REFERAT Z BEZPIECZEŃSTWA SYSTEMÓW KOMPUTEROWYCH

TEMAT:

# Spam – uciążliwość czy zagrożenie

OPRACOWAŁA:

Karolina Zarawska, rok 3.

# SPIS TREŚCI:

# *1. Wstęp.*

## *1.1. Geneza słowa SPAM.*


W 1937 roku Jay C. Hormel wyprodukował pierwsze puszkowane mięso niewymagające przechowywania w lodówce. Mielonka z szynki ("chopped pork shoulder and ham mixture") nazwana została „pikantną szynką Hormel'a" („Hormel Spiced Ham"), jednak nazwa ta nie przyciągała uwagi konsumentów, przez co produkt Hormel'a szybko został wyparty z rynku przez puszkowaną żywność produkowaną przez konkurencję. Ostatnią deską ratunku dla szynki Hormel'a była zmiana nazwy produktu na bardziej „uchwytną i przyciągającą". Ogłoszony konkurs wygrała nazwa „SPAM" (prawdopodobnie od „**S**houlder **P**ork **a**nd h**AM**" lub „**SP**iced h**AM**") i tak zaczęła się historia SPAM'u.

Puszkowana szynka Hormel'a zyskała popularność, szczególnie w czasie II Wojny Światowej. Więcej na temat historii i rozwoju popularności mielonki SPAM można przeczytać na: http://www.cusd.claremont.edu/~mrosenbl/spamstory.html lub na stronie domowej: http://www.spam.com/ w zakładce „SPAM in time".

Nową sławę wyrażeniu SPAM przyniósł skecz Latającego Cyrku Monty Python'a o tym samym tytule. Klient przychodzi do restauracji i pytając się o menu dowiaduje się, że w każdym daniu jest SPAM. (np. „Spam, egg, spam, spam, bacon and spam" ). Pełny tekst skeczu dostępny jest na: http://www.noteboom.demon.nl/spam.html, a sam skecz można ściągnąć m.in. z http://linux.gda.pl/pub/spam/.

Inne teorie na temat, co może oznaczać słowo „SPAM" można także znaleźć na: http://www.cusd.claremont.edu/~mrosenbl/spamtheory.html.

## *1.2. Spam w żargonie internetowym.*

Mianem spamu określa się w żargonie internetowym niechcianą korespondencję. Przyjmuje się, że spamem można nazwać wiadomość elektroniczną, gdy:

- jej treść nie jest zależna od tożsamości odbiorcy, ponieważ jest wysyłana do wielu różnych odbiorców na raz;
- adresat nie wyraził uprzednio świadomej, jednoznacznej zgody na jej otrzymywanie;
- zawarte w niej informacje dają podstawę do przypuszczeń, że nadawca może odnieść korzyści nieproporcjonalne do korzyści odbiorcy wynikających z jej odebrania.

(Szersze wyjaśnienie definicji spamu można znaleźć m.in. w Wikipedii: http://pl.wikipedia.org/wiki/Spam.)

Brad Templeton w swoim artykule „Origin of the term "spam" to mean net abuse" (http://www.templetons.com/brad/spamterm.html) podaje, że najprawdopodobniej nazwę dla niechcianej, masowej korespondencji zaczerpnięto ze skeczu Monty Pyton'a, ponieważ tam Wikingowie (również obecni w restauracji) co chwilę zaczynają śpiewać „Spam, spam, spam, spam, spam, spam, spam, spam, lovely spam! Wonderful spam!" dopóki kelnerka nie krzyknie, żeby się uspokoili. Odtąd termin „spam" przyjął nowe znaczenie: jako coś niechcianego, a uporczywie powtarzanego, aż do wywołania poirytowania w odbiorcach.

Przyjęło się, że „SPAM" pisany drukowanymi literami oznacza nazwę szynki Hormel'a – jest zarejestrowanym w ponad 100 krajach świata znakiem handlowym, natomiast pisany małymi literami „spam" – używany jest do określenia niechcianej korespondencji.

