kaspersky bring on the future

Robo de datos: Análisis del mercado de credenciales en riesgo en la red oscura

Lo que las empresas deben saber sobre esta amenaza y cómo mitigarla

Kaspersky Digital Footprint Intelligence

Kaspersky
Digital Footprint
Intelligence

Introducción

El equipo de Kaspersky Digital Footprint Intelligence elaboró un informe que se basa en datos sobre millones de dispositivos en riesgo por malware específico diseñado para robar información, también llamado "infostealer".

Infostealer es un tipo de malware diseñado para recopilar y robar información confidencial: cuentas y credenciales, cookies, datos de tarjetas bancarias, monederos de criptomonedas, entre otros datos. Los datos robados de millones de dispositivos de todo el mundo se envían al servidor de C&C (Comando y Control) del operador del malware y se reúnen en registros (un archivo de registro suele contener información de un único sistema infectado), para luego distribuirse entre la comunidad de ciberdelincuentes a través de los mercados de la red oscura.

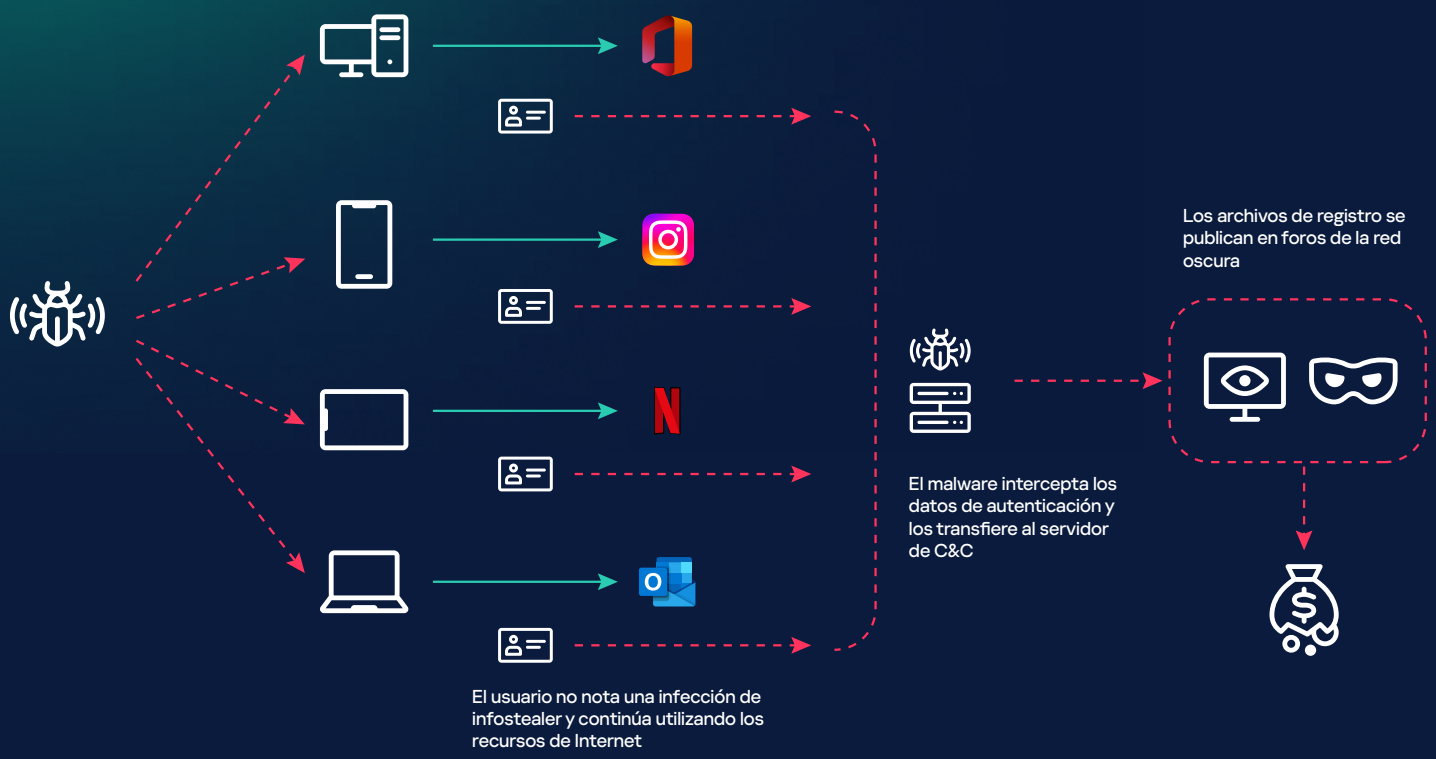
En este informe, se presentan estadísticas y conclusiones clave del procesamiento y análisis de los registros de infostealers recopilados entre 2021-2023.

