

Bármely IP-cím fizikai helyének felfedése

PCLinuxOS Magazine – 2017. november

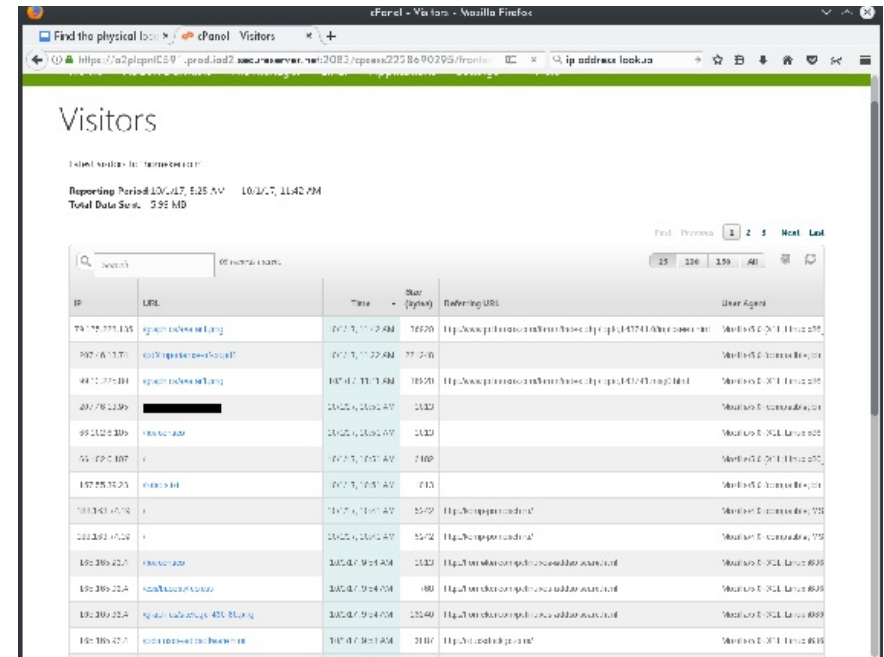
Írta: phorneker

Nemrégiben frissítettem a honlapomat, aminek a GoDaddy.com ad helyet. A GoDaddy néhány hasznos eszközt ad, a domén, a weblap, e-mail szerver és webalkalmazások karbantartására. (A weblapom IP-címe és a home könyvtára biztonsági okokból blokkolva van.)

Mivel csak egy domén van, a nagyítóra kattintottam, hogy belépjek a naplóba.

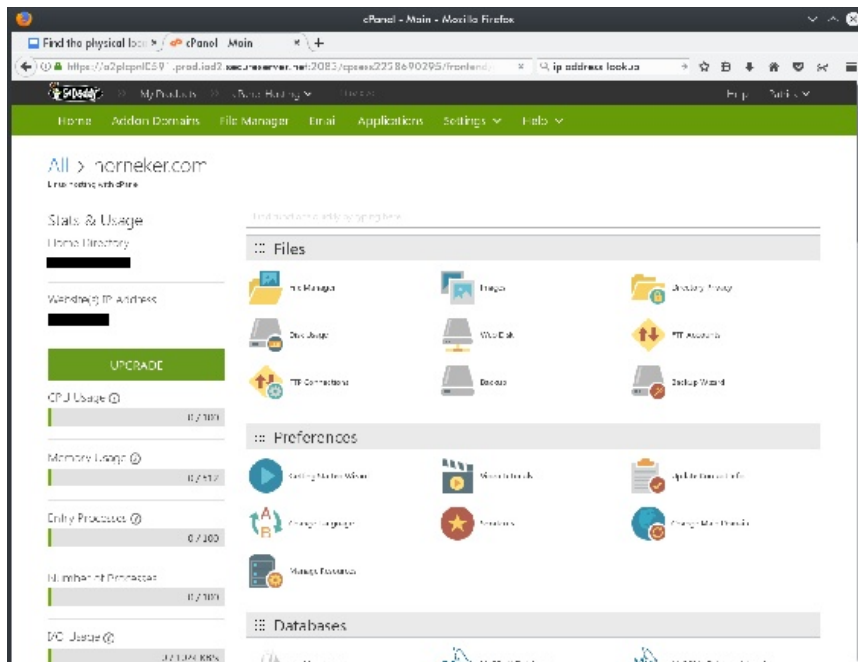


Most már benne vagyok a naplóban.

