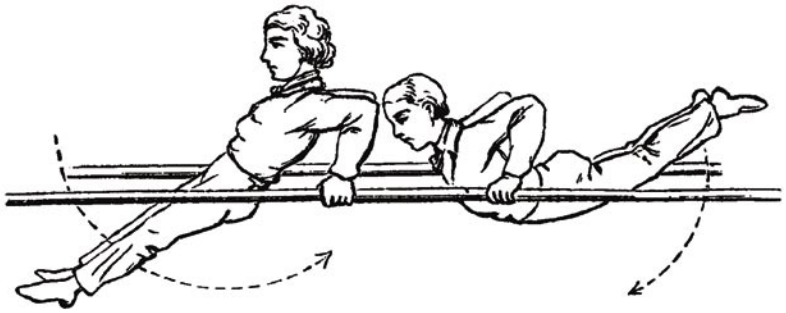
hakin9

Spamerskie sztuczki

John Graham-Cumming

Spamerskie sztuczki

John Graham-Cumming



Spamerzy stosują różnego rodzaju sztuczki, których celem jest oszukanie filtrów antyspamowych. Zobaczmy, jak sztuczki te wyglądają w praktyce i jak filtry antyspamowe pokonują spamerów ich własną bronią.

Sztuczki stosowane przez spamerów można podzielić na trzy rodzaje. Po pierwsze, spamerzy starają się ukryć niepożądane słowa (na przykład *Viagra*) w taki sposób, by nie zostały one zauważone przez filtr. Po drugie, umieszczają w wiadomościach słowa o niewinnym brzmieniu, niewidoczne dla czytającego, lecz wykrywane przez filtr, który w efekcie uznaje, że wiadomość nie jest spamem. Po trzecie, maskują podawane w wiadomościach adresy swoich stron, ponieważ są świadomi tego, że te adresy mogą ich zdradzić.

Ukrywanie niepożądanych słów

Spamerzy najczęściej chcą ukryć słowa, na podstawie których wiadomość można łatwo rozpoznać jako spam. Używają rozmaitych metod przetworzenia słów takich jak *Viagra* do postaci niezrozumiałej dla filtru antyspamowego, jednak czytelnej dla człowieka.

Nieco przestrzeni

Najprostszy sposób polega na wstawieniu do słowa, które ma zostać ukryte, znaków spacji.

```
V I A G R A
```

Pozwala to oszukać najprostsze filtry, które wykrywają obecność słowa *Viagra*; oczywiście bardziej wymyślny filtr potrafi szukać tekstu według schematu `<litera><spacja><litera><spacja>`... i odtworzyć zakamuflowane w ten sposób słowo. Spamerzy używają więc również innych znaków do rozdzielania liter, np.:

```
V'I'A'G'R'A, V.I.A.G.R.A, V*I*A*G*R*A
```

Filtry antyspamowe potrafią jednak w stosunkowo prosty sposób wykryć tego rodzaju zabiegi i orientować się, że w

Z artykułu nauczysz się...

- jakimi sztuczkami posługują się spamerzy w celu oszukania filtrów bayesowskich i heurystycznych.

Co powinieneś wiedzieć...

- znać podstawy filtrowania bayesowskiego i heurystycznego (omówione w poprzednim numerze naszego pisma),
- ogólnie orientować się w językach HTML i Javascript.

wiadomości mowa jest o Viagrze. Na tym prostym przykładzie widać jednak, że nie warto stosować filtrów heurystycznych wymagających samodzielnego aktualizowania reguł – sens ma jedynie stosowanie filtrów aktualizowanych automatycznie. Dostosowanie reguł nawet dla tak prostej sztuczki, jak przedstawiona powyżej, wymagałoby wiele pracy ze strony użytkownika.

Można nawet spotkać wiadomości, w których zastosowano zgoła inną technikę – z tekstu usunięto wszystkie spacje, wstawiając w ich miejsce losowo wybrane litery:

```
DidAyouFknowNyouMcanBget
VprescriptionVmedications
prescribedTonlineTwith
NORPRIORRPRESCRIPTIONRREQUIRED!
```

Nie wydaje się jednak, by technika ta była szczególnie skuteczna, ponieważ taka wiadomość jest w rezultacie nieczytelna dla człowieka.

