Jernej Porenta,
Arnes

Neželena elektronska pošta
Email spam

Povzetek

Neželeno elektronsko pošto poznamo vsi in vsem nam povzroča preglavice. V članku bom predstavil več zanimivosti o ozadju masovnih neželenih sporočil, več nasvetov, kako se braniti pred njimi in kako to počnemo na Arnesu (oziroma kako to počnejo še večji).

Ključne besede: elektronske komunikacije, elektronska pošta, neželena elektronska pošta.

Abstract

Email spam is known to everyone with an email address and makes our life harder. In this paper I will present some information about email spam, senders of it and how to avoid it. I will also present the methods used within ARNES's anti-spam infrastructure and it compares to large ISPs.

Keywords: electronic communications, email, spam

Uvod

Elektronska pošta je dandanes osnova elektronskih komunikacij med posamezniki. Z približno 3.3 miljarde uporabnikov na svetu predstavlja najpogostejši način komunikacije, za katerega se pričakuje, da bo do leta 2016 porasel še za dodatnih 6 % (Radicati & Hoang, 2012).

Ravno zaradi razširjenosti je postala elektronska pošta zanimivo področje za izvajanje oglaševanja s pošiljanjem nenaročene elektronske pošte, ki ji pravimo tudi neželena elektronska pošta (ang. »spam«). V osnovi neželeno elektronsko pošto opredelimo kot elektronsko sporočilo, navadno z oglaševalsko vsebino, razposlano na več naslovov. In ker nam taka sporočila preprečujejo normalno uporabo elektronske pošte, večina ponudnikov internetnih storitev izvaja aktivnosti, ki bi prejemnike obvarovale pred takimi sporočili.

Neželena elektronska pošta

Neželena elektronska pošta predstavlja okrog 64 % vse elektronske pošte, izmenjane med strežniki po svetu, in ravno zaradi tega ovira produktivnost prejemnikov (Intelligence, 2013). Zadnjih nekaj let je moč opaziti trend upadanja količine neželene elektronske pošte zaradi omejevanja glavnih virov neželene elektronske pošte – »botnetov«. To so velika omrežja računalnikov pod nadzorom pošiljateljev neželene elektronske pošte, ki so odgovorna za več kot 70 % vse neželene elektronske pošte.

Razlogi za pošiljanje neželene elektronske pošte se skrivajo predvsem v poceni načinu oglaševanja in enostavnih možnostih, ki dovoljujejo zlorabo. Sama elektronska pošta namreč omogoča ponarejanje pošiljatelja, poceni oglaševanje, saj »kupec nosi stroške«, in predstavlja enostaven način za dostop do posameznikove zasebnosti z oglaševanjem stvari, za katere so običajne oglaševalske poti sicer zaprte ali omejene (Viagra itd.).

Med vire neželene elektronske pošte najpogosteje prištevamo že prej omenjena omrežja (»botnet«) in tudi nevešče oglaševalce, ki velikokrat pošiljajo svoja oglasna sporočila na elektronske naslove, za katere niso predhodno pridobili soglasja (kar je v nasprotju s slovenskim zakonom o elektronskih komunikacijah). Velik delež pošiljateljev neželene elektronske pošte predstavljajo tudi zlorabljeni oziroma slabo zaščiteni strežniki, ki dovoljujejo prepošiljanje elektronske pošte vsem uporabnikom interneta. Nekaj pošiljateljev neželene elektronske pošte najdemo tudi v odprtih brezžičnih omrežjih.

Zaščita pred neželeno elektronsko pošto

V splošnem obstajata dva načina zaščite pred tovrstno elektronsko pošto: pred prejemom in po njem. Pred prejemom elektronske pošte lahko namreč preverimo nekaj lastnosti pošiljatelja (pošiljateljevo ime, lastnosti povezave, pošiljateljev operacijski sistem, geolokacija pošiljatelja, domeno, spoštovanje protokolov itd.) in na podlagi teh lastnosti sprejmemo oziroma zavrnemo elektronsko pošto. Z analizo vsebine po prejemu pa lahko natančneje določimo, ali je prejeta elektronska pošta res neželena ali ne. S pravnega vidika pa za tak poseg potrebujemo predhodno soglasje prejemnika elektronske pošte.

