# MalwareIntelligence

## Inside Carberp Botnet

Francisco Ruiz – Crimeware Research of **MalwareIntelligence** | fruiz@malwareint.com


# Contenido



**IMPORTANT**: This document is technical in nature and has information relating to web addresses, IP addresses, routes downloading binaries, among others, that are directly related to the infection strategies and criminal processes carried out by cybercriminals.

Therefore, we recommend the responsible use of information provided in the present, being under the exclusive and sole responsibility of the reader for any inconvenience that may arise depending on the mishandling and misuse of the data presented.

The paper also has accurate information of the results obtained from the study. Therefore, and by the very nature of the research process has not been provided to 100% of the data collected, but more data are available by sending the request to the author.

# Introducción

Carberp remonta sus inicios a principios de 2010, pero no ha sido hasta los últimos meses del año en cuestión cuando ha saltado la alerta de las compañías de antivirus, tras descubrir ciertos mecanismos empleados hasta entonces por un nuevo malware.

Esta ventana de tiempo, de la cual gozó el código malicioso asociado a la botnet Carberp significa, fundamentalmente, que ha estado operando durante meses con un ratio de detección muy bajo. Incluso, solo algunas de sus características hacían alertar algunos productos antivirus confundiendo su actividad con Zbot, el troyano de ZeuS.

Carberp fue catalogado en febrero de 2010 como trojan-downloader, lo cual provocó que hasta mediados de septiembre este malware estuviera catalogado como un trivial downloader diseñado para automatizar el proceso de descarga de otra pieza de malware, cuando realmente se había convertido en una amenaza muy compleja.

Por otro lado, Carberp es privado y no se dispone de ninguna información sobre como adquirir el crimeware, lo cual se evidencia en los pocos C&C que posee; y sin lugar a dudas, esta categorización de "recurso delictivo privado" lo mantuvo, y aún hoy lo hace, alejado de los índices de detección.

El presente documento expone una descripción en detalle de cada una de las piezas que integra la cadena delictiva que se genera a través de Carberp. Desde sus diferentes generaciones, pasando por los componentes internos hasta el proceso de comercialización del Malware Kit.

Versión en inglés
http://www.malwareint.com/docs/inside-carberp-botnet-en.pdf

Versión en español
http://www.malwareint.com/docs/inside-carberp-botnet-es.pdf

# Generaciones

La primera aparición pública de **Carberp** es como un trojan-downloader, algo muy distante a lo que se acabaría convirtiendo.

A partir de su segunda generación, el crimeware incorpora los recursos necesarios para crear una botnet controlable a través del protocolo HTTP con comunicación directa con su C&C, añadiendo además un complemento (plugin) llamado **Grabber**, encargado de habilita el robo de credenciales de una larga lista de aplicaciones que en futuras páginas se detalla.

La tercera generación, es la que actualmente se encuentra implementada en muchos de los C&C In-the-Wild, y la que se ha sido objeto de investigación por **MalwareIntelligence**.

Esta versión apareció a principios de septiembre y es, la que en gran medida, alertó a las compañías antivirus. Incorpora dos nuevos plugins que se cargan bajo los archivos "**stopav.cfg**" y "**miniav.cfg**". Sin embargo, se han detectado otros plugins diferentes en algunos C&C que evidencian la posibilidad con la que cuentan los delincuentes que se esconden detrás de Carberp se escalar funcionalidad en la botnet adquiriendo una serie de plugins opcionales.

# Proceso de infección

Carberp puede infectar una importante gama de plataformas de la familia Microsoft, entre ellas: Windows 95/98/Me/NT/2000/XP/Vista, Windows Server 2003/2008 y Windows 7. Una vez que se ejecuta en el sistema operativo víctima, realiza las siguientes operaciones:

**Infección del sistema**
Para evitar restricciones del UAC (User Account Control), crea los archivos en carpetas que no requieren permisos de administrador, tales como Startup, Application Data y Temp.

A diferencia de otros códigos maliciosos, Carberp no requiere permisos de Administrador para comprometer el sistema, porque no crea ni realiza modificaciones en el registro, sino que se ejecuta directamente en memoria. Es decir, Carberp tiene que ser activado cada vez que el sistema es reiniciado.

La reactivación luego de cada reinicio se ejecuta mediante una copia alojada en la carpeta Startup. En caso de explorar esta carpeta accediendo a ella desde el Explorador de Windows o a través de línea de comandos, no será posible visualizar el binario ejecutable de Carberp. Esta característica se debe a que Carberp posee técnicas de rootkit para ocultarse dentro del sistema.

Una vez que ha infectado el sistema, se inyecta en varias APIs para lograr ocultar sus archivos, incluyendo APIs desarrolladas para supervisar todo el tráfico que pasa por la máquina.

### Primeras conexiones al C&C

La primera conexión con el C&C se realiza contra el archivo **first.html**, enviando a través del parámetro **POST** el ID único que identifica al bot como perteneciente a determinada botnet de Carberp, y la lista de procesos que se encuentran en ejecución durante ese momento.

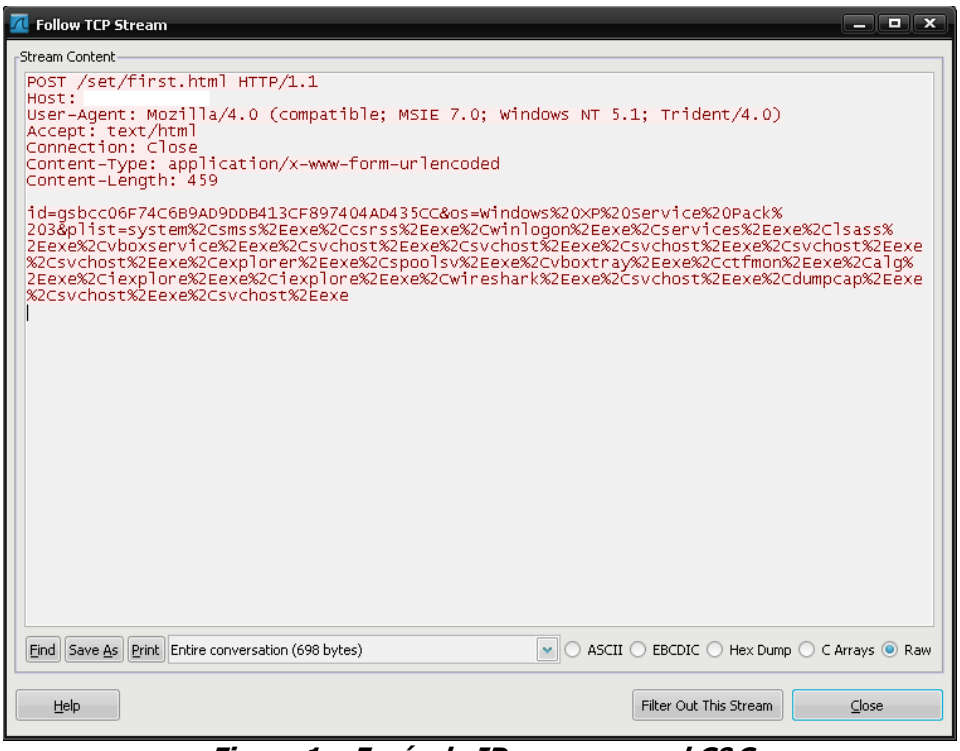



***Figura 1 – Envío de ID y procesos al C&C***

En la segunda conexión con el C&C hace uso de Drive-by para descargar y ejecutar los plugins **passw.plug**, **stopav.plug** y **miniav.plug**. A continuación, descarga el archivo que posee la configuración de la botnet, dentro del directorio */cfg/*, en este caso llamado gsbcc*:*

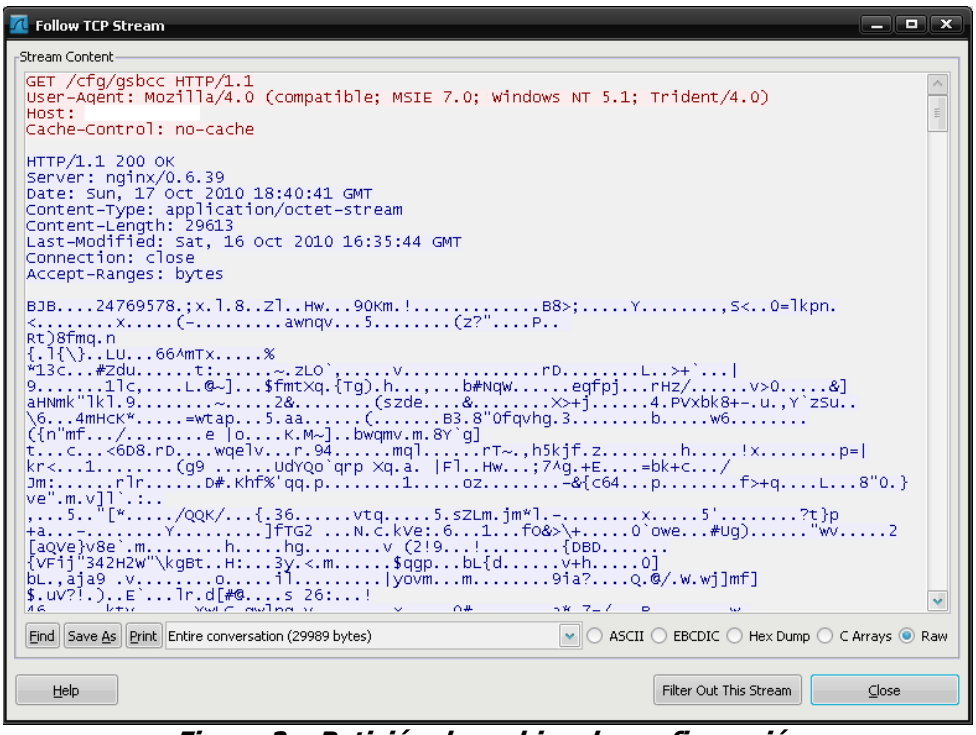



***Figura 2 – Petición de archivo de configuración***

Por último, mantiene su comunicación con el C&C para comprobar si existe configurada alguna tarea que deba realizar.

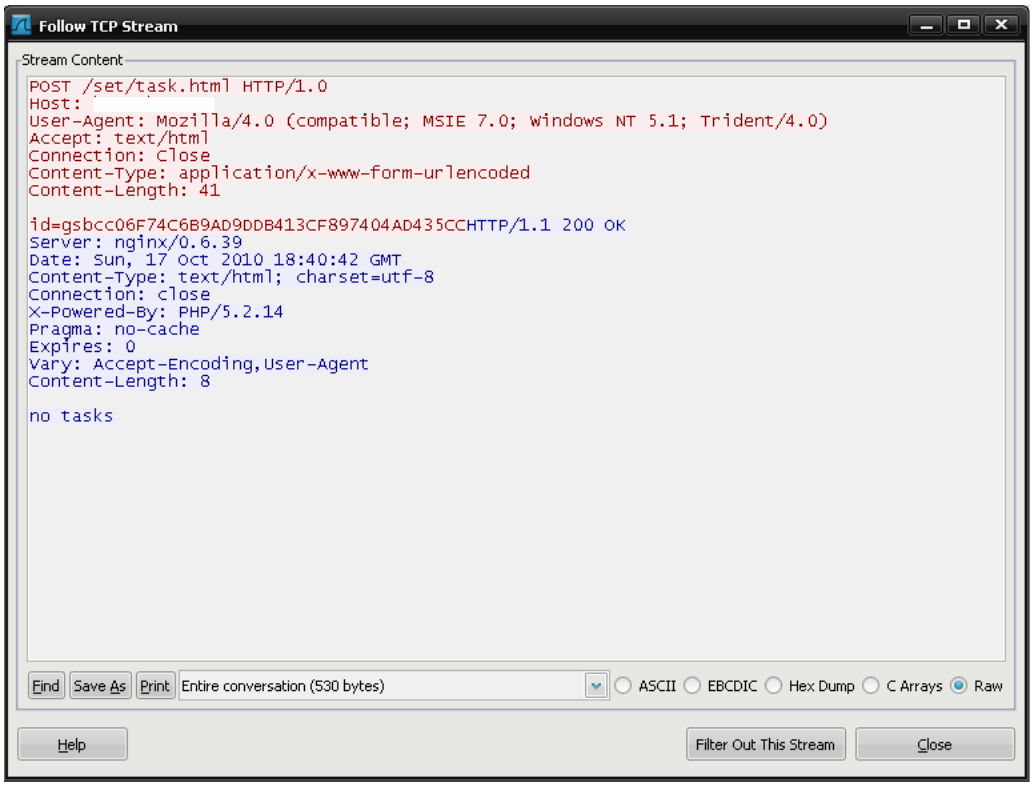



***Figura 3 – Petición de tareas a realizar***

Para ello, como puede observarse en la *Figura 3*, la petición POST se realiza contra el archivo *task.html* que en este caso no contempla tareas cargadas [*no tasks*].