Fuentes de la información analizada

Los ciberdelincuentes utilizan hilos privados en foros clandestinos para publicar los registros recopilados por infostealers. Estos archivos contienen cuentas de usuarios y otros datos, así como información sobre el propio dispositivo en riesgo.

Los ciberdelincuentes suelen vender los registros a otros ciberdelincuentes, pero pueden compartir los datos de forma gratuita. Por ejemplo, pueden compartir lo que quede después de haber extraído toda la información que necesitan para aumentar su reputación ante la comunidad.

Escenario de infección mediante infostealers



Un archivo de registro contiene un promedio de

50.9 cuentas.

La cantidad de infecciones detectadas en 2023 representa un aumento del

35 %

en 2022 según los datos estimados. La fecha de la infección se determina a partir de los metadatos del dispositivo en riesgo que figuran en los registros del infostealer.

Analizamos los registros para aislar las cuentas en riesgo. Si se descubre una cuenta de usuario en los registros de malware (troyano, spyware, etc.), esto es una señal de que el dispositivo del usuario estaba infectado.

Es importante tener en cuenta que un registro corresponde a una infección de una máquina específica, pero puede contener un gran número de cuentas de varios sitios web o aplicaciones que se utilizaron en el dispositivo.

Tendencias de infección observadas

Tenga en cuenta que los registros no aparecen en la red oscura inmediatamente después de que un dispositivo se vea en riesgo. La cuenta puede haber sido pirateada en 2022, pero el archivo de registro correspondiente podría publicarse recién en 2023. Por lo tanto, es razonable esperar que las cifras reales de infección de 2023 experimenten un incremento si tenemos en cuenta las predicciones sobre la cantidad de registros que se publicarán en 2024.

La dinámica observable de los registros sugiere que en los primeros meses del año, la cantidad de registros del año anterior es mayor que en los últimos meses del año.

Estadísticas de infecciones anuales

[1] Los ciberdelincuentes pueden publicar archivos de registro sobre cuentas en riesgo en la red oscura meses o incluso años después de la infección. Hacemos un seguimiento tanto de las fechas de publicación como de las fechas reales en las que el dispositivo estuvo en riesgo. En 2024, esperamos ver más datos de dispositivos en riesgo de 2023 o antes, pero filtrados en la red oscura algún tiempo después. Antes de 2022, la diferencia entre las infecciones observadas y las esperadas era menor, ya que la mayoría de las credenciales de inicio de sesión en riesgo se habían filtrado.

Para elaborar la previsión, comparamos la cantidad de cuentas en riesgo de 2020 a 2023 por mes. Utilizamos estos datos para identificar una tendencia al tiempo que aumentábamos nuestros conjuntos de datos de años anteriores con datos recién obtenidos, lo que ahora nos permite predecir las cifras previstas ajustadas a la cantidad estimada de datos que se agregarán en el futuro[1].

Estadísticas de infección por sistema operativo

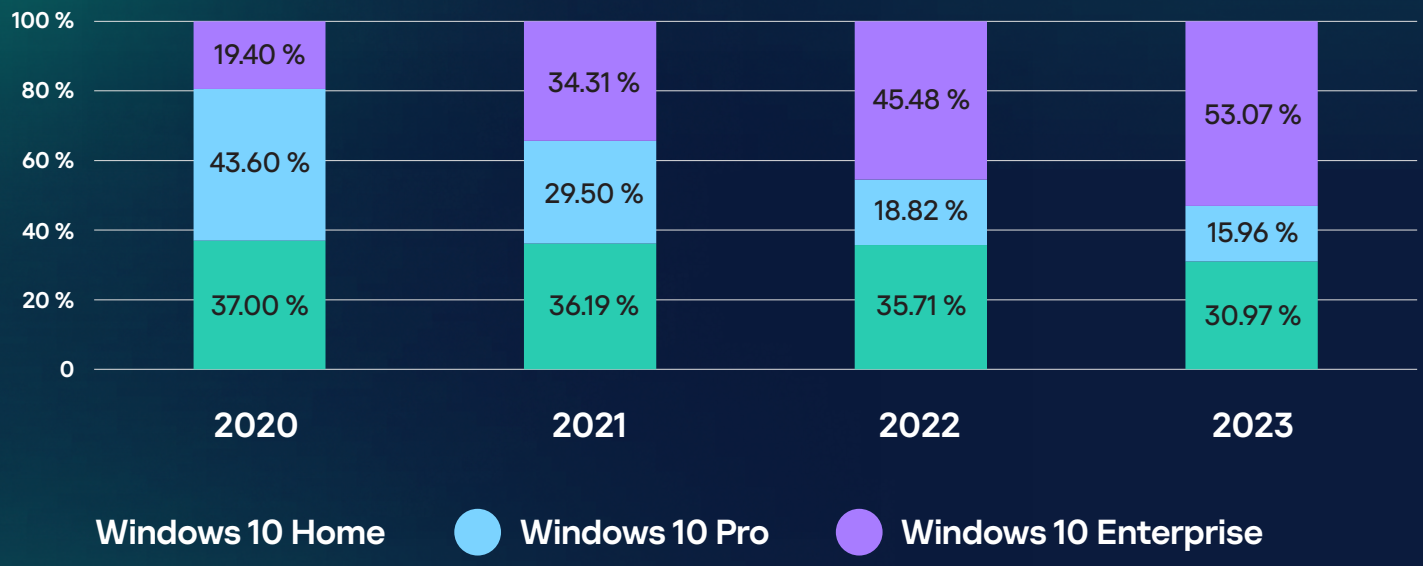
Según los metadatos encontrados en los registros de infostealers, la mayor parte de los dispositivos en riesgo cuentan con tecnología Windows. Esto puede atribuirse a la popularidad general de este sistema operativo, no a cuestiones de seguridad: Windows es uno de los sistemas operativos más utilizados tanto en el ámbito doméstico como en el corporativo.

