



Informe de analistas

Incident Response

Índice



R esumen ejecutivo

Vectores iniciales de ataque



39 %

Exploit de una aplicación pública



31 %

Cuentas válidas



13 %

Relación de confianza

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

Explore y complete tareas

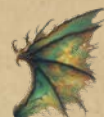
Recomendaciones

- Implementa reglas para detectar las herramientas más comunes que utilizan los atacantes
- Lleva a cabo actividades de evaluación de riesgos con frecuencia
- Utiliza una herramienta de seguridad con telemetría similar a EDR



22 %

Mimikatz



20 %

PsExec



15 %

SoftPerfect Network Scanner

Impacto



42 %

Archivos cifrados



17 %

Filtración de datos



11 %

Persistencia instalada para impactos futuros

Recomendaciones

- Crea copias de seguridad de datos críticos con regularidad y almacénalas de forma segura
- Configura un control de acceso basado en roles
- Trabaja con un partner de IR para garantizar tiempos de respuesta rápidos



24 %

Industria



16 %

Gubernamental



13 %

Finanzas

Conoce a cada adversario y los ataques hacia tu industria y región para priorizar las inversiones en seguridad



51 %

CEI

16 %

Oriente Medio

11 %

Europa

Vista de métricas de operaciones de seguridad

Duración del ataque



Corto

(horas y días)
Menos de 1 día



Media

(semanas)
13 días



Largo plazo

(meses)
253 días

La mayoría de los ataques más veloces son incidentes que tienen un impacto visible y se clasifican como de ransomware

Motivos de la detección

39 %

Archivos cifrados

18 %

Actividad sospechosa en terminales

Los avisos sobre actividades sospechosas de herramientas de seguridad han permitido detectar los ataques en sus primeras etapas y disminuir su impacto

10 %

Archivo sospechoso

10 %

Actividad sospechosa de red

Duración de la corrección

33 horas

(ataques rápidos)

50 horas

(ataques duraderos)

40 horas

(ataques promedio)

Si quieres disminuir el tiempo de corrección, comienza optimizando tu equipo de IR antes de un incidente



Descripción general y recomendaciones

- En 2024 vimos un gran aumento en el uso de cuentas válidas por parte de los atacantes para acceder a diversas infraestructuras. Esto es un indicador de que hay cada vez más empresas que son el objetivo de intermediarios de acceso inicial (IAB) que venden estos datos en la Web oscura para su uso en ataques. En el ámbito del ransomware como servicios (RAAS), los IAB juegan un papel fundamental, ya que permiten a los ciberdelincuentes optimizar sus ataques. Esto significa que las víctimas ya estaban en riesgo: sus credenciales se filtran, pero sus consecuencias no son notorias. Esto resalta la importancia de las actividades frecuentes de evaluación de riesgos.
- Otra tendencia que se ha mantenido sin cambios durante los últimos años es el ransomware. En 2024, el 41,6 % de los incidentes estuvo relacionado con esta clase de amenaza; sin embargo, el año anterior, el ransomware representó el 33,3 %. Parece que el ransomware seguirá siendo la principal amenaza para las organizaciones de todo el mundo en un futuro próximo.
- LockBit fue responsable del 43,6 % de las infecciones, seguido de Babuk con un 9,1 % y Phobos con un 5,5 %. Durante el 2024, también se observó el ascenso de **nuevas familias de ransomware, como ShrinkLocker e Ymir**.
- En 2024 también fue notorio el uso extendido de Mimikatz (21,8 %) y PsExec (20,0 %). Estas herramientas suelen utilizarse después de un exploit en la extracción de contraseñas y el movimiento lateral.

Las herramientas más populares en 2024



Mimikatz

22 %



PsExec

20 %

Nuevas amenazas descubiertas por GERT

Nuestro equipo hizo muchos descubrimientos significativos e interesantes en 2024, desde nuevas familias de malware, como ShrinkLocker¹ y Ymir² hasta descubrir sofisticadas campañas como Tusk³ y la explotación a gran escala de CVE-2023-48788⁴. Al responder ante estos incidentes, nuestro equipo de especialistas también descubrió a atacantes que usaban el compilador filtrado de LockBit 3.0⁵ y ElPaco, la variante de Mimic⁶.

Actividades de APT

El 26,3 % de los ataques se atribuye a grupos reconocidos. De ellos, una tercera parte (31,7 %) no ha podido atribuirse a ningún grupo específico. BlackJack fue el grupo más activo, con un 9,8 % de los ataques, mientras que GREF, DarkStar y CloudAtlas también fueron destacados y contribuyeron cada uno con alrededor de un 5 %. Las empresas industriales y financieras y las instituciones gubernamentales son las que más sufrieron ataques dirigidos: representan el 26,8 %, el 19,5 % y el 19,5 %, respectivamente, de todos los ataques dirigidos.

1 SecureList. ShrinkLocker: Convertir BitLocker en ransomware

2 SecureList. Ymir: nuevo ransomware sigiloso suelto

3 SecureList. Tusk: cómo desentrañar una compleja campaña de robo de información

4 SecureList. Los atacantes aprovechan una vulnerabilidad parcheada suelta de FortiClient EMS

5 SecureList. Uso del creador de LockBit para generar ransomware dirigido

6 SecureList. Análisis de ElPaco: una variante de Mimic



Introducción

Este informe de analistas contiene información sobre los ciberataques que Kaspersky ha investigado en 2024. 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 Rusia, Europa, Asia, América del Norte y del Sur, Oriente Medio y África.

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 los ataques. También nos permite obtener una idea del panorama de amenazas por región e industria.



Acerca de Kaspersky Incident Response

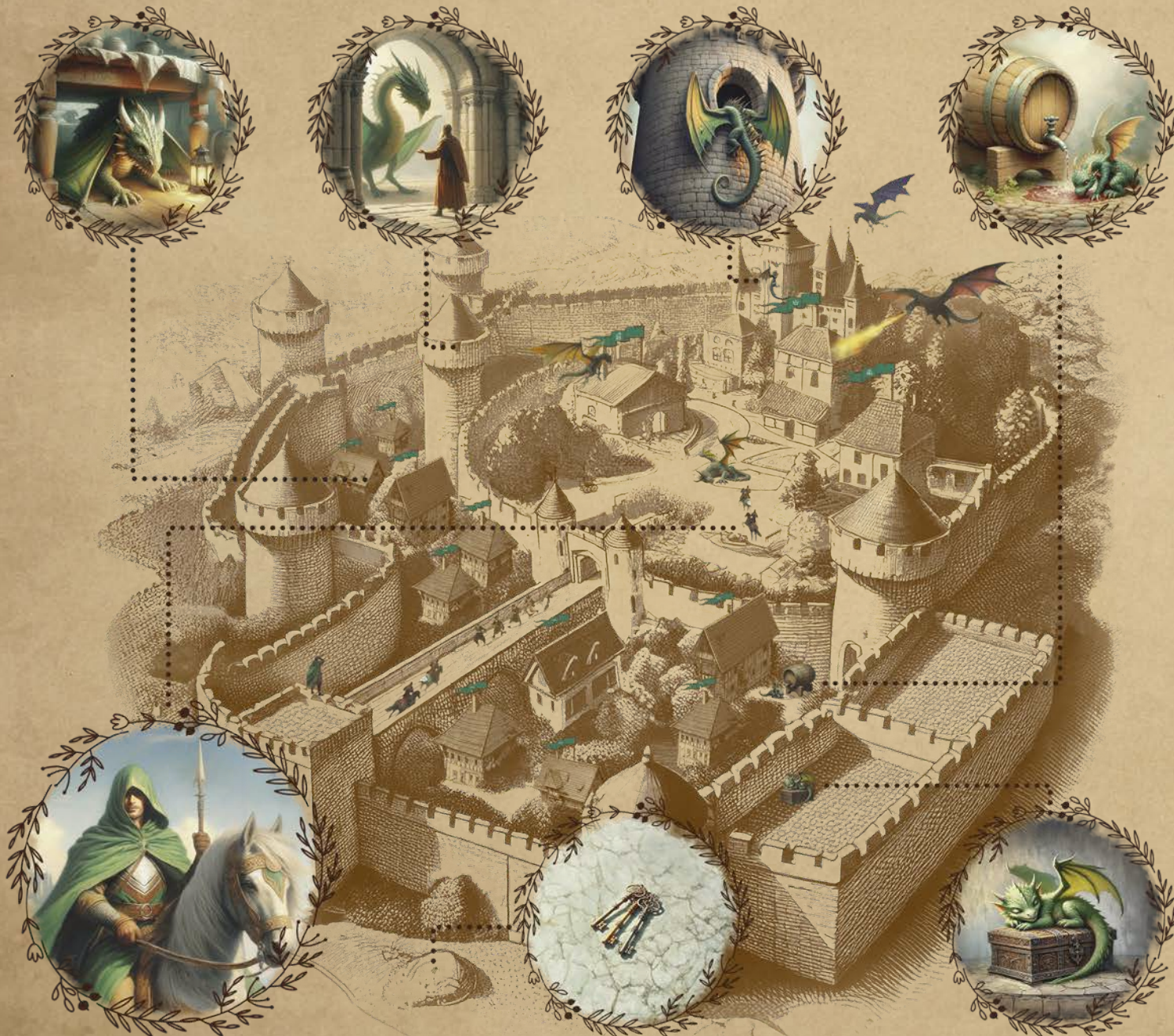
Kaspersky Incident Response (IR) ofrece un análisis completo y detallado sobre los incidentes de seguridad. Este servicio abarca todo el proceso de investigación y respuesta e incluye la respuesta inicial, la recopilación de pruebas, la identificación del vector de ataque principal y el desarrollo de un plan de mitigación. Forma parte integral de Kaspersky Security Services⁷, que garantiza que tu organización cuente con las herramientas necesarias para contener y neutralizar las amenazas con confianza.

