

El ataque de los clones (falsos antivirus)

Autor: Raúl Batista

Edición y Corrección: Lic. Cristian Borghello, CISSP

Fecha Publicación: 22 de agosto de 2009

Publicado en [Segu-Info](http://www.segu-info.com.ar)

Introducción

La (in)seguridad Web sigue dando material para mantenerse actualizados y atentos de los peligros que existen en el uso de Internet.

Esta historia tiene varias partes interesantes, primero se describe un resumen de lo sucedido y luego se irá por partes, analizando los aspectos que llaman la atención de este método de infección utilizado por los delincuentes.

Todo comienza al abrir el navegador (1) para realizar una búsqueda en Internet con instrucciones para un compañero de trabajo. Entonces busqué estas frase: **install SATA "Windows XP"**

El buscador(2) arrojó los resultados y el tercero de ellos, que comenzaba con "How to install .." (Como instalar...), me resultó interesante. Abrí en una nueva pestaña ese resultado, y en ese sitio (3) encontré varios artículos sobre el tema buscado, encontrando las instrucciones que deseaba.

Pero, al cerrar ventanas, me encontré que de fondo había quedado dos ventanas, que no habían sido abiertas por mí, y un cuadro dialogo (en inglés) esperaba mi confirmación (imagen1):



Imagen 1

Gracias a todo lo aprendido sobre estos temas, pude sospechar que me enfrentaba al resultado provocado por alguno de los sitios (¿malicioso? quizás no) que abrí en mi búsqueda. Pero habiéndolas ya cerrado no sabía cuál lo causó. Tome nota mental de investigar eso después. Ahora quería ver de qué se trataba esto.

Al pasar el mouse por una de las dos ventanitas, apareció una nueva ventana (4) con una espléndida animación de un supuesto análisis de malware:

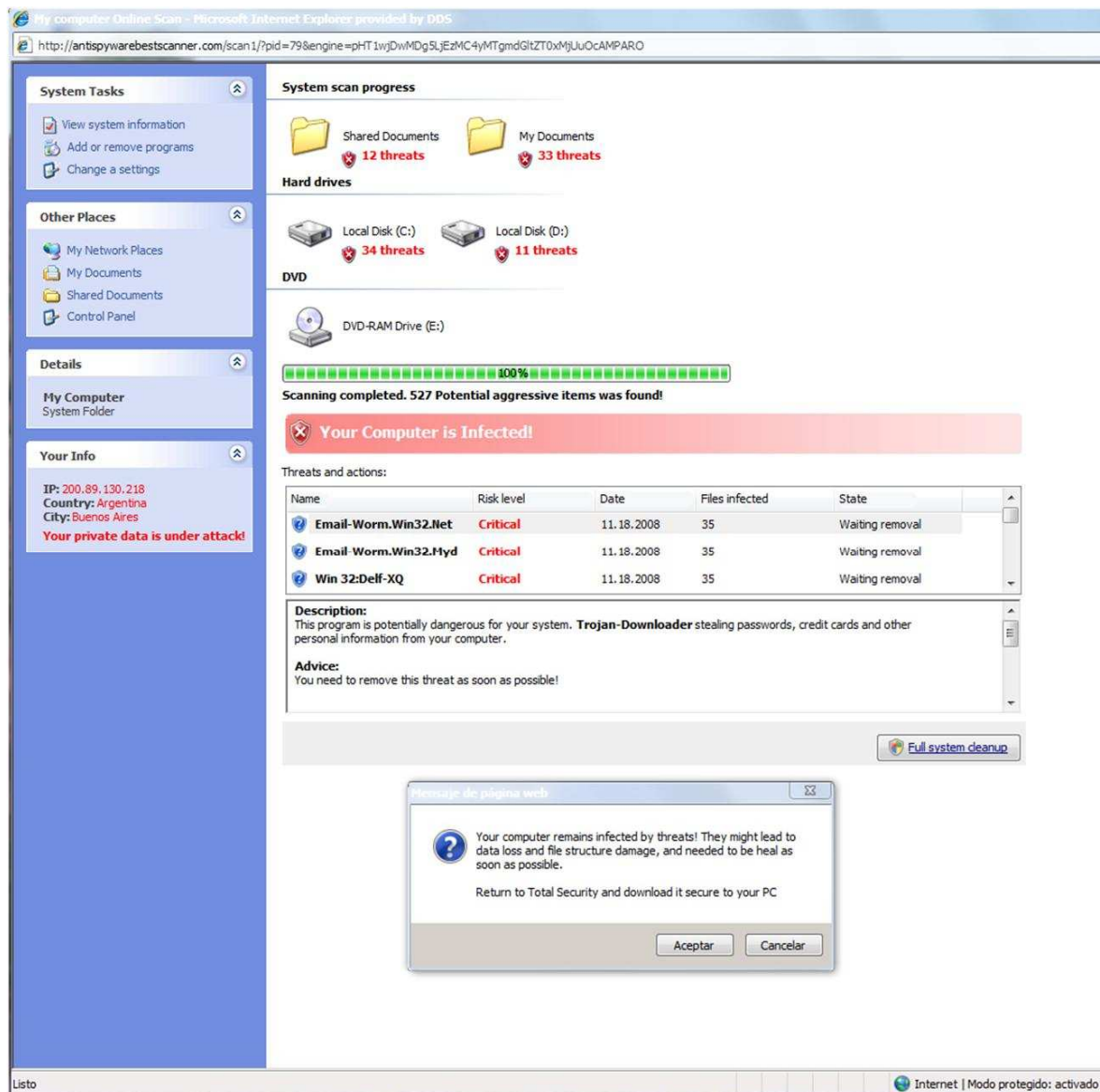


Imagen 2

La barrita verde fue avanzando, increíble, y dando como resultado que la PC estaba infectada, muy infectada, con decenas y centenas de amenazas.

Decidí que era suficiente y no iba a arriesgar más, pulse la "X" para cerrar la ventana y apareció un cuadro con el resumen de las amenazas encontradas, del cual ni quise saber más.

En realidad ese cuadro era una imagen y nada de lo que dice por supuesto es cierto:



Imagen 3

Nuevamente intenté clic en la "X" para cerrarlo pero, ahora mi navegador fue directo a la descarga de un archivo y, el sistema de escaneo de descargas de tres motores AV no detectó nada:



Imagen 4

Y para ver de qué se trataba elegí la opción de grabar el archivo (jamás abriría un EXE en estas condiciones).

Luego con el archivo ya descargado y cuidando de no ejecutarlo lo hice examinar por 5 sitios de "Servicio de análisis de archivos sospechosos" (5):

- <http://www.filterbit.com/>

- <http://scanner.virus.org/>
- <http://virusscan.jotti.org/es/>
- <http://www.virscan.org/>
- <http://www.virustotal.com/>

Solo él último sitio detectó algo. Como era de esperar el servicio que usa mayor cantidad de motores AV logro detectar, con uno sólo de los 41 motores, que tenía en mis manos un archivo sospechoso. Ningún otro sitio detectó nada extraño. Como tampoco los tres motores de AV que controlan las descargas Web en la red ni el AV de la propia PC (!).

Esto demuestra lo bien que trabajan los creadores de malware y cómo perfeccionan sus creaciones para evitar los AV. En cambio, un día después el archivo ya es detectado por varios motores AV.

Finalmente repitiendo la búsqueda encontré cual sitio de mi búsqueda fue el que generó todo esto.

