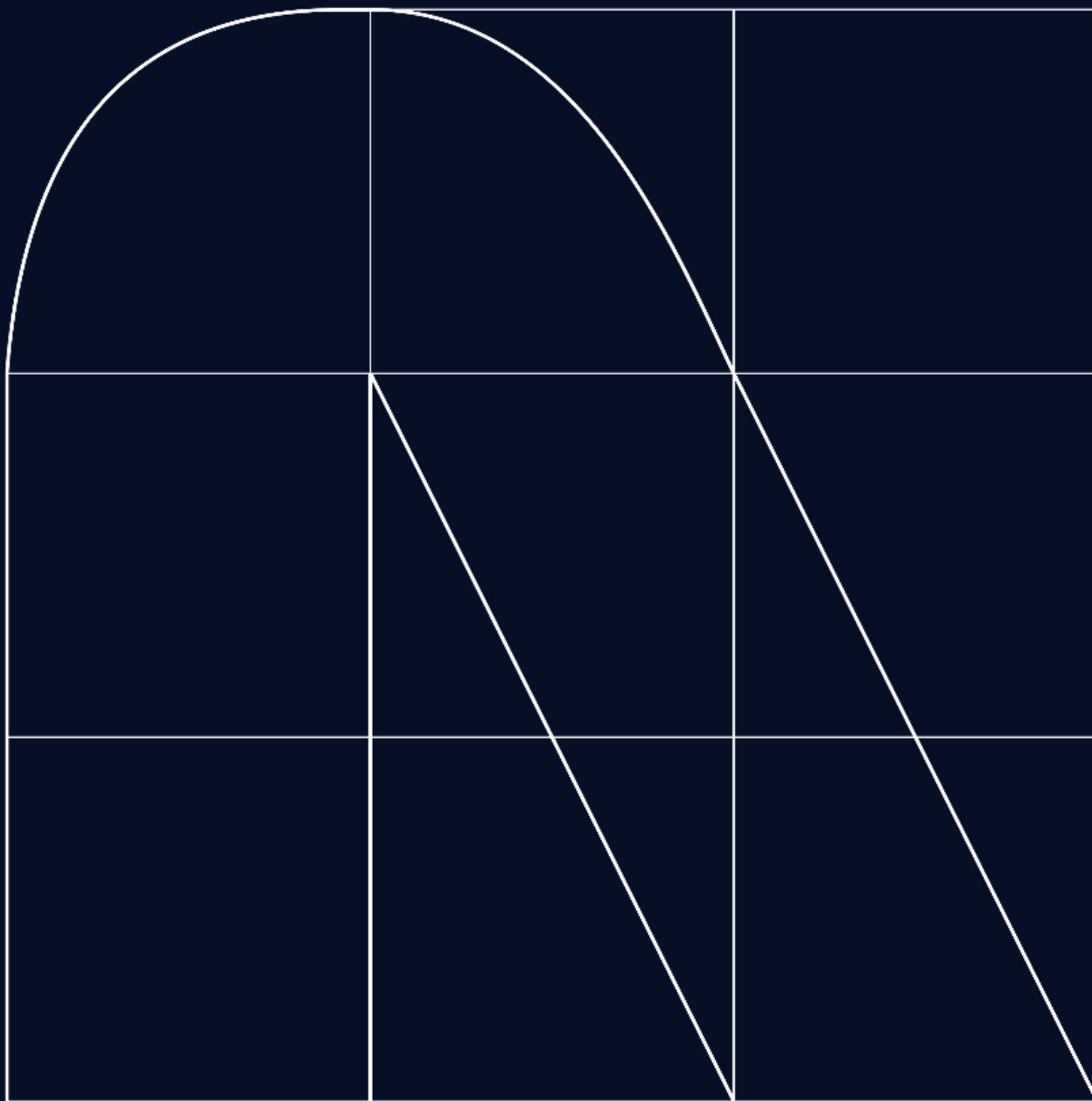
CTI-TEND-JUL-2024

NTT DATA

Tendencias CTI

Ciber Inteligencia de Amenazas

Primer semestre 2024



ÍNDICE

1. Introducción 3
1.1. Alcance del informe 3
1.2. Alcance geográfico y temporal del informe 3
2. Panorama Global de Amenazas 5
2.1. Principales amenazas globales 6
2.2. Tendencias emergentes 8
2.3. Grandes filtraciones de datos o ventas en mercados underground 9
2.4. Estadísticas globales sobre incidentes de seguridad, tipos de ataques y Actores Maliciosos involucrados 10
3. Tendencias de amenazas por sectores 12
3.1. Tipos de ataques más comunes en cada sector 12
3.2. Identificación de los sectores más vulnerables y atacados 13
4. Actores de Amenazas (Threat Actors) 16
4.1. Actores de amenazas patrocinados por el Estado 16
4.2. Grupos de ransomware 18
4.3. Nuevos Actores Maliciosos 19
5. Técnicas, Tácticas y Procedimientos (TTPs) 22
5.1. Descripción de las TTPs más comunes utilizadas por los cibercriminales 22
6. Vulnerabilidades 26
6.1. Análisis de tendencias 26
6.2. Vulnerabilidades más críticas 28
6.3. Vulnerabilidades más explotadas 30
6.4. 0-day detectados o publicados 31
6.5. Parches de seguridad publicados 32

1. Introducción

1.1. Alcance del informe

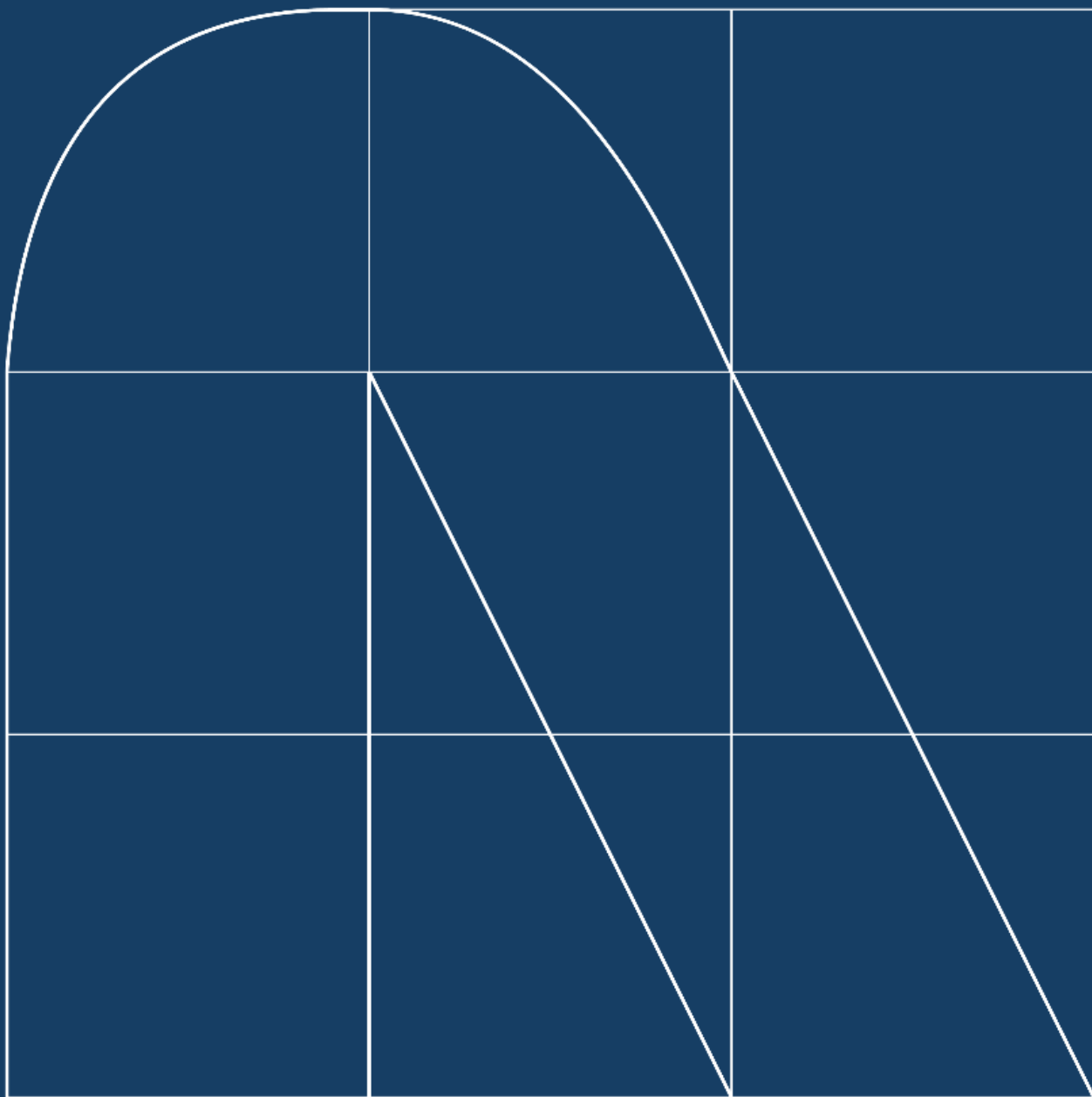
El presente informe tiene como objetivo proporcionar una visión detallada de las tendencias y acontecimientos relevantes en el ámbito de la Inteligencia de Amenazas durante el primer semestre del 2024. Se analizarán las amenazas emergentes, los Actores Maliciosos relevantes, las campañas destacadas y las vulnerabilidades críticas identificadas en este período, con el fin de ofrecer una comprensión profunda del panorama actual de la ciberseguridad.

1.2. Alcance geográfico y temporal del informe

El alcance de este documento pone foco en las tendencias de Ciber Inteligencia de Amenazas en un ámbito geográfico Global, analizando las tendencias que ocurren en todo el panorama de amenazas ocurridas en el primer semestre del año 2024 (de enero a junio).

NTT DATA

Panorama Global de Amenazas



2. Panorama Global de Amenazas

La evolución del panorama en ciberseguridad ha tomado un nuevo flujo, vinculado principalmente con las nuevas tecnologías emergentes y la potencia en el desarrollo de las **Inteligencias Artificiales generativas (GEN-IA)**. Desde el equipo de **Cyber Threat Intelligence** de **NTT DATA**, se han identificado **cuatro puntos clave para 2024**:

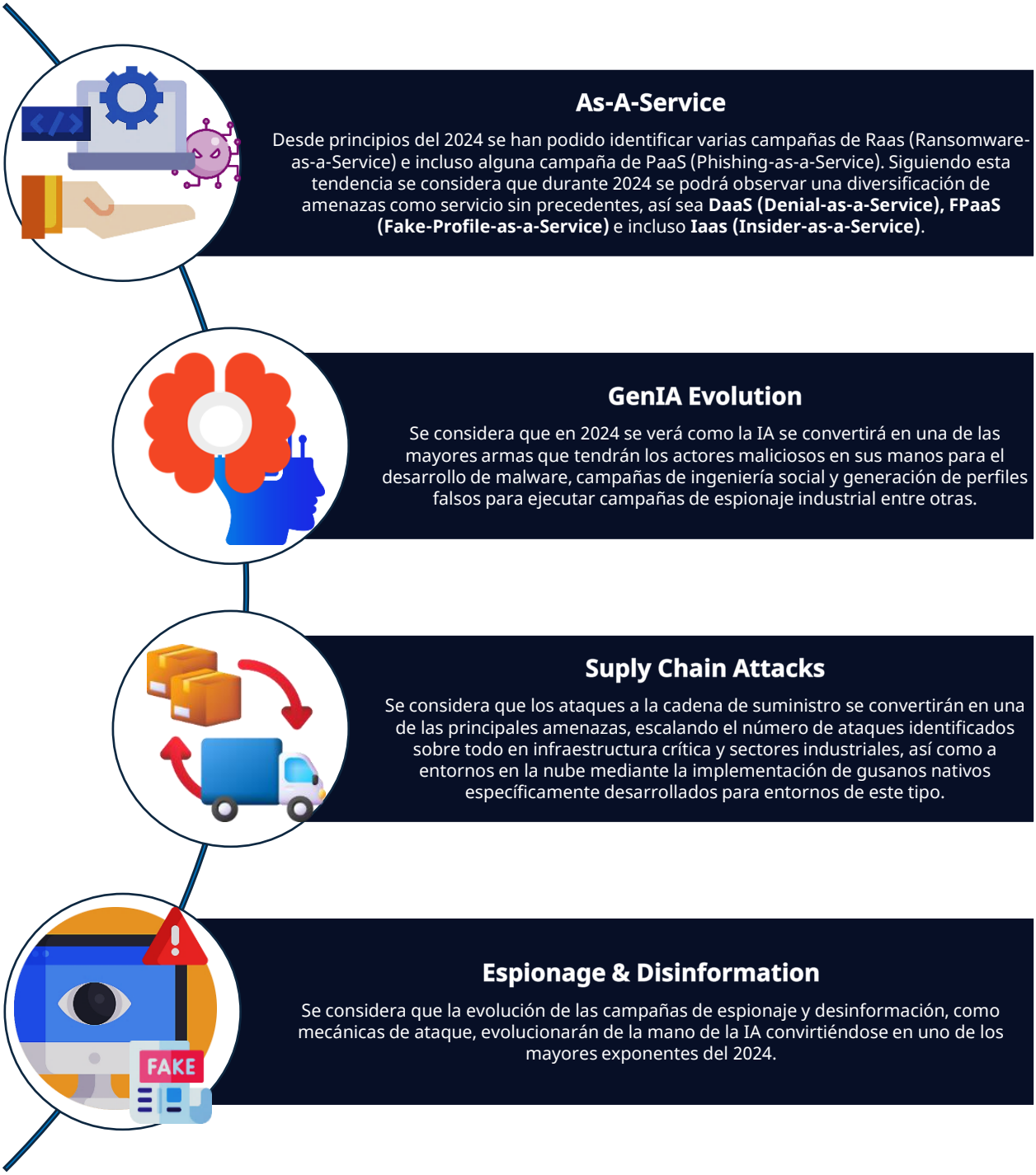


FIGURA 1 - PRINCIPALES TENDENCIAS EN AMENAZAS

2.1. Principales amenazas globales

Entrando en materia, en lo que respecta a las principales amenazas a afrontar en la primera mitad del año 2024, desde el equipo de **Cyber Threat Intelligence** de **NTT DATA** se ha establecido un ranking de amenazas, donde se destacan **los 5 principales ataques con mayor número de registros únicos** para el primer semestre de 2024:

1. **Data Leak**
   - Aumento en 2024 frente al 2023: **30%**
   - Ataques registrados: **2.3 millones**
2. **DDoS**
   - Aumento en 2024 frente al 2023: **25%**
   - Ataques registrados: **1.8 millones**
3. **Phishing y Vishing**
   - Aumento en 2024 frente al 2023: **18%**
   - Ataques registrados: **1.45 millones**
4. **Ransomware**
   - Aumento en 2024 frente al 2023: **20%**
   - Ataques registrados: **623,000**
5. **Defacement**
   - Aumento en 2024 frente al 2023: **10%**
   - Ataques registrados: **150,000**

Según las cifras contrastadas entre los datos registrados en las herramientas de monitorización y fuentes externas verificadas, se ha establecido un **porcentaje general de aumento del 39%**, pudiendo deducir los resultados **para la segunda mitad del año** en una proporción lineal:

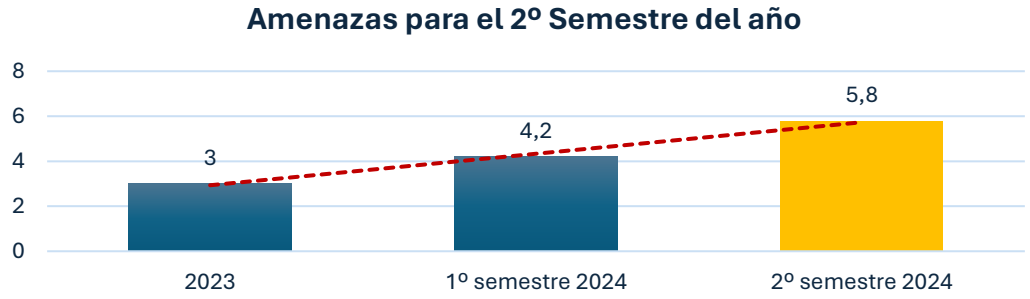
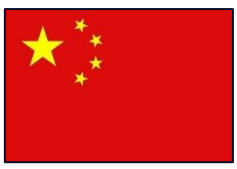


TABLA 1 - PROSPECTIVA DE AMENAZAS PARA EL 2º SEMESTRE DEL AÑO

Respecto a la distribución geográfica de estas amenazas, se ha estimado que los **3 países más activos y con mayor índice de atribución, englobando todos los tipos de ataque, son**:

Rusia



China

Corea del Norte

La tendencia de las amenazas detectadas en el primer semestre apunta a que seguirán avanzando y ganando fuerza para la segunda mitad del año 2024, donde se pueden destacar las siguientes amenazas:

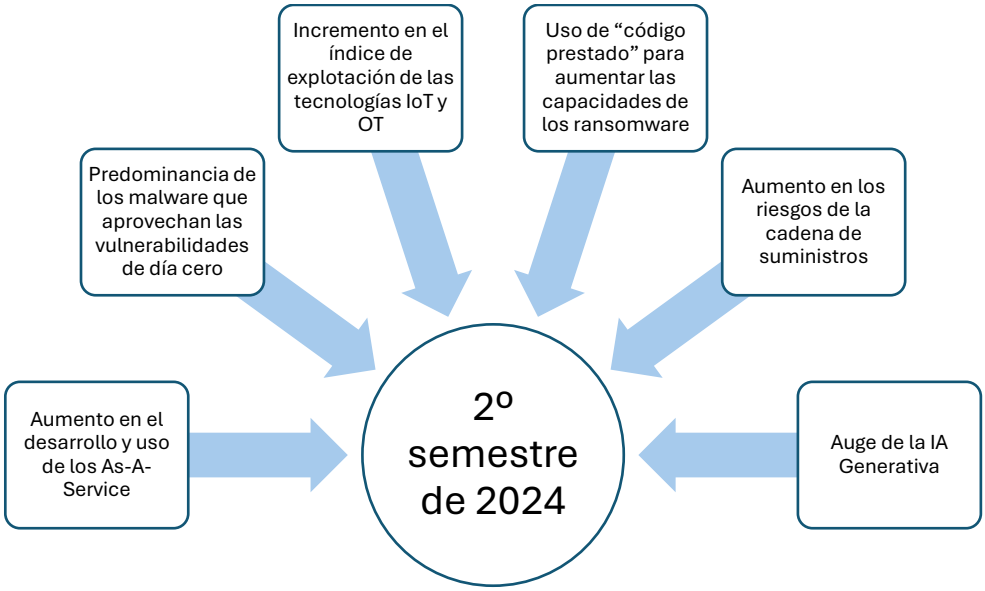


FIGURA 2 - PRINCIPALES AMENAZAS IDENTIFICADAS

Dentro de las amenazas mencionadas, en la primera mitad del año se ha apreciado que los cuatro frentes tecnológicos más amenazados son:

FIGURA 3 - PRINCIPALES TECNOLOGÍAS DE RIESGO IDENTIFICADAS

Como conclusión general, los ataques especializados, la sofisticación y la cantidad de Técnicas y Tácticas están aumentando y evolucionando, alineándose con las nuevas tecnologías emergentes, la interconectividad de los dispositivos y la IA Generativa. Además, se puede concluir que los ataques dirigidos contra países de la **OTAN** y los **BRICS** se han incrementado, principalmente debido a los recientes acontecimientos referidos a los conflictos en Palestina e Irán, así como los acontecimientos sucedidos en Rusia y Ucrania.

Los países pertenecientes a la **OTAN** han acumulado cerca del **36% de los ataques registrados** (**1.500 ataques** directos), mientras que los **BRICS se han establecido en un 28% (1.200 ataques** directos), **destacándose** los **ransomware** y los **DDoS** como principales tipologías de ataque.

2.2. Tendencias emergentes

En lo que respecta a **tendencias emergentes y con carácter general**, desde el equipo de **Cyber Threat Intelligence** de **NTT DATA**, se ha detectado una serie de **patrones de comportamiento** entre los Actores Maliciosos que permiten especular sobre lo que se puede esperar en la **segunda mitad del año**:

FIGURA 4 - TENDENCIAS EMERGENTES

Siguiendo este punto y con especial referencia a las amenazas relativas a **IA, 5G e IoT**, desde el 2º semestre de 2023 hasta el final del 1º semestre de 2024, se ha producido **un incremento en el uso de la IA Generativa del 600%**, lo que repercute principalmente en **estos 5 tipos de ataque**:

Phishing & Vishing	Suplantación de Identidad	Desinformación & Fake News	DDoS Evolution	Credential Stuffing
• Incremento estimado en torno al 70% para el 2º semestre de 2024. • Incremento en el uso de los IA ChatBots, así como el uso de ataques de IA Vishing por suplantación de voz. • Surjen los ataques de phishing de adversario en el medio (AiTM) y los ataques de navegador en el navegador (BiTB). • Incremento en la cantidad de ataques de secuestro DNS para redireccionamiento a sitios web de descarga de malware.	• Suplantación de marcas de prestigio con alta reputación para eludir medidas de seguridad. • Uso de chatbots de LLM que permiten crear comunicaciones y correos de mayor fiabilidad, eliminando la mayor parte de errores ortográficos y gramaticales. • Surgimiento de campañas evolutivas que se apoyan en IA ChatBots que permiten ejecutar campañas simulando ser un soporte técnico que serán casi imposibles de detectar.	• Incremento en la complejidad y sofisticación de las campañas de desinformación gracias a la IA. • Aumento en la capacidad de distribución de datos a través de las tecnologias 5G, aumentando el rango de acción de los grupos maliciosos. • Creación de fotos y vídeos por IA para aumentar la credibilidad de las campañas.	• Incremento sustancial en la volumetría de estos ataques, con 5,2 millones de ataques DDoS HTTP. • Se originan nuevos grupos, muchos de ellos patrocinados por el estado. • Centralización de los ataques DDoS basados en IoT, aprovechándose de la masificación en la conectividad IoT, especialmente en tecnologías OT. • Incrementará el rango botnet para la ejecución de ataques, especializándose en explotar vulnerabilidades asociadas a dispositivos IoT.	• Las herramientas de GenIA que han permitido elaborar métodos y técnicas para la elusión de las medidas de seguridad estándar como CAPTCHA y limitación de velocidad de IP.

Un claro ejemplo del empleo de la IA, y siguiendo el análisis de un incidente de seguridad detectado en esta primera mitad del año, fue un **fraude de casi 26 millones de dólares** donde los Actores Maliciosos simularon una **reunión ejecutada con avatares generados y controlados por IA** (CNN, SCMP ,2024).

2.3. Grandes filtraciones de datos o ventas en mercados underground

En el primer semestre del año, desde el equipo de **Cyber Threat Intelligence** de **NTT DATA**, se han estimado un total de casi **10.000 incidentes confirmados**, con más de **35 billones de datos filtrados**:

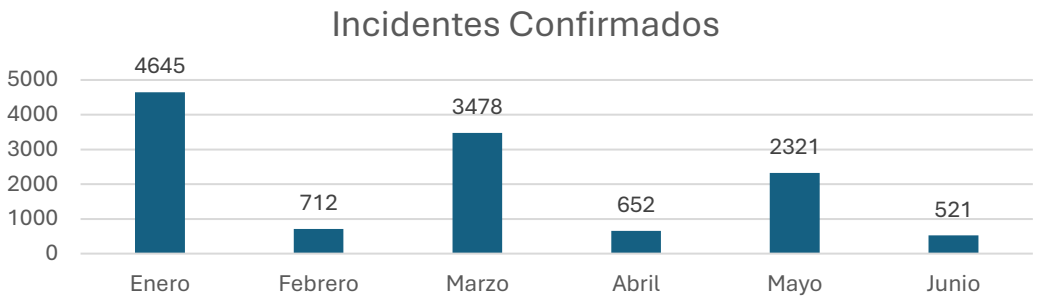


TABLA 2 - INCIDENTES CONFIRMADOS

Las Brechas de Datos más destacadas de los últimos 6 meses son:

MES	ORGANIZACIÓN	PAÍS	SECTOR	RECUENTO DE DATOS FILTRADOS
ENERO	MOAB	Global	Múltiple	± 26.000.000.000
	Indian Mobile Network	India	Telecomunicaciones & Tecnología	± 750.000.000
	IPL Consulting	Rusia	Telecomunicaciones & Tecnología	Desc. [± 60 TB de datos]
FEBRERO	Zenlayer	Estados Unidos	Telecomunicaciones & Tecnología	± 384.658.212
	MRA	Estados Unidos	Servicios Comerciales & Profesionales	Desc. [± 3 TB de datos]
	Optum	Estados Unidos	Sanitario	Desc. [± 6 TB de datos]
MARZO	AMMEGA	Dinamarca	Manufacturero	Desc. [± 3 TB de datos]
	916 Google Firebase	Estados Unidos	Múltiple	± 124.605.664
	NHS Dumfries & Galloway	Reino Unido	Sanitario	Desc. [± 3 TB de datos]
ABRIL	Discord	Estados Unidos	Entretenimiento & Medios	± 4.186.879.104
	iSharingSoft	Estados Unidos	Telecomunicaciones & Tecnología	± 35.000.000
	Baidu, Honor, Huawei, iFlytek, OPPO, Samsung, Tencent, Vivo & Xiaomi	China	Telecomunicaciones & Tecnología	± 1.000.000.000
MAYO	KyungChang's	China	Industria	Desc. [± 1.6 TB de datos]
	Landmark Life	Estados Unidos	Seguros	Desc. [± 2.4 TB de datos]
	99 Digital	Estados Unidos	Telecomunicaciones & Tecnología	Desc. [± 5.2 TB de datos]
JUNIO	Ticketmaster	Múltiple	Entretenimiento & Medios	± 560.000.000
	Tea Group	Estados Unidos	Energía & Recursos Naturales Servicios Profesionales & Comerciales	Desc. [± 1 TB de datos]

