

17/02/2022, Le Plessis-Robinson, France

A tous ceux qui sont concernés,

Depuis un certain temps, il semble que certains de nos partenaires reçoivent périodiquement des courriels prétendant être initiés par l'AETA :

- Christophe Mahoux
- Thomas Fengel

Ces emails sont des scams et doivent être ignorés car ne proviennent pas d'AETA et après de nombreuses investigations, nous pouvons confirmer que le réseau d'AETA n'a pas été piraté.

Il semble en fait qu'il existe une base de données sur le web qui relie certains membres du personnel d'AETA (anciens et actuels) à certains partenaires. Il n'y a malheureusement aucun moyen pour nous de l'effacer. Nous avons cependant pris des mesures pour que cette base de données ne soit pas mise à jour / élargie.

Identifier que l'email ne provient pas de l'AETA est quelque chose qui peut être fait au niveau du destinataire de l'email frauduleux. Dans ce document, nous aimerions décrire les quelques étapes qui vous permettront de reconnaître si l'email provient de l'AETA ou non.

Dans les exemples ci-dessous, on peut voir deux en-têtes d'email :

- Un faux email prétendant provenir de tfengel@aeta-audio.com
- Un autre qui provient réellement de vboulben@aeta-audio.com

Faux email

```
Received: from p3plwbeout12-03.prod.phx3.secureserver.net
(p3plsmtp12-03-2.prod.phx3.secureserver.net. [173.201.192.58]) by
mx.google.com with ESMTPS id x23si3889959pgf.148.2021.09.30.06.02.38
for <recipient> (version=TLS1_2
cipher=ECDHE-ECDHE-AES128-GCM-SHA256 bits=128/128); Thu, 30 Sep 2021
06:02:38 -0700 (PDT)
Received: by 2002:adf:8bd3:0:0:0:0 with SMTP id w19csp317956wra; Thu,
30 Sep 2021 06:02:39 -0700 (PDT)
Received: (gmail) 25122 invoked by uid 99); 30 Sep 2021 13:02:37 -0000
Received: from p3plgemwbe12-06.prod.phx3.secureserver.net ([173.201.192.27])
by :WBEOU: with SMTP id VvhumotCj8oPvVvhumBkFF; Thu, 30 Sep 2021 06:02:38
-0700
Reply-To: Thomas Fengel <distributorssales101@gmail.com>
From: Thomas Fengel <tfengel@aeta-audio.com>
To: Thomas Fengel <tfengel@aeta-audio.com>
Subject: Re: Sales Update
Date: Thu, 30 Sep 2021 13:02:35 +0000
Message-ID: <20210930060234.76cbecca3158562e8542cc5b3e1edb3c.78b8a1f30c.wbe@email12.godaddy.com>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_6831_01D7ED0F.22E1E180"
X-Mailer: Microsoft Outlook 16.0
X-Google-Smtp-Source: ABdhPJwDWN8CBAJduDT9mSQasN/VQ2v8msZvggf5kLnic18A/CCObq6NNFXQFhVnM6o5BXwq5LxS
X-Received: by 2002:a17:90b:2382:: with SMTP id mr2mr2108882pjb.148.1633006959106;
Thu, 30 Sep 2021 06:02:39 -0700 (PDT)
```

AETA AUDIO Systems SAS
La Boursidière
Rue de la Boursidière - BP 82
F-92357 LE PLESSIS ROBINSON CEDEX – FRANCE
Tel : +33.1.41.36.12.00 – <http://www.aeta-audio.com>
SIRET 478 301 351 00027 – APE 2630Z - VAT : FR 40478301351



Authentication-Results: mx.google.com;

spf=neutral google.com: 173.201.192.58 is neither permitted nor denied by best guess record for domain of noor@twaijri.com)

smtp.mailfrom=noor@twaijri.com

X-EsetId: 37303A2963C2DE6C657560

Thread-Index: AQJ1Qkby0Ma9vqHORYKoCRmJmN3f1Q==

X-MAE-Analysis: v=2.4 cv=Ztkol/3G c=1 sm=1 tr=0 ts=6155b56e

a=wlxwqOMWh9nWIR5XrkBuhA==:117 a=DdKd82aFokQA:10 a=X2v0K8pCV7sA:10

a=PB-mS-l7R5EA:10 a=lkTkHD0fZMA:10 a=7QKq2e-ADPsA:10 a=x7bEGLp0ZPQA:10

a=hrWrUuN9xXCKQDgcrPQA:9 a=wgdykqrbGx81Sef:21 a=_W_S_7VecoQA:10

a=QEXdDO2ut3YA:10 a=9N1BXz_py8oyCxFpwYrZ:22

X-SECURESERVER-ACCT: noor@twaijri.com

X-MAE-Envelope:

MS4xfC2pWNfj79Nle2n/0bAF1dfTDMoa4LBEzUzG874k0y4L+DKfDqZAx11yVrLVsKfYCaHB8YE4rAez6l8Dxsk1mgafm0a1iltKYPrHE+LGr6NQV
IKC8LB

gys0UEFc4yPGpCLuvPeu0mZ7wn6tp07RKLqcrSt77l+Stu5e9dG8L7lJUDJHWqcAO9aM2e5OES2bg565/uBXXoRwWAO1QO4TCrZnYAOnA24JLg
G+6Jr2ITC2

x-originating-ip: 105.112.77.29

X-SID: VvhumotCj8oPv

X-Sender: noor@twaijri.com

Vrai email de AETA

Received: from SERVER.aeta.local ([fe80::27f5:21d8:e5c7:814b]) by

SERVER.aeta.local ([fe80::27f5:21d8:e5c7:814b%11]) with mapi id

14.03.0513.000; Tue, 8 Feb 2022 16:14:12 +0100

Content-Type: application/ms-tnef; name="winmail.dat"

Content-Transfer-Encoding: binary

From: Vincent BOULBEN <VBOULBEN@aeta-audio.com>

To: Yann VONARBURG <YVONARBURG@aeta-audio.com>

Subject: TR: AETA Algorithm & latency information VRT

Thread-Topic: AETA Algorithm & latency information VRT

Thread-Index: Adgc/oVH4Ddix0jYT/WRMPTJZWLu4A==

Date: Tue, 8 Feb 2022 16:14:10 +0100

Message-ID: <A9839F3FFF70A04B9CC14E7F1BBA60868AF0D57B@SERVER.aeta.local>

Accept-Language: fr-FR, en-US

Content-Language: fr-FR

X-MS-Has-Attach: yes

X-MS-Exchange-Organization-SCL: -1

X-MS-TNEF-Correlator: <A9839F3FFF70A04B9CC14E7F1BBA60868AF0D57B@SERVER.aeta.local>

MIME-Version: 1.0

X-MS-Exchange-Organization-AuthSource: SERVER.aeta.local

X-MS-Exchange-Organization-AuthAs: Internal

X-MS-Exchange-Organization-AuthMechanism: 04

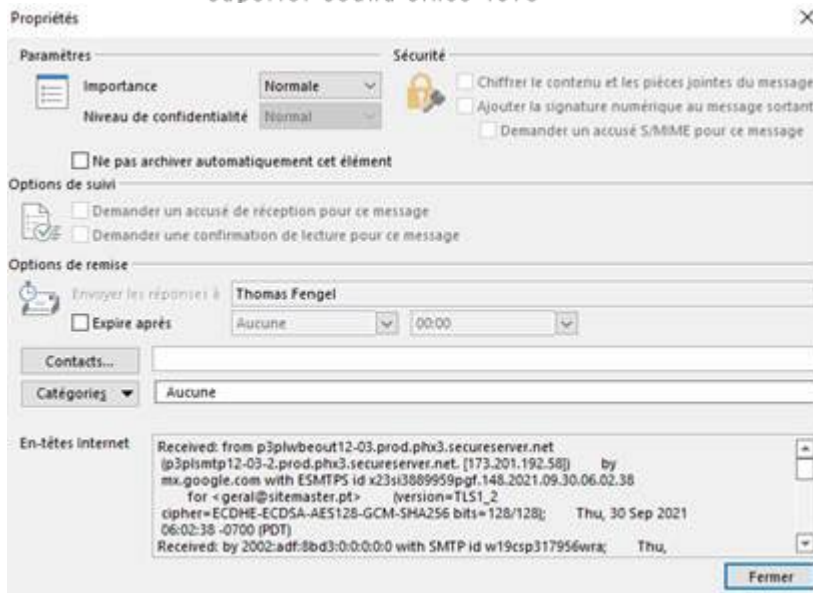
X-Originating-IP: [10.0.20.28]

Cet en-tête peut être extrait d'Outlook comme indiqué ci-dessous :

- Ouvrir l'email
- Cliquer sur " fichier ".
- Cliquer sur "propriétés".

En bas de la boîte, vous trouverez l'en-tête complet comme dans l'exemple ci-dessus.

AETA AUDIO Systems SAS
KEPLER 4 – 18/22, Avenue Edouard HERRIOT
F-92350 LE PLESSIS ROBINSON – FRANCE
Tel : +33.1.41.36.12.00 – Fax : +33.1.41.36.12.69 – <http://www.aeta-audio.com>
SIRET 478 301 351 0019 – APE 322A - VAT : FR 40478301351



Si un email provient d'AETA, "SERVER.aeta.local" doit être mentionné quelque part (comme surligné en jaune dans l'en-tête de l'email correct) et non "google" ou "gmail" (comme surligné en rouge dans l'en-tête de l'email SCAM).

De même, une adresse AETA correcte en tant qu'expéditeur doit apparaître (par exemple : "tfengel@aeta-audio.com") et non "noor@twaijri.com" ou distributorssales101@gmail.com. Ces adresses sont les adresses d'envoi réelles et ne sont en aucun cas liées au personnel d'AETA ou au serveur d'AETA.

Finalement, il est facile de savoir si un email provient réellement d'AETA ou non.

Nous espérons que cette note d'application vous aidera à faire le tri entre les e-mails AETA et les SCAM. Si vous avez des questions, n'hésitez pas à contacter votre contact AETA privilégié.