

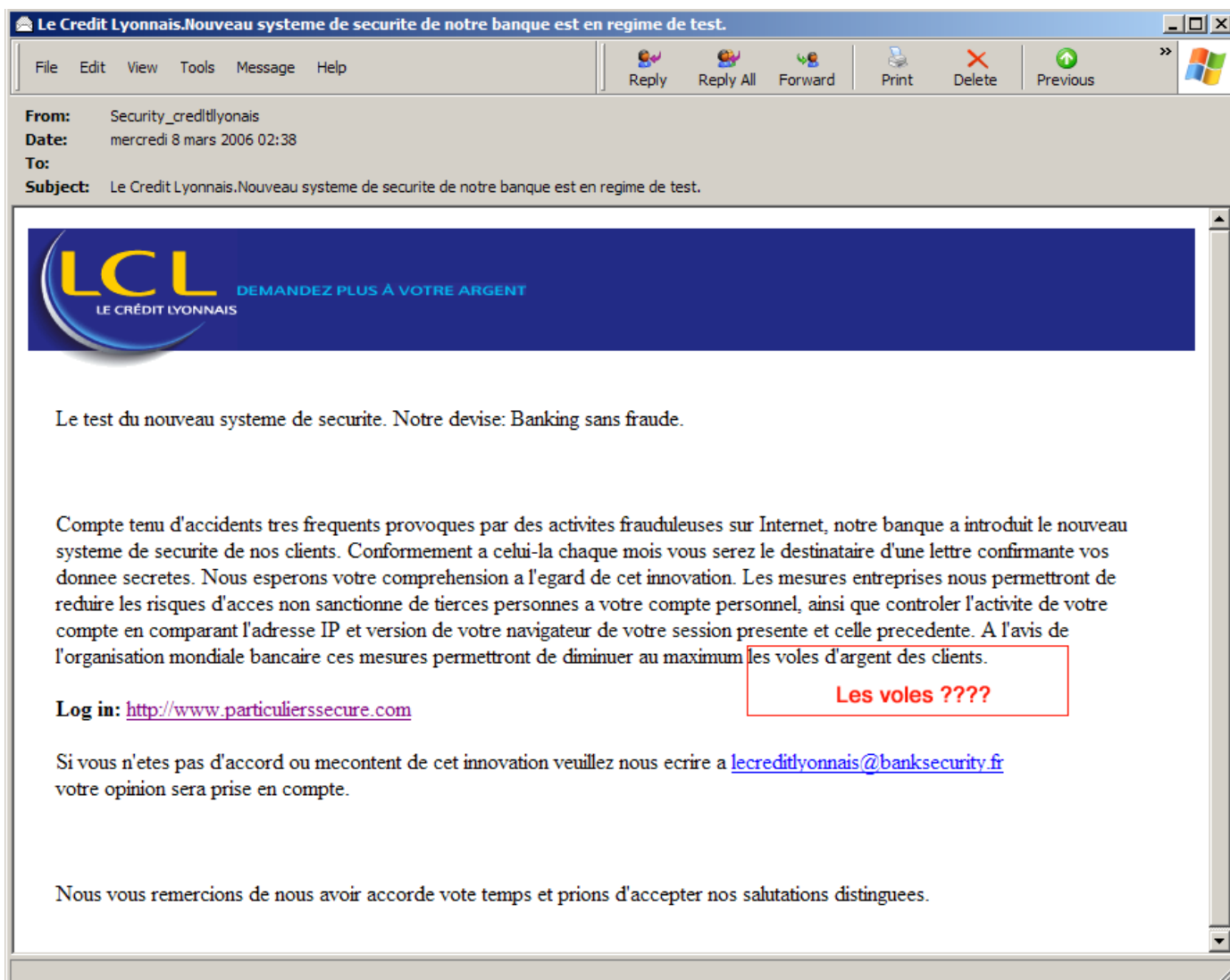
1. Le message, son aspect général :

Ce mardi 7 mars, une troisième tentative de phishing vise les clients du Crédit Lyonnais (banque LCL) :

- le 26 janvier 2006, premier essai : <http://www.associatedwinners.com/phishing/lcl.pdf>
- le 1 janvier 2006, deuxième vague : <http://www.associatedwinners.com/phishing/lcl2.pdf>

Cette tentative se présente sous la forme d'un message en « mauvais français » dont l'objet reste :

« **Le Credit Lyonnais.Nouveau systeme de securite de notre banque est en regime de test.** »



2. La technique utilisée

La technique est celle du classique lien à cliquer : <http://www.particulierssecure.com> ?????

Il suffit de visiter le lien proposé pour reconnaître l'essai de phishing décrit le 1 février 2006.

Les caractéristiques restent les mêmes :

- Pas de session sécurisée HTTPS,
- Un nom de domaine proche du nom réel : <https://particuliers.secure.lcl.fr/index.html>
- Un accès client avec « Date de naissance » ???

3. Localisation de l'origine du phishing :

Lors de nos essais, l'adresse IP hébergeant le piège est **81.57.51.152** (la « Free Box » d'un particulier de l'ISP « Free Telecom »). Le Whois permet de se promener sur le globe :

WHOIS 81.57.51.152 ?

```
% Information related to '81.57.50.0 - 81.57.51.255'
inetnum:      81.57.50.0 - 81.57.51.255
netname:      FR-PROXAD-ADSL
descr:        Proxad / Free Telecom
descr:        Static pool (Freebox)
descr:        palaisrose-1
descr:        NCC#2003034473
country:      FR
admin-c:      ACP23-RIPE
tech-c:       TCP8-RIPE
status:       ASSIGNED PA
mnt-by:       PROXAD-MNT
source:       RIPE # Filtered
```

WHOIS particulierssecure.com ?

```
Registrant:
  Stacy McCullough johnbrown132@mail.com +1.9066358143
  Stacy McCullough
  1432 W. 14th St.
  Sault Ste. Marie,MI,UNITED STATES 49783
Domain Name:particulierssecure.com
Record last updated at 2006-03-05 18:42:28
Record created on 2006/3/5
Domain servers in listed order:
  ns1.dnsservicesforfree.biz   ns2.dnsservicesforfree.biz
```

WHOIS dnsservicesforfree.biz ?

```
Domain Name:      DNSSERVICESFORFREE.BIZ
Domain ID:        D12532872-BIZ
Sponsoring Registrar: ONLINENIC, INC. D/B/A CHINA-CHANNEL.COM
Sponsoring Registrar IANA ID: 82
Domain Status:   ok
Registrant ID:    OLNIC26404412
Registrant Name:   Reiner Holz
Registrant Organization: intelli
Registrant Address1: Eichenfeldstrasse 20
Registrant City:   Langenfeld
Registrant State/Province: Langenfeld
Registrant Postal Code: 40764
Registrant Country: Germany
Registrant Country Code: DE
```

4. Actions engagées

- La publication de ce document,
- Information transmise à Free Telecom via : abuse@free.fr ,
- Ce cas a été reporté au niveau « .org ».