HeaderienTulkinta - Ei-toivottu viestintä Internetissä

Etusivu > SpammiinReagoiminen

Headerien tulkinta

Sisällys

Yleistä

Spämmivalitus on hyvä lähettää ainakin palveluntarjoajalle, jonka verkosta spämmi on lähetetty, ja spämmissä mainostettujen WWW-sivujen palveluntarjoajalle.

Spämmerin palveluntarjoaja selviää sähköpostiviestin **otsikkotietoja (headereita)** tutkimalla. Usein sähköpostispämmin headereita on kuitenkin yritetty väärentää, jotta viestin lähettäjän selvittäminen olisi vaikeampaa. Tässä dokumentissa annetaan pakostakin hiukan tekninen ohje headereiden tulkitsemiseen. Sivulla SpammiinReagoiminen kerrotaan laajemmin spämmiin reagoimisesta ja kenelle spämmistä voi ja kannattaa valittaa.

Headerien tulkinta onnistuu nopeasti ja vaivattomasti esimerkiksi SpamCopin automaattipalveluilla. Joskus on kuitenkin hyvä tietää itsekin, mistä on kyse.

Unix-käyttöjärjestelmän mukana tulevista työkaluista (host, traceroute, whois, dig, ...) on usein hyötyä spämmin alkuperän selvittämisessä. Jos näiden työkalujen käyttöön tai opetteluun ei ole mahdollisuutta, niin esimerkiksi DNS Stuff, SamSpade.org ja UXN tarjoavat nämä palvelut webbipohjaisina. Geektoolsin Whois -palvelun avulla saa selville IP-osoitteeseen liittyvän palveluntarjoajan.

SPAM-L-listan FAQ ja Stopspam.org:n ohje (englanniksi) sisältävät tätä dokumenttia kattavamman kuvauksen headerien tulkitsemisesta.

Spämmin lähettäminen, lyhyt oppimäärä

Sähköpostispämmit lähetetään usein seuraavalla tavalla:

Tyypillisesti spämmeri ottaa yhteyttä johonkin *postia välittävään koneeseen* väliaikaisesta osoitteesta. Postia välittävä kone voi olla *avoin rele* tai *-proxy* tai haittaohjelman saastuttama spämminvälityskoneena toimiva Windows-kone (ks. SvrVukk, “Mikä on avoin rele (open relay) ja miten se korjataan? Entä avoin välityspalvelin (open proxy)?”). Spämmereille tällaisestä postia välittävästä koneesta on kahdenlaista hyötyä: postinvälityskoneen avulla spämmeri voi peittää jälkensä. Toisekseen spämmeri voi pyytää välityskonetta lähettämään saman viestin usealle vastaanottajalle - näin spämmeri säästää aikaa ja välityskoneen omistaja maksaa spämmin lähettämisestä aiheutuvat tietoliikennekulut.

Pahimmassa tapauksessa viestin otsaketiedoista selviää vain Windows-madon saastuttaman välityskoneen osoite.

Headerien lisäksi kannattaa tutkia viestin sisältöä. Usein spämmissä yritetään myydä jotain ja jotta spämmeri saa mitään myytyä, pitää hänen antaa jonkinlaisia yhteystietoja (esim. webbisivun osoite). Nämä yhteystiedot voivat johtaa spämmerin jäljille.

Headerien tulkitseminen

Postiohjelmat eivät oletusarvoisesti näytä täydellisiä headereita. Ensimmäinen askel on täydellisten headerien saaminen näkyviin. Täydelliset headerit saa näkyviin postiohjelmasta riippuvalla tavalla.

Aluksi on hyvä ymmärtää miten sähköpostiviesti kulkee Internetissä. Viesti lähtee liikkeelle, kun *postiasiakas* (esimerkiksi postiohjelma tai spämmerin postitusohjelma) antaa viestin otsikon ja rungon postinvälityspalvelimelle.

Postiasiakkaan antama viestin otsikot sisältävät esimerkiksi Subject-, To- ja From-kentät. Siksi **spämmiviesteissä näkyviin To- ja From-osoitteisiin ei voi luottaa**, ne ovat yleensä spämmerin lisäämiä. Viestin runko sisältää tyypillisesti sähköpostin sisältönä olevan tekstin ja mahdolliset tiedostoliitteet.