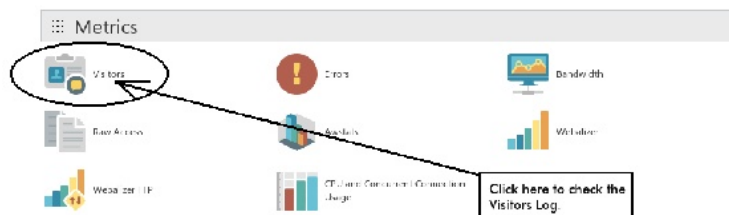


(A képernyőképből a nemkívánatos anyagot kiesztem.)

A látogatók naplóját végignézve találtam néhány furcsa URL-t közöttük. A GoDaddy-nek hála a látogatók IP-címét feljegyezte és a Google-keresőben találtam egy eszközt, amivel ezeknek az IP-címeknek a helyét meg lehet határozni.

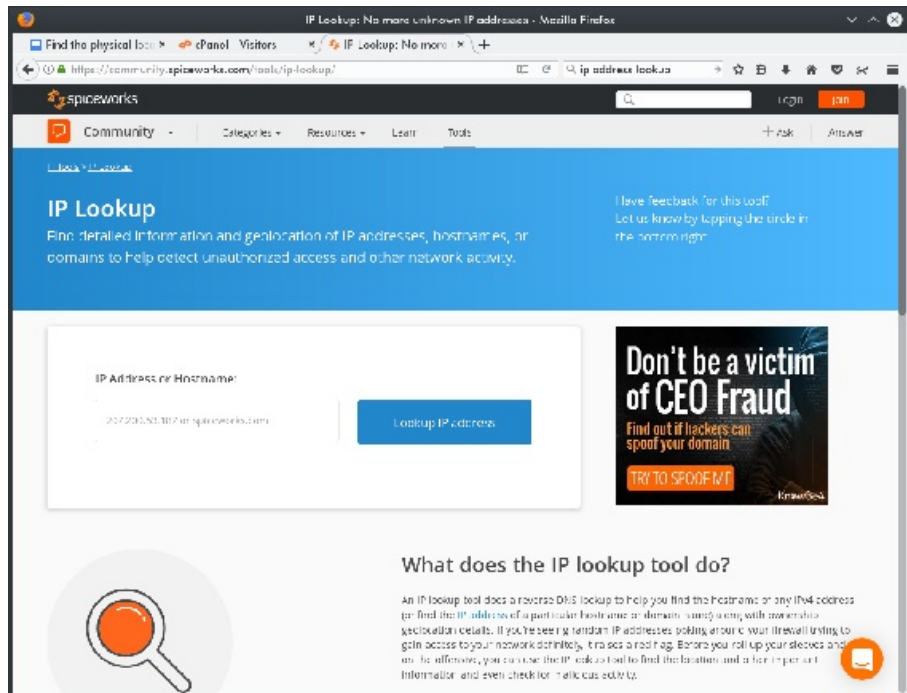


Ezek között az eszközök között van egy látogató naplózó, ami IP-címeket, a meglátogatott URL-t és a használt böngészőt listázza. Ezután legörgettem a Metrics szekcióhoz.



A Spiceworks, hivatásos számítástechnikusok egy csoportja biztosít az IP-cím aktuális helyzetét megjelenítő eszközt, ami egy térkép segítségével megmutatja hol van az IP-cím.

