

1. Le message, son aspect général :

Depuis quelques jours, une tentative de phishing vise les clients de la banque BNP PARIBAS. Par comparaison aux emails visant le LCL en janvier 2006, la disparition des fautes d'orthographe rend cet essai beaucoup plus crédible et la diversité des formes apparues en quelques heures démontre l'agressivité de cette technique de fraude en constante progression.

Nous avons répertorié 4 types de sujet pour l'email et au moins deux origines géographiques (l'une en Bulgarie et l'autre Séoul). Des exemples d'objet pour cet essai :

- « **BNP Paribas: Le message urgent [Mon, 20 Mar 2006 13:44:52 +0400]** »
- « **BNP Paribas: Une importante lettre** »
- « **BNP PARIBAS: UNE IMPORTANTE INFORMATION [Mon, 20 Mar 2006 01:09:29 -0800]** »
- « **L'information officielle [Mon, 20 Mar 2006 10:44:45 +0300]** »

Cet exemple BNP PARIBAS est détaillé dans notre rapport :

<http://www.associatedwinners.com/phishing/bnpparibas.pdf>

Nous constatons que la même tentative de fraude semble viser l'ensemble des banques françaises.



The screenshot shows an email client window titled "Fw: UNE IMPORTANTE INFORMATION". The menu bar includes "File", "Edit", "View", "Tools", "Message", and "Help". On the right, there are buttons for "Reply", "Reply All", and "Forward", along with a Windows logo. The email header shows:

From:
Date: lundi 20 mars 2006 22:38
To: reportphishing@antiphishing.fr
Subject: Fw: UNE IMPORTANTE INFORMATION

The main body of the email features the Société Générale logo (a red square with "SOCIETE GENERALE" in white text) on the left. Below the logo, the text reads:

Cher client de **SOCIÉTÉ GÉNÉRALE**

Le département technique de Société Générale procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

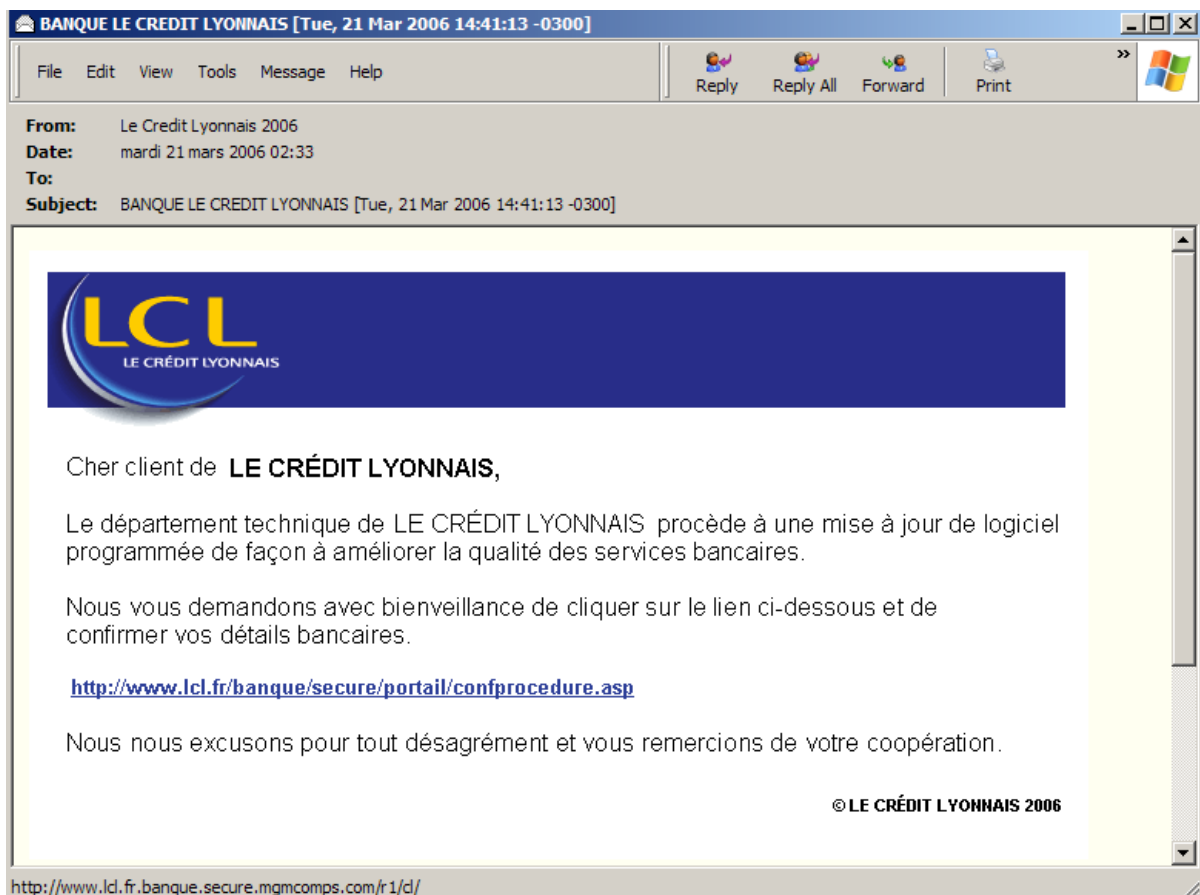
<http://www.societegenerale.fr/customercare/banque/confprocedure.asp>

