Die Tricks der Spammer

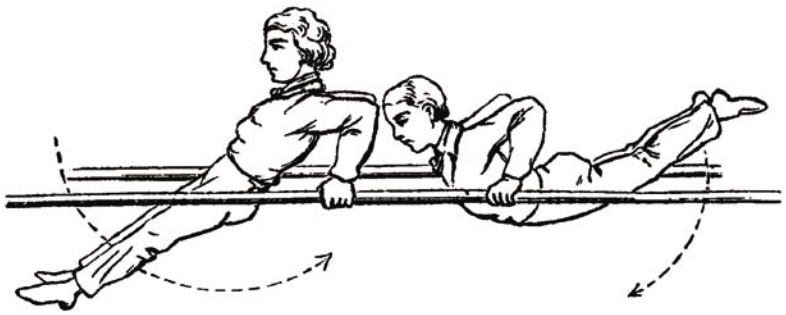
John Graham-Cumming

Der Artikel wurde in der Ausgabe 3/2004 des Magazins *Hakin9* publiziert.

Das Magazin *Hakin9*, Wydawnictwo Software, ul. Lewartowskiego 6, 00-190 Warszawa, hakin9@hakin9.org

Die Tricks der Spammer

John Graham-Cumming



In diesem Artikel zeigen wir, wie Spammer versuchen, aktuelle Spamfilter auszutricksen, wie Spamfilter dies erkennen und zu unserem Vorteil ausnutzen können.

Spammer benutzen drei Arten um Spamfilter auszutricksen. Sie verändern Schlagworte (z.B. *Viagra*) so, dass Filter sie nicht erkennen. Sie benutzen Worte, die der Filter nicht negativ assoziiert so, dass der Filter sie erkennt und die Mail nicht als Spam einstuft, nur für den Leser aber der Spam sichtbar ist. Sie verstecken eingeschlossene URL´s, die dazu führen würden, dass die Mail als Spam eingestuft würde.

Schlagworte

Als erstes versuchen Spammer Worte, die dazu führen würden, dass Filter die Mail wegen ihnen als Spam einstufen, zu verstecken. Es gibt eine Vielzahl von Techniken um Wörter wie *Viagra*, für Spamfilter nicht nachvollziehbar, zu verändern, ohne dass sie für Menschen an Lesbarkeit verlieren.

Lost in Space

Der einfachste Trick von allen ist das Einfügen von Leerzeichen zwischen die einzelnen Buchstaben, z.B.

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

Auf diese Art können einfache Filter umgangen werden, aber natürlich ist es möglich einen Filter so zu Programmieren, dass er auch Zeichenketten der Form `<Buchstabe><Leerzeichen><Buchstabe><Leerzeichen>...` untersucht und so das betreffende Wort rekonstruiert. Deswegen benutzen Spammer mittlerweile eine Vielzahl von unterschiedlich einfügten Zeichen um das Wort für Filter unkenntlich zu machen:

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

Aus diesem Artikel erfahren Sie…

- Die Grundlagen von Bayes´schen und heuristischen Filtern (in dieser Ausgabe zu finden)
- HTML- und Javascript-Basics und was wir ihnen zeigen werden…

Was Sie brauchen…

- Die Tricks, die Spammer nutzen um Bayes´sche und heuristische Filter zu umgehen

```
V*I*A*G*R*A
V-I-A-G-R-A
```

Diese Liste lässt sich beliebig weiterführen. Jedoch ist diese Methode zum Nachteil der Spammer für Filter sehr einfach zu erkennen, da nur nach dem Zeichen das zum Spacen benutzt wird gesucht werden muss, um zu erkennen, dass es in der Mail um Viagra geht.

Eine wichtige Eigenschaft von Spam-Filtern zeigt dieses simple Beispiel jedoch auf. Kaufen sie niemals einen Spamschutz, den sie selbst updaten müssen, sondern wählen sie einen, der durch Autoupdates immer auf aktuellstem Stand ist.