TABLA 3 - PRINCIPALES BRECHAS DE DATOS DEL 1º SEMESTRE DE 2024

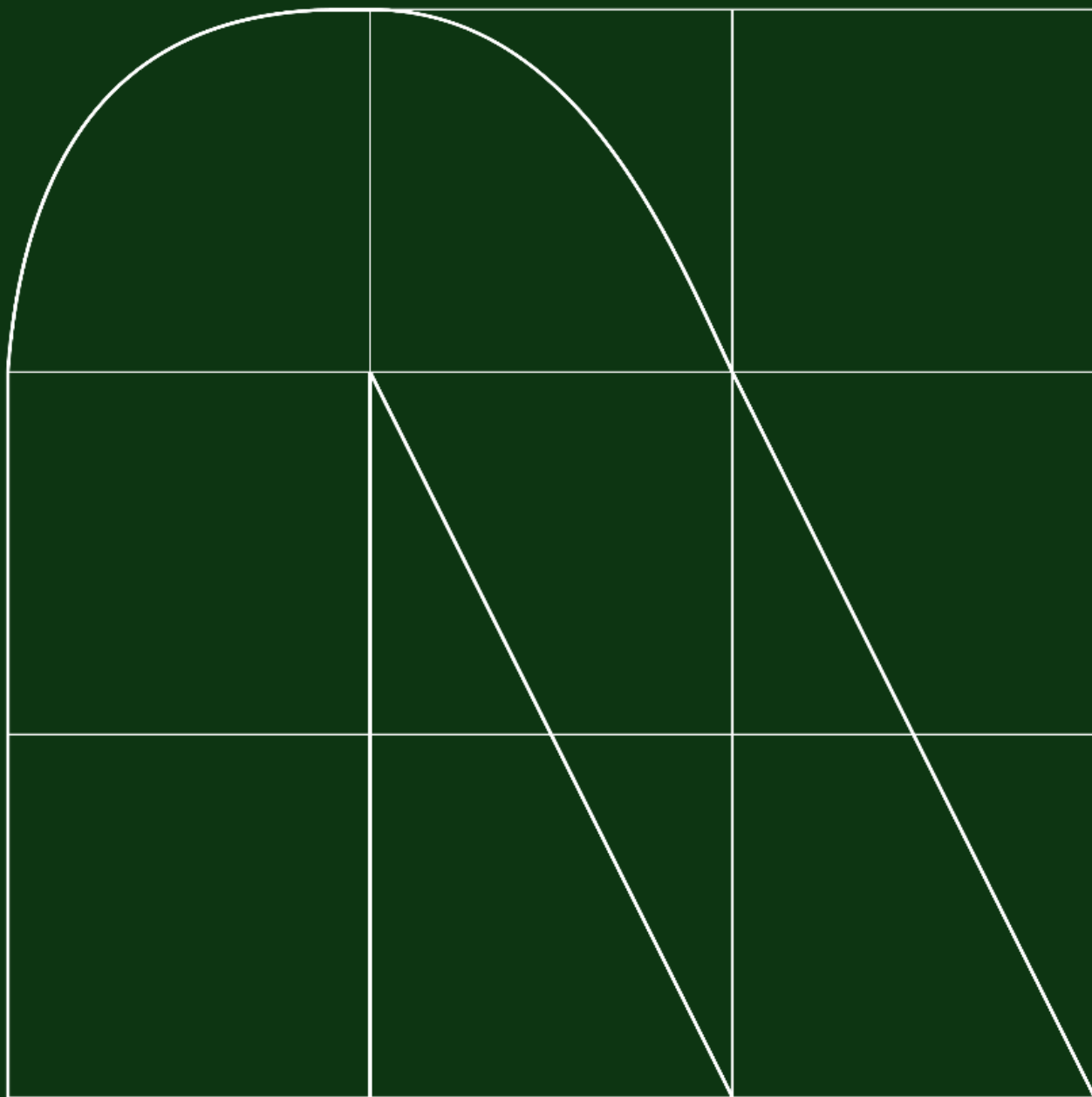
2.4. Estadísticas globales sobre incidentes de seguridad, tipos de ataques y Actores Maliciosos involucrados

Respecto a las tendencias globales sobre incidentes de seguridad, desde el equipo de **Cyber Threat Intelligence** de **NTT DATA**, se ha establecido un ranking de los **10 incidentes de seguridad más graves**, según sus repercusiones:

INCIDENTE	PAÍS AFECTADO	GRUPO DE ATRIBUCIÓN	PAÍS DE ATRIBUCIÓN	INFORMACIÓN DE INTERÉS
Ataque a SolarWinds Parte II	Global	APT29 (Cozy Bear)	Rusia	Un nuevo ataque masivo a **SolarWinds** afectó a miles de organizaciones. Este ataque fue más sofisticado que el anterior, comprometiendo actualizaciones de software críticas y permitiendo a los atacantes acceso persistente a redes sensibles en sectores gubernamentales y privados.
Brecha de Datos de Microsoft Exchange	Global	Hafnium	China	Una vulnerabilidad crítica en **Microsoft Exchange** fue explotada por Actores Maliciosos estatales, permitiendo el acceso a correos electrónicos y datos sensibles de miles de organizaciones. Este ataque afectó tanto a grandes corporaciones como a pequeñas y medianas empresas.
Ataque a Colonial Pipeline 2.0	Estados Unidos	DarkSide (ahora BlackMatter)	Rusia	**Colonial Pipeline** sufrió un segundo ataque de ransomware, paralizando nuevamente la distribución de combustibles en gran parte de la costa este de Estados Unidos. El ataque provocó una respuesta federal masiva y una rápida intervención para restaurar los servicios.
Ataque Ransomware Masivo al Sector Sanitario	Estados Unidos	Conti	Rusia	**El Hospital General de Massachusetts** fue objetivo de un ataque de ransomware, comprometiendo datos de pacientes y sistemas críticos de operación. El ataque resaltó la vulnerabilidad continua del sector salud frente a amenazas cibernéticas.
Ataque a la Cadena de Suministro de Log4j	Global	APT10 (Stone Panda)	China	Una nueva vulnerabilidad en el software de registro **Log4j** fue explotada globalmente, afectando a millones de dispositivos IoT y sistemas de control industrial. El ataque subrayó la importancia de la seguridad en componentes de software comunes.
Compromiso de Cuentas de Google Cloud	Global	Lazarus Group	Corea del Norte	Un ataque masivo comprometió cuentas de **Google Cloud**, afectando a servicios críticos y exponiendo datos de clientes corporativos y personales. Este incidente subrayó la necesidad de mejorar la seguridad en entornos de nube.
Ataque e Intrusión en Infraestructuras Críticas	Alemania	Berserk Bear (Crouching Yeti)	Rusia	Un grupo de hackers patrocinado por el estado atacó **infraestructuras críticas en Alemania**, incluyendo plantas de energía y sistemas de transporte. El ataque causó interrupciones significativas y generó una llamada a reforzar la seguridad en infraestructuras esenciales.
Ataque a Empresas Financieras en Asia	Asia	FIN7 (Carbanak)	Rusia	Un ataque dirigido a grandes **bancos y empresas financieras en Asia** resultó en la exfiltración de grandes cantidades de datos financieros y personales. Este incidente llevó a una revisión de las estrategias de ciberseguridad en el sector financiero asiático.
Campaña de Phishing Masivo	Global	Charming Kitten	Irán	Un sofisticado **ataque de phishing** utilizó deepfakes y técnicas de ingeniería social para comprometer cuentas de alto perfil en plataformas de redes sociales. Este ataque afectó a influencers, políticos y figuras públicas, exponiendo información sensible y dañando reputaciones.
Intrusión en Sistemas de Control de Tráfico Aéreo	Global	APT41 (Winnti)	China	Un ciberataque comprometió **sistemas de control de tráfico aéreo en varios aeropuertos internacionales**, causando retrasos y riesgos de seguridad significativos. Este incidente destacó la vulnerabilidad de los sistemas de transporte frente a amenazas cibernéticas.

TABLA 4 - PRINCIPALES INCIDENTES DEL 1º SEMESTRE DE 2024

Tendencia de amenazas por sectores



3. Tendencias de amenazas por sectores

3.1. Tipos de ataques más comunes en cada sector

Desde el departamento **Cyber Threat Intelligence** de **NTT DATA**, siguiendo los análisis y las detecciones realizadas a lo largo del primer semestre del año, se ha podido observar que las principales amenazas están bien definidas y delimitadas, pudiendo destacar **3 tipos de ataque**:

- **Ransomware**
- **DDoS**
- **Phishing**

Los 5 sectores más afectados a nivel global por esta tipología de ciberataques son:

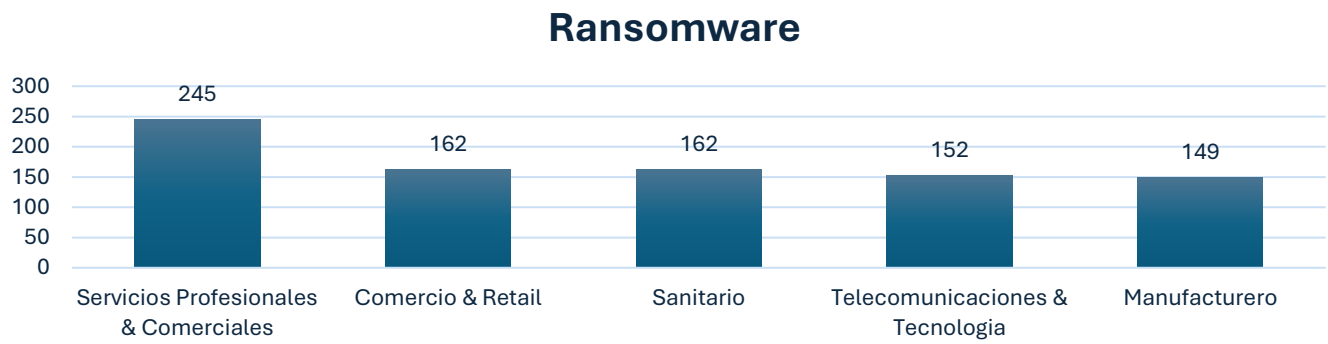


TABLA 5 - 5 SECTORES MAS AFECTADOS POR ATAQUES DE RANSOMWARE

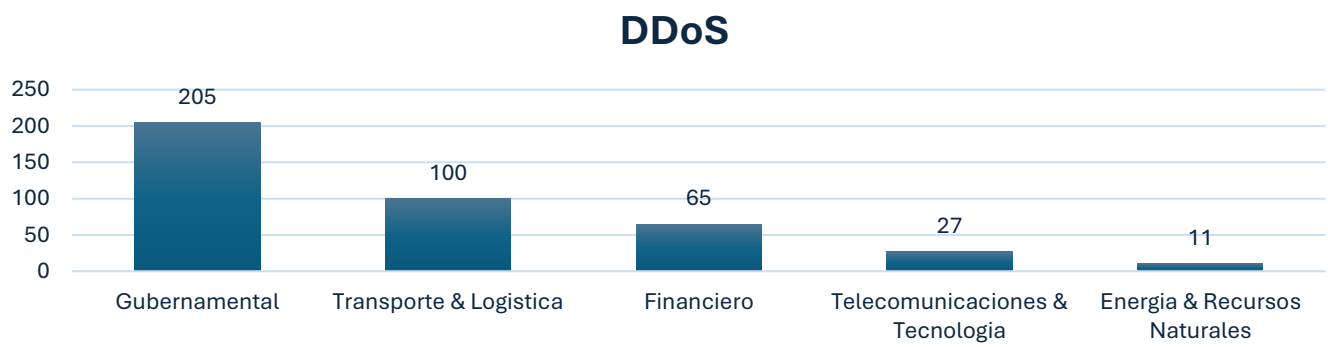


TABLA 6 - 5 SECTORES MAS AFECTADOS POR ATAQUES DE DDOS

TABLA 7 - 5 SECTORES MAS AFECTADOS POR ATAQUES DE PHISHING

Siguiendo la tendencia observada durante el primer semestre del año, los ataques dirigidos contra los sectores de **servicios profesionales y comerciales**, **gubernamental** y **financiero** los sitúan como **los tres sectores más atacados en sus respectivas categorías**, seguidos de los sectores **de comercio y *retail***, **transporte y logística** y **sanitario**.

Desde el departamento **Cyber Threat Intelligence** de **NTT DATA**, tras realizar un análisis de los ataques y los datos recopilados, se ha llegado a las siguientes conclusiones:

Los **actores/grupos maliciosos** que centran su actividad en el **ransomware**, han enfocado los ataques a los **sectores comerciales y profesionales**, principalmente dirigidos contra **PYMES**, al ser empresas con un índice de vulneración de seguridad elevado, en muchos casos con carencias en la aplicación base de los principios de ciberseguridad y que no pueden invertir altas cantidades de capital en mantener sus sistemas y redes seguros incorporando medidas optimizadas.

En los ataques de **denegación de servicio** se observa que están dirigidos contra **instituciones gubernamentales e infraestructuras críticas** y estos se han multiplicado, principalmente debido a los **conflictos internacionales** actuales y el **incremento de grupos patrocinados por estados**.

Los ataques de **phishing** siguen centralizados en sectores como el **financiero y sanitario** por dos motivos, **ganancia económica y valor de los datos**. En el caso del sector financiero se centran en la **suplantación de entidades bancarias o plataformas de pago**, buscando obtener datos de usuarios y credenciales.

3.2. Identificación de los sectores más vulnerables y atacados

El **Sector Gubernamental** y el **sector de servicios** ha sufrido un golpe significativo, lo que lo coloca a la cabeza de las industrias atacadas, seguido por los **sectores de transporte, tecnología de la información (TI) y comercio**, indicando una vulnerabilidad alarmante en sectores que son fundamentales para el funcionamiento de la sociedad.

Sin embargo, es el aumento sustancial interanual de los ataques a las **administraciones gubernamentales** lo que subraya un cambio estratégico en la preferencia de los objetivos por parte de los cibercriminales y grupos patrocinados por el Estado, debido principalmente a los conflictos internacionales actuales, pudiendo hipotetizar sobre las posibles motivaciones políticas y geoestratégicas detrás de estos ataques.

