PandaLabs Bulletins:

Bank details uncovered

Index

1.- Introduction

Banker Trojans continue to represent a serious threat to users. Even though many banks have increased security measures on their websites, these malicious codes have become more sophisticated and include new functions.

One of the greatest concerns to users regarding Internet security is the theft of confidential information, such as passwords, particularly those for bank accounts. That's why banker Trojans are considered one of the most dangerous types of malware for Internet users, as they are designed precisely to steal this type of information.

Banker Trojans, along with fake antivirus programs which we also discuss in this report, would appear to have become the most profitable categories of malware for cyber-criminals.

Social engineering continues to be among the most popular means for distributing this type of malware on users' computers. However, user interaction is not always required, as malware can also be distributed through web pages with kits for installing malware through exploits.

Once installed on a computer, the main aim of all these Trojans is to steal bank details from victims. The Trojans normally go memory-resident, and only activate when users visit the web pages of certain banks. To this end, the Trojans include a list of banks which they can target.

These programs are readily available to cyber-criminals, as there is an extensive black market in *a la carte* Trojans and banking malware kits, allowing users not only to create Trojans with multiple functionalities but also to control them and even send them new instructions.

Among other things, this bulletin examines the main banker Trojan families, explaining how these codes normally enter computers and how they steal information, and analyzing the complex structure that is behind this lucrative criminal business. We also offer a series of recommendations on how users can protect themselves from these threats.

2.- Main families

There are many different families of banker Trojans although, broadly speaking, the most active families fall within three categories:

1) Brazilian banker Trojans (Banbra, Bancos)

These are designed principally for stealing passwords to Brazilian and Portuguese banks, although the "Bancos" family also targets Spanish banks occasionally. They normally transmit the information obtained through FTP or email.

The difference between the families lies in the programming language. Banbra uses Delphi, while Bancos is programmed in Visual Basic.

Unlike other families, they are not created with Trojan generator kits but are programmed individually.

2) Russian banker Trojans 1.0 (Cimuz, Goldun…)

There are many variants of these families, as they are often designed using Trojan creation kits. However the differences between variants created with these tools are minimal, as the kits have not been updated over the last few years.

One consequence of this is that the variants of these families of Trojans do not contain new functions, making them relatively simple to detect with antivirus solutions.

3) Russian banker Trojans 2.0 (Sinowal, Torpig, Bankolimb)

Currently, some of these are the most active families, and as they are continually changing and being updated with the capacity to steal credentials from different banks, they are also the most dangerous. This makes it difficult for antivirus solutions to detect them generically.

All of them have one common function: The list of target banks and organizations is obtained from a configuration file, which can either be included with the Trojan or in a server controlled by the cyber-criminal, so the Trojan itself does not need to be modified in order to add a new target bank. They also use stealth and polymorphic techniques to make detection more difficult.

As can be seen in the following diagram, the most active banker Trojan families are Sinowal, representing 46% of the families designed to steal bank details, followed by Banker at 25% and Banbra at 11%. The remaining 18% corresponds to the rest of the banker Trojan families:

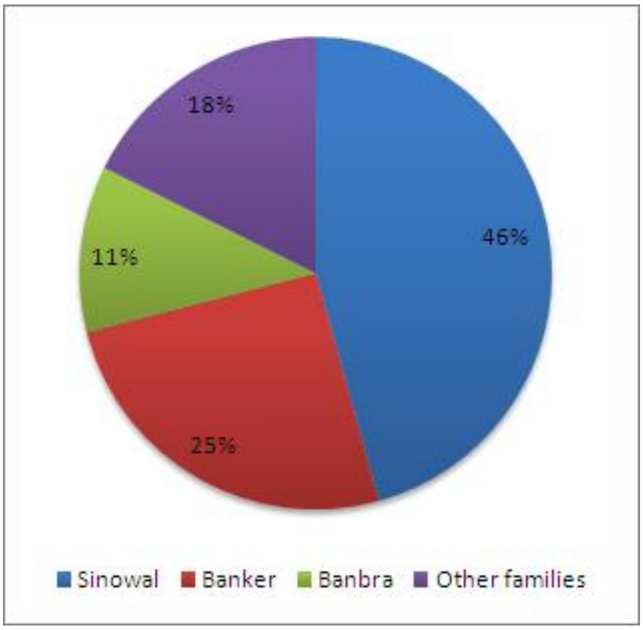


Fig.1 Distribution of banker Trojan families during 2008

3.- Infection channels

Social engineering continues to be among the most popular means for spreading this type of malware on users' computers, and it is often distributed in one of two types of spam messages:

1. Spam with an attachment. These are normally compressed files, with a .zip extension, containing an executable file. However, to trick users into thinking the files are inoffensive, the following techniques are used:

- Inoffensive icon. The icon of the file coincides with the type of file that the attachment claims to be. So in the case of an image, for example, the icon would be as follows:

Fig.2 Image icon

- Double extension. Often, the executable file has a double extension. The first extension is that of the type of file that the attachment claims to be, so in the case of an image it could be .jpg, and the second extension would be .exe. There is normally a gap between the two extensions to prevent users from discovering that the real extension is .exe.
  However it is not always necessary to add an inoffensive extension. If the attachment has an icon that is apparently harmless, users may not pay much attention to the extension itself.