Da Spammer ihre Mails gegen Spam-Filter testen, haben sie erkannt, dass dieser Trick nicht mehr gut funktioniert, weshalb sich die Art zu spammen weiterentwickelt hat. Erst kürzlich bekam ich Mails zu sehen, in der der genau entgegengesetzte Weg gegangen wurde:

```
DidAyouFknowNyouMcanBget
VprescriptionVmedications
prescribedTonlineTwith
NORPRIORRPRESCRIPTIONRREQUIRED!
```

Wobei dies jedoch nicht nach einem effektiven Mittel aussieht, da die Nachricht beinahe unlesbar wird.

Ausländische Akzente

Ein kurzer Blick in die ASCII-Tabelle bringt eine Menge akzentuierter Vokale zutage, die Spammer sich zu Nutze machen können, indem sie die eigentlichen Vokale durch akzentuierte ersetzen.

- 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.

Schon durch diese einfache Maßnahme erreicht ein Spammer in unserem Viagra-Beispiel 144 Möglichkeiten *Viagra* zu schreiben (z.B. *Víagra*, *Viågra*, *Vîãgrä*). Ein Mensch ignoriert die falschen Akzente einfach und liest das Wort, ein Spam-Filter jedoch wäre ausgetrickst.

Natürlich kann man einen Spam-Filter so einstellen, dass er akzentuierte Vokale behandelt, als wenn sie ohne Akzent geschrieben wären und auf diesem Wege die Identifizierung als Spam sicherstellen. Deswegen haben Spammer HTML-Mails für sich entdeckt, da man mit HTML viele Möglichkeiten hat Inhalte zu tarnen.

Zahlenspiel

Eine weitere Möglichkeit das Wort Viagra zu verstecken besteht in der Benutzung eines Features von HTML, das das Einfügen von nicht-englischen Buchstaben in HTML ermöglicht. Diese Sonderzeichen werden mit den Zeichen `&#` begonnen und mit einem Semikolon abgeschlossen. Zum Beispiel wäre ein französisches *é* in HTML `&#233;`, das griechische Zeichen ∑ wäre `&#917;`.

Tatsächlich kann jedes Zeichen, das englische Alphabet eingeschlossen, durch äquivalente Sonderzeichenketten beschrieben werden. Der Spammer in unserem Beispiel könnte dies also ausnutzen und Viagra als `&#86;&#105;&#97;&#103;&#114;&#97;` schreiben.

Natürlich dauerte es nicht lange und so können heutige Spam-Filter auch diese Mails filtern indem sie den Code übersetzen.Viel wichtiger bei der Benutzung von HTML zum Spammen sind jedoch die Formatierungsmöglichkeiten in HTML.

Hypertextus Interruptus

Formatierungen werden in HTML immer in eckige Klammern `< >` eingeschlossen, den HTML-Tags. Um zum Beispiel das Wort *Hallo* in Fettschrift auszugeben schreibt man einfach `<b>Hallo</b>`. Hierbei steht das `<b>` für den Anfang der Fettschrift und `</b>` für dessen Ende. Der Text zwischen diesen beiden Tags erscheint nun fett, sollte unser Email-Programm HTML können.

Wie in jeder Programmiersprache auch gibt es in HTML die Möglichkeit Kommentare in den Quelltext einzubinden, ohne dass diese auf der Anzeige ausgegeben werden. Ein HTML-Kommentar beginnt mit `<!--` und endet mit `-->`, alles dazwischen wird nicht ausgegeben.

Diese Eigenschaft von HTML nutzen wiederum Spammer um einzelne Buchstaben oder Wortteile in Kommentare einzuschliessen. Dies sieht dann so aus:

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

Dieser seltsam anmutende Text wird in einem Email-Programm als *Viagra* ausgegeben. Die meisten Spam-Filter lassen sich so täuschen und erkennen das Wort *Viagra* nicht, schlimmer noch, einige können sogar die Kommentare lesen und stufen die Mail als NoSpam ein.

Der gerade gezeigte Trick ist der am meisten verbreitetste und unter Spammern populärste, deswegen können die neueren Filter mittlerweile Kommentare ignorieren und somit den Spam erkennen.

