabilidades durante el semestre refleja la necesidad de reforzar la gestión de parches, mejorar la colaboración entre equipos de seguridad y priorizar la educación en ingeniería social para mitigar los riesgos derivados de estas amenazas en constante evolución.

Perspectiva futura

9. ¿Qué nos espera en 2025?

Los grupos de amenazas analizados en este informe no desaparecerán en el corto plazo y, con alta probabilidad, continuarán representando riesgos significativos durante el mediano plazo (6-12 meses).

El grupo de *ransomware* **RansomHub** consolidó su posición como el grupo más activo durante el 2024, especialmente tras la baja actividad de **Lockbit** y **ALPHV,** y se presume que su actividad continuará siendo destacada gracias a su propagación a través del modelo de *ransomware* como servicio (RaaS), a sus capacidades técnicas avanzadas para lograr el control remoto de dispositivos y evadir la detección de los sistemas de monitoreo.

La actividad en la *Dark Web*, el robo y la exfiltración de datos confidenciales ha sido, y continuará siendo, uno de los principales peligros en el ámbito digital. El actor de amenazas **IntelBroker** ha robado y publicado varias filtraciones de alto perfil a más de 400 de las empresas más grandes e importantes de la industria tecnológica en el mundo en los últimos meses, aunque el impacto total de estas filtraciones aún está desarrollándose. Por todo ello, se prevé que los ataques a la cadena de suministro, aumenten en frecuencia y complejidad. Al centrarse en socios menos seguros, estos ataques aprovechan la interconexión de las empresas para obtener acceso a redes más seguras. Se prevé que los daños cibernéticos a escala mundial alcancen los 10 billones de dólares en 2025, y que la mayor parte de ellos procedan de robos de identidad utilizados para pedir rescates a empresas y particulares.

Por otro lado, durante el 2025 se estará monitorizando la actividad de "los cuatro grandes" (Rusia, China, Irán y Corea del Norte), que perseguirán sus respectivos objetivos geopolíticos mediante operaciones de ciberespionaje, interrupción e influencia.

Los rápidos avances tecnológicos, especialmente en temas de **Inteligencia Artificial**, están reconfigurando las tácticas de defensores y adversarios. Aunque su uso está aportando rápidamente nuevas herramientas para la detección y respuesta a las amenazas, también proporciona a los actores maliciosos potentes capacidades para la ingeniería social, la desinformación y otros ataques.

Se espera que en 2025 se produzca un aumento significativo en los tiempos de aplicación de parches y mitigación de vulnerabilidades, impulsado por la creciente complejidad de los sistemas de IT y OT y la prevalencia de dispositivos de IoT sin soporte. Múltiples hallazgos de 2024 revelan que las organizaciones tardan un promedio de 97 días en abordar vulnerabilidades críticas y 146 días para las de bajo impacto, muy por encima de las recomendaciones de mejores prácticas de 7 a 30 días. Estos retrasos exponen a las organizaciones a períodos de riesgo prolongados, lo que permite a los atacantes explotar vulnerabilidades conocidas.

Mantenerse proactivo y flexible es crucial. Al monitorizar continuamente los cambios en las tácticas, técnicas y procedimientos (TTPs), los equipos de seguridad pueden anticiparse a los ataques y adaptar sus defensas en consecuencia. Implementar respuestas automatizadas a incidentes puede mejorar la remediación al contener automáticamente las amenazas tras su detección, aislar *hosts*, bloquear IoCs sospechosos, terminar sesiones y rotar credenciales de usuario.

Alinear la inteligencia de amenazas con un modelo de amenazas específico asegura que las amenazas más pertinentes sean priorizadas y mitigadas de manera efectiva. Este enfoque vigilante y adaptativo ayuda a proteger contra riesgos emergentes y mantiene la integridad de los sistemas y datos críticos.