Analizamos las estadísticas de infección para varias versiones de Windows: Home, Pro y Enterprise. Estos datos permiten detectar tendencias y dividirlas entre usuarios corporativos y domésticos.

Estadísticas de infección en Windows 10

En el siguiente diagrama, se muestran los porcentajes de infecciones para varias versiones de Windows 10 divididas por año, desde 2020 hasta 2023.

Distribución de infecciones en versiones de Windows 10 afectadas, 2020–2023

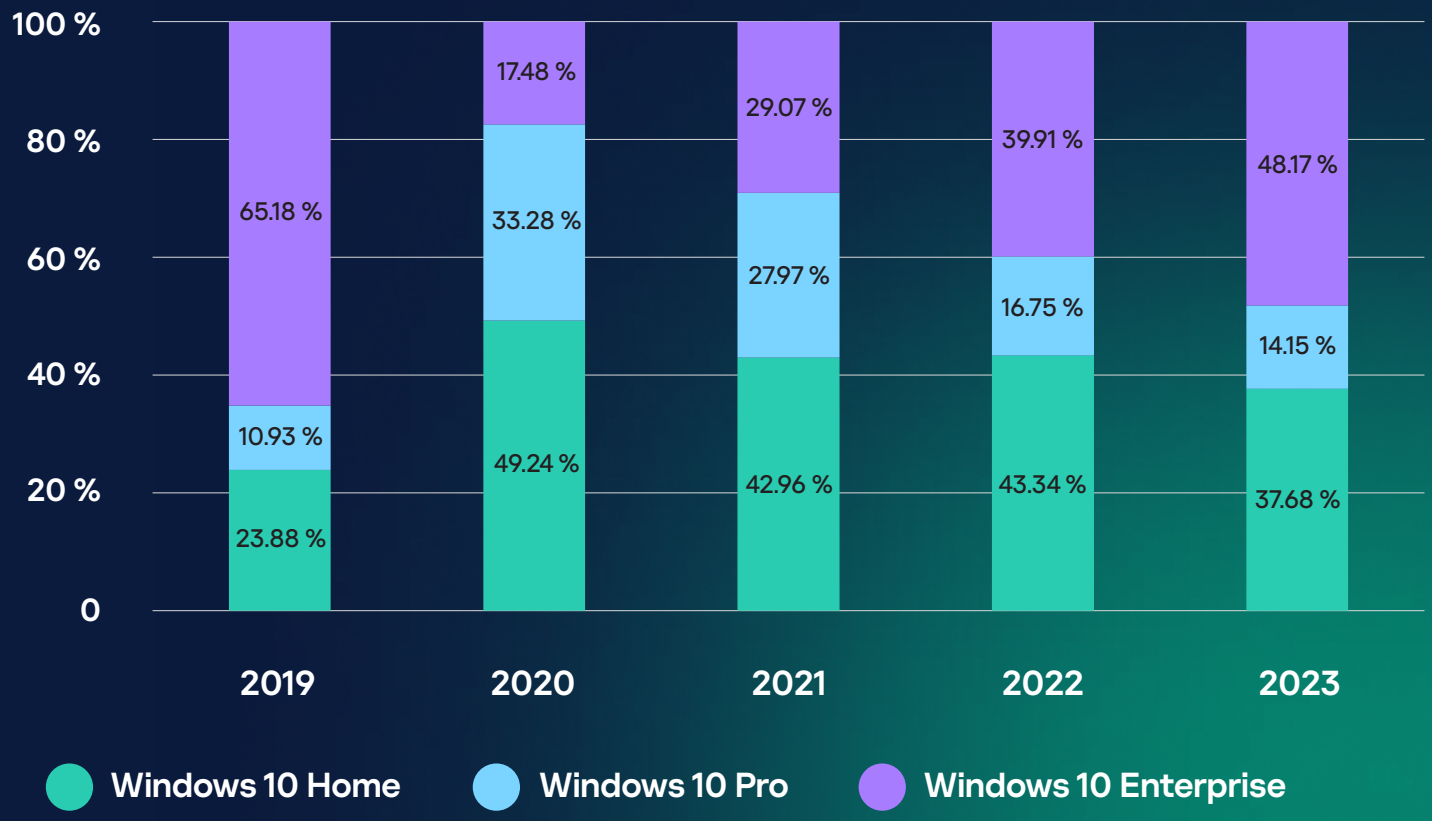


En el diagrama, puede verse que el número relativo de usuarios corporativos en riesgo aumentó año tras año.