## *1.3. Historia spamu.*

**1 maja 1978 Einar Stefferud** wysyła poprzez sieć Arpanet około 1000 zaproszeń na swoje urodziny, otrzymując w odpowiedzi wiele zabawnych jak również i złośliwych wiadomości, których ilość blokuje dyski twarde na serwerze pierwszego spamera.

**1 maja 1978 Gary Thuerk** pisze, a **3 maja** wysyła reklamę mini-komputerów firmy Digital Equipment Corporation, zapraszającą wszystkich użytkowników Arpanetu z Zachodniego Wybrzeża USA na "dzień otwarty" w celu zaprezentowania najnowszych produktów firmy. Program, którego używał do edycji i wysyłania wiadomości po pierwsze wymagał, aby każdy adres odbiorcy został wpisany „ręcznie"- stąd tak długi czas edycji wiadomości, a po drugie pozwalał jedynie na 320 wpisów w polu „odbiorcy". Gary, będąc przedstawicielem firmy działającej na Wschodnim Wybrzeżu, postanowił przy pomocy Arpanetu rozpropagować jej produkty również na Zachodnim Wybrzeżu. W tym celu zdobył adresy użytkowników Arpanetu z Zachodniego Wybrzeża, jednak było ich więcej niż 320 i część z nich przeszła do treści wiadomości, w związku z czym duża liczba osób, które powinny były otrzymać tę wiadomość, jej nie otrzymała. Gary ponowił wysłanie wiadomości, co spowodowało, że niektórzy użytkownicy otrzymali ją kilkakrotnie, co np. u pewnego użytkownika z Uniwersytetu w Utah spowodowało wyłączenie systemu operacyjnego w komputerze. Więcej o tym wydarzeniu, reakcji odbiorców, jak i samą treść „pierwszego spamu" można znaleźć na:
http://www.templetons.com/brad/spamreact.html.

**Późne lata 80'te:** gracze MUD-ów (Multi-user-dungeon) zaczynają używać terminu „spamming" w stosunku do działania niektórych użytkowników, którzy zamiast brać udział w grze: wysyłają dużą ilość bezsensownych komunikatów tylko po to by zablokować serwer lub „spamują bazę danych" przez uruchomienie programu zapełniającego ją dużą ilością wyprodukowanych przez siebie danych.

**31 marca 1993 Richard Depew** próbuje unowocześnić Usenet wprowadzając „moderowanie grup dyskusyjnych" używając programu o nazwie ARMM. Niestety oprogramowanie to zawiera błąd i zamiast wykonywać zamierzone przez Richarda zadania – wysyła 200 wiadomości do użytkowników grupy dyskusyjnej dotyczącej działania sieci (przykład tutaj:
http://groups.google.com/group/news.admin.policy/msg/72ad06e4c0b518?output=gplain). W odpowiedzi Joel Furr pierwszy raz „niechcianą masową korespondencję" nazywa terminem „spamu".

**Kwiecień 1994 Lawrence Canter i Martha Siegel,** dwaj prawnicy z firmy Phoenix wysyłają drogą elektroniczną ofertę swojej pomocy w zdobyciu zielonej karty. Nie było by w tym nic nadzwyczajnego, gdyż robili to już kilkakrotnie, jednak 12 kwietnia tegoż roku zatrudniają programistę, aby napisał im skrypt rozsyłający ich wiadomość do wszystkich użytkowników grup dyskusyjnych Usenetu. Było kilka tysięcy takich grup i każda otrzymała ich reklamę. Działanie Canter'a i Siegel szybko zostało odczytane jako „spam" i nazwa zyskała na dobre popularność w „cyber świecie".

Więcej szczegółów można znaleźć w artykule „Origin of the term "spam" to mean net abuse" (http://www.templetons.com/brad/spamterm.html).

# 2. Typy spamu.

## 2.1. UCE i UBE.

Wikipedia dzieli „masowe e-maile" na dwie kategorie:

- **spam komercyjny** (Unsolicited Commercial Email UCE) – wiadomości o charakterze reklamowym. Jest on zakazany tak przez prawo polskie, jak i dyrektywę Unii Europejskiej. (Polskie regulacje prawne mające związek ze spamem: http://nospam-pl.net/prawo.php ).