Very often, the file executed by the user is a Downloader-style Trojan. These are small files designed simply to connect to a web page to download the real banker Trojan.

2. Spam with links to a web page.

These messages often carry links supposedly pointing to a video on the web. When users click to see the video, they are often prompted to install something such as a codec or flash update, etc.

Once the download is made, to allay any suspicions, users may even be taken to a web page where they can see a video, although this is not always the case.

In the section on the leading banker Trojans, we will also take a look at examples of spam messages used to distribute them.

However, early this year we began to see the popularization of a more sinister technique: the infection of legitimate websites. Code is inserted into the web pages which calls and supplies information to a malicious server about the user's operating system, browser and patches installed in order to exploit vulnerabilities and insert malware including banker Trojans.

4.- How do they steal information?

Hackers use several techniques to steal passwords, from capturing data using keyloggers, to highly sophisticated techniques, capturing data "on-the-fly".

Keyloggers' success depends on the way they are configured, and most of all, on their capacity to filter information. Keyloggers recording all users' keystrokes would generate vast amounts of information that is useless to cyber-crooks.

Consequently, it is important for keyloggers to record only the information cyber-crooks are interested in, in short, users' bank details.

The information must therefore be filtered, according to the web pages visited by users. Trojans therefore monitor users' browsing habits, and are activated when users access the web pages of specific banks.

To do so, Trojans are either in possession of, or download, a list with several strings that can be part of a web address, text strings belonging to a dialog box or the window title of bank pages. The Trojans monitor the system activity and are activated on detecting the filter strings.

Hackers use several techniques to monitor users' browsing habits:

- Register as a BHO (Browser Helper Object), an Internet Explorer function that is run on accessing the browser.

- Search for window titles. To do so, it uses the API's FindWindow function, which searches for windows with a specific title. This way, cyber-crooks can search for active window titles containing the bank names.

- Search for web addresses in the browser. The Trojan has a list of web addresses belonging to different banks. When users type an address in the browser which coincides with an address on the list, the Trojan is activated.

Once hackers detect the user is accessing an online bank, they try to obtain the user's bank details using the following techniques:

- Form capture: when the Trojan detects a form on a web page, it records the information entered by the user.
- Keylogging: Capturing of users' keystrokes on web pages.
- False pages: the Trojan creates a false page that simulates the original. When users try to access the bank's legitimate site, the Trojan runs an application that displays a false web page instead of the original.
- False forms: This technique consists of creating a false web page, by superimposing a window with a false form similar to the original.
- Additional fields in forms: Injects HTML code in the forms of false pages to request more information.
- Pharming: This involves modifying the domain name resolution system (DNS) to redirect users to false web pages.
- "Man-in-the-middle" attacks: cyber-crooks act as intermediaries, reading, inserting and modifying messages between the client and the bank without their knowledge.

5.- The sophistication of banker Trojans

Banks have responded to the threat of banker Trojans, improving security and client authentication procedures. In consequence, the techniques used by this type of malware to steal information have in turn become more sophisticated.

The use of virtual keyboards for user verification was an important step forward for these secure web pages, as it prevented keyloggers from capturing the data entered by users.

However, it was not long before malware creators developed new functions for banker Trojans, enabling them to trace the movements of the mouse or even make video captures of the screen, as in the case of Trj/Banbra. DCY.

Some strains of malware, such as those of the BankoLimb family, have a file with a list of URLs of target banks. When users infected with BankoLimb access a web page in the list, the Trojan is activated and injects HTML code in the bank’s page.

The result is that users are prompted to provide more information than they normally do when registering. The user is actually on the legitimate web page but it has been slightly modified. For this reason users should be alert to anything out of the ordinary on their bank's web page, because as in this case, any additional information provided will be captured.

In other cases, Trojans can superimpose a fake page over the original or simply redirect users to a spoof website. Once the information has been captured, victims may see an error message or are sometimes even taken to the genuine website of the bank.

Some variants of the Sinowal family are highly sophisticated, and are capable of modifying data ‘on-the-fly’. For example, if the user is carrying out a transfer from his bank's web page, these variants can alter the data of the intended recipient of the transfer once a petition has been made. The result of the operation returned to the user includes the original data, thus avoiding any suspicion.

Other variants consult a server to check whether they should take any action depending on the web pages that the user is visiting. This means malicious code does not depend on a configuration file and cyber-crooks can extend the list of websites from which they steal information or inject code, etc.

