Informe de los analistas

Managed Detection and Response

kaspersky bring on the future

2023

Contenido

Introducción

En el informe anual de analistas de Managed Detection and Response (MDR), se destacan los resultados del análisis de los incidentes de MDR que identificó el equipo del SOC de Kaspersky.

El objetivo del informe es proporcionar información acerca de las tácticas, técnicas y herramientas más comunes de los atacantes, la naturaleza de los incidentes identificados y su distribución entre los clientes de MDR por ubicación geográfica y sector.

En este informe se responderán las siguientes preguntas:

¿Quiénes son sus posibles atacantes?

¿Cómo operan en la actualidad?

¿Cómo puede detectar su actividad?

Acerca de Kaspersky Managed Detection and Response

Kaspersky MDR proporciona supervisión y detección de amenazas ininterrumpidas para los incidentes identificados, en función de la experiencia y las soluciones tecnológicas de Kaspersky.

Las soluciones de seguridad para endpoints, instaladas del lado del cliente, recopilan y transmiten telemetría, analizada primero mediante tecnologías de aprendizaje automático y, luego, por un equipo de expertos en detección de ataques que emplean reglas de detección especializadas, indicadores de ataque (IoA) y búsqueda manual de amenazas basadas en eventos de telemetría sin procesar. Como resultado de la investigación, pueden asignarse acciones de respuesta según la decisión de los analistas del SOC y, si el usuario de MDR las aprueba, la plataforma de protección en endpoints (EPP) acciona la respuesta. Si no se puede organizar una respuesta automatizada, se brindan recomendaciones para realizar una investigación y una respuesta manuales, con la ayuda de un equipo forense digital.

Figura 1

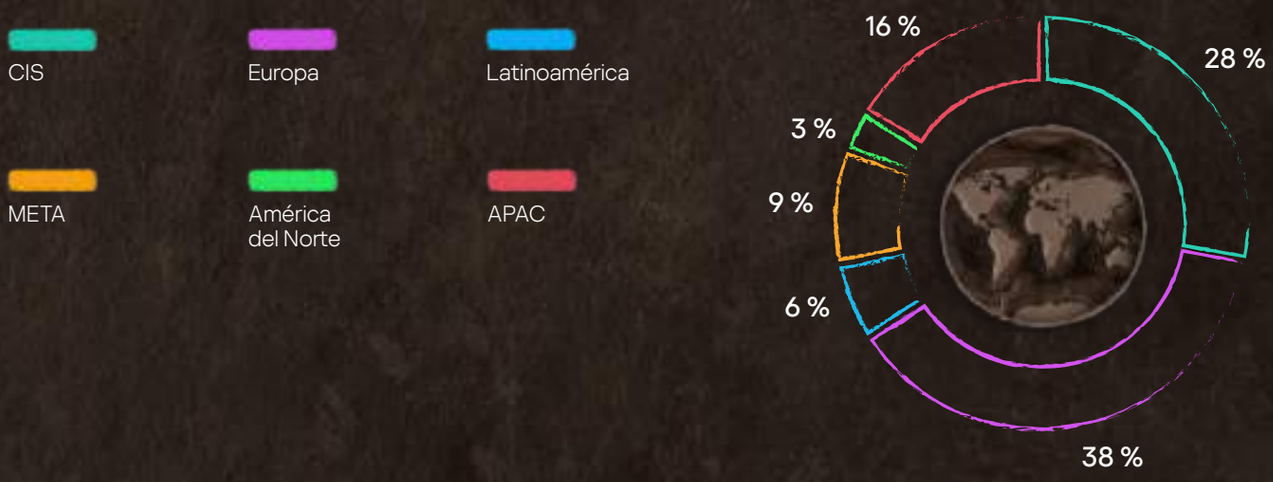
El flujo de trabajo de Kaspersky MDR

Alcance de Kaspersky MDR

Los clientes de Kaspersky MDR están distribuidos por todo el mundo, lo que nos brinda un panorama objetivo de los detalles de los ataques por región.

En el siguiente gráfico, se observa la distribución geográfica de nuestros clientes de MDR.

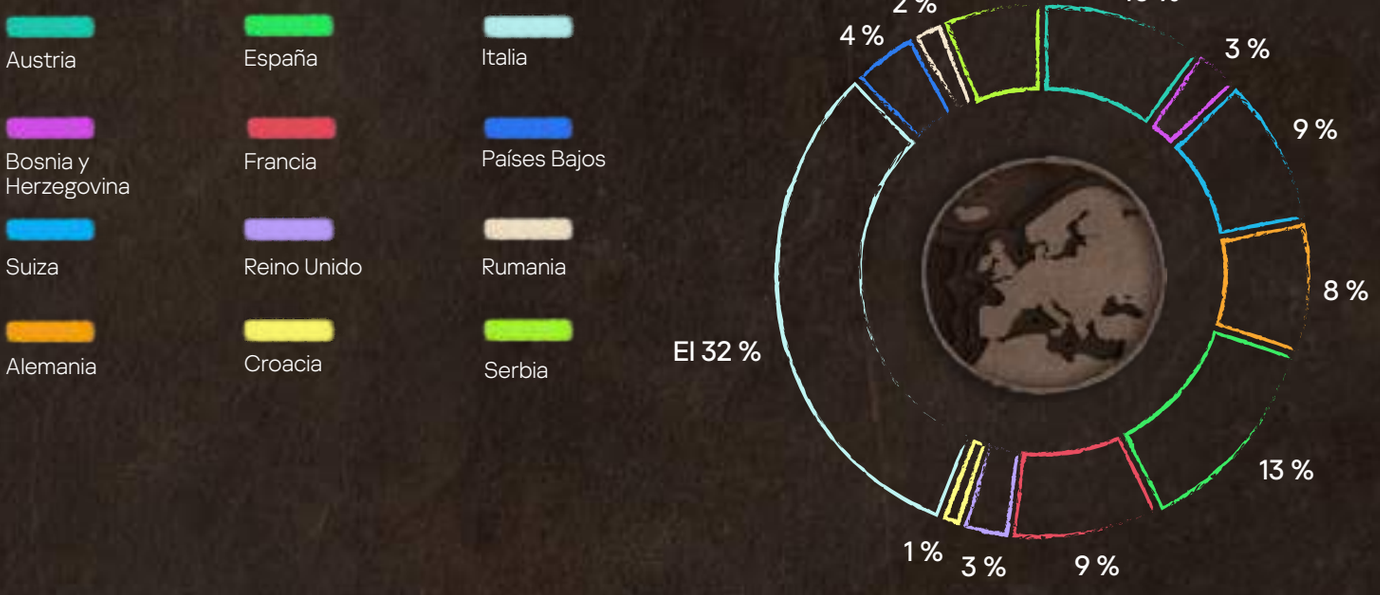
Figura 2 Cobertura global de Kaspersky MDR



En Europa, Kaspersky MDR tiene mayor presencia en Italia, España y Austria.

Figura 3

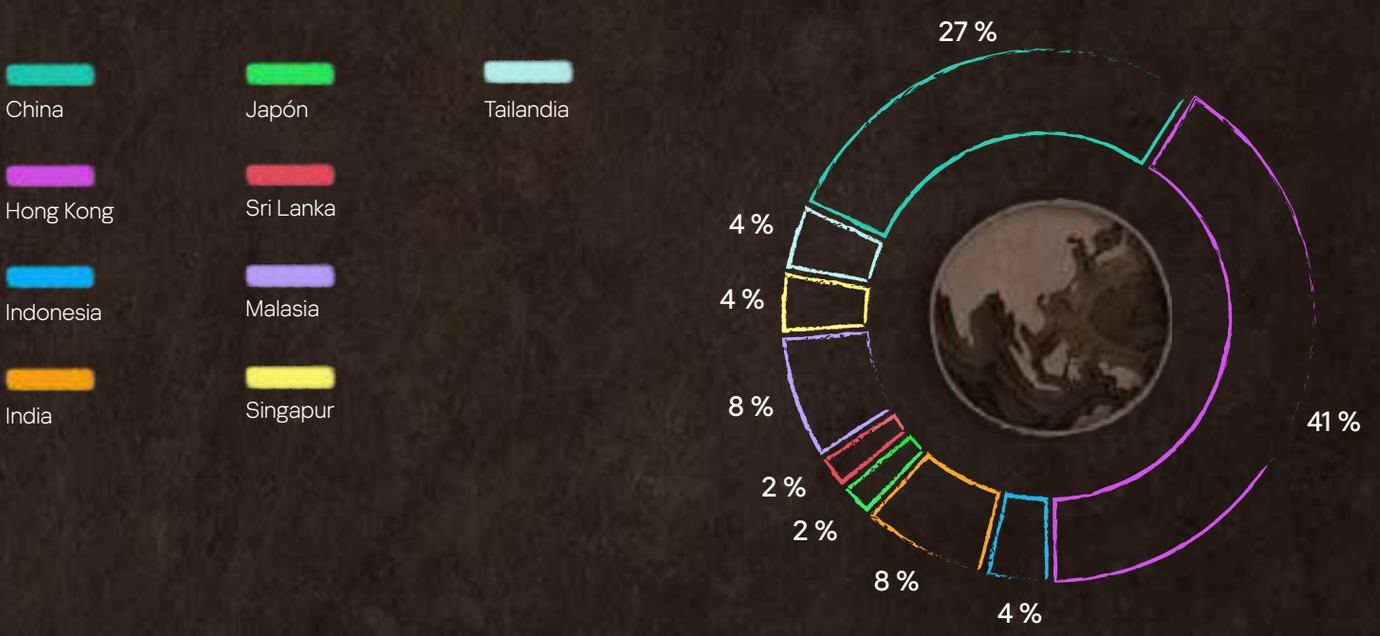
Cobertura de Kaspersky MDR en Europa



En la región de Asia-Pacífico, los líderes son Hong Kong y China.

Figura 4

Cobertura de Kaspersky MDR en la región de Asia-Pacífico

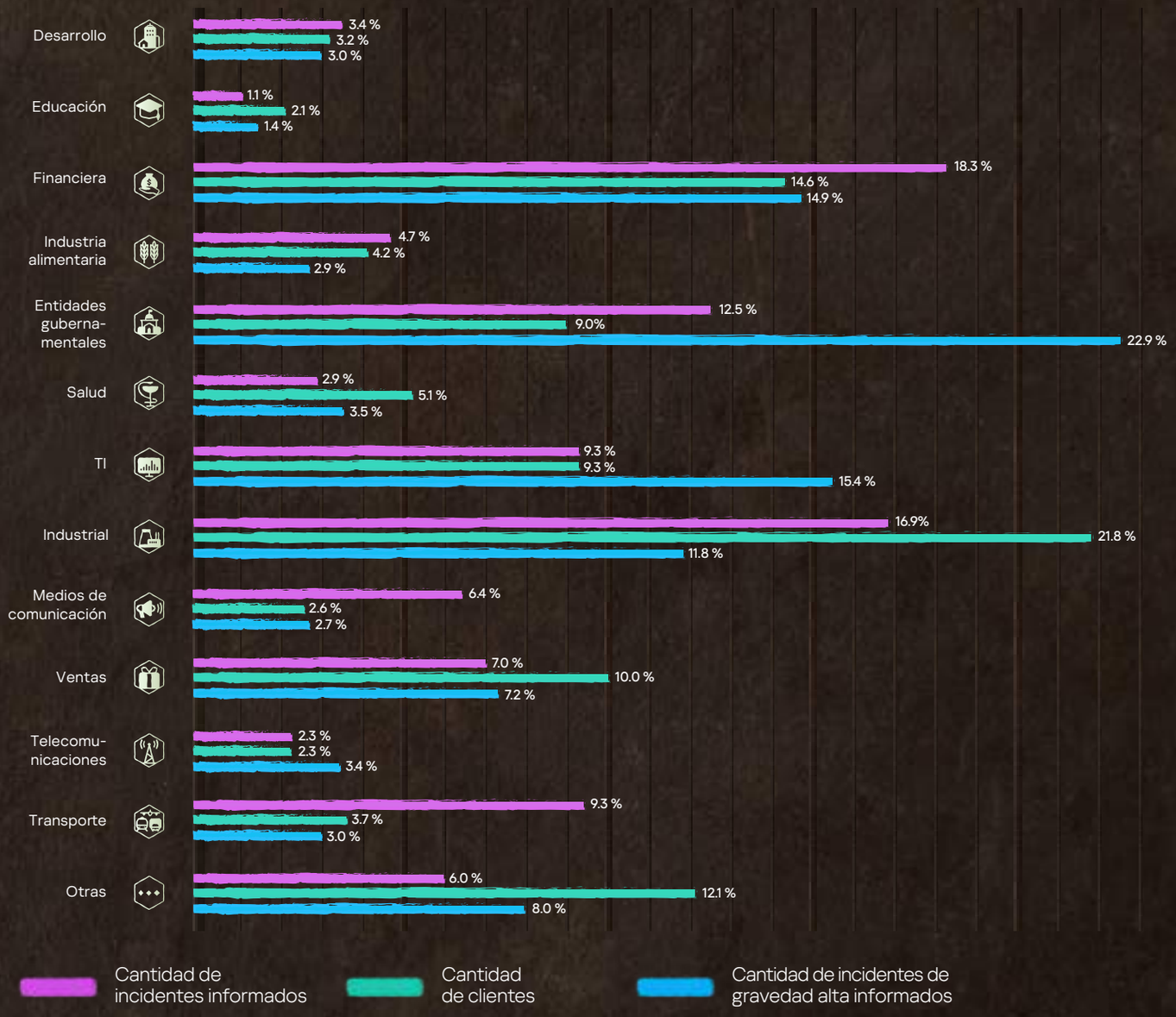


Distribución por sector

En 2023, el equipo de MDR de Kaspersky observó la mayor cantidad de incidentes en el sector financiero (18.3 %), en las empresas industriales (16.9 %) y en entidades gubernamentales (12.5 %).

Figura 5

Segmentos verticales más atacados



El gráfico, por cantidad de clientes, refleja la presencia de MDR en el sector relevante. Si se compara con la distribución por cantidad de incidentes, es posible calcular la frecuencia de los incidentes en dicho sector. Según este indicador, el sector de medios de comunicación se encuentra entre los líderes, en el que el 6.4 % de todos los incidentes se observó en el 2.6 % de los clientes de este sector. Otro de los líderes es el sector de transporte, en el que el porcentaje de incidentes es 9.3 %, con un poco menos del 4 % de clientes.

Cantidad de incidentes

En 2023, la infraestructura de MDR recibió eventos de telemetría todos los días, y después de haberlos procesado, se emitieron alertas de seguridad.

Aproximadamente el 27 % de las alertas emitidas se procesaron con algoritmos basados en aprendizaje automático. El equipo del SOC analizó otro 10 % y consideró que las alertas correspondían a incidentes reales, sobre los cuales se informó a los clientes de Kaspersky MDR a través del portal de Kaspersky MDR.

