CIBERSEGURIDAD

SCP

Fight against Ransomware

Cyberoam

Avira

CRYPTOPHONE

NEXXT SOLUTIONS

open source

Índice

CREDITOS:

Revista virtual de seguridad informática, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:
Consuelo de la Torre
c.delatorre@scprogress.com (+593 979003123)
Marco de la Torre
m.delatorre@scprogress.com (+593 998053611)

Revisado por:
Arturo de la Torre
adltorre@scprogress.com (+593 999025294)

Síguenos en:

www.scprogress.com Facebook Twitter

Proyecto europeo “No More Ransom”

La peor pesadilla en la seguridad informática hoy en día, es el malware muy bien conocido como Ransomware, un software malicioso que al infectar los equipos, los ciberdelincuentes tienen la capacidad de bloquearlos a través de la encriptación de toda la información, quitando el control de todos los datos, hasta que realice el rescate a través de un pago en efectivo o bitcoins dentro de los tres días posteriores a la infección.

Las ciberamenazas dirigidas a empresas se han triplicado desde enero de 2016. Las compañías se enfrentan a un ataque cada 40 segundos y el Ransomware ha conseguido infectar uno de cada cinco negocios del mundo. Para los consumidores las cifras son aún peores, ya sufren un asalto cada 10 segundos.

Siendo Ransomware el mayor problema de ciberseguridad del año 2016, tanto para las empresas como para los consumidores. Durante 2016 hemos vivido casos como el de un hospital de Hollywood que se vio obligado a pagar 17.000 dólares para que sus sistemas volvieran a funcionar después de un ataque. El metro de San Francisco también sufrió en noviembre un Ransomware que afectó a sus servidores y no permitía a los viajeros pagar sus billetes. Además, este tipo de malware ha empezado a extenderse a través de imágenes en Facebook y LinkedIn, se ha creado el proyecto “No More Ransom”.

“No More Ransom” fue puesto en marcha el 25 de julio de 2016 por la Policía Nacional de Holanda, Europol e Intel Security, lo que dio inicio a un nuevo nivel de cooperación entre la policía y el sector privado para luchar juntos contra el Ransomware. El objetivo del portal en línea www.nomoreransom.org es proporcionar un recurso de utilidad para las víctimas de esta amenaza. Los usuarios pueden encontrar información sobre lo que es el Ransomware, cómo funciona y, lo más importante, la forma de protegerse.

Durante los dos primeros meses, más de 2,500 personas han logrado administrar con éxito el descifrado de sus datos sin tener que pagar a los criminales, utilizando las principales herramientas de descifrado

disponibles en la plataforma (CoinVault, Wildfire y Shade). Esto ha privado a los delincuentes, según un estimado, de más de un millón de dólares en rescates.

Mientras más organismos policiales y socios del sector privado trabajen juntos, más herramientas de descifrado pueden crearse y ponerse a disposición de las víctimas. En la actualidad, aparece una lista de cinco herramientas en la página web.

Desde la presentación del portal, se ha agregado WildfireDecryptor y dos herramientas de descifrado han sido actualizadas: RannohDecryptor (con un descifrador para el Ransomware MarsJoke, también conocido como Polyglot) y RakhniDecryptor (con Chimera).

"*Europol está totalmente comprometida con apoyar la ampliación del proyecto No More Ransom en la Unión Europea (UE), así como a nivel internacional para responder al Ransomware de una manera eficaz y concertada",* **dice Steven Wilson, director del Centro Europeo de Ciberdelincuencia**. *"A pesar de los retos cada vez mayores, la iniciativa ha demostrado que un método coordinado por las autoridades de la UE, que incluya todos los asociados pertinentes, puede dar lugar a éxitos significativos en la lucha contra este tipo de delito, al centrarse en las importantes áreas de la prevención y el conocimiento. Estoy seguro de que el portal seguirá mejorando en los próximos meses. Exhortamos amigablemente a todas las fuerzas policiales a unirse a la lucha".*

