Panoptinet

Gardez un oeil sur votre réseau

Attention au nouveau phishing Paypal

admin · Thursday, August 11th, 2011

Fraîche de ce matin, cette tentative de phishing se veut plus sophistiquée que certaines de ses consœurs. Elle vise en particulier les utilisateurs de Paypal, à qui le mail incriminé demande de vérifier des informations personnelles et bancaires. Classique, mais toujours efficace ! A quoi ressemble cette campagne de phishing, et quels sont les indices qui permettent de détecter la fraude ?

C'est un membre de la communauté Panoptinet qui nous a transmis le **mail frauduleux** ce matin. Lui-même utilisateur régulier de **Paypal**, il a n'a pas de suite flairé le **piège**. Mais au fil de la lecture, certains **indices** lui ont mis la puce à l'oreille.

Une tentative de **phishing** (ou hameçonnage) est un **piège tendu par e-mail** : les destinataires reçoivent un message qui revêt l'**apparence d'un mail officiel** d'un prestataire de service courant (Free, CAF, Visa/Mastercard, EDF, etc.). Il s'agit en fait d'un **faux**, qui, sous prétexte de régulariser une situation, invite ses victimes à dévoiler leurs **informations personnelles et bancaires**. C'est hélas une pratique courante aujourd'hui : pas toujours considérés comme étant des spams, ces messages frauduleux détroussent les destinataires peu méfiants.

Cette fois-ci, c'est l'apparence de **Paypal** qui a été reprise (cliquer sur l'image pour l'agrandir) :

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

Subject: PayPal : Mise à jour de vos Informations Pour la Nouvelle Security
Date: Thu, 11 Aug 2011 09:41:56 +0300
From:"PayPal" <service@support.fr>
To: [redacted]@[redacted].com
Reply-To: Support@paypal.fr

PayPal

Informations de compte PayPal:

Bonjour,

Par mesure de sécurité, nous contrôlons régulièrement les activités PayPal. Nous avons récemment remarqué un problème sur votre compte

Nous réalisons actuellement la maintenance standard de nos mesures de sécurité.Votre compte a été sélectionné de manière aléatoire dans le cadre de cette maintenance et vous allez maintenant être guidé à travers une série de pages de vérification d'identité

Numéro de référence :PP-775-597-731

Rien de plus simple !

1. Télécharger le formulaire ci-joint et l'ouvrir à une fenêtre de navigateur sécurisé.
2. Une fois ouvert, vous sera fournie avec des mesures pour rétablir votre accès, puis suivez les instructions.

veuillez nous en informer immédiatement Il est important de nous le signaler pour nous aider à empêcher les fraudeurs de subtiliser vos informations.

Cordialement,
PayPal

Aide | Espace Sécurité

Veuillez ne pas répondre à cet email car les messages reçus à cette adresse ne sont pas lus. Pour nous contacter, connectez-vous à votre compte et cliquez sur Service clientèle en bas de n'importe quelle page.

Conseil clients : PayPal Pte Ltd, détenteur de la fonction de porte-monnaie électronique de PayPal™, ne nécessite pas l'approbation de la Monetary Authority of Singapore. Nous recommandons aux consommateurs (utilisateurs) de lire les conditions générales attentivement .

Adresse email PayPal : PP959

1 pièce jointe : Mise _à_jour_de_vos_Informations.html 29.3 Ko

Le mail proposait aussi une **pièce jointe** HTML. Après un scan avec l'antivirus, le document s'est avéré vierge de tout malware. Il s'agit en fait d'un formulaire web, celui où justement sont demandées les **informations bancaires** (cliquer sur l'image pour l'agrandir) :

PayPal

Recherche PayPal

Rechercher Rechercher

- Dconnexion
- Aide
- Espace scurit

- Mon compte
- Paiement
- Demande de paiement
- Solutions e-commerce
- Solutions eBay

Mise jour de vos Informations

- **1** Mise jour de vos Informations
- **2** Termin

Vous devez enregistrer une carte bancaire pour effectuer vos paiements par PayPal.

Pour les dtenteurs d'e-**Carte Bleue**, nous vous demandons d'entrer le numro figurant rellement sur votre carte et non pas un numro gnr automatiquement par le logiciel e-Carte Bleue.

PayPal vous couvre contre une utilisation frauduleuse de votre compte.

*Prnom

*Nom

*E-mail

*Mot de passe

*Date de naissance

Jourjj /

Moismm /

Anneaaaa

*Adress1

Adress2

*Code Postal

*Ville

*Pays France

*Tlphone

*N Compte Bancaire

*Type de carte Carte Bancaire

*Numro de la carte

*Date d'expiration mois anne

*N° vrification de la carte Aide de votre carte de numro de vrification

*SecureCode

*Signature Card / PIN Pourquoi est-Carte de signature / PIN ncessaire?

Enregistrer cette carte et continuer Annuler

Plus d'informations

- Mobile
- Paiements groups
- Parrainages
- Notre socit
- Types de compte
- Tarifs
- Respect de la vie prive
- Espace scurit
- Service clientle
- Contrats d'utilisation
- Chques-cadeaux

Copyright 1999-2011 PayPal. Tous droits rservs.

