

1. Le message, son aspect général :

Une tentative de phishing vise les clients du Crédit Lyonnais depuis le 26 janvier 2006. Cette tentative se présente sous la forme d'un message en « mauvais français » dont l'objet est :

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

-----Original Message-----

From: Security_credtlyonnais [mailto:inreactiv.creditlyonnais@security.fr]

Sent: jeudi 26 janvier 2006 18:18

To:

Subject: Le Credit Lyonnais.Nouveau systeme de securite de notre banque est en regime de test.



Le test du nouveau systeme de securite. Notre devise: Banking sans fraude.

Compte tenu d'accidents tres frequents provoques par des activites frauduleuses sur Internet, notre banque a introduit le nouveau systeme de securite de nos clients. Conformement a celui-la chaque mois vous serez le destinataire d'une lettre confirmante vos donnee secretes. Nous esperons votre comprehension a l'egard de cet innovation. Les mesures entreprises nous permettront de reduire les risques d'acces non sanctionne de tierces personnes a votre compte personnel, ainsi que controler l'activite de votre compte en comparant l'adresse IP et version de votre navigateur de votre session presente et celle precedente. A l'avis de l'organisation mondiale bancaire ces mesures permettront de diminuer au maximum les voles d'argent des clients.

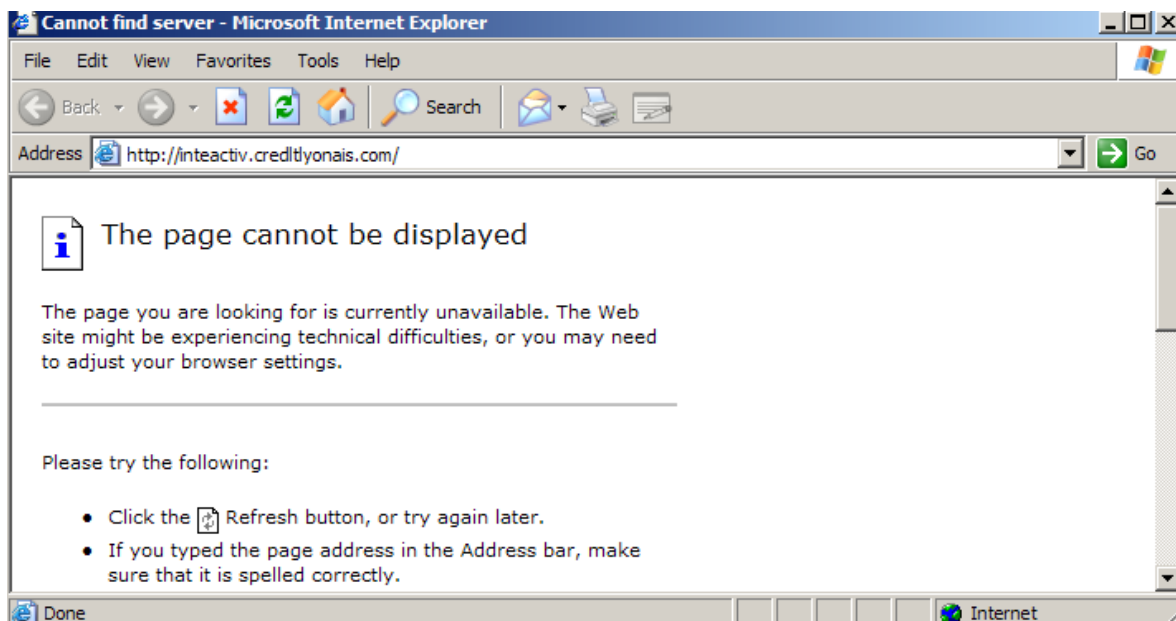
Log in: [lecreditlyonnais](http://lecreditlyonnais.com)

Si vous n'etes pas d'accord ou mecontent de cet innovation veuillez nous ecrire a lecreditlyonnais@banksecurity.fr votre opinion sera prise en compte.

Nous vous remercions de nous avoir accorde vote temps et prions d'accepter nos salutations distinguees.