# Carberp Comando & Control

El centro de comando y control [C&C] se alimenta constantemente con información robada desde las computadoras infectadas. Este proceso de inteligencia es realizado a través de una serie de plugins. Por defecto el paquete incorpora tres llamados **passw.plug**, **stopav.plug** y **miniav.plug.**

## Plugin passw.plug

El plugin *passw.plug* de Carberp es el encargado de robar las credenciales de acceso a diferentes servicios alojados en el sistema víctima. Como mencionamos anteriormente, todas aquellas credenciales relacionadas al navegador son obtenidas al embeberse a las APIs, pero además, cuenta con una lista de programas predefinidos de los cuales es capaz de obtener las credenciales y enviarlas al C&C.

Lista de programas soportados por el plugin es:

- AIM
- AIMPro
- AOLInstantMessenger
- ASP.NETAccount
- AppleSafari
- Becky
- BitKinex
- BlackwoodPRO
- BulletProofFTPClient
- CamFrog
- CiscoVPNClient
- ClassicFTP
- CoffeeCupFTP
- CoreFTP
- CuteFTP
- Dev Zero G FTPUploader
- Digsby
- DirectoryOpus
- Eudora
- ExcitePrivateMessenger
- ExpanDrive
- FARManagerFTP
- FFFTP
- FTPCommander
- FTPExplorer
- FTPRush
- FTPUploader
- FTPWare
- Faim
- FileZilla
- FinamDirect
- FlashFXP
- FlingFTP
- ForteAgent
- FreeCall
- FreeFTP/DirectFTP
- Frigate3FTP
- GAIM
- GizmoProject
- GmailNotifier
- GoogleChrome
- GoogleTalk
- GrayBox
- GroupMailFree
- ICQ2003/Lite
- ICQ99b-2002
- IncrediMail
- InternetExplorer
- JAJC
- LeapFTP
- LTGRoup
- MSNMessenger
- Mail.RuAgent
- MailCommander
- Mbt
- Mirabilis
- MirandaIM
- MozillaFirefox
- MySpaceIM
- Odigo
- Opera
- Opera 9 Beta
- Outlook
- POPPeeper
- PSI
- Paltalk
- Pandion
- Pidgin
- PocoMail
- QIP
- QIP.Online
- Remote Desktop Connection
- RimArts
- Safari
- SaxoTrader
- ScotTrader
- ScreenSaver9x
- Scribe
- SecureFX
- SIM
- SmartFTP
- SoftXFTPClient
- TheBat!
- Trillian
- Trillian Astra
- UltraFXP
- WebSitePublisher
- WS_FTP
- Wi
- WinSCP
- WinSCP 2
- WinVNC
- Windows / TotalCommander
- WindowsCredentials
- WindowsLiveMail
- WindowsLiveMessenger
- Yahoo!Messenger

Las siguientes imágenes son ejemplos mediante los cuales es posible visualizar las conexiones al C&C donde se reportan credenciales o forms:

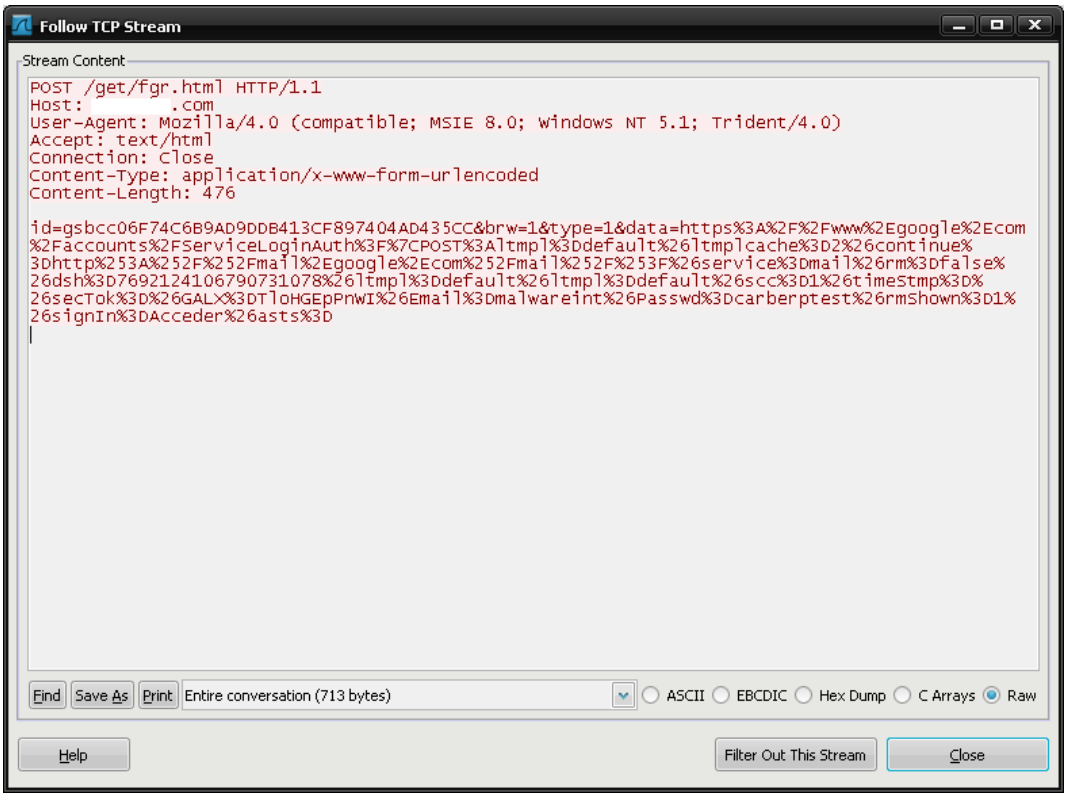



***Figura 4 – Envío de credenciales para acceder a Gmail***

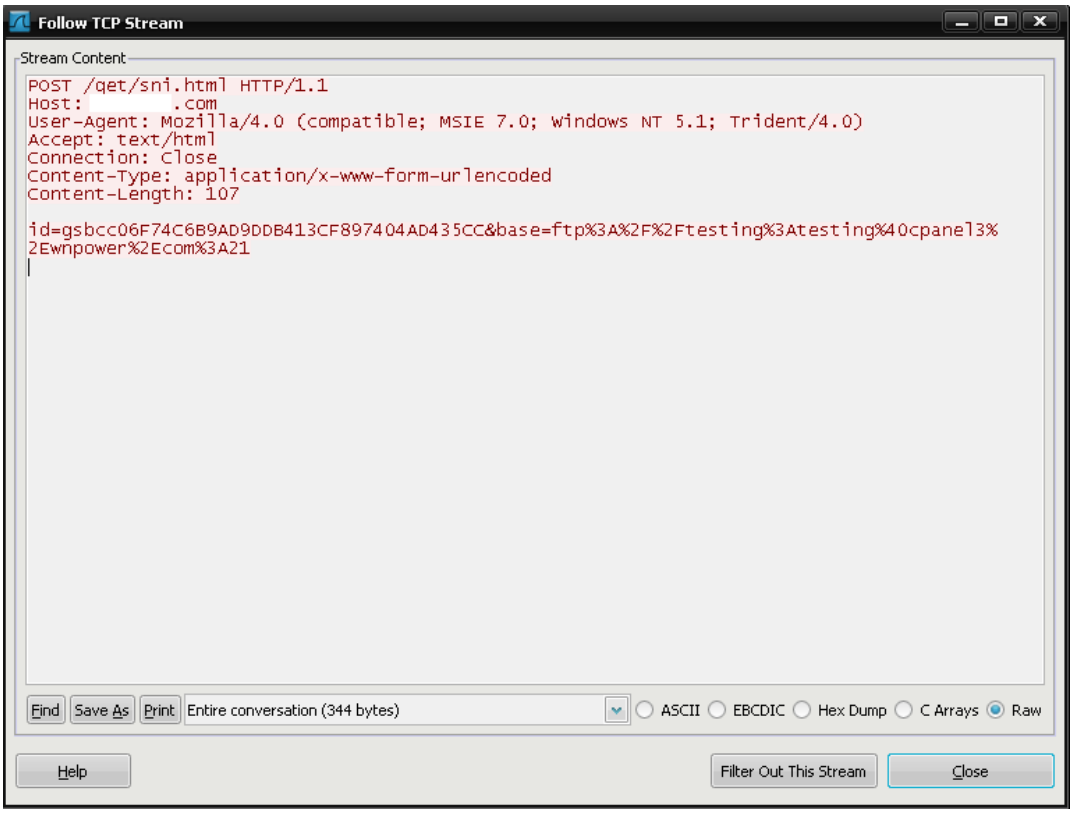



***Figura 5 – Envío de credenciales de acceso a cuenta FTP***

## Plugin stopav.plug

El plugin *stopav.plug* es el encargado de deshabilitar la protección del programa antivirus instalado en el equipo víctima, para evitar la detección del malware en el sistema. Los antivirus que son objeto de este plugin son:

- ESET NOD32 Antivirus
- ESET Smart Security
- ArcaVir Antivirus
- AVG8
- Mcafee Antivirus
- Avast!
- Avast5
- Avast4
- Microsoft Security Essentials
- Sophos
- DrWeb
- BitDeffender
- Avira

## Plugin miniav.plug

El plugin **miniav.plug** sigue la estela entre las "guerras" de creadores de malware, al igual que SpyEye detecta y desinfecta a sus víctimas que previamente han sido infectadas con alguna variante del troyano de ZeuS, Carberp sigue sus pasos eliminando (desinfectando) el malware de una batería de crimeware:

- ZeuS
- Limbo
- ImageFileExecution
- Barracuda And BlackEnergy
- MyLoader
- Adrenalin
- Generetic

# Carberp C&C Panel

El C&C Carberp presenta un falso mensaje de "*This account has been suspended*" cuando se accede al raíz del sitio.


***Figura 6 – Mensaje falso de Carberp***

En versiones anteriores el mensaje era "*404 – Not found*". Para entrar en el C&C, hay que pedir la página de login directamente desde */accounts/authorization.html*.

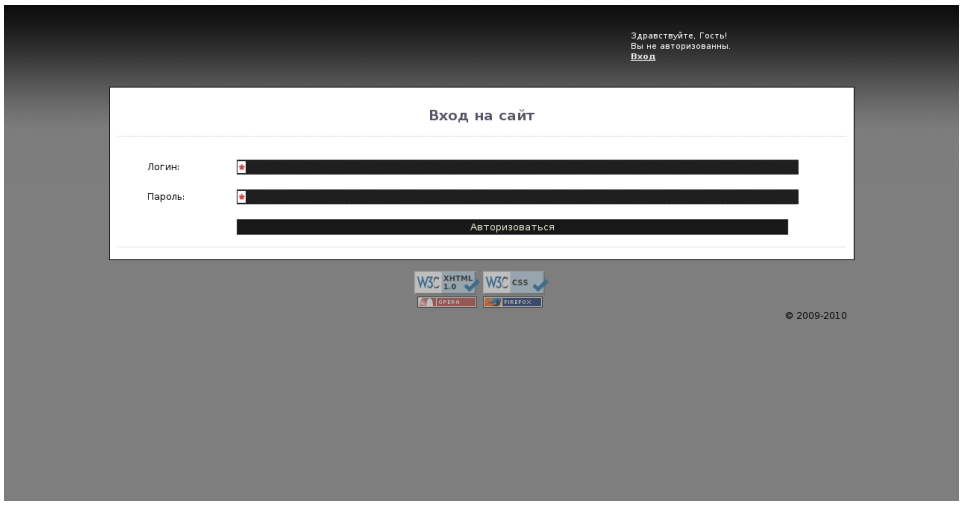



***Figura 7 – Panel de Login del C&C***

Como se puede observar en la figura 7, el C&C está en ruso y no hay opción alguna de establecer otro idioma. Esto es una prueba más, de que este malware no busca una comercialización a gran escala como lo hacen ZeuS o SpyEye, sino que está orientado a un mercado muy específico.

# Primeros datos

Una vez logueados en el panel, nos aparece la siguiente información:


***Figura 8 – Información que se visualiza inmediatamente después del acceso a Carberp***

Otra muestra más de su privatización. Todos los C&C de este crimeware definen un modelo de licencia que funciona solamente en el servidor donde se aloja el paquete y bajo una serie de dominios previamente definidos.