Referencias

- Infosecurity Magazine. (s.f.). Operation Cronos: LockBit Takedown. Recuperado de: https://www.infosecurity-magazine.com/news/operation-cronos-lockbit-takedown/
- CiberPrisma. (2024). Operación Synergia II: Un golpe global contra el cibercrimen. Recuperado de: https://ciberprisma.org/2024/11/09/operacion-synergia-ii-un-golpe-global-contra-el-cibercrimen/
- INTERPOL. (2024). Descubrimiento de una red delictiva: 5,100 detenciones en una vasta operación contra las apuestas futbolísticas ilegales. Recuperado de: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Descubrimiento-de-una-red-delictiva-5-100-de
- T21. (2024). Sectores más atacados por cibercriminales en 2024. Recuperado de: https://t21.pe/sector-atacado-cibercriminales-2024
- Líder Empresarial. (2024). Ciberataques en aumento: nuevos grupos de ransomware emergen en 2024. Recuperado de: https://www.liderempresarial.com/ciberataques-en-aumento-nuevos-grupos-de-ransomware-emergen-en-2024/
- Statista. (2024). Estadísticas de ciberseguridad global. Statista Cybersecurity. Recuperado de: https://www.statista.com/outlook/tmo/cybersecurity/worldwide
- World Economic Forum. (2024). Annual Report. Recuperado de: https://es.weforum.org/publications/series/annual-report/
- Ingecom. (s.f.). Predicciones de ciberseguridad en privacidad de datos. Ingecom Cybersecurity Trends. Recuperado de: https://www.ingecom.net/es/blog/295/tendencias-en-ciberseguridad-para-2024-lo-que-necesitas-saber/
- IBM. (2023). Costos de violaciones de seguridad en 2023. IBM Cost of a Data Breach Report. Recuperado de: https://www.ibm.com/reports/data-breach/

Referencias

- Kaspersky. (2024). *Kaspersky pronostica ransomware más resistente y nuevas amenazas a finanzas móviles para 2025*. Recuperado de: https://latam.kaspersky.com/about/press-releases/kaspersky-pronostica-ransomware-mas-resistente-y-nuevas-amenazas-a-finanzas-moviles-para-2025?srsltid=AfmBOooatD2O-cSpZ4Xfy33s9w_9tRdA5nzsIMn78tnkJVk-JbhEwzzG

- Ciberseguridad.com. (s.f.). Principales tendencias y predicciones para 2024. Ciberseguridad.com. Recuperado de: https://ciberseguridad.com/blog/predicciones-ciberseguridad-2024/

- McKinsey. (s.f.). Impacto de la digitalización y ciberseguridad en la economía global. McKinsey Digital Insights. Recuperado de: https://www.mckinsey.com/business-functions/mckinsey-digital/

- Kroll. (2024). Q2 2024 Threat Landscape Report: Threat Actors, Ransomware, Cloud Risks Accelerate. Recuperado de: https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q2-2024-threat-landscape-report-threat-actors-ransomware-cloud-risks-accelerate

- CRN. (2024). 10 Major Ransomware Attacks and Data Breaches in 2024. Recuperado de: https://www.crn.com/news/security/2024/10-major-ransomware-attacks-and-data-breaches-in-2024

- Semperis. (2024). España: Riesgo de ransomware en 2024. Recuperado de: https://www.semperis.com/es/resources/espana-ransomware-risk/

- ESET. (2024). Reporte de amenazas: Segundo semestre de 2024. Recuperado de: https://www.welivesecurity.com/es/informes/eset-reporte-amenazas-segundo-semestre-2024/

- Europol. (2024). Nuevo informe: La inteligencia artificial como refuerzo de las organizaciones policiales. Recuperado de: https://notesdeseguretat.blog.gencat.cat/2024/10/07/nuevo-informe-de-europol-la-inteligencia-artificial-como-refuerzo-de-las-organizaciones-policiales/

Referencias

- Ciberseguridad Blog. (2024). El impacto del 5G en la ciberseguridad. Recuperado de: https://www.ciberseguridad.blog/el-impacto-del-5g-en-la-ciberseguridad
- Gartner. (2024). Tendencias en ciberseguridad 2024. Recuperado de: https://www.gartner.es/es/tecnologia-de-la-informacion/tendencias/tendencias-ciberseguridad
- Acronis. (2024). Cyberthreats Report H1 2024: Breaking Down Key Findings. Recuperado de: https://www.acronis.com/es-es/blog/posts/acronis-cyberthreats-report-h1-2024-breaking-down-key-findings-from-the-report/
- VPN Ranks. (2024). Tendencias y amenazas de deepfake. Recuperado de: https://www.vpnranks.com/es-es/recursos/tendencias-y-amenazas-deepfake/
- Ramos-Zaga, F. (2024). Deepfake: Análisis de sus implicancias tecnológicas y jurídicas en la era de la Inteligencia Artificial. *Derecho Global. Estudios sobre Derecho y Justicia*, 9(27). https://doi.org/10.32870/dgedj.v9i27.754
- DeuSens. (2024). Innovaciones y desafíos en el metaverso para 2024. Recuperado de: https://deusens.com/es/blog/innovaciones-desafios-metaverso-2024#:~:text=En%20el%20a%C3%B1o%202024%2C%20el,Interfaz%20de%20Usuario%20e%20Interacci%C3%B3n
- Alcoyinnova. (2024). Las 5 tecnologías que están revolucionando el mundo en 2024. Recuperado de: https://alcoyinnova.com/las-5-tecnologias-que-estan-revolucionando-el-mundo-en-2024/
- VPN Ranks. (2024). Tendencias tecnológicas. Recuperado de: https://www.vpnranks.com/es-es/recursos/tendencias-tecnologicas/