- **spam o charakterze niekomercyjnym** (Unsolicited Bulk Email UBE) – wiadomości będące apelami organizacji społecznych i charytatywnych lub partii politycznych, wiadomości zawierające prośby o pomoc, masowo rozsyłane ostrzeżenia np. o wirusach komputerowych, itp. „Próby wprowadzenia zakazu w dyrektywie UE rozsyłania e-maili o charakterze społeczno-politycznym zostały w 2002 r. odrzucone przez Parlament Europejski wobec protestów europejskich partii politycznych i organizacji społecznych." podaje Wikipedia. (http://pl.wikipedia.org/wiki/Spam).

## 2.2. Rozróżnienie ze względu na medium.

Ze względu na medium, za pośrednictwem którego jest propagowany, spam posiada kilka odmian:

- **e-mail spam –** najczęstsza form spamu;

- **spim –** odmiana spamu wysyłana za pomocą komunikatorów internetowych (nazwa pochodzi od **sp**am + **i**nstant **m**essaging);

- **spit –** spam rozsyłany poprzez pocztę głosową telefonii internetowej (nazwa od **sp**am over **i**nternet **t**elephony);

- **splog –** blog wykorzystywany do spamowania wyszukiwarek internetowych (nazwa od **sp**am b**log**);

- **mobile – phone spam** (czy też spam mobilny, m-spam) – spam rozsyłany na telefony komórkowe poprzez krótkie wiadomości tekstowe (SMS). Może być szczególnie irytujący, gdy za odebranie SMS'a musimy zapłacić (np. będąc za granicą);

- **forum spam** (spamowanie grup dyskusyjnych) – spamem na forach dyskusyjnych nazywane są posty niezwiązane z bieżącym tematem, często wysyłane tylko po to, aby nabić sobie tzw. „licznik postów" i podwyższyć swój ranking na forum jako osoba wyjątkowo aktywna (choć rzadko mająca coś istotnego do powiedzenia...).

## *2.3.Rozróżnienie ze względu na treść i sposób „działania".*

### *2.3.1. Hoax.*

Hoax dosłownie oznacza oszustwo, mistyfikację, fałszywy alarm lub głupi kawał. W żargonie mianem „hoax" określa się wiadomość elektroniczną o treści zawierającej ostrzeżenie o wystąpieniu wirusa, prośbę o pomoc, tzw. „łańcuszki szczęścia" itp., oraz dodatkową prośbę o rozesłanie tej wiadomości do jak największej liczby znajomych lub (w przypadku „łańcuszków szczęścia") do pewnej ustalonej N liczby znajomych, aby to, co pisane w e-mailu się spełniło.

W przypadku ostrzeżeń o wirusie bardzo często autor powołuje się na znane firmy (typu Symantec, czy McAfree). Łatwo jest wykryć oszusta, gdyż:

- firmy produkujące oprogramowanie antywirusowe umożliwiając wpisanie się na listę odbiorców informacji o nowych wirusach NIGDY nie proszą o przesłanie tej informacji dalej („do wszystkich ze swojej książki adresowej", itp.) ;

- oszust nigdy nie zamieszcza szczegółów dotyczących działania wirusa. Jedynie pisze np., że „cała jego książka adresowa została zarażona"- są to szczegóły pseudo techniczne, nigdy nie opisujące istoty działania tego wirusa, np. pod jakim programem do odbioru poczty on się uaktywnia i pod jakim systemem operacyjnym;

- w takiej wiadomości dużo jest wykrzykników i środków stylistycznych powodujących napięcie czy strach w czytającym, typu „po otwarciu załącznika stała się masakra! Wirus sformatował wszystkie dyski twarde!";

- listę znanych wirusów można łatwo sprawdzić na stronie np. http://www.mks.com.pl/ .

W przypadku treści oferującej szybki przypływ gotówki, szczęścia, spełnienie marzeń, czy reklamującej jakąś super okazyjną ofertę trzeba pamiętać, że nic nie ma za darmo. Po kilkukrotnym przeczytaniu treści wiadomości „na spokojnie" łatwo rozpoznać naiwność zawartej w niej propozycji/ obietnicy.