Comment savoir si cet e-mail est une tentative de phishing ou pas ?

Si les mails frauduleux sont mieux réalisés que par le passé, il reste toujours des **indices** qui doivent vous guider vers la bonne décision. En l'occurrence **supprimer cet e-mail**, et ne surtout pas y donner suite.

Le message :

- Vous n'êtes pas un utilisateur Paypal ? Passez votre chemin !
- Le **titre** du mail (*PayPal : Mise à jour de vos Informations Pour la Nouvelle Security*) est franchement louche, avec des majuscules mal placées, et un mot non traduit de l'anglais.

Cet élément à lui tout seul est suspect.

- L'**adresse** d'origine (*service@support.fr*) n'est pas fiable : elle devrait se terminer par paypal.com. D'ailleurs l'adresse de réponse (*support@paypal.fr*) est plus crédible, mais comme elle ne sera jamais utilisée par les cybercriminels, ils peuvent écrire ce qu'ils veulent !
- Le **destinataire** n'est pas identifié (nom, pseudo, numéro client, etc.) dans le corps du message, il ne s'agit donc pas d'un mail personnalisé (envoi massif).
- Il n'y a aucune faute d'orthographe, mais l'**argumentaire** du message est vraiment très flou : à cause d'un contrôle de sécurité, un problème sur le compte du destinataire est soit-disant survenu. Mais ce compte a été sélectionné de manière aléatoire dans le cadre d'une activité de maintenance. Cela ne veut rien dire ! La fin du message est encore plus symptomatique d'une escroquerie en ligne.

La pièce jointe :

- Le message invite un remplir le formulaire joint "dans un **navigateur sécurisé**". Aucun sens : une page sécurisée sur Internet est une page hébergée dans des conditions particulières. En aucun cas une pièce jointe, même si elle s'ouvre dans le navigateur, ne saurait remplir les mêmes conditions. D'ailleurs, la barre d'adresse ne précise pas "**HTTPS**" (le S signifie "sécurisé")
- La **mise en forme** est particulièrement pauvre, ce qui serait étonnant avec un vrai formulaire Paypal.
- Tous les **caractères accentués** (é,è) sont manquants. Là non plus pas très professionnel. Probablement un problème de traduction, de clavier étranger ou de norme ISO, que n'aurait pas laissé passer Paypal France.
- Et surtout le formulaire demande des **informations bancaires très poussées** ! Ainsi que des informations personnelles qui peuvent s'avérer utiles pour usurper une identité (par exemple la demande d'adresse mail et de mot de passe).

Les destinataires les plus experts peuvent aussi **analyser le code de l'en-tête** du mail, pour obtenir plus d'informations. Dans l'exemple d'aujourd'hui, on se rend compte que le message est envoyé, non pas par Paypal, mais par un site roumain inconnu : *rodas.ro* (cliquer sur l'image pour l'agrandir).

```
Return-Path: <service@support.fr>
X-Original-To: [redacted]@[redacted].com
Delivered-To: [redacted]@[redacted].com
Received: from localhost (localhost.localdomain [[redacted]])
        by [redacted] (Postfix) with ESMTP id [redacted]
        for <[redacted]@[redacted]>; Thu, 11 Aug 2011 09:32:47 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at [redacted].net
Received: from [redacted].net ([redacted])
        by localhost ([redacted].net [[redacted]]) (amavisd-new, port [redacted])
        with ESMTP id AOi[redacted] for <[redacted]@[redacted].com>;
        Thu, 11 Aug 2011 09:32:45 +0200 (CEST)
X-policyd-weight: passed - too many local DNS-errors in rhsbl.ahbl.org lookups
X-Greylist: delayed 983 seconds by postgrey-1.31 at [redacted]; Thu, 11 Aug 2011 09:32:44 CEST
Received: from rodas.ro (unknown [82.76.24.17])
        by [redacted].net (Postfix) with ESMTP id D2[redacted]
        for <[redacted]@[redacted].com>; Thu, 11 Aug 2011 09:32:16 +0200 (CEST)
Received: from 4e3z2 ([95.183.142.14]) by rodas.ro with Microsoft SMTPSVC(6.0.3790.4675);
         Thu, 11 Aug 2011 09:40:39 +0300
From: "PayPal" <service@support.fr>
Subject: PayPal : Mise =?ISO-8859-1?Q?=E0?= jour de vos Informations Pour la
 Nouvelle Security
To: [redacted]@[redacted].com
Content-Type: multipart/mixed;
 boundary="=_NextPart_2rfkindysadvnqw3nerasdf";
        charset="US-ASCII"
MIME-Version: 1.0
Reply-To: Support@paypal.fr
Date: Thu, 11 Aug 2011 09:41:56 +0300
X-Priority: 3
Message-ID: <RODAS17HWFIhyGuJAq300044e6b@rodas.ro>
X-OriginalArrivalTime: 11 Aug 2011 06:40:39.0625 (UTC) FILETIME=[95A4EB90:01CC57F1]
```

Voilà, vous êtes désormais prêts à **déjouer les pièges du phishing** !

This entry was posted on Thursday, August 11th, 2011 at 4:50 pm and is filed under Actualités décryptées par Panoptinet
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.