Check Point Software Technologies, el mayor proveedor mundial especializado en seguridad, también pasó a formar parte de "No More Ransom". Entre los integrantes se encuentran las fuerzas policiales de 22 países de Europa, la Comisión Europea, las principales empresas de ciberseguridad y entre los nuevos miembros también está la Policía Nacional de Colombia, así como, las fuerzas del orden de Bosnia y Herzegovina, Bulgaria, Francia, Hungría, Irlanda, Italia, Letonia, Lituania, Portugal, España, Suiza y el Reino Unido. Se espera que más autoridades y organizaciones del sector privado se unan al programa en los próximos meses. Su colaboración se traducirá en más herramientas gratuitas de descifrado para ayudar a las víctimas a liberar sus dispositivos y desbloquear su información y así golpear a los delincuentes donde más les duele: en sus carteras.

FUENTES: http://computerhoy.com/noticias/software/que-es-Ransomware-como-evitarlo-6642
http://www.ticpymes.es/informatica-telecomunicaciones/informes/1094678026104/crece-no-more-ransom-el-primer-proyecto-europeo-de-lucha-contra-el-Ransomware.1.html
http://www.delitosfinancieros.org/en-la-lucha-contra-el-Ransomware-10-cosas-para-hacer-en-el-caso-de-un-ataque/
http://Ransomware.phishme.com/

efectivo

Cooperativa de Ahorro y Crédito "General Rumiñahui"

Promoviendo el desarrollo y bienestar de sus socios militares y civiles desde 1993.

- Créditos sin garante hasta 3.000 dólares.
- Otorgamos créditos para consumo, emprendedores y microempresarios.
- Las tasas de interés más bajas del mercado.
- Inversiones a plazo fijo.
- Pagos de créditos y ahorros, a través de ventanillas o con autorización de débitos bancarios del Banco Pichincha, General Rumiñahui e ISSFA.

- Asistencia ambulatoria
- Consultas médicas de primer nivel ilimitadas en cualquiera de las patologías derivadas de: medicina general, ginecología y pediatría.
- Cobertura en asistencia dental.
- Examen clínico y diagnóstico.
- Higiene dental, alivio del dolor.
- Rayos X periapical, profilaxis (Limpieza dental profunda).
- Restauraciones en resina simple.
- Extracciones simples.

Calle Manuel Cabeza de Vaca N53-240 y Av. Los Pinos a 30 mts. Del Cuartel Rumiñahui.
Teléfonos: 2411-731 / 2406-117 / 0984977204

www.cooprumi.fin.ec

Reducir al mínimo amenazas de Ransomware

Una vez utilizado en gran medida por los delincuentes cibernéticos para dirigirse a los consumidores para obtener recursos rápidamente, los ataques Ransomware han escalado a la empresa, con adversarios altamente motivados y focalización hacia las redes corporativas con tácticas cada vez más creativas. Recientemente, los principales medios de comunicación, incluyendo la BBC y The New York Times también se vieron afectadas por el Ransomware que exigía el pago en Bitcoin para desbloquear equipos de los usuarios. Según The Guardian, el malware "se entrega a través de varias redes de anuncios y se utiliza una serie de vulnerabilidades, incluyendo una falla parcheada recientemente en el ex competidor de Flash, Silverlight de Microsoft, el cual fue descontinuado en 2013."

Hay dos tipos de ataques Ransomware que las organizaciones podrían experimentar:

1. La primera de ellas es Ransomware "estándar", que infecta las máquinas de usuarios, que es el mismo Ransomware que infectaría a un consumidor regular en casa. Estos ataques serán oportunistas y menos perjudicial para las organizaciones, que por lo general almacenan la información importante sobre los servidores dedicados y en bases de datos fuera del alcance de los atacantes, por lo que los archivos en las máquinas de los usuarios pueden ser bastante fáciles de reemplazar.