<https://community.spiceworks.com/tools/ip-lookup/>

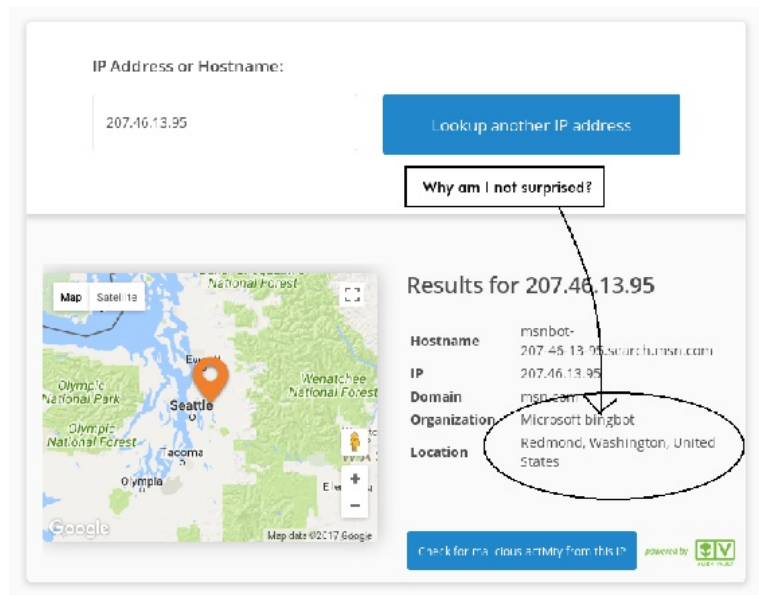


Csak annyit kell tenned, hogy itt beírod az adott IP-címet, vagy a gép host nevét. Például, van egy URL-em nem kívánatos tartalommal (a látogatók naplójában kitarva), aminek az IP-címe 207.46.13.95. Beírom ezt az IP-címet az IP-kereső oldalra a Spiceworks-nél és rákattintok a Lookup IP Adress-re.

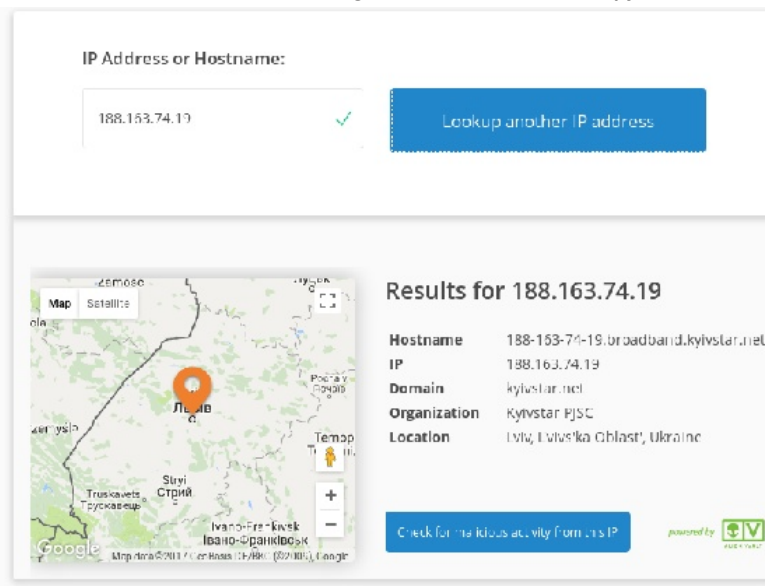
Most legalább tudjuk, hogy van egy robot, amit nem megfelelő tartalmak keresésére programoztak (attól függően, hogy a Microsoft mit tekint nem megfelelőnek. Ki tudja?) a web-en.

Tovább nézve a naplót, a legtöbb hivatkozott URL a Forum lapjaira mutat. Ez elfogadható és elvárható egyben. Van további két URL, ami a legutóbbi USA választás orosz „meghekkelésével” kapcsolatos, a médiában elterjedt vélekedést mutatja alátámasztani. (jobb oldalt

188.163.74.19	/
188.163.74.19	/



Az IP-címet az eszköznek megadva a következőt kapjuk:



Ahogy látható, az IP-cím Ukrajnában található. Kiderült, hogy az IP-cím egy olyan géphez kötődik, ami Windows XP alatti régi böngészőt futtat! Ugyanezen látogató rendelkezik még egy hivatkozó URL-lel:

```
http://komp-pomosch.ru/
http://komp-pomosch.ru/
```

Az URL-t megvizsgálva kiderül, hogy ez egy ukrainai számítógép forgalmazó és javító cég. Tehát semmi gond nincs vele, minden rendben. Vannak még más IP-címeim olyan messziről, mint Dél-Afrika és Ausztrália, egyik sem jelent semmilyen fenyegetést, tehát ismét minden rendben. Sosem lehetsz elég óvatos, amikor digitális tulajdonodról van szó (beleértve a PCLinuxOS telepítéset is). Az is segít, ha a honlapodat egy megbízható cégnél helyezed el, ami ügyel a megrendelőre ... és sose higgy a médiának.



PCLOS-Talk
Instant Messaging Server



Sign up TODAY! <http://pclostalk.pclosusers.com>

Screenshot Showcase

Posted by Hertz, on October 7, 2017, running Mate.