Persistencia instalada para impactos futuros: 11 %

Relación de confianza: 13 %

Exploit de aplicaciones públicas: 39 %

Filtración de datos: 17 %



Incident Response

Cuentas válidas: 31 %

Archivos cifrados: 42 %

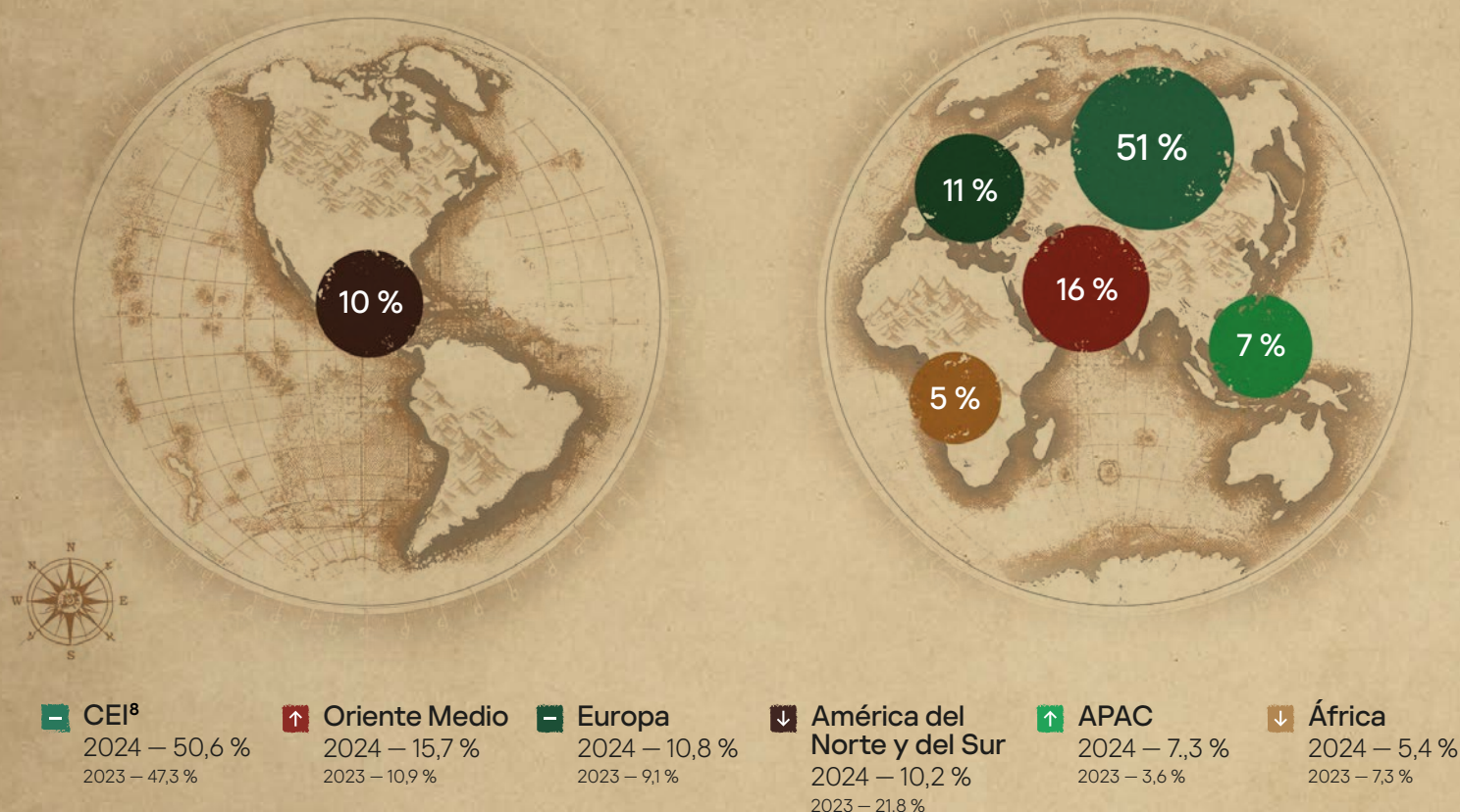
⁷ Servicios de Seguridad de Kaspersky

Ubicaciones geográficas de las solicitudes del servicio IR

El 2024 fue testigo de un cambio en la ubicación geográfica de la cobertura del servicio. La región de Medio Oriente ocupó el segundo lugar en términos de solicitudes de respuesta a incidentes con un 15,7 % de las solicitudes y desplazó a América al cuarto lugar. La CEI⁸ mantiene una posición predominante con el 50,6 % de las solicitudes y continúa en aumento.

Figura 1

Ubicaciones geográficas de las solicitudes del servicio Kaspersky Incident Response en 2024



