

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : E-mail backscatting, pollution par des rapports de non-livraison de courriels

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-004>

Gestion du document

Référence	CERTA-2008-INF-004
Titre	E-mail backscatting, pollution par des rapports de non-livraison de courriels
Date de la première version	19 décembre 2008
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Le contexte

Le protocole *SMTP* prévoit des codes retours et des messages pour informer l'expéditeur d'incidents affectant la transmission de courriels. Cette fonctionnalité peut être détournée de manière malveillante et devenir une forme de pollution des serveurs de messagerie. Cette pollution consiste, par exemple, en l'envoi de nombreux courriers électroniques vers des boîtes aux lettres électroniques inexistantes ou ne pouvant recevoir ces messages en usurpant une ou plusieurs adresses d'émission appartenant à un même domaine (cf. étape 1 de la figure 1). Cet envoi massif de courrier a pour conséquence de saturer le serveur de messagerie de destination (cf. étape 1 de la figure 2) ainsi que le serveur de messagerie légitime du domaine usurpé (cf. étape 3 de la figure 1) en rapport de non livraison de courriels (*NDR* : *Non Delivery Report*).

2 Les faits

Plusieurs cas de réceptions importantes de courriers électroniques non sollicités sur des serveurs de messagerie ont déjà été constatés. Les courriels reçus ont généralement les caractéristiques communes suivantes :

- il s'agit de messages notifiant un échec de remise ;
- ils sont visiblement émis par des serveurs de messagerie. L'adresse émettrice est de la forme `postmaster`, `MAILER-DAEMON`, etc. Le champ de retour `Return-Path` : est vide ou ne contient que les caractères `<>`.

- le sujet est un message d'erreur de type :
 - « Notification d'état de remise (Echec) » ;
 - « NOTICE: mail delivery status » ;
 - « Undeliverable mail: *sujet initial* » ;
 - « Undeliverable Mail » ;
 - « Undeliverable: *sujet initial* » ;
 - « Returned mail: see the transcript[FAILED(1)] » ;
 - « Delivery Notification: Delivery has failed » ;
 - etc.
- le corps du message contient un message d'erreur et/ou un code erreur *SMTP* justifiant l'impossibilité de remettre le courriel, par exemple en signalant qu'un ou plusieurs destinataires n'existent pas.
- le corps du message peut contenir une copie d'un autre message, avec un en-tête bien différent, et avec le champ *From* : faisant apparaître le destinataire du message d'échec de remise ;
- des pièces jointes peuvent également s'ajouter aux données précédentes.

En voici un exemple :

```
Subject: Undelivered Mail
From: <MAILER-DAEMON@domaineC>
Date: Fri, 18 Apr 2008 14:19:42 +0200
To: <monsieurB@domaineB>
X-Account-Key: account2
Return-Path: <>
X-Original-To: monsieurB@domaineB
Delivered-To: monsieurB@domaineB
Received: from serveurMail@domaineC by serveurMail@domaineB (Postfix)
        with ESMTTP id XXXXXXXXX
        for <monsieurB@domaineB>; Fri, 18 Apr 2008 14:10:52 +0200
Received: ....
(...)
```

Your message to the following recipients cannot be delivered:

```
<MonsieurA@domaineC>
#550 5.1.1
The recipient's e-mail address was not found in the recipient's e-mail system.
(...)
```

L'en-tête global du courriel semble dans la majorité des cas légitime. Il ne semble pas « forgé ».

