

Dossier visant à décortiquer le Spam

« NOTIFICATION DE DROITS ET PAIEMENTS »

Table des matières

<u>1 Réception d'un courrier indésirable.....</u>	<u>2</u>
<u>2 Le code source du Spam.....</u>	<u>3</u>
<u>3 Analyse du message</u>	<u>4</u>
<u>4 Informations utiles extraites du code source.....</u>	<u>4</u>
<u>5 Le formulaire de phishing.....</u>	<u>6</u>
<u>6 Conclusion.....</u>	<u>7</u>


Par Guillaume Dualé
g.duale@otasc.org

1 Réception d'un courrier indésirable

J'ai reçu le 19 août 2010 à 17H42 un courrier indésirable.

- Mon adresse mail est la suivante : g.duale@otasc.org
- Elle est hébergée chez OVH.
- Pour information skatemopolite@otasc.org est un alias vers g.duale@otasc.org

Voici à quoi ressemble le Spam que j'ai reçu :

 **CAISSE D'ALLOCATIONS FAMILIALES**

9 77 15 82 27 60 08

NOTIFICATION DE DROITS ET PAIEMENTS

Le 18 août 2010

Bonjour,

Nous avons étudié vos droits à partir du 01 août 2010.
Il apparait apres culcul pour Caisse d'Allocations Familiales pour la periode du 01.07.2010 au 31.08.2010, vous n'avez rien recu alors que vous aviez droit a 415,21 €.

[Cliquez ici pour plus de détails](#)

Votre Caisse d'Allocations familiales. Le 18 août 2010

F. Colinis Inge

La loi n° 78-17 du 6/01/78 modifiée, relative à l'informatique, aux fichiers et aux libertés, vous garantit un droit d'accès à votre dossier auprès du directeur de la Ca
405

--*-- LIQ NDP1AL T 02062008 095619

P2401939

Certes, la qualité du Spam reçu laisse à désirer.

2 Le code source du Spam

Return-Path: <paiement@cnafr.fr>
Delivered-To: g.duale@otasc.org
Received: from b0.ovh.net (HELO queue) (213.186.33.50)
by b0.ovh.net with SMTP; 19 Aug 2010 17:50:12 +0200
Received: from localhost (HELO mail528.ha.ovh.net) (127.0.0.1)
by localhost with SMTP; 19 Aug 2010 17:50:12 +0200
Received: from b0.ovh.net (HELO queueout) (213.186.33.50)
by b0.ovh.net with SMTP; 19 Aug 2010 17:50:12 +0200
Delivered-To: otasc.org-skatemopolite@otasc.org
Received: from b0.ovh.net (HELO queue) (213.186.33.50)
by b0.ovh.net with SMTP; 19 Aug 2010 17:50:11 +0200
Received: from mail.virginiasemi.com (HELO virginiasemi.com)
(98.172.22.185)
by mx1.ovh.net with SMTP; 19 Aug 2010 17:50:10 +0200
Received: from User [72.172.200.4] by virginiasemi.com with ESMTTP
(SMTPD32-8.05) id A09D8080152; Thu, 19 Aug 2010 11:41:17 -0400
Reply-To: <paiement@cnafr.fr>
From: "Caisse nationale des Allocations
Familiales"<paiement@cnafr.fr>
Subject: =?utf-8?Q?Spam?=
NOTIFICATION DE DROITS ET PAIEMENTS
Date: Thu, 19 Aug 2010 10:42:58 -0500
MIME-Version: 1.0
Content-Type: text/html;
charset="Windows-1251"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-SpamInfo: FortiGuard - AntiSpam url, black url
[http://lojaonline.telbeiras.p
t/images/caf.fr/](http://lojaonline.telbeiras.pt/images/caf.fr/)
Message-Id: <201008191141991.SM03384@User>
X-Ovh-Tracer-Id: 5958825257875665202
X-Ovh-Remote: 98.172.22.185 (mail.virginiasemi.com)
X-Ovh-Local: 213.186.33.29 (mx1.ovh.net)
X-Spam-Check: DONE|U 0.549691/N

```
<html>  
<tr><td>  
<a href='http://lojaonline.telbeiras.pt/images/caf.fr/'><img  
src='http://www.saytes.es/images/caf.jpg' alt='CAF' border='0'  
></a></td>  
</tr>  
</html>
```

3 Analyse du message

Le contenu du message est donc simple, c'est du HTML qui nous affiche une image jpg entièrement cliquable, cette image se trouve à l'adresse « <http://www.saytes.es/images/caf.jpg> » et correspond à la capture d'écran de la première page.

