Kako isključiti ugrađenu web kameru?

CCERT i MUP upozoravaju građane na ucjenjivačke mailove koji u zadnje vrijeme stižu u sandučiće e-pošte. Napadači plaše primatelje tvrdnjom da im je korisnički račun provaljen, da su uhvaćeni u nečasnoj radnji, a javno poniženje će izbjeći ako uplate neku sumu.

I mene su, kao i druge sistemce, zvali korisnici i znanci, pitali što da rade? Savjetovao sam im neka najprije promijene password, za svaki slučaj. I inače je zdravo mijenjati ga povremeno. Nakon toga neka incident prijave davatelju usluga. Znanac je nazvao HT, prijavio ucjenu i zamolio da mu promijene zaporku. Dobio je odgovor da su dobili mnoštvo prijava, ali se ne treba uzrujavati, opasnost nije stvarna. Mailove šalje virus, a *password* ne treba mijenjati jer račun nije provaljen. Ako ispravno tumačimo, ispada da se "virus" na mail serveru dočepao mail adresa i slao korisnicima poruke. Znanac je dobio mail u kojem je on sam pošiljatelj i primatelj, što bi trebalo biti dokaz da mu je račun provaljen. Ali čemu savjet tehničke podrške da ne treba mijenjati zaporku? Je li to samo lijenost, ne da im se?

Mediji su popratili zbivanja, pa tako čitamo bombastične naslove: "Gledate li pornografiju? [1] Građani prijavili ucjenjivačke e-mailove." Jedan od načina ucjenjivanja jest prijetnja da je pomoću video kamere na računalu korisnik snimljen dok je gledao porniće, a napadač će objaviti snimku na društvene mreže ako mu se ne pošalje novac.

Većina korisnika uopće ne razmišlja o kameri na vrhu ekrana. Ona se aktivira pomoću aplikacije koju sami pokrenemo. Moguće je da kameru aktivira i malware kojeg smo ne znajući pokupili. Kako provjeriti je li kamera aktivna, kad nam se ništa ne pokazuje na ekranu?

Sistemac koji koristi Linux može to lako provjeriti. Pogledajmo koje su datoteke otvorene, možda neke od njih imaju veze s videom.

```
$ sudo lsof | grep video
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
nautilus  1883                hombre  mem       REG                8,2    545656    4
072114 /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0.803.0
gmain     1883 1932           hombre  mem       REG                8,2    545656    4
072114 /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0.803.0
gdbus     1883 1933           hombre  mem       REG                8,2    545656    4
072114 /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0.803.0
dconf\x20 1883 1969           hombre  mem       REG                8,2    545656    4
072114 /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0.803.0
```

Izlistane su samo biblioteke, srećom nema aplikacije koja te biblioteke koristi. Utješno, znači da nas nitko ne snima! :)

Upozorenje koje kaže da lsof ne može pristupiti gvfsd file sistemu je razumljivo jer tom tipu datotečnog sustava može pristupiti samo njegov vlasnik, a root to nije! Ako želite zaviriti i tamo,

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

izostavite *sudo* prije *lsof.*

```
$ lsof | grep video
nautilus  1883                hombre  mem       REG                8,2    545656    4
072114 /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0.803.0
gmain     1883 1932           hombre  mem       REG                8,2    545656    4
072114 /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0.803.0
gdbus     1883 1933           hombre  mem       REG                8,2    545656    4
072114 /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0.803.0
dconf\x20 1883 1969           hombre  mem       REG                8,2    545656    4
072114 /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0.803.0
unity-sco 4975                hombre  mem       REG                8,2      2430    5
118848 /usr/share/locale-langpack/hr/LC_MESSAGES/unity-lens-video.mo
dconf\x20 4975 4976           hombre  mem       REG                8,2      2430    5
118848 /usr/share/locale-langpack/hr/LC_MESSAGES/unity-lens-video.mo
gmain     4975 4977           hombre  mem       REG                8,2      2430    5
118848 /usr/share/locale-langpack/hr/LC_MESSAGES/unity-lens-video.mo
gdbus     4975 4978           hombre  mem       REG                8,2      2430    5
118848 /usr/share/locale-langpack/hr/LC_MESSAGES/unity-lens-video.mo
unity-sco 4986                hombre  mem       REG                8,2      2430    5
118848 /usr/share/locale-langpack/hr/LC_MESSAGES/unity-lens-video.mo
dconf\x20 4986 4991           hombre  mem       REG                8,2      2430    5
118848 /usr/share/locale-langpack/hr/LC_MESSAGES/unity-lens-video.mo
gmain     4986 4992           hombre  mem       REG                8,2      2430    5
118848 /usr/share/locale-langpack/hr/LC_MESSAGES/unity-lens-video.mo
gdbus     4986 4993           hombre  mem       REG                8,2      2430    5
118848 /usr/share/locale-langpack/hr/LC_MESSAGES/unity-lens-video.mo
```