Øbcÿ ākçênt

Spamerzy, przeprowadzając testy sprawdzające, jak na wysyłane przez nich wiadomości reagują darmowe i komercyjne programy filtrujące, szybko zorientowali się, że tak proste sposoby ukrywania słów nie są zbyt skuteczne. Zaczęli więc stosować metody, w których zamieniane są litery składające się na słowo *Viagra*.

W tablicy znaków ASCII można znaleźć wiele samogłosek ze znakami akcentu, które spamerzy wstawiają do ukrywanego słowa w zastępstwie oryginalnych samogłosek:

- a: à á â ã ä å,
- e: è é ê ë,
- i: ì í î ï,
- o: ò ó ô õ ö,
- u: ù ú û ü.

Przy zastosowaniu różnych wariantów samogłosek *a* oraz *i* spamer może zapisać słowo *Viagra* na 144 różne sposoby, jak choćby *Víagra*, *Viâgrä*, *Vîãgrä*. Anglojęzyczny odbiorca wiadomości przeczyta takie słowo nie zwracając uwagi na samogłoski, jednak filtr może zostać oszukany.

Filtr może poradzić sobie z tego typu sztuczką przypisując każdej samogłosce ze znakiem akcentu jej oryginalny odpowiednik, otrzymując w rezultacie rzeczywiste słowo. Ze względu na łatwość wykrywania obu przedstawionych technik przez stosowane dziś filtry antyspamowe, spamerzy zaczęli szukać nowych sposobów dostawania się do skrzynek pocztowych. Wykorzystują do tego HTML.

Nie z nami takie numery

Kolejnym sposobem zakamuflowania słowa Viagra jest zastosowanie encji języka HTML, które służą do umieszczania w tekście znaków specjalnych lub znaków spoza alfabetu angielskiego. Encje zapisywane są jako liczby poprzedzone znakami `&#`, a zakończone znakiem `;`. Chcąc na przykład umieścić w tekście francuski znak *é*, piszemy w HTML-u `&#233;`, z kolei grecką literę ∑ otrzymamy po wpisaniu `&#917;`.

Znaki należące do podstawowego alfabetu angielskiego także mają odpowiadające im encje. Przykładowo, literę *A* można zapisać jako `&#65;`. Podstępny spamer mógłby zatem zapisać całe słowo *Viagra* przy zastosowaniu encji: `&#86;&#105;&#97;&#103;&#114;&#97;`

Także w tym przypadku odpowiednio przygotowany filtr antyspamowy rozpozna encje HTML i odkryje, jakie słowo zostało w ten sposób zamaskowane. Istnieją jednak znacznie bardziej wyrafinowane metody kamuflowania słowa *Viagra*, wykorzystujące możliwości formatowania dostępne w języku HTML.

HTML tu i tam

Polecenia formatujące języka HTML zapisywane są w postaci tzw. znaczników, czyli instrukcji umieszczanych pomiędzy nawiasami trójkątnymi `< >`.

Przykładowo, chcąc zapisać słowo *Witaj* tekstem pogrubionym, piszemy w HTML-u `<b>Witaj</b>`. Znacznik `<b>` oznacza *początek tekstu pogrubionego*, natomiast `</b>` oznacza *koniec tekstu pogrubionego*. Tekst pomiędzy tymi znacznikami będzie widoczny w przeglądarce lub programie pocztowym obsługującym HTML jako pogrubiony.

Podobnie jak większość języków programowania, HTML umożliwia stosowanie w dokumentach komentarzy. Są one całkowicie pomijane podczas wyświetlania dokumentu HTML. Komentarz rozpoczyna się znakami `<!--`, natomiast kończy `-->`; tekst pomiędzy tymi znakami jest ignorowany przez przeglądarki dokumentów HTML.

Spamerzy używają komentarzy do rozdzielenia fragmentów niepożądanych słów. Dla przykładu, słowo *Viagra* może zostać podzielone w następujący sposób:

```
V<!--anon-->i<!--dinosaur-->
a<!--hexagon-->g<!--two-->r
<!--mouse-->a
```

Ten dziwnie wyglądający fragment tekstu w programie pocztowym odczytującym HTML zostanie wyświetlony jako *Viagra*. Wiele filtrów antyspamowych da się nabrać na tę sztuczkę, ponieważ nie potrafią one przetwarzać składni HTML i nie wyodrębnią słowa *Viagra*. Co gorsza, za sprawą słów w komentarzach filtr może zostać wprowadzony w błąd i uznać, że wiadomość nie jest spamem.

