Problemas comunes ocasionados por malware

Autor: Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica
Fecha: 19 de Julio de 2009

ESET, LLC 610 West Ash Street, Suite 1900
phone: (619) 876 – 5400, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

Contenido

Introducción

Si bien existen herramientas de seguridad antivirus como ESET NOD32 [1] capaces de detectar códigos maliciosos conocidos y desconocidos (malware que no ha recibido identificación pero que ESET NOD32 detecta de forma proactiva) **[1]**, la realidad es que no existe una versión utópica de aplicaciones de seguridad que detecte el 100% de las amenazas.

Sin embargo, bajo ningún punto de vista se recomienda hacer caso omiso de la indicación de implementar una solución de seguridad antivirus, ya que a pesar de existir un mínimo margen de error que puede ser potenciado por la intervención del factor humano (los usuarios), su puesta en marcha es vital para mantener un nivel adecuado de prevención y no ser víctimas de actividades maliciosas similares a la expuesta.

Desde este enfoque, el presente documento intenta mostrar uno de los problemas más comunes y más peligrosos a los que se enfrentan los usuarios como consecuencia de acciones provocadas por códigos maliciosos, cuando no se atienden ciertos aspectos relacionados con las buenas prácticas que hacen a la prevención de potenciales infecciones **[2]**.

Se intenta explicar de manera didáctica las consecuencias provocadas por estas amenazas, y lo difícil que puede ser la tarea de erradicar el problema generado por el malware, para un usuario que ve comprometida la seguridad de su información.

[1] http://www.eset-la.com/download/

El problema y la primera impresión

Un contador público que trabajaba para una importante compañía de seguros y que utilizaba su propia PC (una laptop con sistema operativo Microsoft Windows XP SP2 Professional Edition) para llevar toda la parte contable relacionada con su tarea cotidiana, sospechó que había sido víctima de códigos maliciosos, debido a que aparentemente se habían deshabilitado varias funcionalidades del sistema operativo.

Ante esta situación, decidió pedir ayuda al departamento de IT ya que no podía realizar su trabajo cotidiano con normalidad debido a las insistentes ventanas emergentes (*pop-ups*) **[3]** que continuamente aparecían en el Escritorio del sistema alertando sobre problemas en el mismo.

La computadora poseía dos perfiles de usuario y en cada uno de ellos aparecían síntomas que indicaban alguna anomalía, siendo éstas las típicas consecuencias de infecciones provocadas por códigos maliciosos del tipo rogue **[4]**. El departamento técnico, al verificar si se encontraba algún programa antivirus instalado, estableció que, efectivamente, se encontraba implementado uno.

Como se puede apreciar, hasta esta instancia, sólo se contaba con la información transmitida por el contador. Según sus propias palabras, "*es casi imposible utilizar la computadora para realizar las tareas cotidianas*".

Contrariamente a lo que muchos usuarios puedan pensar, el recorrido expuesto aquí es real y constituye una grave problemática para un gran volumen de usuarios que día a día son víctimas de las actividades maliciosas cometidas por el malware, cuyos diseñadores persiguen fines económicos.

Accediendo al sistema operativo

Al acceder al primero de los perfiles de usuario del sistema (usuario A), se observaba en el Escritorio del mismo una serie de íconos de acceso directo característicos de los programas Adware/Spyware y troyanos del tipo *Dialer* **[5]**.

Este tipo de troyanos fueron diseñados para explotar conexiones Dial-Up (uno de los primeros sistemas de conexión vía módem a través de una línea telefónica) que con el advenimiento de otros tipos de conexiones más modernas no son frecuentes en la actualidad. Este malware se encarga de marcar un determinado número telefónico del extranjero de manera totalmente oculta al usuario y con el consecuente incremento sobre el costo del consumo de la línea telefónica.

Por otra parte, muchos de estos accesos directos suelen redireccionar al usuario a sitios web de juegos online o páginas pornográficas.