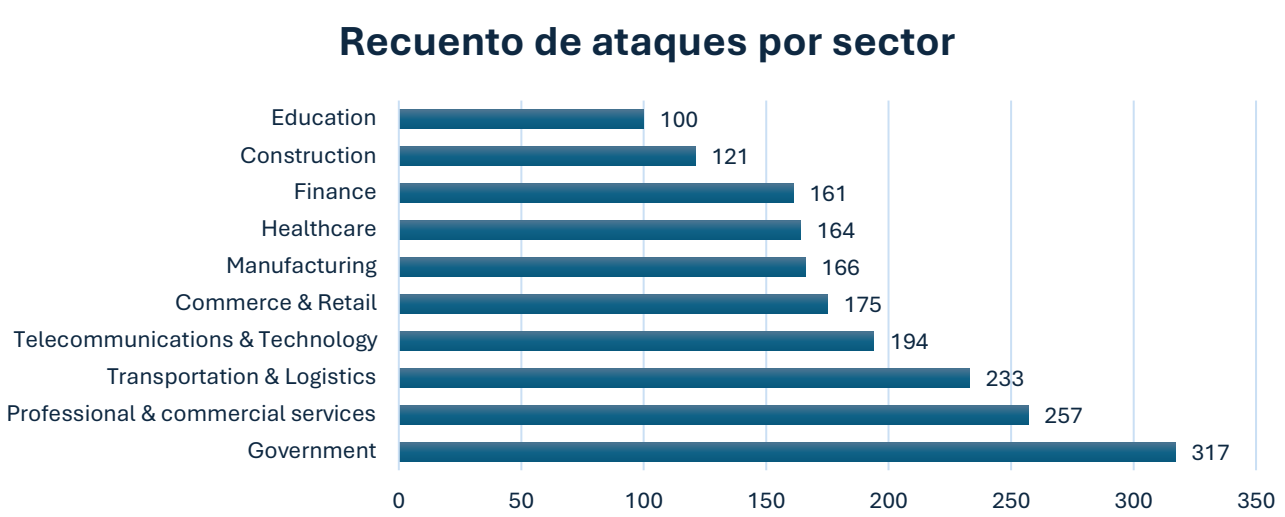


TABLA 8 - RECUENTO DE ATAQUES POR SECTOR

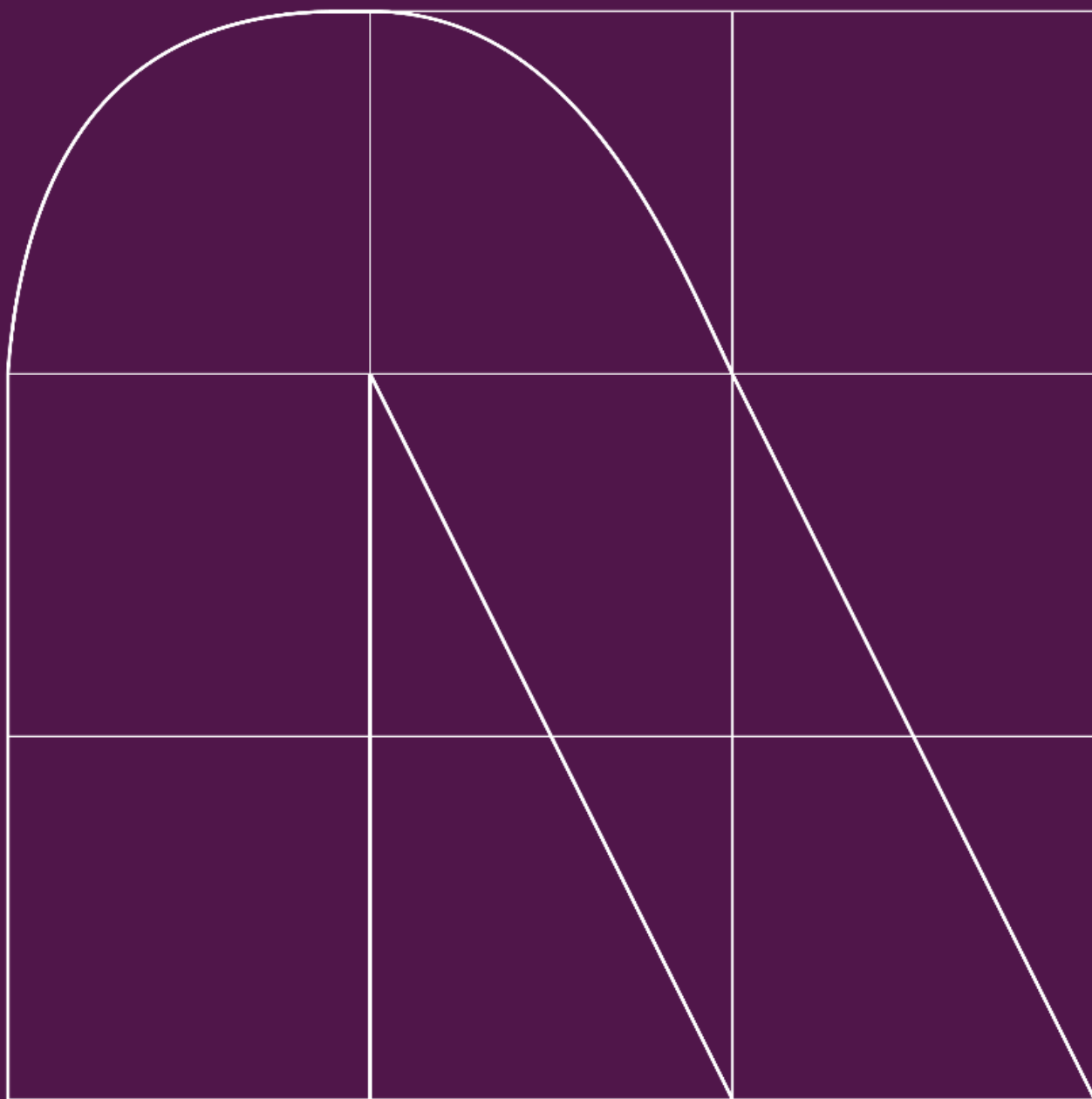
Asimismo, en el primer semestre de 2024, **América del Norte fue la región más afectada** por los ataques de ransomware, **seguida de Europa y la región Asia-Pacifico**.

El mayor aumento de ataques notificados en comparación con el primer semestre de 2023 se observó en **Europa**, con un **aumento significativo del 64%.** Este aumento significativo podría atribuirse a factores como una **mayor digitalización de los servicios y los entornos regulatorios** que pueden hacer que **las organizaciones sean objetivos más vulnerables o visibles**, sumado como se indicaba con anterioridad a los **conflictos internacionales**. Por el contrario, **América del Norte** experimentó un **aumento del 16%**, lo que indica un **enfoque sostenido** de los atacantes en esta región.

Por último, es interesante destacar el **incremento en los ataques contra los sectores manufacturero, educativo y sanitario**, los cuales han sufrido un incremento significativo como objetivo de Actores Maliciosos y grupos maliciosos. Esto es debido principalmente a la **expansión de los dispositivos IoT para la monitorización de sistemas OT y** también debido **al valor de los datos que controlan**, los cuales son **muy rentables como producto en foros y *markets underground***.

Actores de Amenazas

(Threat Actors)



4. Actores de Amenazas (Threat Actors)

En la siguiente sección, se realiza un análisis de los Actores de Amenazas con mayor actividad durante el primer semestre del 2024 así como los nuevos Actores de Amenazas que aparecen por primera vez en el panorama global, identificando las motivaciones, habilidades, recursos y contextos que los identifican.

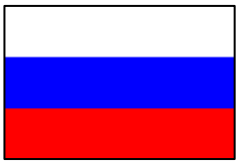
4.1. Actores de amenazas patrocinados por el Estado

En el primer semestre de 2024, los grupos de **Amenazas Persistentes Avanzadas (APT)** de diversas regiones del mundo, como **China**, **Corea del Norte**, **Irán** y **Rusia**, demostraron un aumento de actividades cibernéticas dinámicas e innovadoras.

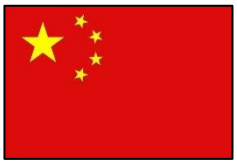
- **Estado de Irán:** Actores Maliciosos como ***Homeland Justice*** y ***Mint Sandstorm*** intensificaron sus esfuerzos de espionaje al atacar a instituciones gubernamentales y académicas en Occidente y Oriente Medio, con sofisticados ataques de phishing y malware novedoso, como ***MediaPI*** y ***MischiefTut***. Además, el Actor Malicioso ***Charming Kitten*** avanzó con sus tácticas de ingeniería social a través de una plataforma de seminarios web falsificados, y el Actor Malicioso **Tortoiseshell** intensificó su enfoque en los **sectores aeroespacial y de defensa** en Oriente Medio, lo que ilustra una mejora amplia y estratégica de las capacidades cibernéticas de Irán.
- **Estado de Rusia**: Actores de Amenaza como ***APT29*** accedieron a objetivos de alto valor, como *Microsoft*, comprometiendo correos electrónicos corporativos y repositorios de código fuente. Este Actor Malicioso también desplazó su atención hacia los ámbitos de políticas europeas, atacando a partidos políticos alemanes con la explotación de una puerta trasera con WINELOADER, recientemente desarrollada. Mientras tanto, el Actor Malicioso ***Gamaredon*** mantuvo sus sofisticados ataques contra el ejército ucraniano, y ***APT28*** aprovechó las vulnerabilidades de los enrutadores ***EdgeRouter*** de Ubiquiti para crear extensas redes de bots, lo que demuestra la adaptabilidad y la profundidad estratégica de Rusia en las operaciones cibernéticas.
- **Estado de China:** Actores Maliciosos, como ***Earth Lusca***, que aprovechó las tensiones geopolíticas con Taiwán aumentando las campañas de phishing dirigidas; ***Evasive Panda*** explotó la diáspora tibetana durante el *Festival Monlam* con software troyanizado, y ***Earth Krahang*** llevó a cabo ataques integrales contra entidades gubernamentales globales. Estas operaciones explotaron vulnerabilidades y aprovecharon los sistemas comprometidos para una amplia recopilación de inteligencia, lo que subraya la búsqueda estratégica y agresiva de inteligencia por parte de Actores de Amenaza patrocinados por el estado chino.
- **Estado Norcoreano:** El Actor Malicioso ***Kimsuky*** expandió su alcance en toda la región APAC utilizando sofisticadas técnicas de implementación de malware para mantener un acceso encubierto y crear oportunidades de ataque a la cadena de suministro utilizando repositorios de software PyPI. Al mismo tiempo, el Actor Malicioso ***Lazarus Group*** aprovechó una nueva **vulnerabilidad del kernel de Windows** para mejorar su **rootkit *FudModule***, lo que facilitó la manipulación profunda del sistema y la evasión de medidas de seguridad avanzadas.

En el primer semestre del 2024, el panorama de APT mostró esfuerzos intensificados por parte de Actores Maliciosos cibernéticos iraníes, rusos, chinos y norcoreanos.

Grupos iraníes como **Homeland Justice** y **Mint Sandstorm** intensificaron sus operaciones con sofisticados ataques contra objetivos nacionales y académicos



Entidades Rusas como **Nobelium** y **Gamaredon** se versaron a utilizar sus tácticas mejoradas contra objetivos corporativos y militares de alto valor.



Los Actores de Amenazas chinos, entre ellos **Earth Lusca** y **Evasive Panda**, aprovecharon los eventos geopolíticos de la región asiática para implementar malware avanzado de múltiples etapas, expandiendo su huella de espionaje a nivel mundial.

Grupos norcoreanos como **Kimsuky** y **Lazarus** demostraron capacidades mejoradas en ataques de múltiples etapas, centrándose en ataques a la cadena de suministro y la explotación de vulnerabilidades de día cero.

Para cada región, se resumen los hechos, hallazgos y conclusiones clave obtenidos de las fuentes de los ataques que pueden ser de utilidad para los profesionales que abordan los problemas prácticos de la ciberseguridad para las empresas.

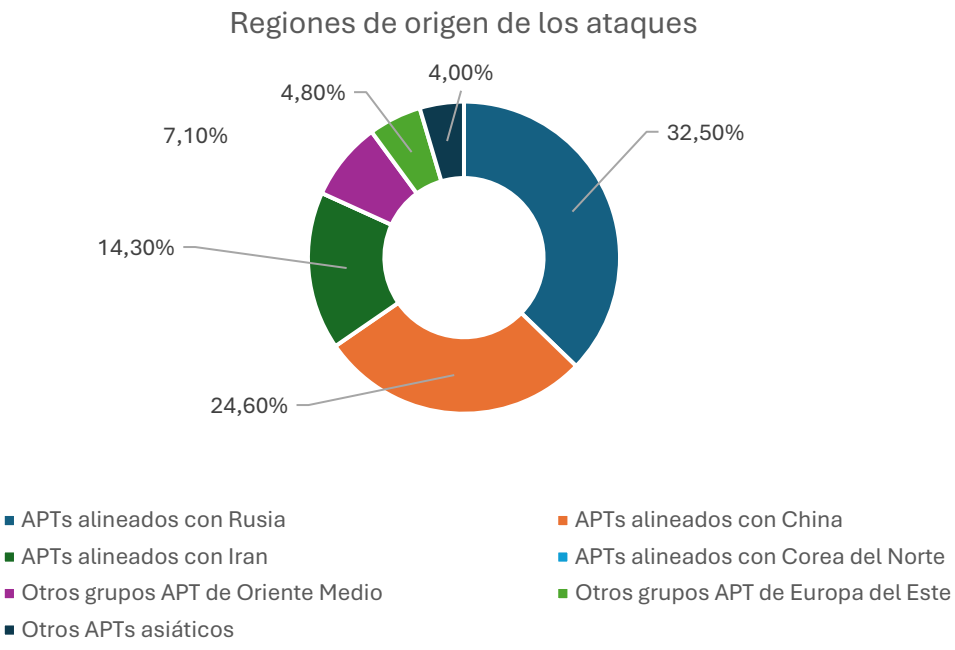


TABLA 9 - PORCENTAJES DE ATAQUES POR ACTORES MALICIOSOS PATROCINADOS POR ESTADOS

4.2. Grupos de ransomware

El año 2024 comenzó con un panorama muy diferente al del año 2023, si bien las cifras se dispararon en el cuarto trimestre de 2023 con 1309 casos, en el primer trimestre de 2024, la industria del ransomware se redujo a 1048 casos. Esto supone una **disminución del 22%** en los ataques de ransomware en comparación con el cuarto trimestre de 2023.