Como medida auto-defensiva, en caso de violación de la licencia el C&C no entra en funcionamiento. Los módulos usados en este C&C son:

**Miembros:** versión 1.0.0.2
**Gráficas:** versión 1.0.0.1
**Bots:** versión 1.0.0.1
**Archivos Cab:** versión 1.0.0.2
**Logs:** versión 1.0.0.1
**Inicio:** versión 1.0.0.3
**Preferencias:** versión 1.0.0.0

## Estado de la botnet

La siguiente pestaña del menú ofrece estadísticas sobre el estado de la botnet:

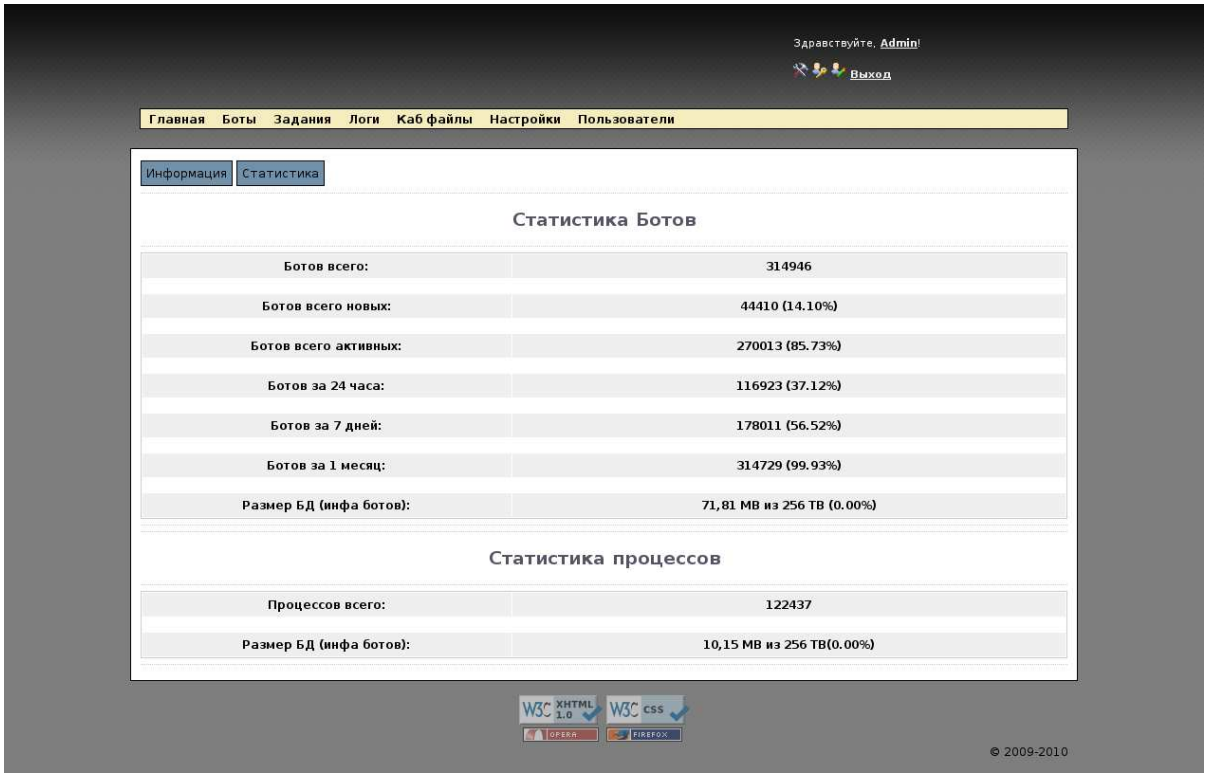



***Figura 9 – Números de la botnet***

**Bots totales:** 314.946
**Bots nuevos:** 44.410
**Bots activos:** 270.013
**Bots activos las últimas 24h:** 116.923
**Bots activos los últimos 7 días:** 178.011
**Bots activos el último mes:** 314.729
**Tamaño de la BD (info bots):** 71.81MB (no incluye logs)

Estos datos dan una idea de la capacidad de infección de Carberp, logrando en algunos C&C investigados por **MalwareIntelligence** superar los 500.000 zombis solo en un mes.

## Módulo de estadísticas

El módulo que ofrece información estadística es uno de los principales de la botnet, proporcionando datos relevantes sobre los sistemas operativos infectados y acceso directo a los logs de estos.

La primera muestra la cantidad de sistemas operativos infectados discriminados por países. Permitiendo seleccionar un país en particular para acceder solo a los registros de ese país.

En las pestañas de la derecha, podemos obtener diferentes gráficos sobre los sistemas infectados:

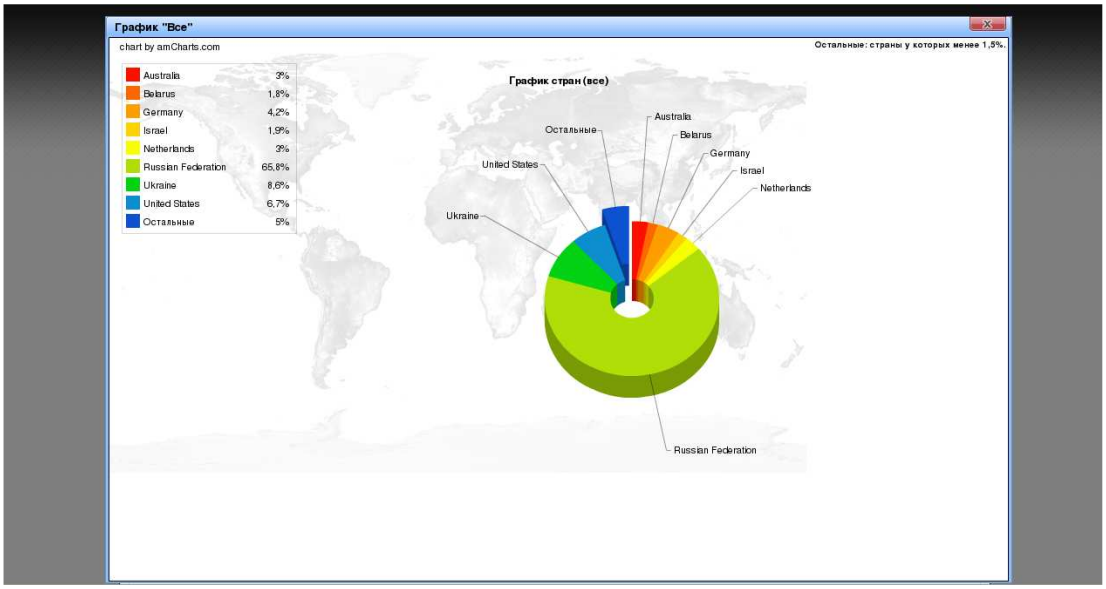



***Figura 10 – Geolocalización de los bots***

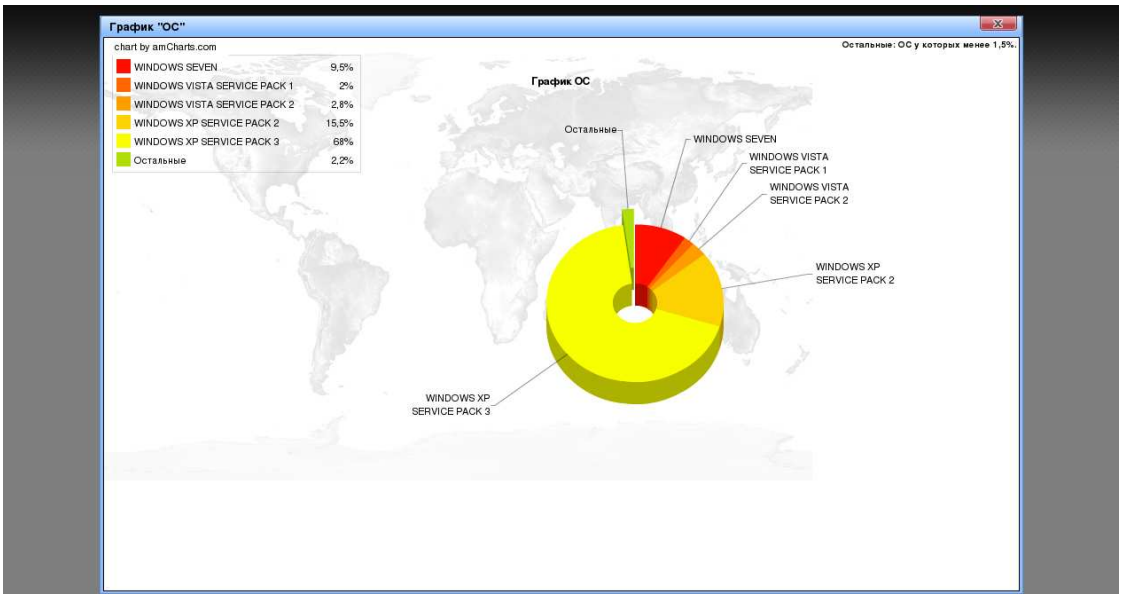



***Figura 11 – Sistemas Operativos de los bots***

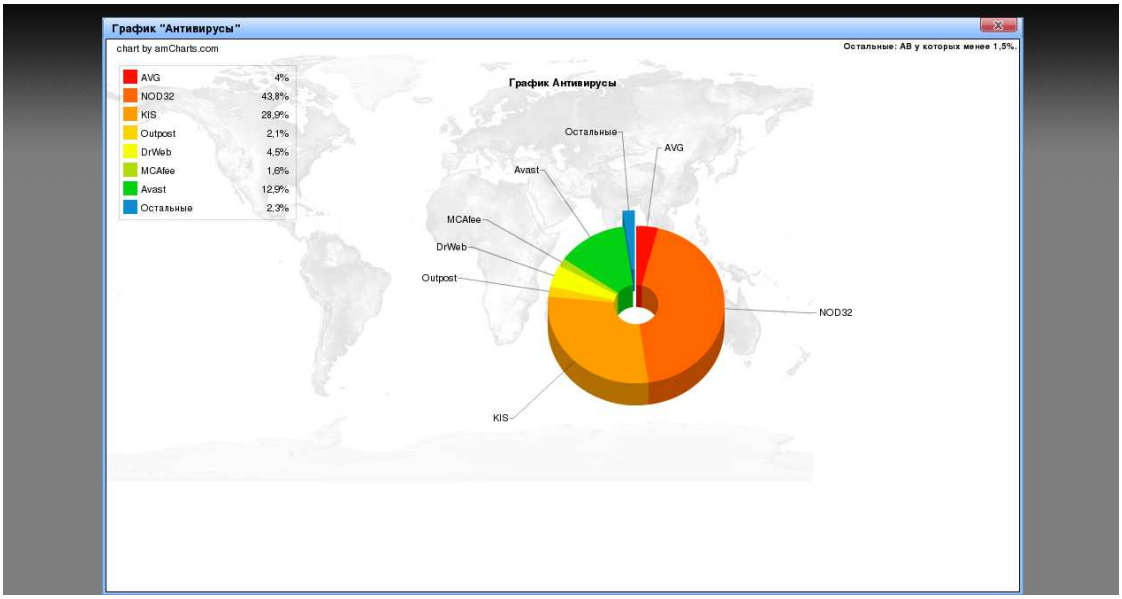



***Figura 12 – Antivirus de los bots***

## Información de Bots

Desde las pestañas de la izquierda contiene las siguientes opciones:

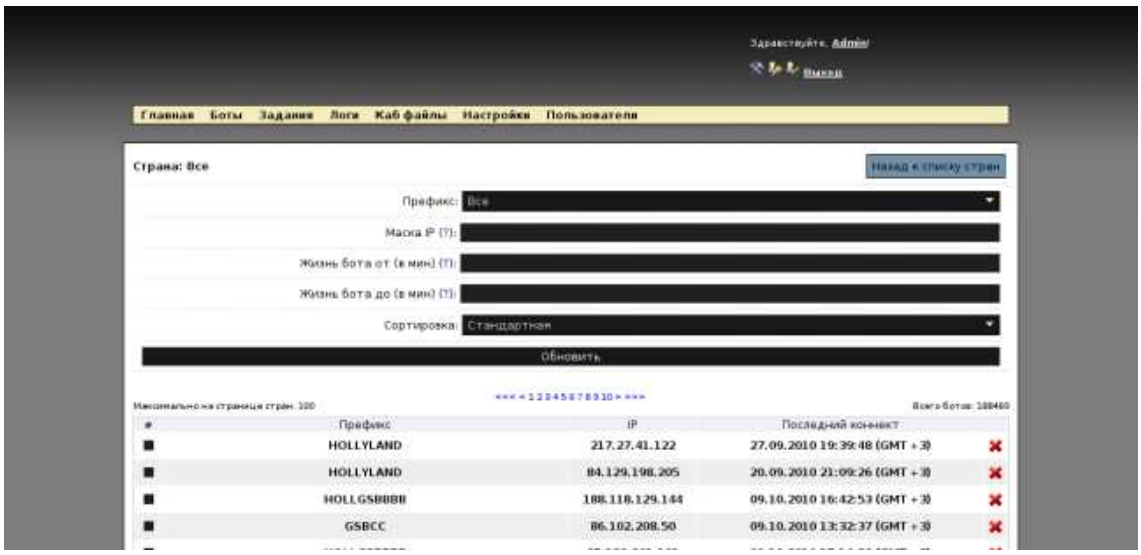
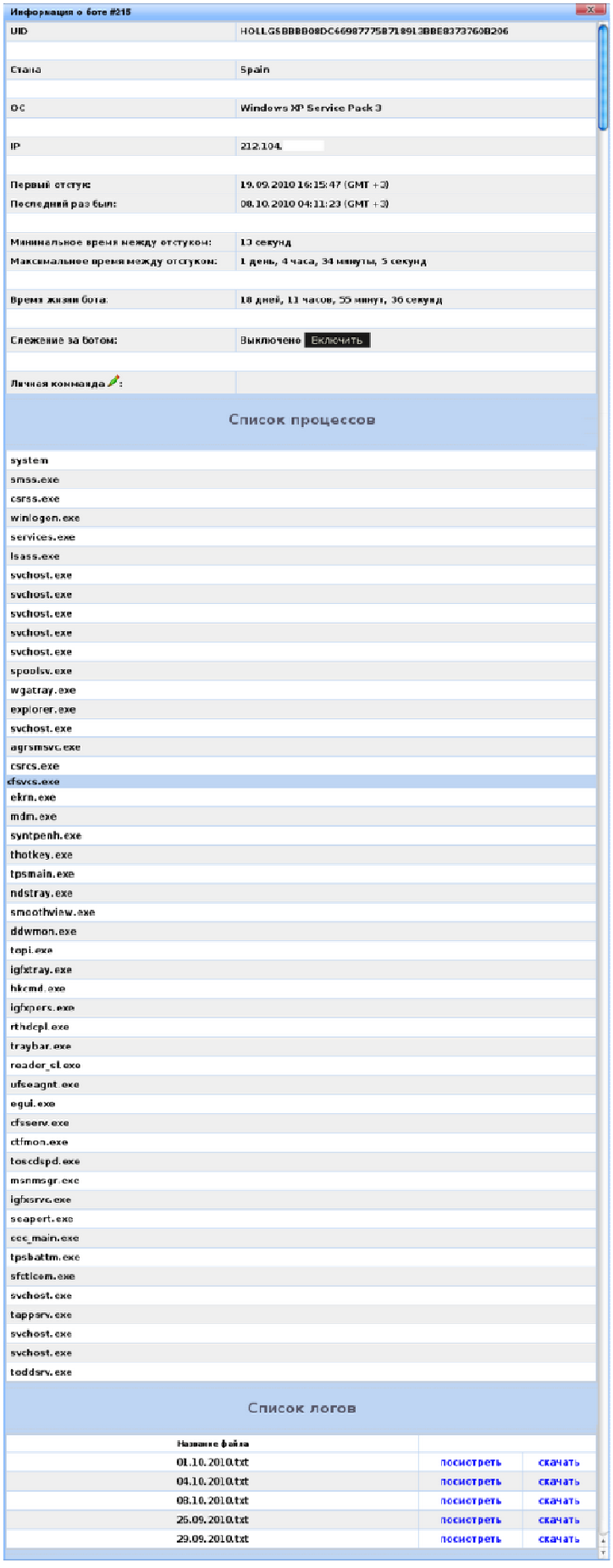



