Kako pronaći spamera u vlastitim redovima

Već smo objavili članke o tome kako se obraniti od prevedenih spamova [1], odnosno, u slučaju webmaila, kako detektirati [2] preko čijeg se korisničkog računa šalje spam. Izravan povod su upiti na sys.help, na adresi syshelp@carnet.hr. Ovim člankom probat ćemo zaokružiti priču, opisati kako otkriti način "provale", kako se šalju spamovi i kako se skinuti sa crnih lista.

Upiti koji nam dolaze najčešće su potaknuti pritužbama korisnika da ne mogu slati mail na određene adrese, najčešće na velike mail providere tipa Gmail i Yahoo. U logovima se lako može pronaći URL na kojem se može zatražiti uklanjanje s crne liste, ali ako se ne pronađu krivci i ne ukloni uzrok vaše će računalo brzo biti vraćeno na crnu listu.

Iz vlastitog iskustva zaključili smo da su tri najčešća načina *spamiranja*i:

1. slanje spama preko webmaila

2. slanje spama uz pomoć SASL-a (SMTP AUTH)

3. slanje preko zaraženog računala iz lokalne mreže

Pa kako to spamer može slati mail iz naše mreže, na primjer preko webmaila? Lako, ukoliko otkrije korisnikovu zaporku. Najčešće je otkriva socijalnim inženjeringom, pomoću lažnih mailova za koje se čini da potječu od administratora sustava ili nekog servisa. Takvi su mailovi najčešće prevedeni, i to sve bolje i bolje. Njih smo obradili u prvom članku [1]iz serije.

Drugi način zloporabe korisnikove zaporke je pomoću SASL mehanizma, koji omogućava korisnicima da šalju mailove iz vanjskih mreža. Uporaba je jednostavna, samo treba u mail klijentu označiti da želimo SMTP autentikaciju i mailovi već prolaze. Ovaj način autentikacije smo obradili u članku http://sistemac.carnet.hr/node/747 [3].

Zadnji, i možda najjednostavniji način je slanje spama sa zaraženog računala u vašoj lokalnoj mreži. Za to nije ni potrebna zaporka, jer će mail poslužitelj bez autentikacije primiti mail s računala iz lokalne mreže i proslijediti ga. Današnji spamerski alati znaju pročitati postavke iz mail klijenta i ponašati se poput normalnih mail klijenata, umjesto da izravno šalju mailove na port 25, što je lako spriječiti na vašem usmjerivaču gdje se to dozvoli samo legalnom mail serveru.

Problem je kako detektirati što se događa, odnosno čija je zaporka provaljena. To nije trivijalno jer je, kako smo opisali, zloporaba moguća na više načina.

Najproblematičnijim se pokazao webmail, jer je logiranje rudimentarno. Problemu smo doskočili instalacijom dodatnog modula (Squirrel Logger [4]), s kojim se definira što će se i kada zapisivati. Na taj način se "iz aviona" vidi tko je odgovoran za problem. Modul smo opisali u spomenutom članku [2].

Ukoliko su spameri posegnuli za SASL autentikacijom, zadatak će vam biti olakšan činjenicom da tu autentikaciju ne rabi mnogo korisnika, osim u slučaju da ste sustav tako konfigurirali. Zbog toga su unosi u logovima prilično uočljivi, te ih je lako usporediti sa spamovima. CARNetov CERT će vam poslati kopiju spama, zajedno sa svim zaglavljima.

Unosi u logovima izgledaju poput ovih:

```
Jan 31 12:43:48 server postfix/smtpd[3298]: connect from
   pc-racunalo.domena.hr[161.53.XX.YYY]
Jan 31 12:43:59 server postfix/smtpd[3298]: 38S753T5957: client=
   pc-racunalo.domena.hr[161.53.XX.YYY], sasl_method=PLAIN,
   sasl_username=korisnik@domena.hr
```

Dakle lako je vidjeti koji korisnik se autenticirao, što nam olakšava posao.

Ostaje nam zadnji slučaj, kada imamo zaraženo računalo u mreži. U tom je slučaju situacija "šarolika" i ovisi o tipu programa/virusa/crva kojije zarazio računalo. Najlakši je slučaj kad računalo šalje mnogo mailova, što ga čini uočljivim u logovima. Tome se može doskočiti stavljanjem više primatelja u **To** ili **Cc** polje, što smanjuje broj konekcija prema Postfixu. Tu dolazimo do granice kada više ne možemo pružiti nekakav konkretniji savjet, nego moramo uopćiti cijelu priču. Pa krenimo...

U istraživanju si možete pomoći tako da pogledate vrijeme slanja mailova, kao i "*message id*" oznaku. Pronaći ćete ih u zaglavlju spama, kojeg će vam poslati druga strana ili CERT, ponekad i prije nego dospijete na crnu listu. Nemojte odmah tražiti po **From** polju, jer se to lako lažira. Za tim posegnite kada više nemate izbora i valja se hvatati za slamku.

Ukoliko i dalje ne možete pronaći ništa sumnjivo, vrijeme je za malo detektivskog rada. Kad nađete kandidate među korisnicima (bilo preko IP adrese, bilo preko *usernamea*), nazovite ih i pitajte jesu li slali kakve mailove, prema kome i koliko puta. Možda su u to vrijeme bili čak odsutni od računala, što je definitivno dokaz da je njihovoračunalo zaraženo.

Moguće je da i nakon toga ništa ne nađete. Spameri mogu na mail poslužitelju pomoću ranjivosti web sučelja instalirati programe koji služe za relay portova i time zaobići mnoge sigurnosne sustave. U ovakvim slučajevima pomažu vatrozidi i Intrusion Detection sustavi, ali to prelazi granice ovog članka.

Što uraditi nakon svega, kada se situacija vrati u normalu, a računalo je brisano s crne liste? Uložite trud u obrazovanje vaših korisnika. Objasnite im da nikada nećete tražiti njihovu zaporku preko maila, da ne klikaju na razne linkove navedene u nemušto prevedenim mailovima. Održite seminar, pošaljite upozorenja, zalijepite obavijest na hodniku. Konkretni postupci ovise o lokalnim navikama i očekivanjima vaših korisnika, a bitan čimbenik je i veličina ustanove na kojoj radite.

Nadamo se da smo s ova tri članka bar malo pomogli rješavanju problema spama.

- Logirajte [5] se za dodavanje komentara

uto, 2012-01-31 22:44 - Željko Borš**Kuharice:** Linux [6]
Kategorije: Servisi [7]
Vote: 0

No votes yet

story_tag: SASL [8]
spam [9]
kako detektirati spam [10]
SMTP AUTH [11]

Source URL: https://sysportal.carnet.hr/node/925

Links
[1] https://sysportal.carnet.hr/node/905
[2] https://sysportal.carnet.hr/node/906
[3] https://sysportal.carnet.hr/node/747
[4] http://www.squirrelmail.org/plugin_view.php?id=52
[5] https://sysportal.carnet.hr/sysportallogin
[6] https://sysportal.carnet.hr/taxonomy/term/17
[7] https://sysportal.carnet.hr/taxonomy/term/28
[8] https://sysportal.carnet.hr/taxonomy/term/143
[9] https://sysportal.carnet.hr/taxonomy/term/363
[10] https://sysportal.carnet.hr/taxonomy/term/364
[11] https://sysportal.carnet.hr/taxonomy/term/144