3 Le problème

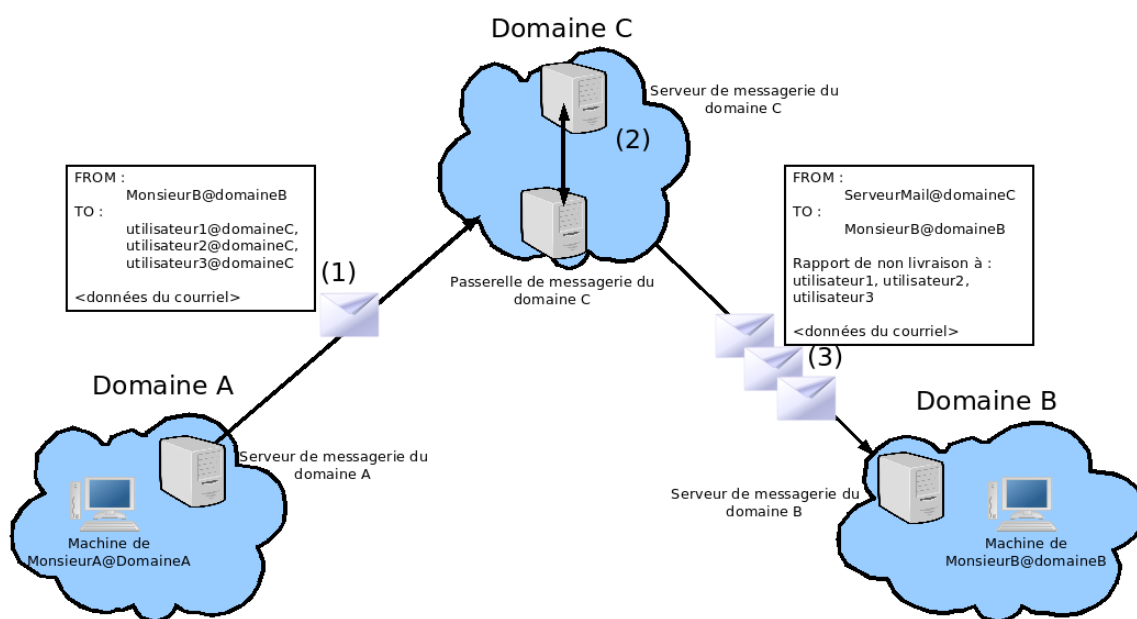
Ces courriels sont les « résidus » de messages envoyés avec une adresse émettrice usurpée et ayant provoqué un message de retour. La cause de ce message de retour peut être :

- l'utilisateur n'existe pas ;
- l'utilisateur a sa boîte de message électronique qui a atteint sa taille maximale autorisée ;
- l'utilisateur est en congé, et il s'agit d'une réponse automatique ;
- le message est refusé car déclaré dangereux (code malveillant ou format de fichier filtré...).

Le terme *backscatter* (« rétrodiffusion » en français) a été utilisé récemment pour caractériser ce comportement. Certains parlent plus justement de "*e-mail backscatters*". Cela peut se définir comme des messages de réponse non sollicités.

Il s'agit donc initialement bien d'une usurpation d'adresse électronique. Cependant, le second problème provient du comportement très hétérogène des serveurs de messagerie.

Dans le meilleur des cas concernant la figure 1, c'est le serveur émetteur de monsieurB qui devrait retourner un rapport de non remise après avoir obtenu une erreur "550 no such user" du serveur de domaineC.



- (1) : envoi d'un courriel usupant l'adresse d'un utilisateur du domaine B
 (2) : réception du courrier par le serveur légitime du domaine C
 (3) : envoi d'un rapport de non livraison au serveur de messagerie du domaine B

FIG. 1 – Schéma présentant un scénario de production de "backscatter"

Cependant le serveur de domaineC ne traite pas toujours directement la réception (usage de passerelles). Sur le schéma précédent, le serveur de domaineC va générer des messages d'erreur qui seront retransmis par la passerelle de messagerie.

Par ailleurs, le comportement peut varier si le message d'origine contient plusieurs destinataires. Pour un message envoyé avec une adresse usurpée, cette dernière peut recevoir autant de messages d'erreur que de destinataires erronés. Ce comportement n'est pas souhaité par le standard RFC 2821 mais est mis en oeuvre par certains serveurs.

Le standard est flou concernant le contenu du message d'erreur : celui-ci doit permettre d'identifier le message d'origine, mais il n'est pas nécessaire de copier tout le corps au format texte ni les pièces jointes.

4 Les motivations

Des personnes malveillantes peuvent être amenées à utiliser les propriétés précédentes pour différentes raisons :

- cibler le serveur de domaineC : le lecteur aura compris que pour un courriel envoyé, cela peut générer le traitement de celui-ci et l'émission d'une ou plusieurs réponses. Ces actions peuvent provoquer une gêne du service de messagerie, mais aussi au niveau de la bande passante générale, si les pièces jointes sont effectivement recopiées dans les messages d'erreur. Cet envoi indirect permet d'amplifier le trafic ;
- déterminer les adresses fonctionnelles du domaineC. Seules celles ne provoquant pas d'erreur récupérées par ailleurs sont acceptées par le serveur. Dans ce cas, la personne malveillante contrôle la machine émettrice (celle de monsieurA), ainsi que celle de réception (celle de monsieur B) ;
- atteindre indirectement monsieurB pour :
 - lui faire parvenir du *spam* indirectement. Ce dernier semble émis de domaineC. Le pourriel peut contenir des liens vers des sites de filoutage ou vers des pages Web au contenu dangereux pour le navigateur ;
 - remplir sa boîte aux lettres jusqu'à saturation. Les filtrages ne sont pas simples, car les sources émettrices peuvent être très différentes (les serveurs manipulés comme domaineC), et la solution consistant à filtrer tout message d'erreur peut être mal perçue par les utilisateurs. Ces derniers n'ont plus de réel moyen pour savoir si leur courriel est envoyé à la bonne adresse, l'accusé de réception étant émis au bon-vouloir du destinataire.