Estadísticas de disponibilidad de acceso corporativo por versión de Windows 10

Otra tendencia es la asociada al peligro en las cuentas en varias versiones de Windows 10 que tienen acceso a recursos corporativos.

Cuentas Windows 10 corporativas en riesgo



Un atacante malicioso puede recopilar información sobre las credenciales de un empleado con un correo electrónico corporativo que se usa como nombre de usuario en una media de 1.85 aplicaciones web a partir de un archivo de registro.

El diagrama muestra que la cantidad de cuentas encontradas en los registros de infostealers asociadas a la versión Home empezó a reducirse a partir de 2020, año en el que también alcanzó su máximo.

Le atribuimos esta tendencia a la pandemia de COVID-19, que comenzó en marzo de 2020 y provocó una migración masiva al trabajo a distancia, en la que los empleados suelen utilizar sus dispositivos personales.

Estos suelen carecer de los sólidos controles de seguridad utilizados en entornos corporativos, como soluciones de protección y políticas corporativas y de contraseñas. Este factor aumenta la probabilidad de que el dispositivo se infecte, ya que carece de la capa de seguridad adicional que impide la descarga y ejecución de malware. Por lo tanto, poner en riesgo el dispositivo personal del empleado que se utilizó para iniciar sesión en los recursos de trabajo puede provocar la filtración de cuentas corporativas e información de acceso.

En los registros,

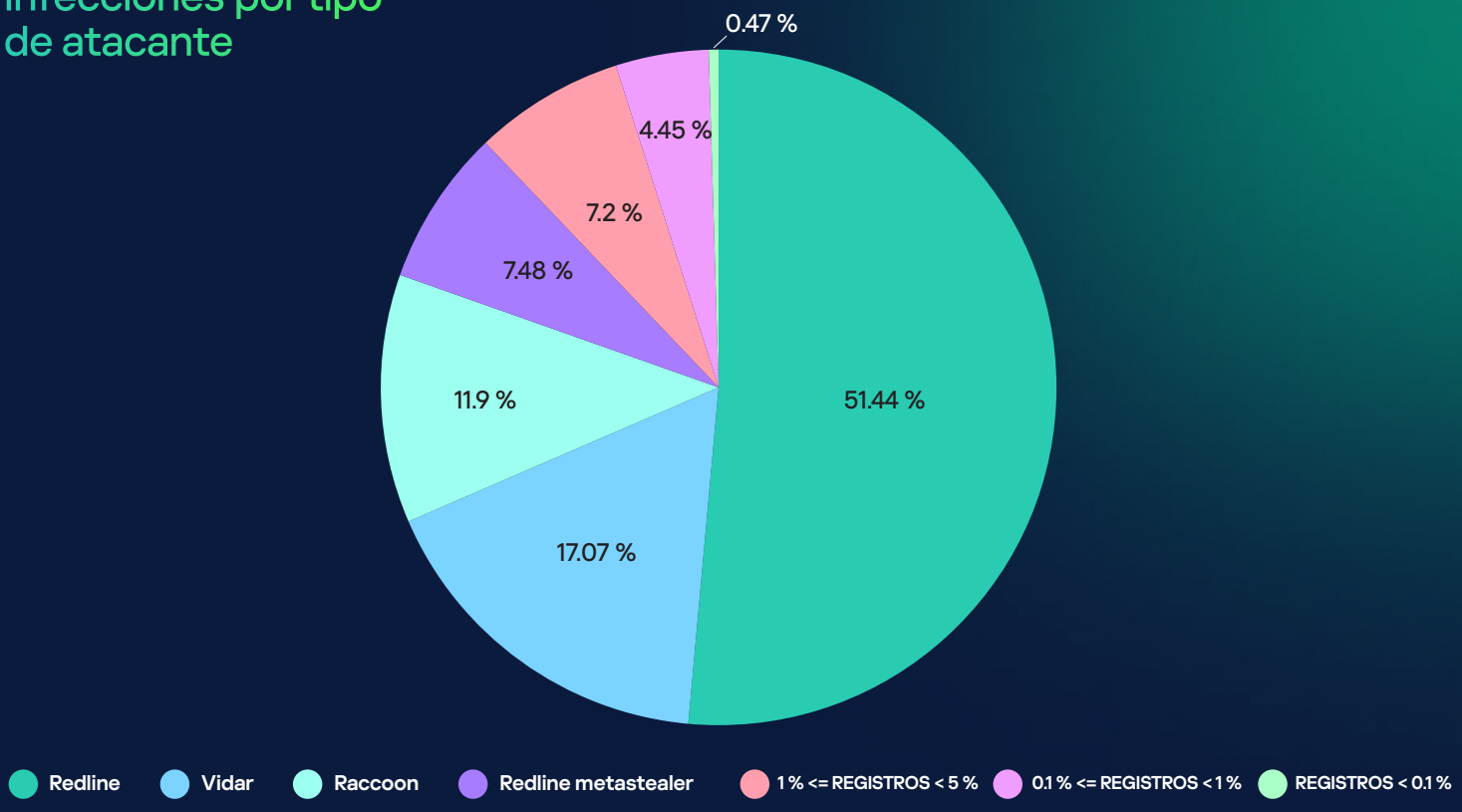
se encontraron alrededor de 100 tipos diferentes de infostealers[1].

