Apache log: w00tw00t.at.blackhats.romanian.anti-sec

Pregledavajući logove, često nailazimo na čudne zapise. Zaokupljeni svakodnevnim poslovima, pogotovo onima koji ne spadaju u opis njihova posla, sistemci često nemaju vremena istraživati o čemu se radi. Tako u apacheovom error logu često možemo naći zapise u kojima piše "File does not exist:", nakon čega slijedi putanja i naziv nepostojeće datoteke.

Ništa strašno, nekad je ta datoteka postojala, pa je uklonjena, ali je ostala zabilježena u Google *cacheu*. No što kad se traže datoteke koje nikad nisu ni postojale na našem siteu?

Evo jednog primjera iz Apacheova *access loga*:

```
66.197.175.87 - - [27/Jan/2013:06:39:22 +0100] "GET /w00tw00t.at.ISC.SANS.DFind:) HTT
P/1.1" 400 511 "-" "-"
```

U *error logu* zapis istog događaja izgleda nešto drugačije:

```
[Sun Jan 27 06:39:22 2013] [error] [client 66.197.175.87] client sent HTTP/1.1 reques
t without hostname (see RFC2616 section 14.23): /w00tw00t.at.ISC.SANS.DFind:)
```

Ili ovako:

```
[Sun Jan 20 02:11:40 2013] [error] [client 202.104.192.162] File does not exist: /hom
e/httpd/htdocs/w00tw00t.at.blackhats.romanian.anti-sec:)
```

Spominjanje SANS-a još nekako djeluje umirujuće, ali rumunjski *blackhats* i to još s kineske IP adrese?

Većina sistemaca ignorira ovakve zapise. Netko je tražio datoteku koja ne postoji, nikakva šteta! Onda ih te poruke počinju nervirati, pa gledaju kako bi ih uklonili iz logova, ili blokirali takve upite. Na kraju će poželjeti saznati o čemu se tu zapravo radi. A istraga može biti zanimljiva, čak zabavna.

U Wikipediji postoji stranica posvećena w00tu! Tamo stoji da je to *leetspeak* koji izražava veselje i uzbuđenje. Izraz se udomaćio na Mreži, tako da je čak dospio u Oxford English Dictionary, ali bez elitnog načina pisanja, kao "woot". A crackeri bi, kada se uspiju dočepati root privilegija na tuđem računalu, slavili porukom: "**w00t, I have r00t!**"

Od kolega koji se bave informacijskom sigurnošću saznat ćemo da se radi o skeniranju obavljenom pomalo zastarjelim alatom DFind, kojeg koriste "scriptie kidz". Alat šalje upit na portove na kojima se obično odaziva web server tražeći w00tw00t stranicu. Upit ne poštuje protokol, otud u logu poruka "request without hostname". Različiti web serveri odgovaraju različito na taj zahtjev, pa se time detektira da li se koristi Apache, IIS ili nešto treće.

Što se tiče blokiranja adresa s kojih stižu ovakvi upiti, kažu da *fail2ban* ne pomaže, jer se sken prekine nakon 5 upita, pa se onda nastavlja s druge adrese.

Ono što funkcionira je traženje stringa pomoću iptablesa.

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

```
# iptables -I INPUT -d xxx.xxx.xxx.xxx -p tcp --dport 80 -m string --to 70  --algo bm
 --string 'GET /w00tw00t.at.ISC.SANS.' -j DROP
```

No filtriranje stringova opterećuje vaš web server, pa razmislite da li vam to uopće treba. Možda je bolje ugraditi filter u vašu svijest, pa da takve zapise jednostavno više ne registrirate. :)

Više možete saznati na ovom linku [1].

čet, 2013-01-31 09:58 - Aco Dmitrović**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1192

Links
[1] http://spamcleaner.org/en/misc/w00tw00t.html

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