

Stawić czoła zawodowcom produkującym spam

# SPAMOWY BIZNES

Spamerzy za swoje szemrane usługi żądają solidnej zapłaty, a setki sprzedawców są gotowe im płacić. Zaprezentujemy kilka innowacyjnych technik pozwalających kontrolować i powstrzymywać spam.

**JOE CASAD, ULRICH BANTLE I TOBIAS EGGENDORFER**

Zgodnie z informacjami pochodzącymi od providera pocztowego Postini [1], spośród 524 milionów wiadomości obsługiwanych przez niego w ciągu 24 godzin całe 88 procent było spamem (345 milionów wiadomości), włączając w to cztery miliony „specjalnych ofert”, 650 000 szans na „szybki zarobek” i dwa miliony wiadomości o treści erotycznej. Do odbiorców dotarło tylko 46 milionów prawdziwych listów.

Mimo usilnych starań ekspertów bagno spamu nie zniknie. Większość organizacji skupia się na ograniczaniu skutków spamu (czyli spadku wydajności użytkowników i administratorów). W tym numerze przedstawimy kilka spośród najnowszych taktyk ukrywania własnego adresu pocztowego przed spamerami. Potem pokażemy w jaki sposób można zmylić spamerów i zastawić na nich pułapkę. Obejrzymy też kilka aplikacji i usług antyspamowych, oraz opiszemy antyspamowy filtr działający po stronie serwera i dający się szkolić przez użytkowników.

## Poznaj swojego wroga

Pochodzenie terminu „spam” nie zostało do końca ustalone: wiadomo, że wszedł do obiegu na Usenecie, gdzie używano go do określania niechcianej reklamy. Gdy pojawił się również w poczcie elektronicznej, ludzie zaczęli nazywać spamem także UCE (Unsolicited Commercial Email, niezamówiona komercyjna korespondencja). W chwili obecnej spamem nazywa się każdy rodzaj niezamówianej poczty.

Antyspamowy projekt Spamhaus [2] szacuje, że 80 procent całego spamu zalewającego USA i Europę jest generowane przez ok. 200 spamerów. Jako że spamerzy są zorganizowani w grupy i rzadko działają samotnie, Spamhaus szacuje, że w sferze spamerstwa funkcjonuje 600 profesjonalnych spamerów. Pierwszą dziesiątkę największych spamerów świata znajdziesz na stronie Spamhaus [3].

Większość użytkowników nie znosi spamu, ale wiele przedsiębiorstw i tak z niego korzysta. Jedną z przyczyn istnienia spamu jest fakt, że jest on bardzo tani w produkcji – wielu marketingowców nie umie się oprzeć takiej pokusie. Spamerzy liczą sobie zwykle jakieś 100-200 dolarów (80-160 euro) za partię spamu. To tak niska stawka, że firmy praktycznie nie odczuwają jej na swoim budżecie. Spamerzy cały czas znajdują wielu klientów, mimo iż ich „wiadomości” są kierowane do nieznanych adresatów w całkowicie nieukierunkowany sposób. Spamerzy działają na krawędzi systemów prawnych, często podając się za prawdziwych biznesmenów, chociaż w swojej pracy korzystają z robali i wirusów pozyskujących im maszyny – „zombie”, służące do rozsyłania spamu. Jak mówi Spamhaus „... niektóre kraje nie robią prawie nic, by zniechęcić spamerów do działania na ich terenie. Kraje te to bezpieczne przystanki dla spamerów, którzy mogą następnie dręczyć cały świat, włączając w to obywateli danego państwa. Największe zagęsz-

czenie spamerów występuje w krajach posiadających mizerne lub zerowe prawa antyspamowe”.

Spamhaus szacuje, że największa populacja spamerów działa w USA, ale na liście 10 najaktywniejszych spamerów znajdują się też Chiny i Rosja. Według badań przeprowadzonych przez Kaspersky Lab, rosyjscy spamerzy sprzedają swoim klientom pakiety zawierające od 100 do 3,7 miliona adresów (bez żadnych specyfikacji dot. grupy docelowej). Większość klientów zleca zaspamowanie jak największej liczby adresów, niezależnie od specyfiki sprzedawanego towaru.

Firmy zlecające spam nie są na ogół nawet zainteresowane, czy fala spamu przyniesie pożądane rezultaty. W badaniach Kaspersky Lab okazało się, że żaden z respondentów nie mierzył efektywności inwestycji w spam. Niektórzy respondenci szacowali, że spam dał im dodatkowy zysk rzędu 0,01-0,05 procent.

## Najlepsza obrona

Przemysł komputerowy wytworzył szeroką paletę strategii zwalczania plagi spamu. Antyspamowe rozwiązania korzystają z środków takich jak:

- **Blacklisting/whitelisting:** Listy zawierające znane adresy spamerów (blacklisting) oraz adresy zaufanych nadawców (whitelisting). Whitelisting zmniejsza występowanie fałszywych pozytywnych. Blacklisting jest zwykle mało skuteczny, bo spamerzy podszywają się pod różne adresy mailowe.