***Figura 13 – Todos los bots de 100 en 100***

Se muestran todos los bots correspondientes a todas las botnets de 100 en 100. En el menú superior se pueden escoger varias opciones para acotar los resultados:

**Botnet:** Todos los bots o excluir solo para una botnet (config) de la botnet global.
**Máscara IP:** Permite realizar búsquedas por IP o con máscara, por ejemplo 127.0.0.1.
**Tiempo de vida expresado en minutos:** Permite buscar los bots que han estado online al menos un número determinado de minutos.
**Tiempo de vida expresado en horas:** Lo mismo que lo anterior.
**Ordenar:** Para ordenar la información de forma ascendente o descendente.

Al hacer clic sobre la información de cada bot, se despliega la siguiente pantalla con información relacionada al bot:




**UID:** Identificador único en la botnet.
**País:** País.
**OS:** Sistema Operativo.
**Lista de procesos:** Lista de procesos enviada en el momento de la infección.
**Logs:** Son todos (grabber, formgrabber, sniffer) los logs reportados al C&C por el bot ordenados por días en un archivo de texto.

Además de las opciones mostradas, existe una opción de *"Seguir"* al bot. Esto da la opción de que cualquier cambio en los registros sea notificado al botmaster.

Ejemplo de una url dentro de un log:

*https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsnv=11&ct=1286261827&rver=6.0.5285.0&wp=MBI&wreply=http://mail.live.com/default.aspx&lc=1043&id=64855&mkt=nl-NL&bk=1286261830?|POST:login=XXXXX@hotmail.com&passwd=XXXXXX&type=11&LoginOptiLog=2&MEST=&PPSX=Passpor&sso=&i1=1&i2=2&i3=3918&i4=&i8=&i9=&i10=&i12=1*

## Módulo de búsquedas

Formulario de búsqueda de bots:

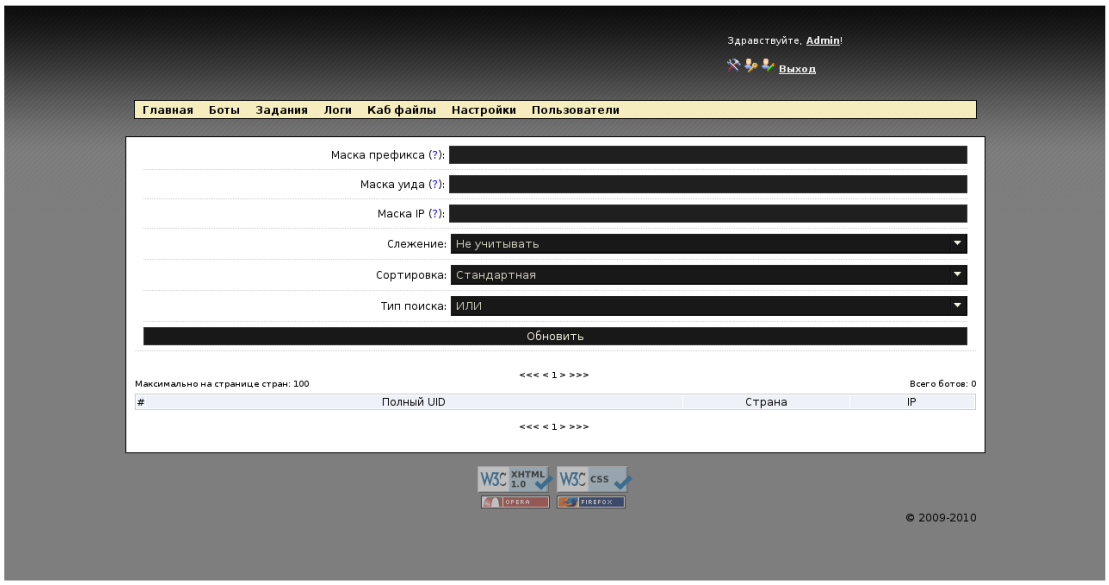



***Figura 14 – Formulario de búsqueda***

En la opción "config" se encuentran los archivos de configuración que utilizan los sistemas infectados junto a los plugins que dispone el C&C. Por defecto, Carberp solo trae 3 plugins que son: stopav.plug, avmini.plug y passw.plug. Lo más probable es que el resto de plugins hayan sido adquiridos como opción extra.

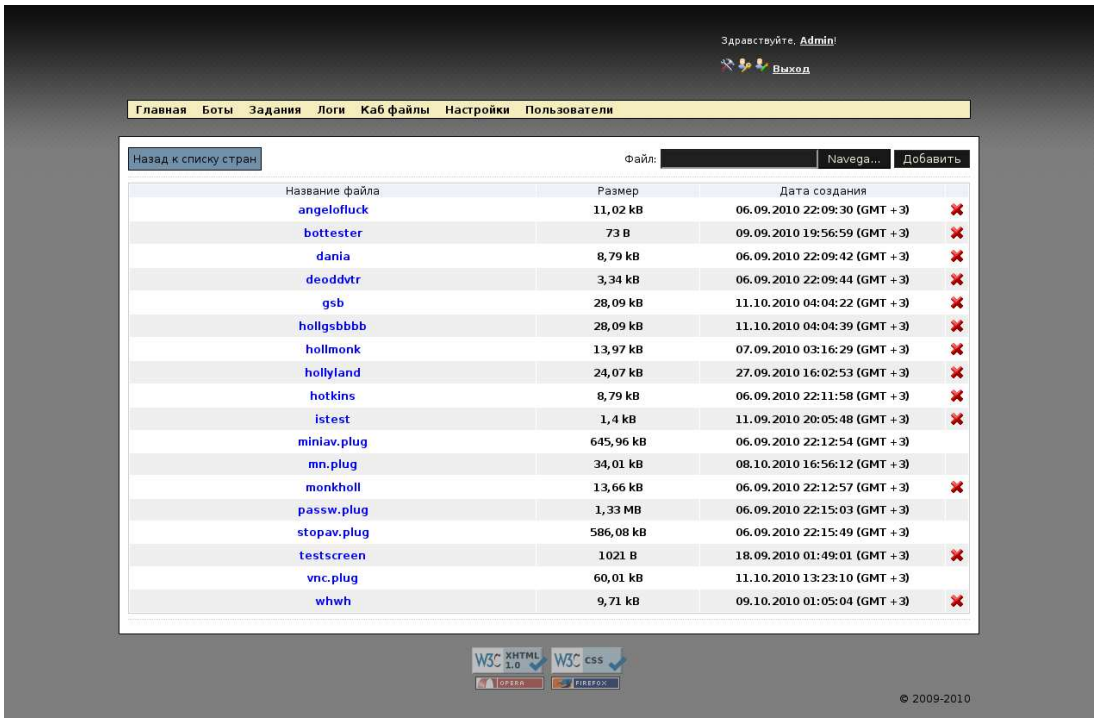



***Figura 15 – Archivos de configuración***

Los demás archivos sin la extensión plug son las configuraciones para los diferentes botnets Carberp de este C&C. Por los nombres, se pueden distinguir diferentes configuraciones por países o algunas pruebas del propio botmaster.

## Administración de tareas

En esta pestaña se muestra las tareas más recientes que el botmaster ha realizado y la opción de añadir nuevas tareas.

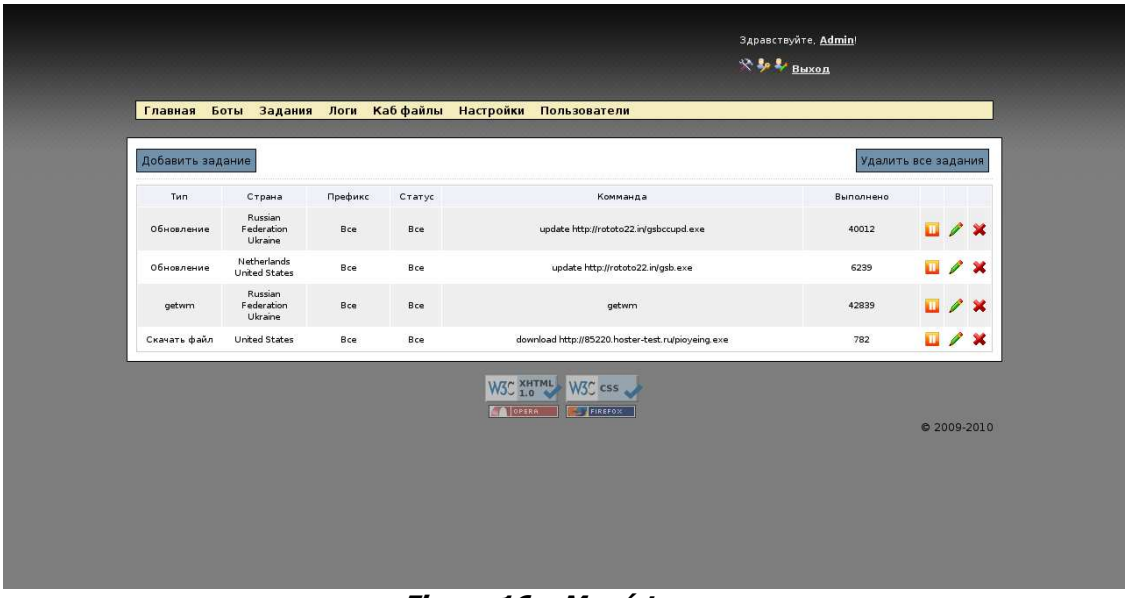



***Figura 16 – Menú tareas***

En este caso particular pudimos ver tres tipos de tareas diferentes: *update, getwm* y *download*. La tarea *update* sirve para que los sistemas infectados que se conecten al C&C, y que cumplan con el perfil requerido, actualicen su versión del bot. Mientras que *getwm* solicita a los bots sus credenciales del popular servicio WebMoney. Por último, *download* descarga un archivo definido por el botmaster y lo ejecuta.