[1] Datos disponibles dentro de nuestro campo de visión

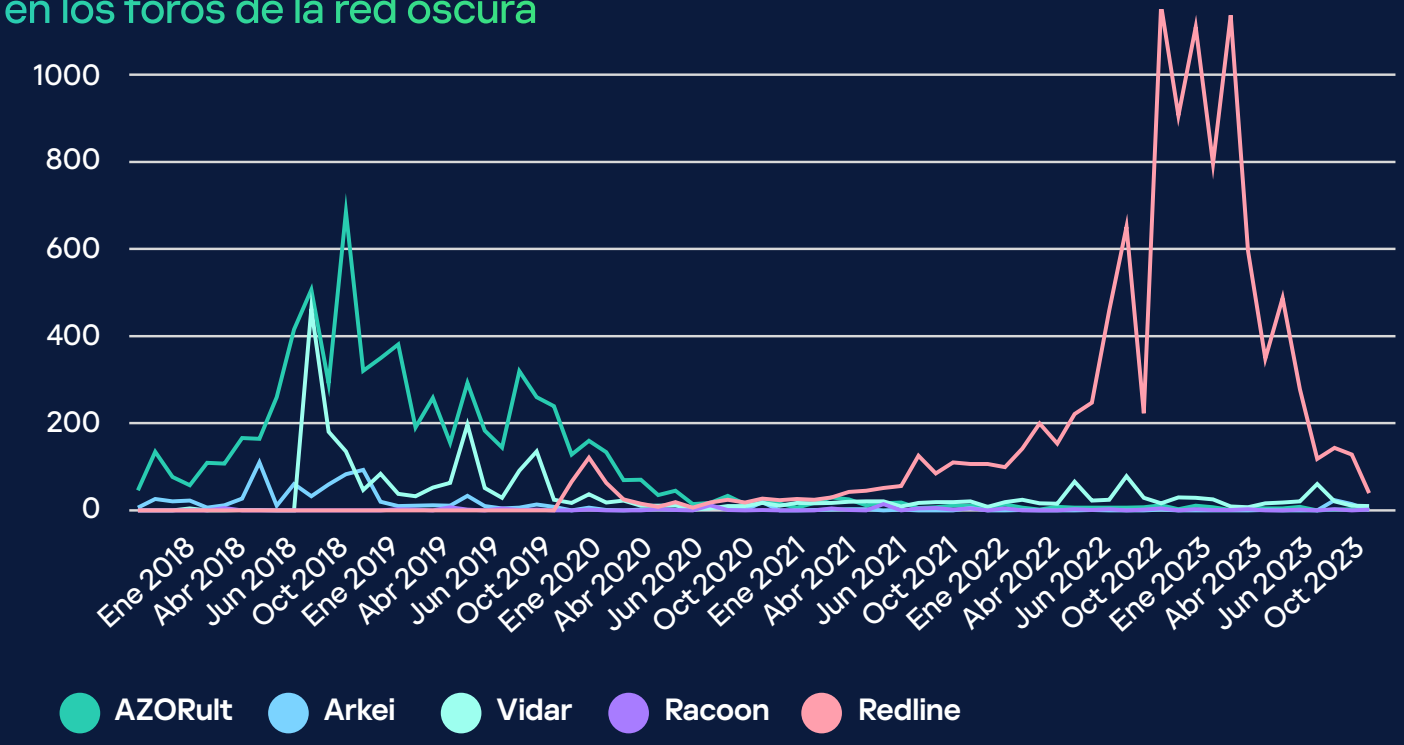
Estadísticas de infección por tipo de atacante

En el siguiente diagrama, se reflejan los porcentajes de los tipos que detectamos en 2020-2023.

