

Rogue: Falsos antivirus gratis



Autor: Cristian Borghello, Technical & Educational Manager de ESET para
Latinoamérica

Fecha: Lunes 05 de agosto de 2008

La mayoría de los productos antivirus actuales son comerciales y generalmente, como sucede con las soluciones de ESET, ofrecen versiones de prueba de 30 días, siendo la excusa perfecta para que los delincuentes ofrezcan antivirus "gratuitos y mágicos" que garantizan solucionar aquellos problemas que el usuario, en realidad, no tiene.

Este tipo de programas reciben el nombre de Rogue y son ofrecidos con el fin de que el usuario los descargue para así poder infectarlo. En este caso, se trata de una técnica de Ingeniería Social [1] en la que se engaña al usuario para que, ante la promesa de productos gratuitos, se descarguen códigos maliciosos.

Actualmente, se distinguen distintos tipos de acciones que ayudan a identificar este tipo de programas:

1. En un sitio web se ofrece una solución gratuita para un malware determinado. Cuando el usuario descarga e instala el producto, se desinfecta al usuario pero se instala otro tipo de programas maliciosos como spyware y adware.
2. Se repite la escena anterior pero con la diferencia de que se informa al usuario sobre una supuesta infección (que puede ser real, o no) y si el usuario desea desinfectar el sistema, se exige una registración del usuario y un pago determinado.
3. Se repite alguna de las escenas anteriores, pero al momento de descargar el producto, se exige el ingreso de datos correspondientes a la tarjeta de crédito.
4. Se repite cualquiera de las escenas anteriores pero además, continuamente se informa al usuario acerca de una infección [2]. El aviso puede realizarse de diversas formas e insistentemente. Tiene el objetivo de "cansar" al usuario o hacerle creer que se trata de un ataque real para que este ingrese sus datos o realice un pago para acreditarse la solución de seguridad que "desinfecte" el sistema.

Lamentablemente, muchas veces se prefiere confiar en la palabra "free" o "gratis" por los supuestos beneficios que ofrecen, en vez de pensar que todo producto de seguridad debe pasar por estrictos controles y evaluaciones que terminan dictaminando la confiabilidad de un producto.

Por ejemplo, es común que se realicen búsquedas de herramientas gratuitas para la eliminación de amenazas y en esos casos se encuentren antivirus o antispyware falsos.



Imagen 1 - Búsqueda de herramientas gratuitas

Cuando se realizan este tipo de búsquedas, es fundamental tener en cuenta que las herramientas de seguridad tengan el aval de certificaciones conocidas y que además cuenten con una trayectoria histórica respetable: no es lo mismo descargar una herramienta “gratuita” como la que se visualiza en la imagen (por más que prometa resultados milagrosos) que descargar un producto con años de respaldo como ESET NOD32, versión de Evaluación Gratuita de 30 días [3].

Análisis de un caso conocido

Para graficar estas metodologías, a continuación se analiza el caso de un rogue muy propagado en Latinoamérica, el de Antivirus XP 2008 (también conocido como Antivirus XP 2009 o MalwareProtector 2008), que ofrece una falsa solución antivirus y que, mediante todas las escenas descritas, intenta que el usuario adquiera la versión registrada de su producto, pagando por el mismo.

Si bien existen diversas maneras por las que el usuario puede llegar al sitio de descarga de este programa, actualmente se utiliza la técnica del spam y si el usuario hace clic en el enlace ofrecido, descargará el antivirus falso:

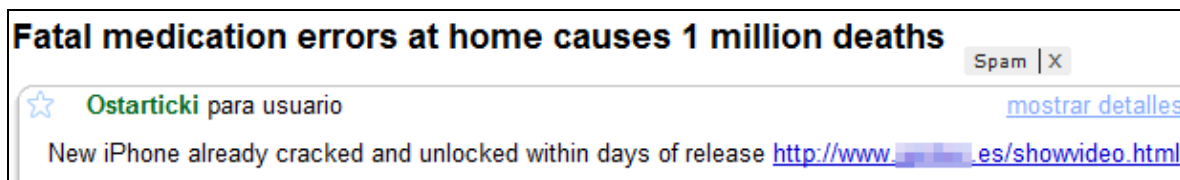


Imagen 2 - Spam promocionando un sitio que apunta a un Rogue

Nota: En algunos casos, el sitio web puede descargar e instalar automáticamente el programa a través de la técnica de Drive-by-Download [4].