Este tipo de opción es muy usada por los botmasters para ejecutar programas de servicios Pay-Per-Install, de los cuales ya hemos hablado en **MalwareIntelligence** en varias ocasiones. Estas tareas serán recibidas por el bot cuando se conecten al C&C en busca de tareas nuevas. A la hora de añadir una nueva tarea aparece el siguiente menú:

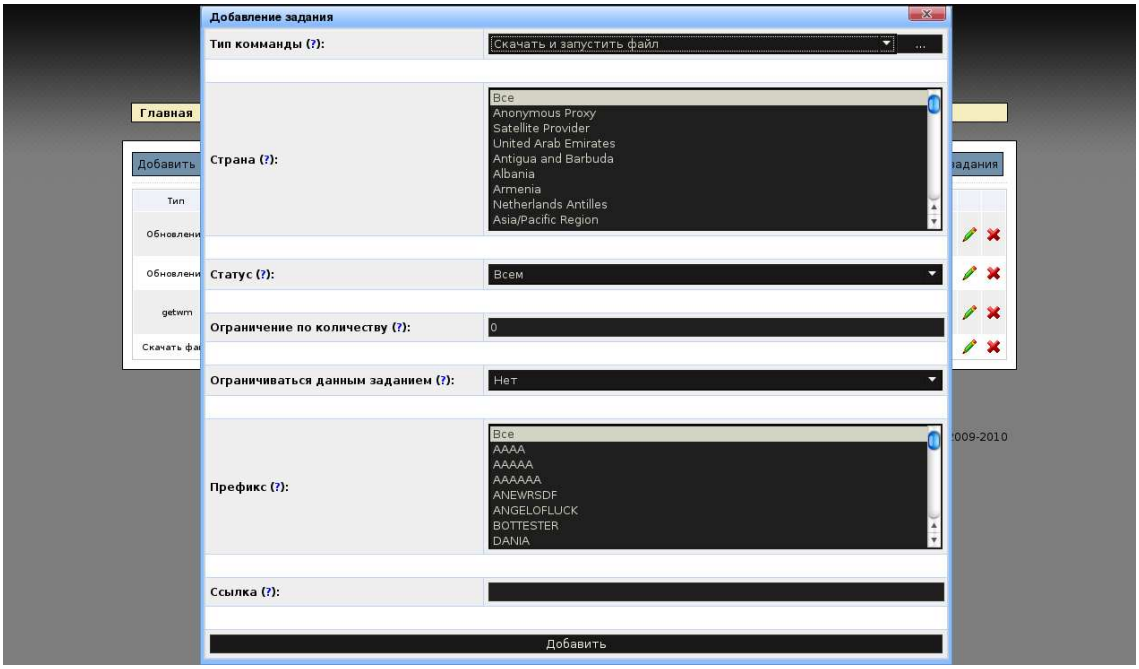



***Figura 17 – Añadir tareas***

En el cual se requieren las siguientes acciones:

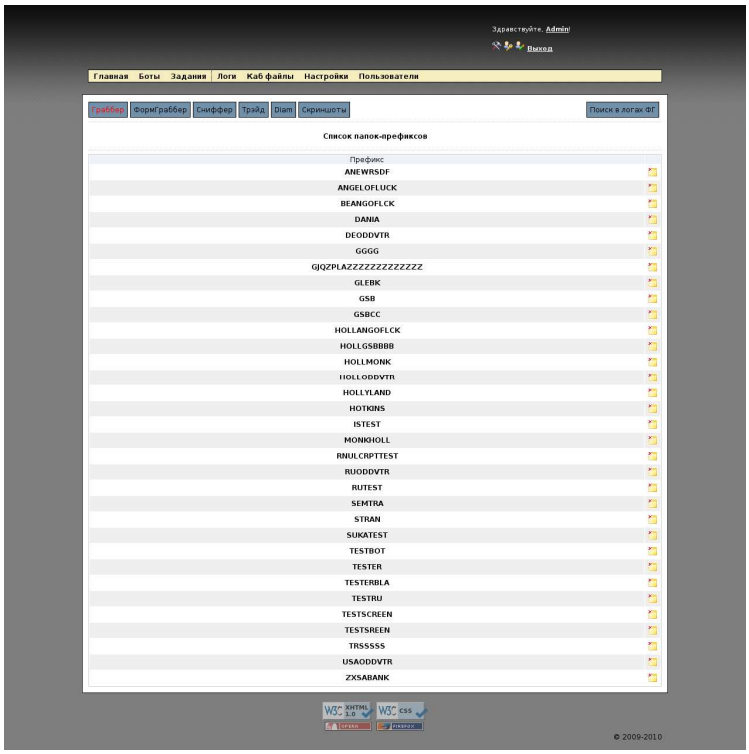
**Tipo de tarea:** Seleccionar de la lista o escribir un comando tipo *update*.
**País:** Escoger el país para la tarea. Puede ser cualquiera.
**Estado:** Seleccionar el estado de los bots que ejecutarán la tarea.
**Limitar a un número:** Limitar el número de bots que ejecutarán la tarea.
**Limitar bot:** Después de ejecutar esta tarea, el bot no ejecutará nuevas tareas si la opción está marcada.
**Botnet:** Seleccionar para qué botnet (config) es la tarea.
**Link:** Si la tarea requiere un link.

## Módulo de registros

El menú Logs es uno de los más importantes de Carberp, ya que da la posibilidad al botmaster de acceder a todo tipo de información relacionada a cada uno de los bots.

Está dividido en los siguientes submenús: **Grabber**, **Formgrabber**, **Sniffer**, **Trade**, **Diam**, **Screens**.

En grabber encontramos los logs de los bots capturados por el plugin "passw.plug". Al acceder nos encontraremos con la siguiente pantalla:




Observamos que está estructurado por las diferentes botnets que componen el C&C.

En este caso vamos a observar la botnet GSB, que es una de las que están operando actualmente.

***Figura 18 – Botnets del C&C***

Al seleccionar la botnet, se despliega la visualización de todos los registros de cada bot, ordenados por días y permitiendo además descargar una copia del archivo en texto plano (.txt).

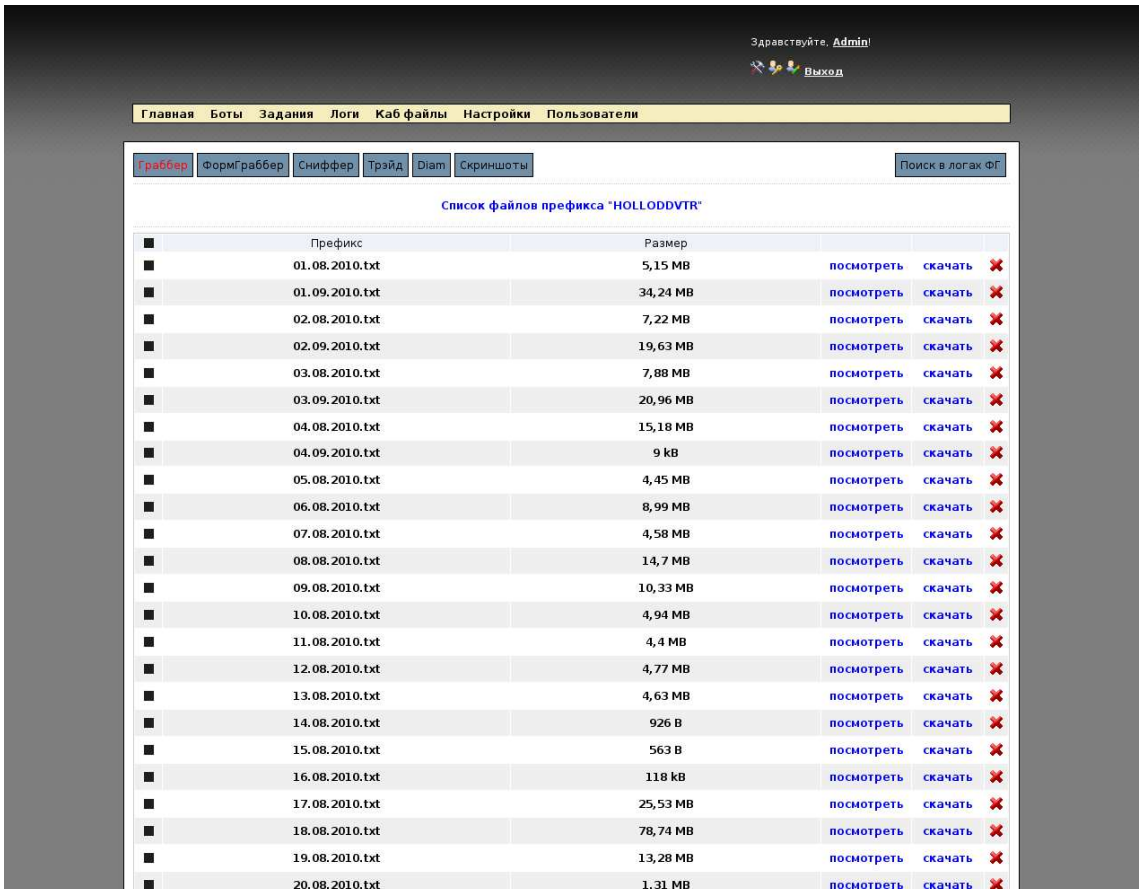



***Figura 19 – Logs del grabber de la botnet seleccionada***

Ejemplo de Log:

---

*#END##START#InternetExplorer#NAME#*
*http://www.werkspot.nl/@@@XXXXX@hotmail.com:XXXX*
*http://www.facebook.com/index.php@@@XXXX@hotmail.com:XXXXX*
*http://www.facebook.com/@@@XXXXXX@hotmail.com:XXXX*
*#END#*
*#START#WindowsLiveMail#NAME#*
*Email: XXXX@live.nl*
*Account name: Live (XXX)*
*Server (HTTP): http://mail.services.live.com/DeltaSync_v2.0.0/sync.aspx*
*Password (HTTP): XXXX*
*User (HTTP): XXX@live.nl*
*#END#*
*#START#Outlook#NAME#*
*Email: XXXX@walla.com*
*User (POP3): XXX*
*Password (POP3): XXX*
*Server (POP3): XXXX*
*User (SMTP): XXXX*
*Server (SMTP): XXXX*
*#START#WindowsLiveMessenger#NAME#*
*UIN/Name: XXXX@hotmail.com*
*Pass: XXXX (hex: XX XX XX XX XX XX)*
*…*

*UIN/Name: XXX@live.nl*
*Pass: XXXX (hex: XX XX XX XX XX XX)*
*#END###START#MozillaFirefox#NAME#*
*http://www.taringa.net@@@XXX:XXX*
*#END###START#GoogleChrome#NAME#*
*https://www.meneame.net/@@@XXXX:XXXX*
*https://www.megaupload.com/@@@XXXX:XXX*
*http://212.178.208.1:2189/@@@XXX:XXX*
*#END###START#CiscoVPNClient#NAME#*
*Host: vpn1.ocurrance.net*
*Password (Group): XXXX*
*Password (User): XXXX*
*...*
*Host: 65.121.79.100*
*Password (Group): XXX*
*Password (User): XXX*
---

## Módulo FormGrabber

En grabber solo se guardan credenciales, así pues, los formularios enviados a través de webs y que puedan contener información importante (también credenciales) son reportados al módulo formgrabber del C&C. Al entrar, al igual que en el módulo grabber, permite seleccionar los datos de interés de determinada botnet (logs).

En la siguiente imagen se observa la información de la botnet **ANGELOFLUCK**, que mantuvo su operatividad desde principios de agosto hasta mediados de septiembre del 2010.

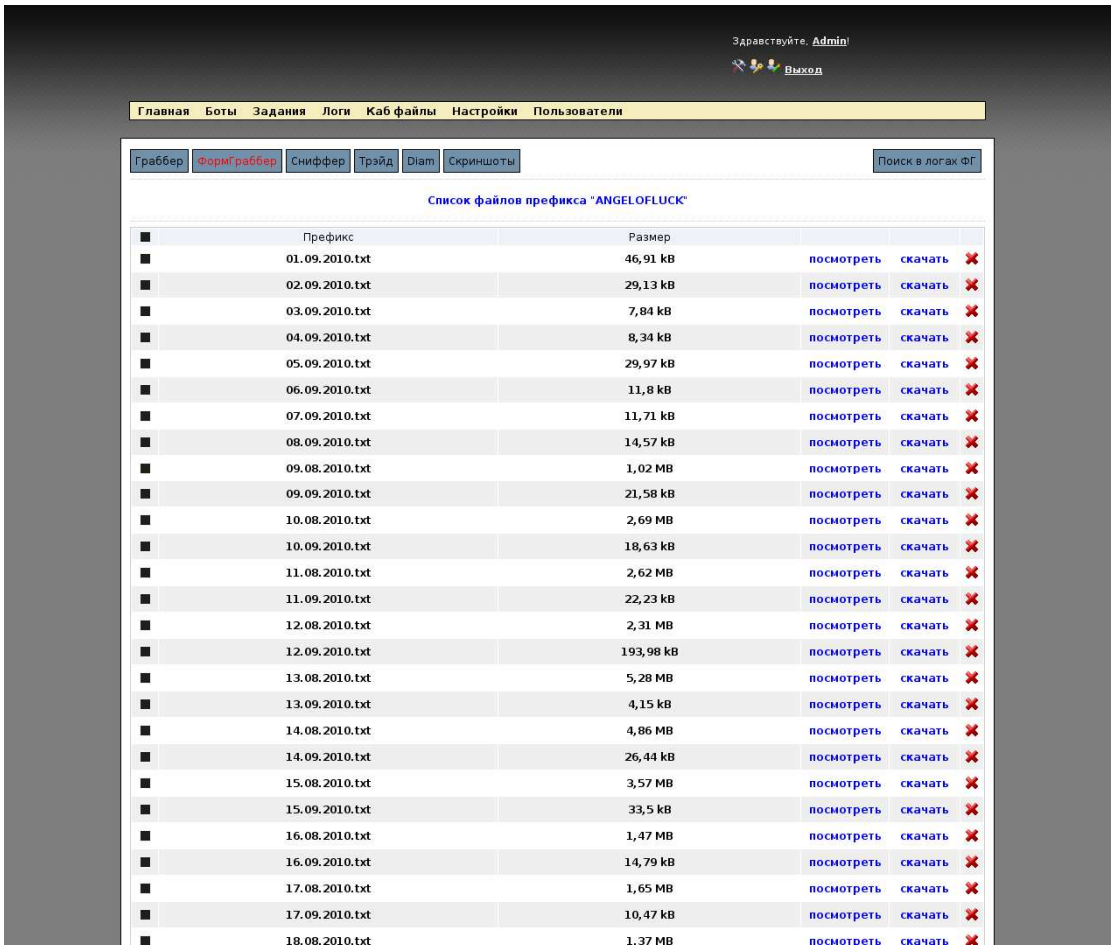



***Figura 20 – Logs del formgrabber de la botnet seleccionada***

Un ejemplo de logs del módulo formgrabber es:

*<ID: GSB09091D9E9F80646B382B7517FCEA64535 BROWSER: IE IP: 85.147.xx.xx 06.10.2010 00:00>*
*URL:*
*https://secure.hyves.org/?module=authentication&action=login&r=d05caa4d?|POST:auth_currentUrl=http://www.hyves.nl/?&auth_username=XXXXX&auth_password=XXXXX&login_initialPresence=offline&btnLogin=Ok*

*<ID: GSB0F3244F659C86233BE262C4FD5AE47A0C BROWSER: IE IP: 85.146.xx.xx 06.10.2010 00:00>*
*URL:https://www.google.com/accounts/ServiceLoginAuth?|POST:ltmpl=default&ltmplcache=2&continue=http://mail.google.com/mail/?&service=mail&rm=false&dsh=6624412014080959272&ltmpl=default&ltmpl=default&scc=1&timeStmp=&secTok=&GALX=qooCR-Zi_f8&Email=XXXXX&Passwd=XXXXX&rmShown=1&signIn=Aanmelden&asts=*

*<ID: GSB04290BD526B63AC08AB5A5F6928F89E17 BROWSER: IE IP: 83.163.xx.xx 06.10.2010 00:00>*
*URL:*
*https://bankieren.rabobank.nl/rib/rib.cgi?|POST:X009=REKSAL&X010=0020&X011=0&X012=XXXXX&X014=1&X015=REKMUT&I916=1000&V024=&V025=&V026=&V048=&V060=01*

*<ID: GSB08CE45588A3C7E77F6CF25AADB2D1877C BROWSER: IE IP: 83.85.xx.xx 06.10.2010 00:00>*
*URL: http://stats.ad-serverparc.nl/view-click/75_TUIdisplay/view.php?|POST:customer_id=XX&magic=a&sec=undefined&banner_id=6701&user_id=XXXX&timestamp=undefined*

*<ID: GSBR02A4D5F9F0970B9AFF9757D6B5899EB0 BROWSER: IE IP: 195.193.xx.xx 03.09.2010 13:42>*
*URL: https://www.bbva.es/DFAUTH/slod/DFServlet?|POST:origen=bbvanet&eai_user=XXXX-XXXXXXXXXX&eai_password=XXXX&eai_URLDestino=&idioma=CAS&eai_url_params=idioma=CAS*

*<ID: GSB024EEEC6F66FE3FA129C649EA4932C570 BROWSER: IE IP: 80.56.XX.XX 03.10.2010 00:02>*
*URL:*
*http://www.vueling.com/booking/booking/selecciona-tu-vuelo?*
*POST:event=search&module=SB&page=SEARCH&language=ES&mode=&sid=&ref=&travel=1&from1=AMS&to1=VLC&from2=&to2=&departDay1=08&departMonth1=201010&displayDate1=vrijdag 08 oktober,*
*2010&depart1FlexBy=0101&departDay2=08&departMonth2=201010&displayDate2=vrijdag 08 oktober, 2010&depart2FlexBy=0101&fechas=0101&ADULT=1&defaultADULT=-1&CHILD=0&defaultCHILD=-1&INFANT=0&defaultINFANT=-1&toCity1=&toCity2=???&departDate1=20101008&departDate2=&numberMarkets=1&cualquier=&nom_cualquier=&m1_cualquier=&m2_cualquier=&frdisc=&mode_orig=&mode_TESTAB=MCYfUBAoU1Q5LFx9eXUwUDcsSw==&mode_TESTABClassB=MQYlGxIeU1Q5IjRof2M0P1A6Jw==*

*<ID: GSB03C52630D7838733D83CD4ED740DB9B74 BROWSER: IE IP: 83.XX.XX.XX 03.10.2010 00:00>*
*URL:*
*https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsnv=11&ct=1286053261&rver=6.0.5285.0&wp=MBI&wreply=http://mail.live.com/default.aspx&lc=1043&id=64855&mkt=nl-NL&bk=1286053262?|POST:login=xxxx@live.nl&passwd=xxxxxxx.&type=11&LoginOptions=3&NewUser=1&MEST=&PPSX=P&PPFT=CYsd7xunc8kCcY2fbzhyBuBTwB59MN!n3DoxYtaFgZFAQyMEb5O2JCczyzeEZ29u3cOhMxkDb4mOKhZjbm7I4Vgeq3wQEUScKoH2gVIDxGT&idsbho=1&PwdPad=&sso=&i1=1&i2=1&i3=12176&i4=&i12=1*

## Módulo Sniffer

En este módulo al igual que en los anteriores, permite seleccionar la botnet de la cual se desea consultar los logs.

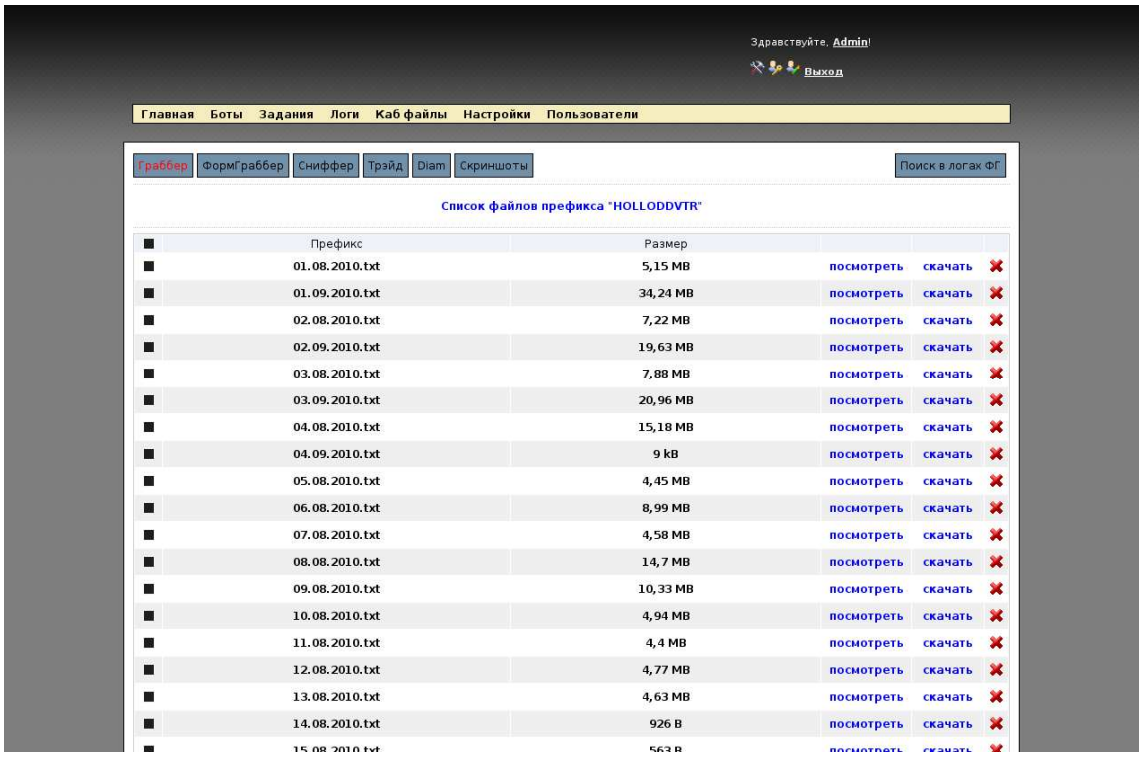



***Figura 21 – Logs del sniffer de la botnet seleccionada***

Estas credenciales robadas juegan un papel importante a la hora de propagar el código malicioso de la botnet. El botmaster usa las credenciales para embeber etiquetas iframes en aquellos FTPs que alojan sitios webs.

Este iframe oculta un código malicioso que direcciona el tráfico web hacia un TDS, que a su vez, dependiendo de unos factores configurados por el botmaster, redirige a la víctima hacia un Exploit Pack.

Ejemplo de log:

ftp://xxxxxx:xxxxxx@webserver2.xhosting24.de:21
ftp://xxxxxx:xxxxxx@host1.nicheprofitclassroom.com:21
ftp://xxxxx:xxxxx@home.arcor.de:21
ftp://xxxx:xxxx@rchgsa.rchland.ibm.com:21
ftp://xxxx:xxxx@www.articorg.com:21
ftp://xxxx:xxxx@www.articorg.com:21

ftp://xxxxx:xxxx@postrigan-241.colo0.kv.wnet.ua:21
ftp://xxxxx:xxxx@red-bolivar.com:21
ftp://xxxx:xxxx@legacy.z8.ru:21
ftp://xxxxx:xxxxx@sgae.es:21

## Módulo trade

Como se mencionó líneas arriba, aparte de registrar las credenciales de sitios web, Carberp incorpora una lista de aplicaciones de las cuales es capaz sustraer sus credenciales. En este módulo, se muestran las credenciales extraídas de aquellas aplicaciones relacionadas con el E-Commerce.

Al acceder se visualizan las botnets que contienen registros E-Commerce. Una vez seleccionada la botnet, muestra todos los logs encontrados.

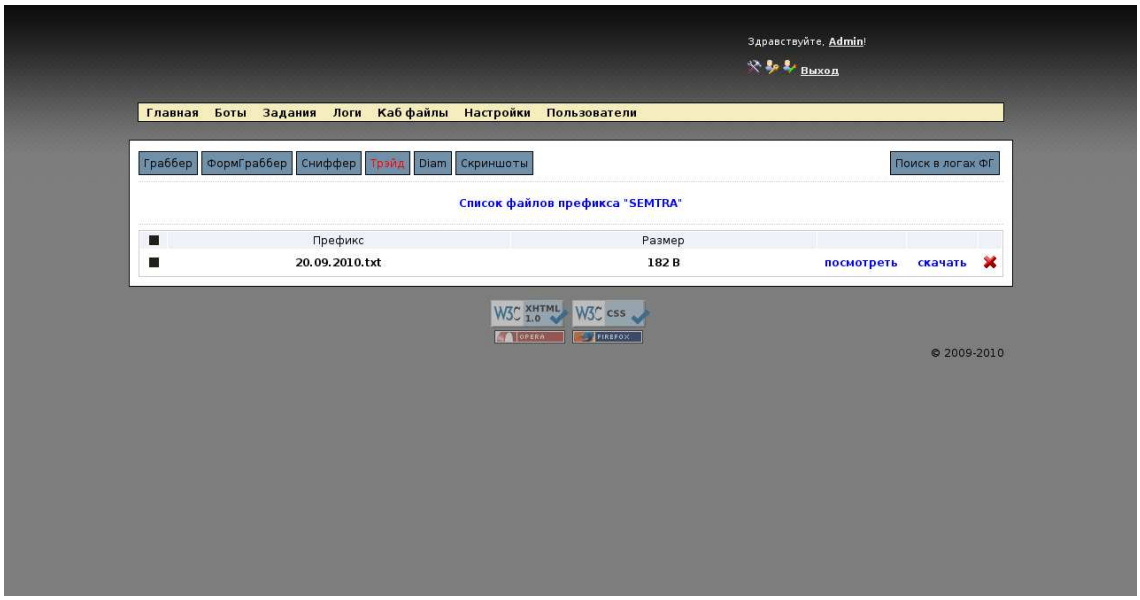



***Figura 22 – Logs de aplicaciones de E-Commerce de la botnet seleccionada***

Ejemplo de logs E-Commerce:

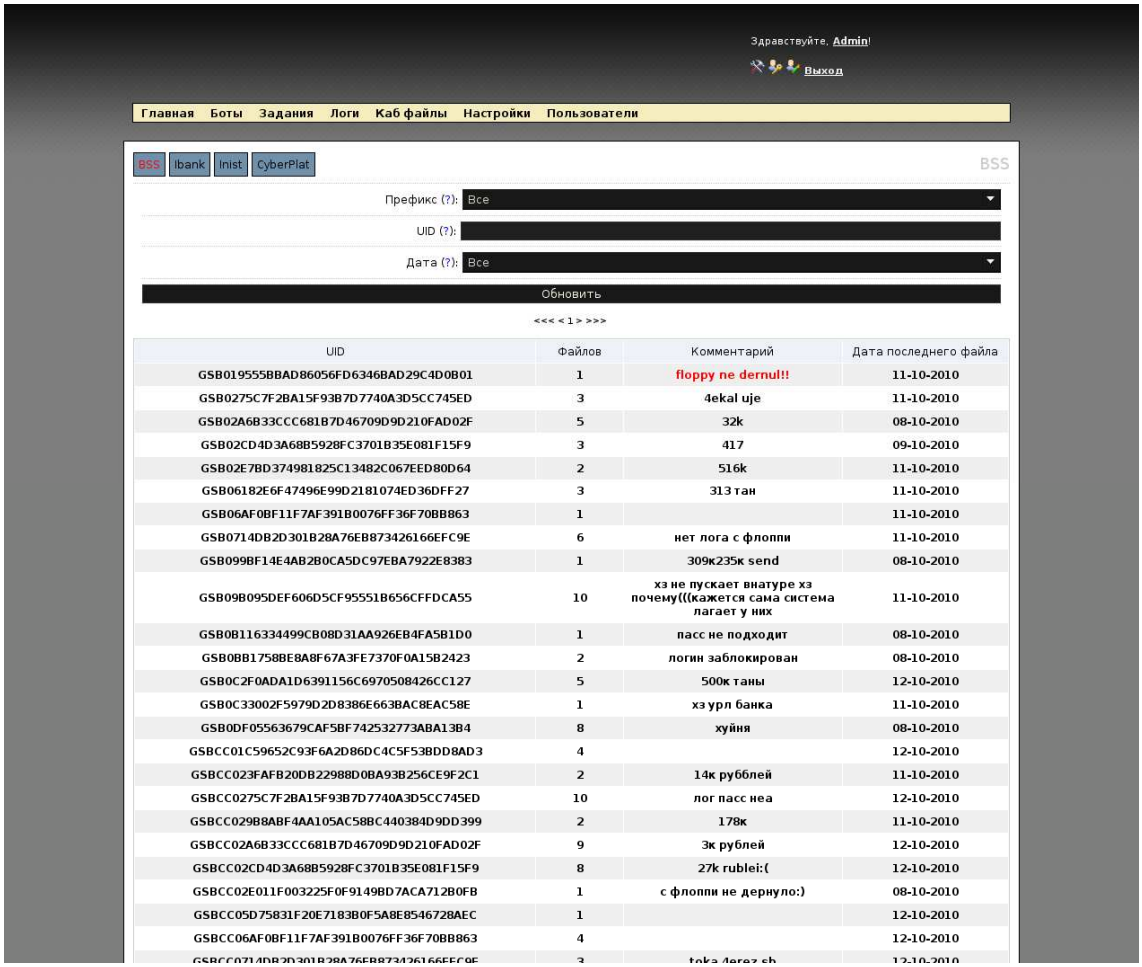
*<ID: EBNKUSDV0891F1FCA477CA7885FB2A83459ADFFA6 IP:87.68.XX.XX 23.09.2010 13:54>*
*Program: SaxoTrader*
*Username: XXX*
*Password: XXX*
*AccountNO: XX*
*Server: XXX*
*<ID: EBNKUSTR051205DBE501882B726E59DE3E2B405FA IP:79.XX.XX.XX 20.09.2010 14:53>*
*Program: ScotTrader*
*Username: XXX*
*Password: XXX*
*AccountNO: XXX*
*Server: XXX*
*<ID: EBNKUSTR051205DBE501882B726E59DE3E2B405FA IP: 109.XX.97.XX 25.09.2010 14:57>*
*Program: BlackwoodPRO*
*Username: XXX*
*Password: XXX*
*AccountNO: XXX*
*Server: XXX*
*<ID: EBNKUSTR051205DBE501882B726E59DE3E2B405FA IP: 91.XX.XX.XX 26.09.2010 15:01>*
*Program: FinamDirect*
*Username: XXX*
*Password: XXX*
*AccountNO: XXX*
*Server: XXX*

## Archivos CAB

La última actualización de Carberp amplió la opción de iBank a este menú de Archivos Cab. En el mismo se encuentra toda la información relacionada con el robo de certificados, keys y credenciales bancarias que se guardan en archivos .CAB. Esta opción transforma a Carberp en un bank-trojan muy peligroso.

## BSS

Los .cab de BSS contienen un archivo llamado *Information.txt* que contienen las credenciales robadas en la petición al bsi.dll y otros dos archivos con las key pública y privada. Como podemos observar, por cada bot hay un campo donde el botmaster va dejando sus comentarios.




| UID | Файлов | Комментарий | Дата последнего файла |
|---|---|---|---|
| GSB019555BBAD86056FD6346BAD29C4D0B01 | 1 | floppy ne dernul!! | 11-10-2010 |
| GSB0275C7F2BA15F93B7D7740A3D5CC745ED | 3 | 4ekal uje | 11-10-2010 |
| GSB02A6B33CCC681B7D46709D9D210FAD02F | 5 | 32k | 08-10-2010 |
| GSB02CD4D3A68B5928FC3701B35E081F15F9 | 3 | 417 | 09-10-2010 |
| GSB02E7BD374981825C13482C067EED80D64 | 2 | 516k | 11-10-2010 |
| GSB06182E6F47496E99D2181074ED36DFF27 | 3 | 313 тан | 11-10-2010 |
| GSB06AF0BF11F7AF391B0076FF36F70BB863 | 1 | | 11-10-2010 |
| GSB0714DB2D301B28A76EB873426166EFC9E | 6 | нет лога с флоппи | 11-10-2010 |
| GSB099BF14E4AB2B0CA5DC97EBA7922E8383 | 1 | 309к235к send | 08-10-2010 |
| GSB09B095DEF606D5CF95551B656CFFDCA55 | 10 | хз не пускает внатуре хз почему(((кажется сама система лагает у них | 11-10-2010 |
| GSB0B116334499CB08D31AA926EB4FA5B1D0 | 1 | пасс не подходит | 08-10-2010 |
| GSB0BB1758BE8A8F67A3FE7370F0A15B2423 | 2 | логин заблокирован | 08-10-2010 |
| GSB0C2F0ADA1D6391156C6970508426CC127 | 5 | 500к таны | 12-10-2010 |
| GSB0C33002F5979D2D8386E663BAC8EAC58E | 1 | хз урл банка | 11-10-2010 |
| GSB0DF05563679CAF5BF742532773ABA13B4 | 8 | хуйня | 08-10-2010 |
| GSBCC01C59652C93F6A2D86DC4C5F53BDD8AD3 | 4 | | 12-10-2010 |
| GSBCC023FAFB20DB22988D0BA93B256CE9F2C1 | 2 | 14к рубблей | 11-10-2010 |
| GSBCC0275C7F2BA15F93B7D7740A3D5CC745ED | 10 | лог пасс неа | 12-10-2010 |
| GSBCC029B8ABF4AA105AC58BC440384D9DD399 | 2 | 178к | 11-10-2010 |
| GSBCC02A6B33CCC681B7D46709D9D210FAD02F | 9 | 3к рублей | 12-10-2010 |
| GSBCC02CD4D3A68B5928FC3701B35E081F15F9 | 8 | 27k rublei:( | 12-10-2010 |
| GSBCC02E011F003225F0F9149BD7ACA712B0FB | 1 | с флоппи не дернуло:) | 08-10-2010 |
| GSBCC05D75831F20E7183B0F5A8E8546728AEC | 1 | | 12-10-2010 |
| GSBCC06AF0BF11F7AF391B0076FF36F70BB863 | 4 | | 12-10-2010 |
| GSBCC0714DB2D301B28A76EB873426166EFC9E | 3 | toka 4erez sb | 12-10-2010 |

***Figura 23 – Logs de BSS con comentarios del botmaster***

**Estructura del CAB**


***Figura 24 – Estructura del cab de BSS***

## IBank

Este complemento también tiene el archivo *Information.txt* con las credenciales del software iBank y derivados. Además añade una captura de pantalla en el momento de hacer login.

