Gmail vas motri! Ili možda ipak ne?

Svjedočili smo nedavno medijskoj buri u čaši vode kada je jedan medij iznio, a mnogi prenijeli, informaciju kako Gmail ima mogućnost znati kada ste i na kojem mjestu pročitali upućenu vam e-mail poruku!

Pošiljatelj poruke tako može znati ne samo kad ste primljenu poruku otvorili, već i gdje ste se za to vrijeme nalazili! Gmail je tako postao više od elektroničke pošte – postao je sredstvo nadzora vašem bračnom partneru, vašem šefu, faktički bilo kome tko želi znati gdje se nalazite.

Stvari ipak nisu baš takve kakvima su ih mediji prikazali. Iako je točno da postoji mogućnost da pošiljalac poruke sazna kad ste pročitali poruku, pa čak i gdje ste se pritom nalazili, ta mogućnost nema izravne veze sa Gmail servisom.

Riječ je, naime, o plug-inu za Google Chrome browser nazvanom Streak [1] koji, u kombinaciji sa on-line servisom https://www.streak.com [2] za praćenje rada s klijentima (CRM – Customer Relationship Manager) zaista omogućuje gore navedene "špijunske aktivnosti" – ali to uistinu nema veze sa Googleovim servisom, a osim toga postoje i načini za onemogućivanje rada tog "dodatka".

O čemu se uopće radi? Zapravo, ni o kakvoj velikoj novosti, već o triku kojeg spammeri koriste već više godina: ubacivanju tracking informacije u tijelo poruke, u nadi da primatelj poruke ima uključenu opciju prikaza HTML podataka – a to, nažalost ili na sreću, danas ima gotovo svatko.

Spammeri bi tako u tijelo poruke ubacili link na sličicu veličine 0x0 na nekom poslužitelju koji je pod njihovom kontrolom. Primatelj poruke otvorio bi poruku i pročitao je, posve nesvjestan da je upravo, ako ima uključenu opciju prikaza HTML sadržaja, kontaktirao poslužitelj u vlasništvu spammera i zatražio tu malu nevidljivu sličicu.

Time je spammeru dao vrlo vrijednu informaciju: da je to e-mail adresa koju netko čita. Pregledom logova web servera spammeri mogu provjeriti kojim sve sličicama (a svaka je vezana uz jednu e-mail adresu) je pristupano i tako pročistiti svoje baze e-mail adresa od onih lažnih i neaktivnih – pročišćene baze podataka na tržištu postižu veću cijenu.

U ovom slučaju poanta nije u nevidljivoj sličici, već o unošenju specifične informacije, tzv. tracking-ID-a. Pogledajmo to primjerom: pretpostavimo da je Ante poslao Barbari e-mail poruku, a na svojem browseru ima instaliran famozni Streak plug-in. Tekst poruke je "Dobar dan, Barbara!", a Barbara će ga u svom gmail prozorčiću vidjeti kao najnormalniju, najneviniju pozdravnu porukicu.

U stvarnosti, Barbarin e-mail će izgledati ovako:

```
From: Ante <ante@gmail.com>
To: Barbara <Barbara@nekiserver.hr>
Content-Type: multipart/alternative; boundary=089e01184528a6b8a604f2dd5fb0
X-Spam-Status: No, score=0.2
X-Spam-Score: 2
X-Spam-Bar: /
X-Spam-Flag: NO

--089e01184528a6b8a604f2dd5fb0
Content-Type: text/plain; charset=UTF-8
```

```
Content-Transfer-Encoding: quoted-printable

Dobar dan, Barbara!
=E1=90=A7

--089e01184528a6b8a604f2dd5fb0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

<div dir=3D"ltr">Dobar dan, Barbara!<div hspace=3D"streak-pt-mark" style=3D=
"max-height:1px"><img style=3D"width:0px; max-height:0px;" src=3D"https://m=
ailfoogae.appspot.com/t?sender=3Dante%40gmail.com&amp;type=3D=
zerocontent&amp;guid=3D352dba38-55b6-4398-9e50-5cd788797998"><font color=3D=
"#ffffff" size=3D"1">=E1=90=A7</font></div>
</div>
--089e01184528a6b8a604f2dd5fb0--
```

I eto trika! Plug-in u poruku ubacuje jedan koji kontaktira (uočite onaj famozni "img") mailfoogae.appspot.com i u zahtjev ubacuje e-mail adresu pošiljatelja i jedinstveni ID kod u obliku slučajnog niza brojeva – heksadecimalnih, naravno. Kad Barbara otvori poruku njen će program interpretirati taj HTML kod i poslati na udaljeni poslužitelj informaciju o pošiljatelju i jedinstveni ID kod; aplikacija sa druge strane zatim će pošiljatelja obavjestiti o tome da je poruka pročitana (ako je poruka poslana na više primatelja, aplikacija – barem ova besplatna – ne može reći tko je točno od primatelja pročitao poruku), te sa kojeg uređaja i sa koje lokacije. Ovaj se kod integrira u postojeći HTML sadržaj i za krajnjeg je korisnika nevidljiv.

