XIV. FIATAL MŰSZAKIAK TUDOMÁNYOS ÜLÉSSZAKA

Kolozsvár, 2009. március 26-27.

SZEMTELEN SPAMEK

Fried Zoltán

Abstract

Spam means the abuse of unsolicited or undesired electronic messages usually appearing as advertisements. The sending price of spams is very low, hence a vast number of spams (more than hundred millions daily) are sent to different users. However, the greatest risk is that spams can harm the computer system, can act as spy programs and can read sensitive information.

Keywords:

spam, email, spam filtering

Összefoglalás

A spam a fogadó által nem kért (illetve nem várt) általában elektronikusan, pl. emailen keresztül tömegesen küldött hirdetés, felhívás. Az email-küldés költségei igen alacsonyak, ezért a „szemetelők” nagyon nagyszámú – akár több száz - millió emailt küldenek szét naponta, melyek jelentősen csökkentik e kommunikációs forma hatékonyságát. A spamek nagy része tudatosan megtévesztő, a fogadó kihasználására, közvetve esetleg számítógép-rendszerének megbénítására, olykor "kémkedés" céljára szolgál.

Kulcsszavak:

spam, email, spamszűrés

1. Nagyon rövid történeti áttekintés

A spam [4,7] nem a korunk találmánya. Az első spam 1978-ban bukkant fel, amit a DEC (Digital Equipment Corporation) egyik marketingese (Gary Thuerk) küldött szét közel 600 címre. Ez akkoriban nagyszámú emailnek számított, ugyanis abban az időben a internet a mai formájában még nem létezett. Az internet neve akkor még arpanet volt, és csak pár ezer, egyetemen levő és kormányzati számítógép volt csatlakoztatva hozzá. Ezután 1994-ig egyfajta szünet következett a spammerek számára, ugyanis a következő incidenst egy ügyvéd házaspár követte el [1]. Ettől az időponttól kezdve hívjuk a kényszerű leveleket spamnek. A spam eredetileg konzerv lönchúst jelent. Ennek ellenére a kényszerű levelek nem a lönchús után kapták a nevüket, hanem a Monty Python 1970-ben előadott egyik darabjának töltelékszava után. Ebben a sketch-ben a vikingek egy csoportja - ha kell, ha nem - minden mondatába beépíti a spam szót, mely több mint 100-szor hangzik el a majdnem 3 és fél perces előadásban [3]. Tíz évvel később a teljes levélforgalom 35%-a, 2007-re - egyes felmérések szerint - már 95%-a spam volt [9].

2. A spamben levő üzlet

A spamek 90%-a reklám. A hirdetést megrendelő cég fizet a spammernek azért, hogy reklámozza a

termékét, és sokszor a spammer fizet a szolgáltatónak, hogy hagyja őt, ezt a tevékenységet szabadon üzni. A cég és a spammer között megkötött "szerződés" legfontosabb része, hogy biztosítsa a spammernek a névtelenséget, valamint hogy a megrendelőről soha se derülhessen ki, hogy ő a finanszírozó, és kapcsolatban van egy spammerrel. A spammer fizetése a spam szétküldése utáni profitból keletkezik. A spameknek több mint 90%-a egy weboldalra irányít mindenkit, ahol megrendelhetjük a reklámozott terméket. Így egzaktul mérhető egy reklámkampány effektív profitja. A spam maradék 10%-nak nem reklám a célja [9].

A spammer munkájához szükség **lehet** a spammer internetszolgáltatójának támogatására is, mégpedig olyan tekintetben, hogy ne zárja ki őt az ügyfelei közül, amiért megszegi a szolgáltató internethasználati előírásait, miszerint spammelni **TILOS**. Ez úgy érető el, hogy egy titkos szerződést köt a szolgáltatójával, melyben külön díjazás fejében már nem vonatkoznak rá a szolgáltató spamellenes szabályai.