Once information has been stolen, it is often transmitted via email or posted to an FTP server.

6.- Organized crime

The creators of banker Trojans that steal confidential information are rarely the same individuals that actually steal money. The criminal business model that has evolved around this type of malware is highly complex.

The following diagram illustrates the complexity of the typical structure behind this kind of activity:

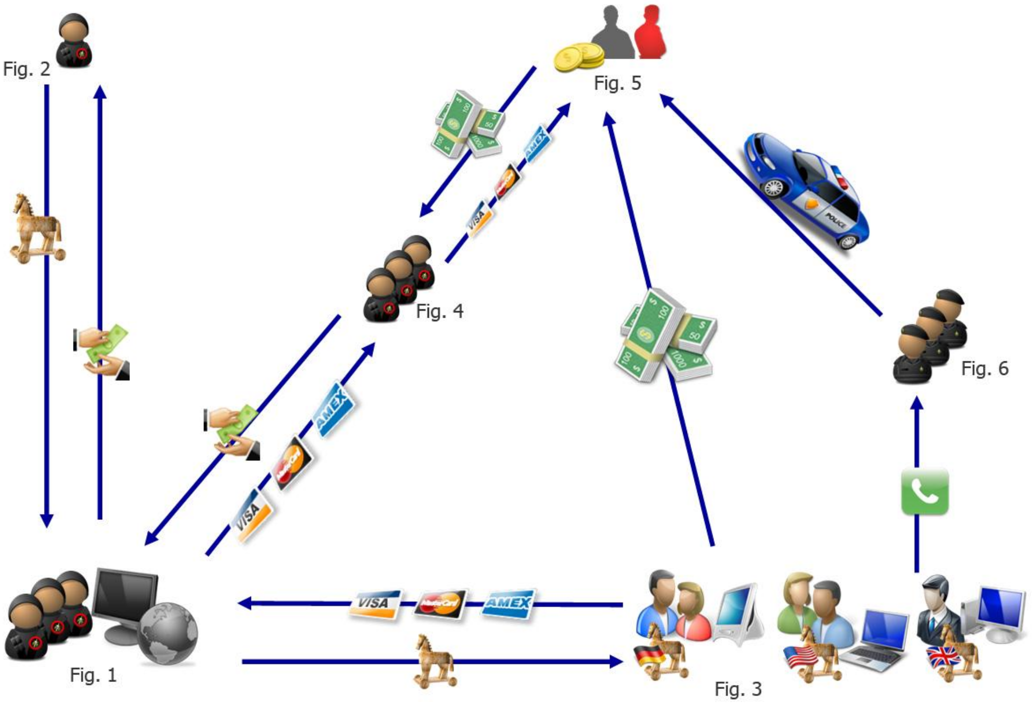


Fig.3 Organized cyber-crime

Firstly, groups of cyber-criminals (fig. 1) commission a purpose-built Trojan with specific characteristics from specialized forums or the malware black market (fig. 2). They may even rent the entire infrastructure needed to distribute the Trojan, either via spam or malware servers using drive-by-download techniques. Through this technique, files can be automatically downloaded to computers by exploiting system flaws without users' knowledge.

Once they have the Trojan, it is distributed to users to steal their bank details (fig. 3). To this end, the most common distribution methods are spam or infected web pages.

The technique for infecting legitimate web pages involves modifying the source code, by adding an iframe-type reference to a malicious server.

These criminals do not steal money directly from users, they steal their bank details which are sold on to others (fig. 4). This makes it even more difficult for law enforcement agencies to follow the trail.

All of the data stolen is sold on the malware market. However, neither do those who buy the stolen bank details actually steal the money. To cover their tracks yet further, they contract other people who act as intermediaries -money mules (fig.5)-, contracted under the pretext of working from home.

The money stolen is transferred to the accounts of the money mules, who keep around 3-5% of the amount transferred and then use a pay-platform or other anonymous form of sending money to send the money on to the real criminals. When the crimes are reported to the police, the only live trail leads directly to the money mules.

This means that everyone wins, except of course the victims and the money mules, who will be held as the only responsible party.

