



MalwareIntelligence

Actividades delictivas desde AS6851 [SAGADE]

Parte uno
91.188.59.9 / 91.188.59.249



Contenido

Introducción, 4

91.188.59.9, 5

91.188.59.10

91.188.59.15

91.188.59.16

91.188.59.17, 6

91.188.59.18

91.188.59.19

91.188.59.21

91.188.59.25, 7

91.188.59.26

91.188.59.27

91.188.59.50, 8

91.188.59.51

91.188.59.52, 9

91.188.59.69

91.188.59.70

91.188.59.71

91.188.59.72, 10

91.188.59.73

91.188.59.74, 11

91.188.59.84

91.188.59.92, 12

91.188.59.93

91.188.59.94

91.188.59.95

91.188.59.98

91.188.59.112, 13

91.188.59.125

91.188.59.139, 14

91.188.59.140

91.188.59.149

91.188.59.197, 15
91.188.59.199
91.188.59.205

91.188.59.211, 16
91.188.59.225
91.188.59.230

91.188.59.231, 17
91.188.59.232
91.188.59.234
91.188.59.235
91.188.59.226
91.188.59.237
91.188.59.238
91.188.59.239
91.188.59.240
91.188.59.241
91.188.59.242
91.188.59.243
91.188.59.249

Conclusión, 18

Sobre MalwareIntelligence, 19

IMPORTANTE: Este documento fue levemente modificado en los párrafos 1, 2 y 3 de la Introducción; y 1 de la conclusión; eliminando la nomenclatura del ISP donde se aloja/ba SAGADE bajo el AS que se menciona en el informe.

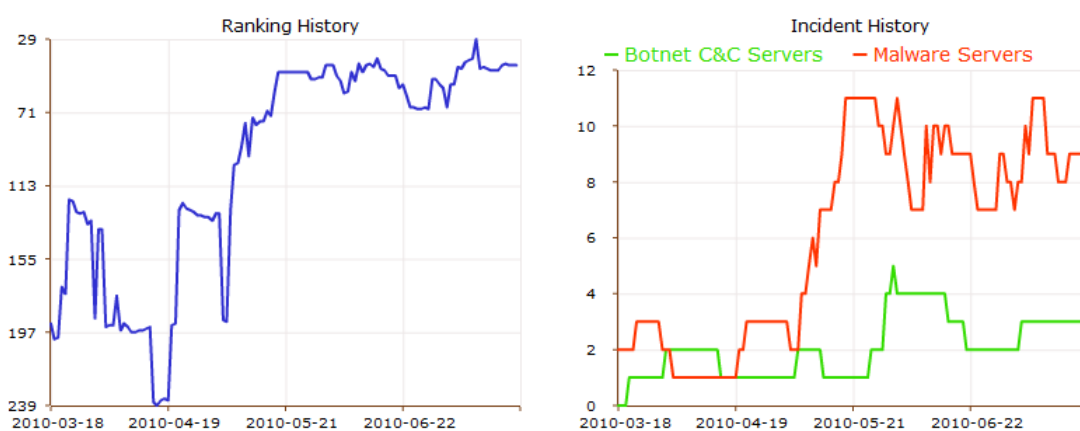
Asimismo, **MalwareIntelligence** no se hace responsable por las interpretaciones erróneas que algunos lectores o medio de información pueden hacer o dar respecto al contenido de este y de cualquier otro documento expuesto en el sitio web bajo cualquier formato.



Introducción

SAGADE, es el nombre que recibe el cliente de un importante ISP de Letonia, cuyo **AS** (**A**utonomous **S**ystem) está designado bajo numeración **6851**. Actualmente, este AS constituye uno de los recursos más activos del crimeware mediante el cual se distribuyen cotidianamente una importante cantidad de códigos maliciosos, además de ser la base de control para el alojamiento de varios C&C que retroalimentan la economía clandestina.

Según algunas fuentes consultadas, este ASN está catalogado como servidor de actividades delictivas variadas que van desde la propagación de diferentes familias de rogue, alojamiento de crimeware como [YES Exploit System](#), durante el 2009 alojó las estrategias de la botnet [Waledac](#) (sucesora de Storm), también a [Zeus](#) y hasta posee relación directa con los delincuentes que se encuentran detrás de las maniobras de la botnet [Koobface](#).



Historial del AS 6851

Tendencia ascendente de las actividades delictivas con base en este AS durante el segundo trimestre de 2010

Actualmente, la mayoría de los códigos maliciosos que se propagan a través de los recursos soportados desde el AS en cuestión y, particularmente por intermedio de SAGADE, responsable de la maniobra que da soporte a la gestión de sistemas de afiliados destinados, precisamente, a incrementar las ganancias de los delincuentes por intermedio del éxito de las infecciones logradas.

A continuación se deja en evidencia las actividades del **AS6851** en el rango de direcciones IP's aglomeradas entre 91.188.59.9 y 91.188.59.249, a la fecha 14 de Agosto de 2010 (en rojo el historial), que responden a maniobras maliciosas.

Versión en inglés

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

Versión en español

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

91.188.59.9

Contiene un **TDS** (Traffic Direction Script) llamado **SUTRA** en <http://91.188.59.9/admin/center.cgi>