Desde el departamento **Cyber Threat Intelligence** de **NTT DATA**, se considera que dos razones de este descenso podrían ser la **intervención de las fuerzas de seguridad**, como se observó **con los Actores Maliciosos LockBit y ALPHV**, y la **disminución del pago de rescates**, lo que llevó a los grupos de ransomware a retirarse y buscar fuentes alternativas de ingresos.

A continuación, se muestra la evolución de los ataques de ransomware en el primer semestre del 2024:

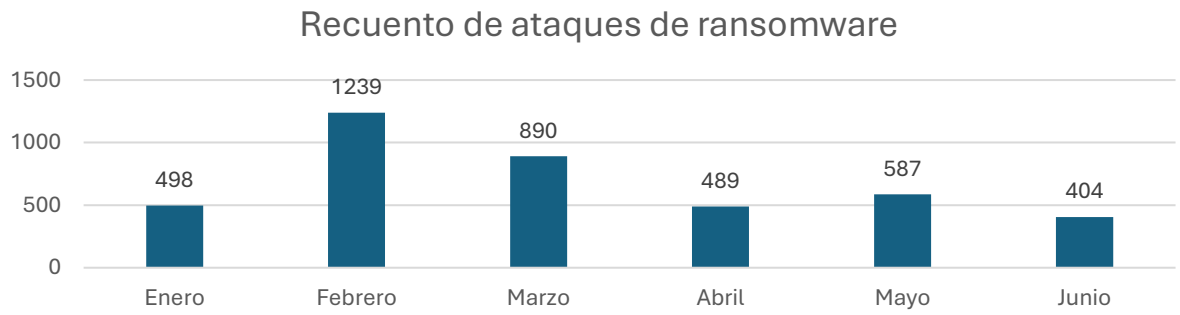


TABLA 1010 - RECUENTO DE ATAQUES DE RANSOMWARE

En el siguiente gráfico se muestran los grupos de ransomware más activos durante el primer semestre del 2024:

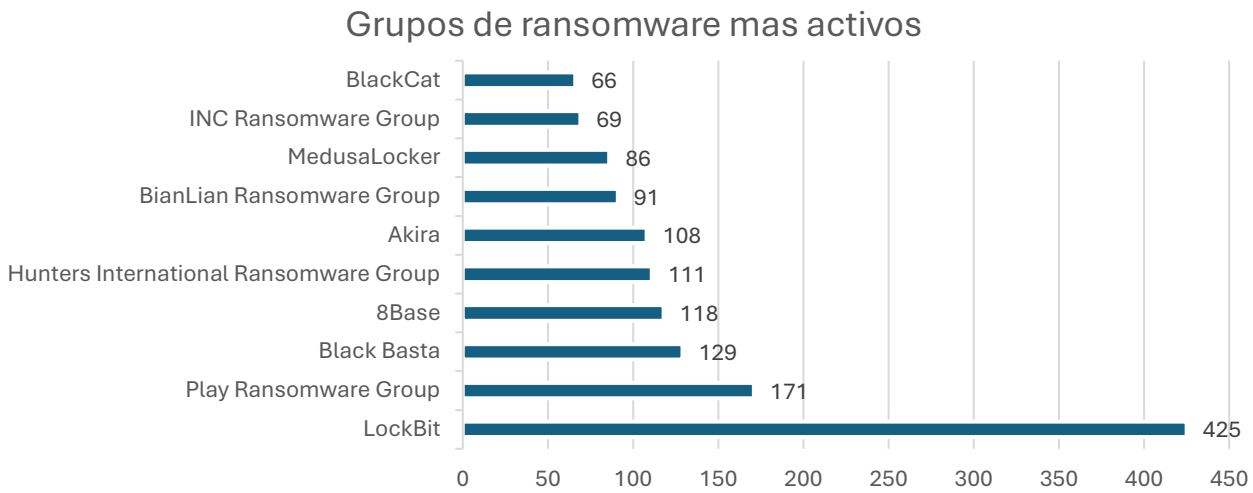


TABLA 1111 - GRUPOS DE RANSOMWARE MÁS ACTIVOS

4.3. Nuevos Actores Maliciosos

Durante este semestre del año, se han identificado nuevos Actores Maliciosos que, aunque parezcan nuevos en este mundo, en ocasiones vienen respaldados por grandes grupos maliciosos, lo que hace que no pasen desapercibidos y deban tenerse en cuenta por las grandes capacidades que pueden llegar a demostrar.

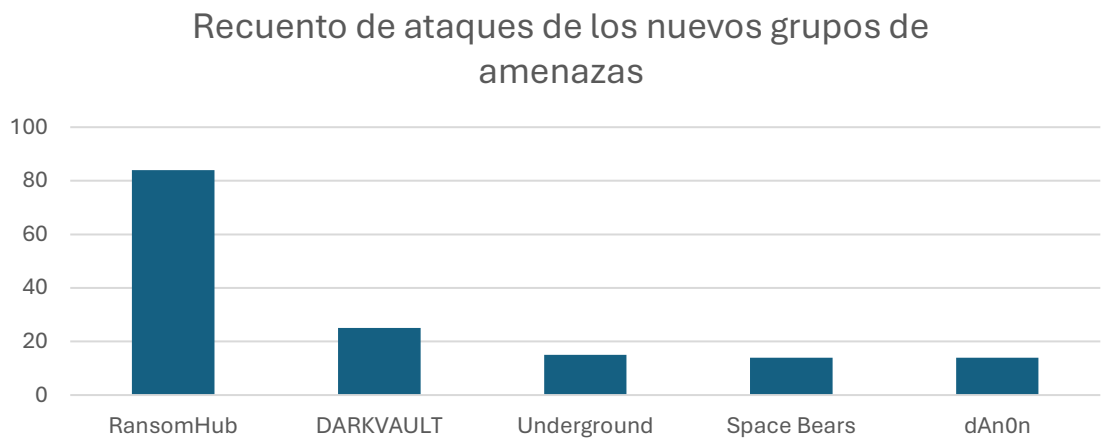


TABLA 1212 – RECUENTO DE ATAQUES DE LOS NUEVOS GRUPOS DE AMENAZAS

RansomHub

RansomHub es un nuevo grupo de ransomware que se ha destacado en el 2024 por sus declaraciones respaldadas por filtraciones de datos. Este grupo presuntamente compuesto por hackers de diversas partes del mundo **persigue objetivos financieros y se abstiene de atacar a naciones como Cuba, Corea del Norte y China, así como a organizaciones sin fines de lucro**. A pesar de su enfoque global, sus operaciones recuerdan a las de los grupos de ransomware rusos tradicionales, compartiendo similitudes en las empresas atacadas y en su postura hacia naciones aliadas a **Rusia**. RansomHub opera como un grupo de Ransomware como servicio (RaaS), colaborando con afiliados y estableciendo pautas estrictas para ellos. Los afiliados deben cumplir con los acuerdos establecidos, y cualquier incumplimiento resulta en la prohibición y terminación de la colaboración. El grupo asegura que proporcionará un descifrador gratuito a las víctimas si el afiliado no lo hace tras recibir el pago o si se dirige a una organización prohibida. RansomHub recluta afiliados del foro **RAMP** y usa cepas de **ransomware ESXi** reescritas en **Golang**, capaces de cifrar datos antes de exfiltrarlos.

DARKVAULT

DarkVault es una comunidad en línea autoproclamada y un grupo de ransomware exclusivo que participa en diversas actividades ilegales como, realizar *doxing*, desfiguración de sitios web, creación de malware, estafas, spam y fraudes. Aunque algunos informes sugieren que **DarkVault** podría ser parte de **LockBit** o estar afiliado a este grupo debido a la similitud de su sitio de filtración de datos (DLS) con el de **LockBit 3.0**, no hay pruebas concluyentes de esta relación. El grupo tiene dos páginas principales: una para publicar víctimas de supuestos ataques de ransomware o exfiltración de datos y otra que detalla

sus actividades ilegales. Sin embargo, fuera de las víctimas publicadas, su DLS y su canal de Telegram carecen de información adicional.

Underground

Underground Team es un nuevo grupo de ransomware que cifra los archivos en las máquinas afectadas y, aunque el ransomware que usan cifra los archivos, las extensiones de los archivos afectados permanecen inalteradas. El grupo de ransomware tiene su sitio de negociación en la red TOR, donde las víctimas pueden hablar con el atacante sobre los detalles del rescate. La URL del sitio TOR está incluida en la nota de rescate **"!!readme!!!.txt"** junto con información adicional sobre dónde el atacante afirma haber exfiltrado la información y el tipo de información. La nota de rescate también afirma que el atacante liberará los datos robados a menos que se pague el rescate en un plazo de tres días. El atacante también afirma estar dispuesto a ayudar a las víctimas a mejorar la seguridad de su red.

Space Bears

SpaceBears es un nuevo grupo en la tendencia de los intermediarios de datos, que ha ganado relevancia recientemente. Se sospecha que el grupo está localizado en Moscú, Rusia y ha reclamado varios ciberataques de alto perfil, mostrando supuestas tácticas avanzadas. En su sitio de filtración de datos (DLS), **SpaceBears** enumera empresas que han filtrado datos confidenciales, incluyendo credenciales de inicio de sesión, propiedad intelectual y datos personales y financieros. Estos grupos utilizan una estrategia de extorsión, presionando a compañías de seguros y preocupando a los clientes para obtener ingresos a partir de los datos comprometidos. El grupo ofrece instrucciones en su DLS para aquellos que creen que sus datos han sido comprometidos, afirmando que, tras recibir el pago, eliminarán la publicación, borrarán los datos de sus servidores y proporcionarán una herramienta de descifrado para los archivos "encriptados". También ofrecen orientación sobre cómo prevenir futuros ataques similares.

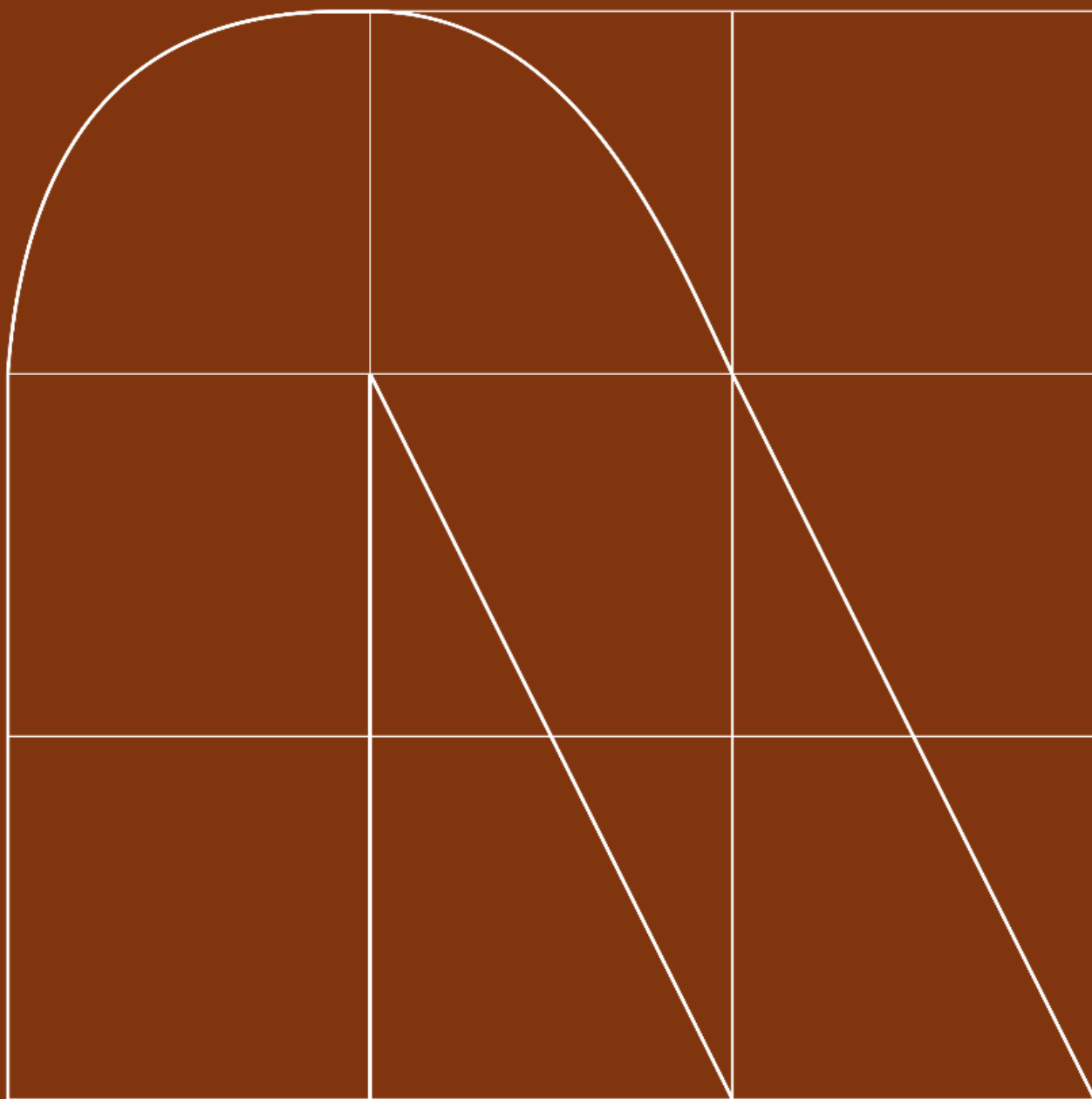
dAn0n

En abril de 2024, surgió el **dAn0n Hacker Group**, que, aunque etiquetado por algunas fuentes como un grupo de ransomware, parece operar más como un intermediario de datos. Han anunciado múltiples víctimas desde marzo hasta finales de mayo, y sus sitios de filtración de datos en clearnet y TOR están activos. Algunas fuentes indican que **dAn0n** participa tanto en la intermediación de datos como en ataques de ransomware, utilizando correos de phishing para el acceso inicial y desplegando ransomware personalizado y scripts ofuscados para ejecutar su carga útil. Emplean tácticas de escalada de privilegios y evasión de defensas para mantener la persistencia y evitar la detección. No obstante, hasta ahora no se ha encontrado evidencia concreta de ransomware o técnicas específicas que respalden estas afirmaciones.