Ngwxk tmmtvd?
Px'ox zhm rhnk utvd,
vhgmtvm nl

Shift son los 2 primeros números del año de la fundación Kaspersky

Ponte en contacto con nosotros

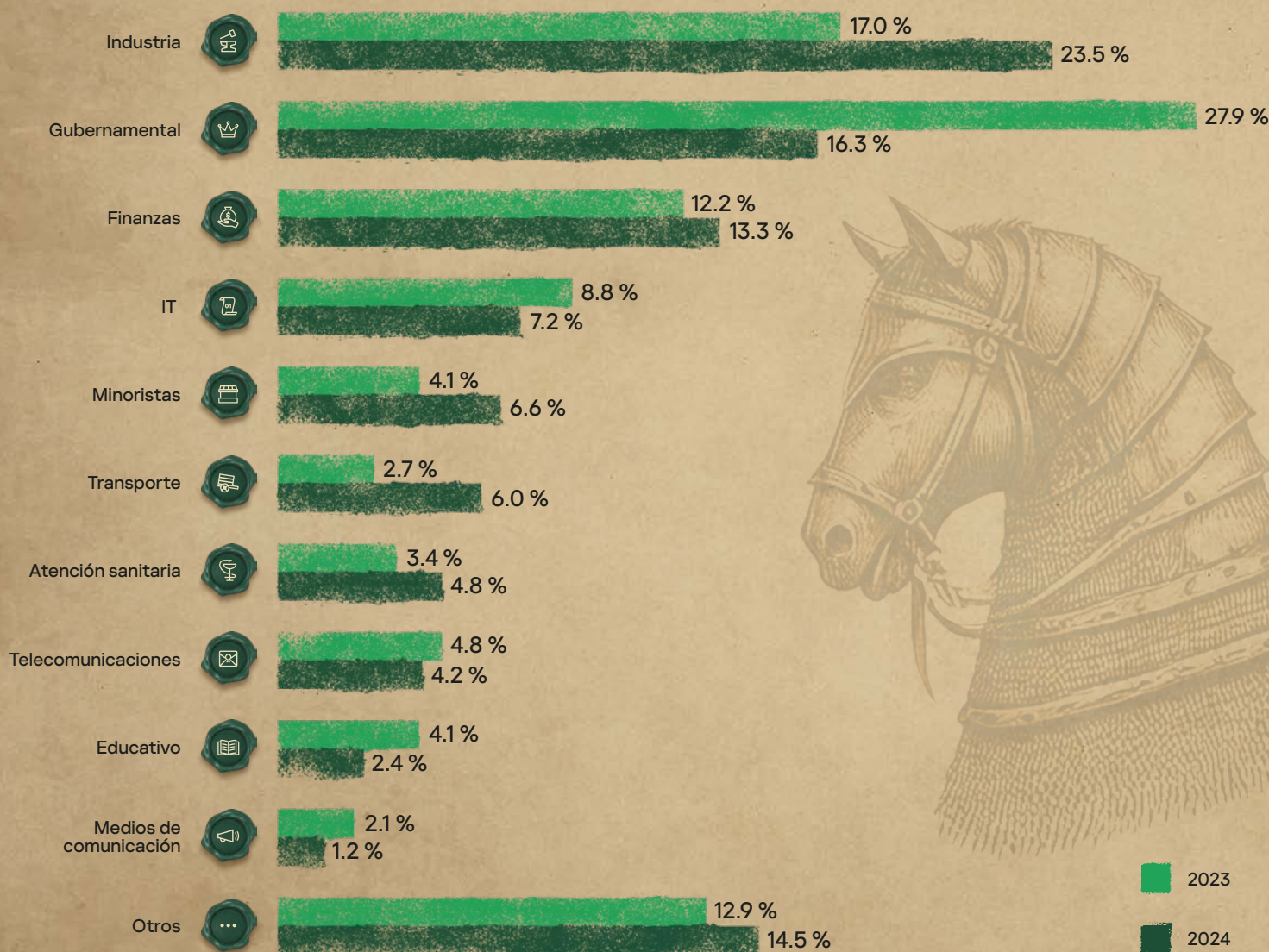
⁸ Comunidad de Estados Independientes (Armenia, Azerbaiyán, Bielorrusia, Kazajistán, Kirguistán, Moldavia, Rusia, Tayikistán, Uzbekistán)

Industrias

Hoy en día, todas las organizaciones son vulnerables a los ciberataques, como reflejan las estadísticas de solicitudes que engloban a diversas industrias. El año pasado, los sectores industrial, gubernamental y financiero fueron los que más nos solicitaron ayuda. Esto se debe, en gran medida, a que estas organizaciones suelen tener más personal y mayores niveles de computarización, lo que aumenta su superficie de ataque. En consecuencia, por un lado son más susceptibles a los ataques y, por el otro, se vuelven objetivos más atractivos para los ciberdelincuentes.

Figura 2

Distribución de las solicitudes de los servicios Kaspersky Incident Response por sector



Madurez de las organizaciones

Tras analizar los motivos de las solicitudes del servicio Kaspersky Incident Response por parte de las organizaciones, 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	41.6 %
Filtración de datos	16.9 %
Destrucción	1.7 %
Robo de dinero	0.6 %
Servicio no disponible	0.6 %

Grupo II

(ataques con indicadores de actividad sospechosa)



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

Persistencia instalada para impactos futuros	10.7 %
Active Directory comprometido	9.6 %
Ninguno (falsa alarma)	5.6 %
Apropiación de cuentas	4.5 %
Ninguno (Ataque prevenido o no completado)	4.5 %
Destrucción de datos	3.4 %
Manipulación de datos	0.6 %

Por supuesto, algunos de estos incidentes también podrían agravarse y convertirse en incidentes más graves. Al detectar los ataques en sus primeras etapas, se podrá minimizar su impacto.



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.

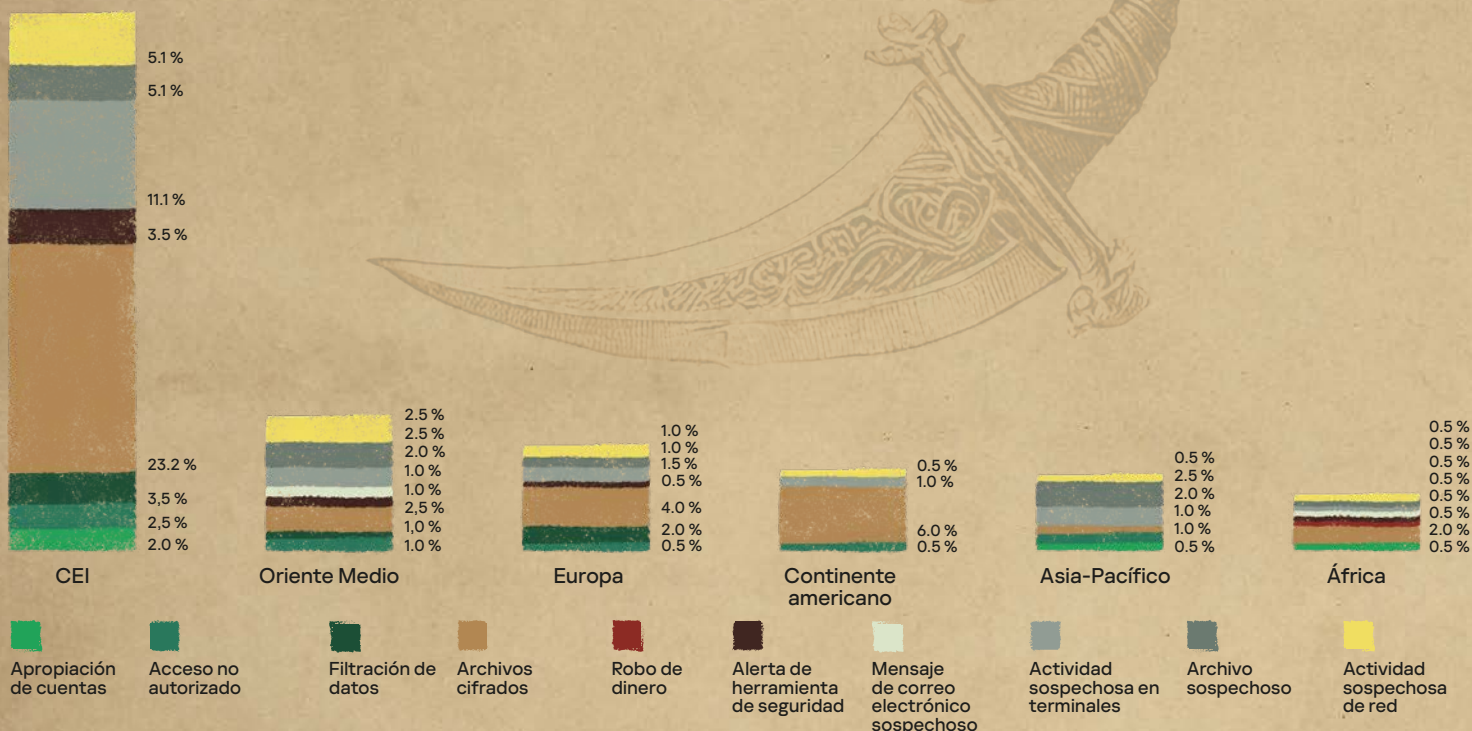
		
Corta (horas y días)	Promedio (semanas)	Duradera (un mes o más)
Principales ataques de ransomware de alta velocidad que representan la mayor amenaza incluso para las operaciones maduras de seguridad. Principalmente, conductas evidentes de agentes maliciosos que aprovechan elementos sencillos: problemas de seguridad fáciles de identificar y de disponibilidad pública	El ransomware cometió numerosos ataques que no pueden distinguirse de los más veloces (ataques de máxima actividad). En muchos casos, en este grupo existe una demora importante entre el acceso inicial y las siguientes etapas del ataque.	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).
Vector inicial		
Cuentas válidas	Exploit de aplicaciones públicas, relación de confianza	Exploit de aplicaciones públicas, relación de confianza, cuentas válidas
Porcentaje de ataques		
44.5 %	20.3 %	35.2 %
Duración promedio (mediana)		
Menos de 1 día	13 días	253 días
Duración de la respuesta ante incidentes (mediana)		
33 horas	40 horas	50 horas
		
