



SOLUTION
Tronix



SOLUTION
Tronix

“ELIMINACION DE VIRUS Y MALWARE”

AUTOR: JEAMPIERRE MUÑOZ

AÑO: 2023

INDICE:

- A. Eliminación de Virus y Malware**
- B. Recomendación de Antivirus.**



SOLUTION
Tronix

Eliminación de Virus y Malware

Paso 1: Identificación del Problema

- Antes de eliminar cualquier virus o malware, debes estar seguro de que tu computadora esté infectada. Algunos síntomas comunes incluyen ralentización del sistema, ventanas emergentes inesperadas, cambios en la configuración del navegador y problemas de rendimiento.
- Utiliza un software antivirus confiable para realizar un análisis completo del sistema y confirmar la presencia de virus o malware.

Paso 2: Aislamiento de la Computadora

- Desconecta tu computadora de Internet para evitar que el malware comunique con su servidor descargue más amenazas.
- Desconecta todos los dispositivos de almacenamiento externo, como unidades USB, para prevenir la propagación.



Paso 3: Realiza una Copia de Seguridad

- Antes de realizar cualquier acción, realiza una copia de seguridad de tus archivos importantes en un dispositivo externo o en la nube.

Paso 4: Reiniciar en Modo Seguro

- Reinicia tu computadora en Seguro. Esto evita que se ejecuten programas y servicios innecesarios, lo que facilita la eliminación de malware.
- El método para acceder al Seguro puede variar según el sistema operativo. Investiga cómo hacerlo en tu sistema específico.



Paso 5: Escaneo con Herramientas Anti-Malware

- Utiliza software anti-malware confiable como Malwarebytes, Spybot Search & Destroy o Windows Defender para realizar un escaneo completo del sistema.
- Sigue las instrucciones del software para eliminar cualquier malware detectado.

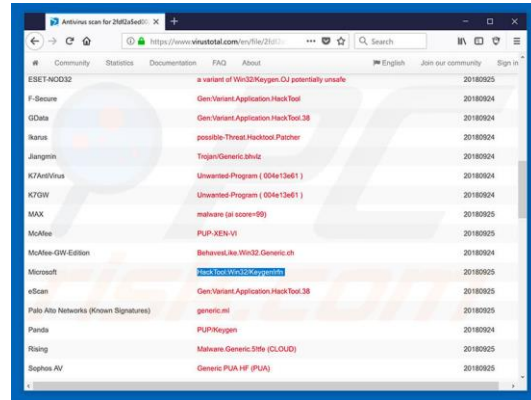


Paso 6: Actualiza y Escanea con Antivirus

- Actualiza tu software antivirus y realiza un escaneo completo del sistema para asegurarte de que no haya quedado ninguna amenaza.

Paso 7: Eliminación Manual

- Si el software antivirus o anti-malware no pudo eliminar algunas amenazas, puedes intentar eliminarlas manualmente.
- Investiga el malware específico encontraste y sigue guías confiables en línea para su eliminación.



que

Paso 8: Limpieza del Sistema

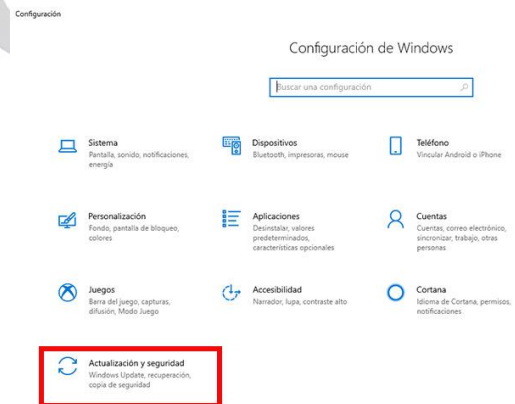
- Utiliza utilidades de limpieza como CCleaner para eliminar archivos temporales y registros no deseados que puedan haber sido dejados por el malware.

Paso 9: Actualiza Contraseñas

- Cambia todas tus contraseñas importantes, especialmente las relacionadas con cuentas en línea, ya que podrían haber sido comprometidas.

Paso 10: Conéctate a Internet y Actualiza el Sistema Operativo

- Una vez que estés seguro de que tu sistema está limpio, conéctate nuevamente a Internet y actualiza tu sistema operativo y software a la última versión para corregir vulnerabilidades.



Paso 11: Monitoreo Continuo

- Realiza análisis periódicos de tu sistema con software antivirus y anti-malware.
- Mantén tu software actualizado y sé cauteloso al descargar y abrir archivos de fuentes desconocidas.

Recomendación de Antivirus

A continuación, los 5 mejores antivirus.