Zusätzlich können Spam-Filter die alleinige Existenz von HTML-Kommentaren als verdächtig einstufen, da kaum jemand HTML-Mails mit Kommentaren versieht. Eine Weiterentwicklung der oben beschriebenen Methode ist die Benutzung von Random-Tags. Diese Tags, die nicht definiert sind und deshalb von jedem Browser bzw. Email-Programm einfach verworfen werden:

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

Das schwarze Loch

Die unglaubliche Popularität der eben gezeigten Tricks mit Kommentaren bzw. Random-Tags bescherte ihnen ihre Niederlage im Kampf mit Spam-Filtern. Trotzdem bleiben diese Tricks die Favoriten der Spammer. Der *schwarze Loch* Trick besteht darin die verdächtigen

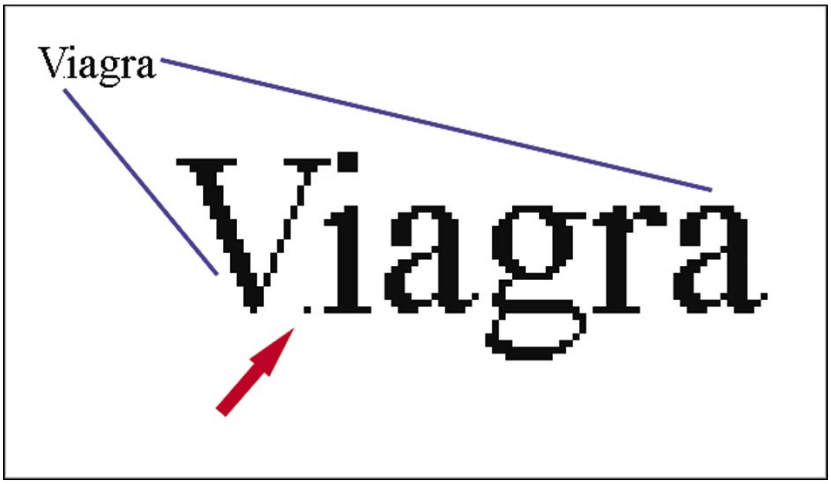


Abbildung 1. *Microdot*

Worte mit Lücken aus nicht existierenden Abständen zu füllen. Dies klingt auf den ersten Blick verwirrend, klärt sich aber mit den nächsten Zeilen auf.

Um in HTML die Textgröße anzugeben benutzt man das Attribut size (`<font size=X>` wobei `X` einen ganzzahligen Wert zwischen 1 und 7 annehmen kann). Um zum Beispiel das Wort Hallo in der kleinsten verfügbaren Größe auszugeben würde man schreiben:

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

Programme wie der Internet Explorer und Outlook/Outlook Express akzeptieren auch die Schriftgröße 0. Dies machen sich Spammer zunutze, indem sie ein Leerzeichen der Schriftgröße null einfügen:

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

und damit z.B. das Wort *Viagra* aufteilen:

```
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
```

Dieses Beispiel zeigt, dass up-to-date-Spam-Filter in der Lage sein müssen, nicht nur HTML-Kommentare, sondern auch fast alle Formatierungen zu erkennen und auszuwerten. Denn sobald der Trick mit Schriftgröße 0 nicht mehr funktioniert, wird etwas anderes benutzt (z.B. Schriftgröße 1).

Der Microdot

Diese neue Erfindung der Spammer ermöglicht es ihnen Zufallszeichen in die Mitte eines Wortes einzufügen (um z.B. einen Spam-Filter der HTML versteht anstelle *Viagra* *Vziagra* erkennen zu lassen), wobei diese eingefügten Zeichen beinahe unlesbar klein gemacht werden. Dies geschieht mit Hilfe der Schriftgröße 1, herzlich willkommen in der Welt des Microdot.

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

Wie in Abbildung 1 zu erkennen schrumpft das z zu einem winzigen, beinahe unsichtbaren Punkt

Slice and Dice

Die trickreichste Technik des Splittings benutzt eine Kombination aus einer bestimmten Schriftgröße und HTML-Tabellen. Hierbei entwirft der Spammer zuerst den Text mit einer bestimmten Schriftgröße, so dass er klar definierte Spalten mit Zeichen erhält:

```
Viagra
samples
FREE
```

Danach legt er eine Tabelle mit einer Spalte pro Zeichen an:

Spam-Filter, die HTML auswerten können werden komplett getäuscht, da sie eine Zeichenkette erkennen, die aus Zufallszeichen gebildet zu sein scheint, da sie den Text von oben nach unten anstelle von links nach rechts lesen.