Impacto		
Datos cifrados	Datos cifrados y robo de dinero	Datos cifrados y fuga de datos



Motivos para solicitar el servicio

Figura 3

Motivos de las solicitudes de los servicios Kaspersky Incident Response por región



Positivos reales

Archivos cifrados	38.9 %
Actividad sospechosa en terminales	18.2 %
Archivo sospechoso	10.1 %
Actividad sospechosa de red	10.1 %
Filtración de datos	6.6 %
Acceso no autorizado	5.6 %
Alerta de herramienta de seguridad	5.6 %
Mensaje de correo electrónico sospechoso	1.5 %
Robo de dinero	0.5 %

Falsas alarmas

Actividad sospechosa de red	42.9 %
Actividad sospechosa en terminales	35.7 %
Archivo sospechoso	7.1 %

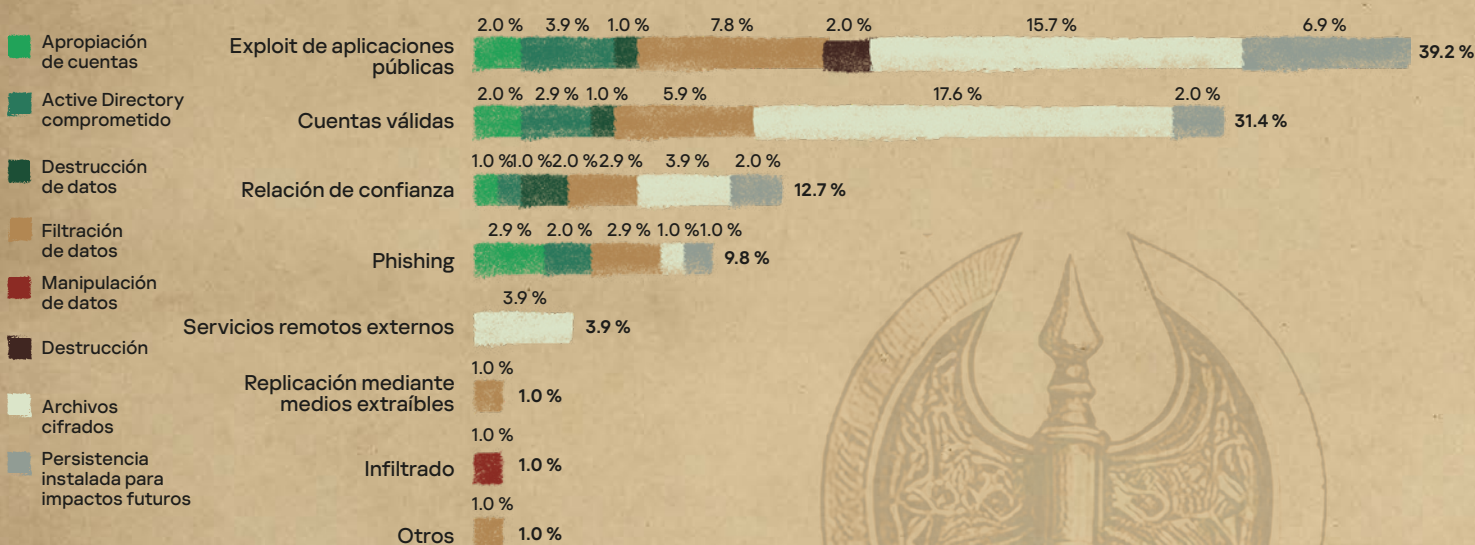
En 2024, el principal motivo de las solicitudes fueron las actividades sospechosas, ya que estas pueden indicar la presencia de atacantes en la red. Sin embargo, las actividades sospechosas también fueron la principal fuente de falsas alarmas. De todos modos, recomendamos investigar toda actividad sospechosa para garantizar la cobertura de todos los ataques reales.

Vector inicial de ataque

Las aplicaciones dirigidas al público son, desde hace años, el principal vector inicial de ataque. En 2024, volvieron a ocupar el primero puesto: representaron el 39,2 % de los incidentes. En comparación con el 2023, las relaciones de confianza vieron un aumento, pero conservaron el tercer puesto con un 12,8 % de los incidentes. Las cuentas válidas conservan su posición como el segundo vector de ataque más común con el 31,4 %. También hemos notado que el phishing sigue siendo un vector inicial y se emplea en casi una de cada 10 situaciones.

Figura 4

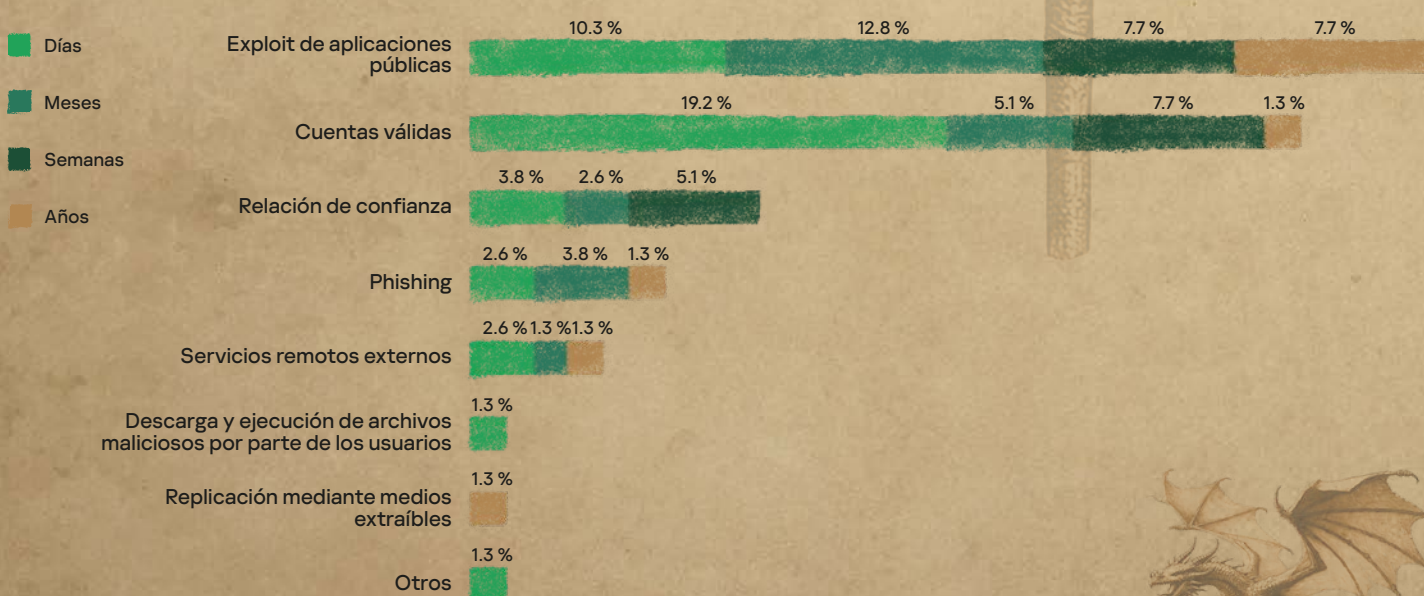
Vector inicial de ataque e impacto resultante



Según estas estadísticas, podemos concluir que, sea cual sea el vector inicial de ataque, el tiempo de detección se ve afectado principalmente por el nivel de seguridad de la información de la organización afectada. Por ejemplo, los ataques que emplean los vectores más populares pueden pasar desapercibidos durante varios días o incluso varios meses.

