Rogue: Antivirus XP 2008

Autores: Subratam Biswas and Scott Wu

Traducción: Jorge Mieres de http://mipistus.blogspot.com/ en exclusiva para Segu-Info.

Recopilación: Lic. Cristian Borghello, CISSP

Fecha Publicación: 20 de noviembre de 2008

Este documento ha sido traducido del original:

"**Rogue Antivirus - A Closer Look at Win32/Antivirusxp**"

http://blogs.technet.com/mmpc/archive/2008/10/02/rogue-antivirus-a-closer-look-at-win32-antivirusxp.aspx

***Nota**: los malware se mencionan según los nombres otorgados por Microsoft y podrían ser detectados con nombre distinto según el Antivirus.*

Una mirada más cercana a Win32/AntivirusXP

Las falsas aplicaciones de seguridad (o **rogue**) han sido la causa de confusión y problemas para los usuarios desde hace algunos años. Estas aplicaciones suelen mostrar falsas advertencias sobre detecciones de códigos maliciosos con el fin de atraer a los usuarios a comprar la aplicación y, por ende, "desinfectar" el sistema.

Con el tiempo, los mecanismos utilizados para evitar la detección y distribuir estas aplicaciones se han vuelto más complejas: ofuscación de código es ahora común y las botnets son utilizadas para la distribución generalizada.

Win32/AntivirusXP (o Antivirus XP 2008) es una de esas aplicaciones y puede llegar a su máquina a través de múltiples canales, incluso, a través de spam que suplanta los principales servicios de noticias en línea (por ejemplo, el Top 10 de CNN y MSNBC).

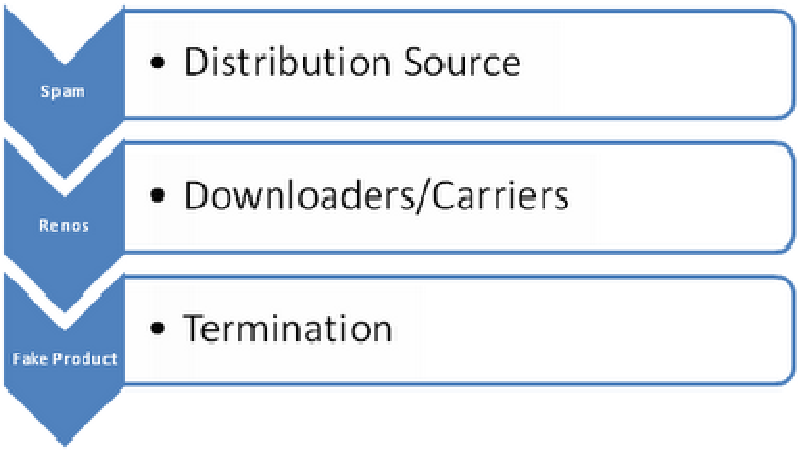

Figura 1. Cadena de infección A

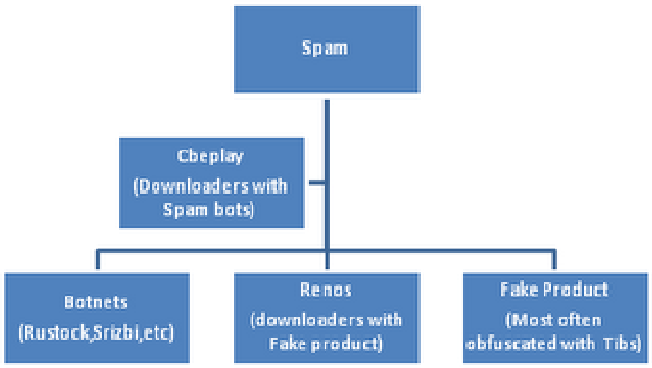

Figura 2. Cadena de infección B

Al igual que muchos otros programas de seguridad falsos, el rogue *AntivirusXP* puede ser descargado por *Win32/Renos*, directamente instalado desde el sitio web que distribuye el producto o sitios web de sus afiliados, o puede ser instalado engañando a los usuarios al hacer clic sobre los vínculos en correos spam.

La Figura **1** muestra un canal simplificado de infección donde, por ejemplo, un usuario recibe correo basura, hace clic en un vínculo incrustado en el spam y luego se infecta con *Win32/Renos*, que a su vez instala *Win32/AntivirusXP* en el sistema.

La Figura **2** muestra otro canal de infección, con otros componentes y complejidad. Tomando como ejemplo real los incidentes del Top 10 de CNN o MSNBC, los usuarios están expuestos, inicialmente, al troyano downloader *Win32/Cbeplay* a través de spam. *Win32/Cbeplay* baja un agente botnet (como *Win32/Rustock* o *Win32/Srizbi)* y variantes de *Win32/Renos*, que a su vez descargan *Win32/AntivirusXP*.

Esto aclara por qué en muchas situaciones en las que *Win32/AntivirusXP* se ha encontrado en un sistema, *Win32/Rustock* (o *Win32/Srizbi*) y *Win32/Renos* también estuvieron presentes. Generalmente, *Renos* se distribuye con la intención específica de mostrar falsas alertas y, a continuación, descargar aplicaciones de seguridad falsas. Los componentes de la cadena de infección de los resultados en la instalación de *Win32/AntivirusXP* son bastante íntegros y la relación entre *Win32/Renos* y *Win32/AntivirusXP* es simbiótica. A continuación son examinados.

Una vez que *Renos* infecta el sistema, pueden suceder una serie de cosas:

Después de una breve demora, el fondo del escritorio cambia para mostrar una imagen generada por *Renos*, esta imagen muestra un falso aviso.