Figura 6

Embudo del procesamiento de alertas por Kaspersky MDR

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 del SOC disponible. A continuación, el analista procesa la alerta según su gravedad y el tiempo garantizado en el acuerdo de nivel de servicio (SLA) para detectar una amenaza. Si el análisis considera que se trata de un falso positivo[1], se ignora la alerta o se crean filtros globales[2]. De lo contrario, se importa la alerta a un incidente nuevo o existente que, tras una investigación detallada, puede cerrarse como falso positivo o informarse al cliente a través del portal de Kaspersky MDR junto con una respuesta recomendada. Si el cliente está de acuerdo con las respuestas recomendadas, los agentes en el endpoint las implementarán de manera automática.

Tabla 1

Tiempo para detectar un incidente

Gravedad	Tiempo en generar un informe, en minutos	Comentarios
Alta 	36.37 min (2023) frente a 43.75 min (2022) frente a 41.45 min (2021)	En el caso de los incidentes más complejos, se necesita más tiempo para recopilar información adicional y crear una cronología del incidente. En comparación con períodos anteriores[3], este tiempo disminuyó aproximadamente 17 %, lo que puede estar asociado con una reducción en la cantidad de incidentes de gravedad alta en 2023.
Mediana 	32.55 min (2023) frente a 30.92 min (2022) frente a 34.88 min (2021)	El nivel de gravedad más frecuente. La mayoría de estos incidentes son una consecuencia de la actividad de malware. En comparación con períodos anteriores, este tiempo disminuyó levemente, lo que se debe al aumento relativo de la cantidad de incidentes de gravedad media y baja.
Baja 	48.01 min (2023) frente a 34.15 min (2022) frente a 40.24 min (2021)	Los incidentes con el nivel de gravedad más bajo, la mayoría de los cuales estaban relacionados con las consecuencias de software potencialmente no deseado, pasaron más tiempo en cola antes de que los analice un miembro del equipo del SOC.

1 Diferenciamos dos tipos principales de falsos positivos: de infraestructura (donde la lógica para crear una alerta es correcta, pero debido a la configuración de la infraestructura del cliente, esta alerta no es consecuencia de un incidente y está relacionada con actividad legítima) y tecnológica (donde la lógica para crear una alerta no funciona de forma adecuada y necesita ajustes)

2 El filtro de cliente es el ajuste de la lógica de detección para la infraestructura de un cliente específico. Estos filtros se crean para corregir falsos positivos relativos a la infraestructura. El filtro global es el ajuste general de la lógica de detección para todos los clientes en el caso de falsos positivos tecnológicos

3 Managed Detection and Response en 2021 Managed Detection and Response en 2022

Principales hallazgos

Más de dos incidentes de gravedad alta todos los días

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

APT
-25 % (2023)
frente a 30 % (2022)
frente a 41 % (2021)

Evaluación de seguridad
-20 % (2023)
frente a 19 % (2022)
frente a 18 % (2021)

Delito[4]
-12 % (2023)
frente a 26 % (2022)
frente a 14 % (2021)

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

powershell.exe

rundll32.exe

msiexec.exe

Las técnicas de MITRE ATT&CK más populares:

T1566: Phishing
(TA0001: Acceso inicial)

T1210: Abuso de servicios remotos
(TA0008: Movimiento lateral)

T1098: Manipulación de cuenta
(TA0003: Manipulación de cuenta)

Sectores con la mayor cantidad de incidentes informados:

Finanzas
-18 %

Industrial
-17 %

Entidades gubernamentales
-12 %

El 74 % (2023) de los incidentes frente al 72 % (2022) se solucionaron correctamente después de recibir la primera alerta de seguridad relevante

Distribución de incidentes informados por gravedad:

Alta: 7 %

Media: 63 %

Baja: 30 %

Tiempo medio para generar un informe:

Gravedad alta del incidente
36.37 min

Gravedad media del incidente
32.55 min

Gravedad baja del incidente
48.01 min

Regiones clave por cantidad de clientes:

- Europa: 38 %
- Rusia y la Comunidad de Estados Independientes: 28 %
- APAC: 16 %

Países europeos clave:

- Italia: 2 %
- España: 13 %
- Austria: 10 %

4 Ataque llevado a cabo con malware sin intervención visible de una persona humana

Recomendaciones

De doscientos LOLBins[5], se encontraron 68 en incidentes el año pasado. El uso de LOLBins se observó en casi 1 de cada 10 incidentes y, si tenemos en cuenta solo los incidentes de gravedad alta, se observó en casi un tercio de ellos. Los LOLBins más populares fueron powershell.exe y rundll32.exe, que se utilizaron en el 2 % de todos los incidentes y en el 12 % de los incidentes críticos. Sin embargo, junto con el uso extendido de LOLBins, su detección está asociada con una gran cantidad de falsos positivos, de modo que **la tarea de adaptar de forma continua la lógica de detección a las características de la infraestructura y las prácticas de las operaciones informáticas es la tarea más importante para aumentar la eficiencia del equipo de supervisión.**

Una cantidad relativamente alta de incidentes está asociada con la detección de la incorporación de cuentas a diferentes grupos con privilegios (administradores de dominio, administradores empresariales, etc.). Con el objetivo de reducir la cantidad de falsos positivos para estos incidentes, **es de suma importancia realizar un inventario regular de los miembros en grupos con privilegios, tener un procedimiento formal para administrar privilegios y accesos y, si la supervisión está a cargo de contratistas, esta información debe ponerse a su disposición de inmediato.**

Recomendaciones generales:

- Cada año, Kaspersky detecta ataques selectivos que se llevaron a cabo con la participación directa de un atacante humano. Para detectarlos con eficacia, es necesario implementar prácticas de detección de amenazas además de la supervisión clásica basada en alertas[6].
- La mejor manera de probar la eficiencia de los mecanismos de seguridad que se emplean en una empresa es realizar diferentes tipos de ciberejercicios[7]. Año tras año, Kaspersky observa un aumento en el interés por estos tipos de proyectos.
- En 2023, Kaspersky detectó una menor cantidad de incidentes de gravedad alta relacionados con el uso de malware, con un aumento simultáneo de incidentes similares, pero de gravedad media y baja, para los cuales el enfoque más efectivo y eficiente es la protección en diferentes niveles[8].
- El uso del marco MITRE ATT&CK®[9] proporciona información contextual adicional a los equipos de detección e investigación de ataques. Los ataques más complejos están compuestos por pasos y técnicas simples; si se logra detectar un paso, se revelará el ataque completo.

5 LolBins

6 Kaspersky MDR

7 Kaspersky Security Assessment

8 Enfoque multicapa de Kaspersky para la seguridad

9 MITRE ATT&CK

Gravedad de los incidentes

En MDR, solo se informan los incidentes que exigen que los clientes tomen medidas[10].

Baja

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

Mediana

No hay evidencia de participación humana directa en el ataque, puede afectar el sistema informático del cliente, pero no tiene consecuencias graves

Alta

Una amenaza de malware o un ataque llevado a cabo por personas humanas que tiene un considerable impacto potencial o real en los sistemas informáticos del cliente

En 2023, la frecuencia de los incidentes de gravedad alta fue tanta que, en promedio, hubo más de dos incidentes críticos por día. El año 2021 fue notorio debido a la cantidad de incidentes críticos, pero desde entonces, se observa una reducción en la proporción de incidentes de gravedad alta y una reducción en incidentes de gravedad baja y media. En 2023, se observó la cantidad más alta de incidentes de gravedad baja hasta el momento.

Figura 7 Nivel de gravedad del incidente

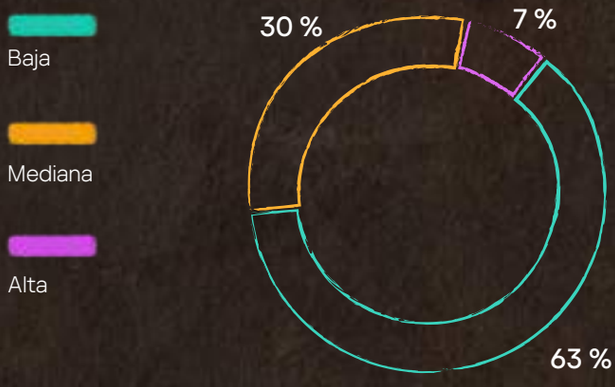
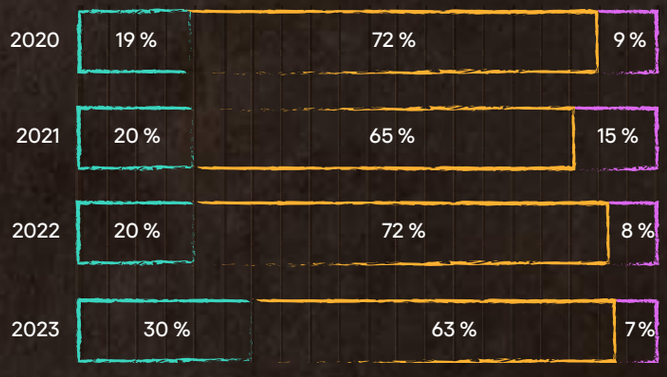


Figura 8 Gravedad de los incidentes de MDR a lo largo de los años



Según la clasificación de Kaspersky, esta redistribución de los incidentes de gravedad alta a incidentes de gravedad baja y media está asociada con la detección de malware sin rastros visibles de participación humana activa en el ataque, y se puede explicar por la "comercialización" de las herramientas. El uso de las herramientas desarrolladas en el pasado para realizar campañas selectivas (como resultado de filtraciones intencionales o accidentales) o por otros motivos, se extendió y estas se reutilizan en intentos de implementar ataques completamente automatizados. Esta tendencia también se ve favorecida por el creciente mercado de malware personalizado y la propagación del modelo de malware como servicio (MaaS). Las EPP modernas permiten proporcionar respuestas bastante eficientes y automáticas para estos ataques completamente automatizados.

Dado que la cantidad de incidentes depende en gran medida del alcance de la supervisión, el panorama más objetivo proviene de la distribución de la proporción entre la cantidad de incidentes y la cantidad de objetos supervisados (en el caso de MDR, endpoints).

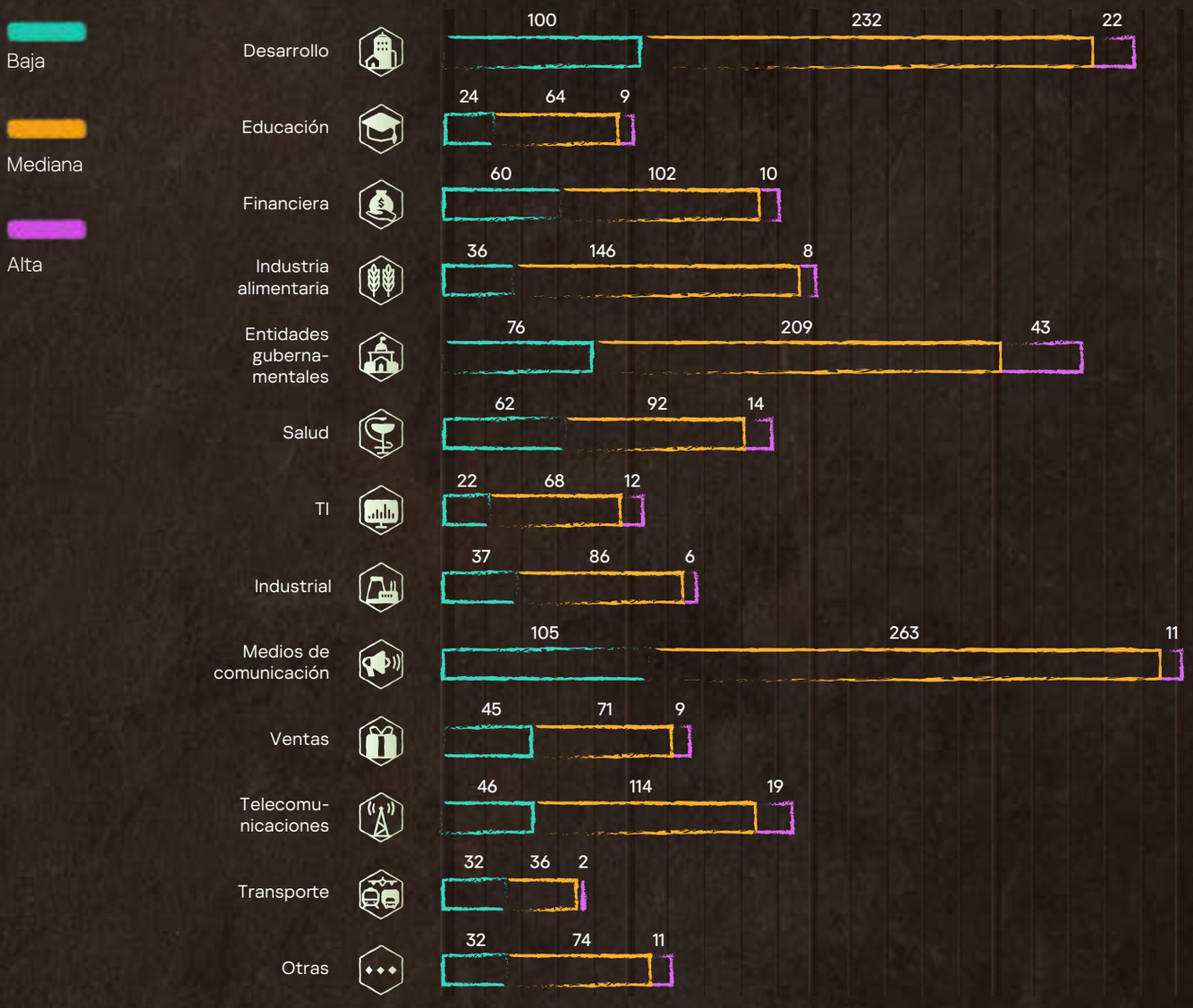
10 Por ejemplo, si un equipo portátil se conecta a una red Wi-Fi pública y el sistema de prevención de intrusiones en la red detecta intentos del exploit EternalBlue, definitivamente se trata de un incidente, pero no requiere una acción de respuesta dado que los equipos en riesgo suelen estar conectados a WLAN públicas. La respuesta a este incidente supera las capacidades del cliente. Es por ello que podría ser un ejemplo de un incidente que no se informará al cliente.

Analicemos un incidente similar, pero que se detecta en una red corporativa, en la que el cliente administra y controla en su totalidad un equipo en riesgo (aunque sin protección de MDR). Este incidente se publicará en el portal de MDR y se le recomendarán al cliente algunas acciones de respuesta.

En el siguiente diagrama, se observa la cantidad prevista de incidentes de cualquier gravedad en 10 000 endpoints supervisados, distribuidos por sector.