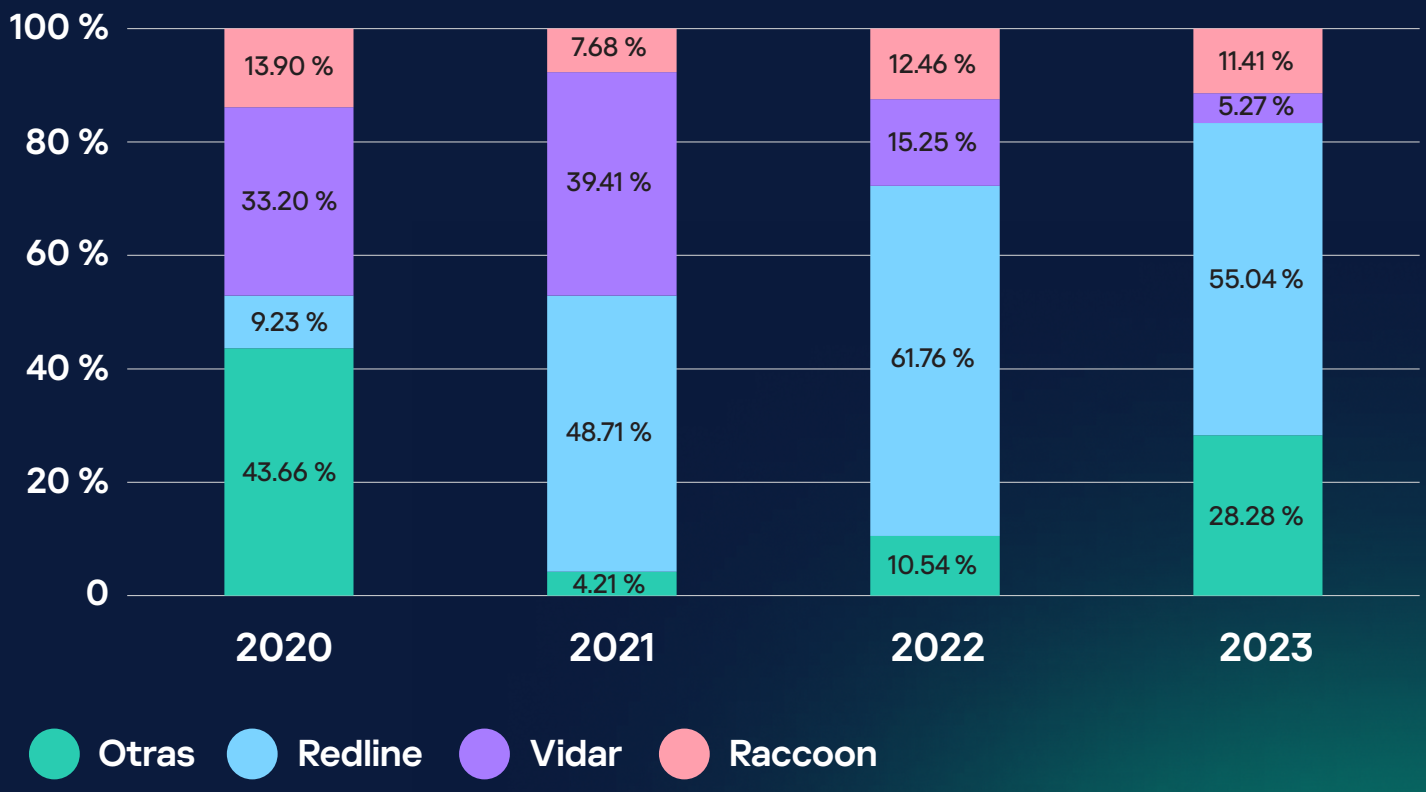
Infecciones por tipo de atacante



Menciones de los diferentes atacantes en los foros de la red oscura



Durante el período, los cambios en la popularidad de los tres atacantes más difundidos fueron los siguientes:



La proporción de infecciones atribuidas a nuevos ataques aumentó del

4.21 % al

28.28 %

en 2021-2023.

Esta tendencia demuestra la actividad del mercado de desarrollo de los infostealers.