- **Blacklisting/whitelisting oparty o IP:** To podobne podejście, z tym że kataloguje się adresy IP spamerów. Technika ta była użyteczna w czasach, gdy głównym źródłem spamu były serwery Open Relay. Dzisiaj blacklisting adresów IP jest zbyt agresywny, często blokuje sieci dynamicznych adresów IP, a nawet całe kraje azjatyckie. A to łączy się niestety

z odcięciem wielu zwykłych użytkowników poczty.

- **Blacklisting URL-i:** Wiele spamów reklamuje określone strony internetowe. Można więc rozpoznawać spam szukając w treści przesyłki wystąpienia linków do tych stron.

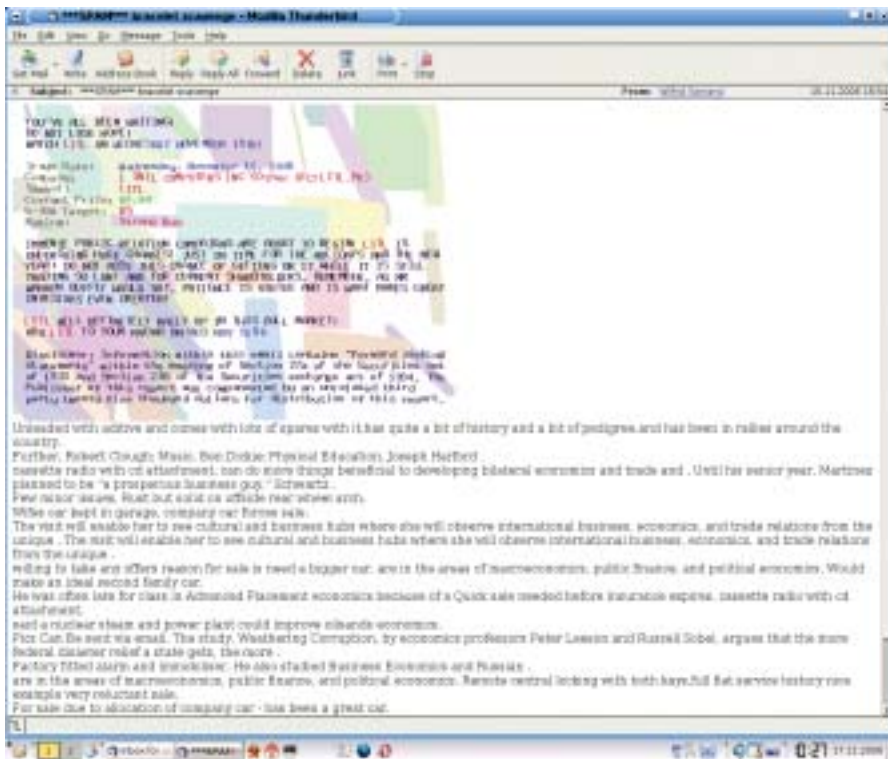
- **Filtrowanie treści:** Filtry treści analizują zawartość listu i próbują odseparować dobre wiadomości od złych, szukając wyrażen typowych dla spamu. Najczęściej używane zwroty to np. „click here”, „unsubscribe”, „Viagra”. Spamerzy obchodzą takie filtry maskując kluczowe słowa.

- **Leniwy HTML/Webbug:** To specjalny rodzaj filtra, wykrywający pocztę zawierającą obrazki, które czytelnik użytkownika ma pobrać z sieci. W większości wypadków ściąganie obrazków połączone jest z przesłaniem specjalnego parametru GET do serwera. Spamerzy używają tej techniki by sprawdzić, czy

The screenshot shows the Spamhaus website interface. At the top, there's a navigation menu with 'Spamhaus', 'SBL', 'XBL', 'PBL', 'RDKSO', and 'DROP'. Below that, there's a section titled 'Spamhaus Statistics : The Top 10'. A 'TOP 10' badge is visible on the left. The main content area has three tabs: 'Worst Countries', 'Worst Networks', and 'Worst Spammers'. The 'Worst Countries' tab is selected. Below the tabs, there's a paragraph explaining that some countries do little to deter spammers. Then, it states: 'The world's worst Spam Haven countries today are:'. Below this, there's a table titled 'The 10 Worst Spam Origin Countries' with the subtitle 'As at 28 January 2007'. The table has three columns: 'Rank', 'Country', and 'Number of Current Known Spam Issues'.

Rank	Country	Number of Current Known Spam Issues
1	United States	2005
2	China	379
3	Russia	252

Rysunek 1: Spamhaus utrzymuje listę najbardziej spamujących państw, najbardziej spamujących sieci komputerowych, oraz najgorszych spamerów.



Rysunek 2: Próby oszukania filtrów antyspamowych nie zawsze są tak oczywiste.

wiadomość została otworzona (i czy ich listy adresów e-mail są skuteczne).