2. El segundo tipo es mucho más peligroso. Estos ataques Ransomware siguen el mismo patrón de ataque general, como los ataques de red específicas, pero para un objetivo final muy diferente. En lugar de robo de información, los atacantes Ransomware buscan causar el caos generalizado a través de la infección masiva y el cifrado de datos de usuario. Para ello, los atacantes suelen buscar cuentas privilegiadas para secuestrar (ambas cuentas de usuarios privilegiados y cuentas de aplicaciones utilizadas por los procesos automatizados, servicios y aplicaciones), y luego explotarlos para propagar el Ransomware en toda la red.

Un ejemplo de ello es un reciente ataque que tenía como objetivo tres diferentes bancos de la India y una compañía farmacéutica, lo que resulta en millones de dólares en daños. El atacante se infiltró en las redes de cada empresa, secuestrando las credenciales con privilegios necesarios, a continuación, se intensificó el acceso a otros ordenadores a través de puertos desprotegidos de escritorio remoto (PDR). Con acceso a una computadora "secuestrada", el atacante descargó el Ransomware desde un servidor y luego comenzó el proceso de cifrado. Sin accesos privilegiados, la misión del atacante no podría haberse logrado.

La eliminación de privilegios locales puede ayudar a defenderse contra los ataques de Ransomware, sin embargo, no es necesariamente suficiente. Por ejemplo, cryptolocker es un ejemplo de malware que cifra los datos utilizando derechos de usuario estándar, por lo que los esfuerzos para eliminar o restringir los derechos administrativos locales sin medidas de seguridad adicionales no mitiga el riesgo por completo. Además, porque cryptolocker cifra (y hace ilegible) todos los archivos que un usuario tiene acceso a en un entorno corporativo, tiene un efecto devastador.

Con el aumento de la atención en el Ransomware, muchas organizaciones se centran en la eliminación de la amenaza de una infección Ransomware. Para defenderse eficazmente contra este tipo de ataques Ransomware, las organizaciones deben combinar el principio del mínimo privilegio y control de aplicaciones para reducir la superficie de ataque y bloquear su progresión. Este enfoque de doble vertiente puede evitar que entren Ransomware una organización de cuatro formas principales:

1. Bloquea las aplicaciones no confiables.
2. Asimismo, se restringe o deniega el acceso a las aplicaciones desconocidas (como cryptolocker).
3. Se monitorea continuamente las aplicaciones que entran en el medio ambiente.
4. Se elimina privilegios de administrador local para bloquear a cryptolocker de suprimir el shadow copy command.
5. Se permite a los equipos de seguridad para restaurar archivos cifrados usando shadow copy.

Las organizaciones deben buscar herramientas flexibles que automatizan la gestión de privilegios de administrador local y el control de las aplicaciones en los puntos finales y servidores. Esta combinación única de privilegio mínimo y control de aplicaciones puede ayudar a las empresas a reducir la superficie de ataque, protección contra las amenazas que han hecho su camino en el interior, y los equipos de seguridad alertar de posibles ataques en proceso – todo ello sin detener la productividad de los usuarios o de los equipos de seguridad de TI abrumadoras.

FUENTE: http://infosecuritymexicoblog.com/2016/11/14/reducir-al-minimo-amenazas-de-Ransomware-mientras-se-consigue-la-seguridad-y-la-productividad-con-privilegio-minimo-y-control-de-aplicacion/

Rincón de los expertos

Seis reglas básicas para combatir el Ransomware en el 2017

Ransomware distribuye software una vez que se encuentra en tu equipo, es decir, realiza la instalación de aplicaciones que cifran toda la información, y posteriormente te exigen pagos de alrededor de 500 USD para permitirte desencriptar y poder nuevamente acceder a tus datos. A continuación te recomiendo algunas sugerencias que te servirán para combatir estos ataques cibernéticos.