Le site www.saytes.es semble être un site espagnol de vente en ligne de produits Hi-Tech. C'est soit un camouflage, soit cette boutique s'est fait pirater et une personne s'est servi de leur site pour stocker cette image.

4 Informations utiles extraites du code source

Adresse e-mail qui sera utilisé si l'on clique sur le bouton répondre de son client de courrier :

- paiement@cnaf.fr

Serveur de courrier qui a envoyé le mail au serveur de courrier OVH :

- mail.virginiasemi.com : 98.172.22.185

Le serveur de courrier mail.virginiasemi.com à transmis le mail expédié par :

- 72.172.200.4
- Un Géolp sur cette adresse nous donne :

Hostname	Country Code	Country Name	Region	Region Name	City	Postal Code	Latitude	Longitude	ISP	Organization	Metro Code	Area Code
72.172.200.4	US	United States	MO	Missouri	Lebanon	65536	37.6989	-92.6620	Fidelity Communication International	Fidelity Communications	604	417

Le spammeur se fait passer pour :

- From: "Caisse nationale des Allocations Familiales"<paiement@cnaf.fr>

Client de courrier du spammeur :

- Microsoft Outlook Express 6

Un anti-spam a réécrit le sujet du mail en ajoutant le mot « Spam » devant ce dernier:

- Logiciel anti-spam : FortiGuard
- *Je ne sais pas à quel niveau du réseau se trouve cet anti-spam, probablement sur la machine mail.virginiasemi.com.*

URL ou se trouve le faux site de la Caf :

- <http://lojaonline.telbeiras.pt/images/caf.fr/>
- C'est un dump basique du site www.caf.fr
- Ils ont laissé l'essentiel : le logo, quelques images pour l'habillage et bien évidemment le formulaire de phishing.
- Le site <http://lojaonline.telbeiras.pt> semble lui aussi être une boutique portugaise de vente en ligne de téléphone portable. Même raisonnement concernant l'hébergement de la copie de caf.fr pour ce site, que pour l'hébergement de l'image sur l'autre boutique.

5 Le formulaire de phishing

Premier formulaire : (index.html)

The screenshot shows the login page for 'ALLOCATIONS FAMILIALES'. The header is red with the logo on the left and navigation links 'RECHERCHE', 'CODE POSTAL', and 'AIDE' on the right. The main content area is white and contains the following elements:

- Page d'accueil > Login
- Veillez vous identifier (with a link for 'Code confidentiel perdu ?')
- Form fields: Code postal, Numéro d'allocataire, Code confidentiel, and Jour et mois de naissance (JJMM).
- Example text: Ex : Ecrire 0106 si vous êtes né(e) le 1er juin
- Checkbox: Allocataire de la Caisse Maritime (checked)
- Submit button: Validez →

Ce premier formulaire fait un GET sur info.html.

Deuxième formulaire : (info.html)

The screenshot shows the 'Details de Virement' page. The header is red with the logo on the left and navigation links 'RECHERCHE', 'CODE POSTAL', and 'AIDE' on the right. The main content area is white and contains the following elements:

- Page d'accueil > Login
- Details
- Form fields and dropdowns: Nom et Prenom (qui apparait sur CB):, Date de naissance: (with 'Jour', 'Mois', 'Annee' dropdowns), Nom de votre mere:, Numero de CB:, Saisissez les 11 chiffres de votre numéro de compte présents sur un relevé de compte, sur un RIB, dans votre chéquier : (with a note about RIB and checkbook), Nom de banque:, Date d'expiration: (with 'Mois', 'Annee' dropdowns), Cryptogramme visuel:.
- Submit button: Continue

At the bottom of the page, there is a red footer with links: Infos légales | Liens utiles | Plan du site

Cette nouvelle page info.html nous demande d'autres informations et fait un POST sur info.php

C'est très probablement la page info.php qui stocke les données.

Si l'on se rend directement sur la page <http://lojaonline.telbeiras.pt/images/caf.fr/info.php> ceci nous redirige sur le vrai site de la caf.fr

6 Conclusion

Une personne physique ou une machine compromise aux Etats-Unis dans le Missouri tente de voler des numéros de carte bleue et des informations personnelles à des Français en prétextant une somme due par la Caf.