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

Um diesen Text auswerten zu können müsste der Filter eine HTML-engine zum interpretieren der Tags besitzen. Dies ist aber Aufgrund der Struktur mit vielen Zellen, die immer nur ein Zeichen beinhalten nicht nötig, da sich die Mail hierüber als Spam identifizieren lässt.

Einfügen versteckter guter Wörter

Nachdem die Wörter, welche die Mail als Spam erkennbar machen, versteckt sind fügen Spammer Wörter hinzu, die dazu führen sollen, dass die Mail als No-Spam eingestuft wird. Da einige Filter Listen mit Wörtern haben, die die Mail weitergelangen lassen, hoffen Spammer durch das hinzufüen dieser Wörter

Listing 1. *Slice and Dice*

```
<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>
```

Listing 2. *Unsichtbare Tinte*

```
<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>
```

eine bessere Quote von nicht abgefangenen Mails zu erreichen. Damit die Aufmerksamkeit des Empfängers jedoch nicht vom intendierten Kontext der Mail abgelenkt wird, soll der zusätzlich eingefügte Text nur für den Filter lesbar sein.

Unsichtbare Tinte

Die mit Sicherheit am weitesten verbreitete Methode um dies zu tun besteht im schreiben weissen Textes auf weissem Hintergrund. (siehe Listing 2). Spammer mögen diese Methode, da der Computer meistens die Farbinformationen vernachlässigt und den beigefügten Text analysiert (wenn der Spammer geschickt war, gelangt die Mail zu ihrem Empfänger).

Gute Spam-Filter erkennen dies und identifizieren die Mail als Spam. Aber auch hier finden Spammer einen Ausweg, sie benutzen zwei ähnliche und nicht mehr zwei gleiche Farben, um den beigefügten Text zu tarnen.

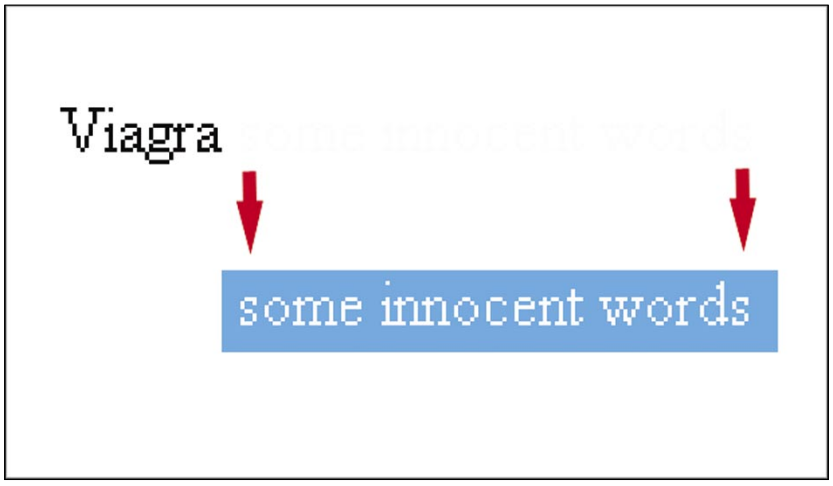


Abbildung 3. *Camouflage*

Camouflage (engl. Tarnen)

Anstelle der gleichen Farbe werden hierbei zwei sehr ähnliche Farben verwendet, z.B. ein sehr helles grau und ein Weiss (siehe Abbildung 3, sowie Listing 3). Da in HTML Farben durch einen hexadezimalen RGB-Wert beschrieben werden bestehen somit 16 Mio. Möglichkeiten.

Der Spammer wählt zuerst einen Wert für den Hintergrund (`#113333`) und dann einen sehr ähnlichen (`#123939`) für die Schrift. Für den Textteil, welcher den Spam enthält nutzt er eine Kontrastfarbe.