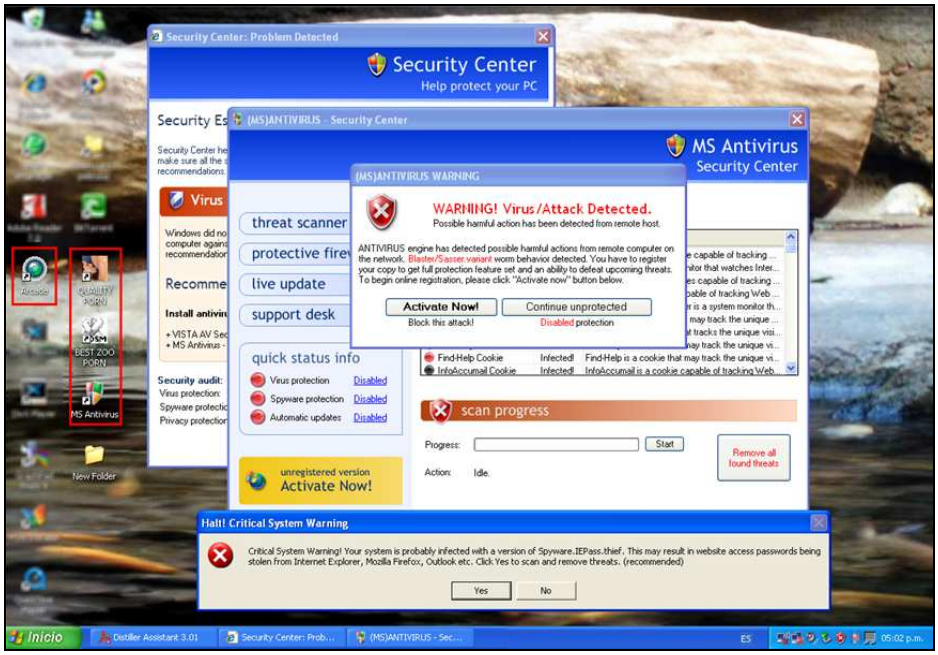

Imagen 1 - Perfil de usuario A

Inmediatamente después del inicio del sistema comienzan a desplegarse varias ventanas emergentes que muestran alertas sobre supuestos problemas de infección, lo que también se aprecia en la captura.

En este caso, las alarmas son generadas por un programa malicioso del tipo rogue detectado por ESET NOD32 bajo el nombre de *Win32/Adware.Antivirus2008*.

Al acceder al sistema bajo el perfil del segundo usuario (usuario B), se manifiestaba un panorama diferente al que poseía el usuario A. En este caso, el código malicioso había secuestrado el fondo de escritorio (*Desktop hijacking*), bloqueando la posibilidad de poder modificarlo.

También había modificado la información que se encuentra en el ángulo inferior derecho de la barra de tareas, agregando la leyenda *VIRUS ALERT!*, presentando el escritorio la siguiente apariencia:

Imagen 2 – Perfil de usuario B

Como se puede apreciar, en ambos casos y a simple vista, se pudo establecer que el sistema había sido víctima de más de un código malicioso.

Entre los principales síntomas que presentaba el equipo se encontraron:

- Inestabilidad del sistema y las aplicaciones
- Lentitud "inexplicable" en la conexión a Internet
- Cambios en las configuraciones del equipo
- Ventanas emergentes con información publicitaria, incluso cuando no se había establecido una conexión con Internet
- Ventanas *pop-up* con alertas de infección
- Lentitud no habitual en el arranque del sistema
- No estaba permitido desinstalar, reinstalar o ejecutar aplicaciones de seguridad
- No se permitía el inicio en Modo a Prueba de Errores

Hasta esta instancia, sólo se tenía una visión global del problema. Sin embargo, es necesario aclarar que lo expuesto en este documento representa una situación real y muy habitual en los equipos de muchos usuarios donde, una vez que han sido víctimas del malware, el sistema se transforma en un verdadero alojamiento de programas indeseables.

Abordando el problema

En consecuencia, se procedió a planificar una estrategia para abordar el problema de manera manual ya que el/los códigos maliciosos (que, en esta instancia, todavía se desconocía para qué estaban concebidos) habían bloqueado toda posibilidad de exploración y monitoreo por parte de las aplicaciones de seguridad instaladas.

Se intentó encontrar procesos sospechosos **[6]** que estuviesen corriendo de forma activa, presionando la combinación de teclas correspondiente para acceder al Administrador de Tareas de Windows (*Ctrl +Alt + Supr*). En ese momento una pequeña ventana informó que el Administrador de Tareas también había sido deshabilitado. La misma situación se presentó cuando se intentó acceder al Registro del sistema.

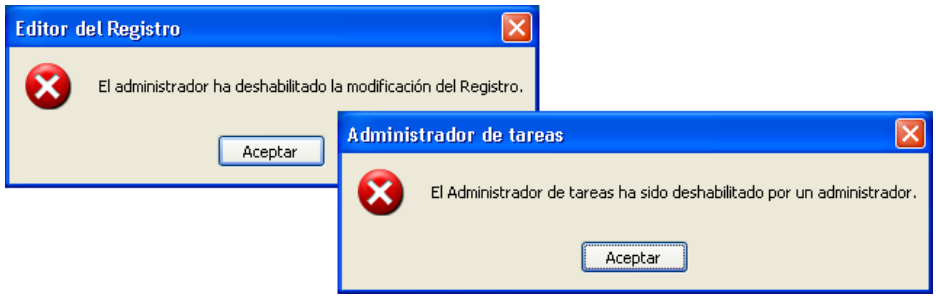

Imagen 3 – Bloqueo del Registro y Administrador de Tareas

Por otro lado, al hacer doble clic sobre el ícono de "Mi PC" no se veían los accesos a las diferentes unidades. Tanto el disco C: como la unidad D: estaban ocultos por lo que tampoco era posible acceder a ellos de manera convencional.