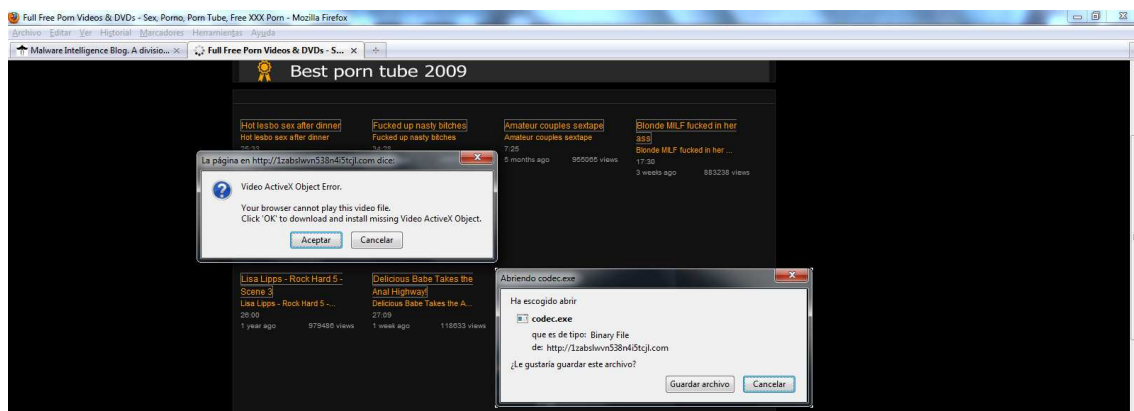
91.188.59.10

Resuelve los dominios **1zabslwvn538n4i5tcjl.com** y **urodinam.net** bajo el sistema **Nginx/0.7.65**. El dominio **urodinam.net** presento actividad en octubre de 2009 bajo la IP **200.63.44.48 (AS27716)**.

Mientras que **1zabslwvn538n4i5tcjl.com** está activo desde marzo de 2010 y aloja **YES Exploit System** (1zabslwvn538n4i5tcjl.com/temp/admin/index.php) con los siguientes códigos maliciosos:

- [18.pdf](#) (b832676595b7d1ef8a1b3a4d6277c32a) **Adobe util.printf** - [CVE-2008-2992](#)
- [wsc.exe](#) (80427b754b11de653758dd5e1ba3de1c) **Koobface**
- [file.exe](#) (5910e59d592781cec3234abf57f8d000) **Koobface**
- [dm.exe](#) (b658d9b812454e99b2915ab2e9594b94) **TDSS**

Además aloja una página pornográfica (1zabslwvn538n4i5tcjl.com/tube) desde la cual se descarga una copia de **Koobface** a través de ingeniería social visual. La página contiene embebido un script haciendo referencia a la descargar del archivo **18.pdf**.



Propagación de Koobface

Ejemplo que muestra una de las últimas campañas de propagación de Koobface. En este caso, a través de una página pornográfica

Más información sobre **91.188.59.10** y **Koobface** en:

<http://malwareint.blogspot.com/2010/07/circuit-koobface-from-911885910-bkcnnet.html>

91.188.59.15

Actualmente resuelve los dominios **mcml1.com** y **trol010.com**. Sin embargo, en marzo/abril de 2010 presento actividad maliciosa bajo los dominios **forca.in**, **oves.in**, **likinto.com**, **fottie.com** e **issto.com** alojando una copia de **NeoSploit**.

91.188.59.16

Resuelve a **kaksy.in** Durante abril de 2010 la IP resolvía a **img.k0n.in** y **1165802610.zalip.net**, y había una copia de **NeoSploit**. Del primer dominio se descargaba un PDF con exploit (9e672ded5f7207e2ded17c607081224d) para [CVE-2009-1492](#).

91.188.59.17

Presento actividad maliciosa durante abril de 2010 resolviendo a los dominios **images.0lis.in** y **movie.c1umb.in**. Tenía una versión de **NeoSploit**.

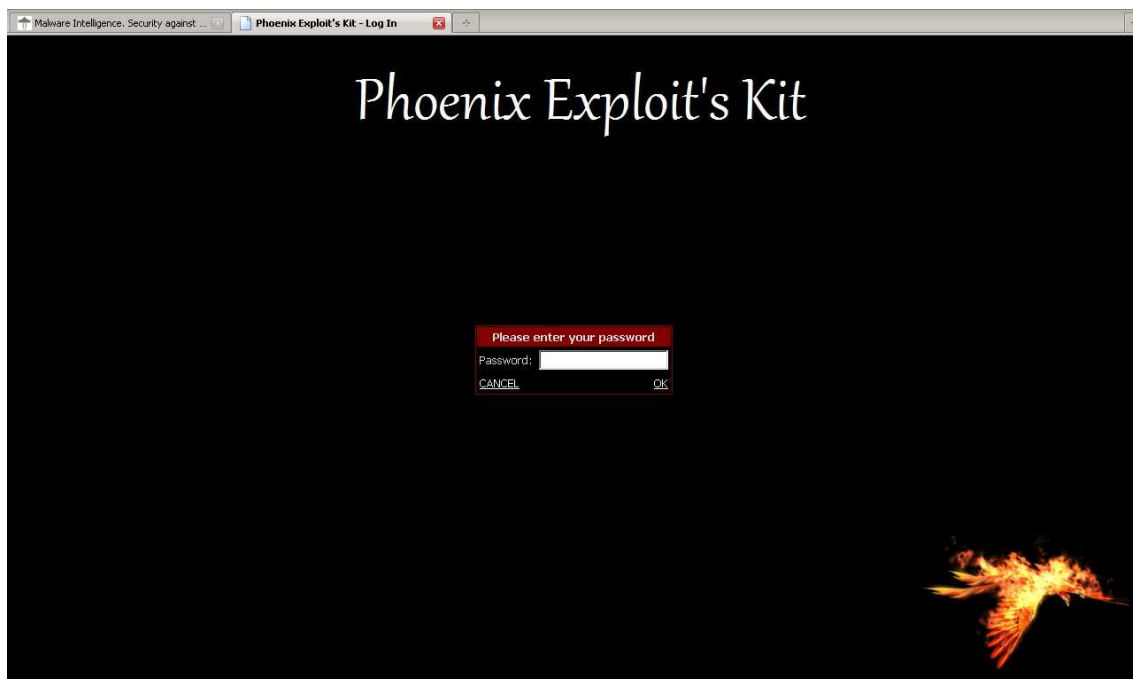
91.188.59.18

En abril de 2010 resolvía al dominio **sun.akkei.com**, alojando una versión de **NeoSploit**. Hoy resuelve a **video.k0x.in**.

91.188.59.19

Alojó una copia de **Phoenix Exploit's Kit**, resolviendo al dominio **utry.in**, desde el cual descargaba el siguiente binario ejecutable. Dejó de resolver estas actividades durante la primera semana de Agosto de 2010.