El nuevo lumma representó el

6.38 %

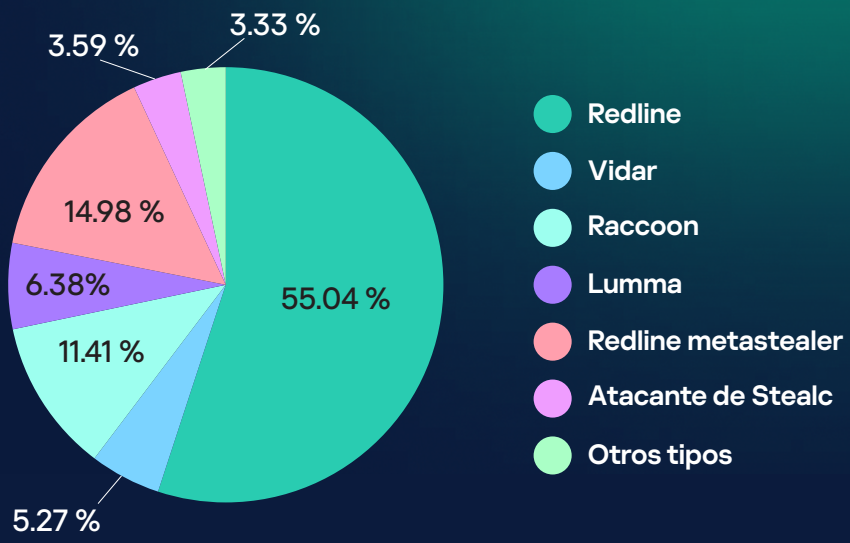
del total de infecciones en 2023.

Redline ganó popularidad en 2021 y, desde entonces, representa la mitad de todas las infecciones. Vidar alcanzó su punto álgido en 2020-2021, pero descendió significativamente en los años siguientes.

Desarrollado en C, lumma surgió en 2022 y empezó a ganar popularidad en 2023 gracias a un modelo de distribución MaaS (malware como servicio). Se trata de un infostealer tradicional, pero con un enfoque agregado sobre monederos de criptomonedas. Se propagó a través de campañas de spam por correo electrónico, YouTube y Discord.

Entre los nuevos atacantes, también se destaca Stealc que representó el 3.59 % de las infecciones en 2023.

Infecciones por tipo de atacante, 2023



Estadísticas de credenciales en riesgo por dominio de nivel superior

Analizamos el número de cuentas en riesgo con sitios web alojados en diversos dominios regionales. La muestra de datos representa dominios de nivel superior genéricos y de caracteres latinos.

A continuación, encontrará una lista de los 30 dominios con el mayor número de cuentas en riesgo en 2023. Estos dominios experimentaron un aumento promedio del 230 % en la cantidad de cuentas en riesgo en comparación con 2021.

Es importante destacar que algunos dominios no se usan únicamente para alojar sitios web locales, sino también para servicios internacionales populares.

Por ejemplo, la plataforma de streaming Twitch funciona con el dominio .tv, aunque es internacional y no está asociada a ningún país en particular. Este hecho puede afectar en gran medida a la frecuencia de los ataques para el dominio .tv, pero, en realidad, no está necesariamente relacionado con el nivel de amenaza de los piratas informáticos en un país determinado. Otros ejemplos son sitios web como linked.in, telegra.ph, etc. En realidad, cualquier dominio puede alojar sitios web internacionales populares, lo que los convierte en objetivos de interés para los ciberdelincuentes. Es esencial reconocer que aunque la existencia de dichos sitios web dentro de la zona del dominio puede tener un impacto en la frecuencia de cuentas en riesgo, no necesariamente se relaciona directamente con el nivel de amenaza de los piratas informáticos en un país vinculado a este dominio.

	Extensión del dominio de nivel superior	Cantidad de credenciales en riesgo por dominio, 2023[1]
1	.com	000 900 325
2	.br	000 800 28
3	.in	000 200 8
4	.co	000 000 6
5	.vn	000 500 5
6	.io	000 800 4
7	.tv	000 700 4
8	.mx	000 600 4
9	.fr	000 500 4
10	.es	000 400 4
11	.id	000 400 4
12	.it	000 200 4
13	.ar	000 200 4
14	.tr	000 800 3
15	.pe	000 400 3
16	.cl	000 900 2
17	.pl	000 700 2
18	.eg	000 700 2
19	.de	000 700 2
20	.sa	000 600 2
21	.ru	000 500 2
22	.uk	000 500 2
23 %	.pk	000 400 2
24	.nz	000 300 2
25	.th	000 200 2
26	.me	000 100 2
27	.us	000 100 2
28	.hu	000 000 2
29	.bd	000 600 1
30	.eu	000 600 1

[1] En la tabla se muestran números redondeados

Análisis de sistemas corporativos

Utilizamos los datos recogidos para recopilar estadísticas sobre reinfecciones de usuarios corporativos.

Seleccionamos 50 entidades bancarias de varias regiones para analizar las cuentas de empleados en riesgo1. Nuestro análisis se centró en las organizaciones de mayor tamaño (con 1000 o más empleados en plantilla), excluidas aquellas en las que solo se produjeron casos aislados de infección.