1) No aceptes correos electrónicos o nuevos contactos en las redes sociales de personas que desconoces o de las cuales no tienes ninguna referencia real.
2) Mantén todo el software de tu computador actualizado, esta medida permitirá reducir la cantidad de vulnerabilidades que pueden ser explotadas para introducir software malicioso a tus equipos.
3) Evita descargar e instalar en tus computadores y dispositivos móviles, supuestos aplicativos o programas que te ayudan a eliminar alguna clase de malware; lo mas probable es que estas soluciones sean temporales y finalmente solo creen nuevas vulnerabilidades en tus equipos.
4) Realiza periódicamente copias de seguridad de tu información, en la nube o en discos duros externos.
5) Instala en tu equipo el mejor antivirus posible, que tenga licencias validas y cuente con soporte de fabrica para ayudarte en caso de que tengas problemas.
6) Evita usar proxy, aunque fue en el pasado la mejor herramienta para acelerar tu red hoy puede ser el principal punto de ataque a tus equipos. Por lo que te recomendamos usar únicamente transparent proxy.

Si requieres mas información no dudes en comunicarte por correo electrónico a la dirección avira@scprogress.com

“Ransomware es único entre los delitos informáticos, porque para que el ataque tenga éxito, se requiere de la víctima para convertirse en un cómplice después del hecho.”

— James Scott —

Empresas o personas interesadas en promocionarse en nuestra revista, por favor contactarse con c.delatorre@scprogress.com

Noticias

El peligroso Ransomware spora se propaga por todo el mundo

Investigadores de seguridad informática advierten que Spora, un peligroso Ransomware que fue detectado a principios de enero orientado a usuarios rusos, ya ha comenzado a propagarse por todo el mundo.

Las primeras infecciones de Spora se conocieron en los foros de Bleeping Computer durante la primera semana del año. De acuerdo con los informes, el malware se estaba extendiendo por correo electrónico camuflado en mensajes que simulaban ser facturas.

Los emails iban con un archivo adjunto en formato ZIP que contenía un fichero en formato HTA, que es una aplicación HTML. Además, empleaban una doble extensión para aparentar normalidad, como PDF.HTA o DOC.HTA, ya que en los equipos Windows donde se oculta la extensión del archivo, el usuario solo ve la primera extensión ficticia.

La infección se produce en caso de ejecutar este archivo, que iniciará el proceso de cifrado de los archivos del ordenador. Mientras se encripta el contenido, Spora extrae y ejecuta un documento de Word dañado que muestra un mensaje de error, con la finalidad de distraer a la víctima.

A diferencia de otras familias de Ransomware, Spora no necesita conexión a Internet y no genera ningún tráfico de red, una característica que lo convierte en muy peligroso. Esto es debido a que, al no conectarse con un servidor de comando y control, genera una clave pública RSA diferente para cada víctima, lo que hace que no funcione la misma herramienta de descifrado para todos los infectados.

Este Ransomware no cifra todo el contenido, sino solo una selección de los documentos que pueden resultar más importantes, entre los que se encuentran ficheros de Excel, Word, imágenes, archivos comprimidos o backups. Una vez finalizado el proceso, muestra al usuario una pantalla con las instrucciones para desbloquear el PC.

En Spora solo había sido detectado en Rusia, pero ahora se ha expandido a otros países, entre los que se encuentra Austria, Países Bajos, Japón o Arabia Saudita. No se descarta que vaya a llegar a otros territorios, así que vigila la bandeja de entrada de tu correo electrónico.

Fuente: http://computerhoy.com
http://noticiasseguridad.com/malware-virus/el-peligroso-Ransomware-spora-se-propaga-por-todo-el-mundo/