Zaprezentowana technika jest bardzo często stosowana przez spamerów, dlatego też skuteczne filtry są wyposażane w funkcje usuwające komentarze HTML-a przed analizą tekstu wiadomości. Odnalezienie i usunięcie tekstu umieszczonego pomiędzy znakami `<!--` i `-->` nie jest trudnym zadaniem: w istocie to właśnie robią programy pocztowe podczas wyświetlania wiadomości HTML. W gruncie rzeczy sama obecność komentarzy HTML może budzić podejrzenia programu filtrującego – dlaczego ktokolwiek miałby umieszczać je w zwyczajnej wiadomości?

Niekiedy spamerzy wykorzystują także nieprawidłowe znaczni-

Rysunek 1. *Mikrokropka*

Listing 1. *Układanka*

```
<table border=0 cellpadding=0 cellspacing=0>

  <tr valign=top>
    <td><font face=Courier>V<br>s<br>F</font></td>
    <td><font face=Courier>i<br>a<br>R</font></td>
    <td><font face=Courier>a<br>m<br>E</font></td>
    <td><font face=Courier>g<br>p<br>E</font></td>
    <td><font face=Courier>r<br>l</font></td>
    <td><font face=Courier>a<br>e</font></td>
    <td><font face=Courier> <br>s</font></td>
  </tr>
</table>
```

ki HTML o przypadkowo wybranych nazwach, ponieważ podobnie jak komentarze zostaną one zignorowane przez przeglądarkę. Wstawienie dowolnych słów pomiędzy znakami < i > ma podobny efekt, jak zastosowanie komentarzy:

```
V<anon>i</dinosaur>a<hexagon>g
<two>r</mouse>a
```

Czarna dziura

Duża popularność powyższej sztuczki wśród spamerów stała się dla niej zgubna, ponieważ doprowadziła do tego, iż większość filtrów antyspamowych usuwa komentarze HTML. Rozdzielanie słów znacznikami HTML pozostaje jednak jedną z ulubionych technik stosowanych przez spamerów. W metodzie zwanej *czarną dziurą* niepożądane słowo rozdzielane jest spacjami o zerowej szerokości.

Chcąc określić rozmiar czcionki fragmentu tekstu, wpisujemy w HTML-u polecenie `<font size=X>`, w miejsce `X` wstawiając wartość od 1 do 7 (7 to największy rozmiar, 1 to najmniejszy). Przykładowo, aby zapisać słowo *Witaj* najmniejszą czcionką, piszemy:

```
<font size=1>Witaj</font>
```

Programy takie jak Microsoft Internet Explorer oraz narzędzia pocztowe Outlook i Outlook Express dopuszczają również stosowanie rozmiaru 0, czyli tekstu o zerowym rozmiarze. Spamerzy mogą więc wykorzystać czcionkę o rozmiarze 0 wraz z encją ` ` odpowiadającą twardej (nieprzełamywanej) spacji, otrzymując w efekcie znak spacji o zerowej szerokości:

```
<font size=0> </font>
```

Stosując tę technikę, słowo *Viagra* może zostać podzielone w następujący sposób:

```
V<font size=0> </font>i
<font size=0> </font>a
<font size=0> </font>g
<font size=0> </font>r
<font size=0> </font>a
```

Skuteczny filtr antyspamowy musi zatem być w stanie rozpoznać nie tylko komentarze HTML (jak w sztuczce omówionej wcześniej), lecz również rozmiary czcionek. Spamerzy wymyślają jednak coraz to nowe metody oszukiwania filtrów: skoro filtry wychwytują czcionkę o rozmiarze 0, to czemu by nie zastosować rozmiaru 1?

