Acronis

Informe semestral sobre ciberamenazas 2023

Informe semestral de Acronis sobre ciberamenazas 2023

De la innovación al riesgo: gestión de las repercusiones de los ciberataques basados en IA

Acronis

Informe semestral sobre ciberamenazas 2023

Acerca del informe

Las principales conclusiones de nuestro último informe sobre ciberamenazas representan una visión global basada en más de 1 millón de endpoints diferentes distribuidos por todo el mundo. La mayoría de las estadísticas que se describen se centran en las amenazas para sistemas operativos Windows, ya que su prevalencia es mucho mayor en comparación con las dirigidas contra macOS y Linux.

5 principales tendencias de ciberseguridad en la primera mitad de 2023

Acronis

Informe semestral sobre ciberamenazas 2023

- Los ataques por correo electrónico se disparan un 464 %
- Ataques contra la cadena de suministro: más de 60 000 clientes afectados
- Auge de ChatGPT: uso de la IA para lanzar ciberataques y crear contenido malicioso
- Los ladrones de datos son la segunda amenaza más extendida
- El ransomware sigue siendo la amenaza número uno para grandes y medianas empresas y aumentó considerablemente en marzo

EE. UU. fue el objetivo de casi la mitad de los 459 ataques que tuvieron éxito en marzo, con 221 víctimas (48 %)