Puntos de Análisis

- (1) Navegador: El utilizado fue **IE8**. Al repetir abrir el mismo sitio maliciosos con **Firefox 3.x** equipado con 'NoScript' y 'WOT' el sitio malicioso no generó ninguna de las acciones descriptas. Las cuales fueron provocadas por script maliciosos. Ver (4)
- (2) Buscador: El utilizado fue **Bing**. Al repetir con **Google** la misma búsqueda, no apareció, al menos entre los primeros 100 resultados, el sitio malicioso que **Bing** arrojó en 3er lugar para nuestra búsqueda. Repitiendo por segunda vez en Google pero indicándole que incluya el dominio de la página maliciosa, se verifica que no es informado como sitio dañino por SafeSearch de Google.
- (3) El sitio malicioso ubicado en 3er lugar por Bing resulta ser un sitio operado por atacantes. Promocionan vía técnicas [de Black Hat SEO](#) y llegan a posicionar bien búsquedas normales como la descripta. Lo mismo puede ocurrir con cualquier buscador.
- (4) La ventana del “escaneo” simulado y falsa detección:
 1. Ese diseño es de Win XP en ingles, pero la PC tenía Windows 7 en español .
 2. La barra de **dirección URL** arriba y de **estado** abajo son de **navegador Web** no de **Explorador de Windows**
 3. La PC no tiene disco D: ni unidad DVD en el E:
 4. Nunca se aceptó instalar ni correr ningún test, lo hizo sólo (mediante scripts maliciosos en Javascript)

- (5) Los scripts encontrados en la página maliciosa obtenida en la búsqueda se ven al comienzo del siguiente código HTML:

```
Fuente de: http://www...n/srch-syt4c1tv5i.html - Mozilla Firefox
Archivo Editar Ver Ayuda

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>How To Install Sata Harddrive Windows XP | XPdeveloper.com</title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<script language="JavaScript" type="text/javascript">var key='How To Install Sata
<script type="text/javascript" src="/eplkjhufyjjdmcmv/feed.js"></script>
<script type="text/javascript" src="/olmjtphaycbq/bfjo.js"></script>
</head>

<body bgcolor="#000000" text="#000000" link="#0000CC" vlink="#0000CC" alink="#0066
<div align="center">
  <table width="900" border="0" cellpadding="0" cellspacing="0" bgcolor="#FFFFFF">
    <tr>
```

Al descargar estos scripts se puede observar una función ofuscada, usada genéricamente por algunas botnet. El HTML y JS se generan automáticamente con estas rutinas ocultando las URL finales, desde donde se descarga el archivo ejecutable que finalmente había obtenido.

Aquí puede observarse el 1er script desofuscado:

<http://wepawet.iseclab.org/view.php?hash=26d2a13e4b9f8914542d80b4b85f2cf5&type=js>

Y, aquí puede observarse el 2do script desofuscado:

<http://wepawet.iseclab.org/view.php?hash=c032cdd8499219ee6ae315bfe8fbe7a6&type=js>

Al final de este se puede ver una URL que termina redireccionando al sitio que simula el scaneo y que luego descarga el EXE.

Además estas URL verifican que el usuario esté ingresando por primera vez. Cuando se detecta un ingreso desde la misma dirección IP más de una vez, el PHP destino no hace nada, para evitar el rastreo por parte de los analistas.

Algunas Conclusiones:

Aún las mejores herramientas de detección antimalware no son suficientes. En este caso fallaron en detectar el malware todos los AV donde está funcionando la PC, las detecciones de los buscadores y casi todos los servicios de análisis de archivos sospechosos.

Entonces sigue siendo necesario como vimos en este caso:

- Tener precaución en la navegación Internet. Y no confiar ciegamente en las protecciones antimalware
- Estar informados actualizados de las técnicas de ataques más comunes
- Aprender a cancelar procesos o ventanas emergentes sospechosos
- Agregar complementos de protección de la navegación como los descriptos NoScript y WOT y aprender a usarlos
- Los atacantes continúan haciendo un trabajo exitoso. No se puede bajar la guardia
- El resultado de haber creído en la supuesta detección de malware hubiera derivado en instalar una **herramienta falsa** de seguridad y pagar por la limpieza de un malware inexistente, aumentando la recaudación de los estafadores.