Mikrokropka

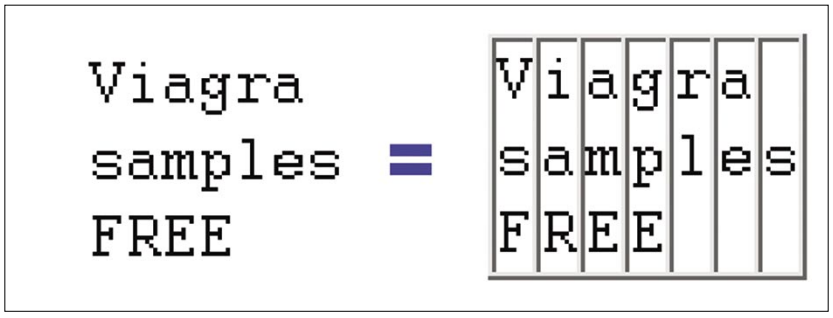
Jeden z najnowszych pomysłów spamerów polega na wstawianiu w środku słowa przypadkowych liter (co powoduje, że po usunięciu znaczników HTML filtr odczyta słowo *Viagra* na przykład jako *Vziagra*) i pomniejszeniu tych liter do takiego rozmiaru, by były prawie niewidoczne dla człowieka. Oto sztuczka zwana *mikrokropką*, wykorzystująca czcionkę o rozmiarze 1.

```
V<font size=1>z</font>iagra
```

W programie pocztowym odczytującym HTML efekt będzie zbliżony do pokazanego na Rysunku 1. Jak widać, litera `z` jest tak mała, że wygląda jak prawie niewidoczna kropka.

Układanka

W jednej z najbardziej przebiegłych metod rozdzielania wyrazów spamerzy wykorzystują czcionkę o sta-



Rysunek 2. *Układanka*

Listing 2. *Atrament sympatyczny*

```
<body bgcolor=white>
  Viagra
  <font color=white>
     Hi, Johnny! It was
     really nice to have
     dinner with you
     last night. See
     you soon, love Mom.
  </font>
</body>
```

łej szerokości oraz tabele. Kamuflowany tekst jest najpierw zapisywany czcionką o stałej szerokości, by można było podzielić go na kolumny:

```
Viagra
samples
FREE
```

Następnie budowana jest tabela, w której w każdej z kolumn zapisywana jest jedna kolumna liter tekstu (patrz Listing 1 i Rysunek 2).

Ta technika jest nader skuteczna w przypadku filtrów antyspamowych, które usuwają znaczniki HTML-a. Filtr otrzymuje tekst wyglądający jak ciąg przypadkowych liter, ponieważ tekst jest odczytywany z góry na dół, zamiast od lewej do prawej.

```
Vsf iaR ame gpe rl ae s
```

Wyodrębnienie treści wiadomości wymagałoby, by filtr był wyposażony w mechanizm rozpoznawania rozmieszczenia elementów HTML-a. W praktyce jednak nie jest to konieczne, ponieważ wiadomość jest łatwo identyfikowana jako spam za sprawą zastosowania złożonej tabeli i czcionek o stałej szerokości. Wykrywane są więc nie same słowa, lecz metody wykorzystane do ich zamaskowania.

Dodawanie niewidocznych niewinnych słów

Po zamaskowaniu niepożądanych słów, spamerzy dodają do wiadomości słowa, które w ich opinii są uważane za niewinne. Ponieważ niektóre filtry antyspamowe korzystają z listy słów, których obecność ma świadczyć o niespamowej naturze wiadomości, spamerzy liczą na to, że umieszczenie w treści tego rodzaju słów spowoduje, że filtr zaakceptuje wiadomość. Ponieważ jednak słowa te mają być niewidoczne dla odbiorcy wiadomości (który ma się skoncentrować na ofercie kupna Viagry), spamerzy stosują różne sposoby ukrywania tych słów przed czytającym wiadomość, jednocześnie pozostawiając je czytelnymi dla filtrów.

Atrament sympatyczny

Jedną z podstawowych metod ukrywania niewinnych słów w treści wiadomości jest zapisywanie ich białym tekstem na białym tle (bądź też innym kolorem, byleby tylko był on taki sam dla tekstu i tła) – patrz Listing 2. Spamerzy stosują ten sposób, ponieważ taki tekst będzie niewidoczny dla człowieka, jednak program filtrujący ignorujący kolory tekstu odczyta go. Niektóre filtry antyspamowe dają się na to nabrać i przy odpowiednim doborze słów wiadomość nie zostaje zidentyfikowana jako spam.

Skuteczne filtry antyspamowe rozpoznają wykorzystanie kolorów HTML-a i wykrywają tę sztuczkę. Jej obecność świadczy o tym, że wiadomość to najprawdopodobniej spam. Popularność tej metody szybko doprowadziła do tego, że filtry zostały wyposażone w mechanizmy jej rozpoznawania, spamerzy wymyślili więc inny sposób ukrywania tekstu, za pomocą kolorów bardzo do siebie zbliżonych, lecz nie identycznych.