NTT DATA

Técnicas, Tácticas y Procedimientos

(TTPs)



5. Técnicas, Tácticas y Procedimientos (TTPs)

5.1. Descripción de las TTPs más comunes utilizadas por los cibercriminales

Mientras que las TTPs de algunos Actores de Amenazas se mantienen constantes a lo largo del tiempo, como la gran dependencia de la ingeniería social como medio para afianzarse en una organización objetivo o comprometer el dispositivo de un individuo, otros han renovado sus herramientas y ampliado el alcance de sus actividades. Estas revisiones semestrales periódicas pretenden destacar las técnicas más significativas y utilizadas relacionados con los grupos APT.

MITRE ATT&CK ID	DESCRIPCIÓN
T1566 - Phishing	Los adversarios pueden enviar mensajes de phishing para obtener acceso a los sistemas de las víctimas. Todas las formas de phishing son ingeniería social que se envían electrónicamente. El phishing puede ser selectivo, conocido como spear phishing. En el spear phishing, el adversario se dirige a una persona, empresa o industria específica. En términos más generales, los adversarios pueden realizar phishing no selectivo, como campañas de spam masivo de malware. Los adversarios pueden enviar a las víctimas correos electrónicos que contienen archivos adjuntos o enlaces maliciosos, generalmente para ejecutar código malicioso en los sistemas de las víctimas. **Mitigaciones:** • Los antivirus pueden poner en cuarentena automáticamente los archivos sospechosos. • Realizar auditorías o análisis de sistemas, permisos, software inseguro, configuraciones inseguras, etc. para identificar posibles debilidades. • Los sistemas de prevención de intrusiones en la red y los sistemas diseñados para analizar y eliminar archivos adjuntos o enlaces de correo electrónico malicioso se pueden utilizar para bloquear la actividad. • Determinar si ciertos sitios web o tipos de archivos adjuntos (p. ej., .scar, .exe, .pif, .cpl, etc.) que se pueden usar • para el phishing son necesarios para las operaciones comerciales y considere bloquear el acceso si la actividad no se puede monitorear bien o si representa un riesgo significativo. • Usar mecanismos de autenticación de correo electrónico y anti-spoofing para filtrar mensajes según controles de validez del dominio del remitente (usando SPF) e integridad de los mensajes (usando DKIM). • Se puede capacitar a los usuarios para que identifiquen técnicas de ingeniería social y correos electrónicos de phishing. **Referencias:** • https://cybersecuritynews.com/facebook-ad-phishing-attack/ • https://cybersecuritynews.com/greatness-paas-tool-microsoft-365/ • https://cybersecuritynews.com/telegram-know-secure-messaging/ • https://gbhackers.com/cryptochameleon-kit/ • https://gbhackers.com/flyingyeti-winrar-vulnerability-malware-attacks
T1059 - Intérprete de comandos y scripts	Los adversarios pueden abusar de los intérpretes de comandos y secuencias de comandos para ejecutar comandos, secuencias de comandos o archivos binarios. Estas interfaces y lenguajes proporcionan formas de interactuar con los sistemas informáticos y son una característica común en muchas plataformas diferentes. **Mitigaciones:** • Se puede utilizar un antivirus para poner en cuarentena automáticamente los archivos sospechosos. • En Windows 10, habilite las reglas de reducción de superficie de ataque (ASR) para evitar que los scripts de Visual Basic y JavaScript ejecuten contenido descargado potencialmente malicioso. • Cuando sea posible, solo permitir la ejecución de scripts firmados. • Deshabilitar o eliminar los intérpretes o shells innecesarios o no utilizados.

	• Usar el control de aplicaciones cuando sea apropiado. Por ejemplo, el modo de lenguaje restringido de PowerShell • se puede utilizar para restringir el acceso a elementos de lenguaje sensibles o peligrosos, como los que se utilizan para ejecutar archivos o API de Windows arbitrarios (p. ej., Add-Type). • Cuando sea necesario PowerShell, considerar restringir la política de ejecución de PowerShell a los administradores. • Las extensiones de bloqueo de scripts pueden ayudar a prevenir la ejecución de scripts y archivos HTA que pueden usarse comúnmente durante el proceso de explotación. **Referencias:** • https://cybersecuritynews.com/poc-exploit-fortisiem/ • https://cybersecuritynews.com/tp-link-archer-c5400x-router-flaw-remote-hack/ • https://cybersecuritynews.com/winrar-flaw-deceive-users/ • https://gbhackers.com/hackers-microsoft-access-malware/ • https://gbhackers.com/social-engineering-black-basta-ransomware
T1203 – Explotación para ejecución del cliente	Los adversarios pueden explotar las vulnerabilidades del software en las aplicaciones cliente para ejecutar código. Las vulnerabilidades pueden existir en el software debido a prácticas de codificación no seguras que pueden conducir a un comportamiento imprevisto. Los adversarios pueden aprovechar ciertas vulnerabilidades a través de la explotación dirigida con el propósito de ejecución de código arbitrario. A menudo, los exploits más valiosos para un conjunto de herramientas ofensivas son aquellos que se pueden utilizar para obtener la ejecución de código en un sistema remoto porque se pueden utilizar para obtener acceso a ese sistema. Los usuarios esperarán ver archivos relacionados con las aplicaciones que usaron comúnmente para trabajar, por lo que son un objetivo útil para la investigación y el desarrollo de exploits debido a su gran utilidad. **Mitigaciones:** • Se pueden utilizar entornos aislados de navegador para mitigar parte del impacto de la explotación, pero aún pueden existir escapes de entornos aislados. Otros tipos de virtualizaciones y microsegmentación de aplicaciones también pueden mitigar el impacto de la explotación del lado del cliente. Aún pueden existir los riesgos de exploits adicionales y debilidades en la implementación. Las aplicaciones de seguridad que buscan el comportamiento utilizado durante la explotación, como Windows Defender Exploit Guard (WDEG) y Enhanced Mitigation Experience Toolkit (EMET), se pueden utilizar para mitigar algunos comportamientos de explotación. La comprobación de la integridad del flujo de control es otra forma de identificar y detener potencialmente la ocurrencia de una explotación de software. • Muchas de estas protecciones dependen de la arquitectura y del binario de la aplicación de destino para su compatibilidad. **Referencias:** • https://cybersecuritynews.com/chrome-security-update-125/ • https://cybersecuritynews.com/hackers-advertising-pulse-connect/
T1219 - Herramientas de acceso remoto	Un adversario puede utilizar software legítimo de soporte de escritorio y acceso remoto para establecer un canal interactivo de comando y control para atacar sistemas dentro de redes. Estos servicios, como VNC, Team Viewer, AnyDesk, ScreenConnect, LogMein, AmmyyAdmin, y otras herramientas de monitoreo y administración remotas (RMM), se utilizan comúnmente como software legítimo de soporte técnico y pueden ser permitidos por el control de aplicaciones dentro de un entorno objetivo. **Mitigación:** • Configurar correctamente los firewalls, firewalls de aplicaciones y servidores proxy para limitar el tráfico saliente a sitios y servicios utilizados por herramientas de acceso remoto. • Los sistemas de prevención y detección de intrusiones de red que utilizan firmas de red también pueden evitar el tráfico a estos servicios. • Usar listas blancas de aplicaciones para mitigar el uso y la instalación de software no aprobado. **Referencias:** • https://attack.mitre.org/techniques/T1219/ • https://gbhackers.com/fbi-cisa-warns-alphv-blackcat-ransomware/ • https://gbhackers.com/hijacking-connectwise-screenconnect-server/ • https://packetstormsecurity.com/news/view/35567/ConnectWise-Exploit-Could-SpurRansomware-Free-For-All.html

	• https://services.google.com/fh/files/misc/connectwise-screenconnect-remediationhardening-guide.pdf • https://thehackernews.com/2024/02/fbi-warns-us-healthcare-sector-of.html
T1486 – Datos encriptados para impactar	Los adversarios pueden cifrar datos en sistemas de destino o en una gran cantidad de sistemas en una red para interrumpir la disponibilidad de los recursos del sistema y de la red. Pueden intentar hacer que los datos almacenados sean inaccesibles cifrando archivos o datos en unidades locales y remotas y reteniendo el acceso a una clave de descifrado. Esto puede hacerse para extraer una compensación monetaria de una víctima a cambio de un descifrado o una clave de descifrado (ransomware) o para hacer que los datos sean permanentemente inaccesibles en casos en los que la clave no se guarde o transmita. **Mitigación** • Considerar implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar copias de seguridad de datos y probarlas periódicamente que se puedan usar para restaurar los datos de la organización. • En algunos casos, los medios para descifrar archivos afectados por una campaña de ransomware se hacen públicos. Investigue fuentes confiables para obtener publicaciones públicas de herramientas/claves de descifrado para revertir los efectos del ransomware. • Identificar software potencialmente malicioso y audite o bloquee el software mediante el uso de herramientas de listas blancas como AppLocker o políticas de restricción de software cuando sea adecuado. • La ejecución consiste en técnicas que dan como resultado la ejecución de código controlado por el adversario en un sistema local o remoto. Las técnicas que ejecutan código malicioso a menudo se combinan con técnicas de todas las demás tácticas para lograr objetivos más amplios, como explorar una red o robar datos. Por ejemplo, un adversario podría usar una herramienta de acceso remoto para ejecutar un script de PowerShell que realiza el descubrimiento remoto del sistema. **Referencias:** • https://attack.mitre.org/techniques/T1486/ • https://gbhackers.com/black-basta-ransomware-decryptor/ • https://gbhackers.com/hackers-hijacking-ms-sql-servers/ • https://gbhackers.com/kasseika-ransomware-kill-antivirus/ • https://gbhackers.com/phobos-ransomware-office-document/ • https://packetstormsecurity.com/news/view/35385/Babuk-Tortilla-Ransomware-DecryptedAfter-Hackers-Arrest.html

TABLA 1313 - TTPS MAS USADAS POR LOS ACTORES MALICIOSOS

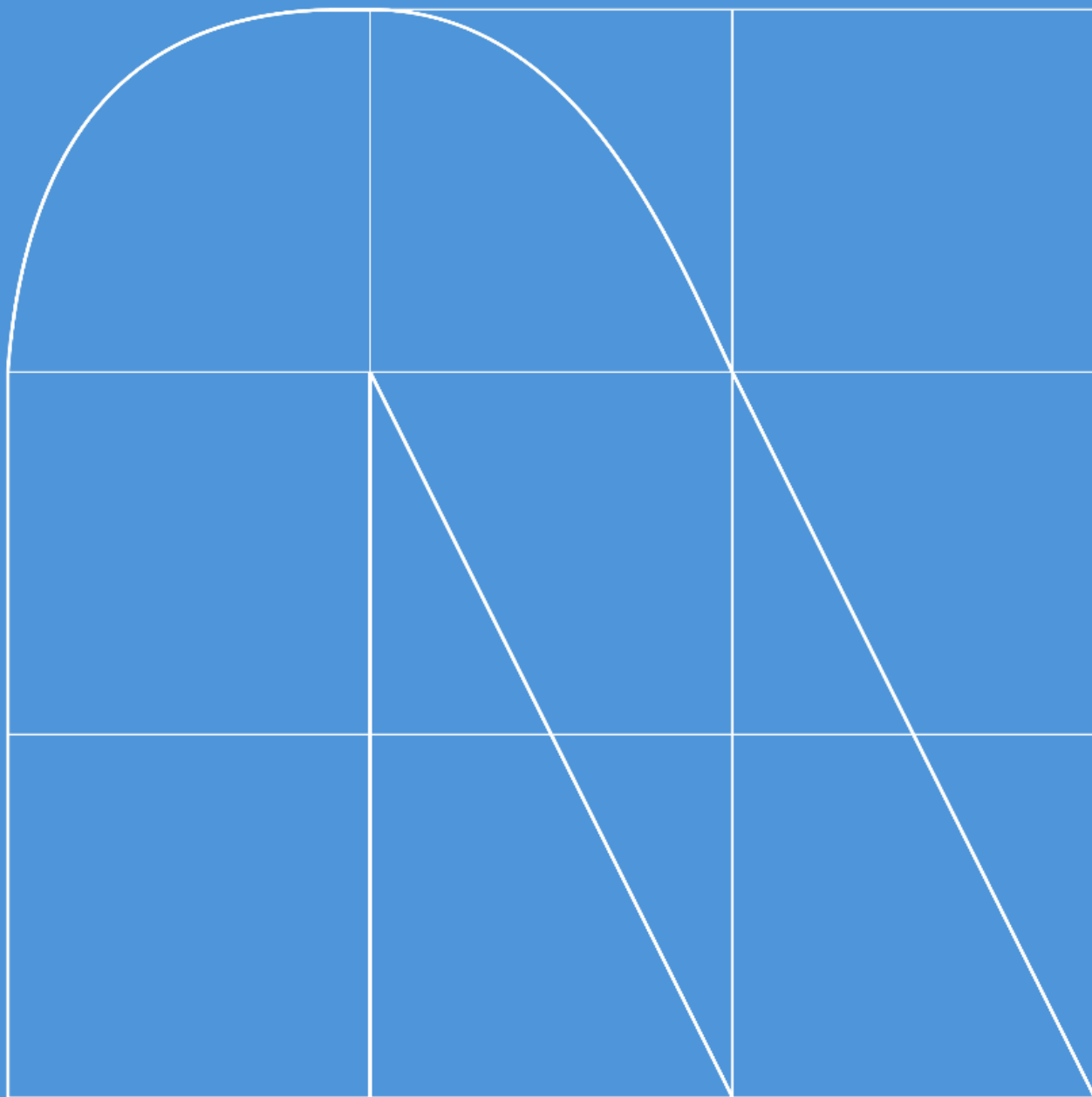
Conforme los Actores de Amenazas continúan adoptando métodos de ataque más furtivos e innovadores, se observa **la utilización activa de aproximadamente dos tercios de las técnicas del marco MITRE ATT&CK**. Entre estas, la evasión de defensas y la inyección de procesos emergen como tácticas predominantes.

