SPAM: Analyser vous-même une En-tête de Mail – Partie 2

11/05/2021

Bonjour le Monde !

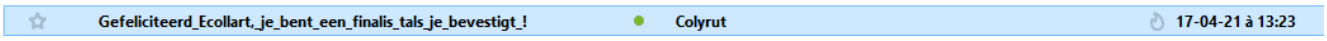
3e article d'une série de 4 sur le sujet (le 4e sera un résumé-conclusion), **nous allons cette fois analyser l'en-tête d'un vrai SPAM** !

Pour afficher l'en-tête d'un mail avec votre programme, reportez-vous au 1er article section « Comment détecter un SPAM vous-même ? »
Tous les programmes ne permettent malheureusement pas d'afficher l'en-tête d'un mail sans l'ouvrir (ce qui devrait pourtant être un « must ») et **je fournis donc un exemple de SPAM au format texte complètement inoffensif à télécharger au bas de cet article** ou depuis le 1er article pour pouvoir l'afficher et suivre les explications fournies ici.

Le SPAM analysé ici semble avoir été envoyé par Colruyt; voyons voir si c'est bien vrai !

Veuillez noter que j'ai remplacé manuellement le "@" de mes adresses mail par " at " pour ne pas que ces adresses soient capturées par des robots automatiques.

Voici comment ce message apparaît dans le dossier SPAM de ma boîte mail Gmail (vue depuis Thunderbird):



Déjà l'objet est en néerlandais, écrit bizarrement avec des « _ » et mon nom n'est pas celui que connaît Colruyt (supermarché) chez qui je suis effectivement client et où j'ai une carte de fidélité.

Si je devais voir un tel mail dans ma boîte de réception, je l'efface immédiatement ou le déclare comme SPAM (je reparlerai de cela dans le 4e et dernier épisode).

Analysons ce message pour le plaisir de lire et comprendre les entrailles d'un mail douteux:

Pour savoir extraire juste l'en-tête du message complet utile pour l'analyse, reportez-vous au 2e article où j'explique comment faire.

Voici l'en-tête du message soi-disant de Colruyt que nous allons analyser:

```
Delivered-To: ecollart at gmail.com
Received: by 2002:a19:550d:0:0:0:0:0 with SMTP id
n13csp1102833lfe;
Sat, 17 Apr 2021 04:23:58 -0700 (PDT)
X-Google-Smtp-Source:
ABdhPJxpjuBKol13YAHXd55j3+wyH/qpBVrvt1GMe2PjWP03DqkyYgcI3nFZkf
p1aLGvxdGJydIF
X-Received: by 2002:adf:d228:: with SMTP id
k8mr3861554wrh.341.1618658637916;
Sat, 17 Apr 2021 04:23:57 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1618658637; cv=none;
d=google.com; s=arc-20160816;
b=Y6xE6mRPdsJF/VNChrgbT5dGBYvPbr1aHhgWkxCLX6zLjV4P/uE+hyVVHdSt
```

8Sh6hu
BPvDhtBTLhdqAubFbBFC4RhGcNKw4LmiYFLPrtRQ/NLJ5JskAMZzS+Fdm4Hszd
HkpLeH
D8fqROytL1sXu5mYFaxX4+LeHczkNW78QA9T+hdYTvsZuMiKCKZ0m7mI0NiQoF
LsGBA/
2DF5mcWtSDKSyI+JknljTPF3EXddD4HRN1PuzlsuajFQXFGkxtgubgwa9aQ0pD
dHb39m
JUYdryYyDDLB9XjjEk8BKlj5uppzWpn5EWDXZGF/6c6xF7MHGYwwrZxuekdTHz
yIGKYG
9X6w==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed;
d=google.com; s=arc-20160816;
h=mime-version:subject:message-id:to:reply-to:from:date
:dkim-signature;
bh=9v7h5TRshvd7prTbAzKv9TB3K0txb0BUX3pkbQntuck=;
b=VjzU9LPMwsdGiGiuNY8oQ8etDymHh1Xmnbf6Yibe9Uv7duFGHsGWj3rYQIxE
vwoKcc
Yu2qNRdRSuwUwkbmRgNH2sG51vyjD30jFM8DW/SqLNX+KFdDefSx3aUjy4aa1p
XTBs57
FLkykyWWX0uWAq2C33vosKVXlekmiKWQmj/+D9mPAMq5CcZ8P45vYO3Op2UIDS
ZtB6gO
0uhyIbyuUrwUnZW5b28x9680yY3Dbhgab0Os1h4iHYaWBxETPhE8hE7fKg1sQz
WJoZWS
dISp9/309x+R5FznxmBZqEq2Xzg99S0srZ1QahtbXuI5yRiqNXZz1fFw3L8DaL
9jb0J8
ln4g==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=neutral (body hash did not verify)
header.i=@thedailybeast.com header.s=Sailthru
header.b=R9YCG6WN;
spf=pass (google.com: best guess record for domain of
751592091m163265@qlidxu4konpacop————————.193-169-20-19.ip323.
fastwebnet.it designates 193.169.20.19 as permitted sender)
smtp.mailfrom=751592091m163265@qlidxu4konpacop————————.193-16
9-20-19.ip323.fastwebnet.it
Return-Path:
<751592091m163265@qlidxu4konpacop————————.193-169-20-19.ip323

