DNS Changer

Nedavno smo vam skrenuli pažnju na virus koji se otkriva time što vaš printer poludi [1] i ispisuje besmislice. Ali što ako vam se korisnik požali da mu "ne radi Internet!", a vi ste uvjereni da je u vašoj mreži sve u redu? Provjerite postavke DNS servisa na korisnikovu računalu. Ako nisu u skladu s vašim lokalnim pravilima, možda je korisnikovo računalo zaraženo nekom od inačica virusa **DNSChanger**? Naziv virusa je **Trojan:W32/DNSChanger**, a osim Windowsa napada i Macove.

FBI je je otkrio botnet od stotina tisuća inficiranih računala kojima su izmijenjene DNS postavke, pa umjesto na legalne DNS servere upite upućuju na neke od "divljih" zamjena koje su postavili kriminalci, kako bi ljude umjesto na prave web siteove usmjeravali kamo oni žele. DNS je jedan od ključnih servisa koji omogućuje rad Interneta, pa činjenica da su kriminalci preuzeli taj servis ne može značiti ništa dobroga. Zamislite da se umjesto u web servis svoje banke ulogirate u lažne stranice koje su vam podmetnuli tipovi koji se žele dočepati saržaja vašeg bankovnog računa?

Istraga je FBI dovela do Estonije, gdje je uhićen lokalni poduzetnik, vlasnik nekoliko tvrtki na koje se sumnjalo da posluju s autorima malwarea. Zaplijenjena su i računala tih tvrtki, među kojima su pronađeni neki od lažnih DNS servera. Iako je time kriminalni lanac prekinut, na Internetu su još uvijek tisuće zaraženih korisničkih računala, koja pokušavaju resolving pomoću nelegalnih DNS servera. FBI se pobrinuo da na njihovo mjesto postavi zamjeske DNS servere, koji štite inficirane korisnike. No ovih dana su zamjene prestale raditi, pa se inficirana računala prepoznaju po tome što im ne radi DNS.

Zarazu ćete brzo otkriti ako, na Windowsima, na komandnoj liniji napišete:

```
ipconfig /all
```

Pokazat će se sve mrežne postavke, između ostalog i zadani DNS serveri. Ako to nisu vaši legalni serveri, provjerite da li je upisana neka od slijedećih adresa:

```
85.255.112.0 - 85.255.127.255
67.210.0.0 - 67.210.15.255
93.188.160.0 - 93.188.167.255
77.67.83.0 - 77.67.83.255
213.109.64.0 - 213.109.79.255
64.28.176.0 - 64.28.191.255
```

Ako ne volite komandnu liniju i više volite prčkati po registryju, potražite ove ključeve:

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{random}
 DhcpNameServer = 85.255.xx.xxx,85.255.xxx.xxx
 HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{random}
 NameServer = 85.255.xxx.133,85.255.xxx.xxx
 HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
 DhcpNameServer = 85.255.xxx.xxx,85.255.xxx.xxx
 HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
 NameServer = 85.255.xxx.xxx,85.255.xxx.xxx
```

Korisnici mogu i sami provjeriti da li su njihova računala zaražena ako posjete web stranicu http://dns-changer.eu [2]. Ako je sve u redu, rezultat će izgledati ovako nekako:

Pripazite, na zaraženim računalima se osim DNS Changera možda kriju još i neki drugi zlćudni programi!

Dokument o DNS Changeru koji je objavio FBI dostupan je ovdje [3].

uto, 2012-07-17 13:37 - Aco Dmitrović**Vijesti:** Sigurnost [4]
Kategorije: Servisi [5]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1065

Links
[1] https://sysportal.carnet.hr/node/1057
[2] http://dns-changer.eu
[3] http://www.fbi.gov/DNS-changer-malware.pdf
[4] https://sysportal.carnet.hr/taxonomy/term/13
[5] https://sysportal.carnet.hr/taxonomy/term/28