Postinvälityspalvelin välittää viestin toiselle postinvälityspalvelimelle, kunnes sähköpostiviesti päätyy viestin vastaanottajan palvelimeen, josta hän lukee sen sähköpostiasiakkaallaan. Viesti kulkee minimissään yhden postinvälityspalvelimen kautta, mutta viesti voi kulkea useankin palvelimen kautta. Jokainen postinvälityspalvelin, jonka kautta sähköpostiviestisti kulkee, lisää *ensimmäiseksi otsakekentäksi* Received-rivin.

Usean palvelimen läpi kulkeneen viestin alussa on siis joukko Received-otsakekenttiä, joista ensimmäinen on viestin vastaanottajan käyttämä postinvälityspalvelin. Viestin lähettäjä voidaan jäljittää aloittamalla *ylimmäisestä* otsakekentästä ja seuraamalla otsakekenttiä, kunnes vastaan tulee ei-luotettu postinvälityspalvelin.

Käytännössä sähköpostin lähettäminen onnistuu esimerkiksi seuraavasti. Alla palvelinkoneen james.hut.fi (IP-osoite 130.233.173.1) käyttäjä on ottanut telnet-yhteyden TKK:n postipalvelimen smtp.hut.fi SMTP-porttiin (portti numero 25), joka tässä on postia välittävä kone:

```
james ~ % telnet smtp.hut.fi 25
Trying 130.233.228.93...
Connected to smtp.hut.fi.
Escape character is '^]'.
220 smtp-3.hut.fi ESMTP Sendmail; Mon, 26 Jul 2004 15:06:36 +0300
HELO whitehouse.gov
250 smtp-3.hut.fi Hello james.hut.fi [130.233.173.1], pleased to meet you
MAIL FROM:<luser2@domain.example>
250 2.1.0 <luser2@domain.example>... Sender ok
RCPT TO:<luser@kaip.iki.fi>
250 2.1.5 <luser@kaip.iki.fi>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Received: from whitehouse.gov (whitehouse.gov [63.161.169.137]) by
        mail.cia.gov 8.12.11/8.12.11) with ESMTP id i6QBVHuG025936
        for <luser@kaip.iki.fi>; Mon, 26 Jul 2004 14:31:17 +0300 (EEST)
Subject: Hi Kai!
Date: Mon, 26 Jul 2004 12:13:58 -0200
Message-ID: <77212391116.98504@whitehouse.gov>
From: George W. Bush <president@whitehouse.gov>
To: luser@kaip.iki.fi

Hi Kai,
```

```
How are you?

Yours truly,
W
.
250 2.0.0 i6QC6aFH018728 Message accepted for delivery
QUIT
221 2.0.0 smtp-3.hut.fi closing connection
Connection closed by foreign host.
```

Yllä lähettäjäksi on annettu `luser2@domain.example` ja vastaanottajaksi `luser@kaip.iki.fi`:

```
MAIL FROM:<luser2@domain.example>
250 2.1.0 <luser2@domain.example>... Sender ok
RCPT TO:<luser@kaip.iki.fi>
250 2.1.5 <luser@kaip.iki.fi>... Recipient ok
```

Mahdolliset virheilmoitukset päätyvisivät keksittyyn osoitteeseen `luser2@domain.example`. Lisäksi lähettäjä on antanut viestiin tekaistuja otsakekenttiä (mm. Received-rivi ja lähettäjän osoite From-rivillä):

```
DATA
354 Enter mail, end with "." on a line by itself
Received: from whitehouse.gov (whitehouse.gov [63.161.169.137]) by
        mail.cia.gov 8.12.11/8.12.11) with ESMTP id i6QBVHuG025936
        for <luser@kaip.iki.fi>; Mon, 26 Jul 2004 14:31:17 +0300 (EEST)
Subject: Hi Kai!
Date: Mon, 26 Jul 2004 12:13:58 -0200
Message-ID: <77212391116.98504@whitehouse.gov>
From: George W. Bush <president@whitehouse.gov>
To: luser@kaip.iki.fi
```

Seuraavassa kerrotaan, miltä viesti näyttää vastaanottajalle ja miten viestin lähettäjän IP-osoite 130.233.173.1 voidaan selvittää.