- [exe.exe \(f36dd53834bcd0997dbbf50f54617941\)](#) **Vundo**



Pantalla de acceso a Phoenix Exploit's Kit

El proceso de autenticación se compone de un solo factor: la contraseña, que se encuentra codificada bajo el algoritmo SHA1

*Más información sobre **Phoenix Exploit's Kit** en:*

- <http://malwareint.blogspot.com/2010/08/campaign-infection-through-phoenix.html>
- <http://malwaredisasters.blogspot.com/2010/08/phoenix-exploits-kit-and-pay-per.html>
- <http://www.malwareint.com/docs/pek-analysis-es.pdf>

91.188.59.21

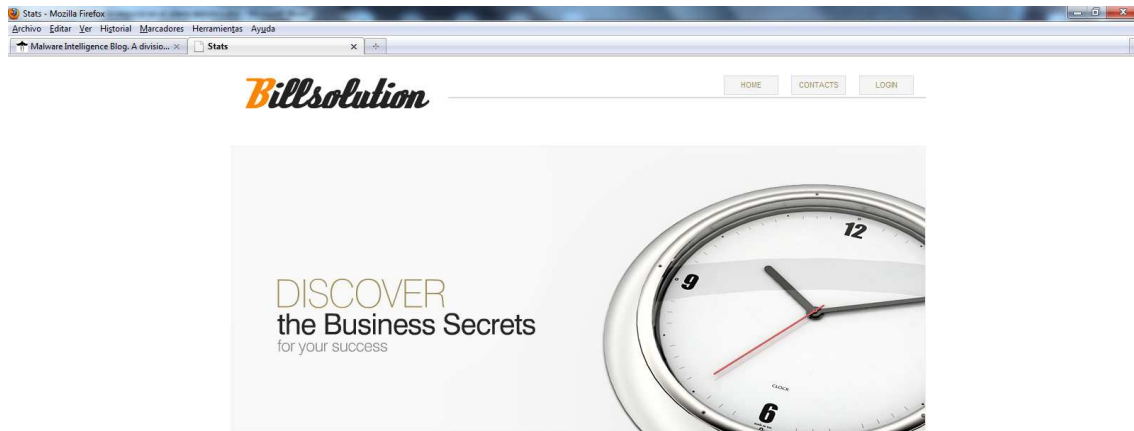
En abril de 2010 alojo el **C&C de Oficla botnet**. Redireccionaba el tráfico hacia el dominio **On0.in** desde donde se intentaba explotar la vulnerabilidad [CVE-2006-0003](#) y de descargaba una copia de Oficla (7a2b3ee45c557ab7a5f0f114860f642a), también conocido como **Sasfis**.

*Más información sobre **Oficla Botnet** en:*

- <http://www.malwareint.com/docs/myloader-oficla-analysis-es.pdf>
- <http://malwareint.blogspot.com/2010/03/oficla-botnet-with-more-than-200000.html>

91.188.59.25

Resuelve los dominios **billsolutions.net** y **fastsecurebilling.com**. **BillSolution** es un sistema de afiliados para la distribución de rogue, cuyo panel de control se encuentra en <http://91.188.59.25/state/index.php>.



BillSolution

Se trata en realidad de un programa de afiliados mediante el cual se propaga rogue, bajo la modalidad de pago Pay-per-Install

91.188.59.26-27

La primera IP resuelve el dominio **fastsecurebilling.com**, sin actividad en este momento. Sin embargo, durante abril de 2010 se registro actividad maliciosa desde **main.php?land=20&affid=12400**, descargando un security rogue.

La segunda resuelve el dominio fast-payments.com.

En http://fast-payments.com/index.php?prodid=antus_02_01&afid=%20 redirige a una pagina para la compra de un security rogue llamado **Antivirus Plus (\$ 69.65)**.

Página de Antivirus Plus

Formulario para la compra online del supuesto programa antivirus

91.188.59.50

En este momento no presenta actividad, pero durante los meses aglomerados entre abril y junio de 2010 alojó un paquete de afiliados de negocio llamado **BOMBA STATS** bajo el dominio **bombastats.com**, con un importante nivel de actividad fraudulenta a través de **Pay-per-Install** (pago por instalación), y descargando los códigos maliciosos:

- **badb-console.exe** (407208005d428ec9fb3f8059d7824da6) – Zeus
- **grabl-ssf.exe** (349265b0a88448a715ff545f4db762d9) - Koobface



Más información sobre BOMBA en:

<http://malwareint.blogspot.com/2010/07/bomba-botnet-new-alternative-crimeware.html>

Al momento de escribir este documento, **BOMBA** sigue adelante con sus actividades delictivas bajo la cobertura de **BKNET "SIA" IZZI** pero resolviendo **bombastats.com** en la dirección IP **85.234.191.40**.

91.188.59.51

Aquí se resolvía el dominio **happyinstalls.com** hasta principios de Agosto de 2010. **HAPPY INSTALLS**, también conocido como **VIVA INSTALLS**, es otro afiliado de negocio del tipo **Pay-per-Install** a través del cual se diseminó el archivo **setup.exe** (971eab628a7aac18bb29cba8849dff61). Un troyano downloader mediante el cual se descarga desde **91.188.59.112** un security rogue llamado **A.fast Antivirus**.



