

H-online: Skype nadzire korisnike



Suvremene komunikacijske tehnologije omogućuju dosad neviđen nadzor nad ljudima. Većina smatra da njih ne nadziru, jer nisu nikome zanimljivi. Uostalom, kako nadzirati toliki promet? Upozoravanje na opasnost od zadiranja u privatnost uglavnom ostaje u domeni fanatika privatnosti, pogotovo u nedostatku konkretnih dokaza zloupotreba. No nedavno su ipak prikupljeni dokazi da se nešto zanimljivo događa korisnicima Skypea.

H-online je objavio rezultate svog istraživanja koje je potaknuto pritužbama njihovih čitatelja da Microsoft nadzire promet preko Skypea. Osmisli su test i postavili zamku. Komunicirajući pomoću Skypea, točnije njegova IM servisa, utipkali su par URL adresa. Nakon nekog vremena iz Microsoftove mreže uslijedilo je spajanje na te adrese. Evo dokaza:

```
65.52.100.214 - - [30/Apr/2013:19:28:32 +0200] "HEAD /.../login.html?user=tbtest&password=geheim HTTP/1.1"
```

Sljeva je adresa s koje je uspostavljena veza, a koja pripada Microsoftu. Ostatak zapisa pokazuje da je Skype server presreo, osim adrese, još i korisničko ime i zaporku kojom se treba ulogirati. Drugi link vodio je na posebno oblikovanu adresu kojom se omogućuje razmjena datoteka spremljenih u oblaku.

Zanimljivo je da se spajanje dogodilo samo na stranice koje imaju kriptirane sadržaje, gdje adresa počinje s <https://>, te da se nisu ustručavali iskoristiti tuđe korisničko ime i zaporku. Pitamo se, da je netko tako s tuđim identitetom upao u Microsoftov web prostor, da li bi se to smatralo kriminalom?

Microsoft je na izazov odgovorio standardnim PR pripćenjem: "Skype može koristiti automatsko skeniranje IM i SMS prometa, da bi identificirao spam i web stranice koje su već prethodno označene kao linkovi na spam, prijevare i *phishing*." Dakle sve se to obavlja radi zaštite korisnika, a korisnici su pristali na to čim su prihvatili uslugu. H-online ne vjeruje u vjerodostojnost te izjave. Iz Microsofta su pristupili samo zaglavlju web stranice, dok bi za provjeru spama trebalo pregledati cijeli sadržaj. H-online zaključuje da su korisnici Skypea pristali na to da Microsoft može nadzirati njihov promet i koristiti njihove podatke kako želi, te da neće objaviti što sve s njima radi.

Electronic Frontier Foundation i *Reporters without Borders* prilikom preuzimanja Skypea izrazili su zabrinutost da će se ubuduće Skype morati pokoriti legislativi SAD koja vladinim obavljajstajnim agencijama dozvoljava nadzor prometa. Prilikom nedavnog gostovanja u Varaždinu, na konferenciji [FSEC](#) [1], Bruce Scheier je upozorio da su samo građani SAD-a zaštićeni od takvog nadzora, dok ostatak svijeta ima razloga za zabrinutost.

Spomenimo nastup još jednog aktivista koji se zalaže za individualne slobode. Richard Stallman je na svom predavanju u Zagrebu otvoreno izjavio da su Microsoft Windowsi najveći *spyware* koji postoji. Windowsi šalju kriptirane pakete u centralu, a EULA koju su svi korisnici prihvatili kad su instalirali SP2 za XP daje Microsoftu pravo da prikuplja informacije o softveru i hardveru s korisničkih računala.

Dakle, ako ste zabrinuti za svoju privatnost, nećete korist Skype, bez obzira na to imate li što kriti ili ne. Zapravo su problematični svi servisi koji su centralizirani. Veću zaštitu korisnicima pružaju *perr-to-peer* servisi, gdje server služi samo da poveže dva klijenta, a dalje oni komuniciraju izravno, po potrebi koristeći enkripciju.

Korisnike treba i dalje upozoravati na potrebu zaštite privatnosti. Nije pri tom uopće važno da li nas

netko stvarno nadzire, brinuti nas treba već sama mogućnost da to mogu, ako žele. Informacije predstavljaju moć, pa ne bi trebalo olako prepustiti moć nad nama nekome u koga nemamo stopostotno povjerenje.

Radoznali mogu pročitati originalni [članak](#) [2] u H-online, te izjave nezavisnih stručnjaka koji su [potvrdili](#) [3] otkrivene činjenice.

ned, 2013-05-26 19:39 - Aco Dmitrović **Vijesti:** [Sigurnost](#) [4]

Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: <https://sysportal.carnet.hr/node/1271>

Links

[1] <https://sysportal.carnet.hr/node/1101>

[2] <http://tinyurl.com/d7h74fw>

[3] <http://tinyurl.com/ngl97e6>

[4] <https://sysportal.carnet.hr/taxonomy/term/13>