Podobnie do „hoax" działają tzw. „dowcipy biurowe" czyli mniej lub bardziej śmieszne listy przesyłane do „wszystkich znajomych".

Dlaczego „hoax" jest groźny?

- wysyłane w dużych ilościach (ich ilość rośnie wykładniczo przy przejściu na kolejny poziom odbiorców- nadawców) – niepotrzebnie blokują sieć;

- nie są wykrywane przez skaner antywirusowy, utrudniając rozpoznanie prawdziwych ostrzeżeń od osób, które np. dotknął dany wirus;

- większość osób przesyłając dalej taką wiadomość nie usuwa e-maili poprzednich nadawców, przez co po pewnym czasie taka „gotowa baza

adresowa" trafia z powrotem do nadawcy. Ten przy kolejnym ataku może zaspamować już o wiele większą rzeszę użytkowników;

- przesyłając taką wiadomość dalej często uzupełnia się listę odbiorców w polu „To" („Do") przez co każdy z odbiorców widzi adresy pozostałych. Niektóre osoby mogą sobie nie życzyć, aby w ten sposób rozpowszechniać ich adres e-mail. Do książek adresowych osób, które się kompletnie nie znają mogą się dostać ich wzajemne adresy, a co za tym idzie, jeżeli komputer którejś z nich zostanie zainfekowany przez wirusa, który sczyta wszystkie adresy z książki adresowej i roześle się „wszystkim znajomym" ta druga osoba jest niepotrzebnie narażona na niebezpieczeństwo.

Jak radzić sobie z „hoax"? Najlepiej nie odpowiadać na takie maile. A jeżeli nas rzeczywiście zaniepokoi ostrzeżenie o wirusie można zawsze sprawdzić dane na jego temat na witrynie mks_viru: http://www.mks.com.pl/ lub na stronie „Hoax page" firmy Symantec http://www.symantec.com/avcenter/hoax.html.

Więcej informacji na temat „hoax'u" można znaleźć m.in. na:

- http://hoaxbusters.ciac.org/;
- http://www.nonprofit.net/hoax/default.htm;
- http://ceti.pl/gralinski/.

### *2.3.2. Reklama.*

Reklama za pośrednictwem poczty elektronicznej jest niejawną formą kradzieży, gdyż ktoś, kto reklamuje swoje usługi – na tym zarabia, ale niczego nie świadomy odbiorca ściągając niechciana reklamę wraz z całą inną swoja pocztą – musi za to zapłacić(impulsy).

### *2.3.3. Nigeryjski szwindel*

Mechanizm tego typu oszustwa jest starszy od Internetu. Polega on na wysyłaniu listu, który w swojej „formalnej" treści zawiera prośbę o pomoc w np. „przechowaniu nielegalnych pieniędzy", czy coś podobnego, z załączoną informacją o wynagrodzeniu za dokonana przysługę. Wynagrodzenie jest oczywiście bardzo wysokie. Na rzecz przyszłego zarobku, odbiorca jest proszony o udzielenie małej pożyczki, czy o opłacenie pewnej usługi, której koszt jest nieporównywalnie mały w porównaniu z sumą obiecywaną za dokonanie tej przysługi. Osoba wysyłająca taką korespondencję zazwyczaj podaje się za kogoś w rodzaju wysokiego urzędnika jednego z państw w Afryce.

Oszustwo to po raz pierwszy pojawiło się w Internecie pod koniec lat 80-tych. Jest ono znane pod kilkoma nazwami, m.in.

- „419" – numer paragrafu Nigeryjskiego Kodeksu Karnego dotyczącego tego rodzaju wyłudzeń;
- Nigeria Scam , czyli Nigeryjski szwindel,
- Adwanced Fee Fraud – oszustwo z kosztami wstępnymi,
- The Nigeria Connection – Nigeryjski łącznik.

