

## 1. Le message, son aspect général :

Différents objets pour le même message diffusé ce lundi 12 septembre 2005 : « CreditAGF », « CreditAGF Verification », « CreditAGF Login », « Update Info » ou « Info » :

De : Sobriety I. Telecommunication [aaaaaaa@creditagf.fr]  
À :  
Cc :  
Objet : CreditAGF

---

**De :** Caging J. Disorientation [mailto:autor@creditagf.fr]  
**Envoyé :** lundi 12 septembre 2005 17:44  
**À :** Entreprise  
**Objet :** Update info

**From:** Convenes V. Annabel  
**Date:** lundi 12 septembre 2005 16:32  
**To:**  
**Subject:** CreditAGF Verification

**From:** Pod P. Catalytic  
**Date:** lundi 12 septembre 2005 19:48  
**To:**  
**Subject:** CreditAGF Login

----- Message de "Tiresias M. Deliveries" <majordomo@creditagf.fr> sur Mon, 12 Sep 2005 12:23:27 -0500 -----

**Pour:**

**Objet:** CreditAGF Login

Perfectionnement de Banque AGF en ligne

**From:** Runt U. Theatres  
**Date:** lundi 12 septembre 2005 16:31  
**To:**  
**Subject:** CreditAGF Verification

*"Undershorts O. Spectator"* <majordomo@creditagf.fr> a écrit :

De: "Undershorts O. Spectator" <majordomo@creditagf.fr>  
À:  
Objet: CreditAGF Verification  
Date: Mon, 12 Sep 2005 09:31:11 -0500

-----Message d'origine-----

**De :** Copulas I. Reemphasizing [mailto:aaaaaaa@creditagf.fr]  
**Envoyé :** lundi 12 septembre 2005 18:17  
**À :**  
**Objet :** CreditAGF Login

**From:** Configurations V. Horseback  
**Date:** lundi 12 septembre 2005 16:29  
**To:**  
**Subject:** CreditAGF Verification

**From:** Barbarity B. Zambia  
**Date:** lundi 12 septembre 2005 16:30  
**To:**  
**Subject:** CreditAGF Verification

**From:** Refuses H. Flouriest  
**Date:** lundi 12 septembre 2005 19:28  
**To:** Info  
**Subject:** CreditAGF Login

L'aspect du message intègre le logo AGF :

CreditAGF - Message (HTML)

Fichier Edition Affichage Insertion Format Outils Actions ?

Tapez une question

Vous avez transféré ce message le 2005-09-13 11:48. Cliquez ici pour rechercher tous les messages pour ce transfert.

De : Sobriety I. Telecommunication [aaaaaaa@creditagf.fr] Date : lun, 2005-09-12 16:20  
 À :  
 Cc :  
 Objet : CreditAGF

**BANQUE AGF**

**PERFECTIONNEMENT DE BANQUE AGF EN LIGNE**

Cher Client,

Nous poursuivons le perfectionnement de notre site web. Comme vous le savez certainement, Banque AGF vous offre un mécanisme idéal pour une gestion optimisée de votre argent au quotidien.

Chaque jour, nous travaillons pour améliorer notre système et nous voulons vous communiquer les résultats de nos efforts :

- Maintenant, lorsque le solde de votre compte dépasse 750 €, l'excédent est automatiquement transféré sur votre Compte sur Livret pour vous rapporter des intérêts en restant disponible à tout moment
- Si vous n'avez pas de contrat d'assurance avec Banque AGF, il est temps d'y penser, car vous bénéficierez de conditions privilégiées en passant par notre banque à distance. Découvrez la gamme Privalis maintenant!
- Banque AGF vous présente l'occasion de donner vie à vos projets – les crédits auto et immobiliers sont désormais disponibles 24h/24 et 7j/7. Pour les abonnés de Banque AGF à distance les prêts Reflexis commencent à 2.90% TEG fixe.
- Etes-vous néophyte en bourse? Banque AGF en ligne vous présente un guide complet qui vous permettra de comprendre les mécanismes boursiers ainsi que les termes spécifiques. Vous saurez la différence entre les actions nominatives et les bons de souscription et pourrez même acheter des actions en ligne de votre domicile.

De plus, nous avons une offre spéciale pour ceux qui travaillent en situation de mobilité externe, c'est-à-dire avec des assistants numériques personnels (PDA) ou des téléphones portables multifonctions. Dès aujourd'hui vous pouvez consulter vos comptes en utilisant ces appareils.

Pour pouvoir profiter de toutes les nouvelles options, veuillez confirmer vos données en passant par le lien en bas de [cette page](#).

démarrer

FR Bureau JLR 12:01

## 2. La technique utilisée :

La technique utilisée est celle du lien « à cliquer ». L'examen du source html permet de mettre en évidence le lien frauduleux :

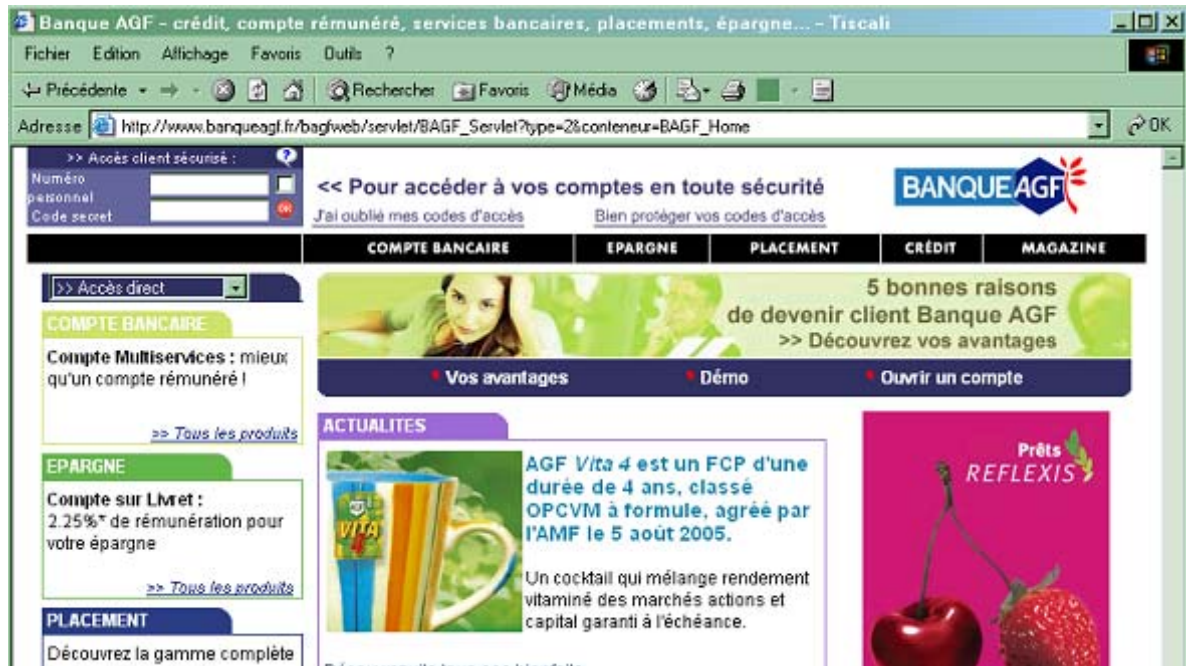
*<p>Pour pouvoir profiter de toutes les nouvelles options, veuillez confirmer vos données en passant par le lien en bas de*

*<a href="http://serverbackup49292.com/creditagf/secure/">cette page</a>. </p>...*

Lors de nos essais, la première IP appelée a été 68.198.37.23. L'écran suivant est associé au lien :

La saisie d'informations (farfelues) est associée à l'écran de confirmation :

Le dernier lien revient au site officiel. On remarquera que la charte graphique est proche du site original ce qui rend plus dangereux l'essai de phishing :



### 3. Identification du site hostile :

Résultat du nslookup (on retrouve la première IP appelée **68.198.37.23**, lors de nos essais) :

```
C:\Documents and Settings\Administrator>nslookup
Default Server: associatedwinners.com
Address: 10.0.0.2

> serverbackup49292.com

Non-authoritative answer:
Name: serverbackup49292.com
Addresses: 70.249.215.240, 216.255.0.88, 217.132.127.72, 68.198.37.23

> exit

C:\Documents and Settings\Administrator>tracert 68.198.37.23

Tracing route to ool-44c62517.dyn.optonline.net [68.198.37.23]
over a maximum of 30 hops:

 1  <1 ms  <1 ms  <1 ms  192.168.111.1
 2
```

Le Whois définit le propriétaire suivant pour l'IP 68.198.37.23 :

Whois **68.198.37.23** ?

Final results obtained from whois.arin.net.

Results:

Optimum Online (Cablevision Systems) NETBLK-OOL-5BLK (NET-68-192-0-0-1)  
68.192.0.0 - 68.199.255.255

Optimum Online (Cablevision Systems) **OOL-6ENYX2NY6-0821 (NET-68-198-32-0-1)**  
68.198.32.0 - 68.198.39.255

L'Url décrit de service « Optimum online » de Cablevision :

[http://www.cablevision.com/index.jhtml?pageType=ool\\_product](http://www.cablevision.com/index.jhtml?pageType=ool_product)

**CABLEVISION**

HOME PRODUCTS & SERVICES CUSTOMER SERVICE MY ACCOUNT

**SERVICE LOCATION:**  
Learn more about pricing and service availability.  
ZIP CODE:


**PRODUCTS & SERVICES:**

- › Products & Services
- › iO Digital Cable
- › Optimum Online
- › Optimum Voice
- › Pay Per View
- › Pricing & Packages
- › Business Services

Products & Services > Optimum Online

**PRODUCTS AND SERVICES**

**HIGH SPEED INTERNET**



**WHAT IS OPTIMUM ONLINE?**

Cablevision's Optimum Online, the industry's first self-install, blazingly fast Internet access cable-modem service is revolutionizing the way people in the tri-state area view and use the Internet. You can check service availability in your area and, if you are in a service area, order your cable modem and installation kit right online at [www.optimumonline.com](http://www.optimumonline.com)!

**More Power.**

- **No phone line needed** — Optimum Online works through fiber-optic cable wires, not phone lines. So you can surf the web without tying up your phone line or blocking incoming calls.
- **Latest technology** — Optimum Online works with the latest in digital cable modems designed to leave skid marks on the information super-highway.
- **Compatible with AOL®** — Do you already use AOL to

**WHAT'S NEW:**

- › HDTV
- › iO Games
- › Optimum Voice
- › The Triple Play Offer
- › Optimum Voice International Rates

**EXISTING CUSTOMERS:**

- › Customer Service
- › Online Account Access
- › Channel Lineups
- › TV Listings
- › Moving? [Click here.](#)

#### 4. Actions engagées

- La publication de ce document,
- Ce cas a été reporté au niveau « .org »,
- Un de nos correspondants a déjà averti le service client de la banque AGF qui vient de placer une alerte de sécurité sur son portail.