Analyse van een aantal haat- en dreigmails (7 juli 2015)

Van een aantal mails (31 haatmails en 14 legitieme mails) zijn de mailheaders geanalyseerd om aanwijzingen te vinden voor een veronderstelde hack. De geanalyseerde mails zijn verstuurd in de jaren 2012 tot en met 2015.

De mailheaders zijn in twee categorieën te verdelen:

1. Mails, verstuurd tot eind 2012. Tot die tijd stuurde Microsoft in de mailheader het attribuut 'X-Originating-IP' mee (het IP-adres van de verzender).
2. Mails, verstuurd na 2012. Microsoft stuurt het genoemde attribuut niet meer mee.

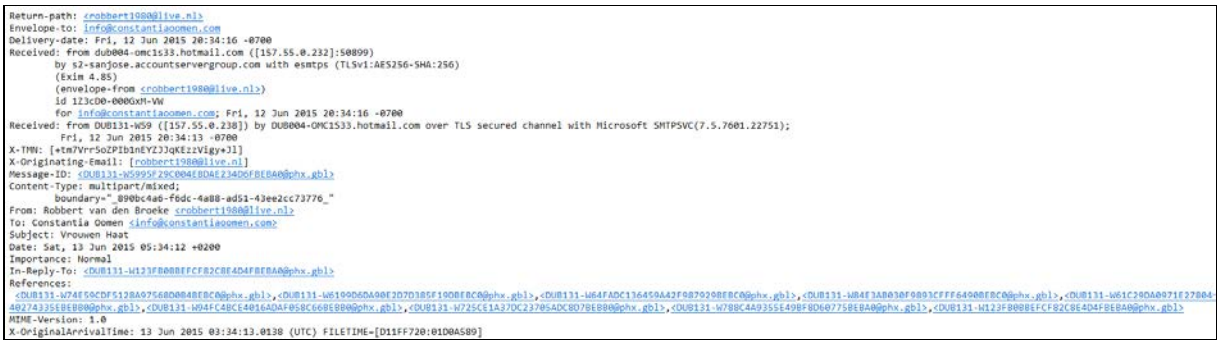
Voorbeelden van vier mailheaders binnen deze categorieën:

```
Delivered-To: constantiaoomen@gmail.com
Received: by 10.64.14.137 with SMTP id p9csp428198iec;
        Thu, 8 Nov 2012 17:38:27 -0800 (PST)
Received: by 10.180.107.136 with SMTP id hc8mr153143wib.9.1352425105588;
        Thu, 08 Nov 2012 17:38:25 -0800 (PST)
Return-Path: <robbert1980@live.nl>
Received: from dub0-omc3-s6.dub0.hotmail.com (dub0-omc3-s6.dub0.hotmail.com. [157.55.2.15])
        by mx.google.com with ESMTP id l80si990972wep.57.2012.11.08.17.38.21;
        Thu, 08 Nov 2012 17:38:25 -0800 (PST)
Received-SPF: pass (google.com: domain of robbert1980@live.nl designates 157.55.2.15 as permitted sender) client-ip=157.55.2.15;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of robbert1980@live.nl designates 157.55.2.15 as permitted sender) smtp.mail=robbert1980@live.nl
Received: from DUB115-W138 ([157.55.2.8]) by dub0-omc3-s6.dub0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675);
         Thu, 8 Nov 2012 17:38:21 -0800
Message-ID: <DUB115-W138B3F03F23CC6BAF4B6439BE680@phx.gbl>
Return-Path: robbert1980@live.nl
Content-Type: multipart/mixed;
        boundary="_6c07d248-fc38-456a-992d-5867f6aa771f_"
X-Originating-IP: [84.86.208.170]
From: Robbert van den Broeke <robbert1980@live.nl>
To: <constantiaoomen@gmail.com>
Subject: Hoi Stenny
Date: Fri, 9 Nov 2012 02:38:21 +0100
Importance: Normal
In-Reply-To: <504D6373.4030906@constantiaoomen.com>
References:
 <SNT131-W52E21604195567D427942EEDAAC0@phx.gbl>,<504D6026.2020504@constantiaoomen.com>
 <SNT131-W27629927EB1B215859808FDAAC0@phx.gbl>,<504D6373.4030906@constantiaoomen.com>
MIME-Version: 1.0
X-OriginalArrivalTime: 09 Nov 2012 01:38:21.0470 (UTC) FILETIME=[E6D41BE0:01CDBE1A]
```