Listing 3. *Kamuflaż*

```
<body bgcolor=#113333>
  <font color=yellow>
    Viagra
  </font>
  <font color=#123939>
    jakieś niewinne słowa
  </font>
</body>
```

Kamuflaż

Zamiast zapisywania białego tekstu na białym tle, spamerzy mogą wykorzystać kolory niewiele się od siebie różniące (np. tekst w kolorze jasnoszarym na białym tle) – patrz Listing 3 i Rysunek 3. Tekst, który ma pozostać widoczny, zapisywany jest kolorem wyraźnie odróżniającym go od tła.

Niewinne słowa są w efekcie prawie niewidoczne, w przeciwieństwie do informacji o oferowanym produkcie. Ta sztuczka jest skuteczna w przypadku filtrów rozpoznających *atrament sympatyczny*, ponieważ tym razem kolory nie są identyczne, a odbiorca wiadomości zauważy jedynie czytelny tekst.

Dobre filtry antyspamowe potrafią odkryć podstęp rozpoznając podobieństwo kolorów na podstawie odległości Euklidesa, wykrywając w ten sposób tekst prawie niewidoczny dla człowieka.

MIME wszystko

Większość programów pocztowych odczytuje MIME, umożliwiające wysyłanie wiadomości złożonych z wielu części, z których każda jest określonego typu (np. tekst, HTML, dokument Worda). Najczęściej programy otwierają automatycznie po-

Rysunek 3. *Kamuflaż*

Listing 4. *MIME wszystko*

```
------=_NextPart_01C29D73.26716240
Content-Type: text/plain;
The modes of letting vacant farms, the duty of supplying buildings
and permanent improvements, and the form in which rent is to be received,
have all been carefully discussed in the older financial treatises. Most
of these questions belong to practical administration, and are, moreover, not
of great interest in modern times.
------=_NextPart_01C29D73.26716240
Content-Type: text/html;
<p><b><font color=red>Viagra</font></b></p>
```

stać HTML-ową, ignorując wersję tekstową.

Spamerzy wykorzystują tę cechę programów pocztowych w taki sposób, że niewinne słowa umieszczają w tekstowej części wiadomości, natomiast treść spamu zawierają w TML-u (patrz Listing 4). Odbiorcy zostaje pokazana wiadomość przygotowana przez spamera, a część tekstowa pozostaje niewidoczna. Filtr antyspamowy przeczyta zarówno wersję HTML, jak i tekstową.

Co w świecie słychać

Kolejną sztuczką jest umieszczanie w wiadomościach fragmentów najnowszych informacji ze świata, pobranych ze stron agencji informacyjnych. Spamerzy liczą na to, że umieszczenie w wiadomości tekstu o aktualnych wydarzeniach zmniejszy prawdopodobieństwo zidentyfikowania jej jako spam.

```
<Despite statements last week from
chief U.N. inspector Hans Blix that
full cooperation was expected from
Iraq, Iraqi Foreign Minister Naji
Sabri lashed out at the United
Nations in a 19-page letter to
Secretary-General Kofi Annan
written in Arabic>
```

Oczywiście, spamerzy nie chcą, by odbiorca wiadomości czytał najnowsze doniesienia prasowe, lecz przygotowaną przez nich ofertę, umieszczają zatem tekst informacji pomiędzy znakami < i >. Programy pocztowe, które potrafią czytać wiadomości w HTML-u, potraktują taki tekst jak nieprawidłowy znacznik i zignorują go.

Dodatkowy tytuł

W HTML-u istnieje znacznik <title>, służący do nadawania tytułu stronie wyświetlanej w przeglądarce. W wiadomościach pocztowych zapisanych w HTML-u jest on zwykle ignorowany, a jego zawartość nigdzie się nie pojawia (za tytuł wiadomości uważany jest zwykle jej temat).

```
<title>dinosaur reptile ghueej
egrjerijg gerrg</title>
```

Jest to zatem kolejna metoda, którą może posłużyć się spamer, chcąc ukryć w wiadomości niewinne słowa niewidoczne dla odbiorcy.

Małe przewijanko

Przewijany element *marquee* umożliwia spamerowi umieszczenie w wiadomości dowolnej ilości niewinnego tekstu na mikroskopijnej powierzchni. W poniższym przykładzie (z życia wziętym) cały tekst jest przewijany wewnątrz prostokąta o rozmiarze 8x8 pikseli, co czyni go praktycznie niewidocznym dla odbiorcy wiadomości (patrz Rysunek 4).

```
<marquee bgcolor="white"
height="8" width="8">
  Did you ever play that game
  when you were a kid where the
  little plastic hippo tries to
  gobble up all your marbles?
</marquee>
```

Kochanie, zmniejszyłem czcionkę

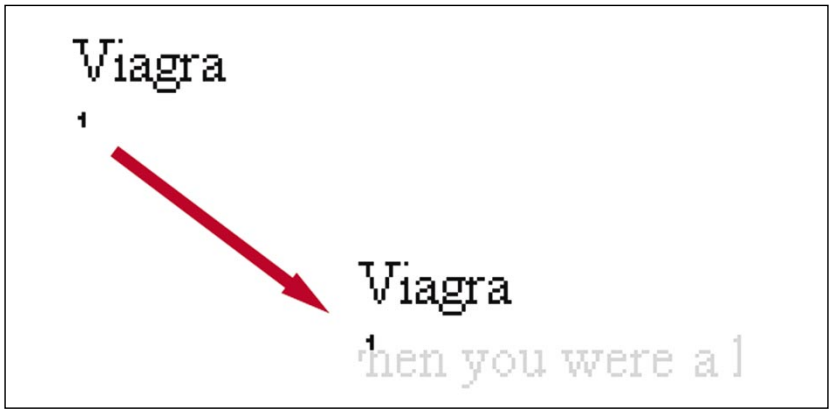
Ostatnią z popularnych wśród spamerów metod ukrywania tekstu jest zapisywanie go czcionką o rozmiarze 1.

```
<font size="1" color="#FFFFFF">
  Dowolne słowo o długości 1-22
  znaków zapisane WIELKIMI LITERAMI
  TSUTHRXJKVUVBECP
</font>
```

Warto też wiedzieć, że losowe, nic nie znaczące zlepki liter pojawiające się w spamie są metodą na oszukanie sieci antyspamowych, które zliczają sumę kontrolną wiadomości (np. *Pyzor*, *Razor*, *DCC* – patrz poprzedni numer naszego pisma).

Maskowanie adresów stron

Jedną z metod, którą posługują się filtry antyspamowe do wykrywania niepożądanych wiadomości, jest analizowanie występujących w tekście adresów stron. W większości spamerskich wiadomości występuje co najmniej jeden odnośnik do stro-



Rysunek 4. *Małe przewijanko*

ny, na której sprzedawane są produkty. Po utworzeniu czarnej listy takich stron możliwe jest identyfikowanie spamu na podstawie adresów występujących w wiadomości. Spamerzy starają się, by adres, który jest sprawdzany przez filtr, nie odpowiadał żadnemu z adresów z czarnej listy; z drugiej strony dbają o to, by nadal prowadził do właściwej strony.

Enigma i Ultra

Adresy są zwykle zapisywane w postaci czytelnej dla człowieka, jednak HTML umożliwia inne postaci zapisu. Oto kilka dostępnych możliwości: w pierwszych trzech wykorzystany jest adres IP strony *(www.yahoo.com),* najpierw zapisany jako jedna liczba dziesiętna, następnie jako jedna liczba szesnastkowa, wreszcie w postaci liczb ósemkowych rozdzielonych kropkami. Czwarta postać to adres zakodowany ze znakiem `%`, w którym każda z liter (lub znaków) została zastąpiona odpowiadającą jej liczbą szesnastkową.

```
http://3631052355/
http://0xD86D7643/
http://0330.0155.0166.0103/
http://%77%77%77%2E%79%61%68
       %6F%6F%2E%63%6F%6D/
```

Skuteczny filtr antyspamowy rozróżnia rozmaite postaci adresu i potrafi odtworzyć właściwy adres przed sprawdzeniem czarnej listy.