Figura 3. Fondo de escritorio con alerta

Una copia del salvapantallas *Sysinternals BSOD* (*Blue Screen Of Death* - Pantalla Azul de la Muerte) a menudo es bajado al directorio del sistema y luego se activa como un salvapantallas.

En la carpeta Temp, se crean los archivos *tt1.tmp* o *tt2.tmp*.

Si hay una conexión activa a Internet, *Renos* intenta descargar e instalar el rogue *AntivirusXP*. No hay interacción con el usuario en esta cadena de infección. El archivo descargado por *Renos*, después de establecer la conexión con los dominios relacionados a *AntivirusXP*, es un archivo de imagen que contiene el instalador del rogue *AntivirusXP*.

El instalador se distribuye cifrado. Es descifrado por *Renos*, guardado en la carpeta *tmp* previamente creada, y luego ejecutado. El instalador está codificado de tal manera que sólo *Renos* es capaz de llevar a cabo el proceso inverso.

Una vez que el rogue *AntivirusXP* se encuentra en el sistema, ya sea a través de los canales de infección mencionados o instalado de forma manual, se crea una carpeta con un nombre aleatorio y baja a la misma el ejecutable principal también con un nombre aleatorio.

Asimismo, baja otro componente que es utilizado para mostrar las falsas alertas y promover la falsa aplicación como capaz de "eliminar" estas amenazas ficticias. Por último, se elimina el instalador del sistema.

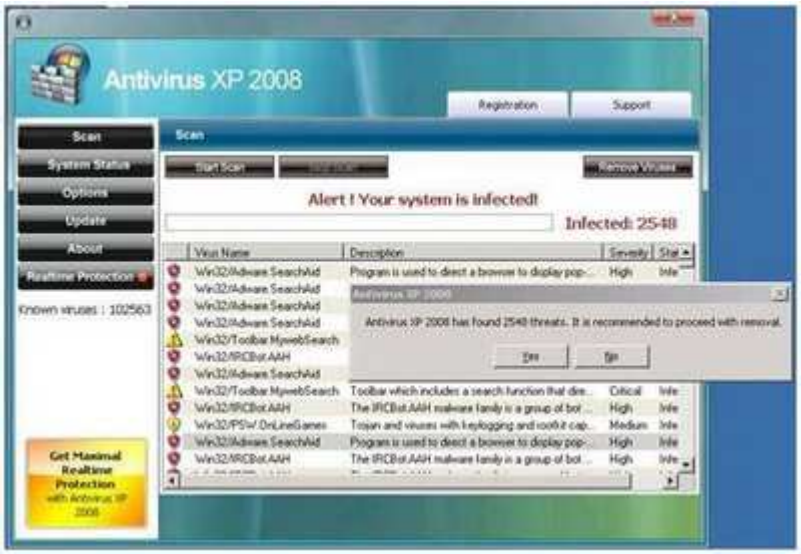

Figura 4. Captura de pantalla del rogue AntivirusXP

Cuando se habla de rogue, *Win32/Renos* tiene una larga historia en la descarga de falsos antivirus. Una variante de *Win32/Renos*, el *TrojanDownloader: Win32/Renos.gen! AQ*, llamó nuestra atención durante las últimas emisiones de MSRT; se lo consideró responsable de un gran volumen de instalaciones de *Win32/AntivirusXP*. Durante las dos primeras semanas de septiembre de la liberación de MSRT, 148.111 máquinas eran limpiadas por la particular infección de *Renos*.

Las falsas aplicaciones de seguridad siempre han sido buenas para confundir a los usuarios finales. *Win32/AntivirusXP* no es diferente en ese sentido, y con nombres tales como *Antivirus2008*, *XPAntivirus*, *Windows Antivirus*, *Antivirus 2008 XP*, la confusión es difícil de evitar.

En lugar de entrar en similitudes, es mejor buscar específicamente en *Win32/AntivirusXP* y buscar si hay algo fácilmente identificable y singular en su comportamiento. La mayoría de las falsas aplicaciones de seguridad, como ya se ha mencionado, pueden tener un menor número de dependencias de *Renos* u otros troyanos downloader similares.

Cuando se instala sin la intervención del usuario *Win32/AntivirusXP* depende de *Renos* para descifrar su instalador. Las siguientes dos características mostradas por *Win32/AntivirusXP* no son típicamente observadas en otros rogues:

- Creación aleatoria del nombre del archivo ejecutable y la carpeta principal.
- Auto-eliminación del instalador de *AntivirusXP*.

Los falsos programas antivirus han crecido significativamente en los últimos tiempos. Ellos generan confusión y falsas alertas de detección, a fin de convencer a los usuarios de adquirir el falso programa de seguridad - a partir del programa *Win32/AntivirusXP*: *Win32/Fakerednefed* y ahora *Win32/AntivirusXP*.

El rogue ha provocado un dramático trastorno tanto para los usuarios finales como para las empresas. Se sugiere encarecidamente implementar un producto antivirus completo para su negocio o computadoras personales. Como mínimo, si usted cree que su máquina se ve afectada por programas maliciosos o programas potencialmente no deseado, le recomendamos que ejecute libremente nuestro escáner en línea disponible en http://safety.live.com.

También puede obtener asistencia para la limpieza de virus a través de la ayuda y soporte técnico de Microsoft. Y si identifica un rogue que no es detectado, por favor envíenos una muestra a través de nuestro portal.

***Nota**: los malware se mencionan según los nombres otorgados por Microsoft y los podrían ser detectados con nombre distinto según el Antivirus.*

Para conocer más sobre Rogue es recomendable que ingrese a:

http://www.segu-info.com.ar/malware/rogue.htm