Az üzlet másik oldala, hogy a reklámozott termék megrendelője igyekszik eltüntetni a nyomokat a spammerhez vezető nyomokat. Ezt úgy érik el, hogy a kettőjük szerződésében kikötik, hogy a reklámozandó terméket nem spam formájában hirdetik. Amint kiderül a turpisság a megrendelő hivatkozva a szerződésben levő kikötésre "azonnal" (persze miután minden levél elküldésre került) megszünteti a kapcsolatát a spammerrel, és mossa kezeit. Addig viszont nagy vehemenciával tagadják, hogy nekik bármi közük is lenne e kétes üzlethez.

Abban az esetben ha valami miatt a spammer nem kapja meg a fizetését, nem sok mindent tehet. A megrendelők tudják, hogy a spammer nem fog bírósághoz fordulni, feljelentéseket tenni [9].

3. A spammer munkájának fázisai dióhéjban

Egy kampány sikere azon áll vagy bukik, hogy minél több levél legyen szétküldve a célközönségnek. A spammer ezért először is megpróbál összegyűjteni több millió email címet, melyek nagy hányada működik is. Egy gyakori módszer, hogy a weblapokat kutatja egy erre a feladatra írt speciális szoftverrel, amely a weboldalon található email címeket gyűjti össze. Másik népszerű módszer, hogy megpróbálja az email címeket kitalálni. A legegyszerűbb, amikor megvásárolnak ilyen listákat valakiktől. Tipikusan minden olyan weblap, ahol meg kell adnunk az email címünket alapul szolgálhat egy eladható címlista összeállítására. A levél tartalmának összeállításához meg kell ismerni minél több spamszűrőt, spamszűrési módszert, hogy azok kicselezésével átcsússzon a levél a spamszűrőkön.

A levél elküldéséhez szükség van SMTP (Simple Mail Transfer Protokoll) szerverre/szerverekre, amelyeknek a segítségével elküldhetők a levelek a címlistáin levő címekre. A levél elküldésének két lehetőség van. Egyik lehetőség a már létező, és legális SMTP szervert/szervereket használunk fel a levelek célba juttatásához, a másik egy vagy több "bot hálózat" (botnet [6]) használata. A botnet hálózatot a legegyszerűbb bérelni, mely hálózat segítségével a gyanútlan internet-felhasználók számítógépe felett a spammer át tudja venni az irányítást és saját céljaira használja azt. Jelen esetben spamküldésre. Egyes felmérések szerint a spamek kb. 75%-ért 3-4 botnet a felelős [8].

Végül a spammernek még gondoskodnia kell arról is, hogy ne csíphessék nyakon. Ezt a fent vázolt botnettel érheti el a legkönnyebben.

4. A levél útja a feladótól a címzettig

Amikor Alice elküld egy levelet Bob-nak (bob@b.org), akkor Alice levelezőkliense (MUA) egy SMTP szervernek (smtp.a.org) küldi a levelet. Ennek a szervernek az a feladata, hogy Alice levélét kézbesítse Bobnak. Ez az SMTP szerver először megkérdezi a saját DNS (Domain Name System) szerverét, hogy a b.org SMTP szerverét hol találja. Ezt a DNS szerverek adatbázisaiban az MX rekord

1. ábra: A levél útja a feladótól a címzettig [5]

tárolja. Egy domainnek (b.org) lehet több SMTP szervere is. A spammerek innen tudják kideríteni, hogy egy kiválasztott domainnek hol vannak az SMTP szerverei. Amikor megvan az MX rekordhoz tartozó cím, az smtp.a.org elküldi a levelet az mx.b.org-on levő SMTP szervernek. Ez a küldési folyamat egy párbeszéd a két szerver között. Ebből a párbeszédből a MAIL FROM mező és az RCPT TO mező az, ami most számunkra érdekes. Ezeket a mezőket általános esetben az Alice levelező programja adja meg a levél FROM és TO mezője alapján az smtp.a.org SMTP szerver számára. Abban az esetben, ha az smtp.a.org SMTP szervert valamint Alice levelező programját kihagyjuk a küldési folyamatból és közvetlenül az mx.b.org SMTP szervernek küldjük a levelet, akkor lehetőség van a MAIL FROM és az RCPT TO mezőt szabadon kitölteni. Ezzel a lehetőséggel akár teljes anonimitást szerezhethetünk, vagy - hamis értékkel feltöltve őket – akár más nevében is írhatunk levelet.

