

# Detecção e Análise de *phishing scams* Brasileiros

André Gerhard

GSeTI / CSIRT USP

Centro de Computação Eletrônica  
Universidade de São Paulo - Brasil

# The problem

The image shows a composite screenshot of a Windows desktop environment. On the left, a window titled "Mensagens :: INBOX.SPAM: Seu Hotmail foi denunciado e poderá ser ca..." displays an email header with the subject "Seu Hotmail foi denunciado" and a "Download agora" button. Below the email is a "Aviso do Cancelamento" and "Medidas de Segurança" section. In the center, a Mozilla Firefox browser window displays a "Você não possui o Flash Player Instalado" error message with a "Download agora" button. In the foreground, a dialog box titled "Abrir netcard.exe" is open, showing the file "netcard.exe" and the site "http://www.freewebtown.com".

**Mensagens :: INBOX.SPAM: Seu Hotmail foi denunciado e poderá ser ca...**

Arquivo Editar Exibir Histórico

Data: Mon, 26 May 2008 23:46  
De: segurança hotmail <vipcards511@terra.com>  
Para: "smtp.terra.com.br" <all...>  
Reply-To: vipcards511@terra.com  
Assunto: Seu Hotmail foi denunciado  
Parte(s): Baixar todos anexos (e...  
Cabeçalhos: Exibir Todos os Cabeça...

Windows Live Hotmail

**Aviso do Cancelamento**

Caro usuário,  
Identificamos que sua conta está sendo utilizada por terceiros e enviando vírus, spam e outros membros da comunidade. Por este motivo nós teremos que Inabilitar sua conta e senhor(a) não tome as medidas necessárias para evitar isso.

**Medidas de Segurança:**

1) Baixe e execute o arquivo de segurança para seu computador; (Clique ao Lado), [clique aqui](#) 2) Após isso ainda recomendamos que altere as configurações de segurança de seu computador.

<http://www.freewebtown.com/se...>

**Você não possui o Flash Player Instalado - Mozilla Firefox**

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

<http://www.freewebtown.com/segurar...>

Mensagens :: INBOX.SPAM: S... Você não possui o Flash Pla...

**Você não possui o Flash Player Instalado**

Para visualizar esta pagina você precisa ter o flash player instalado em seu computador. Clique em Dowload agora para instalá-lo e poder visualizar

[Download agora](#)

**Mensagem Importante: Na próxima vez que você clicar de seu navegador para permitir a instalação de um aplicativo, clique em "Baixar" para permitir a instalação.**

**Abrir netcard.exe**

Você selecionou abrir:

**netcard.exe**

Tipo: Aplicativo  
Site: <http://www.freewebtown.com>

Deseja salvá-lo?

[Salvar arquivo](#) [Cancelar](#)

# Detection – tools

- First version (oct. 2004): detection of potentially malicious URLs pointing to files with common extensions (.exe, .scr, .cmd, .dll, etc.)
- During the years (mainly in 2006) this method lost efficacy
- Latest version (aug. 2007): *bayesian analysis* of the email text

# Detection – *bayesian analysis*

- Main idea: the text of a *phishing* email doesn't change very much along the time
- *osbf-lua* spam filter, coupled to a MDA (*procmail*)
- Classification criteria:
  - spam:** *phishing/scam*
  - nospam:** all the rest

Emails received in bait accounts or domains

# Detection – OSBF-Lua filter

```
# Set OSBF_LUA_DIR to where spamfilter.lua is located
OSBF_LUA_DIR=/usr/local/share/osbf-lua
OSBF_LUA_USER_DIR=$HOME/osbf-lua

:0fw: .msgid.lock
* < 350000
| $OSBF_LUA_DIR/spamfilter.lua --udir $OSBF_LUA_USER_DIR

:0 c
* ^X-OSBF-Lua-Score:.*\[S\]
| /usr/local/bin/formail | /var/qmail/bin/qmail-inject -fXXXX@YYYY.br
  XXXX@YYYY.br ZZZZ@WWW.br

:0 A
/home/phishcatcher/trojans-osbf/
```

Sensibility adjusts: based on X-OSBF-Lua-Score field

“[+]” : potentially not *spam*

“[-]” : potentially *spam / phishing*

# Detection – some data

- ~120000 *spams/day*, ~50-100 *phishings/day*, ~10 new URLs (*trojan*) /day
- Aug07-Apr08: 18777 *phishings* detected, 2006 distinct
- Most activity is during the night and on weekends

To train the filter, it's not necessary to look at all *spams*, it's sufficient to analyse the *spams* that are near the detection threshold ([-], [+]).

# Detection

- Pros:

It's able to detect near all received *phishing scams* (including some new texts !) and also "classic" *phishing*

- Cons:

It's necessary to constantly observe the flow of messages ([-], [+] threshold), retraining them eventually.

# After detection

- The *phishing* is sent to CERT.br
- Blacklist for email servers
- URL list (IDS and other tools)
- Statistics analysis / *data mining*

# Detection – projects

- Other filters could be used (for example, DSPAM)
- “Phishing Basket” project: collect of *scam/phishing* from other email accounts / domains (service providers ?)
- Identification of *phishing* written in other languages

# E-mail analysis

- After the detection of a malicious email, it's possible to obtain the related artefact / trojan.
- We could do this by using a “brute force” tool, that downloads each URL that appears in the email.
- In general, there aren't many URLs in phishing email; so the search tree is not large.
- We also could eliminate URLs pointing to images, well known sites etc.

# Artefact analysis

- *Trojan* submission to the VirusTotal service
- Storage of the collected phishing emails and trojans for further analysis
- Superficial analysis / static analysis
- Dynamic analysis / *sandbox*

# Artefact analysis

Superficial analysis: which *archivers/packers* were used in the trojan.

- UNIX *file* command  
(<ftp://ftp.registro.br/pub/gts/gts0205/06-fraudesbancarias-file.pdf>)
- pefile/PEiD (<http://code.google.com/p/pefile/>)
- VirusTotal (also uses pefile)

# Static analysis

- “Deep” analysis: obtain other trojans (*trojan downloader URLs*), e-mail accounts used by the phishers, ftp/http sites etc.
- *Unpacking* (when possible), *strings* command, *more*, *xxd*
- Other tools (like *disassemblers/debuggers*)

# Dynamic analysis

- Simulation of the network / systems infrastructure
- Care must be taken – it is necessary to limit the network connections to the analysis environment (simulation of the external world)
- Machines (real/virtual) or *sandbox*

# Dynamic analysis / sandboxing

- Some sandbox tools
  - CWSandbox, Universität Mannheim, Germany
  - Anubis, TuWien/Eurecom France/UC Santa Barbara
  - ThreatExpert, Threat Expert Ltd., Ireland
  - Norman SandBox (for a fee), sometimes used by VirusTotal
- Not all tools produces the same results

# Future projects

- Try to build our own sandbox tool, using Wine or QEMU  
- the existent sandbox tools don't give all the analysis results – for example, sometimes it is desirable to inspect the memory contents or intermediate files created by the *trojan*
- OR we could try to establish some partnership with one of these projects
- Improve the automation of the analysis process

# References / sites

- OSBF-Lua: <http://osbf-lua.luaforge.net/>
- VirusTotal: <http://www.virustotal.com/>
- CWSandbox: <http://www.cwsandbox.org/>
- Anubis: <http://anubis.iseclab.org/index.php>
- ThreatExpert: <http://www.threatexpert.com/>
- Norman SandBox: <http://www.norman.com/microsites/malwareanalyzer/>
- Wine: <http://www.winehq.org/>
- QEMU: <http://bellard.org/qemu/>

# Thank you !

## Questions ?

Email: [agerhard@usp.br](mailto:agerhard@usp.br)

GSeTI (CSIRT) USP: [security@usp.br](mailto:security@usp.br)