Prevedeni spamovi opet napadaju - kako smanjiti štetu?

Sigurno ste u ovo praznično vrijeme dobijali povećani broj spamova, lažnih pozitiva u spam mapama te lažiranih mailova na hrvatskom jeziku. Ovi potonji pokušavaju nagovoriti korisnike da im pošalju svoju zaporku ili drugu povjerljivu informaciju. Jednu takvu *phishing* poruku mnogi su dobili pred blagdane:

```
Date: 23 Dec 2011 12:36:17 +0100
From: Porezna Upravat <povrat@porezna-uprava.hr>
Reply-To: noreply@porezna-uprava.hr
To: undisclosed-recipients:  ;
Subject: Obavijest za povrat

MINISTARSTVO FINANCIJA - Porezna uprava
23/12/2011

Dragi poreznog obveznika,

Nakon posljednjeg godisnji obracun svog fiskalne aktivnosti smo utvrdili da
ste podobni za primanje povrat poreza od 857.88 HRK.

Molimo podnesite zahtjev za povrat poreza i dopustiti nam 6-9 dana kako bi
se proces.

Da biste pristupili povrat poreza, slijedite korake u nastavku:

....- Preuzimanje Povrat obrazac u prilogu ovog email
....- Ga otvorite u pregledniku
....- Slijedite upute na zaslonu

Povrat moze biti odgoden za niz razloga. Na primjer podnosenja nevazecih zapisa
ili primjenom nakon isteka roka.
```

Iako je poruka očigleno loš prijevod sa stranog jezika, dovoljno je razumljiva da poneki korisnik u žurbi povjeruje u njenu vjerodostojnost i pošalje tražene podatke. Kada dobiju zaporku, spameri počinju rabiti vaš poslužitelj kao *relay* server, te ubrzo vaša domena dospije na crne liste poput onih koje sami koristite (bl.spamcop.net, dnsbl.njabl.org, zen.spamhaus.org i slične). Kad se to dogodi, vaši će se korisnici početi žaliti da više ne mogu slati poruke, jer ih odredišni serveri odbijaju.

Što učiniti? Jedino dugoročno rješenje je **preventivno** djelovanje i obuka korisnika. Naučite svoje korisnike da provjere takve poruke prije nego im povjeruju. Kada su u nedoumici, neka potraže savjet sistemskog inženjera. I naučite ih da nikad nikome ne otkrivaju svoju zaporku. Uostalom, to bi trebalo biti jasno navedeno u sigurnosnoj politici.

Dobro bi bilo da korisnicima održite barem jedan tečaj godišnje, koji bi odgovarao na njihove najčešće upite, te upoznavao nove zaposlenike i suradnike "kako stvari funkcioniraju".

A što učiniti *postmortem*, u situaciji kad je spam već došao u korisničke sandučiće? Najprije pošaljite

poruku svojim korisnicima i upozorite ih da je ta poruka lažna, da je obrišu i ne odgovaraju na nju (i nadajte se da nitko nije poslao zaporku). Da ovaj mail ne bi ponovo stigao na sustav, naučite SpamAssassin da se radi o spamu. "Trening" SpamAssassina je izvodi ovako: prvo izdvojite mail u datoteku, a potom pozovite naredbu sa-learn:

```
# sa-learn --spam poruka.msg
Learned tokens from 1 message(s) (1 message(s) examined)
```

Vjerojatno to neće biti dovoljno, jer statističkom filteru je potrebno na stotine poruka (i *spam*a i *hama*) kako bi postao efikasan. Brže rješenje je blokiranje poruke po sadržaju. Upišite sljedeće u /etc/spamassassin/local.cf:

```
body SPAM_POREZ      /M<!--p8as-->I<!--p8as-->N<!--p8as-->I<!--p8as-->S<!--p8as-->/i
describe SPAM_POREZ Spam o povratu poreza od 857.88 kuna
score SPAM_POREZ     5.0
```

Ovime smo dodali ocjenu (SA *score*) 5.0 svakoj poruci koji sadrži pojam "MINIS" (od MINISTARSTVO FINANCIJA). Granica reza je obično na 6.31, no nikada ne dajemo ocjenu koja odmah prelazi granicu, jer time dajemo šansu SpamAssassinu da propusti mail ukoliko sadrži dovoljno drugih elemenata za prolaz. Primjerice, nije isto ako dobijete ovaj spam izravno ili vam ga proslijedi korisnik s upitom "što da napravim s ovim?". Želite dobiti upit, ali ne i spam, zato *score* treba biti nešto niži.

Mail je u HTML formatu, moramo ga tako i upisati jer SpamAssassin ne radi dekodiranje HTML-a. Radi jasnoće je stavljeno samo nekoliko slova, no možete staviti i više, dapače, preporučljivo je. Blokiranje po sadržaju nije jednostavno i traži određena predznanja. Treba pripaziti da ne omogućimo *false positive*, blokiranje dobrih mailova, upita vaših korisnika ili savjeta s lista o tome kako ukloniti problem. Stoga, oprezno s ovom mogućnošću, a najbolje je da ovakve *harcodirane* unose izbrišete nakon nekog vremena, kad poruke prestanu stizati. Spameri će već prijeći na neku drugu lažiranu obavijest.

A što učiniti ako su spameri počeli rabiti vaše računalo kao *mail relay*? O tome u drugom članku, u kojem ćemo opisati kako otkriti koji korisnici i preko kojih servisa šalju spamove, te kako popraviti nastale rupe u sustavu.

- Logirajte [1] se za dodavanje komentara

uto, 2011-12-27 16:31 - Željko Borš**Kuharice:** Linux [2]
Kategorije: Servisi [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/905

Links
[1] https://sysportal.carnet.hr./sysportallogin
[2] https://sysportal.carnet.hr./taxonomy/term/17

[3] https://sysportal.carnet.hr./taxonomy/term/28