Estas estrategias empleadas por el malware actual buscan entorpecer la detección y análisis del mismo por parte de los especialistas, y aumentar así su ciclo de vida.

Ante la imposibilidad de tener acceso a determinados sectores del sistema, se comenzó a utilizar algunas herramientas que ayudarían a verificar los problemas que sufre el equipo. Es importante destacar que algunas de ellas también pueden ser bloqueadas por el malware y su uso dependía del tipo de aplicación dañina ya instalada, porque en este momento, este software malicioso mantenía el control del sistema.

En primera instancia, se intentó visualizar los procesos **[7, 8, 9]** para establecer cuál o cuáles de ellos podían ser los causantes de los problemas, utilizando la aplicación ProcessExplorer [2] de Microsoft.

Se estableció que existían varios procesos ejecutándose en memoria bajo el nombre "*YUR*" seguido de un número o una letra asignado a cada uno, aparentemente de manera aleatoria.

Verificado este aspecto, se intentó acceder al registro del sistema operativo en busca de alguna clave "anormal"; y, del mismo modo que en el caso anterior, se recurrió a un programa, en este caso, llamado Autoruns[3], también de Microsoft.

Se observó que cierto malware (aún no se sabía cuál) había manipulado el registro agregando varias claves que hacían referencia a los procesos activos antes mencionados **[10]**; todos ellos, alojados en la carpeta *system32* del sistema.

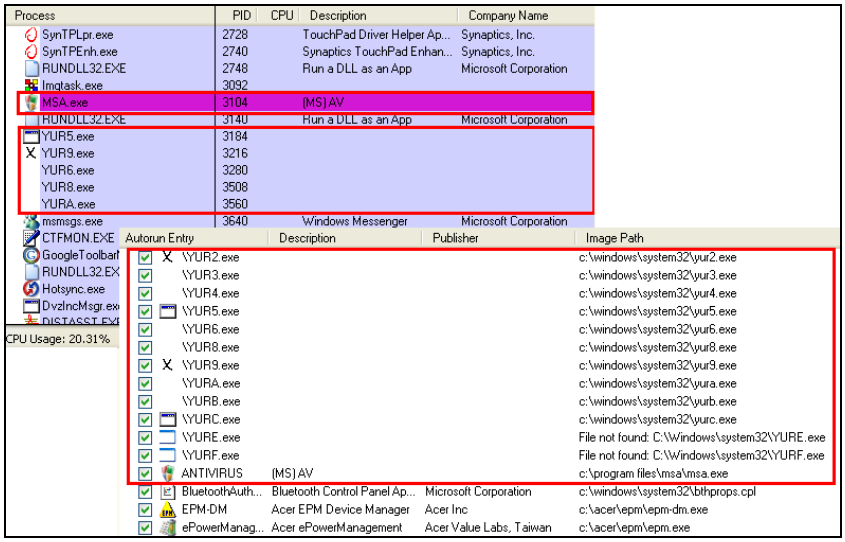

Imagen 4 – Visualización de los procesos y claves del registro

Se determinó, en consecuencia, que el/los códigos maliciosos no solamente habían deshabilitado el acceso al registro del sistema operativo de forma convencional, sino que también lo habían manipulado.

[2] http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

[3] http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx

De esta forma, el código malicioso intentó garantizar que el proceso malicioso se ejecutara en cada inicio del equipo.

Viendo más allá de lo habitual

Sin embargo, todavía quedaban aspectos que se debían dilucidar para lograr la instalación de una solución de seguridad antivirus, que permitiese realizar una exploración profunda, ya que los códigos maliciosos habían bloqueado el antivirus instalado e impedían la eventual reinstalación o implementación de uno nuevo.

En consecuencia, se ejecutó la herramienta de diagnóstico gratuita desarrollada por ESET llamada ESET SysInspector **[11]**, para tratar de obtener más información sobre las actividades que realizaban los códigos maliciosos.