Figura 9

Distribución de incidentes por gravedad y sector



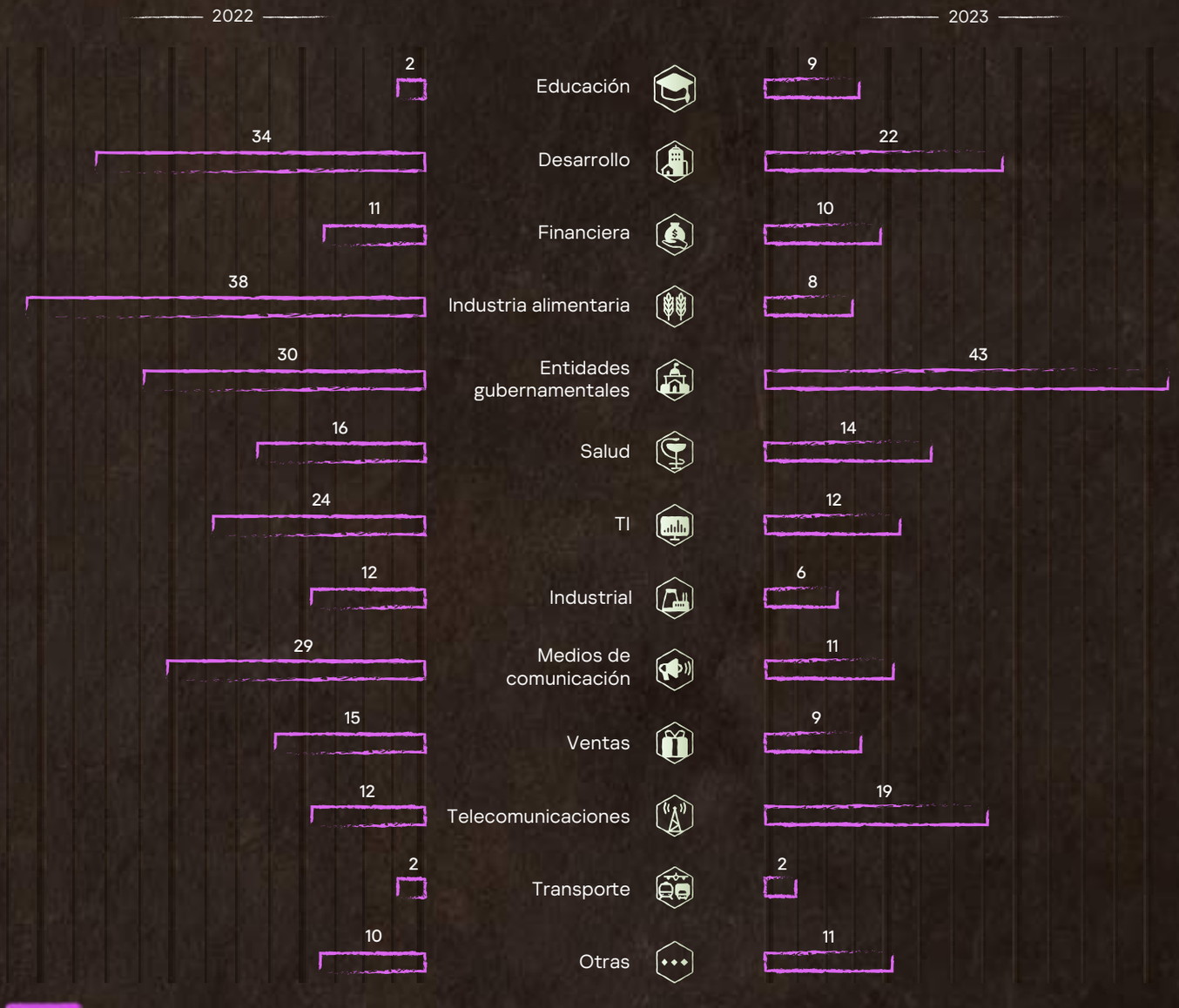
En el diagrama podemos observar que la mayor cantidad relativa de incidentes se observó en los sectores de medios de comunicación, entidades gubernamentales y desarrollo.

En comparación con 2022, observamos un aumento considerable en la cantidad de incidentes en los sectores de medios de comunicación, desarrollo, entidades gubernamentales y telecomunicaciones. También se puede apreciar un pequeño aumento en el sector de ventas, pero son principalmente incidentes de gravedad baja. Diversos sectores mostraron una reducción considerable de incidentes, como los sectores financiero, industrial y de industria alimentaria.

El porcentaje de incidentes de gravedad alta casi nunca superó el 10 % y, por lo tanto, se pierde visualmente en el volumen total de incidentes. En el siguiente diagrama se observan por separado los incidentes de gravedad alta.

Figura 10

Cantidad de incidentes graves por sector en comparación con el año anterior



En este gráfico podemos observar que hubo una disminución general en la cantidad de incidentes de gravedad alta en comparación con el año anterior. Sin embargo, se observa un aumento considerable en el sector educativo, de 2.28 a 8.92 incidentes en 10 000 endpoints, pero si tenemos en cuenta la cantidad total de incidentes en este sector (1.1 %) y la cantidad de clientes (2.1 %), este crecimiento puede considerarse insignificante. No obstante, si consideramos la cantidad de clientes de los sectores de industria alimentaria, TI, medios de comunicación, industrias y ventas en la base de clientes general de MDR, la reducción de la cantidad de incidentes de gravedad alta es considerable. Se observó un aumento relativamente grande de incidentes de gravedad alta en el sector de telecomunicaciones, pero en los sectores de finanzas, salud y transporte, la cantidad de incidentes críticos en 2023 se mantuvo congruente con respecto al año anterior.

Eficacia de las respuestas

Figura 11 Distribución de incidentes por cantidad de alertas relevantes

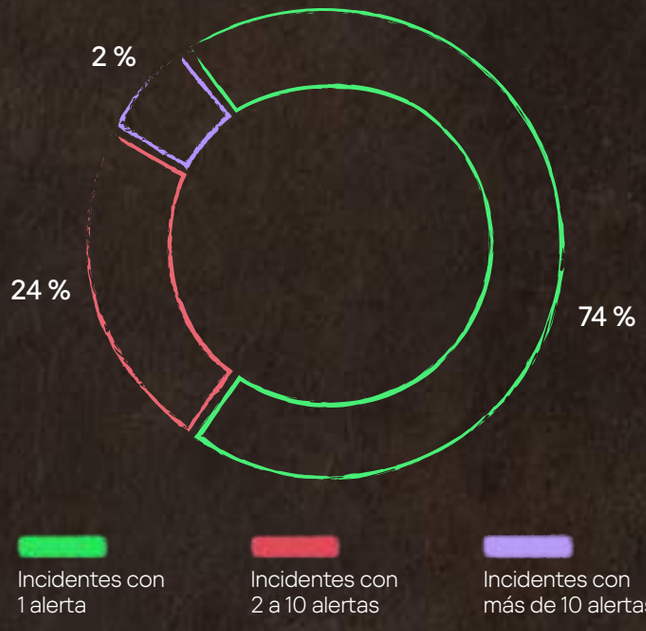
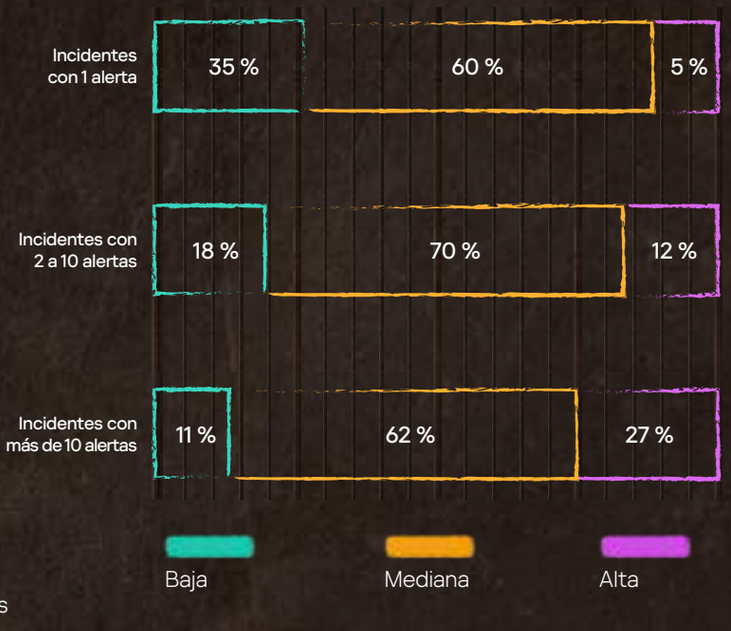


Figura 12 Distribución de incidentes por gravedad y cantidad de alertas relevantes



Aproximadamente el 74 % de los incidentes estuvo relacionado con **una única alerta**, después de la cual se detuvo el ataque. Esta categoría incluye incidentes típicos con situaciones de respuesta clara[11]. El porcentaje de los incidentes críticos es aproximadamente del 5 %. La gran mayoría son incidentes de gravedad media (61 %) y baja (34 %).

Cerca del 24 % de los incidentes se detectó en función de **2 a 10 alertas.** Esta categoría abarca incidentes que no se resolvieron completamente de manera automática. Por ejemplo, la detección de un host que ponía en riesgo la red con EternalBlue[12]: mientras se estaba aprobando el aislamiento, el atacante continuaba sus intentos de aprovechamiento y MDR recibió las alertas. Otro ejemplo son los ataques distribuidos a lo largo del tiempo, como los correos electrónicos de phishing. En primer lugar, no todos los correos electrónicos sospechosos se pueden reconocer automáticamente como maliciosos. Por otro lado, para comprender que un incidente está relacionado con el correo, primero se deben recibir varias alertas, que suelen producirse tras realizar una búsqueda manual de correos electrónicos similares a los detectados automáticamente.

Alrededor del 2 % de los incidentes contenían **más de 10 alertas.** Se trata de casos en los que la respuesta fue rechazada por el cliente o resultó ineficiente: un nuevo tipo de APT que requiere una investigación exhaustiva antes de responder, o el cliente solicitó supervisión sin una respuesta activa (ciberejercicios). El 11 % de los incidentes de gravedad baja se debe a la presencia de medidas de baja prioridad que los usuarios de MDR debían implementar, pero que no hicieron. Esto no provocó el avance del ataque debido a que el incidente era de gravedad baja.

11 Por ejemplo, la detección de malware nuevo con el lanzamiento posterior de las firmas de detección necesarias para su detección y prevención, y la supervisión de su neutralización exitosa por parte del equipo del SOC. Esto también incluye incidentes de detección de artefactos de vulneraciones anteriores que no se investigaron de manera más exhaustiva debido a una decisión del usuario de MDR

12 Microsoft Security Bulletin MS17-010

La naturaleza de los incidentes de gravedad alta

Figura 13 Cantidad de incidentes críticos por tipo

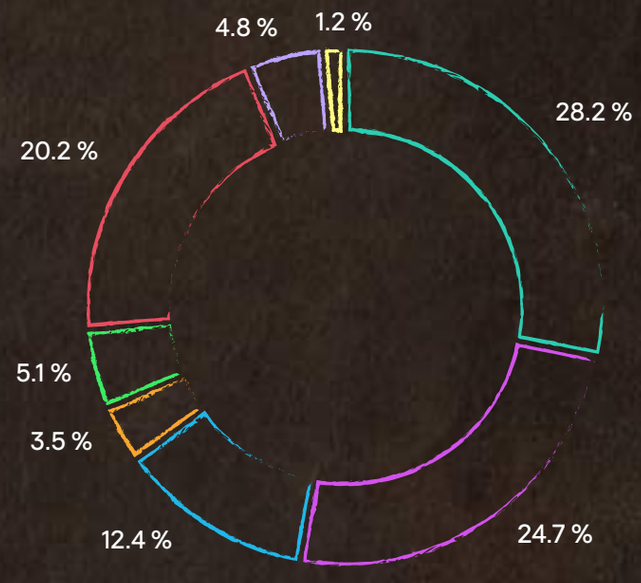
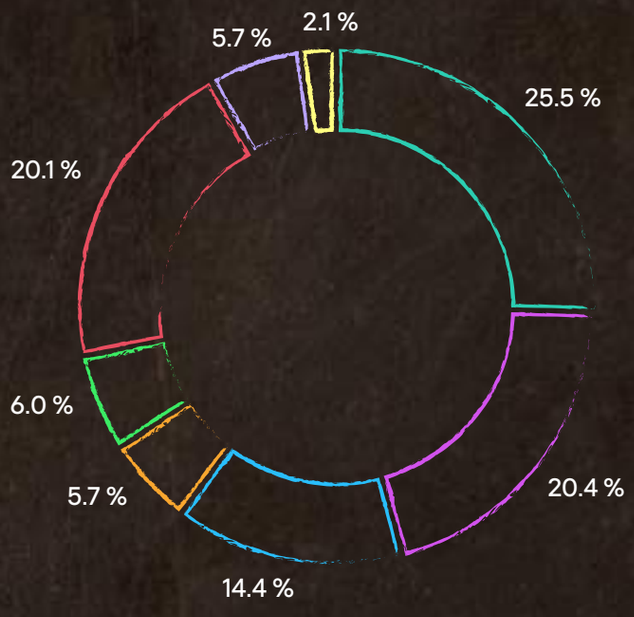


Figura 14 Cantidad de empresas en las que se observaron incidentes críticos, por tipo



Infracción de políticas de seguridad | Ataques selectivos | Software malicioso | Ingeniería social | Artefactos de ataques selectivos | Ciberejercicios | Vulnerabilidad crítica | Ataque interno

Casi un cuarto de los incidentes de gravedad alta fueron ataques llevados a cabo por personas humanas.

Los incidentes en los que se observa una participación activa de personas se clasifican de manera predeterminada como "ataques selectivos", y el tipo de incidente cambia a "ciberejercicios" solo con la confirmación explícita del cliente. En 2023, los clientes informaron que más del 20 % de los incidentes estaban relacionados con ciberejercicios. Por lo general, los incidentes relativos a la detección de artefactos de ataques selectivos reflejan las estadísticas de los ataques selectivos. Sin embargo, en 2023, se detectó solo el 5 % de dichos incidentes, y la mayoría de ellos resultaron ser rastros de ciberejercicios anteriores.

Los ataques de malware superaron ligeramente el 12 %. En comparación con años anteriores, representa la proporción más pequeña de dichos tipos de incidentes. La mayoría de los incidentes relacionados con malware se clasificaron con un nivel de gravedad media o baja.

Menos del 5 % son incidentes relacionados con vulnerabilidades críticas disponibles públicamente.
Menos del 4 % provienen de eventos de ingeniería social exitosos con un desarrollo adicional del ataque.

Menos del 1 % de los incidentes están vinculados con ataques internos, y el porcentaje de incidentes relacionados con actividad sospechosa de cuentas legítimas sin signos visibles de vulneración superó el 28 %[13].