El **phishing mantuvo su posición como el principal vector de acceso inicial** en diversos tipos de incidentes de amenazas, resaltando especialmente la vulneración mediante correos electrónicos de phishing.

Además, durante 2024, se registró un **incremento en los ataques que comenzaron con técnicas de ingeniería social**. También se observó un aumento en los incidentes iniciados por Actores de Amenazas que explotaron aplicaciones públicas, como las redes privadas virtuales Adaptive Security Appliance (ASA) de Cisco y las herramientas de gestión remota ScreenConnect. **Los ataques dirigidos a vulnerabilidades conocidas mostraron una mayor probabilidad de culminar en incidentes de ransomware.**

NTT DATA

Tendencias de Vulnerabilidades



6. Vulnerabilidades

En la siguiente sección se realiza un análisis de las principales vulnerabilidades publicadas a lo largo del primer semestre de este año 2024, detallando aquellas que han tenido un mayor impacto en los sistemas de información.

6.1. Análisis de tendencias

En términos de criticidad, las CVE clasificadas como **críticas** y **altas** representan una parte significativa del total, repercutiendo en un aumento de ataques de **ejecución remota de código**, **denegación de servicio** o **escalada de privilegios**.

Como consecuencia, se espera una respuesta rápida por parte de las organizaciones e instituciones públicas para enfrentarse a dichas amenazas, aplicando las soluciones ofrecidas por los proveedores de las tecnologías afectadas.

Como se puede observar a continuación, las vulnerabilidades de criticidad **media** destacan sobre el resto, pero esto no debe desviar la atención sobre las vulnerabilidades **altas** y **críticas** identificadas, ya que estas son las que mayor impacto negativo pueden ocasionar en una organización o sistema.

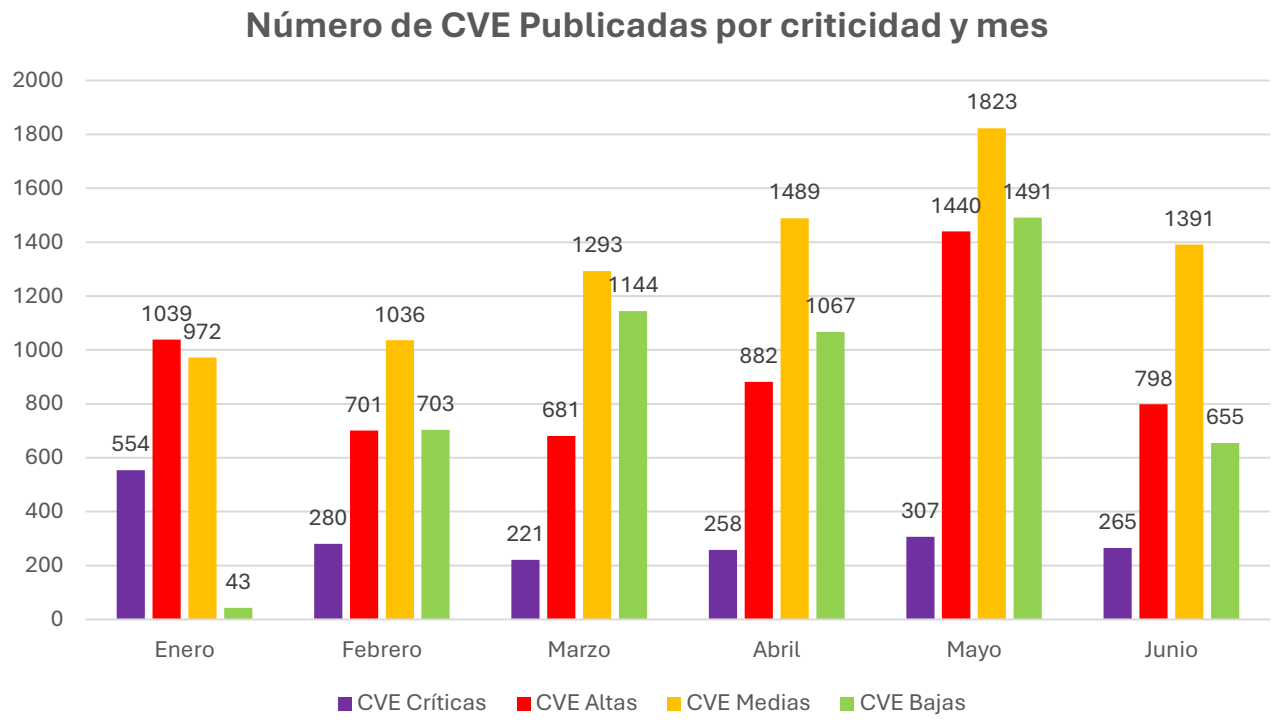


TABLA 1414 - RECUENTO DE CVE POR CRITICIDAD Y MES

Se puede observar una fuerte predominación en la publicación de vulnerabilidades referentes a **Cross-Site-Scripting** (**XSS**), esto es preocupante debido a que se trata de una de las vulnerabilidades con mayor riesgo para un aplicativo, ya que explotando este tipo de vulnerabilidades se podría llegar a obtener las cookies de sesión, realizar suplantaciones de identidad, realizar redirecciones maliciosas, acceso a información sensible, ejecutar acciones no deseadas, entre otras.

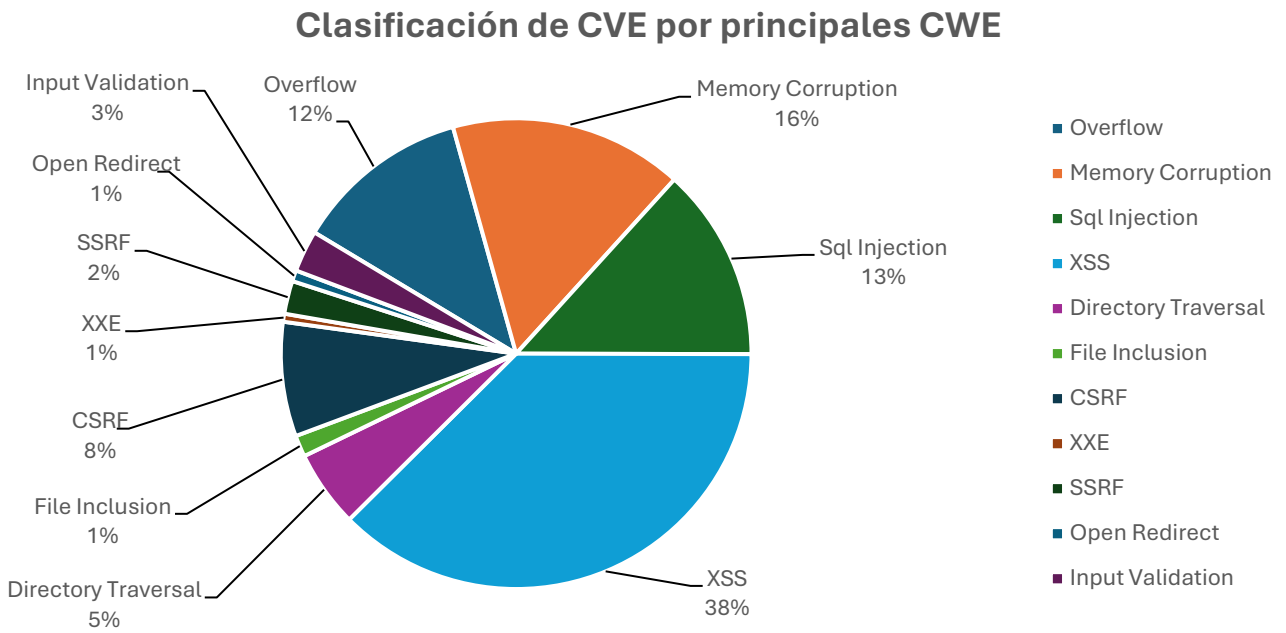


TABLA 1515 - CLASIFICACIÓN DE CVE POR PRINCIPALES CWE (COMMON WEAKNESS ENUMERATION)

6.2. Vulnerabilidades más críticas

A continuación, se indica una lista con las vulnerabilidades publicadas durante el año 2024 que se han considerado más críticas según su CVSS v3:

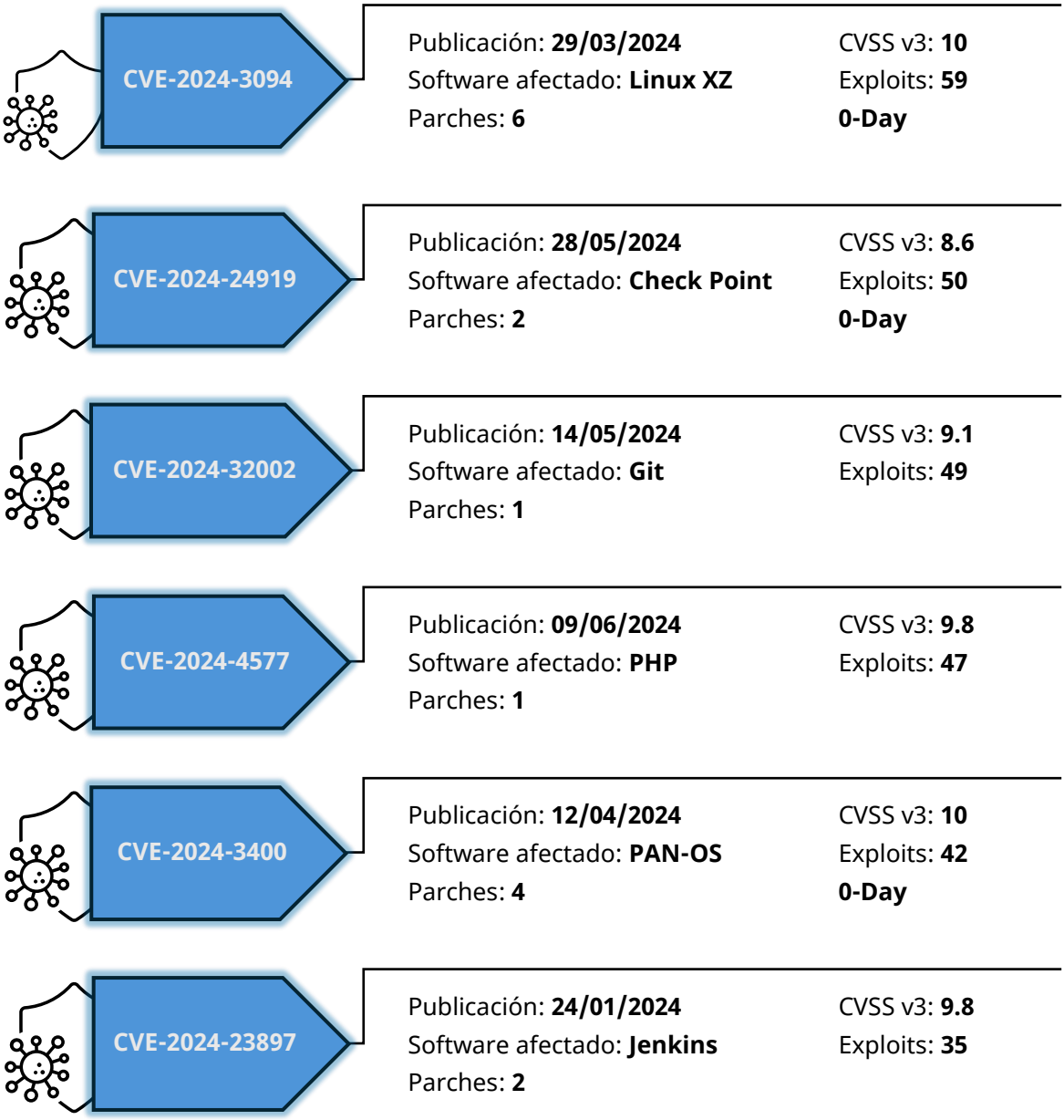
CVE	CVSS v3	DESCRIPCIÓN (ALCANCE)	SOFTWARE AFECTADO	EXPLOITS Y PARCHES
ENERO				
CVE-2024-23897	**9.8 – Crítica**	Vulnerabilidad que permite a atacantes no autenticados **leer archivos arbitrarios** en el sistema de archivos del controlador Jenkins.	**Jenkins** 2.441 y anteriores. **LTS** 2.426.2 y anteriores.	35 exploits. 2 parches.
CVE-2024-0204	**9.8 – Crítica**	La omisión de autenticación permite a un usuario no autorizado **crear un usuario administrador** a través del portal de administración.	GoAnywhere MFT de **Fortra** anterior a 7.4.1.	9 exploits. 1 parche.
CVE-2024-21887	**9.1 – Crítica**	Vulnerabilidad de inyección de comandos en los componentes web que permite a un administrador autenticado **enviar solicitudes** especialmente diseñadas **y ejecutar comandos arbitrarios** en el dispositivo.	**Ivanti Connect Secure** (9.x, 22.x) e **Ivanti Policy Secure** (9.x, 22.x).	0-Day. 10 exploits. 2 parches.
FEBRERO				
CVE-2024-21762	**9.8 – Crítica**	Una **escritura fuera de los límites** que permite a un atacante **ejecutar código o comandos no autorizados** a través de peticiones específicamente diseñadas.	**Fortinet**: **FortiOS** versiones 7.4.0 a 7.4.2, 7.2.0 a 7.2.6, 7.0.0 a 7.0.13, 6.4.0 a 6.4.14, 6.2.0 a 6.2.15, 6.0.0 a 6.0.17. **FortiProxy** versiones 7.4.0 a 7.4.2, 7.2.0 a 7.2.8, 7.0.0 a 7.0.14, 2.0.0 a 2.0.13, 1.2.0 a 1.2.13, 1.1.0 a 1.1.6, 1.0.0 a 1.0.7.	0-Day. 8 exploits. 2 parches.
CVE-2024-1709	**9.8 – Crítica**	Vulnerabilidad de **elusión de autenticación** mediante una ruta o canal alternativo, que puede permitir a un atacante el acceso directo a **información confidencial o sistemas críticos**.	**ConnectWise ScreenConnect** 23.9.7 y anteriores.	0-Day. 17 exploits. 4 parches.
MARZO				
CVE-2023-48788	**9.8 – Crítica**	Una neutralización incorrecta de elementos especiales utilizados en un comando SQL ('**SQL injection**') que permite a un atacante **ejecutar código o comandos no autorizados** a través de paquetes especialmente diseñados.	**Fortinet FortiClientEMS** versión 7.2.0 a 7.2.2 y 7.0.1 a 7.0.10.	2 exploits. 1 parche.
CVE-2024-27198	**9.8 – Crítica**	Vulnerabilidad que permite **eludir la autenticación para realizar acciones de administración**.	**JetBrains**: Servidor de CI/CD (**TeamCity**), versión 2023.11.4 y anteriores.	13 exploits. 1 parche.
ABRIL				
CVE-2024-3400	**10 – Crítica**	Vulnerabilidad de **creación de archivos arbitrarios** en la función **GlobalProtect** que permite la inyección de comandos con **privilegios de raíz en el cortafuegos**.	**Palo Alto Networks**: Algunas versiones específicas de **PAN-OS** 11.1, 11.o y 10.2.	0-Day. 42 exploits. 4 parches.
CVE-2024-4040	**10 – Crítica**	Vulnerabilidad de inyección de plantilla del lado del servidor que permite a atacantes remotos no autenticados **leer archivos del sistema de archivos fuera del Sandbox VFS**, saltarse la autenticación para obtener **acceso**	**CrushFTP** en todas las versiones anteriores a 10.7.1 y 11.1.0.	0-Day. 15 exploits. 4 parches.

		administrativo y realizar la **ejecución remota de código en el servidor**.		
CVE-2024-3273 CVE-2024-3272	**9.8 – Crítica**	Se ve afectada una función desconocida del archivo **/cgi-bin/nas_sharing.cgi del componente HTTP GET Request Handler**. La manipulación del sistema de argumentos conduce a la **inyección de comandos**. Es posible lanzar el ataque de forma **remota**.	**D-Link DNS-320L**, **DNS-325, DNS-327L** y **DNS-340L** hasta 20240403. **NOTA**: Esta vulnerabilidad sólo afecta a productos que ya no reciben soporte por parte del mantenedor.	11 exploits. 1 parche.
MAYO				
CVE-2024-4358	**9.8 – Crítica**	Vulnerabilidad de omisión de autenticación que permite, en IIS, que un atacante no autenticado pueda **obtener acceso a la funcionalidad restringida de Telerik Report Server**.	**Progress Telerik Report Server**, versión 2024 Q1 (10.0.24.305) y anteriores.	7 exploits. 1 parche.
CVE-2024-4671	**9.6 – Crítica** **NOTA:** Gravedad de seguridad de Chromium: Alta.	Vulnerabilidad **Use-Afer-Free** (UAF) que permite a un atacante remoto que hubiera comprometido el proceso del renderizado realizar potencialmente un **escape de sandbox a través de una página HTML crafteada**.	Componente **Visuals** de **Google Chrome** anterior a 124.0.6367.201.	0-Day. 2 parches.
JUNIO				
CVE-2024-4577	**9.8 – Crítica**	Vulnerabilidad que permite a un usuario malicioso **pasar opciones al binario PHP** que se está ejecutando, y así revelar el código fuente de los scripts, ejecutar código PHP arbitrario en el servidor, etc. **NOTA**: cuando se usa Apache y PHP-CGI en Windows, si el sistema está configurado para usar ciertas páginas de código, Windows puede usar el comportamiento "Best-Fit" para reemplazar caracteres en la línea de comandos dados a funciones Win32 API. El módulo PHP CGI puede malinterpretar esos caracteres como opciones PHP.	**PHP**: Versiones 8.1.* anteriores a 8.1.29. Versiones 8.2.* anteriores a 8.2.20. Versiones 8.3.* anteriores a 8.3.8.	46 exploits. 1 parche.
CVE-2024-5806	**9.1 - Crítica**	Vulnerabilidad de autenticación incorrecta en Progress MOVEit Transfer (Módulo SFTP) puede conducir a Authentication Bypass	**MOVEit Transfer:** desde 2023.0.0 antes de 2023.0.11 desde 2023.1.0 antes de 2023.1.6 desde 2024.0.0 antes de 2024.0.2	2 exploits.

TABLA 1616 - VULNERABILIDADES MAS CRITICAS IDENTIFICADAS EN EL PRIMER SEMESTRE DE 2024

6.3. Vulnerabilidades más explotadas

Algunas de las vulnerabilidades más explotadas por los atacantes a lo largo del semestre han sido las siguientes:



6.4. 0-day detectados o publicados

La tendencia de explotación de vulnerabilidades de día 0 (0-Day) marca un **aumento significativo** en comparación con años anteriores, la explotación activa de estas vulnerabilidades sugiere un aumento en la rapidez con la que los actores maliciosos aprovechan las debilidades de software, afectando a una amplia gama de usuarios y organizaciones.

Como datos destacables son el aumento de **exploits 0-click**, que no requieren interacción del usuario para activarse; la **reutilización de exploits** con ligeras modificaciones (más del 40% de los 0-Day descubiertos son variantes de vulnerabilidades previamente reportadas); y el uso de 0-Day para aumentar el impacto en **ataques ransomware**.

PROVEEDORES DE TECNOLOGÍAS Y ACTIVOS

Entorno al **40%** de 0-Day afectan a **Google** en productos como Chrome, dispositivos Pixel y Android, seguido de un **20%** en **Microsoft**, principalmente en sistemas operativos Windows y aplicaciones Outlook. El resto de las vulnerabilidades de día cero se reparten entre proveedores como **Apple**, **VMware**, **Adobe** o **Apache**.
En cuanto a los activos afectados, los **dispositivos móviles** (Pixel, Android e iOS) van en cabeza (**50%**), así mismo las **aplicaciones de escritorio** (**20%**) y los **servidores** y el sector de **virtualización** (**20%**) también van al alza, remarcando la importancia de la seguridad en aplicaciones de productividad e infraestructuras críticas.

ACTORES DE AMENAZAS

Las principales regiones afectadas por la explotación de vulnerabilidades de día cero son **América del Norte**, **Europa** y **Asia**; Se destaca el grupo de ransomware **Black Basta** (Cardinal o UNC4393), los Actores Amenaza estatales como **APT29** (Rusia) y **APT41** (China) centrados en el espionaje, con objetivos estratégicos como infraestructuras críticas o sectores tecnológicos avanzados y grupos como **Lazarus** enfocado en entidades financieras y organizaciones gubernamentales.

Por último, es común que la exposición pública de detalles técnicos de las vulnerabilidades detectadas, como en eventos como **Pwn2Own Vancouver 2024**, fomente una rápida explotación de estas y genere un mayor número de ataques por parte de Actores Maliciosos.

A continuación, se muestran algunos de los 0-Day destacados del 2024:

CVE-2024-0519	MÚLTIPLES 0-DAY EN IVANTI	CVE-2024-29988
Fallo en el motor V8 de Chrome, explotado para ejecución remota de código y parcheado por Google en enero.	**CVE-2023-46805, CVE-2024-21887, CVE-2024-21893, CVE-2024-21888, CVE-2024-22024** Ejecución remota de comandos, acceso sin autenticación a recursos restringidos y acceso persistente. La CISA destacó su explotación para el robo de credenciales y la evasión de medidas de mitigación.	Omisión de las características de seguridad de la función SmartScreen de Microsoft a partir de exploits en archivos comprimidos.
CWE-787 CWE-125 CWE-119 BUFFER OVERFLOW	**CWE-78, CWE-918, CWE-77, CWE-287, CWE-611**	**CWE-693**

TABLA 1717 - 0-DAY MAS EXPLOTADOS

6.5. Parches de seguridad publicados

Analizando las vulnerabilidades por proveedor, los principales afectados son los que mayor cantidad de productos y servicios tecnológicos ofrecen, siendo Microsoft y Google los más afectados en cuanto a número de vulnerabilidades publicadas.

TABLA 1818 - CVE PUBLICADAS Y EXPLOTADAS POR PROVEEDOR

En lo referente al número de **parches de seguridad publicados** ha seguido una tendencia ascendente, siendo marzo el mes con más soluciones registradas.

Acorde a las vulnerabilidades publicadas por proveedor, **las soluciones ofrecidas por Microsoft y Google van en cabeza**, atendiendo la necesidad de una respuesta rápida para mitigar los ataques a los productos afectados.

Puede apreciarse el esfuerzo por parte de los vendedores y de las empresas para reducir los riesgos de seguridad gracias a la publicación de los parches de seguridad y la aplicación de actualizaciones frecuentes.

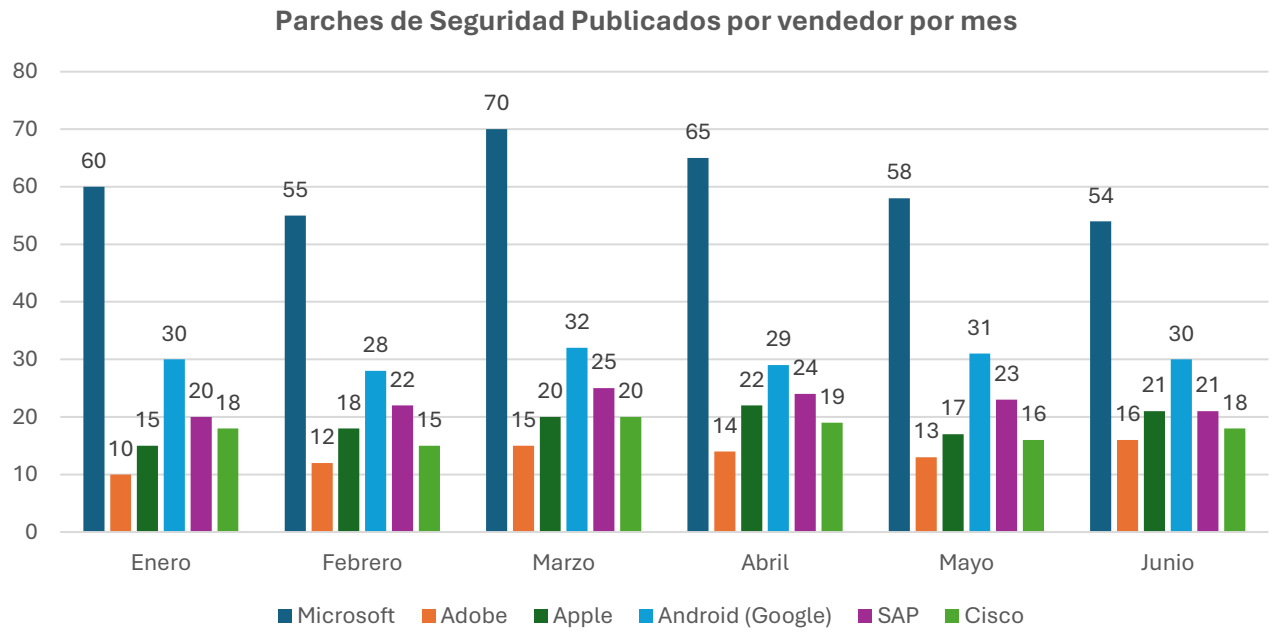


TABLA 1919 - TENDENCIA DE LOS PARCHES DE SEGURIDAD PUBLICADOS POR VENDEDOR POR MES