.fastwebnet.it>
Received: from missogirldrive.fr (193-169-20-19.ip323.fastwebnet.it. [193.169.20.19])
by mx.google.com with ESMTP id e12si4977936wrg.67.2021.04.17.04.23.57
for <ecollart@gmail.com>;
Sat, 17 Apr 2021 04:23:57 -0700 (PDT)
Received-SPF: pass (google.com: best guess record for domain of 751592091m163265@qlidxu4konpacop————————.193-169-20-19.ip323.fastwebnet.it designates 193.169.20.19 as permitted sender) client-ip=193.169.20.19;
Authentication-Results: mx.google.com;
dkim=neutral (body hash did not verify) header.i=@thedailybeast.com header.s=Sailthru header.b=R9YCG6WN;
spf=pass (google.com: best guess record for domain of 751592091m163265@qlidxu4konpacop————————.193-169-20-19.ip323.fastwebnet.it designates 193.169.20.19 as permitted sender) smtp.mailfrom=751592091m163265@qlidxu4konpacop————————.193-169-20-19.ip323.fastwebnet.it
Received: from njmta-53.sailthru.com (173.228.155.53) by dailybeast-a.sailthru.com id h1t86m1qqbs3 for <kzfyof@gmail.com>; Fri, 3 Jan 2020 09:30:14 -0500 (envelope-from <delivery@mx.sailthru.com>)
Received: from nj1-madbrick.flt (172.18.20.7) by njmta-53.sailthru.com id h1t7vc1qqbsf for <kzfyof@gmail.com>; Fri, 3 Jan 2020 09:30:10 -0500 (envelope-from <delivery@mx.sailthru.com>)
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; t=1578061810; s=Sailthru; d=thedailybeast.com; h=Date:From:Reply-To:To:Message-ID:Subject:MIME-Version:Content-Type:List-Unsubscribe; bh=R9YCG6WN+R9YCG6WN=;
b=R9YCG6WN+PSEEOFBXSF/R9YCG6WN+CKSDKET9OO3
CYA1P7IYL/VXDYPRM9LUVKTJ5O7ZAT/NFWKGSUGFV59UD9+
1ZRPW5VCED7WX+MXUVJ8C+R9YCG6WN=

```
From:                                   =?UTF-8?B?Q29seXJ1dA==?=
<nooreply@TYO5.systemprinters.com>
Reply-To: <el@craziesjohn.cellsmutations.com>
To: ecollart@gmail.com
Message-ID: <25249611.17770738385.34128885@sailthru.com>
Subject:
=?UTF-8?B?R2VmZWxpY2l0ZWVyZF9FY29sbGFydCxfamVfYmVudF9lZW5fZmlu
YWxpc190YWxzX2plX2JldmVzdGlndF8h?=
MIME-Version: 1.0
Content-Type:
multipart/alternative;boundary=    »281567-751592091m163265-
S54AVBPTFE15-2N5NP35-XEW1SIWG »
```

Rappelez-vous qu'une analyse d'en-tête commence par sa dernière ligne:

```
MIME-Version: 1.0
Content-Type:
multipart/alternative;boundary=    »281567-751592091m163265-
S54AVBPTFE15-2N5NP35-XEW1SIWG«
```

Ici tout est normal, MIME est utilisé pour encoder le message (voir 1er article) et le corps du message commence à partir de la ligne contenant « 281567-751592091m163265-S54AVBPTFE15-2N5NP35-XEW1SIWG » précédé de quelque traits-d'union « – »

Ligne suivante:

```
Subject:
=?UTF-8?B?R2VmZWxpY2l0ZWVyZF9FY29sbGFydCxfamVfYmVudF9lZW5fZmlu
YWxpc190YWxzX2plX2JldmVzdGlndF8h?=
```

L'objet du mail est encodé en UTF-8 (ce qui est normal) mais on ne sait pas

repérer un seul mot en clair ! **C’est déjà moins normal même si possible et voici un premier indice faisant penser que ce message est peut-être un SPAM !**

On continue:

```
To: ecollart@gmail.com
Message-ID: <25249611.17770738385.34128885@sailthru.com>
```

Ce message m’est bien adressé (ecollart@gmail.com) et semble avoir été créé par un serveur mail du domaine « **sailthru.com** » qui ne doit sans doute pas avoir grand-chose à voir avec Colruyt.

Une petite recherche dans un WHOIS (« qui c’est » en anglais) permet d’en savoir plus sur le domaine « sailthru.com »; vous pouvez faire ça par exemple sur https://www.whois.com/whois

Voici un extrait de la réponse du WHOIS:

```
Registrant Name: Finance Team
Registrant Organization: Sailthru, Inc.
Registrant Street: 1 World Trade Center, Suite 48A
Registrant City: New York
Registrant State/Province: New York
Registrant Postal Code: 10007
Registrant Country: US
Registrant Phone: +1.8778128689
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: zones@sailthru.com
```

Ici on commence par le haut et on voit que c’est l’entité juridique « Finance Team » de la compagnie « Sailthru Incorporated » qui a acheté le domaine sailthru.com.

Comme on ne trouve aucune autre indication se référant à Sailthru Inc dans l'en-tête ni avec Colruyt, nous sommes devant un indice fort que le message soit un SPAM !

L'information de l'en-tête du mail peut avoir été falsifiée pour faire croire qu'un serveur de mail valide a été utilisé.
Il se peut aussi que ce serveur `njmta-53.sailthru.com` ait été compromis et soit sous contrôle d'un pirate qui l'utilise pour envoyer ses SPAMs
L'information fournie par un WHOIS est en principe exacte mais on peut faire une vérification croisée sur plusieurs WHOIS différents pour être certain (oui, ce serveur WHOIS pourrait être contrôlé par des pirates mais il est fort peu probable que tous les WHOIS soient contrôlés par des pirates).

Ligne suivante:

```
Reply-To: <el@craziesjohn.cellsmutations.com>
```

Le « Reply-To » n'a rien à voir avec la compagnie Sailthru Inc. comme un check WHOIS pour le domaine « cellsmutations.com » peut le confirmer (le registrant du domaine cellsmutations.com serait Islandais).

Toujours rien à voir avec Colruyt. Voilà un autre indice fort indiquant que ce message est probablement un SPAM.
Si en plus le Reply-To et le « From » sont différents, c'est plus que probablement un SPAM !

Voyons voir la suite:

```
From:                                =?UTF-8?B?Q29seXJ1dA==?=
<nooreply@TYO5.systemprinters.com>
```

Et voilà un « From » complètement différent du « Reply-To » (même pas le même domaine qui est le nom après le « @ ») et toujours rien à voir avec

Colruyt ce qui est une très forte indication de SPAM !

Continuons l'analyse:

```
Received: from njmta-53.sailthru.com (173.228.155.53) by
dailybeast-a.sailthru.com id h1t86m1qqbs3 for
<kzfyof@gmail.com>; Fri, 3 Jan 2020 09:30:14 -0500 (envelope-
from <delivery@mx.sailthru.com>)
Received: from nj1-madbrick.flt (172.18.20.7) by
njmta-53.sailthru.com id h1t7vc1qqbsf for <kzfyof@gmail.com>;
Fri, 3 Jan 2020 09:30:10 -0500 (envelope-from
<delivery@mx.sailthru.com>)
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt;
c=relaxed/simple; t=1578061810; s=Sailthru;
d=thedailybeast.com; h=Date:From:Reply-To:To:Message-
ID:Subject:MIME-Version:Content-Type:List-Unsubscribe;
bh=R9YCG6WN+R9YCG6WN=;
b=R9YCG6WN+PSEEOFBXSF/R9YCG6WN+CKSDKET9003
CYA1P7IYL/VXDYPRM9LUVKTJ5O7ZAT/NFWKGSUGFV59UD9+
1ZRPW5VCED7WX+MXUVJ8C+R9YCG6WN=
```

Rien à dire à la date sinon que le serveur qui a envoyé ça a son horloge réglée sur le fuseau horaire EDT en GMT-4.
Le DKIM m'a l'air un peu alambiqué mais je ne m'y connais pas suffisamment pour en dire plus.
Il y a 2 « Received: » et même encore un troisième plus haut ! **C'est aussi une indication que quelque chose ne va sans doute pas** même si ça peut être aussi dû à un serveur de mail ayant un souci. On y voit aussi que l'expéditeur supposé est `kzfyof@gmail.com` qui n'a à nouveau pas grand-chose à voir avec Colruyt.

Lorsque vous envoyez un mail, il y a 1,2 ou 4 serveurs impliqués suivant que votre destinataire est chez le même fournisseur de messagerie que vous ou pas.
Disons que vous êtes chez Gmail et que votre destinataire est chez Yahoo, les serveurs mail impliqués seront celui de Gmail sur lequel est située votre boîte aux

lettres électronique, le serveur Gmail qui expédie ce message à l'extérieur de Gmail, celui d'entrée de Yahoo et enfin celui de Yahoo qui contient la boîte aux lettres électronique de votre destinataire. Il y en donc 2 chez l'expéditeur et 2 chez le destinataire.
Si vous en voyez plus que cela ou si ils sont de différents domaines, c'est très louche !

Essayons de voir plus loin:

```
Received-SPF: pass (google.com: best guess record for domain of
751592091m163265@qlidxu4konpacop——————————.193-169-20-19.ip323.fastwebnet.it designates 193.169.20.19 as permitted sender) client-ip=193.169.20.19;
Authentication-Results: mx.google.com;
dkim=neutral (body hash did not verify) header.i=@thedailybeast.com header.s=Sailthru header.b=R9YCG6WN;
spf=pass (google.com: best guess record for domain of 751592091m163265@qlidxu4konpacop——————————.193-169-20-19.ip323.fastwebnet.it designates 193.169.20.19 as permitted sender) smtp.mailfrom=751592091m163265@qlidxu4konpacop——————————.193-169-20-19.ip323.fastwebnet.it
```

Dans la ligne « Authentication-Results », on voit que Gmail n'a pas réussi à analyser le DKIM et indique un « dkim=neutral » au lieu de « dkim=pass » ce qui n'est paaaas bon !
Par contre on voit aussi que l'autre protection SPF a été validée comme non-spammeur par un serveur fastwebnet.it et que Gmail lui fait confiance car on voit « spf=pass ».

Mais encore:

```
Return-Path:
<751592091m163265@qlidxu4konpacop——————————.193-169-20-19.ip323
.fastwebnet.it>
Received:            from            missogirldrive.fr
(193-169-20-19.ip323.fastwebnet.it. [193.169.20.19])
by       mx.google.com       with       ESMTP       id
e12si4977936wrg.67.2021.04.17.04.23.57
for <ecollart at gmail.com>;
Sat, 17 Apr 2021 04:23:57 -0700 (PDT)
```

Et voilà le 3e « Received: » très louche car il y a fort peu de chance que ce serveur soit légitime avec un nom de domaine pareil (missogirldrive.fr) semblant être situé en France (.fr) mais avec une horloge réglée sur le fuseau horaire PDT en GMT-7 !
Le « Return-Path » rajoute une couche aux doutes précédents car semblant renvoyer le message en cas d'erreur vers ce serveur fastwebnet.it…

Voilà, le reste des informations ont été rajoutées par Gmail et sont tout-à-fait valides.

Je peux vous dire que Gmail a directement versé ce message dans le dossier SPAM de ma boîte mail où j'ai été le récupérer pour les besoin de cette série d'articles qui vous aideront, je l'espère, à décider si SPAM ou non en cas de doute et qui ont un peu démystifié le fonctionnement du courrier électronique sur Internet.

Li P'ti Fouineu vous salue bien !

Ressources:

- le 1er article intitulé « **SPAM, l'Arme des Cybercriminels mais pas que !**«
- le 2e article intitulé « **SPAM: Analyser vous même une En-tête de**

Mail – Partie 1«

- le 3e et dernier article est celui que vous lisez et qui s'intitule « **SPAM: Analyser vous même une En-tête de Mail – Partie 2**«

Ouvrir En-tête SPAM Colruyt reçu sur Gmail dans un nouvel onglet
ou le télécharger:

Télécharger