1. Headers van een mail verstuurd in 2012 (haatmail)

```
Delivered-To: stenoomen@gmail.com
Received: by 10.49.74.68 with SMTP id r4csp573082qev;
        Sun, 2 Sep 2012 16:28:56 -0700 (PDT)
Received: by 10.216.133.90 with SMTP id p68mr8250428wei.105.1346628535084;
        Sun, 02 Sep 2012 16:28:55 -0700 (PDT)
Return-Path: <robbert1980@live.nl>
Received: from dub0-omc1-s28.dub0.hotmail.com (dub0-omc1-s28.dub0.hotmail.com. [157.55.0.227])
        by mx.google.com with ESMTP id f2si17596920wiz.13.2012.09.02.16.28.54;
        Sun, 02 Sep 2012 16:28:55 -0700 (PDT)
Received-SPF: pass (google.com: domain of robbert1980@live.nl designates 157.55.0.227 as permitted sender) client-ip=157.55.0.227;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of robbert1980@live.nl designates 157.55.0.227 as permitted sender) smtp.mail=robbert1980@live.nl
Received: from DUB115-W134 ([157.55.0.238]) by dub0-omc1-s28.dub0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675);
         Sun, 2 Sep 2012 16:28:54 -0700
Message-ID: <DUB115-W134BCAC262899A918267122BEA40@phx.gbl>
Return-Path: robbert1980@live.nl
Content-Type: multipart/alternative;
        boundary="_e95c7d89-00a5-4ae4-9119-10e949dc2bc6_"
X-Originating-IP: [84.86.208.170]
From: Robbert van den Broeke <robbert1980@live.nl>
To: <stenoomen@gmail.com>
Subject: Hoi Constantia
Date: Mon, 3 Sep 2012 01:28:54 +0200
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 02 Sep 2012 23:28:54.0668 (UTC) FILETIME=[B7C6ECC0:01CD8962]
```

2. Headers van een mail verstuurd in 2012 (legitieme mail)



3. Headers van een mail verstuurd in 2015 (haatmail)

```
Return-path: <robbert1980@live.nl>
Envelope-to: info@constantiaoomen.com
Delivery-date: Thu, 15 Jan 2015 17:25:44 -0800
Received: from dub004-omc1s15.hotmail.com ([157.55.0.214]:63455)
        by s2-sanjose.accountservergroup.com with esmtps (TLSv1:AES256-SHA:256)
        (Exim 4.82)
        (envelope-from <robbert1980@live.nl>)
        id 1YBvfT-000Afb-Uc
        for info@constantiaoomen.com; Thu, 15 Jan 2015 17:25:44 -0800
Received: from DUB131-W74 ([157.55.0.237]) by DUB004-OMC1S15.hotmail.com over TLS secured channel with Microsoft SMTPSVC(7.5.7601.22751);
         Thu, 15 Jan 2015 17:25:42 -0800
X-TMN: [iFj2DpvCG9rAs2zDFH7Xlfe/dUIF/ieP]
X-Originating-Email: [robbert1980@live.nl]
Message-ID: <DUB131-W74FAA133630FFD772A7574BE4F0@phx.gbl>
Content-Type: multipart/alternative;
        boundary="_0b71a14e-f764-45d8-bfc2-96f9e020c83e_"
From: Robbert van den Broeke <robbert1980@live.nl>
To: Constantia Oomen <info@constantiaoomen.com>
Subject: leuke boekjes lees je
Date: Fri, 16 Jan 2015 02:25:41 +0100
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 16 Jan 2015 01:25:42.0287 (UTC) FILETIME=[57F679F0:01D0312B]
```

4. Headers van een mail verstuurd in 2015 (legitieme mail)

Authenticatie

Het is mogelijk om bepaalde mailheaders te vervalsen (*spoofen*). Heel eenvoudig kan dat al door in het mailprogramma het ‘From’ of ‘Reply-to’ adres aan te passen. Deze headers zijn dan ook niet betrouwbaar, en hier ook niet interessant. Bij de geanalyseerde mails zijn de ‘lijntjes’ tussen de mailservers kort. De ontvangende mailserver krijg de mail van de verzendende mailserver: die van Microsoft. Microsoft geeft een aantal referenties mee die wijzen op een betrouwbare authenticiteit van de verzender. De ‘Received’ headers zijn betrouwbaar. Een onderdeel van deze ‘Received’ headers is het attribuut ‘envelope-from’ (dat Microsoft de laatste jaren meegeeft als headerinformatie). En de waarde hierbij is altijd: ‘robbert1980@live.nl’ (zowel bij de haatmails als de legitieme mails). Dit wijst erop dat de mail daadwerkelijk is verstuurd binnen de Microsoft mailomgeving, met de *credentials* (inloggegevens) van de gebruiker. Er is geen sprake van (IP) spoofing. De mails, verstuurd tot en met 2012, bevatten (een combinatie van) andere headers die op hetzelfde wijzen. Bijvoorbeeld de header:

> *Authentication-Results: mx.google.com; spf=pass (google.com: domain of robbert1980@live.nl designates 157.55.2.15 as permitted sender) smtp.mail=robbert1980@live.nl*

De mail wordt hier door Microsoft afgeleverd aan Google (‘constantiaoomen@gmail.com).

De ‘minder betrouwbare’ headers zoals ‘From’, ‘Reply-to’ en ‘Return-path’ bevatten overigens wel de correcte informatie: ‘robbert1980@live.nl’.

IP en locatie

Tot eind 2012 wordt het IP-adres van de verzender meegestuurd (in de header 'X-Originating-IP'). Het IP-adres wordt toegekend aan de PC (of wireless router of proxy) en is te herleiden tot de unieke gebruiker.

In vrijwel alle gevallen (zowel de haatmails als de legitieme mails) is dit IP: 84.86.208.170. Internet providers leveren vaak dynamische IP-adressen. Het IP-adres van de gebruiker kan op een gegeven moment wijzigen. Omdat het IP-adres hier over de hele geanalyseerde periode hetzelfde is, is het uitgesloten dat dit IP-adres het ene moment aan de legitieme afzender toekomt, en op een ander moment aan een mogelijke hacker (en vervolgens weer aan de legitieme afzender).
De service 'WHOIS' geeft informatie over de eigenaar (provider) van dit IP, en mogelijk een indicatie van de geografische toekenning van dit adres. Momenteel is de WHOIS informatie:

> KPN B.V., Amersfoort (informatie van 2 april 2003; laatste update: 26 juni 2015).
> Dit IP-adres draagt op dit moment de hostnaam 'ip5456d0aa.speed.planet.nl'.

In twee gevallen bevat een legitieme mail (afkomstig van 'stan_van_aalst@live.nl', 30 juli 2012) het IP-adres: 109.169.27.39.

Momenteel verwijst de WHOIS informatie van dit IP-adres naar 'Rapidswich Ltd, UK' als eigenaar. Historische referenties (ftp://ftp.ripe.net/pub/stats/ripencc/2012/) wijzen ook naar Groot Brittannië als 'territorium' waarbinnen dit IP-adres werd uitgedeeld:

> ripencc|GB|ipv4|109.169.0.0|16384|20091102|allocated

Binnen de geanalyseerde mails is gekeken of er haat- of dreigmails bestaan, die te herleiden zijn tot dit IP-adres. Dat blijkt niet het geval.

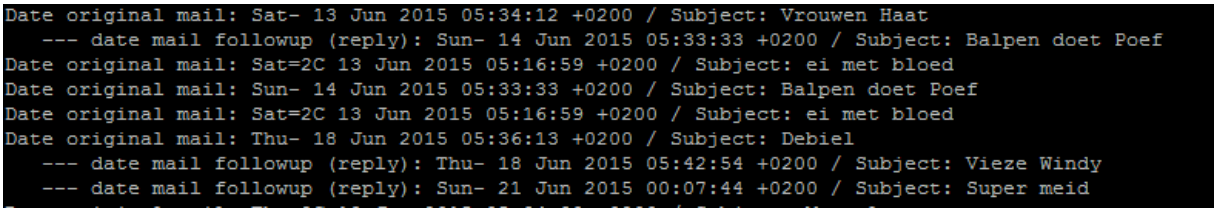
Referenties

Wanneer er vanuit Microsoft een mail wordt verstuurd, krijgt deze mail een uniek ID: het Message-ID. Dit 'Message-ID' wordt als mailheader meegestuurd. Een reply op deze mail bevat ook weer dit 'Message-ID', maar ook een nieuwe header: 'In-Reply-To', dat het ID bevat van de mail waarop wordt gereageerd. Bij meerdere replies (of forwards) bevat de header 'References' alle ID's van de voorgaande mails in de mailthread.