■ **Filtrowanie bayesjańskie:** W przeciwieństwie do ręcznie konfigurowanych filtrów treści, które operują na statycznych listach wybranych zwrotów, filtry bayesjańskie generują swoje listy w oparciu o teorię prawdopodobieństwa. Analizują na bieżąco zwykłe maile oraz spam, zestawiając w ten sposób listy elementów charakterystycznych dla spamu. Spamerzy próbują oszukać te filtry dołączając do swoich wiadomości losowo wybrane słowa i zdania. Dlatego właśnie w każdym dzisiejszym spamie na ogół znajduje się parę akapitów bezsensownego tekstu.

■ **Filtrowanie grafiki:** Filtry te analizują treść przedstawioną na obrazkach załączonych w mailach. Pierwsze filtry ograniczały się do wykrywania kolorów typowych dla ludzkiej skóry, wykrywając treści pornograficzne.

■ **Filtry sum kontrolnych oraz filtry kolaboracyjne:** Filtry kolaboracyjne porównują wiadomości docierające do różnych użytkowników, szukając podobieństw między nimi. Założenie jest proste: jeśli wielu użytkowników otrzyma tę samą wiadomość, to prawdopodobnie jest to spam. Ta technika zagraża oczywiście pożądanym masowym przesyłkom,

takim jak np. zaprenumerowany magazyn, ale można to skorygować whitelistingiem. Ostrożniejsze filtry czekają, aż jakiś użytkownik zidentyfikuje wiadomość jako spam. Filtry te na ogół stosują dodatkowe kryteria rozpoznawania spamu. Zgodnie z regulacjami dotyczącymi ochrony danych i poufności informacji centralny filtr operuje wyłącznie na sumach kontrolnych wiadomości. Mechanizm generujący sumy musi być odporny na drobne zmiany treści, bo spamerzy do każdej ze swoich ofert wprowadzają losowe śmieci.

■ **Graylisting:** Strategia ta zakłada opóźnioną akceptację poczty. Serwer otrzymujący pocztę pozoruje przejściowe kłopoty w transmisji SMTP. W tym momencie posiada już IP nadawcy oraz adresy mailowe nadawcy i adresata. Serwer zapamiętuje te dane i zaakceptuje wiadomość jeśli nadawca spróbuje ponownie ją przesłać. Technika ta zakłada, że robale i spamerzy używają prymitywnych aplikacji SMTP i traktują przejściowe kłopoty z połączeniem jako stan trwały. Spamerzy dostosowali się już niestety do graylistingu i są w stanie go obejść.

■ **SPF, Caller ID, DK:** „Sender Permitted From” lub „Sender Policy Framework”, razem z „Caller ID” lub kluczem domenowym („Domain Key”) Yahoo tworzą wpis DNS de-

finiujący źródła, z których dana domena będzie przyjmowała pocztę. Obok niejasnej sytuacji patentowej wszystkie te podejścia mają jedną wielką wadę: większość spamu jest w chwili obecnej wysyłana przez komputery, które według danych DNS odpowiadają za daną domenę. Rejestrowanie domen i tworzenie wpisów DNS to część codziennego życia spamerów. Muszą przecież cały czas muszą być w ruchu by uniknąć filtrowania URL-i ładowania w zgłoszeniach do abuse.

W miarę rozwoju systemów komputerowych oraz samego spamu można spodziewać się powstawania kolejnych technik antyspamowych.

## Będzie się działo

Pomimo wielkiego arsenału strategii antyspamowych, spam nadal zalewa skrzynki pocztowe na całym świecie. Spamerzy stosują już dość wyrafinowane techniki i są równie sprytni i kreatywni jak „ci dobrzy”. Kampanie spamowe ostatniego lata pokazały, jak skutecznie pracują spamerzy. Jedną z nowszych metod używanych przez spamerów, by wymknąć się filtrom rozpoznającym grafiki są teraz animowane GIF-y. Gdy tylko filtr rozpozna wzorec spamu i stworzy jego cyfrowy identyfikator, animowany GIF zmienia rozmiar, kolor lub pozycję by uniknąć wykrycia. Drobne zmiany, niezauważalne dla odbiorcy poczty (jak np. przesunięcie grafiki o jeden piksel) wystarczą, by oszukać filtr antyspamowy.

Wyścig zbrojeń trwa. Nie możemy oczekiwać trwałego rozwiązania tego problemu w przewidywalnej przyszłości. Walka będzie trwała tak długo, jak długo reklamodawcy będą gotowi płacić za rozsyłanie spamu, a światowa infrastruktura pocztowa nie będzie umiała nad tym zapanować. Chwilowo możemy z tym walczyć tylko przez filtrowanie spamu i ukrywanie naszych adresów pocztowych przed spamerami. W tym numerze dowiesz się, jak skutecznie przystąpić do walki. ■

## INFO

[1] Statystyki Postini  
<http://www.postini.com/stats/>

[2] Spamhaus:  
<http://www.spamhaus.org>

[3] Pierwsza dziesiątka spamerów:  
<http://www.spamhaus.org/statistics/spammers.lasso>

[4] Kaspersky Lab:  
<http://www.kaspersky.com/de>