7.- The most important malware samples

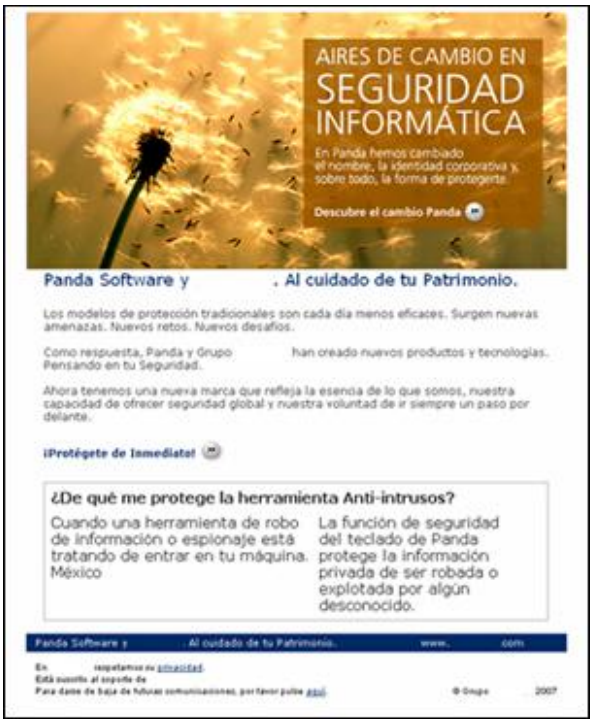
This section includes the most important malware samples according to their features or the emails used for their distribution.

BANCOKILL.A

Detected in August 2007, BancoKill.A was distributed through an email that reported an alleged collaboration between Panda Software and a Mexican bank, to protect its clients from possible threats.

The message could not be more deceitful, as it offered a tool, designed especially for users of a certain bank, to protect against threats. On trying to download this tool, users were really downloading a Trojan designed to steal bank details.

The message in which it was distributed was:



AIRES DE CAMBIO EN SEGURIDAD INFORMÁTICA

En Panda hemos cambiado el nombre, la identidad corporativa y, sobre todo, la forma de protegerte.

Descubre el cambio Panda

Panda Software y . Al cuidado de tu Patrimonio.

Los modelos de protección tradicionales son cada día menos eficaces. Surgen nuevas amenazas. Nuevos retos. Nuevos desafíos.

Como respuesta, Panda y Grupo han creado nuevos productos y tecnologías. Pensando en tu Seguridad.

Ahora tenemos una nueva marca que refleja la esencia de lo que somos, nuestra capacidad de ofrecer seguridad global y nuestra voluntad de ir siempre un paso por delante.

¡Protégete de Inmediato!

¿De qué me protege la herramienta Anti-intrusos?

Cuando una herramienta de robo de información o espionaje está tratando de entrar en tu máquina. México

La función de seguridad del teclado de Panda protege la información privada de ser robada o explotada por algún desconocido.

Panda Software y Al cuidado de tu Patrimonio. www. .com

En respetamos su privacidad.
Está suscrito al soporte de
Para darse de baja de futuras comunicaciones, por favor pulse aquí. © Grupo 2007

Fig.4 Message in which BancoKill.A was distributed

Although Panda Security (previously Panda Software) collaborates with banks to protect their users from these threats, in this case, it was a social engineering technique used by cyber-crooks to fool users.

BANBRA.FTI

Detected in May 2008, Banbra.FTI is a Trojan that reached computers passing itself off as an image displaying a bank statement. On downloading the file (even though it showed the image displaying the bank statement), a malicious file was run on the computer.

It was designed to draw users' attention towards the image, to prevent them from suspecting a Trojan was being run.

To obtain users' bank details, the Trojan enabled the save password option in Internet Explorer, accessed the directory in which the passwords were stored and stole those related to banks. This data was then sent to the malware creator by email.

BANKER.LAX

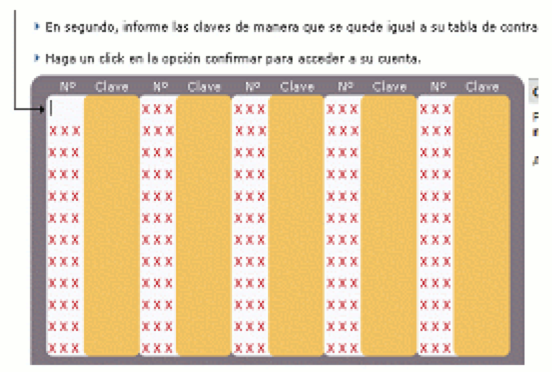
Matrix cards are one of the security elements provided by online banks to their users to increase security. These cards contain about 60 sets of coordinates.

Thanks to these cards, even if cyber-crooks obtain users' access keys, they cannot carry out operations on their accounts, as a second key is requested (randomly selected from the matrix card).

The problem began when a cyber-crook designed a Trojan that requested all the entries on the card, as in the case of Banker.LAX.

This Trojan had a list of the web addresses of banks to be monitored. When users accessed an address on the list, they were redirected to a page simulating the original.

The malicious page requested the initial passwords for starting the session. Once entered, a page was displayed in which the coordinates from the matrix card were requested:



- En segundo, informe las claves de manera que se quede igual a su tabla de contra
- Haga un click en la opción confirmar para acceder a su cuenta.

Nº	Clave	Nº	Clave	Nº	Clave	Nº	Clave	Nº	Clave
		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	
xxx		xxx		xxx		xxx		xxx	

Fig.5 Matrix card shown by the Trojan

The numbers entered by users then ended up in the hands of cyber crooks, who were able to access users' accounts.