Más información sobre VIVA INSTALLS en:

<http://malwareint.blogspot.com/2010/08/pay-per-install-through-viva-installs.html>

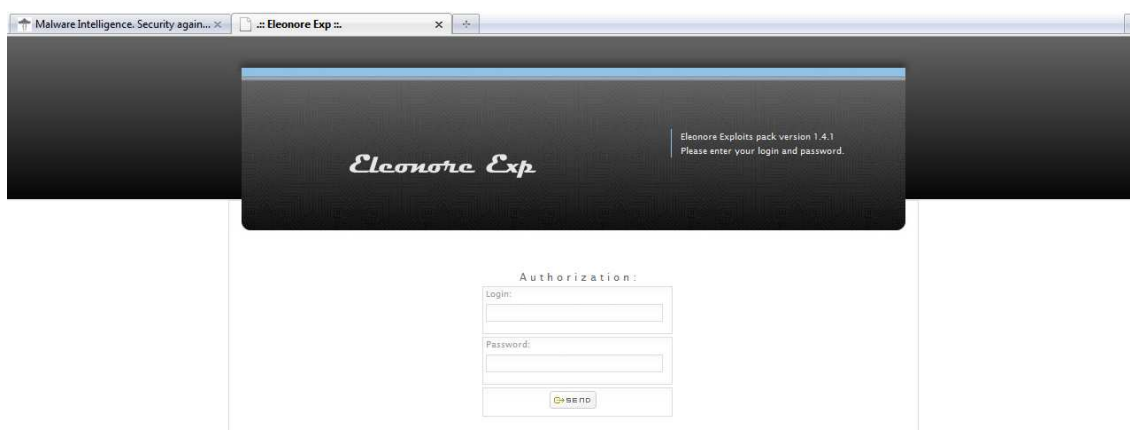
91.188.59.52

Actualmente no presenta actividades. Sin embargo, durante abril de 2010 alojaba una versión de **Phoenix Exploit's Kit** mediante el cual explotaba varias vulnerabilidades, entre ellas Adobe Collab ([CVE-2007-5659](#)), Adobe util.printf ([CVE-2008-2992](#)), Adobe getIcon ([CVE-2009-0927](#)), doc.media.newPlayer ([CVE-2009-4324](#)).

91.188.59.69

Actualmente aloja la versión 1.4.1 de Eleonore Exploits Pack en los dominios **senderdata.co.cc** y **trafficdata.co.cc**, mediante los cuales propaga los siguientes códigos maliciosos:

- [fgc0cb.exe](#) (47b43edebb5d3bb96dac83a0ef450a13) – **Qhost**
- [obigqs7.exe](#) (356dd48f8ef4614b7852ae49499d571a) - **Olmarik**



Pantalla de acceso a Eleonore Exploit Pack v1.4.1

1.4.1 es la última versión de este crimeware, puesto a la venta durante Marzo de 2010

*Más información sobre **Eleonore Exploit Pack** en:*

<http://malwareint.blogspot.com/2010/06/state-of-art-in-eleonore-exploit-pack.html>

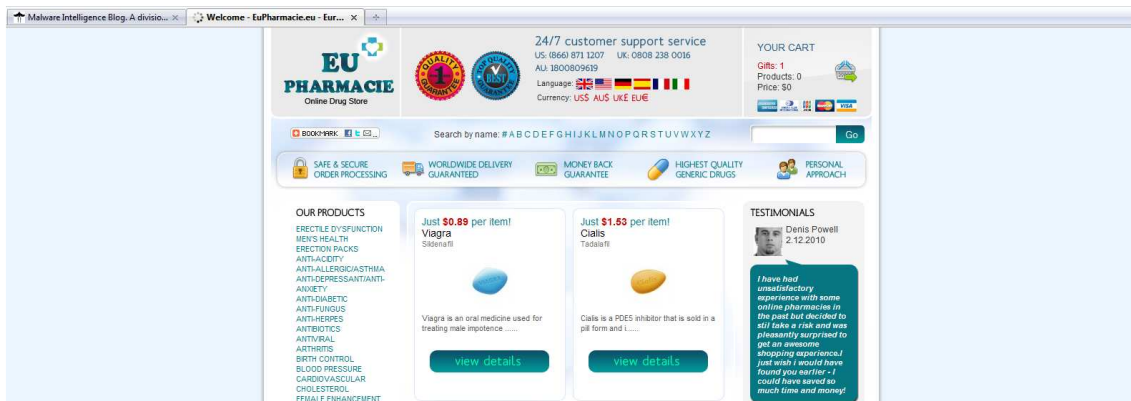
<http://malwareint.blogspot.com/2010/01/state-of-art-in-eleonore-exploit-pack.html>

91.188.59.70-71

Actualmente no presenta actividad maliciosa. Sin embargo, durante Abril de 2010 alojó la descarga de un rogue llamado **Antivirus Plus**, que formaba parte de un sistema de afiliados.

91.188.59.72

Aloja la página de **EU Pharmacie**, una farmacia en línea que los spammers promocionan activamente, sobre todo a través de foros. El panel de acceso para los afiliados se encuentra en 91.188.59.72/admin/index.php/.



Página de Eu Pharmacie

Este template es utilizado por los spammers para promocionar la farmacia en línea

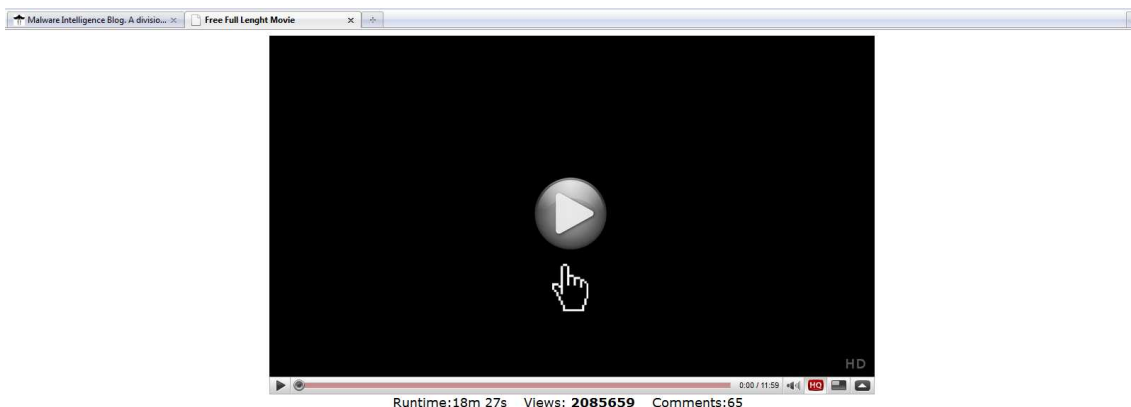
91.188.59.73

Resuelve los siguientes dominios: asianrapemovies.com, hotfilesfordownload.com, hotquickiefuck.com, sasha-blonde.com, you-porn-movies.com, youfoundporn.com y youpornfiles.com.

