Kako se maknuti s crnih lista?

Jedan od najčešćih sigurnosnih problema na poslužiteljima u CARNetovoj mreži je sudjelovanje u **DoS** napadima i slanje spama. Naravno, ovo ne rade korisnici, barem ne svjesno. Napadači pronalaze propuste u raznim servisima, te ih iskorištavaju za svoje potrebe.

Najčešće se napada preko weba, rabeći propuste u CMS-ovima (*Joomla* i drugi), mail servisima (*Squirrelmail*) i samom programskom jeziku PHP (čija sigurnosna reputacija nije nimalo blistava). Kako se rupe i propusti sve teže pronalaze, napadači rabe i druge tehnike, kao što je otkrivanje korisničkih zaporki. Nakon što dobiju zaporku, dobiju i pristup do svih korisnikovih resursa. Obično se zadrže samo na slanju spamova na tisuće adresa. Kako nemate kontrolu nad sadržajem mailova, vrlo brzo vaš poslužitelj dolazi na crnu listu velikih mail providera (Yahoo, Google), a potom i na druge zaštitne sustave (Spamcop), pa problem ubrzo postaje ozbiljan.

Prije nego se možete skinuti s crnih lista (a adresa za tu proceduru najčešće piše u samim logovima - npr. /var/log/mail.log), morate situaciju istražiti i riješiti problem. No, to nije tako lako zbog različitih načina upada.

O ovom problemu smo već pisali u članku "**Kako pronaći spamera u vlastitim redovima** [1]". Tu smo opisali kako pronaći sumnjive logove i kako pronaći odgovornog korisnika, onog čija je zaporka provaljena. Ukoliko je napad došao preko Squirrelmaila, možete se pomoći člankom "Squirrelmailov dodatak Squirrel Logger **[2]**". Pomoću Loggera možete dobiti informaciju koji od korisnika šalje velike količine maila. Inače, u Squirrelmailu je teško doći do ove informacije.

Dio spamova je preveden na hrvatski jezik, a ovdje poglavito mislimo na one mailove koji od korisnika traže da im se pošalje zaporka. Najbolje je takve spamove blokirati čim ih primjetite, da ne bi došli do previše korisnika. Kako, pokazali smo vam u članku **"Prevedeni spamovi opet napadaju - kako smanjiti štetu?".** [3]

Dodatan način detekcije i rješavanja ovog problema na listi **"sistemci"** napisao je kolega Bojan Mauser iz CARNeta:

"*Sa sličnim problemom sam se nedavno susreo... obično spameri provale preko nekog nodržavanog weba i postave svoju skriptu (npr .php file) na server preko koje šalju spam. Vjerojatno postoji neka nesigurna upload forma preko koje uspiju uploadati skriptu u folder gdje ne bi smjeli. Skripta je dohvatljiva preko weba (izvana) pa je tako mogu pokrenuti. Evo par stvari koje možete napraviti:*

- Treba pogledati mailove koji se šalju i u headerima obično bude nešto poput:

```
sender_fullname: www-data
sender: www-data@domana.hr
X-PHP-Originating-Script: 33:favicon.php(6) ...
```

*Ovdje se vidi da je php skripta **favicon.php** poslala taj mail, tj. korisnik **www-data** pod kojim je pokrenut web poslužitelj.*

- Provjeriti gdje sve korisnik pod kojim se web poslužitelj pokreće (obično www-data) može pisati:

```
root$ su www-data
www-data$ find / -writable
```

*Trebate ukinuti dozvolu "**write**" na svim mjestima gdje to nije potrebno. Ako uspiju provaliti, obično će postaviti skripte gdje god mogu pisati na poslužitelju i onda ih probati dohvatiti preko weba.*

*Također treba pripaziti na činjenicu da ukoliko je dozvoljen upload u neki folder da je tamo **zabranjeno** pokretanje skripti (to se podešava u .htaccess). Još bolje da folder nije uopće vidljiv preko weba, ako to nije nužno.*

*- S nekim antimalware alatom pregledati sve foldere gdje se webovi nalaze (ili cijeli datotečni sustav). Obično su to folderi **/var/www**, **/usr/share**, **/srv**, **/home**. Dobar alat za to je **maldet** (http://www.rfxn.com/projects/linux-malware-detect/ [4]) koji daje izvješće ovog tipa:*

```
{CAV}MBL_409495 : /usr/share/doc/rar/copyright
{CAV}Trojan.PHP-43 : /usr/share/squirrelmail/w61665329n.php
{CAV}PHP.Trojan.WebShell-9 : /home/user/web/templates/system/onlines.php
{CAV}PHP.Hide : /home/user/web/w9606659n.php
{CAV}PHP.Trojan.WebShell-9 : /home/user/public_html/favicon.php
```

*- Pogledati apachejev **access.log** (u **/var/log/apache2**). Tamo se mogu naći zapisi tipa:*

```
... "POST /favicon.php HTTP/1.1" ...
```

gdje se može vidjeti da netko neprestano radi POST na skriptu koja šalje mailove, a vidi se i IP adresa s koje napadi dolaze.

- Trebalo bi naći web preko kojeg su provalili (prvo posumnjajte na CMS-ove koje korisnici sami održavaju, obično **wordpress**, **joomla** i sl.) i njega ugasiti dok se ne zakrpa. Često je problem u nekom pluginu, tipa fotogalerije ili slično.

Preporučio bih da webovi korisnika ne budu na istom stroju koji je mail server ustanove i na kojem su drugi važni servisi, jer je zapravo nemoguće kontrolirati i biti siguran da netko nece ostaviti kakvu rupu za spamere. Kada se za to sazna server je vec na spam listama i korisnici se žale da mailovi ne prolaze."

čet, 2013-05-02 09:45 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Servisi [6]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: https://sysportal.carnet.hr/node/1261

Links
[1] https://sysportal.carnet.hr/node/925
[2] https://sysportal.carnet.hr/node/906
[3] https://sysportal.carnet.hr/node/905

[4] http://www.rfxn.com/projects/linux-malware-detect/
[5] https://sysportal.carnet.hr/taxonomy/term/17
[6] https://sysportal.carnet.hr/taxonomy/term/28