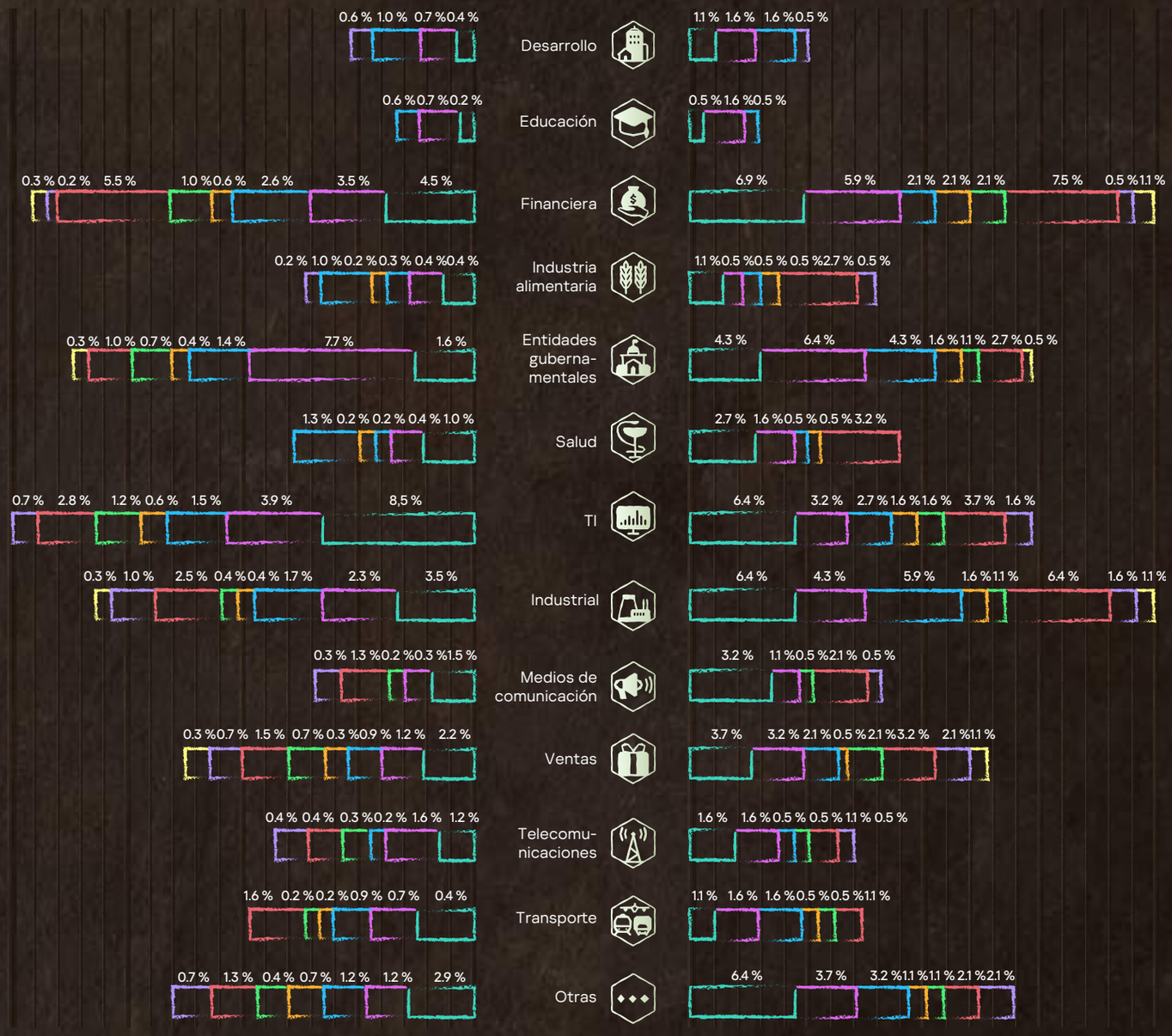
13 En incidentes de este tipo, se detectó actividad sospechosa de cuentas legítimas a pesar de no haber otros signos de vulneración. Si se recibía una confirmación de legitimidad del cliente, dichos incidentes se clasificaban como falsos positivos y no se tenían en cuenta.

Incidentes de gravedad alta por sector

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

Figura 15 Cantidad de incidentes de gravedad alta por sector

Figura 16 Cantidad de organizaciones con incidentes de gravedad alta por sector



Infracción de políticas de seguridad | Ataques selectivos | Software malicioso | Ingeniería social | Artefactos de ataques selectivos | Ciberejercicios | Vulnerabilidad crítica | Ataque interno

A partir de las estadísticas de incidentes, podemos sacar las siguientes conclusiones:

- Se observaron incidentes críticos en todos los sectores.
- Además, se detectaron incidentes relacionados con ataques selectivos en todos los sectores de la economía.
- La mayor cantidad de incidentes de gravedad alta se observó en los sectores de finanzas, TI, entidades gubernamentales e industrial.
- Se observó todo tipo de incidentes de gravedad alta en los sectores financiero, industrial y de ventas.
- Los sectores con mayor cantidad de ataques selectivos fueron entidades gubernamentales, TI y finanzas, y los que tuvieron mayor cantidad de ciberejercicios fueron los sectores financiero, TI e industrial.
- Como se mencionó antes, en 2023, hubo pocos incidentes de gravedad alta relacionados con malware, pero cabe mencionar que en el sector de medios de comunicación no se observaron en lo absoluto. El sector con mayor cantidad de incidentes de gravedad alta relacionados con malware fue el financiero.
- En 2023, las estadísticas de incidentes relacionados con la detección de artefactos utilizados para ataques realizados por personas humanas no replicó completamente las estadísticas de los ataques selectivos: se observaron ataques selectivos en los sectores de desarrollo, educación, industria alimentaria y salud, pero no se produjeron incidentes debido a que se detectaron artefactos de vulneraciones anteriores.
- En casi todos los sectores, con raras excepciones, se observaron incidentes relacionados con el desarrollo de ataques de ingeniería social y la presencia de vulnerabilidades críticas en el perímetro de la red de las organizaciones.
- El tipo "infracción de políticas de seguridad", que se introdujo en 2023, se observó en todos los sectores. Sin embargo, el sector que más lo sufrió fue el de TI, en el que se observó la mayor cantidad de acciones sospechosas de cuentas de usuario existentes, sin confirmarse la legitimidad de su actividad.

A partir de las estadísticas de víctimas de incidentes críticos, se pueden señalar las siguientes observaciones:

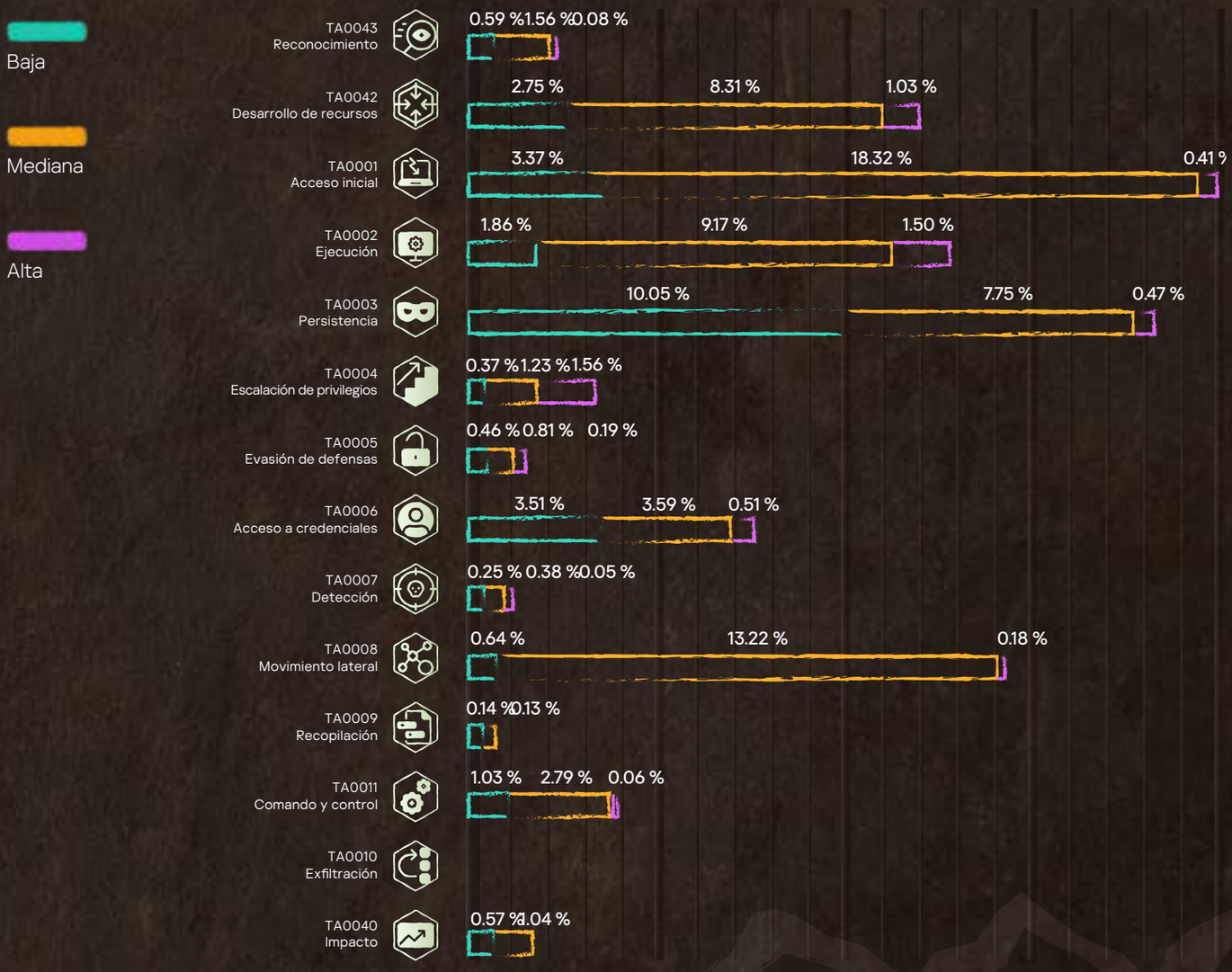
- La mayoría de los ataques realizados por personas humanas se produjeron en empresas de los sectores financiero y gubernamental. Los sectores con menor cantidad de ataques fueron los de medios de comunicación e industria alimentaria.
- Se observaron ataques con malware en la mayor cantidad de empresas del sector industrial (5.85 %) y gubernamental (4.26 %).
- Las organizaciones de los sectores financiero e industrial sufrieron la mayor cantidad de incidentes relacionados con ciberejercicios.
- Se observaron incidentes relacionados con ataques de ingeniería social exitosos y la presencia de vulnerabilidades críticas en el perímetro en empresas de casi todos los sectores, con solo algunas escasas excepciones.

Tecnologías de detección. Tácticas, técnicas y procedimientos de atacantes

Tácticas de atacantes

MDR nos permite detectar incidentes en las diferentes etapas de un ataque. Por lo general, un incidente atraviesa todas las etapas (tácticas de MITRE ATT&CK®), pero en el siguiente diagrama se muestran las primeras tácticas de las alertas asociadas con el incidente.

Figura 17 Nivel de gravedad del incidente



Las principales tácticas que usa Kaspersky para detectar incidentes

TA0043: Reconocimiento

Los incidentes que se detectan en esta etapa están relacionados principalmente con diversos tipos de análisis, y la gravedad de un incidente depende de los objetivos del análisis. Por ejemplo, un análisis regular se clasificaba como un incidente de gravedad baja. Los análisis más específicos, como la detección de redes SIP/VoIP, la búsqueda de vulnerabilidades específicas (tales como CVE-2021-44228, CVE-2020-2551, CVE-2019-19781, entre otras) e intentos de implementar varios tipos de ataques de phishing (técnica MITRE T1598), se clasificaban principalmente como incidentes de gravedad media. Los incidentes clasificados como de gravedad alta están principalmente relacionados con exploits de spear phishing con un desarrollo adicional del ataque.

TA0042: Desarrollo de recursos

Los incidentes que se atribuyen a esta táctica están vinculados principalmente con la detección de cualquier tipo de software malicioso o no deseado que podría utilizarse más adelante para el desarrollo posterior del ataque. La gravedad de las herramientas detectadas determina la gravedad del incidente. Por ejemplo, la detección de Mimikatz, Impacket o Cobalt Strike indica que se trataba de un ataque llevado a cabo por personas humanas, y estos incidentes se clasificaban como de gravedad alta.

TA0001: Acceso inicial

La gran mayoría de los incidentes identificados en esta etapa se relacionaban con la detección de correos electrónicos de phishing que incluían diferentes tipos de objetos maliciosos. En la mayoría de los casos, se clasificaban como incidentes de gravedad media, que también incluían intentos de aprovechar vulnerabilidades en el perímetro de la red. Si se hacía clic en vínculos maliciosos incluidos en correos, el incidente se clasificaba como de gravedad baja. Los incidentes de gravedad alta estaban relacionados con la detección de intentos de implementar un ataque en 3CX[14], intentos de aprovechar el perímetro de la red con campañas dirigidas conocidas (si era posible usar atribuciones) y correos electrónicos de phishing con cargas útiles relativas a APT conocidas.

TA0002: Ejecución

Dado que ejecutar herramientas de ataque especializadas llama la atención, la mayoría de los incidentes de gravedad alta se identifican en esta etapa. En general, la gravedad del incidente en esta etapa está determinada por la clasificación de la herramienta utilizada.

TA0003: Persistencia

En esta etapa, se detectaron incidentes relacionados con la manipulación de cuentas (agregado de administradores, desbloqueos), el reemplazo de características de accesibilidad, configuraciones sospechosas o poco seguras de los recursos de la red, bootkits. Se asignaba la gravedad alta cuando había pruebas irrefutables de que se trataba de un ataque llevado a cabo por personas humanas; en otros casos, los incidentes se registraban como de gravedad media o baja según el posible impacto.

TA0004: Escalación de privilegios

En la gran mayoría de los incidentes, se utilizó esta táctica en las primeras etapas: agregar una cuenta a varios grupos con privilegios como administradores de dominio, administradores empresariales, etc. También incluía incidentes relacionados con el uso de herramientas especializadas para la escalación de privilegios (que se detectaron en forma de archivos independientes o ya cargados en la memoria del sistema), la detección de unidades vulnerables, cambios en la configuración de UAC e intentos de aprovechar determinadas vulnerabilidades (por ejemplo, aquellas que se describen en el boletín MS14-068[15]).

14 Ataque a la cadena de suministro en clientes de 3CX

15 Microsoft Security Bulletin MS14-068

TA0005: Evasión de defensas

En esta etapa se detecta un porcentaje relativamente pequeño de incidentes. Sin embargo, la proporción de falsos positivos es la menor, ya que las técnicas y herramientas detectadas por lo general no son típicas de actividades legítimas.

TA0006: Acceso a credenciales

La gran mayoría de los incidentes relacionados con esta táctica involucra la técnica T1003 (Volcado de credenciales de SO) con casi todas sus subtécnicas. Como en el caso anterior, los incidentes identificados aquí no suelen ser falsos positivos, salvo algunos tipos de ciberejercicios confirmados.

TA0007: Descubrimiento

En este etapa, la detección se asocia con una gran cantidad de falsos positivos, por lo que hay pocos IoA relevantes que se convierten en alertas. Principalmente, se utilizan para enriquecer la telemetría, mientras que los incidentes reales suelen detectarse en etapas anteriores. En esencia, los incidentes existentes se relacionan con diferentes tipos de análisis de redes internas o con la detección del uso de herramientas especializadas, como Bloodhound o AdFind.

TA0008: Movimiento lateral

Dado que la táctica Movimiento lateral muestra un índice bajo de falsos positivos, es prometedora para planificar el desarrollo de nuevos IoA. En 2023, la gran mayoría de los incidentes estaban relacionados con exploits de redes (EternalBlue, vulnerabilidades de Apache Log4j y otros) que provocaron la ejecución remota de código.