Desde los dominios asianrapemovies.com, hotquickiefuck.com, sasha-blonde.com, you-porn-movies.com y youfoundporn.com (páginas pornográficas) se descarga un binario alojado en la carpeta **mov524** del dominio hotxtubeonline.com (91.188.59.74).

Sin embargo, en este dominio (hotxtubeonline.com) se esconden diferentes alternativas de engaño que, siempre bajo la cobertura de representar páginas con contenido pornográfico, redireccionan hacia la descarga del mismo ejecutable **movie.exe**. Sus carpetas y etiquetas web son:

- hotxtubeonline.com/video1483/beast → **BeastTubeVideos**
- hotxtubeonline.com/video1483/incest → **IncestTubeVideos**
- hotxtubeonline.com/video1483/porn → **Free Full Lenght Movie**
- hotxtubeonline.com/video1483/tube → **PornTubeVideos**
- hotxtubeonline.com/video1483/xxx → **Free Full Lenght Movie**



Cada una de estas páginas, direcciona el tráfico hacia **hotxtubeonline.com/mov524/**, desde donde se descarga el archivo [movie.exe](#) (147c9b71838c450df08c8648b0f1fcb4). Además de este archivo, en la carpeta mov524 se guardan los siguientes archivos:

- [movienosoft.exe](#) (59f45ea9a7b5b6514a6e914fdbd5e026) - **FakeAlert**
- [movietemp.exe](#) (5ebf08e98c7fbb132cf212bd151238a5)

El dominio **hotfilesfordownload.com** es utilizado como estrategia de BlackHat SEO.

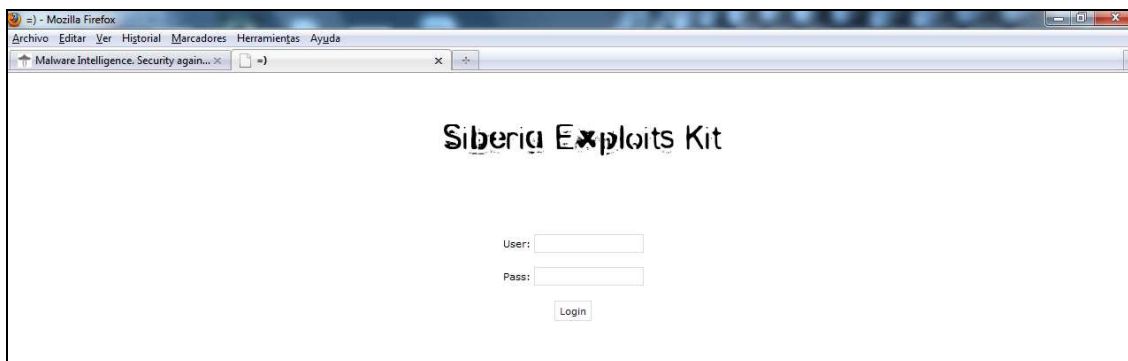
91.188.59.74

Aloja los dominios **freeanalsexubemovies.com**, **freetube06.com**, **hot4youxxx.in**, **hotxtubeonline.com**, **hotxxxtubevideo.com**, **iil10oil0.com**, **porn-tube-video.com**, **porntubefast.com**, **porntube2000.com** y **youvideoxxx.com**.

Utiliza la misma estrategia de propagación que en 91.188.59.73 desde los dominios porn-tube-video.com, freeanalsexubemovies.com, freetube06.com, porntubefast.com, youvideoxxx.com y porntube2000.com.

91.188.59.84

Actualmente no presenta actividades maliciosas. Sin embargo, durante Abril/Mayo y Julio resolvió los siguientes dominios **asspuc.com**, **ckldom.in**, **kinorik.com**, **mazarave.in**, **oyaebu11.ru**, **super-splyotik.in** (en los cuales alojó **Eleonore Exploit Pack 1.3.2**) y **probaki.info** (**Siberia Exploits Kit**).



Pantalla de acceso a Siberia Exploits Kit

Este crimeware fue el sucesor de una fracasada versión anteriormente llamada Napoleon

*Más información sobre **Siberia Exploits Kit** en:*

<http://malwareint.blogspot.com/2010/05/intelligence-and-operational-level-by.html>
<http://malwareint.blogspot.com/2009/12/siberia-exploit-pack-another-package-of.html>

91.188.59.92

Durante Mayo de 2010 alojó una copia de **SEO Sploit Pack** en los dominios **aaqqwweesseerrrgd.ussplatz.com**, **sssdddeerrrrrr.ussprojekt.com**, **gillestmh.com** y **indyvettes.info**.



91.188.59.93

También durante Mayo alojó **SEO Sploit Pack** pero en los dominios **ytoimneyqawernmkla.deswelt.net** y **abcabcabcabcabca.tobsupper.com**. En <http://ytoimneyqawernmkla.deswelt.net/admin.php> se encuentra activo uno de estos crimeware.

91.188.59.94

Resuelve los dominios **buburuzka.com**, **sixteenporn.in** y **viporntube.in**. Desde **buburuzka.com**, durante Abril de 2010 se propagaba un **SMS Ransomware** (a26fafa2ffb28446b371076b4524198d).

*Más información sobre **SMS Ransomware** en:*

<http://malwaredisasters.blogspot.com/2010/07/sms-ransomware-porn-template-update.html>

viporntube.in también presentó actividades maliciosas durante Abril de 2010 descarga un **FakeAV** desde **/xxxfree/lolita-free-video.exe** (6bec79b9622f78f3184bd402c2201a54).

En el caso de **sixteenporn.in**, descargaba otra variante del mismo **FakeAV** desde **/xxxfree/free-animal-sex.exe** (2a883e17803acf54b78cdd96c30b59a8)

91.188.59.95

Resuelve los dominios **ginsdirect.com**, **ginsdirect.net**, **rodfirst.com** y **solaruploaderz.com**.

