Google prisluškivač

Nedavno objavljen sigurnosni problem Google Chrome preglednika podigao je buru u čaši vode: prema navodima autora [1] koji je objavio problem, Google Chrome odnedavno ima ugrađenu mogućnost komunikacije s korisnikom pomoću mikrofona, odnosno moguće je tražilici zadavati naloge izgovaranjem traženog izraza umjesto utipkavanjem.

To samo po sebi ne bi bio poseban problem, ali autor demonstrira kako malizicozne web stranice mogu neopreznog korisnika prisluškivati jednostavnim otvaranjem prozora u pozadini.

Google nije reagirao na prijavljeni problem opravdavajući se argumentacijom kako u postavkama Chrome browsera postoji sekcija u kojoj je moguće dozvoliti ili zabraniti nekoj lokaciji korištenje mikrofona, te da je svaki tab koji pristupa mikrofonu jasno označen crvenim krugom, standardnom ikonom koja označava snimanje zvuka i/ili slike.

Tri su problema u ovakvom rezoniranju: ponajprije, možemo očekivati kako će sve više i više web stranica koristiti mogućnost glasovne komunikacije, zbog čega će ručno kontroliranje prava pristupa nakon nekog vremena postati vrlo zahtjevan posao.

Zatim, od korisnika možemo očekivati samo da se ponašaju poput korisnika: uglavnom nesvjesni potencijalnih rizika, korisnici će odobravati pristup audiovizualnim ulazima na svakoj stranici koja to od njih zatraži. Prebacivanje krivnje za potencijalnu ugrozu privatnosti na krajnjeg korisnika zaista je najlakše učiniti, ali to je istovremeno i najgore moguće rješenje.

Najzad, pogrešno je pretpostaviti da će *malware* igrati "po pravilima": upravo suprotno, autori malicioznih skripti i web stranica iskoristit će sve mogućnosti da korisnika zavaraju – od jednostavnog otvaranja prozora u pozadini (što mnogi korisnici jednostavno ne primjete), pa do sofisticiranog socijalnog *hackinga* čiji je cilj nagovoriti korisnika da malicioznom URL-u dozvoli pristup kameri i mikrofonu.

Idealno rješenje ovog potencijalnog problema privatnosti bio bi jasno označen prekidač na izborniku browsera kojim bi se uključivao i isključivao pristup mikrofonu i kameri za sve sadržaje Chrome preglednika, a za one paranoičnije i pravi hardverski *on/off switch* na računalu.

U nedostatku takvog rješenja, moguće je prava kontrolirati na dva načina:

Selektivnom kontrolom koji URL smije pristupiti uređajima

1. u traku Chrome browsera upišite

```
chrome://settings/contentExceptions#media-stream
```

2. U prozoru koji se pojavi vidjet ćete sve URL-ove koji imaju pravo pristupa kameri i mikrofonu, a one koje ne želite jednostavno obrišite;

3. Periodički provjeravajte ove postavke.

Neselektivnom zabranom korištenja kamere i mikrofona svim aplikacijama

1. u traku Chrome browsera upišite

`chrome://settings/content`

2. Pronađite (Ctrl-F) postavku "microphone" i potvrdite opciju "Do not allow sites to access my camera and microphone"

3. Gumb "Manage exceptions...." omogućuje vam da, unatoč globalnoj zabrani pristupa audiovizualnim uređajima, odredite iznimke.

Iako se ovo čini kao problem (edukacije) krajnjeg korisnika, ovaj potencijalni problem privatnosti jednako je neugodan i za organizacije: primjerice, ciljanim napadom napadač može prisluškivati djelatnike i njihove telefonske razgovore.

U tom smislu ovaj propust postaje problem sigurnosti cijelog IT sustava i kao takav treba biti riješen na organizacijskoj razini: korisnici usluge *Google Chrome for Business and Education* mogu taj problem riješiti centralno, kroz *Google Admin* konzolu, gdje je moguće postaviti zabrane u *group policy;* također, *policy* je moguće kontrolirati kroz sučelje *MS Windows Servera 2003* (ili novijeg). U najgorem slučaju bit će potrebno ručno promjeniti postavke na svim korisničkim računalima.

ned, 2014-01-26 06:49 - Radoslav Dejanović**Vijesti:** Sigurnost [2]
Kategorije: Preglednici [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1344

Links
[1] http://talater.com/chrome-is-listening/
[2] https://sysportal.carnet.hr./taxonomy/term/13
[3] https://sysportal.carnet.hr./taxonomy/term/27