TA0009: Recolección

Las situaciones que no implican el uso de herramientas especializadas en esta etapa son extremadamente difíciles de detectar, dado que no se pueden diferenciar de las actividades legítimas. Sin embargo, los IoA existentes pueden utilizarse con eficacia para enriquecer la telemetría, lo que permite proporcionar un contexto adicional para los incidentes que se identifican en otras etapas.

TA0011: Comando y control

En esta etapa, la gran mayoría de las detecciones se realizaron en función de la TI: acceso a un recurso malicioso. La gravedad del incidente se determina por el propósito conocido de C2. Si está asociado con una APT, el incidente se clasificaba como de gravedad alta.

TA0010: Exfiltración

En 2023, algunos incidentes se las ingeniaron para llegar a esta etapa, y los incidentes detectados son extremadamente difíciles de extinguir de TA0011, ya que la situación más común es T1041 (Exfiltración en el canal C2) y el protocolo de capa de aplicación utilizado es DNS.

TA0040: Impacto

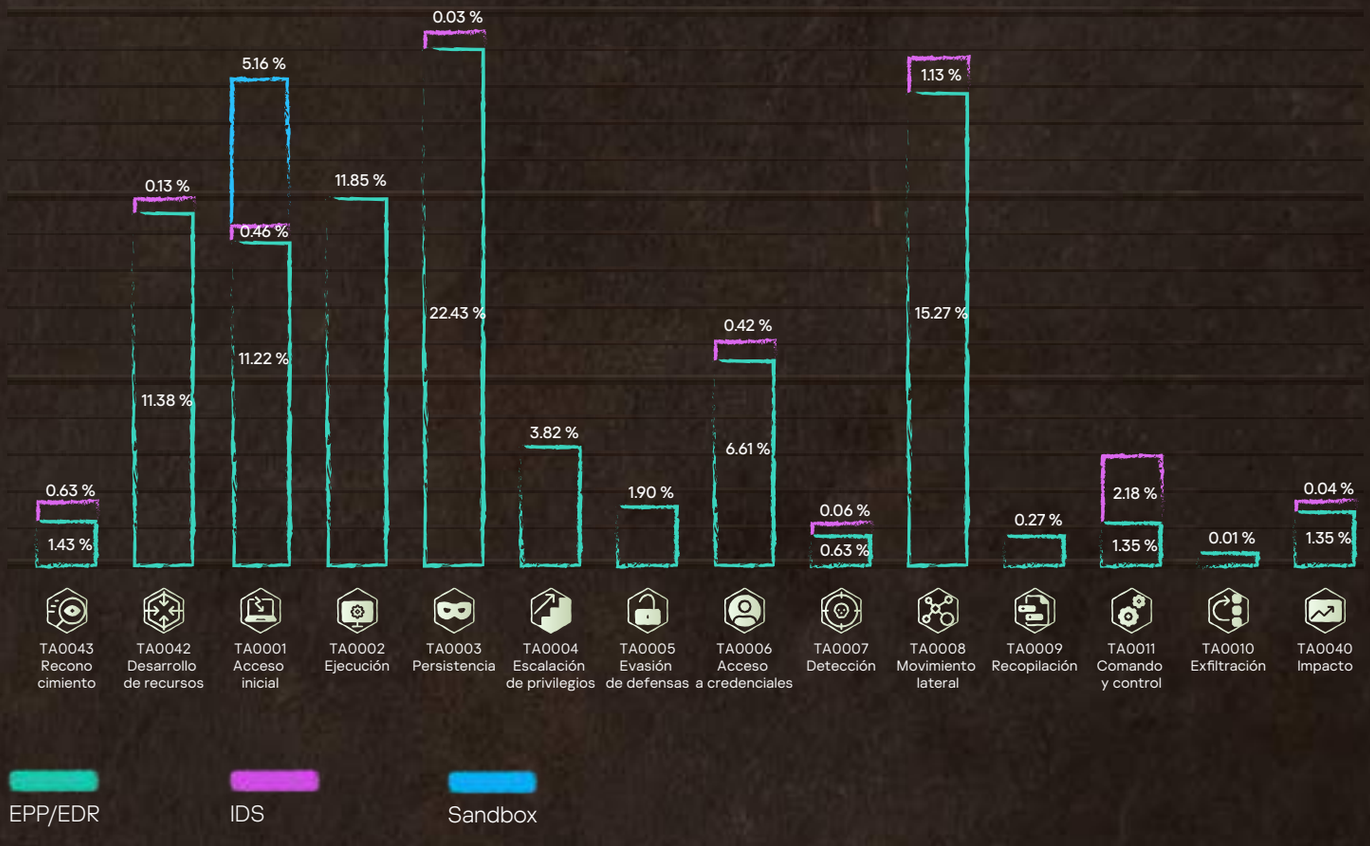
En esta táctica, la detección de malware específico es la base de la mayoría de los incidentes, y si no fue posible detectarlo y responder en una etapa anterior, solo la prevención automática con EPP moderna puede ayudar en este caso. La gran mayoría de los incidentes que llegaron a esta etapa en 2023 estaban relacionados con la detección de criptomineros o ransomware.

Tácticas y tecnologías de detección de atacantes

El predominio de incidentes en EPP no implica fallas del sistema de detección de intrusiones (IDS) o del entorno de pruebas, ya que en la mayoría de los casos, todos los sensores confirmaron el incidente, pero se consideró la fuente de la alerta que informó el incidente. En la Figura 18, se observan los porcentajes de incidentes detectados inicialmente por varios sensores.

Figura 18

Cantidad de incidentes detectados inicialmente por los sensores implementados



La alta eficiencia alta del entorno de pruebas y el IDS en **TA0001 (Acceso inicial)** es el resultado de usar el escenario popular de KATA en el perímetro de la red. El IDS es eficiente en las etapas **TA0008 (Movimiento lateral)** y **TA0011 (Comando y control)**. Además, el IDS funciona de forma correcta para detectar análisis de red (**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 según comunicaciones conocidas con su C2.

De **TA0002 (Ejecución)** a **TA0006 (Acceso a credenciales),** la EPP es predominante, pero IDS también detecta herramientas con tráfico de red típico, como shells web y puertas traseras (**TA0003 Persistencia**), mineros (**TA0040 Impacto**) y adivinación de contraseñas de la red (**TA0006 Acceso a credenciales**).

Técnicas de atacantes

Herramientas utilizadas en ataques

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

Tabla 2

Los LOLBins más populares y su frecuencia de su uso en todos los incidentes y en los incidentes de gravedad alta

	Todos los incidentes	Incidentes de gravedad alta
powershell.exe	1.21 %	7.17 %
rundll32.exe	0.70 %	4.78 %
comsvcs.dll	0.20 %	1.79 %
msiexec.exe	0.34 %	1.39 %
msedge.exe	1.18 %	1.20 %
reg.exe	0.24 %	1.20 %
certutil.exe	0.13 %	1.00 %

Los LOL-bins[16] más populares que se observaron en casi todos los incidentes son **powershell.exe, rundll32.exe** y **reg.exe.**

16 LOLBAS

PowerShell, que es un shell de Windows estándar con un gran número de características, se utiliza en muchas situaciones. A continuación, presentamos algunos ejemplos:

- Ejecución de contenido malicioso con intentos de ofuscación

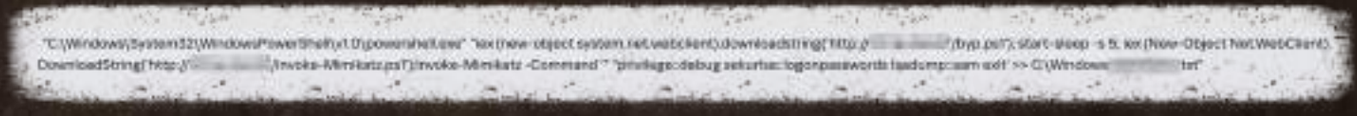
Figura 19 Ejecución de contenido malicioso ofuscado con PowerShell

- Deshabilitación de sistemas de seguridad o cambios en su configuración

Figura 20 Creación de una exclusión de Windows Defender con PowerShell

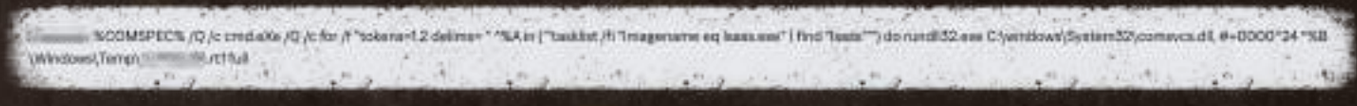
- Uso de herramientas de ataque prediseñadas

Figura 21 Uso de la implementación PowerShell de Mimikatz



A menudo, los componentes maliciosos se implementan como bibliotecas dinámicas, lo que explica la popularidad de **rundll32:**

Figura 22 Uso de rundll32 para acceder a la memoria de LSASS



La implementación de cambios en la configuración de los subsistemas de seguridad y el acceso a datos de autenticación locales son las tácticas elegidas por los atacantes que usan la utilidad **reg.exe** estándar:

Figura 23 Uso de reg para modificar el registro a fin de deshabilitar UAC

Figura 24 Uso de reg para acceder a datos de autenticación del registro

El año pasado, como había sucedió el año anterior, hubo incidentes que usaban **comsvcs.dll**[17], a pesar de que la técnica no es nueva:

Figura 25 Uso de comsvcs.dll para acceder a la memoria de LSASS

Entre los atacantes, certutil.exe[18]**,** que ya no es difícil de detectar, mantiene su popularidad:

Figura 26 Uso de certutil para descargar herramientas en un host en riesgo

A menudo, se implementan cargas útiles maliciosas[19] en etapas posteriores a **TA0001 (Acceso inicial)** como un paquete de MSI. Esto explica la popularidad de **msiexec.exe**[20] en general y en los incidentes de gravedad alta en particular.

Con casi la misma frecuencia entre incidentes de gravedad alta y todos los incidentes en general, la presencia de **msedge.exe**[21] en la lista es una novedad para 2023. Esto indica un porcentaje relativamente alto de incidentes relacionados con usuarios que hacen clic en vínculos de phishing, así como un aumento en la cantidad de ataques de descarga oculta en 2023.

17 Comsvcs.dll

18 Certutil.exe

19 Por ejemplo, MSF Meterpreter o CobaltStrike Beacon

20 Msiexec.exe

21 Msedge.exe

Clasificación de incidentes de MITRE ATT&CK®

Los IoA utilizados en MDR también están vinculados con las técnicas de MITRE ATT&CK®. Para controlar la calidad de la detección en MDR, para cada IoA, el equipo de Ingeniería de Detección calcula la conversión y la contribución[22], de modo que también puedan calcularse para las técnicas de MITRE ATT&CK®. A continuación, se indican las nueve técnicas que mostraron a mejor **conversión**[23] y, en el diagrama, se observa la **contribución** de las técnicas observadas. El índice bajo de conversión se explica 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

T1110.001: Adivinación de contraseñas	36.41 %	Aunque los sensores de red y los agentes en endpoints detectan de forma eficaz la adivinación de contraseñas, esta técnica mantiene su popularidad en proyectos de evaluación de seguridad y entre atacantes reales
T1098: Manipulación de cuenta	32.91 %	Las cuentas y los grupos con privilegios suelen estar bien controlados, pero, a pesar de ello, los atacantes suelen habilitar cuentas desactivadas o agregan miembros a grupos
T1078: Cuentas válidas	31.60 %	A menudo, los atacantes utilizan cuentas locales y dominios para eludir las soluciones de seguridad y, posteriormente, ganar persistencia en un sistema en riesgo. Esta técnica es popular, en particular, en ciberejercicios y ataques selectivos bien preparados
T1210: Abuso de servicios remotos	22.33 %	Los intentos de aprovechar la ejecución remota de código (RCE) son muy populares respecto de incidentes por motivos de movimiento lateral, independientemente de su gravedad. En este caso, a menudo se utilizan exploits bastante antiguos, como EternalBlue, lo que confirma el mal estado general de la administración de vulnerabilidades corporativas
T1566.002: Enlace de spear phishing	16.82 %	El phishing es la técnica más popular para obtener el primer acceso. En 2023, los correos con vínculos maliciosos dominaban la escena. A diferencia de años anteriores, los archivos adjuntos eran más comunes
T1021.002: Recursos compartidos de administrador de SMB/Windows	15.88 %	En la infraestructura de Windows, los recursos compartidos predeterminados de la red son muy populares para los movimientos laterales. Junto con T1078 (Cuentas válidas), no se pueden diferenciar de actividades legítimas
T1547.001: Claves de ejecución de registro/carpeta de inicio	14.19 %	Esta es la técnica de persistencia más popular, independientemente de la gravedad del incidente. Dado que, en el caso de situaciones de LotL[24], se utilizan mecanismos de SO estándar, sin contexto adicional, es extremadamente difícil distinguirla de acciones legítimas
T1021: Servicios remotos	13.19 %	Este es el segundo mecanismo de movimiento lateral más popular que se utilizó en todo tipo de incidentes, junto con T1078 (Cuentas válidas)
T1003.001: Memoria de LSASS	10.85 %	Los atacantes a menudo intentan acceder a la memoria de LSASS. Pero los esfuerzos tanto de Microsoft como de Kaspersky lo hacen mucho más difícil y, como resultado, observamos relativamente pocas conversiones

22 La conversión hace referencia a la relación entre las alertas clasificadas como incidentes y la cantidad total de alertas que corresponden a una técnica específica de MITRE ATT&CK®. La contribución es la relación entre los incidentes en los que se observó una técnica particular y la cantidad total de incidentes informados

23 Para obtener una cifra representativa, se tuvieron en cuenta las técnicas cuya contribución excedían el 5 %; es decir, aquellas que se produjeron en más del 5 % de los incidentes.

24 Ataque Living off the land (LotL)

Las reglas de detección activadas con mayor frecuencia

En 2023, la cantidad total de situaciones únicas que se activaron en MDR y tuvieron una conversión superior a cero fue de 673. En esta sección, se observan las activadas con mayor frecuencia, cuya contribución acumulada total superó el 70 % (es decir, se detectó más del 70 % de todos los incidentes, incluidas estas reglas de detección).

Por conveniencia, las dividimos en dos grupos: detecciones basadas en productos y en eventos del SO.
En comparación con el año anterior, el porcentaje de situaciones eficientes basado únicamente en el análisis de eventos del SO disminuyó en gran medida. Sin embargo, esto no le resta importancia a la recopilación y al análisis de eventos del SO con el fin de detectar e investigar incidentes, en especial dado que es el enfoque más evidente.

Detección basada en XDR

En esta sección, "XDR" implica una combinación de los siguientes proveedores de telemetría: IDS del sistema, plataforma de protección en endpoints y entorno de pruebas.

Contribución acumulada **~53 %**

Conversión promedio **~23 %**

No creamos un incidente por la detección de cada producto. El enriquecimiento contextual adicional, junto con el veredicto del producto, pueden ser la base para iniciar una investigación. Debido al uso de proveedores de telemetría de alta tecnología[25], estos veredictos siguen siendo las alertas más frecuentes y razonablemente precisas que llevan a la detección de incidentes graves.

La conversión promedio es menor de un cuarto; es decir, en promedio, tres de cuatro alertas son falsos positivos. A primera vista, puede parecer una cifra baja; sin embargo, es más del doble que la conversión promedio en toda la solución MDR, y la contribución de dichas situaciones (el porcentaje de incidentes reales detectados a través de su uso) es más de la mitad. Es decir, más de la mitad de todos los incidentes de MDR se detectaron con tecnologías personalizadas de detección de ataques, lo que compensa en gran medida la tasa de conversión relativamente baja.

En 2023, las siguientes situaciones fueron las más comunes (en orden descendente).

Tabla 4 Técnicas con la mayor cantidad de conversiones

Situación de detección	Descripción	Telemetría requerida y enriquecimiento
Detección de IDS de red	Al activar el IDS de una red (como parte de KATA y como un componente de EPP), no se observa una fuente de ataque dentro del alcance de la supervisión, de modo que no hay manera de verificar un falso positivo usando la telemetría disponible	◆ Veredicto de NIDS ◆ **Supervisión de la configuración de red de hosts**
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	◆ En el caso de Kaspersky MDR, cualquier evento de telemetría que contiene el proceso que inicia el evento ◆ **Reputación del archivo, script o documento de Office**

25 Enfoque multicapa para la seguridad

26 Reputación de archivos en línea de Kaspersky

Situación de detección	Descripción	Telemetría requerida y enriquecimiento
Detección del entorno de pruebas	Activación del entorno de pruebas como parte de KATA. No hay un veredicto de EPP exacto para el objeto sospechoso	◆ Veredicto de Sandbox ◆ **Veredicto de EPP para el objeto**
Intento de acceder a un host malicioso	Intento de acceder a un host con mala reputación	◆ Veredicto del producto ◆ Conexión HTTP ◆ Conexión de red ◆ Solicitud de DNS ◆ **Reputación del host de destino**
Archivo adjunto en un mensaje de correo electrónico malicioso	Activación de EPP en el archivo adjunto del correo electrónico	◆ Veredicto de EPP ◆ Recepción de archivo adjunto de un correo electrónico
URL maliciosa detectada en una línea de comandos	En cualquier campo del evento (la situación más común es la línea de comandos, lo 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 información disponible de amenazas	◆ **Reputación de URL**
Detección relacionada con APT	Lista de veredictos de EPP exactos y no exactos[27] (actividad sospechosa)	◆ Veredicto de EPP
Acceso a un recurso web malicioso desde una aplicación no basada en navegador	Se analizan las solicitudes HTTP y DNS, excepto las aplicaciones de navegadores conocidos	◆ Solicitud HTTP ◆ Solicitud de DNS ◆ **Reputación de la URL o del sitio**
Detección de EPP exacta en un servidor	Activación de una EPP instalada en un servidor. Un caso especial ocurre cuando se activa una EPP en un controlador de dominio o en cualquier otro servidor crítico	◆ Veredicto de EPP ◆ **Configuración de EPP** ◆ **Lista de servidores críticos**
Detección de ransomware	Lista de veredictos exactos o de actividad sospechosa relevantes para esta amenaza en particular	◆ Veredicto de EPP
Detección de KICS[28] en el segmento de tecnología operativa	Lista de veredictos particulares de KICS for Nodes[29]	◆ Veredicto de EPP ◆ **Configuración de EPP**
Detección de usuarios del sistema	La regla analiza líneas de comandos basadas en expresiones regulares a fin de detectar técnicas conocidas para recopilar datos sobre los usuarios del sistema	◆ Cualquier evento de telemetría que tenga un campo de línea de comandos
Creación de una herramienta de hacking	Se crea un objeto en el sistema de archivos, que EPP clasifica como una "herramienta de hacking"	◆ Creación de archivos ◆ Veredicto de EPP
Detección en memoria	Activación de EPP en memoria	◆ Veredicto de EPP
Detección de adivinación de contraseñas	El evento de seguridad más común es adivinar la contraseña de una conexión de RDP. Tanto la correlación de eventos del SO como los productos pueden detectar este evento	◆ Veredicto de EPP ◆ Evento de inicio de sesión en la red del SO

27 El veredicto exacto significa que la actividad detectada por EPP es definitivamente maliciosa. En este caso, la EPP previene la amenaza de forma automática. Los veredictos no exactos o la actividad sospechosa significa que la EPP detectó una anomalía, pero la probabilidad de un falso positivo es bastante alta, de modo que no hay una respuesta activa, pero el equipo de MDR recibe una notificación

28 Plataforma de Kaspersky Industrial CyberSecurity

29 Kaspersky Industrial CyberSecurity for Nodes

Detección basada en eventos del sistema operativo

Los eventos del sistema operativo, por toda su evidencia y accesibilidad, también proporcionan muchas oportunidades para detectar ataques. Enriquecidos con datos de amenazas y correlacionados con otros eventos de XDR, demuestran tasas altas de conversión y, para una variedad de situaciones de ataque, son indispensables.

Contribución acumulada **~21 %**

Conversión promedio **~47 %**

Una posible desventaja de la tasa de conversión relativamente alta es la contribución baja de un poco más de una quinta parte de los incidentes, lo que confirma la dificultad de detectar de forma oportuna ataques modernos sin el uso de herramientas ni productos especializados.

Tabla 5

Los escenarios más utilizados

Situación de detección	Descripción	Telemetría requerida
Se activó la cuenta integrada	Se desbloquearon las cuentas integradas, como las de administrador o invitado	◆ Evento del SO: se habilitó una cuenta de usuario
Derechos de acceso sospechosos a una carpeta compartida de la red	La regla detecta configuraciones poco seguras y, en general, sospechosas de los recursos de la red	◆ Evento del SO: se modificó un objeto compartido de la red
Inicio de sesión en la red por parte de una herramienta de hacking	Eventos de inicio de sesión en la red detectados de una herramienta conocida (Kali, Nmap, etc.)	◆ Eventos del SO: inicio de sesión, cierre de sesión
Se agregó al usuario a un grupo con privilegios	Se agregó a un usuario a un grupo con privilegios (administradores de dominio, administradores empresariales, editores de certificados, etc.)	◆ Eventos del SO: cambio en la pertenencia a grupos

Diagrama de tácticas y técnicas de MITRE ATT&CK

TA0001: Acceso inicial

T1003: Volcado de credenciales de SO	0.36 %
T1005: Datos del sistema local	0.05 %
T1012: Consulta en registro	0.20 %
T1016: Descubrimiento de configuración de red del sistema	0.15 %
T1021: Servicios remotos	0.87 %
T1027: Archivos o información ofuscados	0.46 %
T1036: Ocultación mediante disfraces	1.74 %
T1046: Descubrimiento de servicio de red	0.10 %
T1047: Instrumental de administración de Windows	0.10 %
T1048: Exfiltración por sobre protocolo alternativo	0.10 %
T1049: Descubrimiento de conexiones de red del sistema	0.05 %
T1053: Tarea o trabajo programados	0.26 %
T1055: Inyección de procesos	0.15 %
T1059: Intérprete de comandos y scripts	1.69 %
T1070: Eliminación de indicadores	0.15 %
T1071: Protocolo de capa de aplicación	9.32 %
T1078: Cuentas válidas	1.18 %
T1082: Descubrimiento de información del sistema	0.05 %
T1087: Descubrimiento de cuenta	0.15 %
T1090: Proxy	0.20 %
T1091: Replicación mediante medios extraíbles	1.13 %
T1092: Comunicación mediante medios extraíbles	0.10 %
T1095: Sin protocolo de capa de aplicación	0.05 %
T1098: Manipulación de cuenta	0.05 %
T1102: Servicio web	0.20 %
T1105: Transferencia de herramienta de ingreso	1.08 %
T1110: Fuerza bruta	2.51 %
T1132: Codificación de datos	0.05 %
T1133: Servicios remotos externos	0.77 %
T1136: Crear cuenta	0.15 %
T1140: Decodificación/cancelación de ofuscación de archivos o información	0.05 %
T1176: Extensiones de navegador	0.10 %
T1189: Infección oculta	1.95 %
T1190: Exploit de aplicación de atención al cliente	11.27 %
T1193: Archivo adjunto de spear phishing	0.36 %
T1195: Compromiso de cadena de suministro	1.79 %
T1200: Agregados de hardware	0.05 %
T1203: Explotación para la ejecución de los clientes	0.31 %
T1204: Ejecución de usuario	13.32 %
T1210: Abuso de servicios remotos	4.00 %
T1218: Ejecución por proxy de binario de sistema	0.56 %
T1219: Software de acceso remoto	0.05 %
T1496: Secuestro de recursos	0.15 %
T1499: Denegación de servicio de endpoints	0.20 %
T1505: Componente de software de servidor	0.36 %
T1534: Spear phishing interno	2.15 %
T1543: Creación o modificación de procesos del sistema	0.51 %
T1546: Ejecución activada por evento	0.26 %
T1547: Ejecución automática de arranque o inicio de sesión	0.92 %
T1548: Abuso del mecanismo de control de elevación	0.10 %
T1552: Credenciales no protegidas	0.05 %
T1553: Alteración de controles de confianza	1.54 %
T1555: Credenciales desde almacenes de contraseña	0.20 %
T1556: Modificación en proceso de autenticación	0.10 %
T1557: Adversario intermediario	0.05 %
T1558: Robo o falsificación de tickets de Kerberos	0.05 %
T1562: Afectar defensas	0.05 %
T1564: Ocultamiento de artefactos	0.46 %
T1565: Manipulación de datos	0.77 %
T1566: Phishing	99.33 %
T1568: Resolución dinámica	5.79 %
T1569: Servicios del sistema	0.46 %
T1570: Transferencia lateral de herramienta	0.05 %
T1573: Canal cifrado	0.10 %
T1574: Flujo de ejecución de secuestro	0.61 %
T1587: Desarrollo de capacidades	0.97 %
T1588: Obtención de capacidades	0.26 %
T1595: Análisis activo	0.26 %
T1598: Phishing para obtener información	2.15 %
T1620: Carga de código reflectivo	0.05 %

TA0002: Ejecución

T1001: Confusión de datos	0.05 %
T1003: Volcado de credenciales de SO	4.56 %
T1005: Datos del sistema local	0.31 %
T1007: Descubrimiento de servicios del sistema	1.43 %
T1010: Detección de la ventana de la aplicación	0.15 %
T1011: Exfiltración por otro medio de la red	0.10 %
T1012: Consulta en registro	0.97 %
T1014: Rootkit	0.20 %
T1016: Descubrimiento de configuración de red del sistema	1.43 %
T1018: Descubrimiento de sistema remoto	0.36 %
T1021: Servicios remotos	9.94 %
T1027: Archivos o información ofuscados	3.33 %
T1029: Transferencia programada	0.05 %
T1033: Descubrimiento de usuario/propietario del sistem	2.36 %
T1036: Ocultación mediante disfraces	6.05 %
T1037: Scripts de inicialización de arranque o inicio de sesión	0.10 %
T1039: Datos de unidad compartida de red	0.20 %
T1041: Exfiltración por canal C2	0.26 %
T1046: Descubrimiento de servicio de red	0.46 %
T1047: Instrumental de administración de Windows	3.59 %
T1048: Exfiltración por sobre protocolo alternativo	0.46 %
T1049: Descubrimiento de conexiones de red del sistema	2.10 %
T1053: Tarea o trabajo programados	5.84 %
T1055: Inyección de procesos	1.69 %
T1056: Captura de entrada	0.41 %
T1057: Descubrimiento de procesos	0.36 %
T1059: Intérprete de comandos y scripts	21.36 %
T1068: Uso de exploit de escalación de privilegios	0.26 %
T1069: Descubrimiento de grupos de permiso	2.00 %
T1070: Eliminación de indicadores	1.18 %
T1071: Protocolo de capa de aplicación	21.82 %
T1078: Cuentas válidas	0.92 %
T1082: Descubrimiento de información del sistema	2.20 %
T1083: Descubrimiento de archivos y directorios	0.26 %
T1087: Descubrimiento de cuenta	3.38 %
T1090: Proxy	0.56 %
T1091: Replicación mediante medios extraíbles	0.15 %
T1095: Sin protocolo de capa de aplicación	0.31 %
T1098: Manipulación de cuenta	1.23 %
T1102: Servicio web	0.31 %
T1104: Canales multietapa	0.05 %
T1105: Transferencia de herramienta de ingreso	4.00 %
T1106: API nativa	0.31 %
T1110: Fuerza bruta	0.10 %
T1112: Modificación de registro	2.05 %
T1113: Captura de pantalla	0.15 %

1-5 % | 6-10 % | 11-15 % | >16 %

TA0002: Ejecución

T1114: Recopilación de correos electrónicos	0.10 %
T1119: Recolección automatizada	0.26 %
T1124: Detección de la hora del sistema	0.10 %
T1125: Captura de video	0.10 %
T1127: Ejecución por proxy de utilidades de desarrollador de confianza	0.20 %
T1129: Módulos compartidos	0.51 %
T1133: Servicios remotos externos	0.05 %
T1134: Manipulación del token de acceso	0.31 %
T1135: Descubrimiento de recurso compartido de red	0.36 %
T1136: Crear cuenta	0.77 %
T1137: Inicio de aplicación de Office	0.10 %
T1140: Decodificación/cancelación de ofuscación de archivos o información	0.36 %
T1187: Autenticación forzada	0.05 %
T1197: Trabajos de BITS	0.15 %
T1201: Descubrimiento de directivas de contraseñas	0.05 %
T1203: Explotación para la ejecución de los clientes	0.46 %
T1204: Ejecución de usuario	60.09 %
T1205: Señalización de tráfico	0.05 %
T1210: Abuso de servicios remotos	1.54 %
T1218: Ejecución por proxy de binario de sistema	5.43 %
T1219: Software de acceso remoto	0.15 %
T1220: Procesamiento de script XSL	0.05 %
T1222: Modificación de permisos de archivos y directorios	0.15 %
T1482: Descubrimiento de confianza de dominio	0.31 %
T1484: Modificación de directivas de dominios	0.10 %
T1485: Destrucción de datos	0.56 %
T1486: Datos cifrados por el impacto	0.82 %
T1489: Detención de servicios	0.10 %
T1496: Secuestro de recursos	2.00 %
T1497: Evasión de virtualización/sandbox	0.31 %
T1505: Componente de software de servidor	0.92 %
T1518: Detección de software	0.36 %
T1531: Eliminación de acceso a la cuenta	0.10 %
T1543: Creación o modificación de procesos del sistema	2.56 %
T1546: Ejecución activada por evento	2.36 %
T1547: Ejecución automática de arranque o inicio de sesión	7.89 %
T1548: Abuso del mecanismo de control de elevación	0.41 %
T1550: Uso de material de autenticación alternativo	0.15 %
T1552: Credenciales no protegidas	0.56 %
T1553: Alteración de controles de confianza	0.10 %
T1555: Credenciales desde almacenes de contraseña	0.97 %
T1558: Robo o falsificación de tickets de Kerberos	0.56 %
T1559: Comunicación entre procesos	1.18 %
T1560: Datos recolectados de archivos	0.51 %
T1561: Borrado de disco	1.08 %
T1562: Afectar defensas	0.87 %
T1563: Secuestro de sesión de servicio remoto	0.10 %
T1564: Ocultamiento de artefactos	1.64 %
T1565: Manipulación de datos	2.82 %
T1566: Phishing	0.26 %
T1567: Exfiltración por servicio web	0.31 %
T1568: Resolución dinámica	3.64 %
T1569: Servicios del sistema	7.79 %
T1570: Transferencia lateral de herramienta	1.18 %
T1571: Puerto no estándar	0.05 %
T1572: Tunelización de protocolo	0.15 %
T1573: Canal cifrado	0.15 %
T1574: Flujo de ejecución de secuestro	2.31 %
T1583: Adquisición de infraestructura	0.05 %
T1587: Desarrollo de capacidades	1.33 %
T1588: Obtención de capacidades	0.56 %
T1590: Recolección de información de red de la víctima	0.61 %
T1595: Análisis activo	0.05 %
T1615: Descubrimiento de directivas de grupos	0.36 %
T1620: Carga de código reflectivo	1.02 %