Desde **ginsdirect.net** se realiza un **Drive-by-Execute** hacia diferentes páginas pornográficas hasta llegar a **free.porndirt.com.powered-by.securewebsiteaccess.com** desde donde se descarga un conocido adware – **setup.exe** (45049f6c8c95a4e821a85ba8798ded56): **HotBar** de **Zango**.

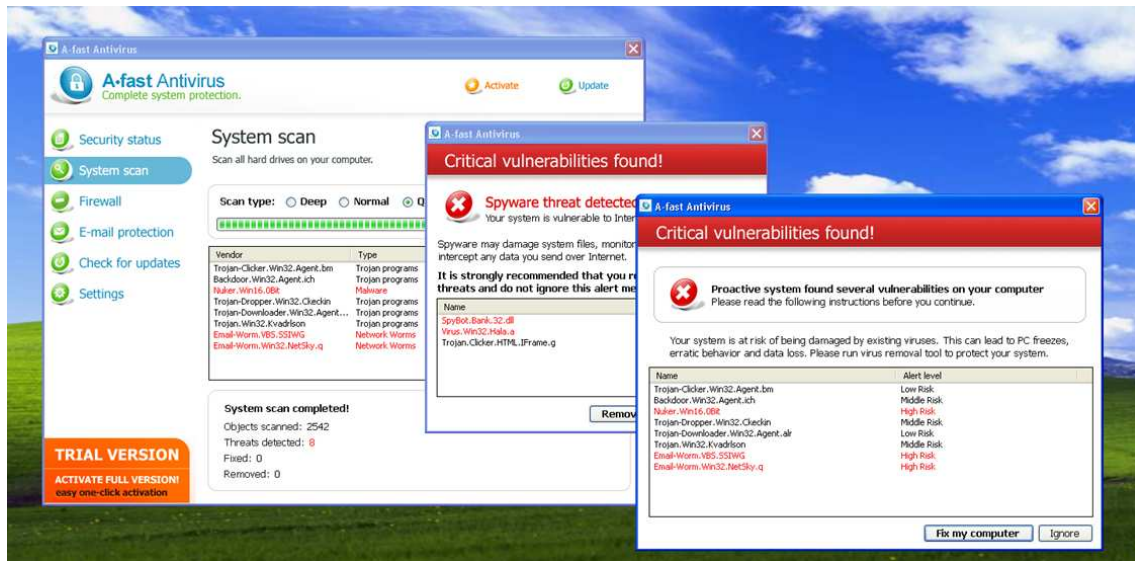
Durante Febrero, Abril, Mayo y Julio de 2010, presentó actividades maliciosas descargando varios tipos de códigos maliciosos alojando también una versión de **SEO Sploit Pack**.

91.188.59.98

Durante Abril/Mayo de 2010 resolvía en **kdjfkjskdfjlskdjf.com** desde donde se realizó una campaña de propagación de malware del tipo rogue (21259760d7afcee68bd77d175b1e6ad1).

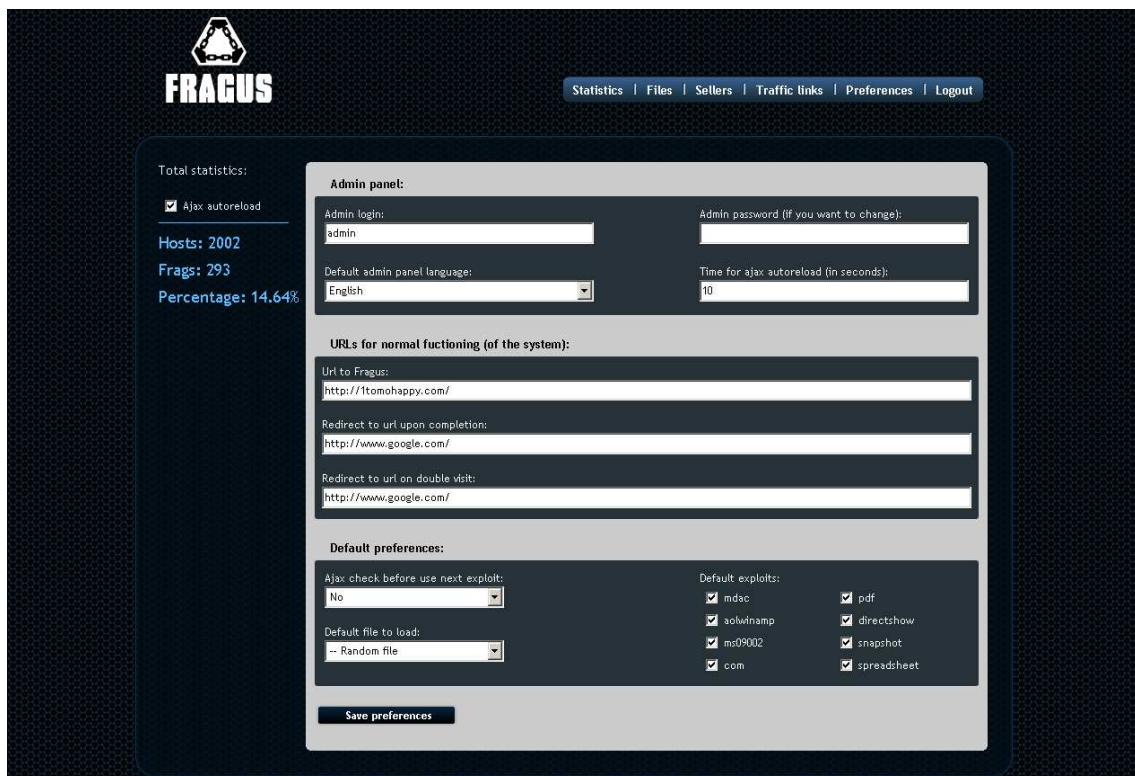
91.188.59.112

Utilizado por el programa de afiliados **VIVA INSTALLS** para diseminar el rogue **A-Fast Antivirus** (971eab628a7aac18bb29cba8849dff61), resolviendo el dominio **a-fast.com**.