Działanie oszustów (bez względu na szczegóły treści wiadomości) jest zawsze takie same – przedstawiając swoją ofertę w jak najlepszym świetle, oferując wysoki zarobek za pomoc w nie do końca legalnych przedsięwzięciach zachęcają odbiorcę do współpracy, po czym na rzecz pokrycia coraz to wyższych, acz nieoczekiwanych, dodatkowych kosztów – wyciągają od ofiary duże sumy pieniędzy. Często oszuści tworzą strony www, podające się za strony rządowe, czy też jakiegoś banku w Afryce, gdzie ofiara może sprawdzić ich autentyczność lub po uprzednim zalogowaniu, że obiecane jej pieniądze już są na koncie.

Najlepszą radą na tego typu oszustów jest po prostu nie wierzenie w możliwość szybkiego zarobku tak niebotycznych sum, za działalność, o która proszą i nie odpowiadanie na ich maile.

Więcej na ten temat można przeczytać na: http://home.rica.net/alphae/419coal/.
O mechanizmach ochrony i walki z takimi oszustami:
http://www.419fraud.com/.
Przykłady tego typu korespondencji na: http://www.geocities.com/a_kerenx/.

### *2.3.4. Joe –Job.*

Joe –Job, czyli podszywanie się pod nadawcę, wzięło swą nazwę od Joe'go Doll'a, właściciela serwisu Joe's CyberPost. Witryna działająca od 1994 roku oferowała darmowe konta na strony WWW, jednak aby móc skorzystać z tej usługi trzeba było sprostać rygorystycznym wymaganiom zawartym w regulaminie. W 1996 roku jeden z użytkowników zaczął reklamować swoją witrynę za pomocą spamu, za co jego konto zostało zamknięte. Wkrótce po tym rozpoczęła się lawina spamu o różnorakiej treści zalewającego różnorodnych odbiorców, będącego rzekomo autorstwa Joe'go Doll'a. Odbiorcy nieświadomi podstępu odpowiedzieli „mailowym atakiem" na serwis joes.com, w wyniku czego został on unieruchomiony na 10 dni.

Można wyróżnić dwa rodzaje Joe – Job:

- wysyłany z adresu jednego użytkownika, w celu skompromitowania go;
- wysyłany z różnych, często losowych, adresów w jednej domenie (uprzednio nie kojarzonej ze spamem), w celu ominięcia filtrów antyspamowych.

Więcej można przeczytać m.in. na: http://en.wikipedia.org/wiki/Joe_job.

### *2.3.5. Zombie*

Coraz częściej nadawcy spamu stosują bardzo agresywne techniki wysyłając przesyłki, które po otworzeniu zaczynają (bez wiedzy odbiorcy) instalować oprogramowanie na komputerze ofiary, które posłuży spamerowi do wysyłania spamu z maszyny nieświadomego użytkownika. Spamerzy dokonując ataków DoS (Denial of Service) na komputery indywidualnych użytkowników przejmują nad nimi kontrolę i zaczynają ich używać jako tzw. „wzmacniaczy" do ataku DDoS (Distributed DoS) na duże instytucje, jak np. banki, czy firmy komputerowe. Takie wykorzystanie komputerów „zombie" uniemożliwia wykrycie rzeczywistego źródła spamu, a co za tym idzie – utrudnia walkę z działalnością tego typu.

Istotnym faktem jest, że spamerzy w tym przypadku wykorzystują możliwe błędy w używanym przez nas oprogramowaniu do obsługi poczty i przeglądania stron www, aby przesłać i zainstalować swój program na naszym komputerze. Częste aktualizacje oprogramowania, bądź wybór mało popularnych programów do tych celów może nas częściowo uchronić przed tego typu atakiem.

O wykrywaniu, czy nasz komputer został wykorzystany jako „spam zombie" można przeczytać m.in. na: http://www.spambutcher.com/spamzombies/.

Szersze studium o „spam zombie" na: http://nospam-pl.net/zombie.php.

