Virus Conficker još uvijek napada

O crvu Confickeru pisali smo još početkom "davne" 2009. godine, kada smo pokazali kako ga otkriti pomoću *nmapa*. U to ga vrijeme antivirusni programi još nisu pouzdano detektirali. Počeo se širiti 2008. i jedan je od "najuspješnijih" virusa, zarazio je milione računala širom svijeta. No zanimljivo je da je nakon tolikih godina Conficker još uvijek aktivan!

Čovjek bi pomislio da su do sada već svi instalirali zakrpe koje onemogućavaju njegovo širenja. No Sophosov godišnji izvještaj tvrdi da u 2011. Conficker vodi na listi najraširenijeg zloćudnog softvera, sa 14,8% pokušaja infekcije.

Prisjetimo se događaja s početka 2009. godine. Conficker je koristio pogrešku u RPC protokolu da bi, zaobilazeći autentikaciju, zarazio računala koja nisu imala instaliranu zakrpu MS08-067. Nakon uklanjanja virusa i instalacije zakrpe, ponovo bi se vratio na računala koja nisu imala instaliran SP3 za Windowse XP. Kad je i to sređeno, pronašli smo ga još jednom na računalima čiji su korisnici imali trivijalne zaporke. Educirali smo ih kako smisliti složenu zaporku i kako je češće mijenjati. Conficker je očigledno koristio više "vektora" napada, a jedan od njih bio je autorun na USB memorijama, pa je trebalo pregledati i korisničke stickove.

Nakon višekratnog čišćenja inficiranih računala zavladao je mir. Sve do trenutka, dobrih godinu dana kasnije, kad sam instalirao open source IDS *Snort*. *Snort* je pronašao računala inficirana Confickerom koja pokušavaju uspostaviti vezu s kontrolnim računalom. Naime, Conficker je generirao nazive domena koje su napadači namjeravali koristiti za upravljanje napadom. Sigurnosna je zajednica te domene blokirala, da bi inficirana računala ostala nepovezana. Snort je očigledno imao aktivan filter koji otkriva SYN pakete usmjerene na generirane nazive domena.

Na inficiranim računalima pokrenuli smo antivirusni softver, koji nije pronašao ništa! Zapržili smo CD-ove preuzete sa weba nekolicine AV tvrtki te bootali računala s njih, provjeravajući datoteke na disku. Opet ništa! Niti jedan antivirusni program nije otkrio Confickera, ali su paketi usmjereni na blokirane domene i dalje odlazili s tih računala. Nije preostalo ništa drugo nego presnimiti korisničke podatke, formatirati diskove, reinstalirati Windowse. Nakon toga tragovi Confickera su nestali. Po svemu sudeći, alati za uklanjanje nisu počistili sve što je trebalo, ostavljajući nedirnut dio koda u nekoj skrivenoj datoteci.

Čitanje Sophosova izvještaja za 2011. ponukalo nas je da ponovimo test *nmapom*.

```
sudo nmap --script smb-check-vulns.nse --script-args=unsafe=1 -p445 192.168.1.0/24
```

Evo tipičnog rezultata:

```
Host script results:
| smb-check-vulns:
|   MS08-067: NOT VULNERABLE
|   Conficker: Likely CLEAN
|   regsvc DoS: NOT VULNERABLE
|_  SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
```

Za sigurnosno osviještenog sistemca uvijek se nađe posla.

Vezani članci:
Kako pomoću nmapa otkriti Confickera [1]
Conficker počeo donositi zaradu [2]
Conficker, prvoaprilska šala ili stvarna prijetnja [3]

čet, 2012-02-16 18:55 - Aco Dmitrović**Vijesti:** Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/938

Links
[1] https://sysportal.carnet.hr./node/549
[2] https://sysportal.carnet.hr./node/556
[3] https://sysportal.carnet.hr./node/550
[4] https://sysportal.carnet.hr./taxonomy/term/13