Online bank authentication requires a random combination of coordinates, not all of them, as the effectiveness of the system lies in the high number of possible combinations.

BANBRA.FUD

Detected in June 2008, Banbra.FUD, reached computers by spoofing a web page. When run, a Trojan was installed on the affected computer.

As well as stealing bank details, this Trojan was designed to steal other data, such as the computer name, IP address or operating system version.

To obtain data, it monitored users' browsing habits and when they logged onto certain Brazilian banks. It then displayed an error message and opened a false page resembling the original.

The false web page asked users to enter their login details again and requested information from the matrix card. All the information entered by users was recorded and sent to its creator.

Cyber-crooks usually create web pages that simulate legitimate bank pages to prevent users from suspecting anything is amiss. However, these false pages differ in that they request more information than usual. It is important not to trust these web pages.

BANBRA.FXT

Detected in July 2008, Banbra.FXT, was a Trojan that targeted Brazilian users, as it was distributed in a message that claimed to have been sent from Brazil's Federal Ministry. In the message, users were asked to appear in court for the reason specified in the attached document.

Curiosity led users to run the attached file and enter the Trojan onto their computers.

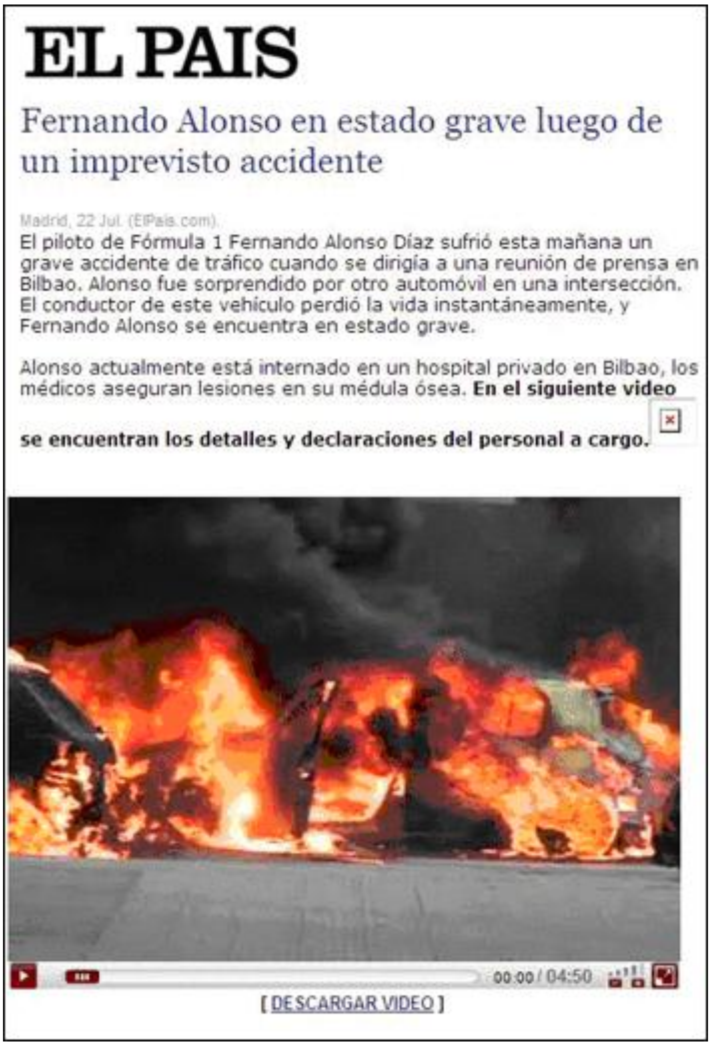
Once installed, the Trojan monitored users' browsing and on users accessing certain online banks, recorded their bank details.

BANKER.LGC

Detected in July 2008, Banker.LGC targeted the users of a specific Spanish bank. It used a spoof sensational news story to fools users: a report about a car crash suffered by F1 racer Fernando Alonso. The message included a brief report and a video in which two cars were on fire, which supposedly corresponded to the car crash.

This story enticed unwary users into viewing the video. Additionally, the message claimed and appeared to have been sent by *El Paiś* (Spanish newspaper) and users probably thought it was real.

The article was the following:



EL PAIS

Fernando Alonso en estado grave luego de un imprevisto accidente

Madrid, 22 Jul. (ElPais.com).

El piloto de Fórmula 1 Fernando Alonso Díaz sufrió esta mañana un grave accidente de tráfico cuando se dirigía a una reunión de prensa en Bilbao. Alonso fue sorprendido por otro automóvil en una intersección. El conductor de este vehiculo perdió la vida instantáneamente, y Fernando Alonso se encuentra en estado grave.