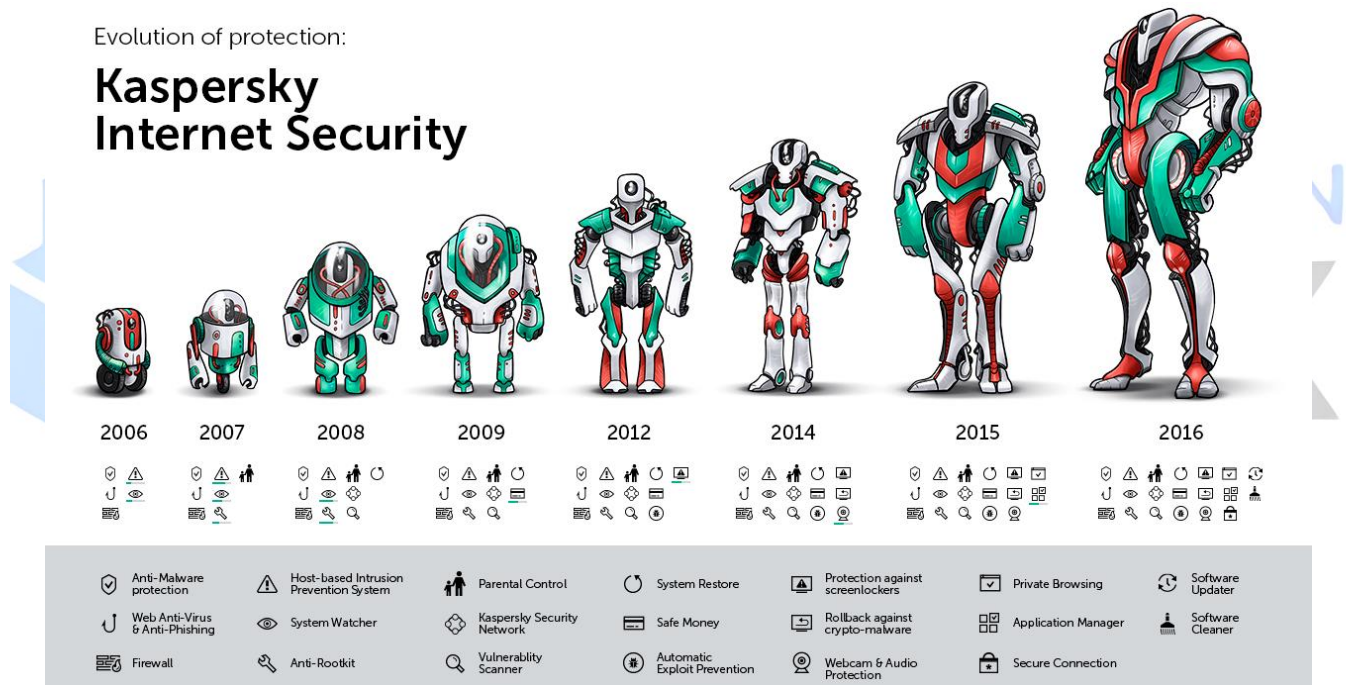
1. Kaspersky Lab



- Procedencia: Rusia
- Alcance: Ofrece una amplia protección contra malware, ransomware, phishing y otras amenazas en múltiples plataformas, incluyendo Windows, macOS, Android e iOS.
- Estrategia: Utiliza tecnologías avanzadas como el aprendizaje automático y la inteligencia artificial para detectar amenazas. Ofrece características adicionales como control parental y protección de la privacidad en línea.

Evolution of protection:

Kaspersky Internet Security



2. Norton Antivirus



- Procedencia: Estados Unidos
- Alcance: Proporciona protección contra virus, malware, ransomware y estafas en línea en diversas plataformas.

- Estrategia: Norton utiliza una amplia red de inteligencia de amenazas para identificar y bloquear amenazas en tiempo real. Ofrece características como firewall y administración de contraseñas.

	Norton Standard	Norton Deluxe	Norton Premium
Online Threat Protection	✓	✓	✓
Identity Protection	✓	✓	✓
Android App Monitoring	✓	✓	✓
Across Multiple Devices	✓	✓	✓
Easy Management Through Web Portal		✓	✓
Parental Controls		✓	✓
Documents Back Up			✓
25 GB Online Storage			✓
Number of Protected Devices	1 Device	3 or 5 Devices	10 Devices

3. Bitdefender



- Procedencia: Rumania
- Alcance: Ofrece protección completa contra malware, incluyendo ransomware, junto con características de seguridad adicionales.
- Estrategia: Bitdefender utiliza tecnologías avanzadas de detección basadas en la nube y realiza análisis de comportamiento para identificar amenazas. También incluye un cortafuegos y un administrador de contraseñas.

	Bitdefender Premium Security	Bitdefender Total Security	Bitdefender Internet Security
Unlimited VPN traffic	✓	×	×
Priority Support	✓	×	×
Device Optimizer	✓	✓	×
Windows, macOS, Android and iOS protection	✓	✓	Windows
Parental Control	✓	✓	✓
Protection against malware, spyware, adware	✓	✓	✓
Multi-Layer Ransomware Protection	✓	✓	✓

4. McAfee



- Procedencia: Estados Unidos
- Alcance: Proporciona protección contra virus, malware, ransomware y phishing en una variedad de plataformas.
- Estrategia: McAfee utiliza inteligencia de amenazas y análisis de comportamiento para detectar y bloquear amenazas. Ofrece características como control parental y protección de identidad en línea.

McAfee Livesafe Premium Plus:					
	Windows 10 Home/Pro	Windows 10 in S mode	Mac OS	Android	iOS
WebAdvisor	✓	✓	✓	✓	✓
Password Manager	✓	✓	✓	✓	✓
Personal VPN - Up to 5 Devices	✓	✓		✓	✓
Parental Controls	✓			✓	✓
Antivirus Protection	✓		✓	✓	
PC Optimisation Tools	✓				
Web Management Portal	✓	✓	✓	✓	✓

5. Avast Antivirus



- Procedencia: República Checa
- Alcance: Ofrece protección antivirus básica y avanzada contra malware, ransomware y phishing en múltiples plataformas.
- Estrategia: Avast utiliza una amplia red de detección basada en la nube y actualizaciones frecuentes para proteger contra amenazas emergentes. También incluye una VPN y un administrador de contraseñas.