# 3. Ofensywa i defensywa.

## 3.1. Sposób działania spamerów.

Metody pozyskiwania adresów e-mail:

- najczęstsze jest skanowanie sieci w celu pozyskania adresów e-mail i wysłania danej wiadomości na wszystkie znalezione adresy. Do tego typu działań służą m.in. programy o nazwie harvester, przeszukujące Internet w poszukiwaniu tekstów wyglądających jak adresy mailowe. Ponieważ adres e-mail musi zawierać znak małpy „@", więc teksty w otoczeniu tego znaku są brane pod uwagę, jako potencjalne adresy e-mail (http://pl.wikipedia.org/wiki/Harvester);

- wysyłanie maili z wirusami typu koń trojański (http://pl.wikipedia.org/wiki/Ko%C5%84_troja%C5%84ski_%28informatyka%29 ), które po zainstalowaniu się na komputerze odbiorcy wysyłają spamerowi wiele cennych informacji – m.in. zawartość książki adresowej ofiary;

- wymienianie adresów między spamerami lub generowanie ich automatycznie od imion, czy też popularnych nicków i sprawdzanie ich autentyczności poprzez wysyłanie maila o treści typu „jeżeli nie chcesz więcej dostawać maila z tego adresu, to odeślij maila (na ten adres) następującej treści / wejdź na stronę www.(...) i wpisz swój adres na listę...". Intencje nadawcy są oczywiście wręcz przeciwne do tych wpisanych w treść wiadomości;

- inną metodą sprawdzenia autentyczności adresu e-mail jest wysłanie na niego maila z tekstem w formacie HTML i skryptami w języku JavaScript. Wiele programów pocztowych po odebraniu takiego emaila automatycznie połączy się z serwerem spamera w celu np. ściągnięcia obrazka. Wystarczy, że spamer przeglądnie sobie logi serwera i już otrzymuje potwierdzenie, które adresy są rzeczywiście używane.

Metody maskowania się przez spamerów:

- wykorzystanie serwera typu „open relay", czyli takiego, którego oprogramowanie służące do obsługi poczty elektronicznej nie jest odpowiednio zabezpieczone przed wykorzystaniem przez osoby trzecie. Najczęściej jest to wynikiem złej konfiguracji serwera;

- łamanie zabezpieczeń serwera i wysłanie za jego pośrednictwem tyle spamu, ile się da zanim administrator się zorientuje o włamaniu;

- przejęcie kontroli nad komputerami indywidualnych użytkowników przy pomocy wirusów i robaków rozsyłanych jako załączniki do spamu i stworzenie sieci tzw, komputerów „zombie" do maskowania rzeczywistego źródła spamu. Takie sieci noszą nazwę botnetu (http://pl.wikipedia.org/wiki/Botnet_%28zombie%29).

W jakich celach spam jest wysyłany:

- w celach reklamowych, choć (za Wikipedią) poważne firmy nie korzystają z tej formy reklamy ze względu na ogólne potępianie tej metody. „Najczęstszymi produktami reklamowanymi poprzez spam są środki farmaceutyczne.”

- w celu przejęcia kontroli nad komputerem, aby włączyć go do bonetu i wykorzystać do innych ataków;

- w celu pozyskania informacji poufnych, jak np. nr i haseł do kont bankowych. W tym celu spamer wysyła wiadomość treści: „twoje konto bankowe zostało zmienione. W celu aktualizacji zaloguj się na stronę … i wypełnij zamieszczony tam formularz.”. Strona ta oczywiście jest fałszywką napisaną przez spamera w celu przejęcia informacji, choć często jej adres jest łudząco podobny do adresu oficjalnej strony banku. Poza tym formularz, który należy wypełnić na tej stronie zawiera wszystkie poufne informacje potrzebne spamerowi do przejęcia konta. Taka metoda nosi nazwę phishingu. Więcej na jej temat: http://pl.wikipedia.org/wiki/Phishing;

- w celu wyłudzenie pieniędzy – nigeryjski szwindel opisany w pkt2.3.3

Źródło: http://pl.wikipedia.org/wiki/Spam.