Figura 5

Acceso inicial y duración del ataque



Herramientas de los atacantes

En casi todas las investigaciones se utilizan herramientas legítimas en diversas etapas de los ataques. Aunque los grupos de atacantes emplean su propio conjunto de herramientas que podrían identificarlos, casi cualquier atacante puede utilizar herramientas de uso extendido (como Mimikatz o PsExec) en la extracción de contraseñas y el movimiento lateral después de aprovechar una vulnerabilidad.

Distribución y frecuencia de las herramientas utilizadas en incidentes

Frecuente: 8-22 %

Promedio: 4-8 %

Inusual: 1-4 %

Mimikatz

PsExec

ProcDump

PowerShell

BloodHound

Process Hacker

SoftPerfect Network Scanner

Impacket

ADRecon

gs-netcat

Nmap

NSSM

WMIC

Ngrok

AnyDesk

Advanced Port Scanner

Chisel

DiskCryptor

gmer.exe

Remcom

Advanced IP Scanner

netscan.exe

LaZagne

Los atacantes suelen utilizar diversas herramientas en el control remoto, la evasión de defensas y la exploración de la infraestructura de la víctima.

Comando y control	18.9 %	AnyDesk	SSH	gs-netcat	Revssocks	Gost	Cloudflared	RDP	PuTTY	Tactical RMM				
Evasión de defensas	18.3 %	Chisel	Process Hacker	Localtonet	gmer	Kavremvr	Tor	FRP	HRSword	PCHunter	IObit Unlocker	Neo-reGeorg	Defender Control	TDSSKiller
Detección	15.2 %	SoftPerfect Network Scanner	NetScan	Advanced Port Scanner	Advanced IP Scanner	ADRecon	FScan	BloodHound	Nmap	LAN Search Pro	Everything	PingCastle	adPEAS	
Ejecución	12.2 %	PsExec	PowerShell	SMBExec	WMIC	NSSM	Wmiexec	MeshAgent	Remcom	WSO WebShell	ATExec	WinSW	PAExec	
Acceso a credenciales	11.6 %	Mimikatz	ProcDump	SecretsDump	LaZagne	CredentialsFileView	Nanodump	WebBrowserPassView	XenAllPasswordPro	Gosecretsdump	grabFF			
Impacto	9.8 %	BitLocker	DiskCryptor	Eraser	WipeDisk	SDelete								
Recopilación	4.9 %	7zip	WinRAR	7z	Adminer	SharpHound	Raw Copy	FileZilla						
Movimiento lateral	3.7 %	Impacket	Cobalt Strike	PowerSploit	Metasploit	NXC	Havoc							
Exfiltración	3.7 %	Ngrok	Rclone	WinSCP	WinGet	Wget	MEGASync							
Escalamiento de privilegios	1.8 %	Invoke-sAMSpoofting	EfsPotato	JuicyPotato										





Ejemplos de herramientas usadas en casos reales

Intrusión de ransomware: detección de archivos y directorios

ID: T1083⁹

Táctica: detección

Tras la intrusión, el grupo de atacantes detrás del ransomware LockBit usó credenciales en riesgo y el protocolo de acceso remoto (RDP) para acceder a un servidor de archivos y a las búsquedas en el Explorador de archivos a fin de identificar archivos con palabras clave y fechas específicas:

```
"Restricted" OR ="Confidential" OR ="Private" OR ="Operational & Inventory" OR ~="Finance" datemodified: 1/1/2022..today
"Balance" datemodified: 1/1/2022..today
"ssn" OR ="Restricted" OR ="Confidential" OR ="Private" OR ~="Operational & Inventory" datemodified: 1/1/2022..today
"tax" OR ="Income Statement" OR ="Balance" OR ="Cash" OR ="Financial Footnotes" OR ="Compensations" OR ="Customer
Information" OR ="Employee Data" OR ~="Intellectual Property" datemodified: 1/1/2022..today
```

Con estos filtros, el grupo de atacantes identificó archivos críticos en el servidor de archivos y creó una carpeta comprimida .zip para filtrar información con el objetivo de presionar a la víctima para que pague el rescate.

Intrusión: detección de cuenta (cuenta de dominio)

ID: T1087.002¹⁰

Táctica: detección

Una vez obtenido el acceso a la infraestructura, el grupo de atacantes utilizó PowerShell para ejecutar una serie de instrucciones que les permitieron realizar las siguientes acciones:

- ◆ Instalar módulos adicionales para administrar Active Directory:

```
Import-Module ActiveDirectory
Install-Module ActiveDirectory
Register-PSRepository -Name "PSGallery" -SourceLocation "https://www.powershellgallery.com/api/v2/" -InstallationPolicy
Trusted
Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Register-PSRepository -Default -InstallationPolicy Trusted
Install-Module -Name ActiveDirectory -Force
```

- ◆ Administrar cuentas de dominio:

```
Import-Module .\Microsoft.ActiveDirectory.Management.dll -Verbose
Unlock-ADAccount -Identity "<edited>"
Get-LAPS
```

- ◆ Confirmar la instalación de módulos específicos:

```
gc "c:\program files\LAPS\CSE\Admpwd.dll"
```

- ◆ Obtener información sobre controladores de dominio y cuentas con privilegios:

```
$laps = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd,ms-Mcs-
AdmPwdExpirationTime -Server <edited> | ? {$.'ms-Mcs-AdmPwd'} | select Name,ms-Mcs-
AdmPwd,@{label="ExpDate";Expression={([datetime]::FromFileTime([convert]::ToInt64($.'ms-
Mcs-AdmPwdExpirationTime'))}}
nltest /domain_controllers
nltest /dclist
nltest /dclist:<domain_edited>
Import-Module AdmPwd.PS
```

⁹ T1083: Detección de archivos y directorios

¹⁰ T1087.002: Detección de cuenta (cuenta de dominio)

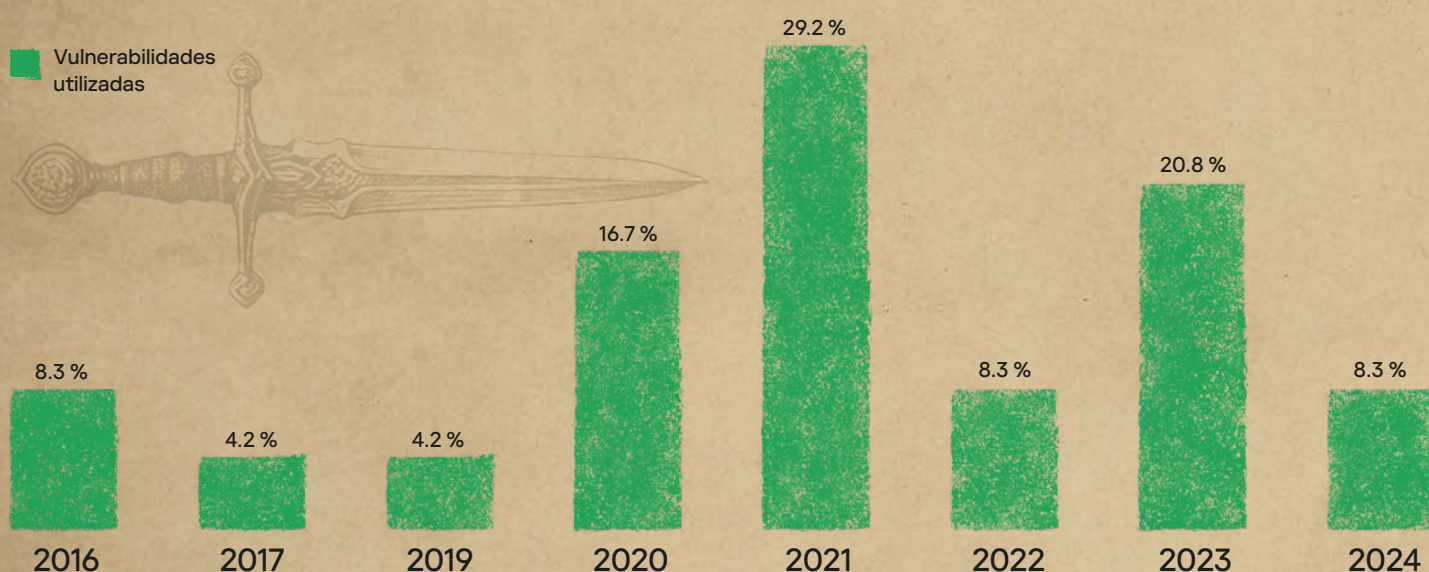


Las vulnerabilidades más habituales

En el siguiente diagrama se observan las vulnerabilidades de años anteriores que se aprovecharon en 2024. Más del 90 % de las vulnerabilidades aprovechadas por atacantes en 2024 fueron publicadas hace más de un año, lo que indica que las organizaciones atacadas tienen políticas de actualización poco efectivas.

Figura 6

Vulnerabilidades de años anteriores aprovechadas en 2024



Las vulnerabilidades más frecuentes encontradas en nuestro conjunto de datos para 2024 estaban relacionadas con productos de Microsoft (Windows, Exchange, Active Directory, SharePoint), such as CVE-2016-0099, CVE-2017-0176, CVE-2019-1458, CVE-2020-1472, CVE-2020-0688, CVE-2020-0787, CVE-2021-42287, CVE-2021-34523, CVE-2021-34473 y CVE-2023-29357. También descubrimos un aumento notorio en la cantidad de vulnerabilidades en el servidor de OpenSSH (sshd): CVE-2023-38408, CVE-2024-6387 (regreSSHion) y CVE-2024-6409. Además, se observaron vulnerabilidades en la interfaz de usuario web del software Cisco IOS XE (CVE-2023-20273 y CVE-2023-20198).

Alrededor del 40 % de las vulnerabilidades detectadas durante estas respuestas a incidentes indicaba la ejecución remota de código (RCE) y un porcentaje similar estaba relacionado con exploits de escalamiento de privilegios. En particular, un gran número de vulnerabilidades graves y críticas en estas categorías tienen exploits de prueba de concepto (PoC) disponibles en plataformas como GitHub y Exploit-DB. Esto facilita a los atacantes el acceso a diferentes entornos y la realización de movimientos laterales.

Entre las categorías repetidas de Common Weakness Enumeration (CWE), encontramos que las más predominantes eran CWE-120 (saturación clásica del búfer), CWE-269 (administración incorrecta de privilegios), CWE-287 (autenticación inadecuada) y CWE-918 (falsificación de solicitudes en el servidor, SSRF). Todas estas vulnerabilidades podrían haberse evitado si se hubieran empleado prácticas de codificación seguras, como el análisis estático de código y el análisis dinámico automático. Esto resalta la importancia de que el equipo de desarrollo debe priorizar la seguridad en todas las etapas del ciclo de vida de desarrollo y adoptar principio seguros y de privacidad por diseño. Además, los clientes deben asegurarse de tener actualizaciones regulares y aplicar parches de seguridad a tiempo.

Lista completa de CVE empleadas

PoC disponible: Microsoft Windows (servicio Secondary Logon)

CVE-2016-0099

CVSS 7.8 HIGH

CWE-120

Escalamiento de privilegios

También conocida como MS16-032, una vulnerabilidad en el servicio Secondary Logon permite a los usuarios locales obtener privilegios mediante una aplicación personalizada.

Microsoft Windows (gpkcsp.dll)

CVE-2017-0176

CVSS 8.1 HIGH

CWE-120

Ejecución remota de código (RCE)

Un desbordamiento del búfer en el código de autenticación de tarjetas inteligentes en gpkcsp.dll en Microsoft Windows XP (hasta SP3) y Server 2003 (hasta SP2) permite que cualquier atacante ejecute software de forma remota si el equipo objetivo forma parte de un dominio de Windows y tiene un protocolo de escritorio remoto habilitado (o Terminal Services).

PoC disponible: Microsoft Windows (Win32k)

CVE-2019-1458

CVSS 7.8 HIGH

CWE-1219

Escalamiento de privilegios

Esta vulnerabilidad surge de un error en la aplicación al procesar un archivo malicioso, que permite a los atacantes remotos aprovecharla para escalar sus privilegios en sistemas vulnerables.

PoC disponible: Microsoft Windows (Netlogon)

CVE-2020-1472

CVSS 10.0 CRÍTICO

CWE-330

Escalamiento de privilegios

Esta vulnerabilidad de escalamiento de privilegios ocurre cuando un grupo de atacantes establece una conexión vulnerable de un canal seguro de Netlogon con un controlador de dominio mediante el protocolo remoto de Netlogon (MS-NRPC). Si se aprovecha la vulnerabilidad, el grupo de atacantes puede ejecutar una aplicación personalizada en un dispositivo en red.

PoC disponible: Microsoft Exchange Server

CVE-2020-0688

CVSS 8.8 HIGH

CWE-287

Ejecución remota de código (RCE)

Esta vulnerabilidad de ejecución remota de código en Microsoft Exchange ocurre debido al manejo inadecuado de objetos en memoria.

PoC disponible: Microsoft Windows (Servicio de transferencia inteligente en segundo plano, BITS)

CVE-2020-0787

CVSS 7.8 HIGH

CWE-59

Escalamiento de privilegios

Es una vulnerabilidad de escalamiento de privilegios en el Servicio de transferencia inteligente en segundo plano (BITS) de Windows.

PoC disponible: Microsoft (Active Directory Domain Services)

CVE-2021-42287

CVSS 8.8 HIGH

CWE-269

Escalamiento de privilegios

Esta vulnerabilidad de escalamiento de privilegios en Active Directory Domain Services permite a un grupo de atacantes hacerse pasar por el administrador del dominio desde un usuario estándar del dominio.

PoC disponible: Microsoft Exchange Server

CVE-2021-26855

CVSS 9.8 CRITICAL

CWE-918

Ejecución remota de código (RCE)

Esta vulnerabilidad en Microsoft Exchange Server permite a un grupo de atacantes eludir la autenticación y hacerse pasar por el administrador.

Microsoft Exchange Server

CVE-2021-31207

CVSS 6.6 MEDIUM

CWE-434

Desviación de medidas de seguridad

Esta vulnerabilidad permite a un grupo de atacantes remoto ejecutar código arbitrario en instalaciones vulnerables de Microsoft Exchange Server. En el peor de los escenarios, se podría ejecutar código arbitrario en SYSTEM.

PoC disponible: Microsoft (Active Directory Domain Services)**CVE-2021-42278****CVSS 7.5 HIGH****CWE-269**

Escalamiento de privilegios

Esta vulnerabilidad de escalamiento de privilegios en Active Directory Domain Services permite a un usuario estándar del dominio hacerse pasar por el administrador del dominio.

PoC disponible: Microsoft Exchange Server**CVE-2021-34523****CVSS 9.8 CRITICAL****CWE-287**

Escalamiento de privilegios

Esta vulnerabilidad de escalamiento de privilegios en Microsoft Exchange Server surge de la validación inadecuada de las solicitudes de comunicación remota de PowerShell.

PoC disponible: Microsoft Exchange Server (Autodiscover)**CVE-2021-34473****CVSS 9.8 CRITICAL****CWE-918**

Ejecución remota de código (RCE)

Esta vulnerabilidad en el servicio Autodiscover permite a los atacantes remotos ejecutar código arbitrario en la instancia afectada de Microsoft Exchange Server.

Bitrix Site Manager**CVE-2022-27228****CVSS 9.8 CRITICAL****CWE-20**

Ejecución remota de código (RCE)

Esta vulnerabilidad está presente en el módulo vote (< 21.0.100) de Bitrix Site Manager. Permite a los atacantes remotos sin autenticación ejecutar código arbitrario.