Alonso actualmente está internado en un hospital privado en Bilbao, los médicos aseguran lesiones en su médula ósea. **En el siguiente video se encuentran los detalles y declaraciones del personal a cargo.**

Fig.6 News report about Fernando Alonso's alleged car accident

On clicking the video, users did not see any images, instead they downloaded a copy of the Trojan onto their computers.

This type of spoof news story seeks to tempt users into viewing the video report while remaining unaware of other details that could make them suspect that the whole thing is a trick.

SINOWAL.VTJ

Some banker Trojan variants are distributed through emails aimed at scaring users with false threats in order to get them to run a file or click a link.

In the message in which Sinowal.VTJ (detected in September 2008) was distributed, an anonymous person claimed the recipient had been sending them viruses and threatened to inform the police.

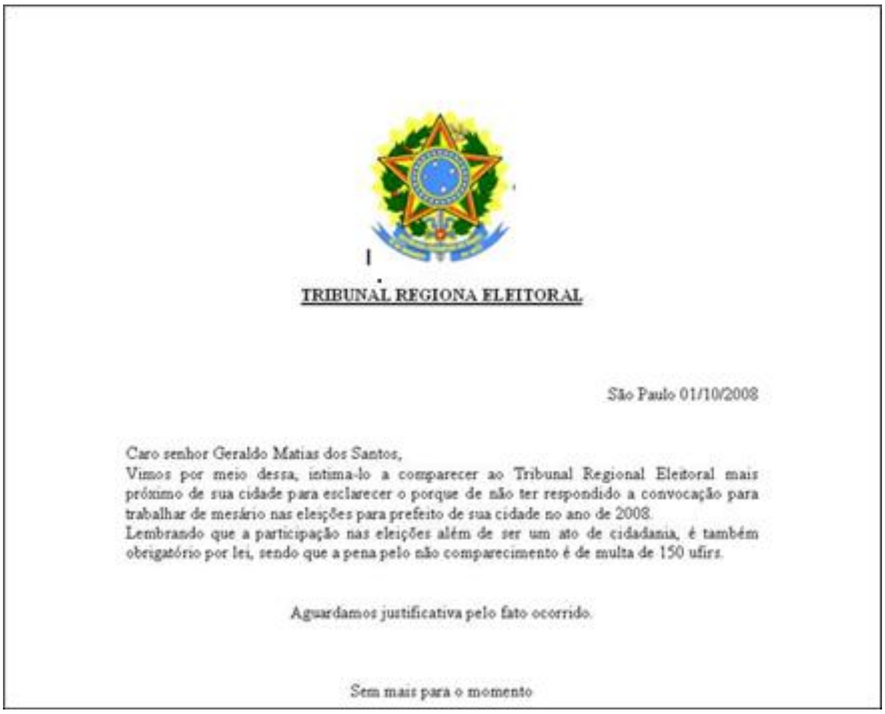
It attempted to trick the user into opening and printing an attachment which it claimed was proof of the messages that were sent and asked the user to send it to its ISP (Internet Service Provider) to solve the problem.

The message had a file attached which supposedly contained evidence. In fact, it contained a copy of the Trojan.

BANBRA.GBQ

Another typical strategy of this type of malware is to use the disguise of an inoffensive document (Word, Excel or pdf). The files however, really have two extensions (doc and exe), but the Trojans usually hide the .exe extension.

Such is the case of Banbra.GBQ, detected in October 2008, which reached computers in a file with a Word document icon. When run, the following document was opened, which looked like a notification from an official organization:



TRIBUNAL REGIONA ELEITORAL

São Paulo 01/10/2008

Caro senhor Geraldo Matias dos Santos,
Vimos por meio dessa, intima-lo a comparecer ao Tribunal Regional Eleitoral mais próximo de sua cidade para esclarecer o porque de não ter respondido a convocação para trabalhar de mesário nas eleições para prefeito de sua cidade no ano de 2008.
Lembrando que a participação nas eleições além de ser um ato de cidadania, é também obrigatório por lei, sendo que a pena pelo não comparecimento é de multa de 150 ufirs.

Aguardamos justificativa pelo fato ocorrido.

Sem mais para o momento

Fig.7 Notification sent by an alleged official organization

While users read the notification, the Trojan was installed on the computer without arousing suspicion.

BANKER.LLN

This banker Trojan was detected soon after Barack Obama was elected U.S. president. More specifically, Banker.LLN was designed to steal the access keys of users of a Peruvian bank. To do so, it first modified the HOSTS file, so that if users accessed the web page of the Peruvian bank, they were redirected to another page similar to the original.

If users entered their bank details, they were captured by the Trojan and sent to its creator.

It reached computers in a file called BARACKOBAMA.EXE and a US flag icon.