## *3.2. Lepiej chronić niż bronić.*

Jednym ze sposobów ochrony przed spamem jest ochrona własnego adresu e-mail przed dostaniem się „w ręce" spamerów. W tym celu należy:

- unikać podawania swojego adresu e-mail, tam gdzie to nie jest konieczne;
- podając adres w miejscu ogólno dostępnym (jak np. fora dyskusyjne, strony www, itp.) – unikać wpisywania go wprost. Zalecane jest „udziwnianie" swojego adresu przez wstawki rozumiane przez człowieka, w stylu „usuń_to" lub „małpa", „at" zamiast „@", a niezrozumiałe dla programu typu „harvester". Niestety te coraz częściej stają się bardzo wyczulone na niektóre typowe wstawki, więc trzeba być pomysłowym, żeby je przechytrzyć. Więcej na temat kodowania swojego adresu na http://nospam-pl.net/obrona2.php.

Stopień bezpieczeństwa zastosowanej „blokady", czyli zafałszowania swojego adresu e-mail można sprawdzić na stronie: http://js.webhelp.pl/nospamcheck.php.

- jeżeli konieczne jest podanie adresu wprost- przeznaczmy na to osobne konto pocztowe (najlepiej darmowe) lub używajmy aliasu (o ile to możliwe).

Oprócz tego zaleca się:

- wyłączenie w programie pocztowym obsługi HTML i JavaScript oraz automatycznego otwierania załączników do maili;
- częstą aktualizację swojego programu pocztowego poprzez doinstalowywanie dostępnych łat;
- używanie niestandardowych programów do obsługi poczty, ponieważ wirusy są najczęściej pisane pod najpopularniejsze programy pocztowe, bo w ten sposób można łatwo zawładnąć szerokim kręgiem komputerów. Mało kto będzie się trudził pisaniem wirusa pod program używany sporadycznie przez nieliczne grono użytkowników Internetu;
- zainstalowanie programu antywirusowego;
- zainstalowanie filtra antyspamowego.

Źródło: http://pl.wikipedia.org/wiki/Spam.

### *3.3. Gdy zostaniemy zaatakowani.*

Po pierwsze nie należy odpowiadać spamem na spam – osoba, której adres znajduje się w polu nadawcy może być niczego nie świadomą ofiarą ataku spamerów. Nie zaleca się otwierania załączników do poczty, jeżeli przyszła ona z nieznanego adresu (część programów antywirusowych odcina „podejrzane" załączniki, często również te, na które czekaliśmy…). Jeżeli w treści wiadomości widnieje konieczność odwiedzenia jakiejś witryny w celu np. zweryfikowania swoich danych – pod żadnym pozorem nie należy tego robić.

Jeżeli wiadomości z pewnego adresu zaczynają napływać masowo, a my sobie tego nie życzymy – nie zostaje nam nic, jak zainstalować filtr antyspamowy. Jeżeli posiadamy konto unixowe z dostępem do shella, możemy skorzystać z programu procmail, który umożliwia m.in. własnoręczne konfigurowanie reguł selekcji poczty i w zależności od sklasyfikowania danej wiadomości – umieszcza ją w odpowiednim katalogu lub odsyła (po uprzedniej obróbce) do nadawcy, np. z adnotacją „Adresat nieznany.". Więcej na ten temat na: http://nospam-pl.net/obrona1.php .

Nie posiadając konta unixowego pozostaje nam zainstalowanie narzędzia do filtrowania spamu działającego po stronie klienta. Tego typu programy zazwyczaj „uczą się" wyszukiwać pewne słowa charakterystyczne dla przesyłek będących spamem. Niestety często – przy zbyt mocnych regułach filtrujących – odfiltrowują listy niebędące spamem. Listę takich programów można znaleźć np. na: http://dmoz.org/Computers/Software/Shareware/Windows/Internet/Email/Spam_Filtering/ lub na http://dmoz.org/Computers/Internet/Abuse/Spam/Filtering/.

Jest jeszcze jedno wyjście – filtracja poczty po stronie serwera. Służą do tego programy podobne do tych filtrujących po stronie klienta, jednak albo na serwerze pocztowym, na którym mamy konto – taki filtr jest założony, albo zostaje nam kontakt z administratorem lub zmiana konta pocztowego. Przykładowy wykaz programów do filtracji po stronie serwera:
http://dmoz.org/Computers/Software/Internet/Servers/Mail/Spam_Filtering/.