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

© Société Générale 2000-2006

At the bottom of the window, the URL <http://www.societegenerale.fr.customercare.banque.mgmcomps.com/r1/sg/> is visible in the status bar.

D'autres exemples de l'email envoyé :



2. La technique utilisée

La technique est celle du classique lien à cliquer associé à une image. Cet exemple est décrit dans notre rapport BNP PARIBAS : <http://www.associatedwinners.com/phishing/bnpparibas.pdf>

Les antivirus détectent cette attaque connue sous le code « **HTML.Phishing.Bank-345** » :

3. Localisation de l'origine du phishing :

Lors de nos essais, les adresses IP suivantes sont associées aux pièges Web est **211.169.77.192** et **60.196.158.130**. Le Whois permet de localiser ses sites en Corée :

Whois 211.169.77.192 ?

```
inetnum:      211.169.0.0 - 211.169.255.255
netname:      BORANET-NET-211-169
descr:        DACOM Corp.
descr:        Facility-based Telecommunication Service Provider
descr:        providing Internet leased-ine, on-line service, BLL etc.
country:      KR
admin-c:      DB50-AP
tech-c:       DB50-AP
mnt-by:       APNIC-HM
mnt-lower:    MNT-KRNIC-AP
changed:      hm-changed@apnic.net 20021025
status:       ALLOCATED PORTABLE
source:       APNIC
```

```
role:         DACOM BORANET
address:      DACOM Bldg., 706-1, Yoeksam-dong, Kangnam-ku, Seoul
country:      KR
phone:        +82-2-2089-7755
fax-no:       +82-2-2089-0706
e-mail:       ipadm@nic.bora.net
e-mail:       abuse@bora.net
e-mail:       security@bora.net
admin-c:      EC115-AP
tech-c:       SIJ1-AP
nic-hdl:      DB50-AP
mnt-by:       MNT-KRNIC-AP
```

Whois 60.196.158.130 ?

```
% [whois.apnic.net node-1]
% Whois data copyright terms   http://www.apnic.net/db/dbcopyright.html
```

```
inetnum:      60.196.0.0 - 60.197.255.255
netname:      BORANET
descr:        DACOM, Internet Service Provider, Seoul, Korea
country:      KR
admin-c:      SP50-AP
tech-c:       SIJ1-A
```

4. Actions engagées

- La publication de ce document,
- Ce cas a été reporté au niveau « .org ».