Alla on viesti, joka tuli `luser@kaip.iki.fi`:n postilaatikkoon, kuten tyypillinen postiohjelma sen näyttäisi:

```
Subject: Hi Kai!
Date: Mon, 26 Jul 2004 12:13:58 -0200
From: George W. Bush <president@whitehouse.gov>
To: luser@kaip.iki.fi

Hi Kai,

How are you?

Yours truly,
W
```

Äkkiä katsottuna näyttää siltä, kuin USA:n presidentti olisi lähettänyt terveiset `luser@kaip.iki.fi`:lle. Oikeasti kyse on tietysti aiempana kuvatusta viestistä, jonka headerit jonka headerit on väärennetty näyttämään siltä, kuin viesti olisi George W. Bushin lähettämä.

Kun myös täydelliset headerit näytetään, näyttää sama viesti seuraavalta (viestiin on lisätty rivinumerot pedagogisista syistä):

```
 1. From luser2@domain.example  Mon Jul 26 15:11:03 2004
 2. Return-Path: <luser2@domain.example>
 3. Received: from smtp-3.hut.fi (smtp-3.hut.fi [130.233.228.93])
 4.         by kaip.iki.fi (8.12.11/8.12.11) with ESMTP id i6QCB2N0005011
 5.         for <luser@kaip.iki.fi>; Mon, 26 Jul 2004 15:11:02 +0300 (EEST)
 6. Received: from whitehouse.gov (james.hut.fi [130.233.173.1])
 7.         by smtp-3.hut.fi (8.12.10/8.12.10) with SMTP id i6QC6aFH018728
 8.         for <luser@kaip.iki.fi>; Mon, 26 Jul 2004 15:07:19 +0300
 9. Received: from whitehouse.gov (whitehouse.gov [63.161.169.137]) by
10.         mail.cia.gov 8.12.11/8.12.11) with ESMTP id i6QBVHuG025936
11.         for <luser@kaip.iki.fi>; Mon, 26 Jul 2004 14:31:17 +0300 (EEST)
12. Subject: Hi Kai!
13. Date: Mon, 26 Jul 2004 12:13:58 -0200
14. Message-ID: <77212391116.98504@whitehouse.gov>
15. From: George W. Bush <president@whitehouse.gov>
16. To: luser@kaip.iki.fi
17.
18. Hi Kai,
19.
20. How are you?
21.
22. Yours truly,
23. W
```

Viestin headerit näkyvät riveillä 1-16 ja viestin runko riveillä 18-23. Rivillä 1 on postilaatikkoformaattiin liittyvä From -kenttä ja rivillä 2 näkyy postinvälitysohjelmani näyttämä osoite (`luser2@domain.example`), johon viestistä aiheutuvat virheilmoitukset päätyvät.

Viestin lähettäjä voi siis varsin vapaasti valita osoitteen, johon virheilmoitukset päätyvät. Tästä syystä on yleistä, että perille toimittamattomasta spämmistä aiheutuvia virheilmoituksia satelee syyttömien postilaatikkoihin.

Riveillä 3-5 on vastaanottajan postinvälitysohjelman lisäämä Received-rivi ja riveillä 6-8 on viestin lähettämiseen käytetyn TKK:n palvelimen lisäämä Received-rivi. Riveillä 9-12 on itse viestiä lähettäessäni lisäämiä rivejä, niiden sisältö (mukaanlukien viestin lähettäjä) voisi siis periaatteessa olla mitä tahansa.

Katsotaan Received-rivejä tarkemmin:

```
3. Received: from smtp-3.hut.fi (smtp-3.hut.fi [130.233.228.93])
4.         by kaip.iki.fi (8.12.11/8.12.11) with ESMTP id i6QCB2N0005011
5.         for <luser@kaip.iki.fi>; Mon, 26 Jul 2004 15:11:02 +0300 (EEST)
```

Vastaanottajan postipalvelimen (kaip.iki.fi) lisäämä Received-rivi kertoo, että se vastaanotti viestin IP-osoitteesta 130.233.228.93, joka on TKK:n postipalvelin (smtp-3.hut.fi). IP-osoitteeseen liittyvän nimen voi selvittää alussa mainituilla webbipalveluilla tai host-komennolla esimerkiksi seuraavasti:

```
kaip@kaip ~ % host 130.233.228.93
93.228.233.130.in-addr.arpa domain name pointer smtp-3.hut.fi.
```

Seuraava Received-rivi:

```
6. Received: from whitehouse.gov (james.hut.fi [130.233.173.1])
7.         by smtp-3.hut.fi (8.12.10/8.12.10) with SMTP id i6QC6aFH018728
8.         for <luser@kaip.iki.fi>; Mon, 26 Jul 2004 15:07:19 +0300
```

smtp-3.hut.fi:n lisäämän Received-rivin mukaan palvelin sai viestin IP-osoitteesta 130.233.173.1, joka kuuluu palvelimelle james.hut.fi. Postin lähettäjä kuitenkin valehteli olevansa “whitehouse.gov”

(HELO-nimi). Yllä olevalla Received-rivillä voi siis luottaa IP-osoitteeseen 130.233.173.1, mutta ei HELO-nimeen (whitehouse.gov).

Seuraava Received-rivi (rivit 9-11) ja sen jälkeiset otsikkorivit (rivit 12-16) ovatkin jo kokonaan hatusta vedettyjä:

```
 9. Received: from whitehouse.gov (whitehouse.gov [63.161.169.137]) by
10.         mail.cia.gov 8.12.11/8.12.11) with ESMTP id i6QBVHuG025936
11.         for <luser@kaip.iki.fi>; Mon, 26 Jul 2004 14:31:17 +0300 (EEST)
12. Subject: Hi Kai!
13. Date: Mon, 26 Jul 2004 12:13:58 -0200
14. Message-ID: <77212391116.98504@whitehouse.gov>
15. From: George W. Bush <president@whitehouse.gov>
16. To: luser@kaip.iki.fi
```

Viesti ei oikeasti kulkenut CIA:n palvelimen (mail.cia.gov) kautta eikä se ole peräisin valkoisen talon palvelimelta (whitehouse.gov).

Received-rivejä siis seurataan ylhäältä alas kunnes vastaan tulee ei-luotetun palvelimen lisäämä Received-rivi. Esimerkkitapauksessa headereista voidaan päätellä (jos luotamme TKK:n postipalvelimeen smtp-3.hut.fi), että viesti on peräisin palvelimelta james.hut.fi, jonka IP-osoite on 130.233.173.1.

Viestin rungon tulkinta

Usein viestin runko kertoo eniten spämmeristä. Spämmiviestissä voi esimerkiksi olla webbilinkkejä.

Valitusosoitteen löytäminen

IP-osoitteeseen liittyvän valitusosoitteen voi löytää esimerkiksi edellä mainittujen webbipalvelujen avulla tai komentoriviltä käyttäen Geektoolsin Whois-palvelua. Esimerkiksi helmikuussa 2004 tulleessa spämmissä olevan IP-osoitteen 69.160.182.25 palveluntarjoajan selvittäminen whois-komennolla:

```
kaip@kaip ~ % whois -h whois.geektools.com 69.160.182.25
GeekTools Whois Proxy v5.0.4 Ready.
Checking access for 217.30.177.41... ok.
Final results obtained from whois.arin.net.
Results:
Adelphia Cable Communications ADELPHIA-CABLE-7 (NET-69-160-0-0-1)
                                  69.160.0.0 - 69.175.255.255
Adelphia 69-160-160-0-Z3 (NET-69-160-160-0-1)
                                  69.160.160.0 - 69.160.191.255

# ARIN WHOIS database, last updated 2004-07-25 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Kyseessä on Adelphia Cable Communicationsin verkossa oleva osoite. Adelphiasta löytyy enemmän tietoa yllä näkyvästä Arinin whois-tietokannasta:

```
kaip@kaip ~ % whois -h whois.arin.net ADELPHIA-CABLE-7

OrgName:    Adelphia Cable Communications
OrgID:      ADEL
Address:    1 North Main Street
City:       Coudersport
StateProv:  PA
PostalCode: 16915
Country:    US
```

```
NetRange:   69.160.0.0 - 69.175.255.255
CIDR:       69.160.0.0/12
NetName:    ADELPHIA-CABLE-7
NetHandle:  NET-69-160-0-0-1
Parent:     NET-69-0-0-0-0
NetType:    Direct Allocation
NameServer: NS1.ADELPHIA.NET
NameServer: NS2.ADELPHIA.NET
Comment:
RegDate:    2003-08-28
Updated:    2004-04-26

OrgAbuseHandle: IPE-ARIN
OrgAbuseName:   Internet Policy Enforcement
OrgAbusePhone:  +1-866-473-2909
OrgAbuseEmail:  abuse@adelphia.net

