MOTIVACE A METODY ROZESÍLÁNÍ NEVYŽÁDANÉ ELEKTRONICKÉ POŠTY

Ing. Karel Šrámek
Univerzita Hradec Králové
Fakulta informatiky a managementu
karel.sramek@uhk.cz

ÚVOD

Nevyžádaná elektronická pošta se stala pojmem doby, parazitem, který infikoval mikrokosmos poštovních zpráv a celosvětově spotřebovává řadu zdrojů. Jedním z možných způsobů jak lépe porozumět odesílatelům pošty (a najít cestu jak proti nim uspět) je vidět jejich situaci z pozice motivace a metod v konfrontaci s jejich „podnikatelským záměrem“ resp. „obchodním modelem“.

MOTIVACE A METODY SPAMMERŮ

Rozesílání nevyžádané pošty není zábava ani ideologická válka, ale skutečný podnikatelský proces. Rozesílání nevyžádané pošty je komerční aktivita a stejně jako každé jiné podnikání má jediný cíl – vytváření zisku. Tato skutečnost je užitečná v procesu porozumění rychlého nárůstu a rozšíření nevyžádané pošty v e-mailových systémech, alespoň do té doby než poznáme jak protivník myslí a poznáme faktory vedoucí k vítězství v této válce.

Obchodní model odesílatelů musí obsahovat několik základních aktivit vedoucích k dosažení zisku:

1. Nalezení potenciálního zákazníka

Nelze vydělávat peníze bez zákazníků, kteří je chtějí utrácet. Pro rozesílatele nevyžádané pošty to znamená v prvním kroku získání seznamu e-mailových adres potenciálních zákazníků. Bohužel, z pohledu spammera, je potenciálním zákazníkem každý, kdo má e-mailovou adresu a sídlí na zeměkouli. Vzhledem k nízké distribuční ceně nevyžádané pošty není mezi spammery zájem o sofistikovanější tradiční direct marketingové kampaně a analýzy zamířené na cílovou skupinu. Vzhledem k zanedbatelné ceně distribuce spamu nemají spammeři žádný stimul odebírat kontakty ze seznamu adres a neuvažovat o všech emailových adresátech jako o potencionálních zákaznících.

2. Nabídka produktu nebo služby potenciálnímu zákazníkovi

Jakmile je potenciální zákazník nalezen, je mu nabídnut produkt nebo služby (nebo bohužel i podvod a hrozba odcizení identity, tzv. phishing) výměnou za platbu.

3. Uzavření obchodu

Cílem je prodat a dodat produkt nebo službu příjemcům kampaně. Jakmile byl ale spam rozeslán, pak odesílatel pouze čeká a sleduje jak se akumulují objednávky na základě odezvy jeho inzertní kampaně.

Úspěch spamu jako podnikání je založen na nízkých cenách za nalezení potenciálního zákazníka o oslovení ho produktem či službou.

NALEZENÍ POTENCIÁLNÍHO ZÁKAZNÍKA

Nalezení potenciálního zákazníka znamená pro spammera nalezení e-mailových adres, to lze udělat především dvěma způsoby:

1) nákupem adres

2) sběrem adres

Sběr adres je proces použití nástrojů a pomůcek k automatickému sběru e-mailových adres na Internetu.

Nákup adres

Pro nákup adres mluví především jeho jednoduchost, kdy je možné využít následujících variant:

Seznamy adres o nízké kvalitě

Nákup těchto adres je nabízen za v ceně pod 20USD za 1 milion adres. Adresy jsou prodávány na spammerských fórech i v legitimních internetových aukcích

Použité emailové adresy

Cena těchto adres se pohybuje okolo cca 150USD za 1000 adres nebo 150 000USD za 1 milion adres. Jedná se o kompilát adres použitých k jiným účelům jako byl například masivní marketing na velké již existující zákazníky telekomunikačních společností atp.

Adresy bývalých zákazníků

Spammeři často znovu užívají adresy zákazníků, kteří již zareagovali nebo dokonce nakoupili. Seznam těchto adres je ovšem výrazně menší než v předchozích dvou případech a také výrazně dražší.

Sběr adres

Pro sběr adres se používají nejčastěji nástroje a postupy označované jako spambot, directory harvesting attack, hoax, viry a trojské koně.

Do kategorie sběru adres patří i tzv. *phishing*. Je to hromadná distribuce zavádějících e-mailových zpráv se zpátečními adresami, odkazy a oficiálně se tvářícím označením, které vypadají, jako by přišly z bank, pojišťovacích agentur, maloobchodníků nebo společností, vydávajících kreditní karty.

Zprávy jsou vytvořené tak, aby zmátly příjemce, a ti vyzradili osobní údaje, jako jsou údaje o účtech, uživatelská hesla, hesla, čísla PIN kreditních karet, čísla sociálního zabezpečení atd. Udává se, že až 20% lidí věří, že tyto e-maily byly původně pravé. Předpokládá se, že 1% z nich skutečně poskytne své osobní údaje. Roste také problém s padělanými webovými stránkami, virovými útoky a hackery. Minulý rok bylo téměř 50 bank a poskytovatelů finančních služeb zasaženo odesílateli nevyžádaných e-mailů phishingu.

NABÍDKA PRODUKTU NEBO SLUŽBY

Proces nabídky prováděný spammery začíná odesláním zprávy na sestavený seznam e-mailových dres. Odesílatelé používají sofistikované programy, které pomáhají náhodně vytvářet záhlaví zprávy a informaci označující odesilatele, stejně tak jako vkládat do těla zpráv kódy pomáhající obcházet antispamová řešení.

Jiným způsobem, jak se spammeři snaží uspět při rozesílání zpráva je využití tzv. „botnetů“. Botnet je kompromitovaný stroj, na které běží trojský kůň tzv. „bot“, který se připojuje do Internet Relay Chat (IRC) provozovaných spammery.

Nízká cena umísťování nabídky dělá spam mnohem atraktivnější než jsou jiné „konkurenční“ přístupy jako je například reklama, telemarketing a direct mail.

Použití phishingu nejen udržuje velmi nízké náklady, ale současně přináší výrazný nárůst na straně zisku. Podvodné e-maily rozeslané na velké množství adres na první pohled vypadají jako informace z určité banky. Tyto e-maily plně využívají tzv. sociální inženýrství. Příjemce je informován o údajné nutnosti vyplnit údaje v připraveném formuláři, jinak mu může být zablokován účet, nebo jinak omezena možnost využití svých finančních prostředků. V e-mailu bývá uveden odkaz na připravené stránky s formulářem, které jakoby odkazovaly na server banky. Ve skutečnosti je uživatel přesměrován na cizí server, ale vytvořený ve stejném stylu, jako jsou stránky příslušné instituce. Chycený uživatel nepozná rozdíl a může vyplnit předvolená políčka, kde jsou po něm požadovány důvěrné informace.

UZAVŘENÍ OBCHODU

Spam je tak cenově efektivní, že i přes nízkou odezvu od příjemců, je odesílatel schopen realizovat významný profit. Ukazuje se, že spam je až 2800krát cenově výhodnější než standardní způsoby oslovování zákazníků (viz. Tabulka 1).

Způsob oslovení zákazníka	Celková cena [v USD]	Počet příjemců	Cena na příjemce
direct mail	9 700	7 000	1,39
telemarketing	160	240	0,66
tiskoviny cílené	7 500	100 000	0,075
tiskoviny necílené	30 000	442 000	0,067
fax	30	600	0,05
spam	250	500 000	0,0005

Tabulka 1

ŠKODLIVOST SPAMU

Nevyžádaná pošta snižuje produktivitu pracovníků, zahlcuje sítě i úložiště dat, může poškodit dobré jméno organizace a vést i k soudním žalobám. Nicméně v odvětvích, která nabízejí legální produkty a služby, a přitom používají technologii zneužívanou spamery, je problém daleko větší. Odborníci na informační technologie musejí zajistit, aby adresáti dostávali legitimní elektronickou poštu a mohli ji také odesílat, a to aniž by byli zaplaveni spamem.

Kromě využívaní standardních postupů, taktik a technologií se do popředí zájmu odborné veřejnosti dostává možnost prostřednictvím získávání nových informací stále zaujímat nová (modifikovaná) stanoviska oproti původním výchozím (apriorním) postojům. Tedy způsob

uvažování ve kterém je libovolný jev interpretován jako individuální postoj jednotlivce, jako stupeň důvěry v tento jev.

Nevyžádané e-maily, označované jako spam, se stávají stále větším problémem pro využití elektronické pošty a představují dle některých autorů až 80% obsahu všech poštovních schránek. Nevyžádané e-maily způsobují svou existencí i obsahem znehodnocování zdrojů, jak na straně poskytovatelů Internetu, tak na straně koncových uživatelů - ať jsou jimi domácí uživatelé nebo podnikové korporace.

Nevyžádané e-maily se různí nejen od uživatele k uživateli, ale jejich forma a obsah se mění s časem. Prostředky k boji proti nevyžádané poště musí být proto velmi jemně laděny (často manuálně) pro dosažení požadované účinnosti. Ladění těchto prostředků však vyžaduje znalosti a prostor, který nemusí být vždy k dispozici. Spolu s rostoucí kvalifikací spamerů a adaptabilitou nevyžádané pošty roste i nutnost nasazení poštovních filtrů, které jsou schopny učení se a přizpůsobování změnám.

Hranice mezi vyžádanou a nevyžádanou poštou je přinejmenším zastřená. Spam může mít mnoho vlastností jako legitimní pošta. Koneckonců vždy záleží na příjemci pošty, který musí rozhodnout zda se jedná o spam či nikoliv. V důsledku toho je rozdíl mezi nevyžádanou a legitimní poštou subjektivní. Identický mail může být tak dnes považován za nevyžádanou poštu, když ještě včera byl legitimním emailem. Nepříjemné, nevyžádané e-maily jednomu uživateli, mohou poskytovat druhému cenné informace.

Tato skutečnost s sebou nese pro firmy závažný problém v podobě vysokých výdajů navíc. Zaměstnanci, kteří jsou nuceni třídit svou poštu a mazat spam, totiž tvoří náklady, aniž by vykonávali jakoukoli produktivní činnost.

OCHRANA PROTI SPAMU

V boji proti spamu je používáno řady metod. Některé z nich jsou charakterizovány vysokou efektivitou, ale mnohé způsobují, že část neškodné pošty se nedostane k adresátovi.

Techniky používané k ochraně proti spamu lze rozdělit na tři funkční skupiny:

- MTA (Mail Transfer Agent), tj. agentem na straně serveru zodpovědným za předávání dopisů mezi servery,
- MDA (Mail Delivery Agent), tj. agentem na straně serveru zodpovědným za doručení zprávy,
- MUA (Mail User Agent), tj. agentem na straně klienta

Vážným aspektem praktického nasazení poštovních filtrů je jejich použitelnost, resp. poměr ceny/výkonu.

ZÁVĚR

Stejně tak, jako anti-spamová komunita pracuje na omezení zisku plynoucího ze zneužívání elektronické pošty, tak i se spammeři agresivně snaží dosáhnout mety profitability z jejich činností. V práci byly naznačeny aktuální trendy, kterým spamměři věnují pozornost, přesto je stále je nutné diskutovat ochranu proti:

- nárůstu množství spamu
- obcházení poštovních filtrů
- směřování podvodným e-mailům

Tlak technologie a legislativy je protiváhou proti spammerským aktivitám. Nehledě na úsilí, které je tomuto věnováno. Tak spammeři neváhají vyhledávat stále nové rafinovanější způsoby jejich práce.

POUŽITÁ LITERATURA :

[1] JUDGE, Paul, ALPEROVITCH, Dimitri, YANG, Weilai. Understanding and Reversing the Profit Model of Spam [online]. Dostupný z <http://citeseer.ist.psu.edu/748505.html>