PoC disponible: Veeam Backup & Replication**CVE-2023-27532****CVSS 7.5 HIGH****CWE-306**

Falta de autenticación

Esta vulnerabilidad en un componente de Veeam Backup & Replication permite a un grupo de atacantes obtener las credenciales cifradas que se almacenan en la base de datos de la configuración.

PoC disponible: OpenSSH (ssh-agent)**CVE-2023-38408****CVSS 9.8 CRITICAL****CWE-428**

Ejecución remota de código (RCE)

En las versiones de OpenSSH anteriores a 9.3p2, la característica PKCS#11 de ssh-agent tiene una ruta de búsqueda vulnerable que la vuelve poco fiable. Esto puede provocar la ejecución remota de código si un sistema bajo el control de atacantes recibe a un agente reenviado.

PoC disponible: Microsoft SharePoint Server**CVE-2023-29357****CVSS 9.8 CRÍTICO****CWE-303**

Escalamiento de privilegios

Esta vulnerabilidad en Microsoft SharePoint Server permite a los atacantes remotos escalar privilegios.

PoC disponible: Cisco IOS XE (interfaz de usuario web)**CVE-2023-20273****CVSS 7.2 HIGH****CWE-78**

Ejecución remota de código (RCE)

La función de interfaz de usuario web del software Cisco IOS XE podría permitir a un atacante remoto con autenticación inyectar comandos con privilegios raíz.

PoC disponible: Cisco IOS XE (interfaz de usuario web)**CVE-2023-20198****CVSS 10.0 CRITICAL****CWE-420**

Escalamiento de privilegios

Esta vulnerabilidad permite a un atacante sin autenticación crear una cuenta con "acceso con privilegios de nivel 15", es decir, acceso total a todos los comandos.

PoC disponible: FortiClientEMS

CVE-2023-48788

CVSS 9.8 CRITICAL

CWE-89

Inyección SQL

La neutralización inadecuada de elementos especiales usados en un comando de SQL (inyección SQL) en Fortinet FortiClientEMS permite a un grupo de atacantes ejecutar comandos o código no autorizado mediante paquetes personalizados.

PoC disponible: OpenSSH (sshd)

CVE-2024-6387

CVSS 8.1 HIGH

CWE-362

Ejecución remota de código (RCE)

Esta vulnerabilidad en el servidor de OpenSSH (ssh), también conocida como "regreSSHion", podría permitir ejecutar código de forma remota en el servidor vulnerable.

OpenSSH (sshd)

CVE-2024-6409

CVSS 7.0 HIGH

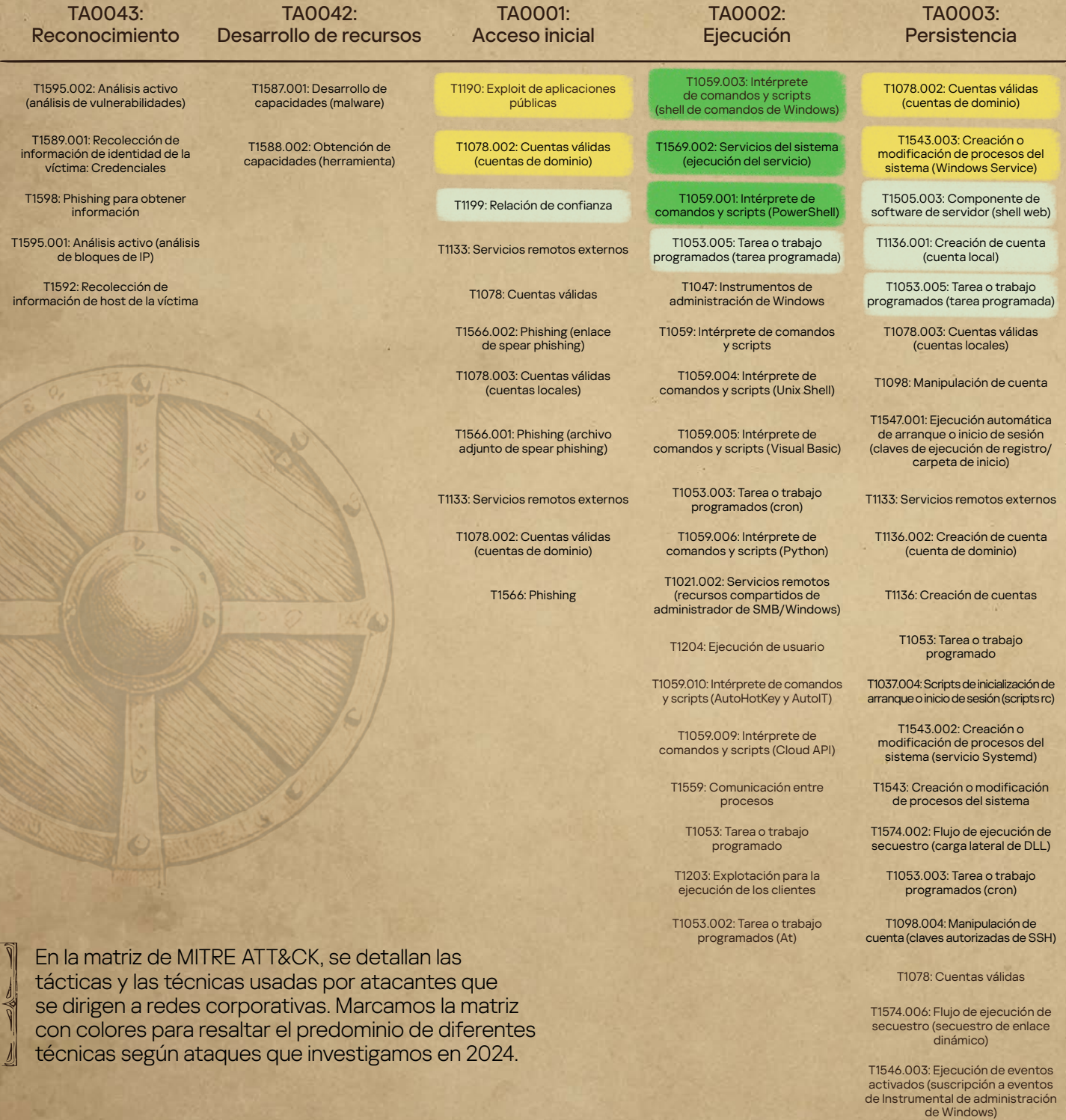
CWE-364

Ejecución remota de código (RCE)

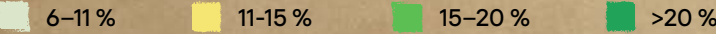
Esta vulnerabilidad de condición de carrera descubierta en el servidor de OpenSSH (sshd) podría permitirle a un usuario sin privilegios ejecutar código de forma remota.



Diagrama de tácticas y técnicas de MITRE ATT&CK



En la matriz de MITRE ATT&CK, se detallan las tácticas y las técnicas usadas por atacantes que se dirigen a redes corporativas. Marcamos la matriz con colores para resaltar el predominio de diferentes técnicas según ataques que investigamos en 2024.