Wikipedia podaje, że osoby tworzące i utrzymujące strony internetowe mogą włączyć się do walki ze spamem „tworząc generatory fałszywych stron zawierających generowane dynamicznie adresy e-mail w domenach nieistniejących lub należących do spamerów". W ten sposób zwiększa się koszt działania, jednocześnie zmniejszając efektywność programów typu „harvester", zmniejsza się wartość baz adresów, a przez zastosowanie w adresach domen znanych spamerów – daje im szansę odczuć „ na własnej skórze", co to jest spam, który tworzą. Oprócz tego stosuje się tzw. adresy pułapki, służące potem do uczenia filtrów antyspamowych. Przykładem takiego projektu jest SpamPoison: http://polish-605837225l4.spampoison.com/.

Źródło: http://pl.wikipedia.org/wiki/Spam.

# *4. Podsumowanie.*

Spam jest z jednej strony uciążliwością – zaśmiecając nasze skrzynki pocztowe, zabiera nam cenny czas na jego usuwanie. W dodatku przez przypadek można podczas takich akcji przeoczyć ważną korespondencję. Filtry antyspamowe albo filtrują za mało, czyli nie wychwytują wszystkiego spamu, albo odfiltrowują oczekiwaną przez nas pocztę. Filtracja po stronie serwera – spowalnia jego pracę, a nawet może zablokować jego działanie – w przypadku napływu zbyt dużej ilości podejrzanych wiadomości.

Z drugiej strony spam może być tylko środkiem pośrednim do przechwycenia naszych poufnych informacji, czy kontroli nad naszym komputerem. Okazuje się, że spam jest zagrożeniem, o którego mocy mało kto sobie faktycznie zdaje sprawę.

Tak czy inaczej – trzeba na wszelkie dostępne sposoby przeciwdziałać akcjom podejmowanym przez spamerów.

## *5. Bibliografia – spis odsyłaczy.*

Wikipedia:

- o spamie: http://pl.wikipedia.org/wiki/Spam;
- Joe –Job: :http://en.wikipedia.org/wiki/Joe_job;
- harvester: http://pl.wikipedia.org/wiki/Harvester;
- koń trojański: http://pl.wikipedia.org/wiki/Ko%C5%84_troja%C5%84ski_%28informatyka%29
- zombie: http://pl.wikipedia.org/wiki/Botnet_%28zombie%29;
- phishing: http://pl.wikipedia.org/wiki/Phishing.

Inne:

- historia SPAMu: http://www.cusd.claremont.edu/~mrosenbl/spamstory.html, : http://www.spam.com/;
- skecz Monty Python'a: http://www.noteboom.demon.nl/spam.html, http://linux.gda.pl/pub/spam/;
- teorie na temat znaczenia słowa SPAM: http://www.cusd.claremont.edu/~mrosenbl/spamtheory.html;
- artykuł Brada Templetona na temat „Origin of the term "spam" to mean net abuse": http://www.templetons.com/brad/spamterm.html;
- reakcja na pierszy spam: http://www.templetons.com/brad/spamreact.html;
- strona: http://nospam-pl.net/ i jej podstrony;
- lista znanych wirusów: http://www.mks.com.pl/;
- hoax: http://www.symantec.com/avcenter/hoax.html, http://hoaxbusters.ciac.org/, http://www.nonprofit.net/hoax/default.htm, http://ceti.pl/gralinski/;
- nigeryjski szwindel: http://home.rica.net/alphae/419coal/, http://www.419fraud.com/, http://www.geocities.com/a_kerenx/;
- zombie: http://www.spambutcher.com/spamzombies/, http://nospam-pl.net/zombie.php
- ochrona adresu przed spamerami: http://nospam-pl.net/obrona2.php, http://js.webhelp.pl/nospamcheck.php;
- lista programów do filtracji poczty: http://dmoz.org/Computers/Software/Shareware/Windows/Internet/Email/Spam_Filtering/,http://dmoz.org/Computers/Internet/Abuse/Spam/Filtering/, http://dmoz.org/Computers/Software/Internet/Servers/Mail/Spam_Filtering/;
- projekt SpamPoison: http://polish-60583722514.spampoison.com/.