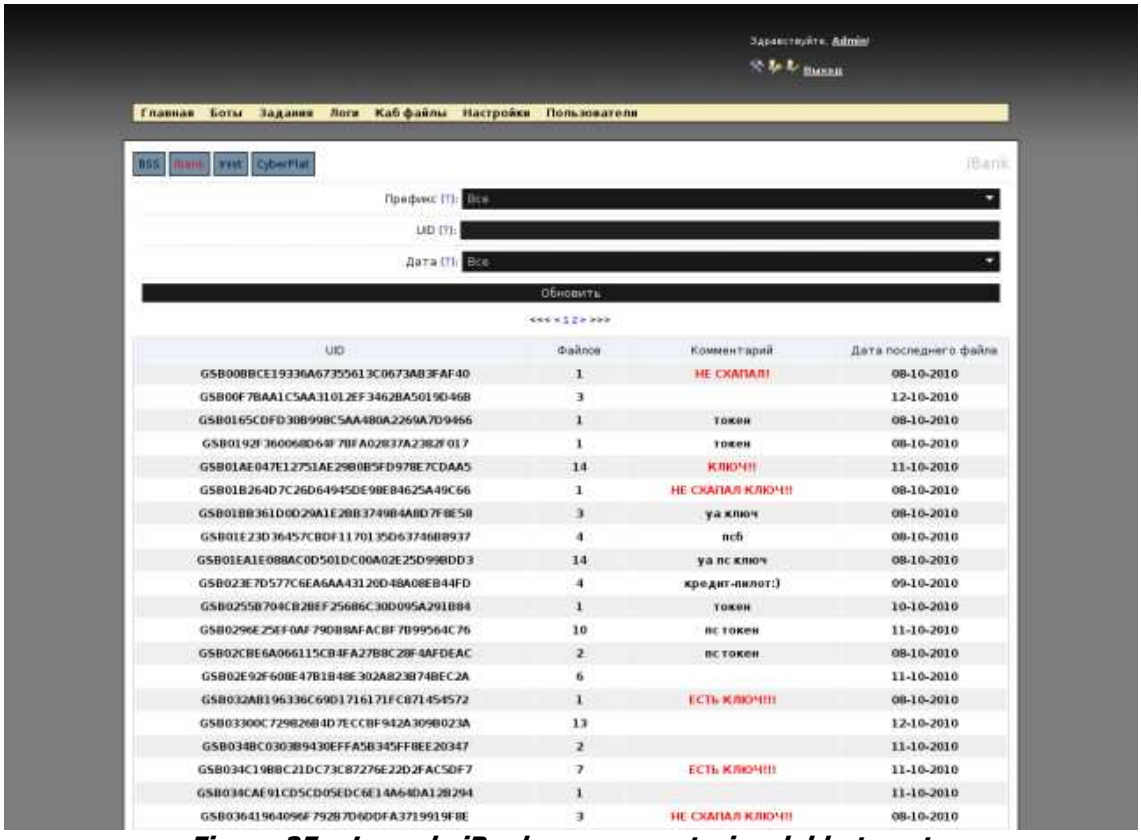



***Figura 25 – Logs de iBank con comentarios del botmaster***

## Estructura del CAB

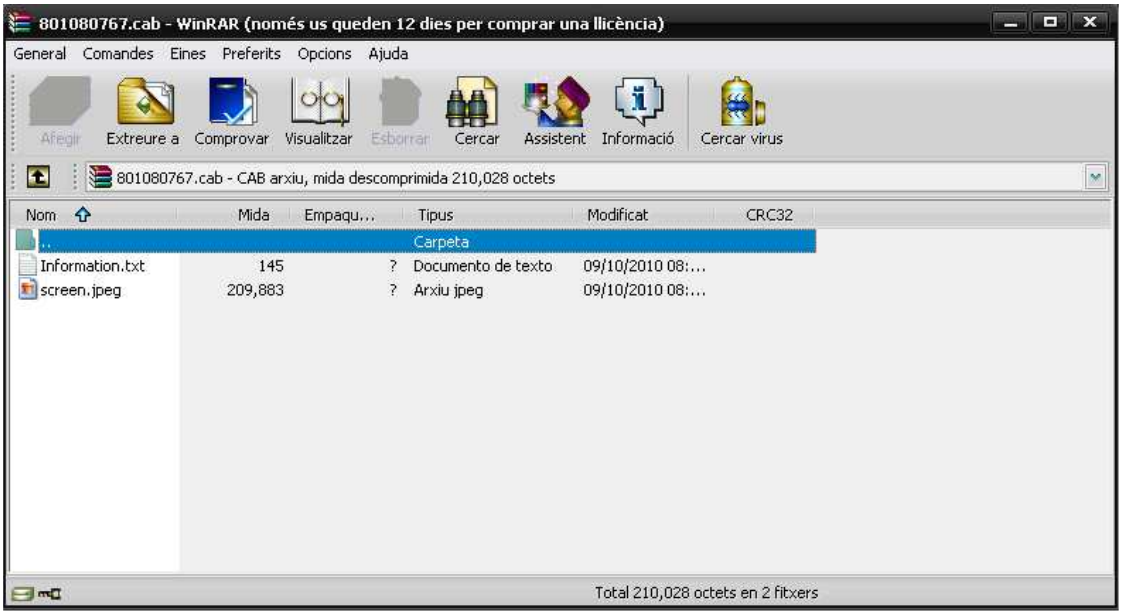



***Figura 26 – Estructura del archivo CAB de iBank***

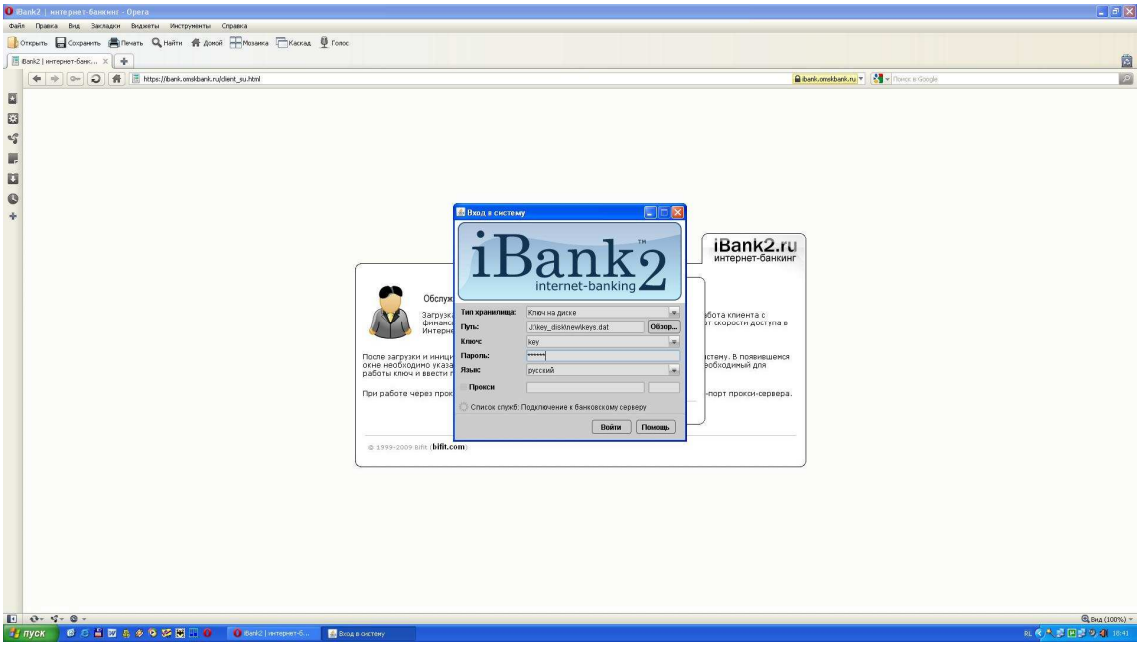



***Figura 27 – Captura de pantalla alojada en el CAB***

## CyberPlat

Igual que en iBank, contienen las credenciales de este sistema de pago en el *Information.txt* y guarda una captura de pantalla en el momento de login. Además, también contiene la *secret.key* usada en el momento del login.

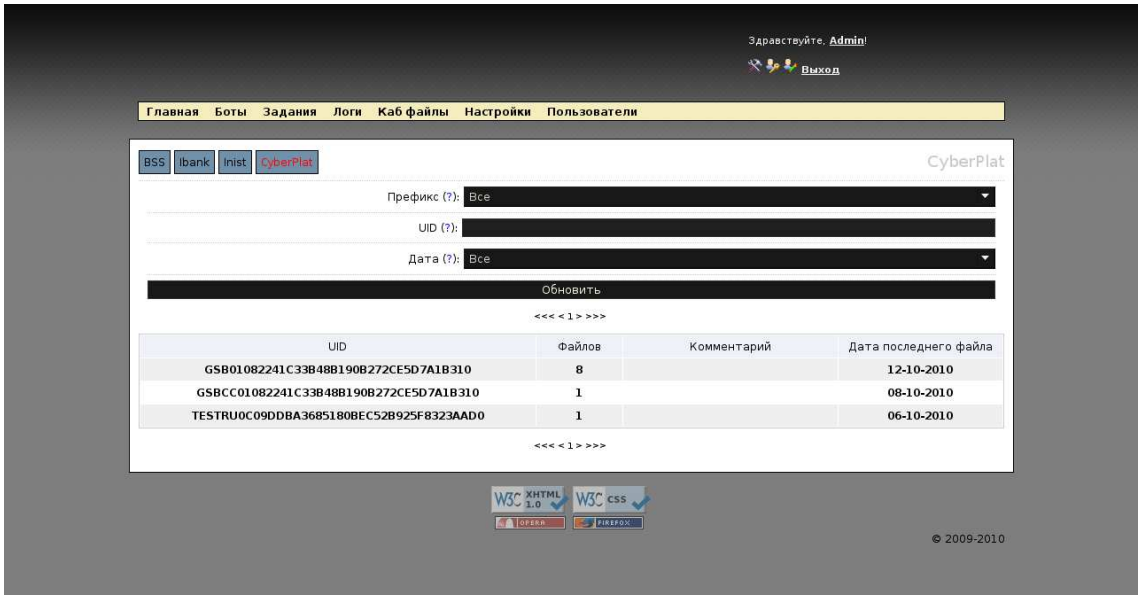



***Figura 28 – Logs de CyberPlat***

### Estructura del CAB


***Figura 29 – Estructura del cab de Cyberplat***

A los archivos cab, también hay que unir el hecho de que Carberp al igual que sus competidores cuenta con un sistema back-connect (comando *startsb*) que permite al botmaster realizar las operaciones bancarias desde el mismo ordenador de la víctima.

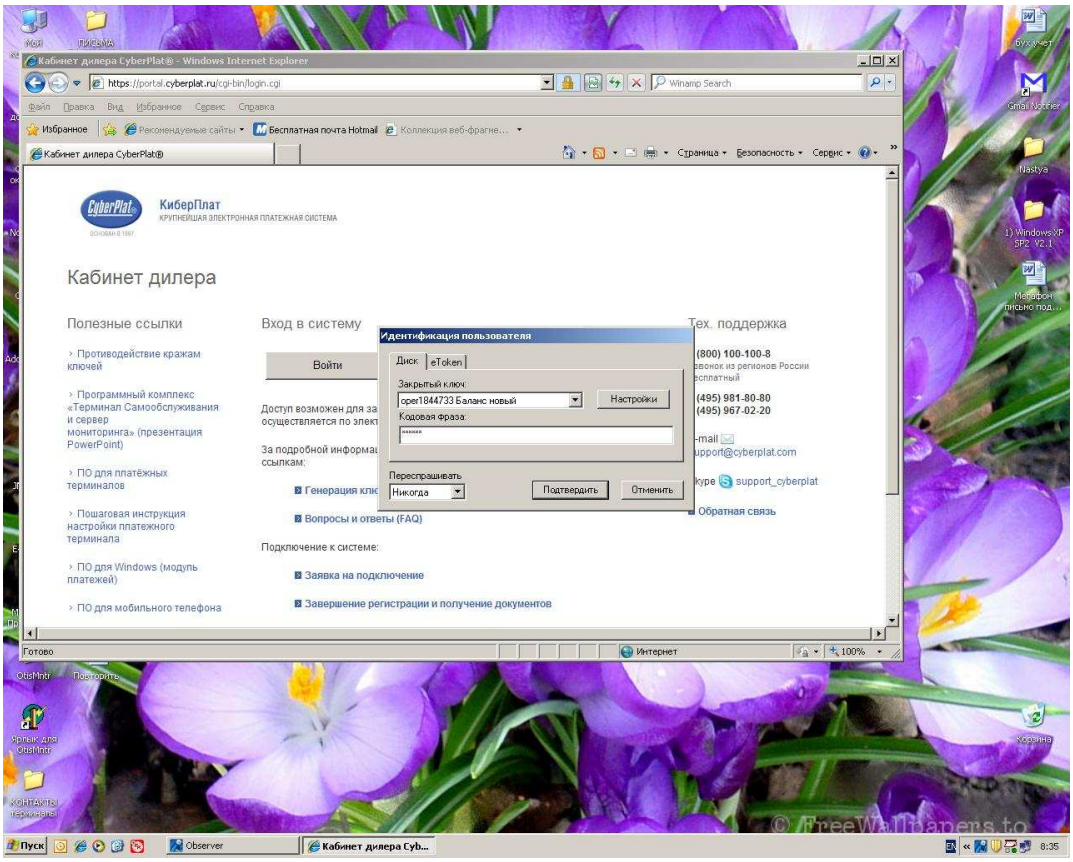



***Figura 30 – Captura de pantalla de CyberPlat***

## Screens

En esta opción del menú se puede acceder a las capturas de pantalla realizadas en los sistemas operativos infectados. Estás capturas de pantalla se realizan cuando se detecta que el sistema víctima está visitando una URL pre-definida, normalmente relacionadas con la banca online.

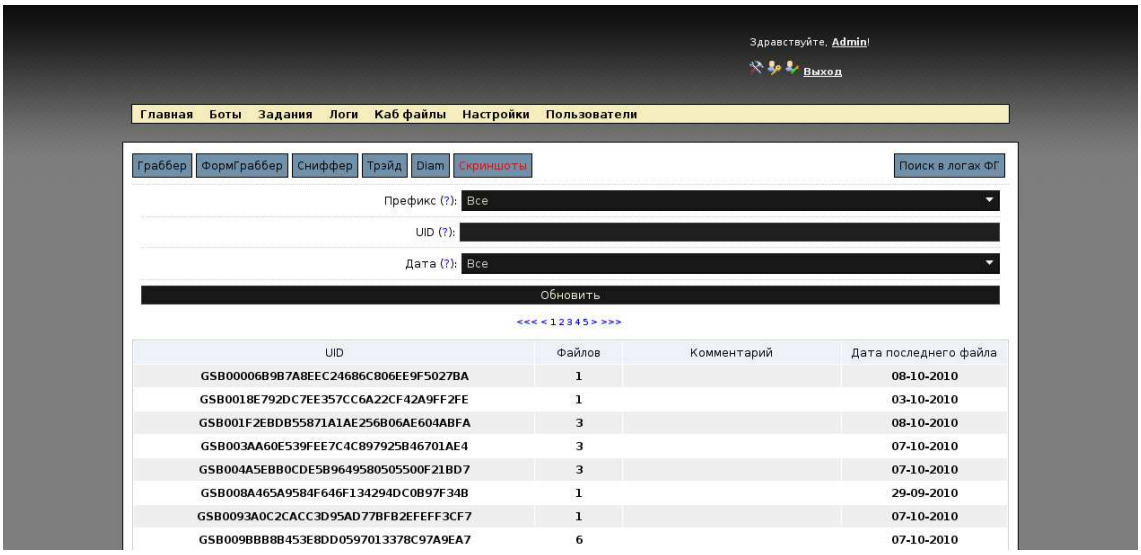



***Figura 31 – Logs de screens***

# Conclusión

Carberp ha entrado por la puerta de atrás sin hacer mucho ruido, por ejemplo a diferencia de SpyEye que entró llamando la atención de todos. Esto ha sido gracias a su distribución como una botnet privada y a que su adquisición no posible a través de foros underground ya sean estos públicos o privados, sino que parece distribuirse por intermedio de contactos de confianza.

Esta forma de distribución le ha permitido operar muchos meses casi desde la oscuridad consiguiendo ratios de infección muy elevados (500.000 bots por mes). Recordemos que Carberp ha estado operando desde principios de 2010 y no ha sido hasta septiembre que han aparecido las primeras informaciones de la mano de algunas compañías de antivirus.

Sin embargo, cuando más parecía que este nuevo malware entraba en el mundo del crimeware para quedarse, los principales C&C han ido desapareciendo poco a poco. El motivo de su desaparición es desconocido y da a todo tipo de especulaciones, ya que esta botnet recibía actualizaciones por parte de sus creadores mensualmente y lejos estaba de ser considerado un crimeware desatendido.

# ¡Actualización importante!

En los últimos días hemos estado recibiendo algunas noticias que referencian actividad de algunos C&C de Carberp aún operativos. Si bien es cierto que aún quedan algunos C&C activos, estos operan al margen del desarrollo original de Carberp y solo se trata de algunos botmaster que, a pesar de no tener actualizaciones, siguen usando versiones antiguas del crimeware.

También ha aparecido una *nueva versión* de Carberp, de la cual se habla en: http://blog.seculert.com/2011/01/new-trend-in-malware-evolution.html

Sin embargo, es necesario mencionar que, si bien esta versión puede tratarse de la continuación, hay varios motivos que nos hacen desconfiar de que se trate la última versión de Carberp.

El primero de ellos es que el sistema interno de administración y desarrollo de Carberp está totalmente fuera de servicio en estos momentos. Este sistema quedó fuera de servicio casi al mismo tiempo que desaparecieron los C&C y era el encargado de proporcionar las licencias y los paquetes de Carberp.

El segundo motivo es que solo hay un C&C operativo con esta versión. Carberp era un sistema privado, pero aunque su objetivo no fuera la comercialización a gran escala, este era comercializado cada vez más y esto no se corresponde con solo encontrar un C&C.

Así una de las opciones que toman más validez, es que quizás esta versión del crimeware haya sido desarrollada con la última versión oficial del bot al margen del equipo de Carberp.

**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