5 Que faire en cas de réception importante de courriels de ce type ?

Il n'existe pas de solution absolue. Les messages d'erreur sont légitimes et intrinsèques au fonctionnement de *SMTP*. Ils peuvent cependant se manifester par un volume anormal de messages que le serveur a du mal à gérer correctement et provoquent ainsi un déni de service.

Certaines solutions sont proposées ci-dessous :

- mise en place d'une passerelle en amont gérant un premier filtrage, afin de délester la tâche du serveur ;
- mise en place de serveurs MX supplémentaires en cas d'indisponibilité temporaire de l'un d'eux ;
- définition au niveau réseau d'une liste « blanche » ou de confiance des serveurs courants. Une priorité plus importante peut être éventuellement donnée aux communications avec ceux-ci ;
- mise en place de limitations ou quotas de connexions, au niveau du pare-feu ou du service de messagerie ;
- filtrage de certains champs d'en-tête par le serveur de messagerie, quand cette fonctionnalité est offerte. Attention! Cela peut aussi avoir des impacts sur des messages légitimes. Par exemple, il est possible dans Postfix de personnaliser le fichier `/etc/postfix/header_checks` afin de limiter la réception des rapports de livraison de courriels aux seuls domaines dont il a la charge :

```
/^Content-Type: multipart\/report; report-type=delivery-status\/; / REJECT
no third-party DSNs
```

```
/^Content-Type: message\/delivery-status; / REJECT no third-party DSNs
```

Il est également possible de filtrer certaines adresses. Sous Postfix, une solution consiste à ajouter une liste dans `smtpd_recipient_restrictions` et/ou `smtpd_sender_restrictions` :

Ajout d'une ligne comme :

```
check_sender_access hash:/chemin_Postfix/maps/access_sender
```

Et dans le fichier `/chemin_Postfix/maps/access_sender` :

```
serveurMail@domaineC REJECT
```

Puis lancer la commande :

```
postmap access_sender
```

- le filtrage vérifiant la légitimité des utilisateurs émetteurs (aussi appelé SAV pour *Sender Address Verification* ou *callback*). Cette technique est supportée par Exim et Postfix. Elle consiste à contrôler l'adresse de retour. Néanmoins, son impact reste limité quand les courriels utilisent des adresses émettrices existantes ;
- utiliser des propriétés dédiées aux applications déployées. Ainsi, il existe pour l'outil SpamAssassin des outils pour définir des règles dédiées : `VBounceRuleset` ;
- surveiller les journaux de messagerie, en s'aidant si besoin d'utilitaires comme `logparser` (pour les journaux Exchange) ou `maillogconverter.pl` du projet `awstats` (pour les journaux Postfix, `sendmail` ou `qmail`). Les commandes en ligne classiques (`cut`, `sort`, `cat`, `sed`, etc.) sont aussi très pratiques pour analyser des points particuliers dans les journaux ;
- vérifier la légitimité de l'adresse IP pour émettre sur le domaine. Même si cette mesure ne limite en rien la réception de *NDR*, elle permet d'assurer un contrôle sur son réseau des machines autorisées à émettre des courriels.

6 Documentation

- Site du projet `awstats`, page de configuration pour les journaux de messagerie :
http://awstats.sourceforge.net/docs/awstats_faq.html#MAIL
- RFC 5321, "Simple Mail Transfer Protocol", octobre 2008 :
<http://www.ietf.org/rfc/rfc5321.txt>
- RFC 3464, "An Extensible Message Format for Delivery Status Notifications", janvier 2003 :
<http://www.ietf.org/rfc/rfc3464.txt>
- RFC 3834, "Recommendations for Automatic Responses to electronic Mail", août 2004 :
<http://www.ietf.org/rfc/rfc3834.txt>
- RFC 821, "Simple Mail Transfer Protocol", août 1982 :
<http://www.ietf.org/rfc/rfc821.txt>
- Note d'information, "Postfix Address Verification Howto" :
http://www.postfix.org/ADDRESS_VERIFICATION_README.html

- Notes concernant VBounceRuleset pour SpamAssassin :
<http://wiki.apache.org/spamassassin/VBounceRuleset>
- S. Frei, I. Silvestri, G. Ollmann, "Mail Non-Delivery Message DDoS Attacks", 2004 :
<http://www.techzoom.net/publications/mail-non-delivery-attack/index.en>
- Note d'information CERTA-2008-INF-002 du 25 juillet 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002/>
- Note d'information CERTA-2005-INF-004 du 03 octobre 2005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/>

Gestion détaillée du document

19 décembre 2008 version initiale.