2. La technique utilisée :

Lors de nos essais, le site Web hébergeant le phishing venait déjà d'être désactivé :



La technique est celle du classique lien à cliquer :

-----Original Message-----

From: Security_credlityonnais [mailto:inteactiv.credlityonnais@security.fr]

Sent: jeudi 26 janvier 2006 18:18

To:

Subject: Le Credit Lyonnais.Nouveau systeme de securite de notre banque est en regime de test.



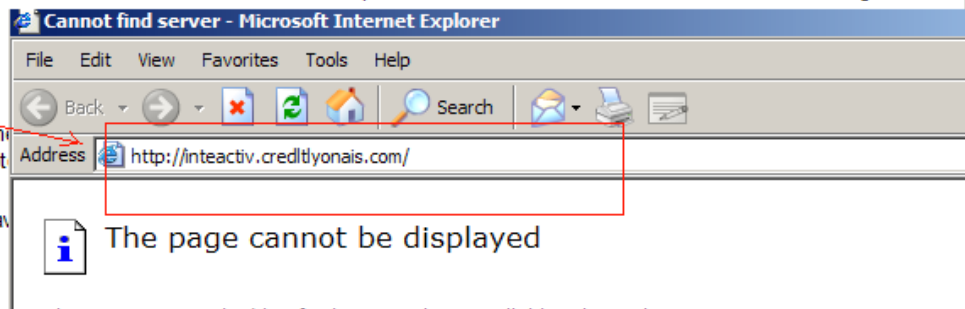
Le test du nouveau systeme de securite. Notre devise: Banking sans fraude.

Compte tenu d'accidents tres frequents provoques par des activites frauduleuses sur Internet, notre banque a introduit le nouveau systeme de securite de nos clients. Conformement a celui-la chaque mois vous serez le destinataire d'une lettre confirmante vos donnee secretes. Nous esperons votre comprehension a l'egard de cet innovation. Les mesures entreprises nous permettront de reduire les risques d'accès non sanctionne de tierces personnes a votre compte personnel, ainsi que controler l'activite de votre compte en comparant l'adresse IP et version de votre navigateur de votre session presente et celle precedente. A l'avis de l'organisation mondiale bancaire ces mesures permettront de diminuer au maximum les voles d'argent des clients.

Log in: [lecredityonnais](http://lecredityonnais.com)

Si vous n'etes pas d'accord ou mecontent de cet innovation veuillez nous ecrire a lecredityonnais@banksecurity.fr votre opinion sera prise en compte.

Nous vous remercions de nous avoir accorde vote temps et prions d'accepter nos salutations distinguees.



Le lien HTML est visible dans le code :

```
<table width="100%" border="0" cellspacing="0" cellpadding="20">
  <tr>
    <td class="text">
      <p class="style1">Le test du nouveau systeme de securite. Notre devise: Banking sans fraude. </p>
      <p>&nbsp;</p>
      <p>Compte tenu d'accidents tres frequents provoques par des activites frauduleuses sur Internet, notre banque a introduit le nouveau systeme de securite de nos clients. Conformement a celui-la chaque mois vous serez le destinataire d'une lettre confirmante vos donnee secretes. Nous esperons votre comprehension a l'egard de cet innovation. Les mesures entreprises nous permettront de reduire les risques d'accès non sanctionne de tierces personnes a votre compte personnel, ainsi que controler l'activite de votre compte en comparant l'adresse IP et version de votre navigateur de votre session presente et celle precedente. A l'avis de l'organisation mondiale bancaire ces mesures permettront de diminuer au maximum les voles d'argent des clients. </p>
      <p><strong>Log in:</strong> <a href="http://inteactiv.credlityonnais.com/">lecredityonnais</a></p>
      <p>Si vous n'etes pas d'accord ou mecontent de cet innovation veuillez nous ecrire a <a href="mailto:lecredityonnais@banksecurity.fr">lecredityonnais@banksecurity.fr</a><br> votre opinion sera prise en compte. </p>
      <p>&nbsp;</p>
      <p>Nous vous remercions de nous avoir accorde vote temps et prions d'accepter nos salutations distinguees. </p></td>
  </tr>
</table>
```

3. Localisation de l'origine du phishing :

La recherche sur le domaine proposé donne peu de résultats :

```

c:\WINDOWS\system32\cmd.exe - nslookup
C:\Documents and Settings\Administrator>nslookup
Default Server:  associatedwinners.com
Address:  10.0.0.2

> set type=all
> inteactiv.credltlyonais.com
Server:  associatedwinners.com
Address:  10.0.0.2

*** associatedwinners.com can't find inteactiv.credltlyonais.com: Non-existent domain

```

L'analyse du header des emails fournit l'origine géographique du serveur de messagerie à l'origine de l'envoi.