Vrijwel alle haatmails bevatten de header 'References', met meerdere ID's daarbij vermeld. Dat betekent dat een haatmail als bron is gebruikt om een nieuwe mail te sturen (bijvoorbeeld middels een reply op de oorspronkelijke haatmail, waarna het subject en de mailbody worden aangepast). Dit kan een eenvoudige manier zijn om snel een nieuwe mail te sturen, zonder het mailadres op te zoeken. Dat deze 'References' aanwezig zijn, impliceert dat er haatmails zijn opgeslagen in de mailbox, anders kunnen deze niet worden gebruikt om een nieuwe mail te sturen.

Met behulp van de drie headers ('Message-ID', 'In-Reply-To' en 'References') is het mogelijk om de hele keten (*thread*) van een mailing in kaart te brengen: welke mail is origineel opgesteld, en welke replies (of forwards) volgen er op welke mails?

De geanalyseerde mails vormen slechts een deelverzameling van het totaal; dus dit overzicht kan niet compleet in kaart worden gebracht.



Voorbeeld van een stukje mailketen die begint met een originele nieuwe mail. Artifacten van de haatmails hebben hier in ieder geval in de periodes 13 tot 14 en 18 tot 21 juni 2015 in de mailbox gestaan.

Het zou een nieuw perspectief opleveren wanneer een haatmail wordt gebruikt om een legitieme mail op te stellen. Want dan zou de legitieme verzender doelbewust een haatmail openen, om die nogmaals te versturen met andere inhoud. Dan zou in een legitieme mail, in de sectie 'References' het 'Message-ID' genoemd worden van een haatmail. In de beperkte verzameling geanalyseerde mails is deze koppeling niet gevonden.

Samenvatting voorlopige conclusies

1. De headers van de mail tonen (los van de mailinhoud) geen abnormaal beeld en geven geen aanleiding tot een verdenking van een hack. Zowel de legitieme mails als de haatmails tonen eenzelfde opbouw van de headers.
2. De haat- en dreigmails zijn verstuurd vanuit het account van 'robbert1980@live.nl', met de credentials van dat account.
3. In ieder geval tot eind 2012 zijn de haat- en dreigmails verstuurd vanuit hetzelfde IP-adres, en daarmee ook de locatie, als de legitieme gebruiker. Na 2012 is het IP-adres, en daarmee de locatie niet meer te achterhalen (behalve dan door de mailprovider zelf).
4. De haat- en dreigmails zijn overwegend verstuurd vanuit een bestaande haatmail (door middel van een reply, of forward hierop, met aanpassing van subject en inhoud). Daarom zullen een of meerdere haatmails langere tijd aanwezig moeten zijn geweest in de mailbox (bijv. in de 'sent items' folder) van de gebruiker.
5. Een hack 'op afstand' (zoals het 'overnemen' van de computer, om vervolgens mail te versturen namens de legitieme afzender) vereist hier een zeer ingewikkelde opzet, en wordt bovendien onwaarschijnlijk wanneer er beveiligingsmaatregelen op de PC en de mailclient zijn genomen. Goede beveiligingsmaatregelen en twee-factor authenticatie (tegenwoordig vrij gebruikelijk) voorkomen in de praktijk een (nieuwe) hack.

Mogelijke suggesties

Het zou voor toekomstig forensisch onderzoek interessant kunnen zijn:

1. Om de gehele mailketens (welke replies volgden op welke mails…) in kaart te brengen;
2. om ook hiermee te achterhalen of er een haat- of dreigmail is gebruikt om een legitieme mail te construeren. Hoewel er geen aanwijzingen zijn dat dit gebeurt is, kan dit – indien het wel voorkomt – een andere kijk op de zaak werpen.

Het kan hierbij interessant zijn (1) te weten wie de andere ‘getroffenen’ zijn en wat de hoeveelheid mailverkeer bij hen is geweest en (2) de mailheaders van die mails mee te nemen in het onderzoek.

Het staat vrij, en is zelfs aan te raden, om andere deskundigen hun mening te laten geven over de hier verrichtte analyse.

Het is aan te bevelen het misbruik (versturen van haat- en dreigmails) in ieder geval ook te melden aan het ‘abuse’ kontaktadres van de mailprovider: abuse@hotmail.com en mogelijk ook de eigen provider. Zij kunnen diepgaander onderzoek verrichten en indien nodig ook maatregelen treffen.