TA0003: Persistencia

T1003: Volcado de credenciales de SO	4.66 %
T1007: Descubrimiento de servicios del sistema	0.26 %
T1012: Consulta en registro	1.23 %
T1014: Rootkit	0.10 %
T1016: Descubrimiento de configuración de red del sistema	0.36 %
T1021: Servicios remotos	36.83 %
T1027: Archivos o información ofuscados	0.05 %
T1033: Descubrimiento de usuario/propietario del sistema	0.46 %
T1036: Ocultación mediante disfraces	6.45 %
T1037: Scripts de inicialización de arranque o inicio de sesión	0.10 %
T1039: Datos de unidad compartida de red	0.05 %
T1046: Descubrimiento de servicio de red	0.05 %
T1047: Instrumental de administración de Windows	0.31 %
T1049: Descubrimiento de conexiones de red del sistema	0.15 %
T1053: Tarea o trabajo programados	2.51 %
T1055: Inyección de procesos	0.51 %
T1057: Descubrimiento de procesos	0.05 %
T1059: Intérprete de comandos y scripts	0.46 %
T1068: Uso de exploit de escalación de privilegios	0.51 %
T1069: Descubrimiento de grupos de permiso	0.20 %
T1070: Eliminación de indicadores	0.46 %
T1071: Protocolo de capa de aplicación	0.36 %
T1078: Cuentas válidas	25.82 %
T1082: Descubrimiento de información del sistema	0.20 %
T1083: Descubrimiento de archivos y directorios	0.05 %
T1087: Descubrimiento de cuenta	6.56 %
T1090: Proxy	0.10 %
T1095: Sin protocolo de capa de aplicación	0.10 %
T1098: Manipulación de cuenta	87.50 %
T1105: Transferencia de herramienta de ingreso	0.05 %
T1110: Fuerza bruta	0.05 %
T1112: Modificación de registro	2.05 %
T1113: Captura de pantalla	0.05 %
T1134: Manipulación del token de acceso	0.10 %
T1135: Descubrimiento de recurso compartido de red	0.10 %
T1136: Crear cuenta	0.67 %
T1137: Inicio de aplicación de Office	0.36 %
T1140: Decodificación/cancelación de ofuscación de archivos o información	0.10 %
T1176: Extensiones de navegador	0.87 %
T1197: Trabajos de BITS	0.05 %
T1204: Ejecución de usuario	0.56 %
T1207: Controlador de dominio falso	0.46 %
T1211: Abuso para evadir defensas	0.26 %
T1212: Exploit de acceso mediante credenciales	0.05 %
T1218: Ejecución por proxy de binario de sistema	0.46 %
T1219: Software de acceso remoto	0.10 %
T1222: Modificación de permisos de archivos y directorios	0.15 %
T1484: Modificación de directivas de dominios	0.10 %
T1496: Secuestro de recursos	1.64 %
T1505: Componente de software de servidor	6.81 %
T1531: Eliminación de acceso a la cuenta	0.20 %
T1542: Arranque previo al SO	0.26 %
T1543: Creación o modificación de procesos del sistema	2.00 %
T1546: Ejecución activada por evento	7.48 %
T1547: Ejecución automática de arranque o inicio de sesión	9.43 %
T1548: Abuso del mecanismo de control de elevación	0.20 %
T1552: Credenciales no protegidas	1.33 %
T1554: Binario de software de cliente comprometido	0.05 %
T1556: Modificación en proceso de autenticación	0.51 %
T1558: Robo o falsificación de tickets de Kerberos	0.15 %
T1559: Comunicación entre procesos	0.05 %

1-5 % 6-10 % 11-15 % >16 %

TA0003: Persistencia

T1561: Borrado de disco	0.05 %
T1562: Afectar defensas	0.41 %
T1563: Secuestro de sesión de servicio remoto	0.05 %
T1564: Ocultamiento de artefactos	2.10 %
T1565: Manipulación de datos	0.05 %
T1567: Exfiltración por servicio web	0.10 %
T1569: Servicios del sistema	0.10 %
T1570: Transferencia lateral de herramienta	0.15 %
T1571: Puerto no estándar	0.05 %
T1574: Flujo de ejecución de secuestro	1.13 %
T1587: Desarrollo de capacidades	0.05 %
T1588: Obtención de capacidades	0.10 %
T1600: Debilitamiento de cifrado	0.26 %
T1608: Capacidades de etapas	0.05 %
T1620: Carga de código reflectivo	0.10 %
T1649: Robo o falsificación de certificados de autenticación	0.05 %
T1620: Carga de código reflectivo	1.02 %

TA0004: Escalación de privilegios

T1003: Volcado de credenciales de SO	0.10 %
T1014: Rootkit	0.56 %
T1021: Servicios remotos	0.26 %
T1033: Descubrimiento de usuario/propietario del sistema	0.10 %
T1036: Ocultación mediante disfraces	0.05 %
T1055: Inyección de procesos	0.67 %
T1068: Uso de exploit de escalación de privilegios	1.02 %
T1078: Cuentas válidas	22.69 %
T1082: Descubrimiento de información del sistema	0.05 %
T1098: Manipulación de cuenta	21.98 %
T1112: Modificación de registro	0.10 %
T1134: Manipulación del token de acceso	0.26 %
T1135: Descubrimiento de recurso compartido de red	0.05 %
T1203: Explotación para la ejecución de los clientes	0.05 %
T1210: Abuso de servicios remotos	0.10 %
T1212: Exploit de acceso mediante credenciales	0.26 %
T1543: Creación o modificación de procesos del sistema	0.05 %
T1546: Ejecución activada por evento	0.20 %
T1548: Abuso del mecanismo de control de elevación	1.18 %
T1552: Credenciales no protegidas	0.05 %
T1558: Robo o falsificación de tickets de Kerberos	0.10 %
T1562: Afectar defensas	0.05 %
T1574: Flujo de ejecución de secuestro	0.05 %
T1620: Carga de código reflectivo	0.10 %
T1649: Robo o falsificación de certificados de autenticación	0.05 %

TA0005: Evasión de defensas

T1003: Volcado de credenciales de SO	2.05 %
T1005: Datos del sistema local	0.15 %
T1010: Detección de la ventana de la aplicación	0.77 %
T1014: Rootkit	0.41 %
T1021: Servicios remotos	0.41 %
T1027: Archivos o información ofuscados	0.20 %
T1033: Descubrimiento de usuario/propietario del sistema	0.15 %
T1036: Ocultación mediante disfraces	1.84 %
T1047: Instrumental de administración de Windows	0.10 %
T1049: Descubrimiento de conexiones de red del sistema	0.10 %
T1055: Inyección de procesos	0.72 %
T1056: Captura de entrada	0.92 %
T1059: Intérprete de comandos y scripts	0.15 %
T1069: Descubrimiento de grupos de permiso	0.05 %
T1070: Eliminación de indicadores	1.64 %
T1071: Protocolo de capa de aplicación	0.36 %
T1074: Datos preparados	0.05 %
T1082: Descubrimiento de información del sistema	0.31 %
T1083: Descubrimiento de archivos y directorios	0.10 %
T1087: Descubrimiento de cuenta	0.15 %
T1098: Manipulación de cuenta	0.05 %
T1105: Transferencia de herramienta de ingreso	0.10 %
T1112: Modificación de registro	0.51 %
T1119: Recolección automatizada	0.10 %
T1120: Detección de dispositivos periféricos	0.10 %
T1140: Decodificación/cancelación de ofuscación de archivos o información	0.41 %
T1185: Secuestro de sesión de navegador	0.05 %
T1204: Ejecución de usuario	0.51 %
T1207: Controlador de dominio falso	1.64 %
T1210: Abuso de servicios remotos	0.10 %
T1218: Ejecución por proxy de binario de sistema	0.72 %
T1219: Software de acceso remoto	0.05 %
T1222: Modificación de permisos de archivos y directorios	0.15 %
T1482: Descubrimiento de confianza de dominio	0.05 %
T1484: Modificación de directivas de dominios	0.10 %
T1485: Destrucción de datos	0.05 %
T1486: Datos cifrados por el impacto	0.05 %
T1489: Detención de servicios	0.10 %
T1490: Inhibición de recuperación del sistema	0.10 %
T1496: Secuestro de recursos	0.05 %
T1497: Evasión de virtualización/sandbox	0.05 %
T1505: Componente de software de servidor	0.15 %
T1518: Detección de software	0.05 %
T1531: Eliminación de acceso a la cuenta	0.10 %
T1547: Ejecución automática de arranque o inicio de sesión	0.05 %
T1548: Abuso del mecanismo de control de elevación	0.05 %
T1550: Uso de material de autenticación alternativo	0.10 %
T1552: Credenciales no protegidas	0.15 %
T1553: Alteración de controles de confianza	1.28 %
T1555: Credenciales desde almacenes de contraseña	0.05 %
T1558: Robo o falsificación de tickets de Kerberos	0.10 %
T1559: Comunicación entre procesos	0.05 %
T1560: Datos recolectados de archivos	0.05 %
T1561: Borrado de disco	0.10 %
T1562: Afectar defensas	2.77 %
T1563: Secuestro de sesión de servicio remoto	0.15 %
T1564: Ocultamiento de artefactos	0.51 %
T1565: Manipulación de datos	0.41 %
T1570: Transferencia lateral de herramienta	0.05 %
T1572: Tunelización de protocolo	0.15 %
T1574: Flujo de ejecución de secuestro	0.36 %
T1588: Obtención de capacidades	0.05 %
T1620: Carga de código reflectivo	0.05 %

TA0006: Acceso a credenciales

T1003: Volcado de credenciales de SO	39.91 %
T1005: Datos del sistema local	0.05 %
T1007: Descubrimiento de servicios del sistema	0.05 %
T1010: Detección de la ventana de la aplicación	0.05 %
T1012: Consulta en registro	0.05 %
T1018: Descubrimiento de sistema remoto	0.05 %
T1021: Servicios remotos	2.46 %
T1033: Descubrimiento de usuario/propietario del sistema	0.05 %
T1040: Rastreo de red	0.26 %
T1047: Instrumental de administración de Windows	0.10 %
T1055: Inyección de procesos	0.05 %
T1056: Captura de entrada	0.92 %
T1071: Protocolo de capa de aplicación	0.15 %
T1078: Cuentas válidas	0.20 %
T1082: Descubrimiento de información del sistema	0.05 %
T1083: Descubrimiento de archivos y directorios	0.05 %
T1087: Descubrimiento de cuenta	0.15 %

1-5 % 6-10 % 11-15 % >16 %

TA0006: Acceso a credenciales

T1098: Manipulación de cuenta	0.05 %
T1110: Fuerza bruta	35.66 %
T1113: Captura de pantalla	0.10 %
T1204: Ejecución de usuario	0.67 %
T1210: Abuso de servicios remotos	0.31 %
T1212: Exploit de acceso mediante credenciales	0.05 %
T1482: Descubrimiento de confianza de dominio	0.05 %
T1539: Robo de cookies de sesión web	0.05 %
T1547: Ejecución automática de arranque o inicio de sesión	0.05 %
T1552: Credenciales no protegidas	2.20 %
T1552: Credenciales no protegidas	2.20 %
T1555: Credenciales desde almacenes de contraseña	2.61 %
T1557: Adversario intermediario	0.20 %
T1558: Robo o falsificación de tickets de Kerberos	1.69 %
T1559: Comunicación entre procesos	0.10 %
T1562: Afectar defensas	0.26 %
T1565: Manipulación de datos	0.15 %
T1572: Tunelización de protocolo	0.05 %
T1588: Obtención de capacidades	0.05 %
T1600: Debilitamiento de cifrado	0.20 %
T1608: Capacidades de etapas	0.05 %
T1649: Robo o falsificación de certificados de autenticación	0.20 %

TA0007: Descubrimiento

T1007: Descubrimiento de servicios del sistema	0.87 %
T1012: Consulta en registro	0.15 %
T1016: Descubrimiento de configuración de red del sistema	0.92 %
T1018: Descubrimiento de sistema remoto	0.51 %
T1021: Servicios remotos	1.02 %
T1033: Descubrimiento de usuario/propietario del sistema	0.97 %
T1039: Datos de unidad compartida de red	0.05 %
T1040: Rastreo de red	0.05 %
T1046: Descubrimiento de servicio de red	1.64 %
T1047: Instrumental de administración de Windows	0.15 %
T1049: Descubrimiento de conexiones de red del sistema	1.23 %
T1059: Intérprete de comandos y scripts	0.05 %
T1069: Descubrimiento de grupos de permiso	0.31 %
T1082: Descubrimiento de información del sistema	0.31 %
T1083: Descubrimiento de archivos y directorios	0.05 %
T1087: Descubrimiento de cuenta	0.92 %
T1105: Transferencia de herramienta de ingreso	0.26 %
T1110: Fuerza bruta	0.05 %
T1135: Descubrimiento de recurso compartido de red	0.20 %
T1210: Abuso de servicios remotos	0.31 %
T1482: Descubrimiento de confianza de dominio	0.10 %
T1518: Detección de software	0.15 %
T1552: Credenciales no protegidas	0.20 %
T1552: Credenciales no protegidas	0.20 %
T1559: Comunicación entre procesos	0.05 %
T1560: Datos recolectados de archivos	0.10 %
T1595: Análisis activo	0.72 %
T1615: Descubrimiento de directivas de grupos	0.15 %

TA0008: Movimiento lateral

T1021: Servicios remotos	14.96 %
T1047: Instrumental de administración de Windows	0.82 %
T1071: Protocolo de capa de aplicación	0.36 %
T1090: Proxy	0.05 %
T1091: Replicación mediante medios extraíbles	0.10 %
T1110: Fuerza bruta	0.31 %
T1112: Modificación de registro	0.05 %
T1133: Servicios remotos externos	0.41 %
T1190: Exploit de aplicación de atención al cliente	0.46 %
T1204: Ejecución de usuario	0.10 %
T1210: Abuso de servicios remotos	100 %
T1219: Software de acceso remoto	0.31 %
T1484: Modificación de directivas de dominios	0.15 %
T1486: Datos cifrados por el impacto	0.05 %
T1534: Spear phishing interno	0.05 %
T1546: Ejecución activada por evento	0.05 %
T1550: Uso de material de autenticación alternativo	0.26 %
T1559: Comunicación entre procesos	0.87 %
T1570: Transferencia lateral de herramienta	0.15 %
T1572: Tunelización de protocolo	0.05 %
T1587: Desarrollo de capacidades	0.05 %

TA0009: Recolección

T1005: Datos del sistema local	0.15 %
T1005: Datos del sistema local	0.15 %
T1020: Exfiltración automatizada	0.05 %
T1056: Captura de entrada	0.46 %
T1113: Captura de pantalla	1.28 %
T1114: Recopilación de correos electrónicos	0.10 %
T1119: Recolección automatizada	0.10 %
T1125: Captura de video	0.87 %
T1560: Datos recolectados de archivos	0.05 %

TA0010: Exfiltración

T1030: Límites de tamaño de transferencia de datos	0.05 %
T1041: Exfiltración por canal C2	0.05 %

TA0011: Comando y control

T1048: Exfiltración por sobre protocolo alternativo	0.10 %
T1071: Protocolo de capa de aplicación	18.60 %
T1090: Proxy	0.61 %
T1095: Sin protocolo de capa de aplicación	3.33 %
T1102: Servicio web	0.10 %
T1105: Transferencia de herramienta de ingreso	0.97 %
T1204: Ejecución de usuario	0.10 %
T1205: Señalización de tráfico	0.05 %
T1210: Abuso de servicios remotos	0.10 %
T1219: Software de acceso remoto	0.36 %
T1486: Datos cifrados por el impacto	0.05 %
T1496: Secuestro de recursos	0.20 %
T1566: Phishing	0.05 %
T1568: Resolución dinámica	2.72 %
T1571: Puerto no estándar	0.05 %
T1572: Tunelización de protocolo	1.28 %
T1583: Adquisición de infraestructura	0.05 %
T1588: Obtención de capacidades	0.05 %
T1590: Recolección de información de red de la víctima	0.05 %

TA0040: Impacto

T1059: Intérprete de comandos y scripts	0.05 %
T1204: Ejecución de usuario	7.99 %
T1485: Destrucción de datos	2.36 %
T1486: Datos cifrados por el impacto	2.66 %
T1496: Secuestro de recursos	3.18 %
T1531: Eliminación de acceso a la cuenta	0.05 %
T1561: Borrado de disco	5.17 %
T1565: Manipulación de datos	8.20 %
T1587: Desarrollo de capacidades	0.05 %
T1588: Obtención de capacidades	0.05 %

1-5 % | 6-10 % | 11-15 % | >16 %

TA0042: Desarrollo de recursos

T1001: Confusión de datos	0.10 %
T1003: Volcado de credenciales de SO	3.89 %
T1005: Datos del sistema local	0.10 %
T1007: Descubrimiento de servicios del sistema	0.46 %
T1010: Detección de la ventana de la aplicación	0.10 %
T1012: Consulta en registro	0.20 %
T1014: Rootkit	0.51 %
T1016: Descubrimiento de configuración de red del sistema	0.51 %
T1018: Descubrimiento de sistema remoto	1.74 %
T1021: Servicios remotos	4.41 %
T1027: Archivos o información ofuscados	0.77 %
T1033: Descubrimiento de usuario/propietario del sistema	0.87 %
T1036: Ocultación mediante disfraces	1.69 %
T1037: Scripts de inicialización de arranque o inicio de sesión	0.10 %
T1041: Exfiltración por canal C2	0.05 %
T1046: Descubrimiento de servicio de red	0.05 %
T1047: Instrumental de administración de Windows	0.51 %
T1049: Descubrimiento de conexiones de red del sistema	0.46 %
T1053: Tarea o trabajo programados	1.74 %
T1055: Inyección de procesos	5.53 %
T1056: Captura de entrada	0.36 %
T1057: Descubrimiento de procesos	0.10 %
T1059: Intérprete de comandos y scripts	3.18 %
T1068: Uso de exploit de escalación de privilegios	0.51 %
T1069: Descubrimiento de grupos de permiso	2.20 %
T1070: Eliminación de indicadores	0.20 %
T1071: Protocolo de capa de aplicación	2.66 %
T1074: Datos preparados	0.05 %
T1087: Descubrimiento de cuenta	2.61 %
T1090: Proxy	0.20 %
T1091: Replicación mediante medios extraíbles	0.20 %
T1092: Comunicación mediante medios extraíbles	0.05 %
T1095: Sin protocolo de capa de aplicación	0.20 %
T1098: Manipulación de cuenta	0.20 %
T1102: Servicio web	0.10 %
T1105: Transferencia de herramienta de ingreso	0.82 %
T1106: API nativa	0.15 %
T1110: Fuerza bruta	0.36 %
T1112: Modificación de registro	0.51 %
T1113: Captura de pantalla	0.05 %
T1119: Recolección automatizada	0.10 %
T1125: Captura de video	0.05 %
T1127: Ejecución por proxy de utilidades de desarrollador de confianza	0.05 %
T1129: Módulos compartidos	0.20 %
T1133: Servicios remotos externos	0.10 %
T1134: Manipulación del token de acceso	0.05 %
T1135: Descubrimiento de recurso compartido de red	0.20 %
T1137: Inicio de aplicación de Office	0.05 %
T1140: Decodificación/cancelación de ofuscación de archivos o información	0.10 %
T1187: Autenticación forzada	0.05 %
T1189: Infección oculta	0.41 %
T1190: Exploit de aplicación de atención al cliente	0.36 %
T1195: Compromiso de cadena de suministro	0.05 %
T1203: Explotación para la ejecución de los clientes	0.05 %
T1204: Ejecución de usuario	20.18 %
T1210: Abuso de servicios remotos	3.13 %
T1211: Abuso para evadir defensas	0.10 %
T1212: Exploit de acceso mediante credenciales	0.15 %
T1218: Ejecución por proxy de binario de sistema	0.92 %
T1482: Descubrimiento de confianza de dominio	1.69 %
T1484: Modificación de directivas de dominios	0.05 %
T1485: Destrucción de datos	0.51 %
T1486: Datos cifrados por el impacto	0.82 %
T1490: Inhibición de recuperación del sistema	0.05 %
T1496: Secuestro de recursos	1.43 %
T1498: Denegación de servicio de red	0.10 %
T1499: Denegación de servicio de endpoints	0.51 %
T1505: Componente de software de servidor	1.64 %
T1518: Detección de software	0.10 %
T1534: Spear phishing interno	0.05 %
T1539: Robo de cookies de sesión web	0.05 %
T1543: Creación o modificación de procesos del sistema	0.97 %
T1546: Ejecución activada por evento	0.15 %
T1547: Ejecución automática de arranque o inicio de sesión	2.25 %
T1548: Abuso del mecanismo de control de elevación	0.10 %
T1550: Uso de material de autenticación alternativo	0.10 %
T1552: Credenciales no protegidas	0.20 %
T1553: Alteración de controles de confianza	0.36 %
T1554: Binario de software de cliente comprometido	0.05 %
T1555: Credenciales desde almacenes de contraseña	2.00 %
T1556: Modificación en proceso de autenticación	0.31 %
T1558: Robo o falsificación de tickets de Kerberos	0.15 %
T1559: Comunicación entre procesos	0.46 %
T1560: Datos recolectados de archivos	0.36 %
T1561: Borrado de disco	1.23 %
T1562: Afectar defensas	0.15 %
T1564: Ocultamiento de artefactos	0.67 %
T1565: Manipulación de datos	4.76 %
T1566: Phishing	1.08 %
T1567: Exfiltración por servicio web	0.15 %
T1569: Servicios del sistema	3.38 %
T1570: Transferencia lateral de herramienta	0.46 %
T1572: Tunelización de protocolo	0.10 %
T1573: Canal cifrado	0.10 %
T1574: Flujo de ejecución de secuestro	1.33 %
T1583: Adquisición de infraestructura	0.41 %
T1584: Compromiso de infraestructura	0.41 %
T1586: Compromiso de cuentas	0.05 %
T1587: Desarrollo de capacidades	45.08 %
T1588: Obtención de capacidades	43.49 %
T1595: Análisis activo	0.10 %
T1608: Capacidades de etapas	6.10 %
T1615: Descubrimiento de directivas de grupos	1.69 %
T1620: Carga de código reflectivo	2.20 %

TA0043: Reconocimiento

T1003: Volcado de credenciales de SO	0.10 %
T1018: Descubrimiento de sistema remoto	0.05 %
T1021: Servicios remotos	0.46 %
T1027: Archivos o información ofuscados	0.05 %
T1046: Descubrimiento de servicio de red	3.38 %
T1059: Intérprete de comandos y scripts	0.15 %
T1070: Eliminación de indicadores	0.05 %
T1071: Protocolo de capa de aplicación	3.23 %
T1082: Descubrimiento de información del sistema	0.05 %
T1095: Sin protocolo de capa de aplicación	0.31 %
T1105: Transferencia de herramienta de ingreso	0.15 %
T1110: Fuerza bruta	0.46 %
T1133: Servicios remotos externos	0.05 %
T1190: Exploit de aplicación de atención al cliente	0.36 %
T1204: Ejecución de usuario	3.69 %
T1210: Abuso de servicios remotos	0.46 %
T1486: Datos cifrados por el impacto	0.05 %
T1498: Denegación de servicio de red	0.05 %
T1499: Denegación de servicio de endpoints	0.26 %
T1505: Componente de software de servidor	0.05 %
T1543: Creación o modificación de procesos del sistema	0.05 %
T1547: Ejecución automática de arranque o inicio de sesión	0.10 %
T1566: Phishing	3.84 %
T1568: Resolución dinámica	1.84 %
T1569: Servicios del sistema	0.15 %
T1587: Desarrollo de capacidades	0.56 %
T1588: Obtención de capacidades	0.26 %
T1589: Recolección de información de identidad de la víctima	0.05 %
T1590: Recolección de información de red de la víctima	0.56 %
T1592: Recolección de información de host de la víctima	0.36 %
T1595: Análisis activo	10.35 %
T1598: Phishing para obtener información	3.74 %

1-5 % | 6-10 % | 11-15 % | >16 %

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 Kaspersky Lab se transforman constantemente en soluciones y servicios de seguridad para proteger empresas, infraestructuras críticas, gobiernos y consumidores de todo el mundo. Nuestra cartera integral de seguridad incluye protección líder en endpoints, y soluciones y servicios de seguridad especializados para combatir amenazas digitales sofisticadas y en evolución.

Servicios de ciberseguridad

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky Compromise Assessment

Kaspersky Digital Footprint Intelligence

Kaspersky Security Assessment

Kaspersky SOC Consulting

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 premiada.

Más información

Más de 5000
profesionales trabajan en Kaspersky

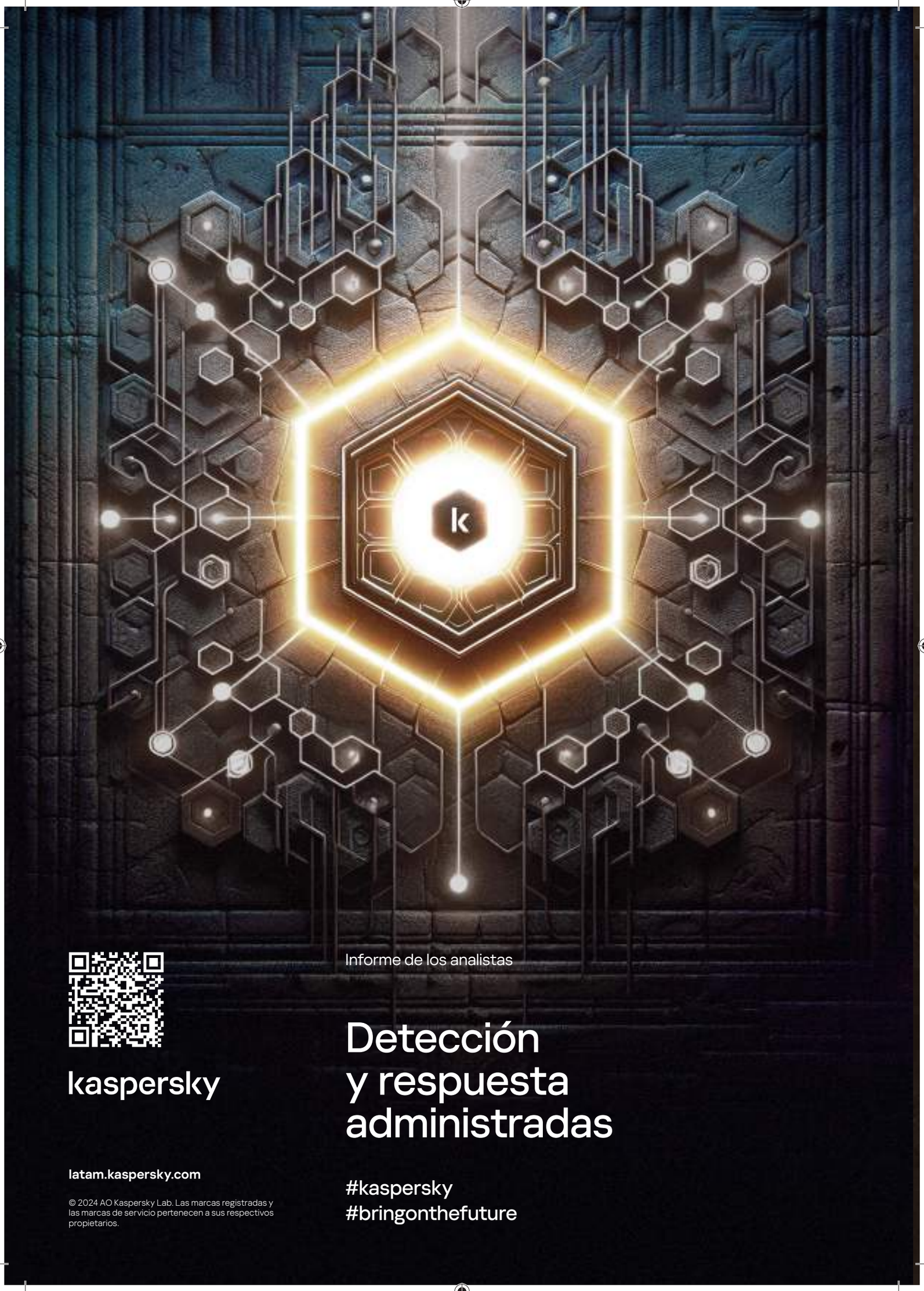
50 %
de los empleados son especialistas en I+D

5
centros de excelencia únicos

Más de 410 000
nuevos archivos maliciosos detectados por Kaspersky cada día

Más de 220 000
clientes corporativos en todo el mundo

6100 millones
de ciberataques detectados por nuestras soluciones en 2023



Informe de los analistas

Detección y respuesta administradas

#kaspersky
#bringonthefuture

kaspersky

latam.kaspersky.com