91.188.59.125

Durante Mayo de 2010 presentó actividades de **Fragus** a través del dominio **kerrimckeeq.info**. En dicha oportunidad, a través de este crimeware, uno de los códigos maliciosos que se diseminaba era **cdert.jar** (ea7e971ad8a57908bae5a0e85729e9e1), un exploit para Java.

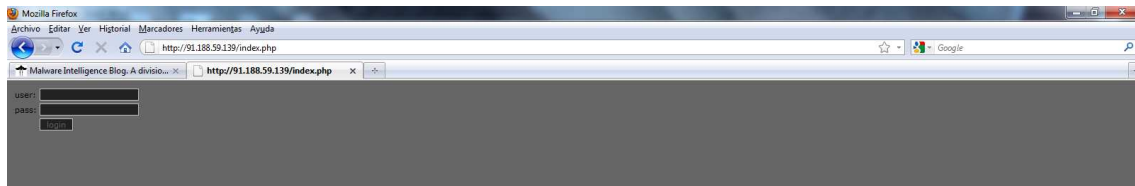


Más información sobre **Fragus** en:

<http://mipistus.blogspot.com/2009/12/una-breve-mirada-al-interior-de-fragus.html>

91.188.59.139

Actualmente aloja una aplicación web cuyo panel de acceso se encuentra en **91.188.59.139/index.php**.

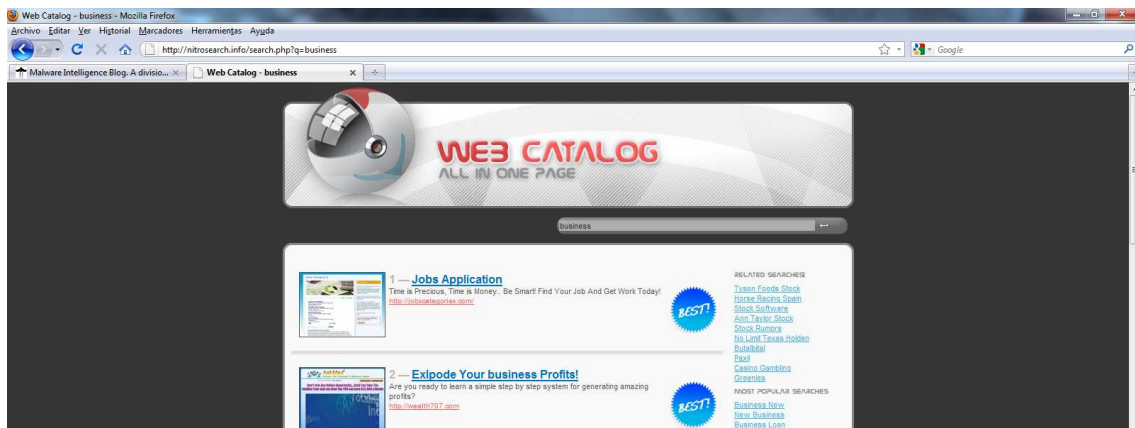


Panel de acceso

Corresponde a una aplicación web maliciosa no identificada por el autor de este documento

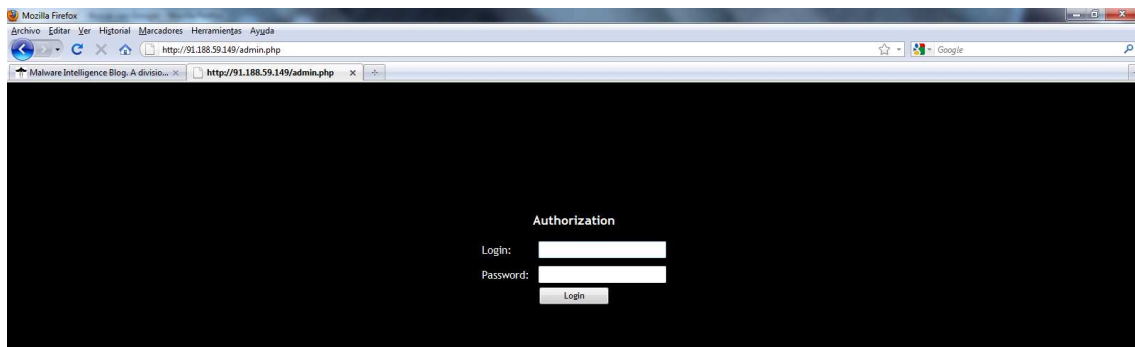
91.188.59.140

Resuelve en **nitrosearch.info**, lo que parecería ser un nido de mulas.



91.188.59.149

Actualmente presenta actividad maliciosa alojando una versión de **Fragus**. Descarga un archivo llamado **setup.exe** (7ffb83fda56e91d691b602691a15cb18), un **FakeAV**, desde **91.188.59.149/load.php**. El panel de acceso se encuentra en **91.188.59.149/admin.php**.



Pantalla de acceso a Fragus

Fragus, al igual que la mayoría de los crimeware de este estilo, es de origen ruso. Su primera versión se puso a la venta en foros underground durante el mes de Julio de 2009

91.188.59.197

Actualmente resuelve los siguientes dominios **ad.lometr.pl**, **brenz.pl**, **chura.pl**, **jl.chura.pl**, **lometr.pl**, **speedsearch4you.in**, **trenz.pl** y **zief.pl**. Presenta una tasa muy alta de actividades maliciosas diseminando una versión del troyano de Zeus a través del dominio **lometr.pl** ([6ccee7d98e91f569d83fc0729e243c65](https://www.virustotal.com/hispano-es/urls/6ccee7d98e91f569d83fc0729e243c65/)).

Durante Julio resolvía también el dominio **ad.ghura.pl**. Este dominio actualmente se encuentra activo pero resolviendo en la dirección IP **91.188.59.199**.

A principios de Agosto alojó un programa de afiliados bajo el dominio **traffcash.biz**.