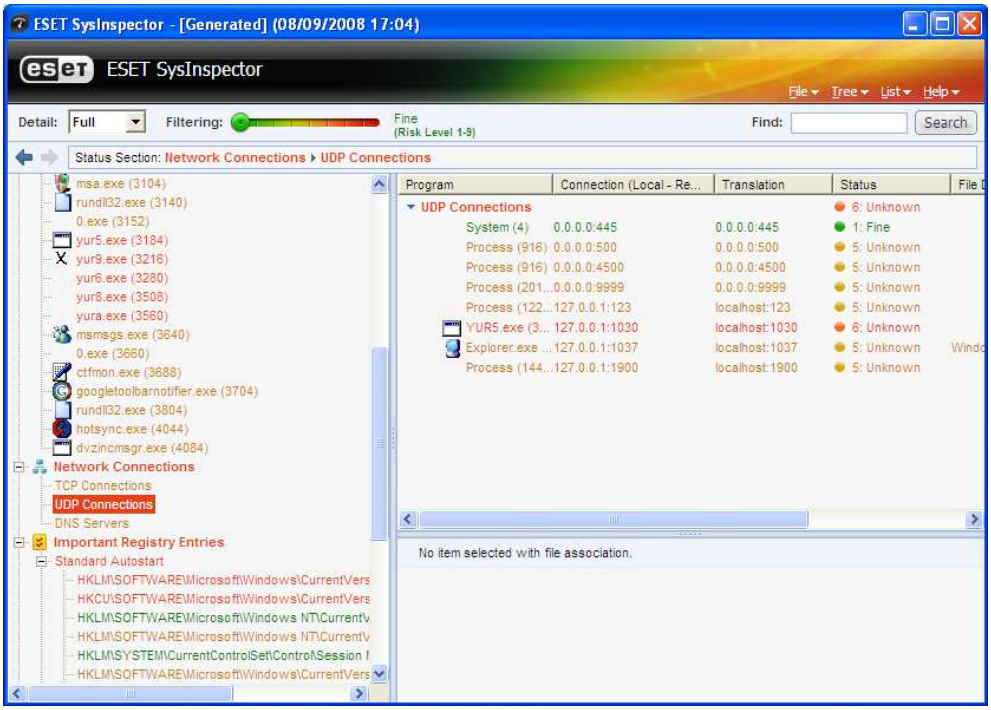

Imagen 5 – ESET SysInspector

Esta herramienta provee información muy útil y detallada relacionada no sólo con los procesos activos y las modificaciones llevadas a cabo en el registro, sino con aspectos relativos a los archivos críticos del sistema (*win.ini*, *system.ini* y *hosts*), conexiones establecidas a través de los protocolos TCP [4] (*Transmission Control Protocol*, en español Protocolo de Control de Transmisión) y UDP [5] (*User Datagram Protocol*, en español Protocolo de Datagrama de Usuario), y diferentes servicios, entre otros componentes del sistema.

Una característica interesante de esta aplicación es que no permite realizar modificación alguna sobre la información que muestra. Es decir, sólo permite ver los datos sin manipularlos, tomando una "fotografía" del estado actual del sistema.

En este caso permitió verificar que uno de los archivos ejecutables (*YURS.exe*), que se estaba ejecutando en memoria, intentaba establecer una comunicación hacia Internet a través del protocolo UDP.

A partir de ese análisis se conoció un mayor caudal de información sobre las actividades del malware, y quedó pendiente, por el momento, establecer otras actividades de los códigos maliciosos, cuyas identidades todavía se desconocían.

Identificando lo desconocido

Luego de identificar y obtener los archivos dañinos para su análisis, de detener los procesos asociados y de restablecer algunas de las funcionalidades básicas deshabilitadas por el malware, la performance del sistema aumentó considerablemente y, a continuación, se debía proceder a la instalación de ESET NOD32 Antivirus para realizar una exploración profunda del sistema. El resultado fue que éste se encontraba infectado con los siguientes códigos maliciosos:

- *Win32/Spy.Webmoner.NAW*: un troyano diseñado para robar información **[12]** relacionada con el servicio WebMoney que permite realizar transacciones monetarias en línea.
- *Win32/AutoRun.XH*: este gusano se disemina a través de recursos compartidos del equipo y dispositivos que se conecten al puerto USB **[13, 14, 15]**.
- *Win32/AutoRun.YP*: otro gusano cuyos objetivos son similares al anterior.
- *Win32/Adware.Antivirus2008*: un código malicioso que se propaga simulando ser un programa de seguridad antivirus, desplegando falsas alertas sobre supuestas infecciones en el sistema víctima **[16]**.