Analiza vsebine elektronske pošte poteka z iskanjem vzorcev v elektronskem sporočilu. Programska oprema išče ključne besede (»loose weight«, »earn money« itd.), preveri samo strukturo elektronske pošte (HTML, plain, MIME), preveri priponke in slabo besedišče. Precej pogosto je namreč, da so neželena sporočila med sabo zelo podobna, saj jih pošiljatelji generirajo kar iz predlog. Programi za označevanje neželene elektronske pošte preverijo tudi spletne povezave v elektronski pošti na javno dostopnih bazah zlorabljenih naslovov. Z metodami strojnega učenja (naivni Bayes, CRM114, dspam, bogofilter) ta programska oprema precej natančno določi vsebino elektronskega sporočila, vendar se zanaša na predhodno ročno učenje.

V zadnjem času je precej pogosto tudi podpisovanje elektronskih sporočil s podpisi DKIM, kar omogoča preverjanje pošiljatelja in zagotavlja, da je elektronska pošta res prišla od pravega pošiljatelja (Leiba & Fenton, 2007).

Arnes in neželena elektronska pošta

Na trgu najdemo kar nekaj programske opreme, ki omogoča dobro označevanje neželene elektronske pošte (IronPort, TrustedSource, PineApp, Commtouch, Barracuda, Microsoft Exchange, TrendGate itd.), a na Arnesu uporabljamo skupek prostodostopne programske opreme:

- programsko opremo »postfix« za SMTP-strežnik;
- v Sloveniji razvito programsko opremo »amavisd«, ki za določevanje vsebine elektronske pošte uporablja programe »SpamAssassin«, »CRM114«, »clamd« in ostale.

Samostojno razvita rešitev nam omogoča dobro zanesljivost našega sistema, saj pravilno označimo kar 99.9 % vse prejete elektronske pošte, ki jo pregleda naš sistem. Še največ napak naš sistem naredi pri napačni klasifikaciji neželene pošte, ki jo označi kot želeno, medtem ko želena elektronska pošta redko konča med neželeno.

Kako označujejo neželeno elektronsko pošto veliki?

Veliki ponudniki spletnih storitev in elektronske pošte (Google, Yahoo, Yandex, Hotmail itd.) za označevanje neželene elektronske pošte uporabljajo lastno razvito programsko opremo, ki se predvsem zanaša na DKIM-podpisovanje, lastne podatkovne baze in veliko tudi na povratne informacije samih uporabnikov (Taylor, 2006).

Google svoje rešitve ponuja tudi v produktu podjetja Postini, vendar zanesljivost storitve ni na tako dobrem nivoju, kot je sam Googlov sistem za zaznavo neželene elektronske pošte, kar kaže na dejstvo, da je dobra povratna informacija bistvena lastnost dobrega in učinkovitega boja proti neželeni elektronski pošti.

Zaključek

Neželena elektronska pošta ne glede na pogosta (oglasna) sporočila, ki sporočajo o rešenem problemu, ostajajo trn v peti vseh ponudnikov spletnih storitev. Za boj proti njej pa ponudniki storitev uporabljamo različne metode, ki končne prejemnike dobro varujejo pred vsemi pastmi, ki jih predstavlja neželena elektronska pošta.

Viri

Intelligence, S. (2013). *Symantec Intelligence Report: January 2013* (pp. 1–7).

Leiba, B., & Fenton, J. (2007). DomainKeys Identified Mail (DKIM): Using digital signatures for domain verification. *Proceedings of the Fourth Conference on Email and Anti-Spam (CEAS)*.

Radicati, S., & Hoang, Q. (2012). *Email Statistics Report , 2012-2016* (Vol. 44).

Taylor, B. (2006). Sender reputation in a large webmail service. *Proceedings of the Third Conference on Email and Anti-Spam (CEAS)*.