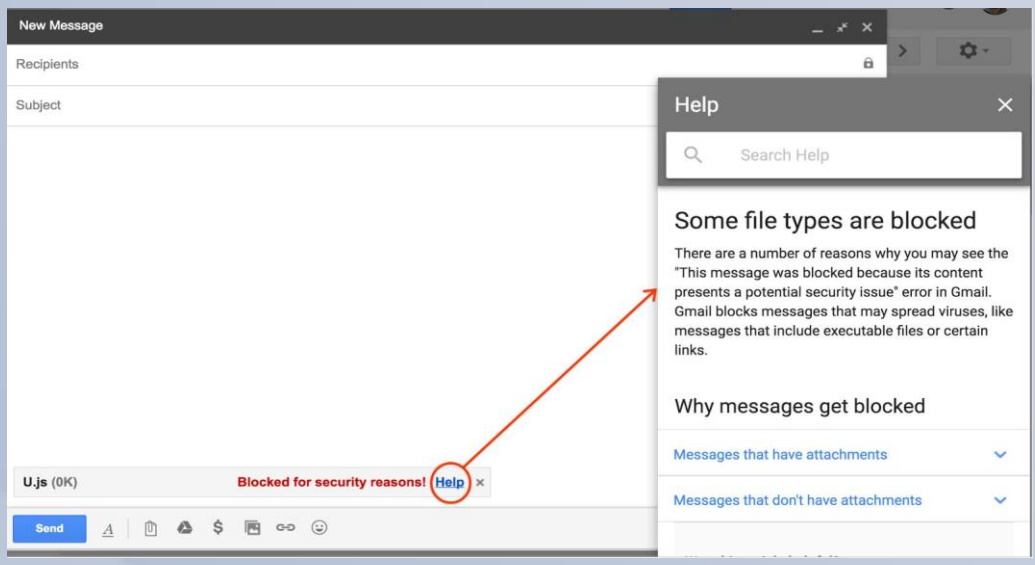
Gmail no permitirá adjuntar ficheros JavaScript a partir de febrero

Los servicios de email suelen bloquear ciertos tipos de ficheros que pueden terminar siendo un peligro para la seguridad de los usuarios, con especial mención a los ejecutables y scripts de Windows, ya que el sistema operativo de Microsoft ha sido durante años el único objetivo prioritario del malware.

Gmail, que es uno de los servicios de email más conocidos y usados, bloquea una cantidad nada desdeñable de tipos de ficheros, los cuales son los siguientes:

```
.ADE, .ADP, .BAT, .CHM, .CMD, .COM, .CPL, .EXE, .HTA, .INS, .ISP, .JAR, .JSE, .LIB, .LNK,
.MDE, .MSC, .MSP, .MST, .PIF, .SCR, .SCT, .SHB, .SYS, .VB, .VBE, .VBS, .VXD, .WSC, .WSF y .WSH
```

Gmail sumará el 13 de febrero de 2017 un nuevo tipo de fichero entre los que serán bloqueados cuando quieran adjuntarse a un email, los JavaScript, que tienen por extensión *.js*.



Recordamos que Gmail también supervisa los ficheros contenidos dentro de los archivos comprimidos, así que habrá que ingeniárselas para poder enviar ficheros JavaScript a través de ahí. Viendo las circunstancias y como bien apunta la compañía, sería más sensato recurrir a alternativas como Google Drive y Google Cloud Storage.

En la imagen se puede ver que Google esgrime **"razones de seguridad"** para bloquear los ficheros JavaScript en su servicio de correo electrónico, y motivos no les falta, ya que con el paso del tiempo vamos viendo como poco a poco el malware multiplataforma se está abriendo paso, habiendo incluso Ransomware construido con esta tecnología.

Fuente: Google
http://muyseguridad.net/2017/01/26/gmail-no-adjuntar-javascript/

Humor


SOY TÉCNICO INFORMÁTICO. TENÍA EL ENCARGO DE PONER ESTOS ORDENADORES EN RED Y YO PENSÉ QUE...
VENTURA 2000


necesito más espacio...
128 MB
64 GB


¿¿SE PUEDE SABER QUÉ ES ESTA CARTA EN EL BOLSILLO DE TU AMERICANA DIRIGIDA A «CUCURUCHITO MÍO»?!
EH...
¡SPAM!
ESO, SPAM


Cuando el fuego era una nueva tecnología...
ESTE FUEGO FUNCIONA MAL... DA POCO CALOR Y DEJA LA CARNE MEDIO CRUDA
¿PROBÓ APAGARLO Y VOLVER A ENCENDERLO?
Daniel para PAZ Dattatec

¿Cuáles son los mejores programas gratuitos de eliminación de malware de 2017?