[4] http://es.wikipedia.org/wiki/Transmission_Control_Protocol
[5] http://es.wikipedia.org/wiki/UDP

- *Win32/Adware*.Virtumonde: un adware que se encarga, entre otras cosas, de robar información confidencial de los usuarios **[17]**.
- *Win32/TrojanDownloader.Delf.OGZ*: este troyano downloader **[5]** está diseñado para descargar otros códigos maliciosos una vez que ha comprometido el sistema.

En definitiva, se podría describir a este equipo como "un cóctel de códigos maliciosos" que gracias a la implementación oportuna de una estrategia de análisis llevada a cabo de manera "artesanal", pudo ser rescatado sin perder la información alojada en el equipo.

Cabe mencionar nuevamente que este breve procedimiento no reemplaza la acción preventiva de las soluciones de seguridad antivirus que, en todo caso, protegerán al usuario ante la mayoría de las aplicaciones dañinas; y sí revela que ante determinados problemas relacionados con el malware, la solución no recae en el formateo del sistema.

Conclusión

Muchos códigos maliciosos de la actualidad se han diseñado para robar información privada de los usuarios, que luego podrá ser utilizada en acciones delictivas como estafas y otras actividades ilícitas de índole financiera.

Lamentablemente este aspecto presentado por el malware ha ido en un constante crecimiento que se manifiesta a través del importante aumento de la actividad de desarrolladores maliciosos, que han convertido todo esto en un negocio clandestino donde la pieza esencial es el malware.

El usuario queda a merced de variados tipos de amenazas, con el enorme riesgo para la seguridad que representan situaciones como éstas, además de generar una mala experiencia debido a los síntomas desagradables que provocan en el sistema víctima.

El recorrido detallado en este artículo representa una situación frecuente en algunos equipos. Para evitar que un usuario sea víctima de la misma se requiere la implementación de una solución de seguridad antivirus proactiva, que permita prevenir y bloquear las acciones maliciosas del malware actual.

Más información

Plataforma Educativa de ESET Latinoamérica
http://edu.eset-la.com

Blog del Laboratorio de ESET Latinoamérica
http://blogs.eset-la.com/laboratorio

Referencias

[1] Análisis Heurístico: detectando malware desconocido
http://www.eset-la.com/threat-center/1625-analisis-heuristico-detectando-malware-desconocido
[2] Buenas prácticas en seguridad informática
http://www.eset-la.com/threat-center/2175-buenas-practicas-seguridad-informatica
[3] Adware, la fábrica de pop-pups
http://blogs.eset-la.com/laboratorio/2008/02/22/adware-fabrica-pop-pups/
[4] Rogue: falsos antivirus gratis
http://www.eset-la.com/threat-center/1793-rogue-falsos-antivirus-gratis
[5] Tipos de troyanos
http://blogs.eset-la.com/laboratorio/2008/04/08/tipos-troyano/
[6] Identificando procesos maliciosos en sistemas Windows
http://blogs.eset-la.com/laboratorio/2007/10/25/identificando-procesos-maliciosos-windows/
[7] Procesos legítimos y nativos del sistema operativo III
http://blogs.eset-la.com/laboratorio/2009/06/03/procesos-legitimos-nativos-del-sistema-operativo-iii/
[8] Procesos legítimos y nativos del sistema operativo II
http://blogs.eset-la.com/laboratorio/2009/05/18/procesos-legitimos-nativos-sistema-operativo-ii/
[9] Procesos legítimos y nativos del sistema operativo I
http://blogs.eset-la.com/laboratorio/2009/05/07/procesos-legitimos-nativos-sistema-operativo-i/
[10] Cuando quedan rastros del malware
http://blogs.eset-la.com/laboratorio/2007/10/08/cuando-quedan-rastros-del-malware/
[11] ESET SysInspector
http://blogs.eset-la.com/laboratorio/2008/01/16/eset-sysinspector/
[12] Robo de información personal online
http://www.eset-la.com/threat-center/1774-robo-informacion-personal-online
[13] Bloqueo del puerto USB con ESET NOD32
http://blogs.eset-la.com/laboratorio/2009/04/16/bloqueo-puertos-usb-eset-nod32/
[14] Propagación de malware a través de dispositivos USB

http://www.eset-la.com/threat-center/1705-propagacion-malware-usb
[15] Video Educativo. Malware en Dispositivos USB
http://www.eset-la.com/threat-center/videos-educativos/1720-malware-dispositivos-usb
[16] Video educativo. Rogue: falsos antivirus
http://www.eset-la.com/threat-center/videos-educativos/1794-rogue-falsos-antivirus
[17] Virtumonde: Crónica de una muerte anunciada
http://www.eset-la.com/threat-center/1674-analisis-tecnico-eset-virtumonde