TA0004:
Escalamiento de privilegiosTA0005:
Evasión de defensasTA0006:
Acceso a credencialesTA0007:
Descubrimiento

T1078.002: Cuentas válidas (cuentas de dominio)	T1070.004: Eliminación de indicadores (eliminación de archivos)	T1003: Volcado de credenciales de SO	T1046: Detección de servicio en red
T1068: Explotación de escalación de privilegios	T1562.001: Alteración de las defensas (desactivación o modificación de herramientas)	T1003.001: Volcado de credenciales de SO (memoria de LSASS)	T1018: Detección de sistemas remotos
T1484.001: Modificación de directivas de dominios (modificación de directivas de grupos)	T1070.001: Eliminación de indicadores (eliminación de registros de eventos de Windows)	T1552.001: Credenciales no protegidas (credenciales en archivos)	T1135: Detección de recursos compartidos en red
T1078.002: Cuentas válidas (cuentas de dominio)	T1140: Decodificar/desofuscar archivos o información	T1555: Credenciales procedentes de almacenes de contraseñas	T1082: Detección de información del sistema
T1547.005: Ejecución automática de arranque o inicio de sesión (proveedor de soporte de seguridad)	T1036.005: Enmascaramiento (coincidencia con nombre o ubicación verdadera)	T1110.001: Fuerza bruta (adivinación de contraseñas)	T1087.002: Detección de cuenta (cuenta de dominio)
T1098: Manipulación de cuenta	T1036.004: Enmascaramiento (replicación de tarea o servicio)	T1110: Fuerza bruta	T1482: Detección de confianza de dominio
T1543.003: Creación o modificación de procesos del sistema (Windows Service)	T1027.002: Archivos o información ofuscados (creación de paquetes de software)	T1003.006: Volcado de credenciales de SO (DCSync)	T1069.002: Detección de grupos y permisos (grupos de dominio)
T1548.002: Abuso del mecanismo de control de elevación (circunvención de control de cuentas de usuarios)	T1078.002: Cuentas válidas (cuentas de dominio)	T1003.003: Volcado de credenciales de SO (NTDS)	T1057: Detección de procesos
T1548.001: Abuso del mecanismo de control de elevación (setuid y setgid)	T1112: Modificación de registro	T1003.001: Volcado de credenciales de SO (memoria de LSASS)	T1033: Detección de usuarios/proprietarios del sistema
	T1027.009: Archivos o información ofuscados (cargas útiles integradas)	T1555.005: Credenciales procedentes de almacenes de contraseñas (gestores de contraseñas)	T1049: Descubrimiento de conexiones en la red del sistema
	T1218.011: Ejecución por proxy de binario de sistema (rundll32)	T1110.003: Fuerza bruta (pulverización de contraseñas)	T1016: Detección de configuración de red en el sistema
	T1070.009: Eliminación de indicadores (eliminación de la persistencia)	T1555.004: Credenciales procedentes de almacenes de contraseñas (Administrador de contraseñas de Windows)	T1615: Descubrimiento de políticas de grupos
	T1078.003: Cuentas válidas (cuentas locales)	T1212: Exploit de acceso mediante credenciales	T1083: Detección de archivos y directorios
	T1055: Incursiones en procesos	T1557: Adversary-in-the-Middle	T1087.001: Detección de cuenta (cuenta local)
	T1070.006: Eliminación de indicadores (timestamp)	T1528: Robo del token para acceso a aplicaciones	T1087: Detección de cuentas
	T1027.010: Archivos o información ofuscados (ofuscación de comandos)	T1552: Credenciales no protegidas	T1560.001: Archivado de datos recopilados (archivado mediante utilidad)
	T1027.001: Archivos o información ofuscados (relleno binario)	T1056.001: Captura de entrada (registradores de pulsaciones de teclas)	T1124: Detección de la hora del sistema
	T1027.013: Archivos o información ofuscados (archivo cifrado o codificado)	T1552.004: Credenciales no protegidas (claves privadas)	T1201: Descubrimiento de políticas de contraseñas
	T1562.001: Alteración de las defensas (desactivación o modificación de herramientas)	T1555.003: Credenciales procedentes de almacenes de contraseñas (credenciales de navegadores web)	T1012: Consulta en registro
	T1574.001: Flujo de ejecución de secuestro (secuestro de orden de búsquedas de DLL)	T1552.002: Credenciales no protegidas (credenciales en el registro)	T1614.001: Detección de ubicación del sistema (detección del idioma del sistema)
	T1562: Alteración de las defensas	T1040: Rastreo de red	
	T1574.002: Flujo de ejecución de secuestro (carga lateral de DLL)		
	T1070.003: Eliminación de indicadores (eliminación del historial de comandos)		
	T1622: Evasión del depurador		
	T1562.002: Alteración de las defensas (desactivación del registro de eventos de Windows)		
	T1070: Eliminación de indicadores		
	T1027.003: Archivos o información ofuscados (esteganografía)		
	T1564.006: Ocultación de artefactos (ejecución de instancia virtual)		
	T1484.001: Modificación de directivas de dominios (modificación de directivas de grupos)		
	T1218.005: Ejecución por proxy de objeto binario del sistema (mshta)		

6–11 % 11–15 % 15–20 % >20 %



TA0008: Movimiento lateral	TA0009: Recopilación	TA0011: Comando y control	TA0010: Exfiltración	TA0040: Impacto
T1021.001: Servicios remotos (protocolo de escritorio remoto)	T1560.001: Archivado de datos recopilados (archivado mediante utilidad)	T1572: Tunelización de protocolo	T1567: Exfiltración por servicio web	T1486: Datos cifrados para mayor impacto
T1021.002: Servicios remotos (recursos compartidos de administrador de SMB/Windows)	T1005: Datos del sistema local	T1105: Transferencia de herramientas de infiltración	T1537: Transferencia de datos a cuenta en la nube	T1485: Destrucción de datos
T1021.004: Servicios remotos (SSH)	T1039: Datos de unidad compartida de red	T1071.001: Protocolo de capa de aplicación (protocolos web)	T1020: Exfiltración automatizada	T1561: Borrado de disco
T1021: Servicios remotos	T1119: Recolección automatizada	T1219: Software de acceso remoto	T1567.002: Filtración sobre servicio web (filtración al almacenamiento en la nube)	T1561.002: Borrado de disco (borrado de la estructura de disco)
T1570: Transferencia lateral de herramientas	T1114.001: Recopilación de correos electrónicos (recopilación local de correos electrónicos)	T1090.001: Proxy (proxy interno)	T1048: Exfiltración sobre protocolo alternativo	T1565: Manipulación de datos
T1021.006: Servicios remotos (administración remota de Windows)	T1560: Archivado de datos recopilados	T1132.001: Codificación de datos (codificación estándar)	T1041: Exfiltración por canal C2	
T1550.002: Uso de material de autenticación alternativo (Pass the Hash)	T1113: Captura de pantalla	T1090: Proxy		
T1021.003: Servicios remotos (Modelo de objetos componentes distribuido)	T1572: Tunelización de protocolo	T1665: Ocultación de infraestructura		
T1021: Servicios remotos		T1071.004: Protocolo de capa de aplicación (DNS)		
T1021.001: Servicios remotos (protocolo de escritorio remoto)		T1568.002: Resolución dinámica (algoritmos de generación de dominios)		
T1021.002: Servicios remotos (recursos compartidos de administrador de SMB/Windows)		T1102: Servicio web		
T1210: Explotación de servicios remotos		T1568: Resolución dinámica		
T1563.002: Secuestro de sesión de servicio remoto (secuestro de RDP)		T1573.001: Canal cifrado (criptografía simétrica)		
		T1041: Exfiltración por canal C2		
		T1071: Protocolo de capa de aplicación		

6–11 %

11-15 %

15–20 %

>20 %

Sobre Kaspersky

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

Servicios de Seguridad de Kaspersky



**Kaspersky
Managed Detection
and Response**



**Kaspersky
Incident Response**



**Kaspersky
SOC Consulting**



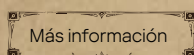
**Kaspersky
Digital Footprint
Intelligence**



**Kaspersky
Security
Assessment**



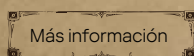
**Kaspersky
Compromise
Assessment**



Más información

Reconocimiento global

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



Más información

Más de 5000

profesionales trabajan
en Kaspersky

50 %

de nuestro equipo está
especializado en I+D

5

centros de experiencia
únicos

467.000

nuevos archivos maliciosos
detectados por Kaspersky
cada día

200.000

clientes corporativos
en todo el mundo

4900 millones

de ciberataques detectados
por Kaspersky en 2024



¿Bajo ataque?
¡Te guardamos
las espaldas!
Ponte en
contacto con
nosotros



kaspersky

Incident
Response

www.kaspersky.es

© 2025 AO Kaspersky Lab. Las marcas comerciales
y marcas de servicios registradas pertenecen a sus
respectivos propietarios.

#kaspersky
#bringonthefuture