91.188.59.199

Resuelve el dominio **ad.ghura.pl**, alojando los siguientes códigos maliciosos:

- [rc.exe](#) (9362a3aee38102dde68211ccb63c3e07) **Qhost**
- [iv.exe](#) (1cc189dade04a31ada04730177b706c5) **Olmarik/TDSS**
- [rus.php](#) (05265022c4a4af578149f3e14403ded5) **Wigon/HareBot**

91.188.59.205

Durante la primera semana de Agosto de 2010 resolvía el dominio **spandating.com** desde el cual se descargaba un binario ejecutable con MD5 [0d3521574fc4d457c505be1468685a64](https://www.virustotal.com/hispano-es/urls/0d3521574fc4d457c505be1468685a64/).

Actualmente esta dirección IP resuelve los dominios **compromendes.com** y **macromediasetup.com**. Este último se encuentra inactivo, pero durante Julio de 2010 alojó una versión del crimeware **Zombie Exploitation Kit**. El panel de acceso estaba en macromediasetup.com/zombie/stats.php.

También una copia de **Eleonore Exploit Pack 1.3.3** cuyo panel de acceso estaba en macromediasetup.com/eleos/stat.php.



Java (jdt)	175	49.58 %
cve-2010-1885 (hcp)	67	18.98 %
PDF	66	18.7 %
ms06-014 (mdac)	31	8.78 %
Java (gif parse)	8	2.27 %
cve-2009-1862 (swf2)	4	1.13 %
cve-2007-0071 (swf1)	2	0.57 %

© 2010 Zombie Infection Kit™

Zombie Exploitation Kit

Módulo de este crimeware de reciente aparición en el cual se visualiza su repertorio de exploits

91.188.59.231

Resuelve los dominios **abhivakshita-adedagbo.freeblogshost.in** y **freeblogshost.in**, a través de los cuales emplea la misma estrategia de ingeniería social aplicada desde 91.188.59.230, empleando **BlackHat SEO** para la descarga e FakeAV.

91.188.59.232

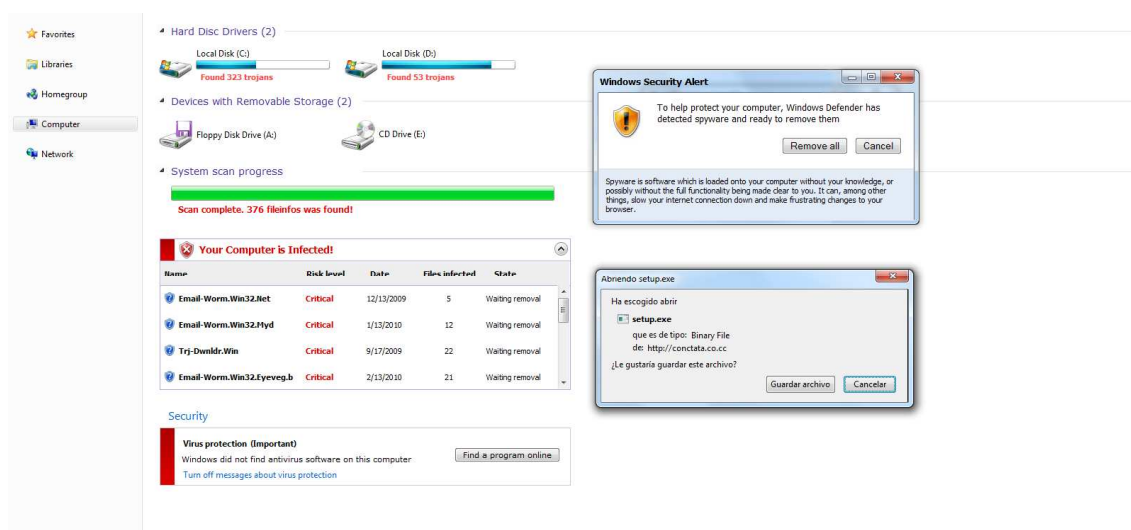
Resuelve los dominios **eurys-jessamyn.livefreeblogs.in** y **livefreeblogs.in**. Misma estrategia de **BlackHat SEO** a través de blogs para la diseminación de FakeAV.

91.188.59.234-235-237-238-239-240-241-242-243-249

Resuelven diferentes dominios en los cuales se alojan blogs, preparados para inyectar la redirección del tráfico a través de un TDS (Traffic Direction Script) para diseminar FakeAV.

91.188.59.236

Resuelve los dominios **aalok.freeliveblog.in** y **freeliveblog.in**, a través de los cuales emplea la misma estrategia de ingeniería social aplicada desde 91.188.59.230, empleando **BlackHat SEO** para la descarga e FakeAV.



Otra variante de falso escaneo

Se trata de otra de las estrategias de Ingeniería social ampliamente utilizadas para la propagación de falsos antivirus

Más información sobre una nueva estrategia para la propagación de rogue en:

<http://malwareint.blogspot.com/2010/08/fakeav-via-new-strategy-of-deception.html>

Conclusión

Al realizar la triangulación de la información, es evidente que existe una fuerte conexión entre las diferentes direcciones IP y que se trata de un mismo grupo delictivo. Un grupo delictivo que está muy bien organizado y que, de forma intencional o no, opera desde hace mucho tiempo bajo el mismo AS, que es en realidad un nido de actividades delictivas y fraudulentas comandado por un grupo de delincuentes.

No escapan de la órbita que les ofrece la diseminación de diferentes códigos maliciosos a través de diferentes recursos delictivos como distintos sistemas de afiliados, paquetes de exploits y malware kit como Phoenix Exploit's Kit, YES Exploit System, Eleonore Exploit Pack, ZeuS, entre otros, manejando diferentes modelos de negocio que abarcan un amplio porfolio de estrategias, siendo altamente posible que se trate del mismo que distribuye Koobface, ya que existen evidencias de que al menos podría haber una conexión entre los integrantes y estrategias para distribuir koobface a través, en este caso, la cobertura de este AS.

Aunque en el presente sólo se cubrió un determinado rango de IP, queda evidenciada la magnitud de la problemática que actualmente constituyen los grupos delictivos que conforman las mafias en Internet.

Existen otros rangos altamente explotados con fines similares y seguramente muchos de los dominios expuestos en el presente, se darán de baja, se crearán otros y se migrarán hacia diferentes direcciones IP, ya que los mecanismos empleados son muy dinámicos.



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>