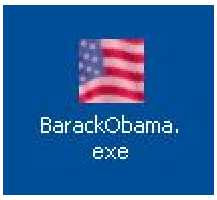


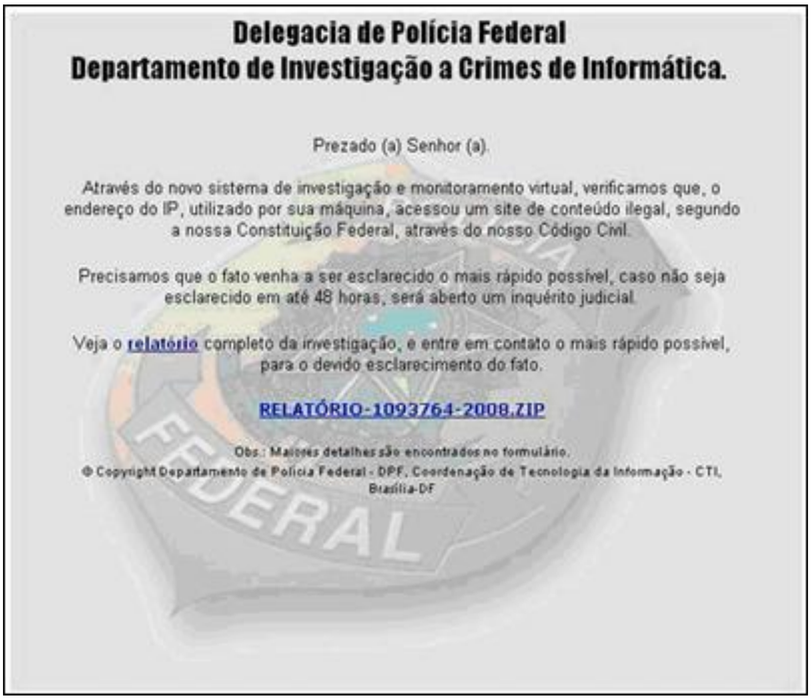
Fig.8 File name and icon

BANBRA.GDB

One of the limitations of banker Trojans is that they cannot spread on their own. They are usually distributed in spam messages sent by hackers.

However, some variants of the banker Trojan families have been detected, which have a worm's ability to spread. Such is the case of W32/Banbra.GDB.worm. This worm is distributed through two messages with different subjects.

One of them seems to come from the computer crime investigation department:



Delegacia de Polícia Federal
Departamento de Investigação a Crimes de Informática.

Prezado (a) Senhor (a).

Através do novo sistema de investigação e monitoramento virtual, verificamos que, o endereço do IP, utilizado por sua máquina, acessou um site de conteúdo ilegal, segundo a nossa Constituição Federal, através do nosso Código Civil.

Precisamos que o fato venha a ser esclarecido o mais rápido possível, caso não seja esclarecido em até 48 horas, será aberto um inquérito judicial.

Veja o relatório completo da investigação, e entre em contato o mais rápido possível, para o devido esclarecimento do fato.

RELATÓRIO-1093764-2008.ZIP

Obs.: Maiores detalhes são encontrados no formulário.
© Copyright Departamento de Polícia Federal - DPF, Coordenação de Tecnologia da Informação - CTI, Brasília-DF

Fig.9 One of the messages used to distribute Banbra.GDB

It is also distributed in a message about friendship and love that uses the infected user as the sender.

Both messages include a link that if clicked, redirects users to a web page that downloads a copy of the malware.

BANKERFOX.A

Internet Explorer is the browser hackers most frequently use to carry out computer crimes. This is mainly due to its popularity. However, other browsers are slowly catching up, i.e. Firefox.

Aware of this, cyber-crooks designed a Trojan for Firefox: BankerFox.A, detected in December 2008.

Although this Trojan's *modus operandi* was not typical, the number of affected countries and banks was surprising. The affected countries included Spain, Italy, UK, France, USA and Australia.

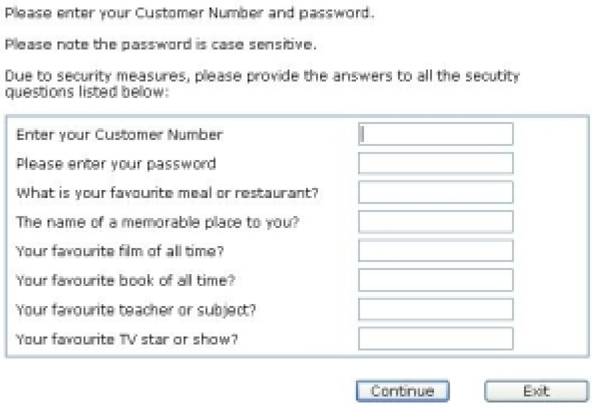
The Trojan contained a list of web pages belonging to banks in different countries. It monitored users' Internet activity with Firefox and if they visited one of the affected web pages, the Trojan was activated and recorded the information entered.

SINOWAL.VXR

Detected in December 2008, Sinowal.VXR, was designed to steal confidential information from certain British banks. It was activated when users accessed one of these online banks.

