

Banking in Silence

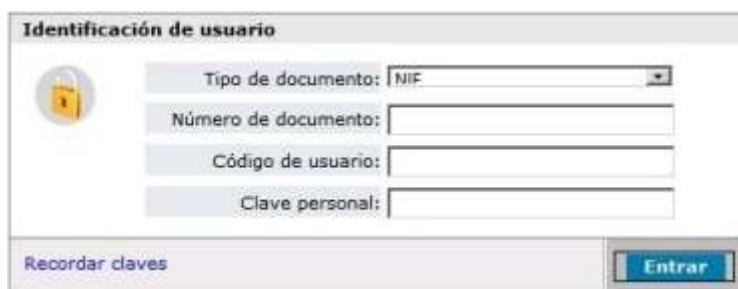
Targeting over 400 banks (including my own :(!) and having the ability to circumvent two-factor authentication are just two of the features that push Trojan.Silentbanker into the limelight. The scale and sophistication of this emerging banking Trojan is worrying, even for someone who sees banking Trojans on a daily basis.

This Trojan downloads a configuration file that contains the domain names of over 400 banks. Not only are the usual large American banks targeted but banks in many other countries are also targeted, including France, Spain, Ireland, the UK, Finland, Turkey—the list goes on.

The ability of this Trojan to perform man-in-the-middle attacks on valid transactions is what is most worrying. The Trojan can intercept transactions that require two-factor authentication. It can then silently change the user-entered destination bank account details to the attacker's account details instead. Of course the Trojan ensures that the user does not notice this change by presenting the user with the details they expect to see, while all the time sending the bank the attacker's details instead. Since the user doesn't notice anything wrong with the transaction, they will enter the second authentication password, in effect handing over their money to the attackers. The Trojan intercepts all of this traffic before it is encrypted, so even if the transaction takes place over SSL the attack is still valid. Unfortunately, we were unable to reproduce exactly such a transaction in the lab. However, through analysis of the Trojan's code it can be seen that this feature is available to the attackers.

The Trojan does not use this attack vector for all banks, however. It only uses this route when an easier route is not available. If a transaction can occur at the targeted bank using just a username and password then the Trojan will take that information, if a certificate is also required the Trojan can steal that too, if cookies are required the Trojan will steal those. In fact, even if the attacker is missing a piece of information to conduct a transaction, extra HTML can be added to the page to ask the user for that extra information. (In the example below the user is asked to enter their encryption key, in addition to the regular information.)

Here is the login form viewed on a clean machine:




The screenshot shows a web form titled "Identificación de usuario" with a yellow padlock icon on the left. The form contains the following fields:

- Tipo de documento: NIF (dropdown menu)
- Número de documento: (text input)
- Código de usuario: (text input)
- Clave personal: (text input)

At the bottom left is a link "Recordar claves" and at the bottom right is a blue button labeled "Entrar".

Below the form presented to an infected user is shown, the input box added by the Trojan has been marked in red:

Identificación de usuario



Tipo de documento: NIF

Número de documento:

Código de usuario:

Clave personal:

Clave de firma:

Recordar claves

Entrar

When instructed, the Trojan can also redirect users to an attacker-controlled server instead of the real bank in order to perform a classic man-in-the-middle attack. Currently there is only one bank targeted in this way; however, recent updates to the Trojan change the user's DNS settings to point to an attacker-controlled server. Using this technique the Trojan can start redirecting any site to an attacker site at any time. This feature could also mean that if the Trojan is removed but the DNS settings are left unchanged then the user may still be at risk. (See below for the attackers' DNS server addresses.)

Add to all of the above the ability to steal FTP, POP, Web mail, protected storage, and cached passwords and then we start to see the capabilities of this Trojan. But, it doesn't stop there – don't forget the porn! The Trojan also contains over 600 pornographic Web site URLs that can be shown to the infected user so that the attacker can make money from the referrals.

Lastly, the Trojan can also download updates, which it regularly does. It can also download other executables and it can use the infected machine as a proxy or as a Web server on any chosen port (in tests the http port used was 18102).

The multiple configuration files that the Trojan downloads are updated several times per day and currently the Trojan is capable of injecting HTML into about 200 different URLs. The configuration files are compressed and encrypted; however, after decrypting them we can see how the Trojan works in more detail.

The configuration files are structured as .ini files and each section of an .ini file represents a different task. Here is a snippet from the configuration file that was used to inject HTML into the banking form shown in the example above:

```
jhw21]
pok=insert
qas=someBankSite.com/xpage/loginxxxxxxxxxs.htm
njd=name="oppasswd;
dfr=14
xzn=/>n
xzq=2
rek=<div class="clear sep4"></div>
<label for="clave">Clave de firma: </label>
<input name="ESpass" type="password" size="8" maxlength="8"
class="input01 aleft w180"/>'
req=166
```

The configuration options in the snippet above are as follows:

| Token: | Purpose: |
|---------------|--------------------------|
| pok | Action to take |
| qas | URL to take action on |
| njd | String to search for |
| xzn | End string to search for |
| rek | HTML to insert |

The Trojan searches for the string name="opasswd; then it finds the end tag /> then it inserts the string into the page:

```
<div class="clear sep4"></div>
<label for="clave">Clave de firma: </label>
<input name="ESpass" type="password" size="8" maxlength="8"
class="input01 aleft w180"/>
```

Shown below is the HTML shown to the user on a non-infected computer:

```
<label for="clave">Clave personal: </label>
<input id="clave" name="opasswd" type="password" size="8" maxlength="8"
class="input01 aleft w180"/>
</div>
```

And on an infected computer:

```
<label for="clave">Clave personal: </label>
<input id="clave" name="opasswd" type="password" size="8" maxlength="8"
class="input01 aleft w180"/>
<div class="clear sep4"></div>
<label for="clave">Clave de firma: </label>
<input name="ESpass" type="password" size="8" maxlength="8"
class="input01 aleft w180"/>
</div>
```

The Trojan can take any of the following actions when altering the HTML of a page: insert, delete, replace, and replace all. The Trojan uses the keyword "ESpass" (see the form above) as a keyword when the user sends a page to the bank and the Trojan checks if the page contains that keyword. Using this technique the Trojan can recognize pages it has altered and can extract the relevant data from the page and send it to the attacker as well as to the bank.

The configuration files for this Trojan currently contain over 200kb of data; however, new URLs and HTML are being added to the configuration files on a daily basis. The Trojan is easily updated since the full HTML of any banking-related Web site is sent to the attackers. Using these submissions they can target banks for which they do not have bank accounts already. We are currently monitoring all of the updates to this Trojan.

The Trojan accesses the following URLs for configuration, updates, and to send stolen data:

- iloveie.info
- webcounterstat.info
- microcbs.com
- rezervaza.com
- screensaversfor-fun.com
- mystabcounter.info
- 85.255.119.218

The Trojan also downloads a copy of Trojan.Flush.J, which changes the users DNS settings to the following attacker settings:

- 85.255.116.133
- 85.255.112.87

For protection, please keep your antivirus definitions up to date and block the above addresses at the firewall.

Note: Not only did this Trojan grab my attention for obvious reasons, but the Trojan also installed itself as a .midi driver, causing my music to stop! For the record, the Trojan adds itself the following registry key so that it is loaded in all applications that use sound:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\midi1"

Posted by Liam OMurchu on January 14, 2008 05:00 AM