Una vez descargado, el producto se instala en un directorio formado aleatoriamente por letras y números. Con esto se intenta confundir al usuario y dificultar la búsqueda en caso de que el mismo decida remover la falsa solución de seguridad:

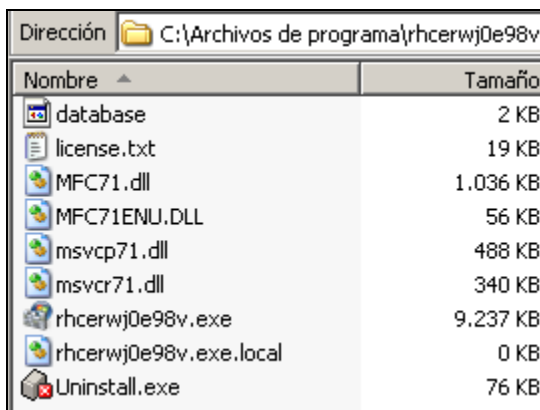


Imagen 3 - Instalación del producto

Cada instalación generará un directorio distinto impidiendo la búsqueda del usuario en el caso de sospechas.

Una vez ejecutado, el programa procederá a realizar una falsa exploración en busca de malware en el equipo del usuario e indefectiblemente informará que el mismo se encuentra infectado. Los métodos para informar al usuario suelen ser invasivos y dificultan el uso normal del sistema operativo.

En este caso, se muestra cómo se informa al usuario a través de la modificación del fondo de pantalla e imposibilitando que el mismo pueda ser cambiado. Además, se informa continuamente (cada un minuto aproximadamente) acerca de una supuesta infección en la barra de tareas, incomodando al usuario.

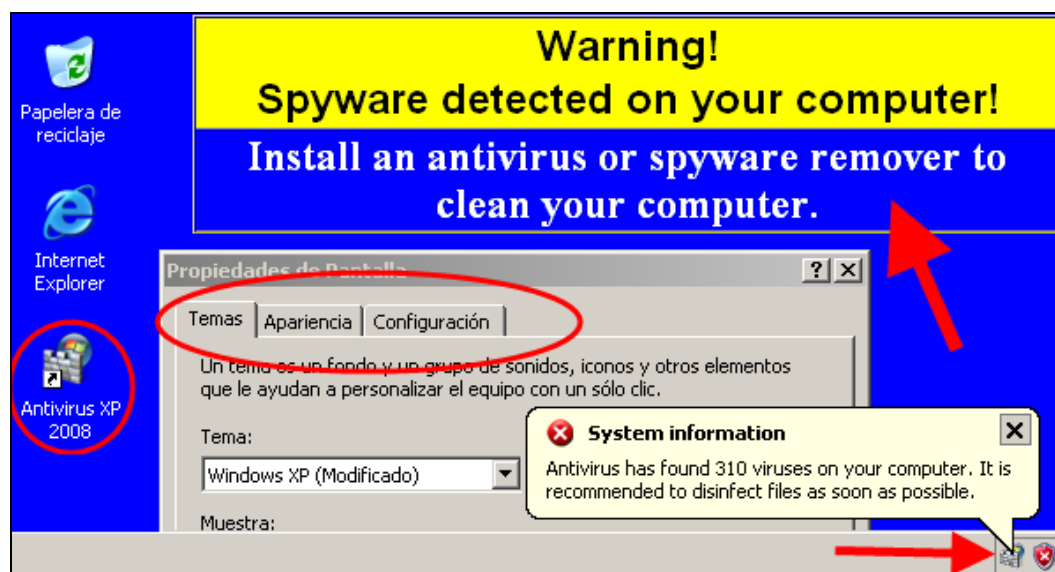


Imagen 4 - Informe del programa sobre una falsa infección

Si el usuario cae en el engaño y decide actualizar el programa o intenta desinfectar su sistema, deberá registrar el producto para lo cual deberá proporcionar sus datos personales y los de su tarjeta de crédito:

<p>ARS 129.95 Pay by credit card</p> <p>Antivirus XP 2008 Standard edition + 1 year free updates Scanner + Spyware Remover + Real-Time Protection + bonus fe... PRICE:ARS 129.95 (This is a One Time Only Charge, your credit c... never be rebilled and you will receive UPGRADES FOR FREE!)</p>
<p>ARS 252.95 Pay by credit card</p> <p>Antivirus XP 2008 Standard edition + 3 years free updates</p>

Imagen 5 - Solicitud de pago para registrar el producto

Para completar el engaño, el producto también informa acerca de la supuesta infección al intentar navegar en Internet. Con este mensaje, se informa al usuario que debe registrar el producto para limpiar su sistema:

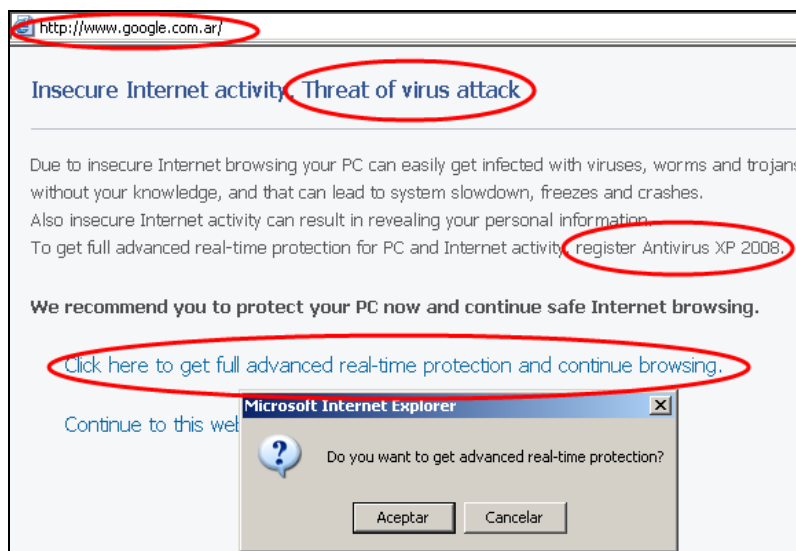


Imagen 6 - Página web mostrada al intentar navegar

Este tipo de programas modifican de manera significativa el sistema en el cual se instalan y buscan que el usuario registre el producto por diversos medios. Además, generalmente instalan otros códigos maliciosos como adware y spyware para controlar y vigilar las acciones del usuario, enviándolas al creador del malware.

Si se decide verificar qué ocurre al intentar desinstalar el programa, cuando se reinicie el sistema el mismo volverá a informar acerca de la supuesta amenaza y la desinstalación no se lleva a cabo:

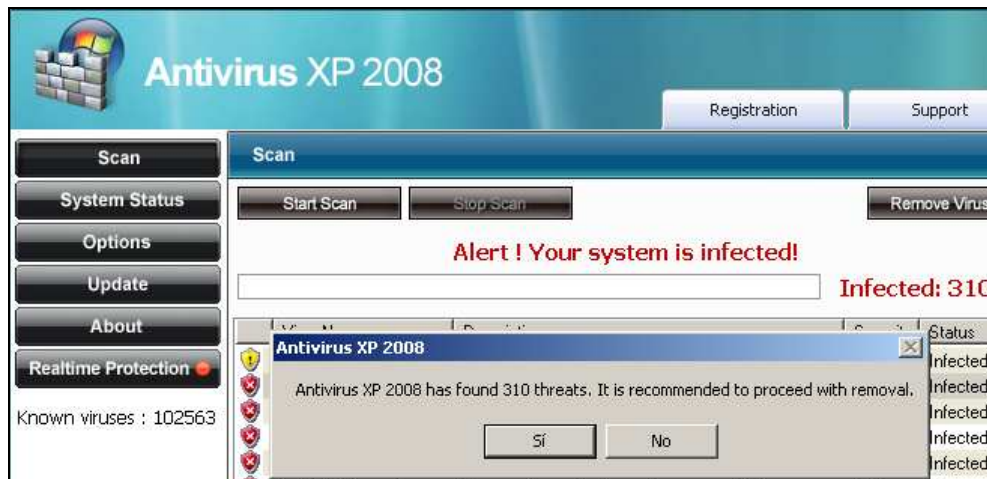


Imagen 7 - Falsa detección de malware

En el caso descrito, la amenaza es detectada por ESET NOD32 como *Win32/TrojanDownloader.FakeAlert* y los diferentes sitios web del programa son bloqueados al intentar ingresar a los mismos. Esta última opción evita que el usuario ingrese e instale por error el programa dañino.

Conclusiones

Los rogue, o falsas herramientas de seguridad, se han transformado rápidamente en los productos preferidos de los creadores de malware para engañar al usuario, ya que con el pretexto del “producto gratuito para limpiar el sistema”, el usuario prefiere probar estas herramientas en vez de descargar versiones de productos conocidos en el mercado y que incluso ofrecen soluciones en línea como ESET Online Scanner [5]. Por todo esto, es fundamental que el usuario esté informado y al momento de elegir una efectiva solución de seguridad, esta cuente con una protección antivirus en tiempo real verdadera y con capacidades proactivas que permitan detectar a través de la heurística este tipo de falsos programas y las variantes que aparecen día a día.

A fin de ilustrar de la mejor manera posible el funcionamiento de este rogue, ESET Latinoamérica desarrolló un Video Educativo [6] mostrando su forma de funcionamiento y lo que el usuario debe hacer para evitar la infección con el mismo.

Más información:

[1] Ingeniería Social

<http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social>

[2] ¿Centro de seguridad de Windows malicioso?

<http://blogs.eset-la.com/laboratorio/2008/06/27/centro-seguridad-windows-malicioso/>

[3] Evaluación gratuita de ESET NOD32 Antivirus

<http://www.eset-la.com/download>

[4] Drive-by-Download

<http://www.eset-la.com/threat-center/1792-drive-by-download-infeccion-web>

[5] ESET Online Scanner

<http://www.eset-la.com/online-scanner/>

[6] Vídeo Educativo sobre Rogue, falsos antivirus

<http://www.eset-la.com/threat-center/videos-educativos/1794-rogue-falsos-antivirus>

Plataforma Educativa de ESET Latinoamérica

<http://edu.eset-la.com>

Blog de Laboratorio de ESET Latinoamérica

<http://blogs.eset-la.com/laboratorio>