

## 1. Le message, son aspect général :

Nous avons reçu cet email par deux voies :

- une fois, en pièce jointe, via le réseau « reportphishing@antiphishing.fr »,
- et, en direct à travers notre passerelle sécurisée.

Ce qui nous a permis de tester le cas de phishing jusqu'au site plagié.

---

**From:** REGIONS AND UNION PLANTERS [mailto:support\_refnum\_5834325@regions.com]  
**Sent:** Wednesday, March 02, 2005 12:59 PM  
**To:**  
**Subject:** Customer notification: details confirmation



Dear client of the Regions Bank,

Technical services of the Regions Bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

<https://online.regions.com/ibsregions/cmserver/users/default/confirm.cfm>

We present our apologies and thank you for co-operating.  
Please do not answer to this email – follow the instruction given above.  
This instruction has been sent to all bank customers and is obligatory to follow.

© 2005. Regions and Union Planters

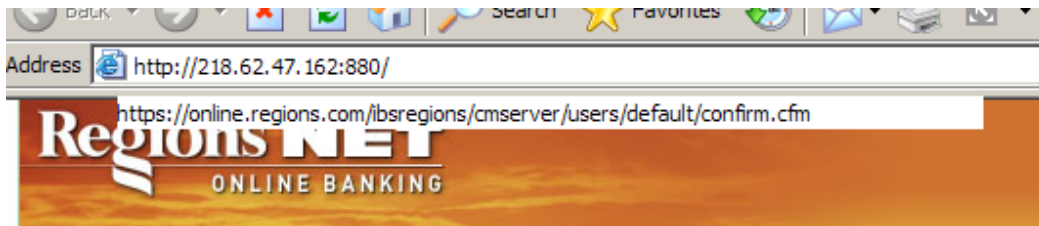
## 2. Le code html du message :

```
From: REGIONS AND UNION PLANTERS [mailto:support_refnum_5834325@regions.com]
Sent: Wednesday, March 02, 2005 12:59 PM
To:
Subject: Customer notification: details confirmation
<https://online.regions.com/ibsregions/cmserver/users/default/confirm.cfm>
Melboune Cup Open your 'N Sync Pearl Harbor Cindy Crawford
-----=_NextPart_001_0017_01C51F33.9AB31D30
Content-Type: text/html;
    charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Dus-ascii"><MAP=20
name=3DFPMap0><AREA shape=3DRECT coords=3D0,0,623,349=20
href=3D"http://218.62.47.162:880"></MAP>
<META content=3D"MSHTML 6.00.2900.2604" name=3DGENERATOR></HEAD>
```

l'image associée (via « enregistrer sous... ») :

!cid\_part1.07090109.09010105@custservice\_id\_012@regions[1]

La technique utilisée est une image du type « MAP » qui renvoie sur <http://218.62.47.162:880/> :



D'après le Whois, l'adresse 218.62.47.162 est basée en Chine :

```
inetnum: 218.62.47.160 - 218.62.47.167
netname: TH-SHUANGQIFENG-NETBAR
country: CN
descr: TongHua City,ShuangQiFeng NetBar, TeiNan Road No.47,TongHua City,JiLin
Province. China.

source: APNIC

address: 96,JieFang Road ChangChun 130021 China.

country: CN
changed: wtg@mail.jl.cn 20030117
mnt-by: MAINT-CNCGROUP-JL
source: APNIC
```

Notre passerelle antivirus (Trend Micro + ClamAV + Symantec) a détecté la possibilité d'un cheval de Troie attaché à l'image :

Madame, Monsieur,

Nous venons d'arrêter le message de ... qui vous était destiné, car l'anti-virus installé sur nos serveurs de messagerie a détecté la présence d'un virus (**HTML.Phishing.Bank-1**).

*280948 03/03/05 03:53:23 smtp-proxy[15509] (spamscreen) Email received from  
<support\_id\_874826713@regions.com>, marked as spam*

*Date, "Time", "Filename", "AVText"  
2005-03-03, "03:53:16", "c:\imail\spool\d7c19016003b693e9.smd", "clamav: Infected  
[HTML.Phishing.Bank-1]"*

Votre ordinateur n'a donc pas été contaminé par le virus contenu dans ce message.

NOTA : certains virus utilisent de fausses identités pour se propager, ... n'est donc pas nécessairement l'expéditeur du message que nous avons stoppé.