Sad se pojavio unity-lens, što je opet sastavni dio OS-a, odnosno Unity desktopa. "Leće" nam ubrzavaju traženje sadržaja po vrsti datoteke (glazba, video, torrenti itd.) na računalu, ali i na webu, ukoliko uključimo takvu vrstu pretraživanja u postavkama. Dakle, opet ništa sumnjivao.

List open files će nam pomoći u traženju otvorenih datoteka, ali korisnik bi morao biti paranoičan i stalno provjeravati da li mu neka aplikacija koristi kameru. Možemo li problem riješiti "sistemski", tako da možemo opuštenije koristiti računalo?

Potražimo aktivne module kernela. Za to će nam poslužiti naredba *lsmod*.

```
$ sudo lsmod | grep video
uvcvideo               86016  0
videobuf2_vmalloc      16384  1 uvcvideo
videobuf2_memops       16384  1 videobuf2_vmalloc
videobuf2_v4l2         24576  1 uvcvideo
videobuf2_core         40960  2 uvcvideo,videobuf2_v4l2
videodev              180224  3 uvcvideo,videobuf2_core,videobuf2_v4l2
media                  40960  2 uvcvideo,videodev
video                  45056  1 i915
```

Modul ***video*** donosi podršku za Intelove grafičke čipove, dok moduli ***uvcvideo*** omogućavaju rad kamerama napravljenim po UVC standardu [2].

Ako ne želimo stalno provjeravati rad kamere, najbolje je maknuti *uvcvideo* module.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

```
$ sudo modprobe -r uvcvideo
```

Pogledajmo da li su svi uklonjeni

```
$ sudo lsmod | grep video
video                  45056  1 i915
```

Dobro je, ostao je aktivan samo modul koji podržava grafički čip. Radoznalosti radi, pokušavamo i njega "ugasiti".

```
$ sudo modprobe -r i915
modprobe: FATAL: Module i915 is in use.
```

Dobro da brzopleti prsti nisu uspjeli u nakani. i915 je driver za Intelov grafički čip. Maknuti i njega bilo bi riskantno, zar ne? Izgubili bismo sliku na ekranu..

Ali što će se dogoditi nakon restarta? Pogađate, svi će moduli opet biti aktivni. Pitanje je da li smo toliko paranoični da ih želimo zauvijek ukloniti? Mislim da bi to bilo pretjerano. Bit će dovoljno dodati redak u neku startup skriptu da se moduli za kameru deaktiviraju automatski. Za to može poslužiti .bashrc u home direktoriju, ili, još bolje, /etc/rc.local. Tu će trebati upisati cijelu putanju do naredbe:

```
# Isklju?i drivere za video kameru
/sbin/modprobe -r uvcvideo
```

Na taj način će se moduli pokrenuti, ali prije nego se korisnik ulogira bit će uklonjeni, pa ne moramo brinuti o kameri. Ako želimo sudjelovati u nekoj video komunikaciji, dovoljno ih je aktivirati.

```
$ sudo modprobe -a uvcvideo
```

I to je to! Digli smo letvicu potencijalnom napadaču, neće moći samo tako koristiti kameru na vrhu ekrana.

Istina, "zdravo seljačka" metoda bila bi jednostavno zalijepiti izolir traku preko kamere - viđali smo to kod korisnika koji su spretniji s rukama nego s glavom. Ali to smo odbacili, jer će nakon uklanjanja ostati ljepljiva prljavština preko leće.

sub, 2018-10-27 17:45 - Aco Dmitrović**Kuharice:** Linux [3]
Vote: 0

No votes yet

story_tag: Linux [4]
kamera [5]
uvcvideo [6]

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Source URL: https://sysportal.carnet.hr/node/1827?page=0

Links
[1] http://novilist.hr/Vijesti/Hrvatska/Gledate-li-pornografiju-Gradani-prijavili-ucjenjivacke-e-mailove.-Evo-sto-policija-preporucuje-za-zastitu?meta_refresh=true
[2] https://www.linuxtv.org/wiki/index.php/Uvcvideo
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/119
[5] https://sysportal.carnet.hr/taxonomy/term/280
[6] https://sysportal.carnet.hr/taxonomy/term/281

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr