Obrázkový spam - historie a budoucnost

Vložil/a MaxCerny [1], 26 Březen, 2007 - 20:53

- Security [2]
- Spam [3]
- Virus & Worms [4]

Obrázkový spam - nevyžádaná zpráva, která zpravidla obsahuje své sdělení vložené v obrázku, není nic nového. Spammeři tuto techniku začali využívat již před deseti lety. Stejně jako se zkvalitňovali antispamové systémy, snažili se i spammeři více a více znemožňovat detekci jejich spamů.

V posledních šesti měsících byl zaznamenán značný nárůst obrázkových spamů. Podle posledních analýz je tohoto druhu nejméně 30 % veškeré nevyžádané pošty.

1997 První generace obrázkového spamu

Kolem roku 1997, kdy antispamovou ochranu nabízelo jen několik společností a spam byl ještě na počátku svého šíření, spammeři přišli na snadný způsob, jak zjistit, zda emailové adresy, které mají v databázích, skutečně někdo vlastní nebo jestli pošta jimi poslaná končí v propadlišti dějin. Jednoduše do emailu vložili odkaz na obrázek v internetu. Pokud si uživatel email otevřel a obrázek se automaticky načetl, mohl spammer poznat, zda je adresa aktivní či nikoli. V reakci na tento spam již emailový klienti automaticky nestahují obrázky z internetu.

2003 Druhá generace: Spamová zpráva v obrázku

S rozšířením antispamových filtrů, které byly schopny analýzou textu odhadnout, zda je text spam či ne, hledali spammeři nový způsob, jak dostat své zprávy přes čím dál více početně zastoupené spamfiltery. Svá sdělení proto začali psát do obrázků. Protože ale počet rozesílaných spamů ku počtu příjemců příliš velký, spammeři rozesílali pokaždé stejný obrázek. Časem si proto antispamové filtry vytvořili databázi otisků obrázkového spamu a bylo poměrně snadné takové zprávy blokovat.

2005 Různé variace obrázkového spamu

Jsou tomu dva roky, kdy tehdejší obrázkový spam byl z velké většiny rozpoznán a blokován pomocí databáze otisků. Logicky se proto spammeři snažili, aby jejich obrázky neměly stejný otisk. Proto různě měnili styly písma, velikosti, okraje, barvy... Zde již databáze otisků sloužit nemohla, narostla by totiž do obrovských rozměrů. Hledal se tedy nový způsob, jak obrázkový spam blokovat.
Začala se využívat technologie OCR (Optical Character Recognition - optické rozpoznávání znaků), do té doby známá především z oblasti archivace různých dokumentů do PC.
Protože bylo náročné rozeznávat text z obrázku a zprvu neexistoval žádný antispamový software, který by tuto analýzu mohl provádět, byli spammeři poprvé o krok před námi.

2006 Animovaný spam

Když OCR technologie slavila v boji proti spamu první úspěchy, spammeři nelenili a své zprávy stále více před filtry maskovali. Během minulého roku se nejvíce šířily spamy s animovanými GIF obrázky. Tak mohla animace začínat bílým pruhem, který však trval jen několik milisekund - lidské oko takové probliky ani nezachytí. Následně se bílý pruh změnil na reklamu na Viagru, která ale uživateli na monitoru zůstala již delší dobu.

2007 Unikátní spamy generované botnety

Poslední novinkou je šíření spamu přes tzv. botnety - virem infikované počítače nic netušících uživatelů Internetu. Po infikování pomocí algoritmu vytvoří zcela unikátní obrázek, který má nadefinovanou velikost, písmo, okraje a další vlastnosti. Současně se text spammerů předsune před generované pozadí obrázku, kde jsou různé linky a textury. To má za úkol ztížit rozpoznání textu.

V dnešní době se setkáváme se stále sofistikovanějším spamem. Dnes již nejde jednoduše odlišit spamovou zprávu od té legitimní. Je pravda, že se antispamové filtry také zdokonalují, a to velmi rychlým tempem. Bohužel jsou to však spammeři, kteří budou vždy o krok před námi vymýšlet nové triky a postupy, jak nám zaplnit emailové schránky svými reklamami.

MaxCerny
http://www.spamy.cz [5]

URL článku: https://security-portal.cz/clanky/obr%C3%A1zkov%C3%BD-spam-historie-budoucnost

Odkazy:
[1] https://security-portal.cz/users/maxcerny
[2] https://security-portal.cz/category/tagy/security
[3] https://security-portal.cz/category/tagy/spam
[4] https://security-portal.cz/category/tagy/virus-worms
[5] http://www.spamy.cz