

1. Le message, son aspect général :

Ce dimanche 19 mars, une tentative de phishing a visé 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.

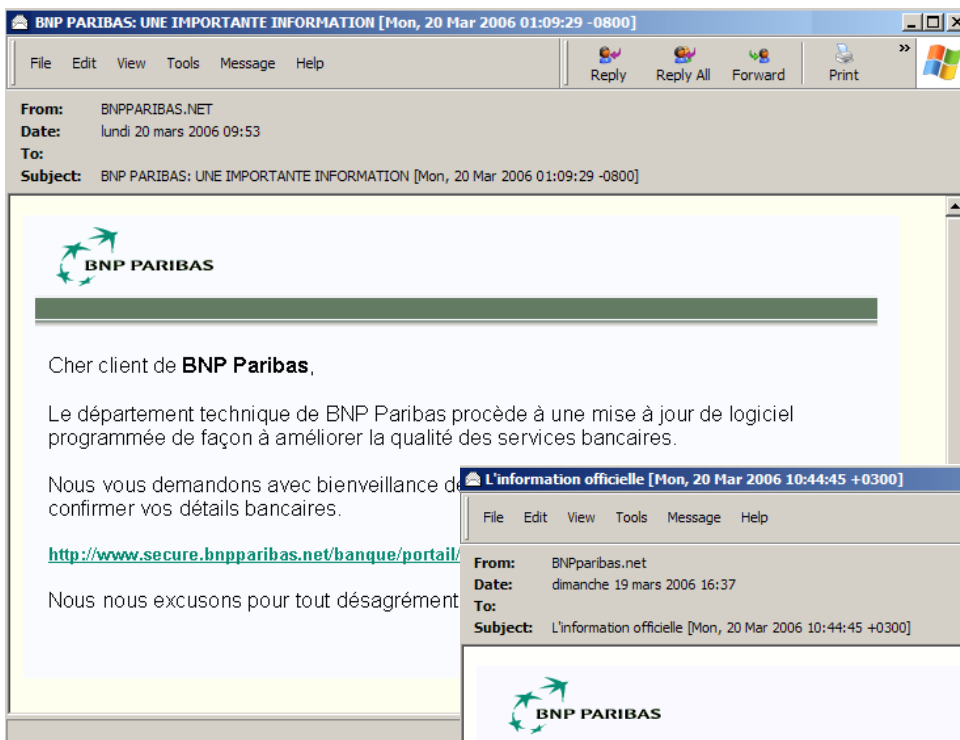
Nous avons répertorié 4 types de sujet pour l'email et au moins deux origines géographiques (l'une en Bulgarie et l'autre Séoul). Cette liste n'est certainement pas exhaustive !

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]** »



D'autres exemples de l'email envoyé :



2. La technique utilisée

La technique est celle du classique lien à cliquer associé à une image. L'examen d'un des codes html permet de voir le lien caché :

```
<p> <a href=http://www.secure.bnpparibas.net.banque.dlinfo.tv/r1/bn >
</a>

<p><font style='font-size:12.0pt; color:white'>The Annie in him knew. doff aeneas &quot;Get
busy right away. She was staring at him with horrified eyes, her hands
pressed so tightly over her mouth that the nails were white. the interior voice
whispered, and he jumped a little. Still, he had decided to live. Its eyes.
Hungry. The letter was an exhaustive (and ultimately exhausting) manual of
where Mrs Roman D. The operation was called hobbling, Paul, and that is what
I'm going to do to you. decompose</font></p>
```

On retrouve la signature surréaliste via une phrase en caractères blancs dont non lisibles...

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

```
"Date", "Time", "Filename", "AVText"
"2006-03-19", "16:35:33", "c:\...\spool\d7a43025e01704d75.smd", "clamav: Infected
[HTML.Phishing.Bank-345]"
```

Une autre origine a été détectée via une autre vague du même email :

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ascii">
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=utf-8">
<META content="MSHTML 6.00.2800.1522" name=GENERATOR></HEAD>
<BODY bgcolor="#FFFFFFC" text="#5D9DD7">
<a href=http://www.secure.bnpparibas.net.banque.dlinfo.cc/r1/bn/>
</a>
</p><p><font color="#FFFFFFB">The scene would not leave his mind. cavernous
composite So he cried from guilt.</font></p><p><font color="#FFFFFFF">"For the next two
days life went on just as it had before Duane Kushner; it was almost possible to believe Duane
Kushner had never happened at all. Mrs R. 1 Anger? Her baseball cap had fallen off.
Paul did not need a notarised statement telegram to tell him that this was Annie's sainted
mother. "("Folks, Sheldon has performed heroically today, but this has got to be his last shot.
build</font></p>
</BODY>
</HTML>
```

Suivons un des liens ...

BNPPARIBAS.NET : Tous les produits et services de votre banque en France - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.secure.bnpparibas.net.banque.dlinfo.tv/r1/bn/> Go

BNPPARIBAS.NET visite guidée messagerie ACCES Comptes Titres et Bourse

Magazine Services et Assurances Produits Votre Banque Recherche OK

Vos Besoins

- Famille et enfants
- Logement
- Auto
- Argent pratique
- Placement épargne
- Retraite
- Jeunes 18 +
- Expatriés

Votre banque

- Trouver une agence
- Devenir client
- Contactez-nous

Produits

- Services en ligne
- Comptes chèques
- Cartes bancaires
- Prêts Personnels
- Crédits Immobiliers
- Assurance Vie
- Assurances
- Tarifs 2006

Assistances

- BNPPARIBAS.NET : comment se connecter
- BNPPARIBAS.NET : obtenir ses codes d'accès
- Opposition carte bancaire

Services

- Calculer son crédit immobilier
- Simuler et demander votre crédit immobilier
- Calculer son crédit auto
- Calculer son devis assurance auto

Magazine

- Tous nos dossiers pratiques

Groupe BNP PARIBAS

- Groupe BNP Paribas
- Entreprises
- Entrepreneurs et Professionnels libéraux
- Banque Privée
- Associations
- Epargne entreprise
- Recrutement

Accédez à l'espace sécurisé de BNPPARIBAS.NET

Page de confirmation de détails de client.

Veuillez remplir tous les champs du formulaire ci-dessous. Après avoir rentré toutes les données, appuyez sur le bouton au bas du formulaire pour passer à la page suivante.

- J'utilise le clavier pour saisir mon numéro client
- J'utilise la souris pour sélectionner les chiffres de mon code secret
- Je choisis "Comptes", "Titres et Bourse" ou "Messagerie"

1 Saisissez votre numéro client à l'aide du clavier **Numéro client**

2 Cliquez pour composer les 6 chiffres de votre **Code secret**

1	2	3
4		5
	6	7
		8
	9	0

Code secret

[Corriger](#)

3 Cliquez pour accéder à :

- Comptes**
- Titres et Bourse**
- Messagerie

- [Si vous n'êtes pas en possession de vos codes d'accès, cliquez ici.](#)
- [Vous avez besoin d'une assistance technique, cliquez ici.](#)

Centre de Relations Clients 0820 820 001 (0,12 € ttc/min)
 Serveur vocal disponible 24h/24 et 7j/7. Accès à un conseiller clientèle à distance : du lundi au vendredi de 8h à 22h et le samedi de 8h à 18h (hors jours fériés).

[Contactez-nous par mail](#)

Magazine - Services et Assurances - Produits - Votre banque

Ce document a un caractère strictement informatif, il n'emporte aucun engagement juridique ni accord contractuel de la part de BNP Paribas qui se réserve par ailleurs la faculté de modifier les caractéristiques des produits présentés. BNP Paribas, SA au capital de 1 876 495 744 euros - siège social : 18 bd des Italiens 75009 PARIS, immatriculée sous le numéro 662 042 449 RCS PARIS-Identifiant CE FR7662042449

[mentions légales](#)

<https://www.secure.bnpparibas.net/banque/portail/particulier/HomePage?type=site> Internet

L'ergonomie générale du site visé est effectivement très bien reproduite.

Nous avons fourni des informations aléatoires pour connaître la suite : elle est très classique. L'écran suivant consiste simplement à revenir sur le site original de la banque !

3. Localisation de l'origine du phishing :

Lors de nos essais, une des adresses IP hébergeant le piège est **211.195.221.187**. Le Whois permet de localiser le site Web à Séoul en Corée (mais un des autres emails est associé à un site Web en Bulgarie ...):

Whois 211.195.221.187 ?

```
% [whois.apnic.net node-2]
% Whois data copyright terms      http://www.apnic.net/db/dbcopyright.html

inetnum:      211.172.0.0 - 211.199.255.255
netname:      KRNIC-KR
descr:        KRNIC
descr:        Korea Network Information Center
country:      KR
admin-c:      HM127-AP
tech-c:       HM127-AP
remarks:      *****
remarks:      KRNIC is the National Internet Registry
remarks:      in Korea under APNIC. If you would like to
remarks:      find assignment information in detail
remarks:      please refer to the KRNIC Whois DB
remarks:      http://whois.nic.or.kr/english/index.html
remarks:      *****
mnt-by:       APNIC-HM
mnt-lower:    MNT-KRNIC-AP
changed:      hostmaster@apnic.net 20000607
changed:      hostmaster@apnic.net 20010606
status:       ALLOCATED PORTABLE
source:       APNIC

person:       Host Master
address:      11F, KTF B/D, 1321-11, Seocho2-Dong, Seocho-Gu,
address:      Seoul, Korea, 137-857
country:      KR
phone:        +82-2-2186-4500
fax-no:       +82-2-2186-4496
e-mail:       hostmaster@nic.or.kr
nic-hdl:      HM127-AP
mnt-by:       MNT-KRNIC-AP
changed:      hostmaster@nic.or.kr 20020507
source:       APNIC
```

4. Actions engagées

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