Acronis

Informe semestral sobre ciberamenazas 2023

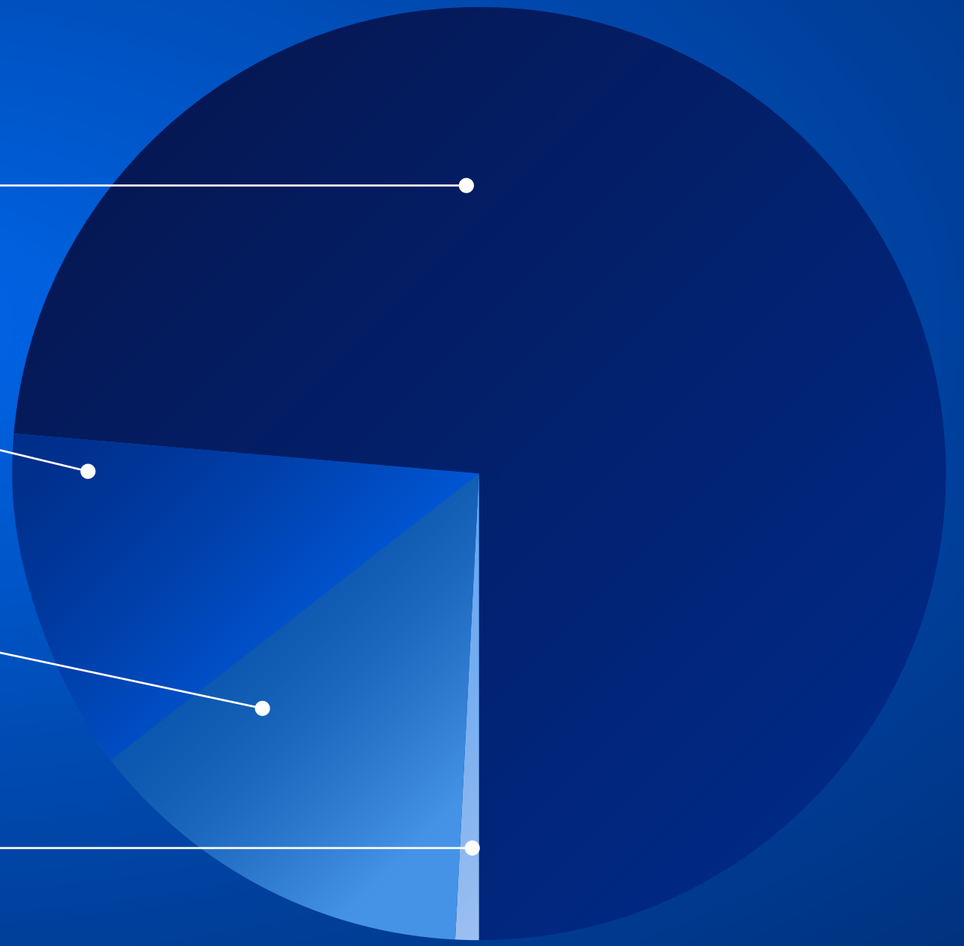
Ciberamenazas más utilizadas

73 % Phishing

15 % Ingeniería social/BEC

11 % Malware

1 % Ataques avanzados



Acronis

Informe semestral sobre ciberamenazas 2023

5 principales bandas de ransomware por número de víctimas

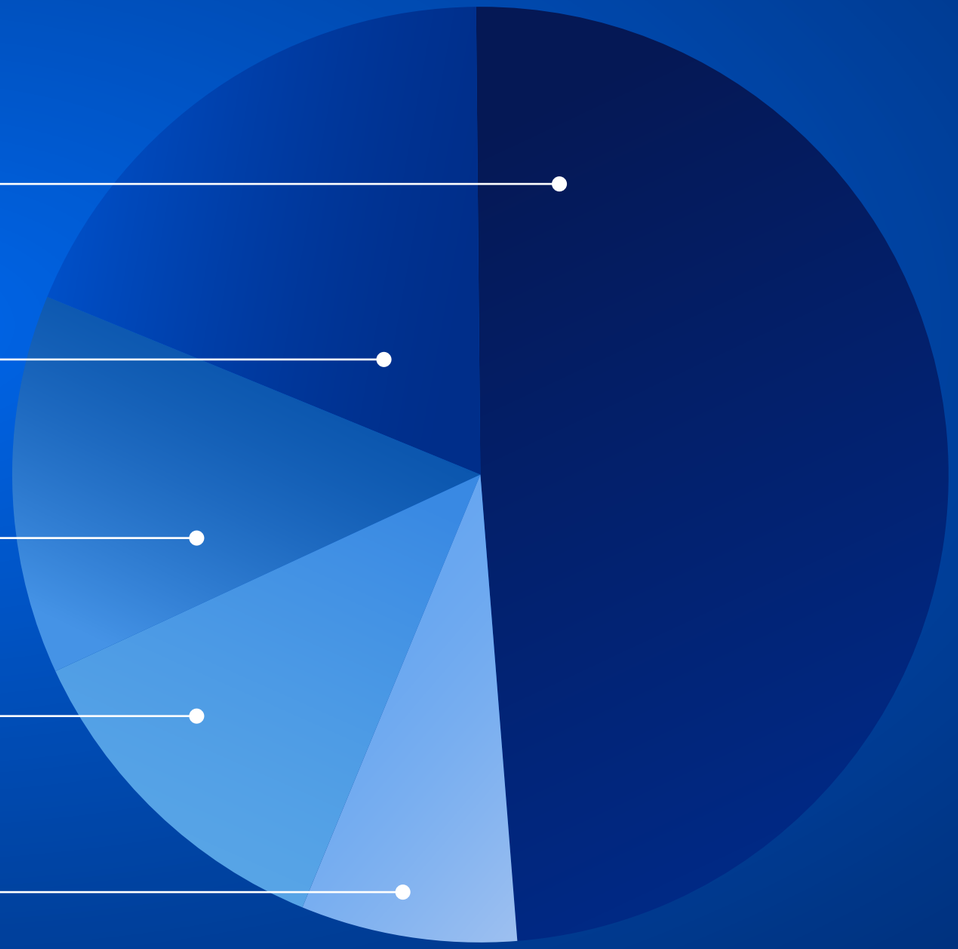
49 % LockBit

19 % Clop

13 % BlackCat / ALPHV

12 % Royal

7 % Play



Acronis

Informe semestral sobre ciberamenazas 2023

10 países con el mayor número de URL bloqueadas en abril de 2023

Ranking	País	Porcentaje de URL bloqueadas en abril de 2023
1	Alemania	20,9
2	Singapur	13,9
3	Italia	11,7
4	Reino Unido	10,3
5	Suiza	9,1
6	Japón	9
7	Francia	7,1
8	España	4,5
9	India	4,4
10	Países Bajos	2,6

10 países con el mayor número de detecciones de malware en abril de 2023

Acronis

Informe semestral sobre ciberamenazas 2023

Ranking	País	Porcentaje de detecciones de malware en abril de 2023
1	Corea del Sur	26
2	Egipto	25,7
3	Singapur	23,2
4	Taiwán	21,1
5	China	20,4
6	Vietnam	18,2
7	Marruecos	17,1
8	Argentina	16,3
9	Turquía	15,7
10	Nigeria	14,5

Acronis

Informe semestral sobre ciberamenazas 2023

Auge de la IA

No es de extrañar que los ciberdelincuentes experimenten con esta nueva generación de inteligencia artificial (IA) para optimizar sus ataques. Los ciberdelincuentes pueden utilizar la IA para crear, automatizar, escalar y mejorar nuevos ataques mediante el aprendizaje activo.

La disponibilidad de modelos de lenguaje de gran tamaño (Large Language Models, LLM), como ChatGPT, permite a los ciberdelincuentes aumentar aún más el número de ataques con automatización y repetición. Como consecuencia, también ha crecido el número de operadores en el mercado del ransomware.

En el primer trimestre de 2023, observamos la aparición de 10 grupos nuevos que sumaron en total 61 ciberataques en todo el mundo.

En el primer trimestre de 2023, observamos la aparición de 10 grupos nuevos que sumaron en total 61 ciberataques en todo el mundo.

Abyss	1	Vendetta	3
Dark Power	10	Cryptnet	2
Akira	9	CrossLock	1
Money Message	8	Nevada	0
Trigona	7		
Do it	7		

Cómo prepararse #CyberFit para el futuro

Acronis

Informe semestral sobre ciberamenazas 2023

Los ciberataques modernos, las fugas de datos y los brotes de ransomware señalan todos lo mismo: el enfoque de ciberseguridad actual está fallando. Para combatir esta situación, siga estos consejos:

1. Utilice una solución de ciberprotección integrada (como Acronis Cyber Protect) que combine protección antimalware, EDR, DLP, seguridad del correo electrónico, evaluaciones de vulnerabilidades, administración de parches, RMM y funciones de copia de seguridad en un único agente.

2. Implemente una solución de detección y respuesta para endpoints (EDR) que le proporcione la visibilidad necesaria para entender los ataques y que, a la vez, simplifique el contexto para los administradores y facilite una corrección eficaz.

3. Aplique continuamente parches a su sistema operativo y sus aplicaciones. Muchos ataques consiguen sus objetivos debido a que hay vulnerabilidades sin parche. Utilice regularmente las funciones de evaluación de vulnerabilidades y administración de parches.

4. Tenga cuidado con los intentos de phishing. El uso de funciones adicionales y específicas de filtrado de URL puede ayudar a filtrar los mensajes de phishing y los enlaces sospechosos.

5. Asegúrese de que su solución de ciberseguridad está configurada correctamente. Debe realizar un análisis completo al menos una vez al día y habilitar los análisis bajo demanda y en el momento del acceso (en tiempo real) para que se activen siempre que se instale o se ejecute software nuevo.

6. Consejo de seguridad número uno: proteja la privacidad de sus contraseñas y los espacios de trabajo. Asegúrese de que sus contraseñas son robustas y no las comparta nunca con nadie.