Header du message 1 :

```

Received: from ... (antivirus [10.0.0.6]) by ... (8.9.3+Sun/8.9.3) with ESMTP id HAA13287
for...; Fri, 27 Jan 2006 07:01:16 +0100 (MET)
...
Received: from unknown(221.151.12.15) by ... via smap (4.5) id xma027231; Fri, 27 Jan 2006
08:01:46 +0100
Received: from security.fr (-1211793768 [-1211533864]) by ... (Qmailv1) with ESMTP id
3EDF2FA056 for ...; Thu, 26 Jan 2006 12:44:29 -0500
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----_=_NextPart_003_01C62307.158DDE00"
Content-class: urn:content-classes:message
Subject: Le Credit Lyonnais.Nouveau systeme de securite de notre banque est en regime de test.
X-MimeOLE: Produced By Microsoft Exchange V6.5.7226.0
Date: Thu, 26 Jan 2006 18:44:29 +0100
Message-ID: <7521296848.20060126124429@security.fr>
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: Le Credit Lyonnais.Nouveau systeme de securite de notre banque est en regime de
test.
From: "Security_credltlyonais" <inteactiv.credltlyonais@security.fr>

```

This is a multi-part message in MIME format.

Header du message 2 :

```

Received: from ... by mwinb0806 (SMTP Server) with LMTP; Fri, 27 Jan 2006 06:33:13 +0100
X-Sieve: Server Sieve 2.2
Received: from ...et (localhost [127.0.0.1])
  by ... (SMTP Server) with ESMTP id 52C3CB80008C...; Fri, 27
  Jan 2006 06:33:13 +0100 (CET)
Received: from 141746488 (unknown [211.204.137.125])
  by ... (SMTP Server) with SMTP id ACD9EB80008D

Received: from security.fr (144535128 [135240880])
  by notimexico.com (Qmailv1) with ESMTP id 134B450FF0 for...; Thu, 26 Jan 2006 12:18:12 -0500
Date: Thu, 26 Jan 2006 12:18:12 -0500
From: Security_credtlyyonais <inteactiv.credtlyyonais@security.fr>
X-RAV-AntiVirus: This message has been scanned for viruses on notimexico.com

```

Les adresses **221.151.12.15** et **211.204.137.125** appartiennent un ISP à Séoul:

```

inetnum: 211.200.0.0 - 211.205.255.255
netname: HANANET
descr: Hanaro Telecom, Inc.
address: Hanaro Telecom Co.
address: Kukje Electornics Cneter Bldg. 1445-3 Seocho-Dong Seocho-Ku
address: SEOUL
address: 137-070
country: KR
phone: +82-2-106
fax-no: +82-2-6266-6483
e-mail: info@hananet.net
nic-hdl: IS37-AP
mnt-by: MNT-KRNIC-AP
changed: hostmaster@nic.or.kr 20010523
source: APNIC

inetnum: 221.144.0.0 - 221.168.255.255
netname: KORNET
descr: KOREA TELECOM
descr: Network Management Center
country: KR
admin-c: DL248-AP
tech-c: GK40-AP
person: Dong-Joo Lee
address: 128-9 Yeong-Dong Jongro-Ku Seoul
address: Network Management Center
country: KR
phone: +82-2-766-1407
fax-no: +82-2-766-6008
e-mail: ip@ns.kornet.net
nic-hdl: DL248-AP
mnt-by: MAINT-NEW
changed: hostmaster@nic.or.kr 20010425
source: APNIC

```

4. Actions engagées

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