La passerelle sécurité de la société Associated Winners.

Un grand bravo donc à ClamAV ! ([www.clamav.net](http://www.clamav.net) existe aussi pour Windows)

Cette observation nous a conduit sur : <http://viruspool.vanderkooij.org/virus.cms>

HTML.Phishing.Bank-1

Aliases:

HTML/Bankfraud.gen ESET NOD32 on demand scanner for Linux

Phish-BankFraud.eml McAfee Virus Scan for Linux

Trojan-Spy.HTML.Bankfraud.cr Kaspersky On-Demand Scanner for Linux

Trojan-Spy.HTML.Bankfraud.cr [AVP] F-Secure Anti-Virus for Linux

Detected by: Clam AntiVirus

Date: 2005-02-18

En synthèse :

- Notre correspondant a été victime de la malveillance connue sous le nom de « HTML.Phishing.Bank-1 ».
- ClamAV a lui seul sait filtrer cette attaque.
- Le phishing est très facile à reconnaître via le lien fantaisiste :

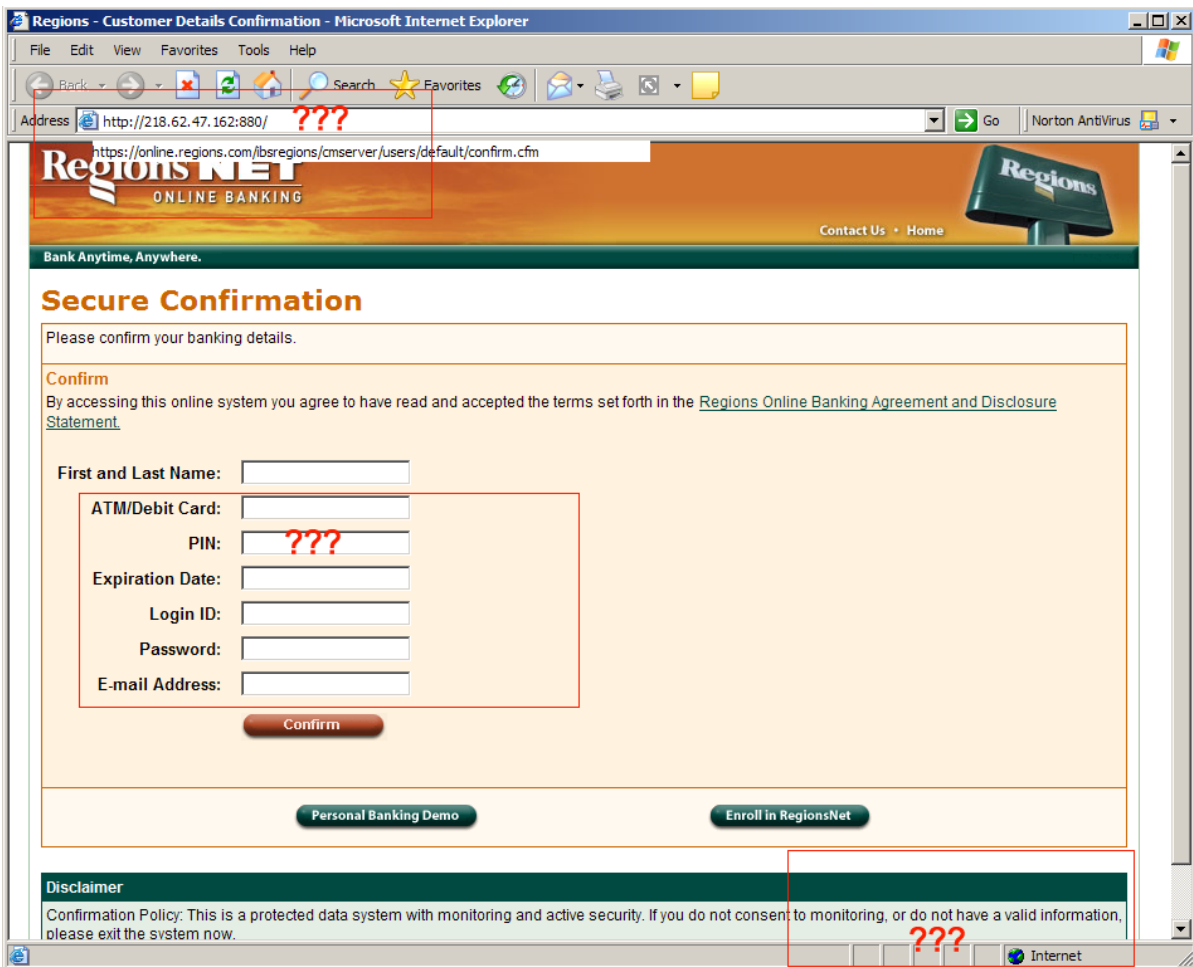


- La reconnaissance via le code source est aussi facile car le message caché suivant ne peut pas être attribuée à Regions.com :

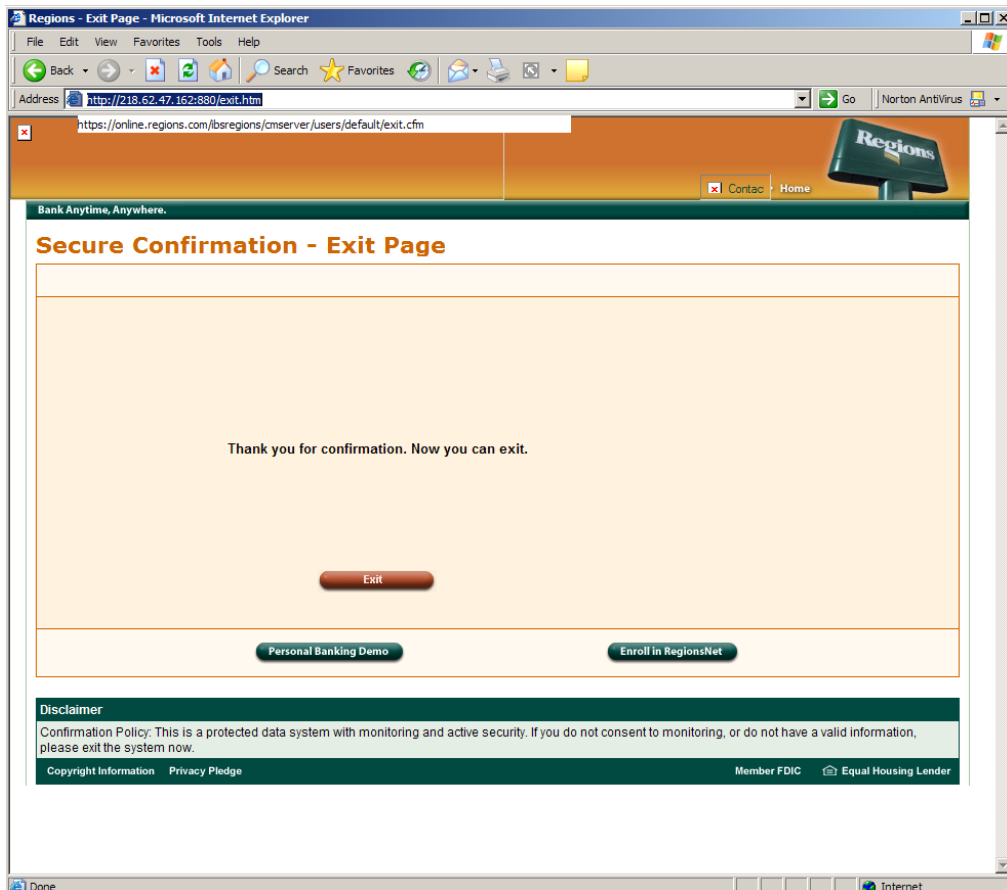
Melboune Cup Open your 'N Sync Pearl Harbor Cindy Crawford

### 3. Le scénario du phishing

Puisque nous avons reçu l'email original en pièce jointe, nous avons pu suivre le lien proposé. La simulation d'une connexion sécurisée est assez peu convaincante :



Après avoir rempli d'une manière farfelue les champs, nous avons obtenu une page de remerciement:



**« Thank you for confirmation. Now you can exit. »...**

**4. Actions déclenchées :**

- La publication de ce document,
- Bien que le cas « HTML.Phishing.Bank-1 » soit connu, nous avons communiqué ce document au niveau « .org » car nous avons pu le documenter.
- Les contacts Whois de Regions.com ont été informés.