Conficker: prvoaprilska šala ili stvarna prijetnja?

Otkako je jučer objavljen članak o tome kako pronaći **Confikera** pomoću nmap-a, javilo mi se nekoliko kolega. Priča o **Confikeru** još nije završena, pa sam odlučio napisati nastavak.

Jedan od spomenutih kolega bio je uvjeren kako se riješio tog crva, ali mu je **nmap** pronašao još šest sumnjivih PC-ja. Naravno, na svima su nedostajale zakrpe. **Conficker-C** se pritaji i ne pokušava zaraziti nova računala, ali ga se može otkriti po specifičnom odgovoru koji uslijedi nakon spajanja na **RPC** servis, što je iskorišteno u **nmapu**.

Drugi kolega smatra da je sve to *provaprilska šala*, da nam se autori **Confikera** rugaju. Osobno, bio bih zadovoljan kad bi to bila samo šala. No ne možemo si priuštiti pasivnost. Taj je crv sposoban povući sa mreže dodatne programe, *Trojance* i *rootkite*.

Jedna od njegovih osobina je generiranje "proizvoljnih" naziva domena i pokušaj spajanja na njih. Ako se na samo jednoj odazove hakerski program, cijela će stvar eskalirati. Mnogi smatraju ovog crva vrlo ozbiljnom prijetnjom, iako prve inačice nisu radile nikakvu štetu, samo su se nastojale proširiti na što više računala.

Microsoft je ponudio nagradu za otkrivanje autora **Confickera**, a nekoliko je tvrtki udružilo snage u borbi protiv njega. Registrirali su domene čije nazive generira crv i osluškivali promet koji dolazi do njih. Na taj način su izbrojali da je zaraženo preko 10 miliona računala i proučavali ponašanje crva.

Javio se i kolega koji je jutros na konzoli AV programa otkrio novu napast koju F-Secure imenuje kao **Trojan:W32/Downadup**.

Na kraju, vrlo konkretan i koristan doprinos kolege Vlatka Košturjaka koji javlja da je izašla nova verzija **nmapa**, koja još bolje detektira **Confickera**. Zasučite rukave i na posao. Smijat ćemo se kasnije, kad opasnost prođe.

```
http://nmap.ucsd.edu/nmap/dist/nmap-4.85BETA6-setup.exe
```

sri, 2009-04-01 10:46 - Aco Dmitrović**Vijesti:** Windows [1]
Kategorije: Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/550

Links

[1] https://sysportal.carnet.hr/taxonomy/term/12
[2] https://sysportal.carnet.hr/taxonomy/term/30