Referencias

- Recorded Future. (s.f.). Threat Intelligence 101: Ransomware Attack Vectors. Recuperado de: https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-attack-vectors
- Balbix. (s.f.). Attack Vectors and Breach Methods. Recuperado de: https://www.balbix.com/insights/attack-vectors-and-breach-methods/
- AIMultiple. (s.f.). Most Common Cyber Attack Vectors. Recuperado de: https://research.aimultiple.com/most-common-cyber-attack-vectors/
- Arctic Wolf. (s.f.). Top Five Cyberattack Vectors. Recuperado de: https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/
- Bleeping Computer. (2024). Russian Hackers Use RDP Proxies to Steal Data in MiTM Attacks. Recuperado de: https://www.bleepingcomputer.com/news/security/russian-hackers-use-rdp-proxies-to-steal-data-in-mitm-attacks/
- Hackers4U. (s.f.). Top Cyber Attack Vectors and How to Mitigate Them. Recuperado de: https://www.hackers4u.com/top-cyber-attack-vectors-and-how-to-mitigate-them
- Hispasec. (2024). La Botnet Matrix desata ataques DDoS masivos explotando dispositivos IoT vulnerables. Recuperado de: https://unaaldia.hispasec.com/2024/11/la-botnet-matrix-desata-ataques-ddos-masivos-explotando-dispositivos-iot-vulnerables.html
- Weber, M. (2024). Hybrid Warfare and Cybersecurity. *Journal of Global Threats*, 14(3), 25–47. Recuperado de: https://www.sia-partners.com/en/insights/publications/hybrid-warfare-how-cyber-warfare-transforming-international-relations

Referencias

- European Union Agency for Cybersecurity (ENISA). (2024). *ENISA Threat Landscape 2024: July 2023 to June 2024*. European Union Agency for Cybersecurity. Recuperado de: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

- Gartner. (2024). Cybersecurity Predictions for 2024. Recuperado de: https://www.gartner.com/en/webinar/619414/1383687

- Sonatype. (2023). The Evolution of Supply Chain Attacks. Recuperado de: https://www.sonatype.com/hubfs/WP-Evolution-of-SSC-Attacks_03152023.pdf

- Ámbito. (2024). BRICS vs G20: El ascenso del bloque señala un cambio en el poder global. Recuperado de: https://www.ambito.com/finanzas/brics-vs-g20-el-ascenso-del-bloque-senala-un-cambio-el-poder-global-n6073582

- TV BRICS. (2024). Países del G20 apoyan la cooperación en la regulación de la IA en la declaración final de la cumbre. Recuperado de: https://tvbrics.com/es/news/pa-ses-del-g20-apoyan-la-cooperaci-n-en-la-regulaci-n-final-de-la-cumbre

- Carnegie Endowment for International Peace. (2024). Emerging Middle Powers: BRICS Summit and Its Global Implications. Recuperado de: https://carnegieendowment.org/research/2024/10/brics-summit-emerging-middle-powers-g7-g20?lang=en

- Foro Económico Mundial. (2024). Foco en la ciberseguridad: 10 cosas que necesitas saber en 2024. Recuperado de: https://es.weforum.org/stories/2024/10/foco-en-la-ciberseguridad-10-cosas-que-necesitas-saber-en-2024

- CrowdStrike. (2024). Global Threat Report 2024. Recuperado de: https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

Referencias

- Google Threat Analysis Group. (2024). APT44 and Sandworm Activities. Recuperado de: https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm/

- CISA. (2024). People's Republic of China-Linked Cyber Actors Hide in Router Firmware. Recuperado de: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a

- Mandiant. (2024). Chinese Espionage Group UNC3886 Found Exploiting VMware Vulnerabilities Since 2021. Recuperado de: https://www.mandiant.com/resources/blog/chinese-vmware-exploitation-since-2021

- JPCERT. (2024). New Malicious PyPI Packages Used by Lazarus. Recuperado de: https://blogs.jpcert.or.jp/en/2024/02/lazarus_pypi.html

- Lisa Institute. (2024). Tendencias Globales en Seguridad. Recuperado de: https://www.lisainstitute.com/blogs/blog/lista-10-riesgos-geopoliticos-tendencias-seguridad-2019-2025


NTT DATA