Definimos tres categorías de reinfección:

1

Corto plazo: menos de tres días entre reinfecciones[2]

2

Largo plazo: más de tres días entre reinfecciones

3

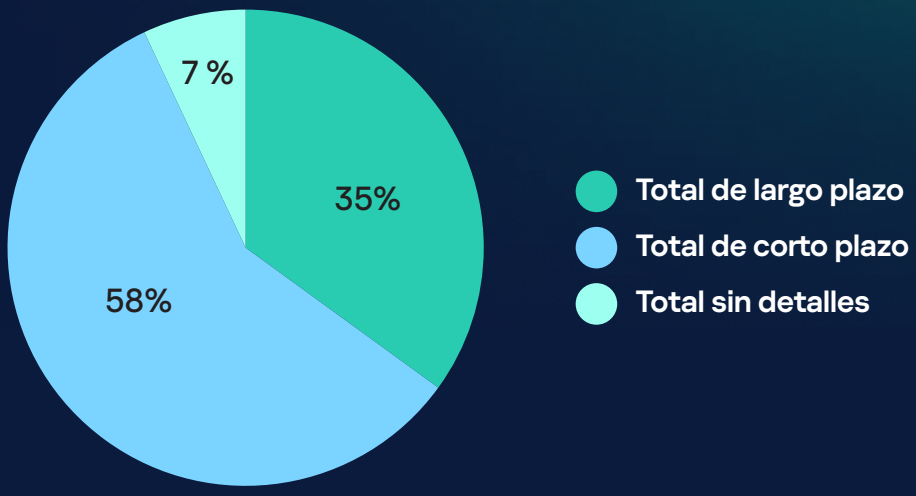
Otros: el intervalo entre infecciones no puede determinarse a partir de los metadatos disponibles

1 El estudio utilizó direcciones de correo electrónico de archivos de registro encontrados en la red oscura y que se creía que estaban asociados a una empresa específica en una muestra. Los datos en riesgo no se verificaron para impedir el acceso no autorizado a la infraestructura de cualquier empresa.

[2] El análisis comparativo se basó en el período promedio en el que podía detectarse un incidente crítico, teniendo en cuenta fines de semana, vacaciones y posibles ausencias de empleados

Según nuestros datos, presentados en el diagrama siguiente, la mayoría de las reinfecciones correspondieron a la categoría de corto plazo, y el 35 % a la categoría de largo plazo.

Reinfecciones



Además, podemos sacar las siguientes conclusiones:

21.07 %

de todos los empleados examinados cuyos dispositivos fueron infectados volvieron a ejecutar malware.

8.94 %

de los empleados con dispositivos infectados volvieron a ejecutar malware tres o más días después de la primera infección.

Conclusión y consejos

En los últimos tres años, observamos un aumento constante de las infecciones por infostealer que aparecen en nuestro campo visual. Windows 10 Enterprise es responsable de un número cada vez mayor de dispositivos en riesgo, lo que sugiere un aumento en la cantidad de dispositivos corporativos infectados.

Los atacantes maliciosos están desarrollando activamente nuevas estrategias y utilizándolas en sus ataques. La proporción de dispositivos en riesgo con malware que no estaba presente entre los tres tipos más populares aumentó más del 20 % en 2021-2023.

Observamos tendencias de reinfección. Las reinfecciones a largo plazo pueden ser un síntoma de varios problemas:

Insuficiente concientización de los empleados

Medidas ineficaces de detección y respuesta a incidentes

Confianza en que basta con cambiar la contraseña si la cuenta estuvo en riesgo

Rechazo a investigar el incidente

Las cuentas de servicio en riesgo son una amenaza directa para la seguridad de usuarios y otros datos, pero el mero hecho de que el dispositivo haya sido infectado sugiere que los datos allí almacenados pueden haberse filtrado. Además, en algunos casos, los actores maliciosos pueden conservar el acceso a la máquina infectada durante mucho tiempo.

Por lo tanto, a continuación se indican las medidas que deben tomarse si se detectó una filtración de datos a través de registros:

- Cambiar inmediatamente las contraseñas de las cuentas presuntamente en riesgo y buscar eventos sospechosos asociados a esas cuentas.
- Notificar a los usuarios cuyos dispositivos puedan estar infectados de la necesidad de realizar análisis antivirus completos de todos sus dispositivos y eliminar cualquier malware que encuentren.
- Empezar a vigilar de forma proactiva los mercados de la red oscura para detectar cuentas en riesgo antes de que afecten la ciberseguridad de clientes o empleados. Aquí encontrará una guía detallada para configurar la supervisión.
- Utilizar Kaspersky Digital Footprint Intelligence para mantenerse al tanto de lo que los atacantes maliciosos saben sobre los recursos de la empresa, detectar con prontitud posibles vectores de ataque y configurar la protección o tomar medidas para eliminar las amenazas cibernéticas de manera oportuna.

Para garantizar una protección eficaz y reducir los riesgos asociados con la infección por infostealers, recomendamos hacer lo siguiente:

- Diseñar un programa de concientización sobre la seguridad de la información para empleados y proporcionar capacitaciones periódicas y evaluaciones de rendimiento.
- Implementar una directiva estricta de contraseñas para todos los recursos corporativos.

https://latam.kaspersky.com