Trefny login

Rzadko wykorzystywaną cechą adresów (przynajmniej w przypadku protokołu HTTP) jest możliwość zastosowania składni `http://użytkownik@host/` (najczęściej spotyka się po prostu zapis `http://host/`). Spamerzy używają dowolnie wybranych nazw użytkowników, aby podejrzany adres zyskał niewinny wygląd. W poniższym przykładzie adres nie prowadzi do strony *www.microsoft.com*, lecz do strony o adresie IP `3631052355` (który został dodatkowo zakamuflowany jedną z powyższych metod).

```
http://www.microsoft.com@3631052355/
```

Listing 5. *Lampa Alladyna*

```
<HTML><HEAD><SCRIPT LANGUAGE="Javascript">
  <!-- var Words="%3CHTML%3E%0D%0A%3CHEAD%3E%0D%0A%3CTITLE%3E%3C/TITLE%3E
  %0D%0A%3CMETA%20HTTP-EQUIV%3D%22Content-Type%22%20CONTENT%3D%22text/html
  %3B%20charset%3DBig5%22%3E%0D%0A%3CMETA%20HTTP-EQUIV%3D%22Expires%22%20
  CONTENT%3D%22Sat%2C%201%20Jan%202000%2000%3A00%3A00%20GMT%22%3E%0D%0A%3C
  META%20HTTP-EQUIV%3D%22Pragma%22%20CONTENT%3D%22no-cache%22%3E%0D%0A%3C
  /HEAD%3E%0D%0A%3CFRAMESET%20ROWS%3D%22100%25%2C0%2220FRAMEBORDER%3DNO%20
  BORDER%3D%220%"; function SetNewWords(){ var NewWords; NewWords =
  unescape(Words);document.write(NewWords);} SetNewWords();
// --></SCRIPT></HEAD><BODY></BODY></HTML>
```

Listing 6. *Niekoniecznie WYSIWYG*

```
Remove My e-mail from my Friends Contact
<a href="http://sex.com/bPqjOL09yGCHw/"
onmouseover=  "window.status='http://%77%77%77%77.3%65%653--%69%6c11%6c%69
  --3%6c%69%6c%6c.%6f%72%67/bPqjOL09yGCHw/remove.htm';return true;"
onmouseout= "window.status=' ';return true;">ClickHere</a>
```

Do strony zostanie przekazana nazwa użytkownika *www.microsoft.com*, która bez wątpienia zostanie zignorowana.

Internet Exploiter

Błąd w popularnej przeglądarce Internet Explorer firmy Microsoft pozwala spamerom pójść o krok dalej, i nie tylko zmienić postać adresu na niewinną, lecz także zmodyfikować adres pokazywany w pasku stanu przeglądarki:

```
<a href=http://www.microsoft.com
=01%01%00@3631052355>
  www.microsoft.com</a>
```

Podobne, jak we wcześniejszym przykładzie, prawdziwym adresem strony jest `http://3631052355/`, jednak w programie pocztowym pokazany zostanie adres *www.microsoft.com*, także w pasku stanu, ponieważ symbol `%00` umieszczony przez znakiem `@` powoduje, że reszta adresu nie jest pokazywana. W tej krótkiej sztuczce wykorzystane zostają jednocześnie: zamaskowany adres strony, *trefny login* i błąd w programie!

Sztuczki w Javascript

Wymienione sztuczki to nie wszystko, na co stać spamerów. Niekiedy wykorzystują oni język Javascript, by w jeszcze większym stopniu zamaskować wysyłane wiadomości.

Lampa Alladyna

Przy stosowaniu tej metody cały tekst wiadomości zostaje umieszczony w zmiennej (patrz Listing 5), która pozostaje zakodowana aż do momentu otworzenia wiadomości przez odbiorcę. Spamer liczy na to, że wiadomość nie wzbudzi podejrzeń filtru antyspamowego, oraz że program pocztowy odbiorcy odczytuje Javascript.

Niekoniecznie WYSIWYG

Javascript jest także wykorzystywany do maskowania adresów stron. Rzeczywisty adres strony zostaje ukryty, ponieważ skrypt zmienia tekst ukazujący się na pasku stanu w chwili, gdy kursor myszki znajduje się nad napisem `ClickHere` – patrz Listing 6.

Odbiorca wiadomości sądzi, że klikając na odnośnik trafi na stronę o wskazanym adresie, w rzeczywistości jednak zostanie skierowany na zupełnie inną stronę.

Ironia losu

Jak na ironię, im więcej sztuczek mających na celu ukrycie prawdziwego charakteru wiadomości stosują spamerzy, tym łatwiej jest zidentyfikować wiadomość jako spam. Bo w końcu komu przyszłoby do głowy wysyłać prawdziwe wiadomości z wykorzystaniem sztuczek takich jak *czarna dziura*, *atrament sympatyczny* lub *mikrokropka*? ■