OrgTechHandle: CKI8-ARIN
OrgTechName:   Kio, Carolyn
OrgTechPhone:  +1-888-512-5111
OrgTechEmail:  arin@adelphiacom.net

# ARIN WHOIS database, last updated 2004-07-25 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Yllä näkyykin osoite, johon valitukset voi lähettää (`abuse@adelphia.net`):

```
OrgAbuseHandle: IPE-ARIN
OrgAbuseName:   Internet Policy Enforcement
OrgAbusePhone:  +1-866-473-2909
OrgAbuseEmail:  abuse@adelphia.net
```

Spämmivalitusosoitteita (jos domain-nimi on tiedossa) voi etsiä Abuse.netin tietokannasta. Yleisesti ottaen spämmivalitukset voi lähettää osoitteeseen `abuse@palveluntarjoajan.domain.example` (jokaisella palveluntarjoajalla pitää olla toimiva abuse-osoite).

Saman olisi voinut selvittää myös traceroute-komennolla:

```
kaip@kaip ~ % traceroute 69.160.182.25
traceroute to 69.160.182.25 (69.160.182.25), 64 hops max, 40 byte packets
 1  stargate.local (192.168.0.1)  0.695 ms  0.790 ms  0.743 ms
 2  r2-atm1.hki.nbl.fi (217.30.176.254)  13.668 ms  13.202 ms  13.751 ms
 3  r1-ge1.hki.nbl.fi (217.30.183.140)  13.299 ms  13.237 ms  22.32 ms
 4  r4-ge1.hki.nbl.fi (80.81.160.233)  14.625 ms  14.143 ms  72.884 ms
 5  ge-0-0-0.no-oslms001-pe-
1.tu.telenor.net (212.105.101.98)  32.487 ms  32.570 ms  31.953 ms
 6  nb01b12-ge3-
1.nb.telenor.net (217.70.229.33)  33.688 ms  32.398 ms  33.478 ms
 7  nb03b11-ge2-
0.nb.telenor.net (217.70.227.18)  124.774 ms  124.79 ms  123.762 ms
 8  nb10b11-pos4-
3.nb.telenor.net (217.70.227.102)  123.187 ms  124.848 ms  139.470 ms
 9  pos2-
0.ar.paixnycny.aleron.net (205.198.19.121)  121.268 ms  120.974 ms  121.405 ms
```

```
10  pos2-
0.cr.paixnycny.aleron.net (205.198.18.66)  120.849 ms  120.525 ms  120.749 ms
11  205.198.18.38 (205.198.18.38)  120.338 ms  120.512 ms  120.772 ms
12  paix-
nyc.adelphiacom.net (198.32.118.15)  122.144 ms  121.138 ms  120.570 ms
13  g1-01-00-
00.r0.nyc90.adelphiacom.net (66.109.1.13)  120.888 ms  120.792 ms  120.696 ms
14  p3-00-00-
00.a0.alb75.adelphiacom.net (66.109.1.22)  129.470 ms  130.152 ms  129.623 ms
15  g1-00-00-00.ber01.albyny.adelphia.net (66.109.14.130)  129.477 ms g1-
01-00-00.ber01.albyny.adelphia.net (66.109.14.134)  128.456 ms g1-00-00-
00.ber01.albyny.adelphia.net (66.109.14.130)  129.82 ms
16  24.48.204.214 (24.48.204.214)  132.390 ms  132.804 ms  132.946 ms
17  10.177.192.1 (10.177.192.1)  134.317 ms  133.961 ms  134.218 ms
18  * * *
19  * * *
```

Traceroute näyttää reitin, jota paketit menevät kohteeseen 69.160.182.25. Paketit voivat kulkea usean palveluntarjoajan reitittimen kautta. Viimeisinä olevat reitittimet kuuluvat spämmerin Internet-palveluntarjoajalle, adelphia.netille. Traceroutea voi käyttää myös webin kautta DNS Stuff -sivuilta ("Tracert").

IP-osoite 69.160.182.25 on tätä kirjoitettaessa (26.7.2004) myös useassa spämmilähteitten IP-osoitteita sisältävässä tietokannassa, kuten esimerkiksi DNS Stuffin hausta ("Spam database lookup") selviää. Samaten Openrbl-haulla näkee, että IP-osoite on useilla estolistoilla.