En el mundo de hoy día, el grado de cibercrimen no es para nada corto de épica. El malware, por supuesto, es la principal herramienta usada por los ciber criminales para tomar el control ilegalmente de los ordenadores de las víctimas, y cada usuario de ordenador debería tomar ciertas acciones con el fin de parar estos ataques de malware a tiempo. Aunque la conciencia sobre el cibercrimen también es importante, seamos realistas, toma mucho tiempo leer todas las noticias sobre las últimas tendencias de distribución de malware y engaños usados por los estafadores, y lo que es más, mucha gente encuentra estos tópicos aburridos y solo hechos para gente con conocimientos técnicos. Por ello, la mejor solución es instalar un buen programa anti-malware, el cual pueda soportar la carga de mantener la seguridad de tu ordenador así como de tu navegación por Internet.

Sin embargo, no es un secreto que la vasta mayoría de eliminadores de malware top son programas de pago y solo algunos ofrecen versiones de prueba gratuitas. ¿Qué hacer si no tienes o no quieres pagar dinero por un programa de seguridad? Esto es totalmente legítimo, aunque los programas de pago son conocidos por ser más eficientes en la lucha contra malware. Aun así, hay muchos eliminadores de malware gratuitos que son beneficiosos y útiles y que pueden solucionar tu ordenador si accidentalmente has instalado algún tipo de malware en él. Abajo, te proporcionamos una lista de eliminadores de malware top que pueden limpiar tu ordenador de malware gratis.

CONSEJO: Por favor, ten cuidado cuando instales nuevos programas. Descarga programas solo de fuentes fiables de Internet y selecciona siempre las opciones de instalación Avanzadas o Personalizadas cuando los instales, con el fin de desmarcar todos los programas adicionales indeseados, como toolbars y otras aplicaciones que no quieres instalar.

1. Avira Free Antivirus

Avira Free Antivirus es conocido por sus excelentes habilidades de detección de malware. La versión gratuita proporciona protección contra malware, como virus, troyanos y spywares. El programa está basado en la Nube de Protección, que es un sistema que analiza anónimamente detecciones sospechosas en la nube. Aunque la versión gratuita comprueba el sistema más lentamente que la versión Pro, el programa proporciona un amplio set de características útiles. Con su altamente personalizable motor de escaneo, un gran rango de características add-on, es una de las mejores herramientas gratuitas de eliminación de malware que definitivamente puede llamar tu atención.

2. Malwarebytes Free 3.0

Malwarebytes es un nombre fácilmente reconocible para aquellos que al menos están algo familiarizados con el tema de la ciber seguridad. Esta compañía ha estado trabajando en productos para usuarios de casa y negocios durante años. Su producto reciente, Malwarebytes 3.0, es un nuevo programa de eliminación de malware que ofrece una versión gratuita para gente que no quiera pagar por un programa de seguridad. El programa ofrece una versión de prueba de 14 días de Malwarebytes Premium y la revierte a versión gratuita tras este tiempo. La versión gratuita funciona como anti-malware/anti-spyware, lo que significa

que detecta y elimina varios tipos de malware. Además, Malwarebytes 3.0 Free tiene característica anti-rootkit, lo cual ayuda a eliminar rootkits y reparar los archivos que corrompen.

3. Spybot Search and Destroy

La versión Spybot Free es una buena opción para aquellos que buscan una herramienta de eliminación de malware gratuita y también para aquellos que buscan alguna capa más de protección gratuitamente. Su escáner puede detectar rootkits, spyware, y amenazas malware y, aunque el programa es relativamente lento, es una herramienta útil que puede funcionar junto a la mayoría de programas antivirus. El programa también proporciona un panel para usuarios más avanzados de PC, lo que permite escanear localizaciones particulares de autoinicio, comprobar archivos individuales o carpetas sin importar si están localizadas en los discos duros o en redes de compartición. Por encima de esto, Spybot Search & Destroy escanea archivos basados en la lista blanca, lo que ayuda a determinar si son seguros o no. Finalmente, este producto gratuito también ofrece soporte gratuito, por lo que puedes siempre apoyarte en el equipo de asistencia de Spybot a través de email. Lee más sobre este producto en el análisis de Spybot.