When users logged on, a false web page was displayed with a form that included several personal questions as well as the user name and password, claiming they were for security reasons. Questions included what their favorite food or restaurant was, the name of a memorable place or their favorite movie.

The high number of personal questions should have aroused suspicion.



Please enter your Customer Number and password.

Please note the password is case sensitive.

Due to security measures, please provide the answers to all the secutity questions listed below:

Enter your Customer Number

Please enter your password

What is your favourite meal or restaurant?

The name of a memorable place to you?

Your favourite film of all time?

Your favourite book of all time?

Your favourite teacher or subject?

Your favourite TV star or show?

Fig.10 Information requested for authentication

8.- Recommendations

Spam still represents a weak point for users in terms of preventing malware from entering their computers. Sometimes, the content itself of messages will be enough to make users suspicious.

However, there are often other indications such as spelling mistakes or incoherent information, which should warn users and prevent them from running files or clicking links.

In the case of messages with attachments, it is important that before opening them, users scan them with an antivirus solution to check if they contain malware.

Similarly, before clicking on any links in emails, you can place the cursor on the link to check if the link really points to the website that it claims to. Very often, links in these messages are camouflaged, and point to malicious addresses from which they download malware.

Criminals also infect legitimate web pages as a means for infecting users with banker Trojans. Be sure to keep systems fully up-to-date and patched to prevent any such malware exploiting vulnerabilities on your computers.

09.- Annex

In the Introduction and in the Organized crime section, we mentioned the simplicity of creating banker Trojans through the use of banking malware kits.

Zeus is a good example of this.

ZEUS CRIMEWARE KIT

This is a banking malware kit for creating Trojans of the Sinowal family.

Anyone can buy this kit -known as Zeus- for 700 dollars.

The kit has three parts:

- Bot (Trojan).
- Web control panel.
- Trojan generator.

The Trojan runs on the affected user's computer and can carry out the following actions:

- Socket and Proxy server.
- Auto update.
- Using the polymorphic encrypter to generate different copies of itself.
- Capturing certificates.
- Changing local DNS.
- Removing cookies to get the user to re-enter the passwords.
- Capturing screenshots of the affected computers.
- Receiving remote control commands.
- Adding additional fields to a website and monitor the data sent.
- Stealing passwords stored in several programs (Protected Storage data…) and pop3 and ftp passwords, regardless of the port.

It sends the following information to the infected computers:

- Version of the operating system.
- Service Pack.
- Language.

The Trojan enters hooks in Windows API functions to intercept them. These hooks indicate the pages requested by browsers using Windows API. These requests are compared to the list of banks to be monitored which the Trojan downloads from the server.

Capture methods

If the browser's requests and the monitoring strings coincide totally or partially, the credential theft mechanism is activated.

The hooks entered in the API functions can also intercept network traffic, redirect traffic, capture data entered in forms and record keystrokes (on detecting access to a bank being monitored).

The web control panel allows cyber-crooks to monitor and manage the entire botnet. Actions include:

- Checking infection statistics.
- Checking the files loaded.
- Searching for stored information.

The Trojan generator allows hackers to configure and create malware samples. There are different configuration options:

StaticConfig

botnet – Name of the botnet. It is usually "btn1" by default.

timer_config – time required to obtain the configuration.

timer_logs – time taken to send the logs to the server.

timer_stats – frequency with which the statistics are sent to the server.

url_config - URL to the server's main configuration file.

url_compip – location in which the computer's IP address can be checked.

blacklist_languages – code list of Windows languages: RU - 1049, EN - 1033…

DynamicConfig,

url_loader – URL from which the bot update can be downloaded.
url_server - URL to which the statistics, files, logs, etc. of the infected computers are sent.

file_webinjects – name of the file that includes the list of URLs in which additional fields are injected.

AdvancedConfigs – list of URLs from which a backup copy of the configuration file can be downloaded.

WebFilters – URLs of websites to be monitored.

WebFakes – list of addresses that redirect users to false websites. First, the legitimate bank's address must be indicated and then the address of the false page.

TanGrabber - URLs of banks to be monitored.

DnsMap - List of urls and their IPs to be added to the file: %SystemRoot%\Drivers\etc\hosts.

10.- References

Blog Panda Research

http://research.pandasecurity.com/archive/Banking-Trojans-I.aspx

http://research.pandasecurity.com/archive/Banking-Trojans-II.aspx

http://research.pandasecurity.com/archive/Banking-Trojans-III.aspx

Malware Encyclopedia

http://www.pandasecurity.com/homeusers/security-info/

Pharming

http://www.pandasecurity.com/homeusers/security-info/cybercrime/phishing/

Press releases

http://www.pandasecurity.com/enterprise/media/press-releases/viewnews?noticia=9290

Iframe attacks

http://www.pandasecurity.com/img/enc/Boletines%20PandaLabs_1_Pag_Web_legales_jaque_en.pdf