


1. Le message, son aspect général :

----- Original Message -----
From: [Smith Barney](#) ; [citigroup](#)
To:
Sent: Thursday, February 24, 2005 11:07 PM
Subject: Urgent Notification From Smith Barney Billing Department [Fri, 25 Feb 2005 04:02:28 +0600]




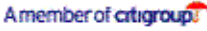
Dear Smith Barney customer,

Technical services of the Smith Barney 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://www.smithbarney.com/cgi-bin/login/confirm.cgi>

This instruction has been sent to all Smith Barney customers and is obligatory to follow.

Customers support service

2. Le code html du message :

```
<div style="BACKGROUND: #e4e4e4; font-color: black">
  <b>From:</b> <a title="Smith Barney" href="mailto:Smith%20Barney">Smith Barney</a>
; <a title="identifdep_id18347138690@smithbarney.com"
href="mailto:identifdep_id18347138690@smithbarney.com">citigroup</a>
</div>
```

```
<div>
```

```
  <b>Sent:</b> Thursday, February 24, 2005 11:07 PM
```

```
</div>
```

```
<div>
```

```
  <b>Subject:</b> Urgent Notification From Smith Barney Billing Department [Fri, 25
Feb 2005 04:02:28 +0600]
```

```
</div>
```

```
<p>
```

```
  <font face="Arial"><a href="https://www.smithbarney.com/cgi-
bin/login/confirm.cgi"></a></font>
```

```
</p>
```

```
<p>
```

```
  <font color="#fffff3">Marijuana Chinesse New Year in 1871 in 1948 Michael
Jordan</font>
```

```
</p>
```

dans le source de l'email :

```
-----=_NextPart_000_0011_01C51B32.C360C160
```

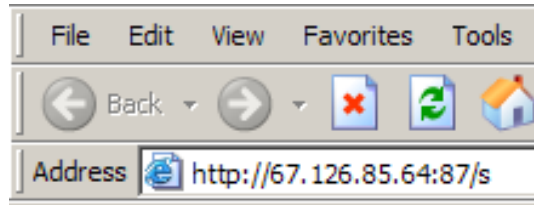
```
Content-Type: image/gif;
```

```
  name="caspien.GIF"
```

```
Content-Transfer-Encoding: base64
```

```
Content-ID: <001001c51b2a$616591f0$61f76254@ordi>
```

La technique utilisée est une image du type « usemap » qui renvoie sur un lien n'appartenant pas à SmithBarney Group :



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 (**Trojan-Spy.HTML.Bankfraud.ci**).

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.

Cette observation nous a conduit sur le site de www.viruslist.com :

<http://www.viruslist.com/en/viruses/encyclopedia?virusid=72731>

1. Trojan-Spy.HTML.Bankfraud.ci

Other versions: [.w](#)

Aliases

Trojan-Spy.HTML.Bankfraud.ci ([Kaspersky Lab](#)) is also known as: **HTML.Phishing.Bank-1 (ClamAV)**, HTML/Bankfraud.gen ([Eset](#))

Detection added Feb 02 2005

Behavior [TrojanSpy](#)

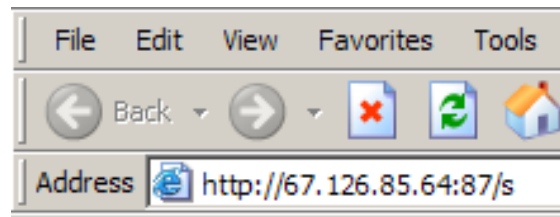
Currently there is no description available for this malicious program.

As many viruses and worms are modifications of earlier versions, it may help you to check the descriptions of similar malicious software. If such descriptions are available, they will be listed at the top of the page.

Our virus analysts work hard to ensure that descriptions of the commonest and most dangerous malicious software are available to users. The Virus Encyclopedia is updated on a regular basis.

En synthèse :

- Notre correspondant a été victime de la malveillance connue sous le nom de « HTML.Phishing.Bank-1 ».
- Une passerelle sécurisée professionnelle filtre cette attaque en reconnaissant « Trojan-Spy.HTML.Bankfraud.ci ».
- 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 la banque concernée:

```
<font color="#ffffff3">Marijuana Chinesse New Year in 1871 in 1948 Michael  
Jordan</font>
```

3. Actions déclenchées :

- La publication de ce document,
- Le cas « HTML.Phishing.Bank-1 » étant connu, il est inutile de le centraliser au niveau .org
- Une information a été faite au contact fournis par l'ISP (via le Whois) de CityGroup :

domain.admin@citigroup.com et dns@citicorp.com