4**. Panda Free Antivirus**

Panda Free Antivirus es uno de los mejores programas gratuitos de seguridad disponibles a día de hoy. Este programa de peso ligero es fácil de usar y poderoso. La versión gratuita de Panda Antivirus proporciona máxima protección contra los últimos ejemplos de malware, se actualiza a sí mismo automáticamente y no abruma al usuario con complicadas opciones de configuración. Sin embargo, Panda Free Antivirus no puede presumir de velocidad de exploración, ya que se toma un tiempo mientras el programa comprueba el sistema entero en busca de amenazas. Aun así, considerando que este programa ofrece protección a tiempo real contra spyware y malware, asegura dispositivos USB contra infecciones y ofrece un Kit de Rescate para limpiar tu PC en situaciones críticas, es un producto a considerar si estás buscando una herramienta anti-malware gratuita.

5. Emsisoft Emergency Kit

Aunque Emsisoft ofrece una versión de prueba gratuita del software Emsisoft Anti-Malware, un mes de protección no es suficiente. Si quieres tener una herramienta de eliminación de malware gratuita, deberías considerar instalar Emsisoft Emergency Kit. Este kit puede ser definido como programas que pueden ser usados sin instalación para comprobar y eliminar infecciones del ordenador. Una característica ventajosa de este programa es que es fácilmente portable – puedes transferirlo a un dispositivo USB y usarlo en diferentes ordenadores. Este kit consiste en Emsisoft Emergency Kit Scanner, el cual proporciona una interfaz gráfica de usuario, y Emsisoft Commandline Scanner, el cual es controlado a través de Símbolos del Sistema. Este kit puede detectar y limpiar virus, gusanos, troyanos, dialers, keyloggers y muchos otros ejemplos de spyware/malware. Una desventaja de este programa es que no proporciona protección a tiempo real y funciona relativamente más lento en comparación con otras herramientas alternativas.

6. Microsoft Security Essentials/Windows Defender

Microsoft proporciona un software gratuito de seguridad para cada usuario de Windows. En el pasado, el programa Microsoft Security Essentials fue usado para defender ordenadores con sistemas Windows Vista y Windows 7 contra virus y spyware, y en Windows 8, se ha reemplazado con Windows Defender, el cual muestra protección contra virus, malware y spyware. Windows Defender ofrece protección a tiempo real, basada en la nube y también protección en el arranque, y todas estas características ayudan a crear un ambiente seguro para cada usuario de Windows. Tristemente, usar Windows Defender junto a otros programas anti-malware puede ser contra-productivo y puede causar ralentizaciones del sistema y

similares problemas. Sin embargo, esta herramienta de seguridad no apunta alto en las pruebas de detección de malware, aunque puede defenderte contra amenazas bien conocidas, no deberías esperar mucho de ella.

¿No te gusta gastar dinero? Instala un programa todo-en-uno

Con muchos antivirus, anti-malwares, optimizaciones de ordenador y programas de limpieza del registro disponibles hoy en día, puede ser difícil seleccionar el correcto. Sin embargo, hay programas que pueden hacer muchas cosas a la vez, y Reimage es exactamente ese tipo de producto. Aunque en el pasado había varios análisis negativos sobre el marketing de Reimage en Internet, esta compañía ha cambiado y ahora es un producto top que se está construyendo rápidamente confianza y reputación entre los usuarios. Nosotros encontramos Reimage extremadamente beneficioso, ya que combina características de eliminador de malware, optimizador de ordenador y también herramienta de recuperación. El programa tiene la tecnología de escaneo Avira AntiVir integrada, lo que garantiza un gran ratio de detección de malware. Además, Reimage puede solucionar errores de Windows, mejorar la velocidad del ordenador y también reemplazar archivos corruptos o eliminados del sistema Windows para asegurar la funcionalidad adecuada del PC. Aunque este producto es de pago, te sugerimos que leas más información sobre él en este análisis.

FUENTE: http://losvirus.es/las-mejores-herramientas-gratuitas-de-eliminacion-de-malware-de-2017/

www.scprogress.com

Febrero 2017