5. A spam elleni védelem helyei

A spamek küldését megnehezítheti a szolgáltató úgy, hogy az internetre kapcsolt otthoni számítógépeknek csak a szolgáltató saját SMTP szerverén keresztül lehet emailt küldeni, amihez csak helyes felhasználónév és jelszó megadása után kapcsolódhatunk. Ezt a tiltást a felhasználó kérésére a

felhasználó internet-szolgáltatója feloldhatja. A következő beavatkozási pont, amikor a két SMTP szerver párbeszédét figyeljük, és bármilyen gyanús kérdésre vagy válaszra valamilyen, de jól definiált módon és válaszüzenettel megszakítjuk a kapcsolatot a két szerver között. A harmadik lehetőség, amikor a megérkezett, de még át nem vett levél tartalmát elemezzük, és ezen információk alapján döntünk a levél további sorsáról és a feladó SMTP szervernek küldött válaszüzenet tartalmáról.

Elvileg email nem veszhet el. Sajnos a szűrési technikák és adott „csillagállások” miatt az emailek nagyon kis hányada mégis eltűnik az internet bugyaiban. Ezen adatvesztések elkerülése nagy odafigyelést, tapasztalatot és hozzáértést igényel.

6. Törvényi szabályozás

A spam által okozott problémákat már a törvényalkotók is felismerték, és számos országban született törvény a tömeges reklámkampányok szabályozására. Ezek a szabályok közel sem egyformák, hol szigorúbbak, hol megengedőbbek, de mindig tartalmazznak kibúvókat. Mindegyikben szinte közös jellemző, hogyha ismert a reklámküldő, és lehetőséget biztosít a kampányból való leiratkozásra, valamint a címzett beleegyezést ad adott cégnek a reklámcélú emailekre, a spamelés törvényesen megengedett tevékenységgé válik. [10]

Magyarországon a spamkérdést a 2001. évi CVIII. törvény szabályozza, melyet a 2005. évi CLXXI. törvény módosított. A törvény egy opt-in rendszert vezet be, mely azt jelenti, hogy elektronikus úton kizárólag a címzettnek előzetes és egyértelmű hozzájárulása esetén küldhető reklám. A 2007-ben elfogadott az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvény szerint az előzetes beleegyezést kérő email ugyancsak spamnek tekinthető [9].

Léteznek országok, ahol az opt-out rendszert használják, ami annyi tesz, hogy meg kell adni a címzettnek a lehetőséget, hogy leiratkozzon, és ezt a feladónak tiszteletben kell tartania [9, 10].

Irodalom

- [1] Michael Specter: Damn Spam, newyorker.com, 2007
- [2] C. Kanich, C. Kreibich és mások: Spamalytics: An Empirical Analysis of Spam Marketing Conversion, ACM, 2008
- [3] Wikipédia: Spam_(Monty_Python), en.wikipedia.org, 2008
- [4] Wikipédia: Spam, hu.wikipedia.org, 2008
- [5] Wikipédia: email, hu.wikipedia.org, 2008
- [6] Wikipédia: Internet bot, en.wikipedia.org, 2008
- [7] Trend Micro: Definition of Spam, mail-abuse.com, 2005
- [8] Dojcsák Dániel: Visszatérnek a spamek, hwsz.hu, 2008
- [9] Sütő János: Spamtelenül, Szak Kiadó, 2008
- [10] Spam laws, spamlaws.com/eu.shtml

Fried Zoltán, informatikus

Munkahely: Unicredit Leasing Kft.

Cím: Magyarország, 1016 Budapest, Hegyalja út 7-13.

E-mail: kolozsvar@deirf.hu