Kako, k vragu, mogu znati sa kojeg uređaja i odakle? Vjerujem da je čitateljima koji prate sistemac.carnet.hr radi posla ili iz čistog gušta nepotrebno posebno pojašnjavati otkud dolaze ti čudesni podaci: poslao ih je web browser koji se rado identificira kad uspostavlja HTTP vezu prema poslužitelju, a što se lokacije tiče – i nju je poslao browser jer mnogi ljudi daju browseru dozvolu da šalje podatke o trenutnoj lokaciji, što je vrlo praktična stvarčica na mobilnim telefonima i tabletima.

I to je to – mnogo bure u čaši vode, oko servisa koji je niti prvi niti zadnji servis koji bi rado znao gdje ste i što ste. I nikakve veze nema ni sa Google-om, ni sa Gmailom, niti sa svjetskim zavjerama.

Naravno, ostaje vrlo ozbiljno pitanje – treba li dozvoliti nekom servisu koji se ne zove NSA da tako lako prikuplja podatke o našim elektroničko-poštansko-čitalačkim navikama i o tome gdje se nalazimo, pa te informacije prosljeđuje našim najmilijima, ili ljudima kojima smo rekli da smo na jednom kraju grada a zapravo smo na drugom, te najzad posve nepoznatim osobama koje samo trebaju znati našu e-mail adresu da bi mogli saznati i gdje se nalazimo u nekom trenutku?

Ako ne pristajete na takve igre, možete iskoristiti tri načina borbe protiv neželjenih cyber-špijuna.

Prvi način je danas pomalo nekonvencionalan i nezgodan: jednostavno u svom programu za čitanje elektroničke pošte isključite prikazivanje HTML koda. To je malo nezgodno učiniti na webmail sučeljima kakva koriste Gmail, Outlook.com, Yahoo Mail i bratija, ali njima možete pristupati iz "običnog" programa za čitanje elektroničke pošte jer podržavaju POP ili IMAP protokol (koristite kriptiranu verziju!), a takvih programa imate i na pametnofonima i na tabletima.

Ako aplikacija ne prikazuje (tj. ne "izvršava") HTML kod skriven u e-mail poruci, tada famozni trik sa praznom sličicom nikad neće biti izvršen i primatelj nikad neće saznati jeste li ili niste pročitali njegovu poruku. Velika prednost ovog asketskog pristupa problemu je što će automatski onemogućiti špijuniranje te vrste bilo kojem drugom servisu koji koristi takve prljave trikove.

Ako ipak volite gledati šarene HTML formatizirane elektroničke poruke ili se jednostavno ne želite odreći web sučelja omiljenog e-mail servisa, i za to postoji rješenje: Disconnect(https://chrome.google.com/webstore/detail/disconnect/jeoacafpbcihiomhlakheieifhpjdfeo?hl=en) ekstenzija za Google Chrome koja će blokirati slične pokušaje na velikom broju sličnih mjesta koja vas na ovaj ili onaj način špijuniraju; prednost ove ekstenzije je što možete izabrati što ćete dozvoliti a što nećete, ali s

druge strane nema garantirane zaštite od svih poznatih, a posebice od manje poznatih špijunskih adresa.

Najzad, želite li vježbati vaše H4X0Rske skillzove, pomoću ovih par koraka možete i sami zauzdati nedolične digitalne paparazze:

1. Pošaljite sami sebi jedan e-mail sa uključenim trackingom (ovog ili onog davatelja špijunskih usluga), ili zamolite prijatelja koji koristi takav servis da vam pošalje poruku;

2. Otvorite e-mail poruku kao tekstualnu poruku (Ctrl-U na Thunderbirdu) ili poruku snimite kao tekstualnu datoteku;

3. Otvorite datoteku ili u pop-up prozoru pregledajte e-mail poruku i pronađite uobičajene sumnjivce: link na sliku na udaljenom poslužitelju, nešto što sliči na ID, bilo kakvu komunikaciju sa udaljenim poslužiteljem koja ne pripada sadržaju poruke, te zapišite, kopirajte ili zapamtite adresu udaljenog poslužitelja;

4. U resolver po želji (/etc/hosts ili gdje vam se već sviđa, samo imajte na umu resolving order) upišite adresu udaljenog poslužitelja i dajte mu IP 127.0.0.1;

5. Ako su špijuni lukavi pa umjesto FQDN adrese koriste IP adresu, lijepo vi nju krknite na blacklist vašeg firewalla (ovo je, primjerice, dobar razlog zašto imati rootane tablete i pametnofone);

6. Proceduru ponavljajte za svakog novog gnjaveža koji se pojavi.

pet, 2014-02-21 06:26 - Radoslav Dejanović**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1355

Links
[1] https://chrome.google.com/webstore/detail/streak-for-gmail/pnnfemgpilpdaojpnkjdgfgbnnjojfik?hl=en
[2] https://www.streak.com/