Wie unschwer zu erkennen, ist der getarnte Text kaum noch sichtbar, wobei der Text des angebotenen Produkts deutlich erkennbar ist. Wie zu vermuten stand: Gute Filter erkennen auch dies (durch die Nähe der Farben im euklidschen System).

MIME is Money

Die meisten Emailprogramme bieten MIME-Unterstützung (MIME – Multipurpose Internet Mail Extensions), was es ermöglicht eine Nachricht in mehreren Teilen zu verschicken, wobei jeder Teil ein anderer Dateityp sein kann (HTML, text ,...). Bei mehreren Alternativen wird immer die HTML-Version angezeigt.

Spammer nutzen dies nun aus, indem sie den No-Spam-Text im plain-Teil, den Spam jedoch im HTML-Teil verschicken (Listing 4). Es wird nur der Spam-Teil angezeigt, der Filter analysiert jedoch die gesamte Mail.

Der Nachrichtentrick

Sehr beliebt bei Spammern ist auch das extrahieren von online-News und anhängen dieser an die Mail in der Hoffnung den Filter so zu täuschen.

```
<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
```

Listing 3. *Camouflage*

```
<body bgcolor=#113333>
  <font color=yellow>
    Viagra
  </font>
  <font color=#123939>
    getarnter Text
  </font>
</body>
```

Abbildung 2. *Slice and Dice*

Listing 4. *MIME is Money*

```
------=_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>
```

```
Nations in a 19-page letter to
Secretary-General Kofi Annan
written in Arabic>
```

Natürlich ist es nicht im Interesse des Spammers, dass sie anstelle des Spams die Nachricht lesen. Deshalb umfasst er den Text mit < und >, um ihn nicht auf der Anzeige erscheinen zu lassen.

Der Titeltrick

Ein weiterer Trick um NoSpam-Text in Mails einfließen zu lassen besteht darin ihn in `<title></title>`-Tags zu fassen, da diese ordentlich analysiert werden, jedoch nicht angezeigt werden, da der Titel der Mail im Betreff steht.

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

Das Minifenster

Das *scrolling marquee tag* macht es möglich einen nicht unerheblichen Text (hier NoSpam) in einem sehr kleinen Teil der Nachricht zu verstecken. In folgendem Beispiel ist der gesamte Text in einem 8 x 8 Pixel großen Fenster untergebracht, also fast nicht erkennbar (siehe Abbildung 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>
```

Honey, I shrunk the font

Mittlerweile existieren immer mehr Spamfilter auf der Basis verteilter Netze, bei denen nur ein Nutzer eine Email als Spam identifiziert, diese an einen Server schickt der die Checksumme der Mail dann als Spam in eine Spamdatenbank aufnimmt. Um diese Art Spamfilter auszutricksen benutzen Spammer eine zufällig generierte Zeichenkette, um die Checksum zu verändern, so dass die Mails bei einem Checksum-Vergleich nicht mehr als mit dem gleichen Inhalt identifiziert werden können. Diese Zeichenkette sieht dann etwa so aus:

```
<font size="1" color="#FFFFFF">
  Zufälliges Wort in GROSSBUCHSTABEN
  Länge von 1 bis 22 Zeichen
  TSUTHRXJKVUVBECP </font>
```

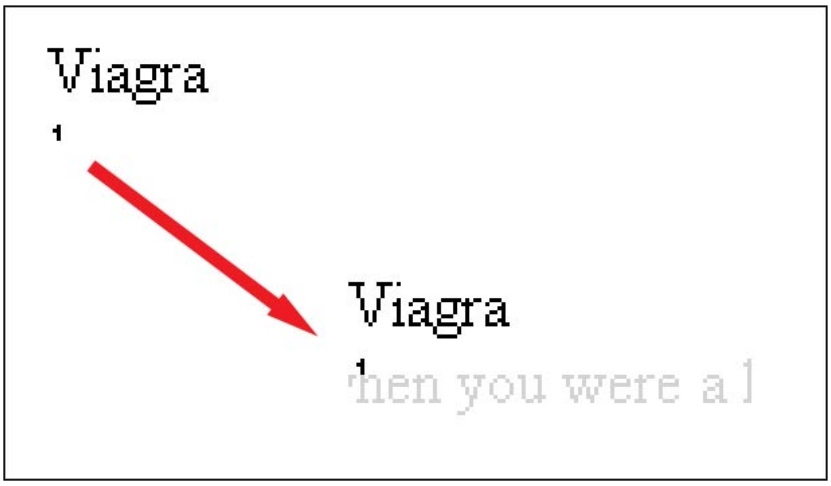


Abbildung 4. *Mini Marquee*

Verschleierte URLs

Eine weitere Möglichkeit Spam zu identifizieren besteht darin die URLs, die in der Mail enthalten sind zu überprüfen. Ein Großteil der Spammails enthält mindestens einen Link zu einer URL unter der der Spammer die angebotene Ware anbietet. Erstellt man nun eine Blacklist basierend auf diesen URLs, so wird eine Mail, die zu dieser URL linkt, als Spam eingestuft. Natürlich missfällt dies den Spammern, weshalb sie nach Möglichkeiten suchen URLs derart zu verändern, dass ein Filter sie nicht erkennt, wobei der Link aber trotzdem funktionieren muss.

Enigma und Ultra

URLs werden normalerweise für Menschen in lesbarer Form dargestellt. Der HTML-Standard und somit die Browser unterstützen jedoch noch weitere Formen der Darstellung. Ein Spammer hat vier Möglichkeiten die URL zu verlinken; erstens: er stellt sie als Dezimalzahl dar, zweitens: er stellt sie als Hexadezimalzahl dar, drittens: er stellt sie als Oktalzahl dar und viertens: er benutzt das %-Zeichen, welches die gleiche Bedeutung wie die entsprechende Hexadezimalzahl hat.

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

Ein guter Spam-Filter erkennt auch solche Links und vergleicht sie mit denen aus der Blacklist.

Bogus Login

Ein selten benutztes Feature von URLs ist die Syntax `http://benutzer@host/`(die übliche Form ist `http://host/`). Spammer nutzen dies nun, um URLs durch Zufallsbenutzer zu erweitern um sie nicht vergleichbar zu machen. Im folgenden Beispiel wird nicht zur Seite *www.microsoft.com* verlinkt, sondern zu der Seite mit der umgerechneten IP-Adresse `3631052355`.

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

Der username ist hier *www.microsoft.com* und wird vollkommen ignoriert, da er nicht existiert.

Internet Exploiter

Ein ärgerlicher Bug in Microsofts populärem Internet Explorer (patch unter: *http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-004.asp)* ermöglicht es Spammern nicht nur wie oben gezeigt zu einer Website zu verlinken, sondern sie auch noch in der Statusbar des IE legitimiert erscheinen zu lassen.

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

Wie oben verlinkt auch diese URL zur Seite http://`3631052355`/, zeigt im Email-Programm, wie auch in der Statusbar jedoch *www.microsoft.com* an. In diesem Beispiel haben wir uns gleich drei Dinge zu Nutze gemacht: 1. verschleierte Spammer-Seite, 2. bogus login, 3. Benutzung eines Exploits.

Listing 5. *Script Writer*

```
<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%20CONTENT
  %3D%22Sat%2C%201%20Jan%202000%2000%3A00%3A00%20GMT%22
  %3E%0D%0A%3CMETA%20HTTP-EQUIV%3D%22Pragma%22%20CONTENT%3D
  %22no-cache%22%3E%0D%0A%3C/HEAD%3E%0D%0A%3CFRAMESET%20
  ROWS%3D%22100%25%2C0%2220FRAMEBORDER%3DNO%20BORDER%3D
  %220%"; function SetNewWords(){ var NewWords; NewWords =
  unescape(Words);document.write(NewWords);} SetNewWords();
// --></SCRIPT></HEAD><BODY></BODY></HTML>
```

Listing 6. *WYSI nicht WYG*

```
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>
```

Javascript Tricks

Und als wenn all diese Tricks nicht schon genug wären benutzen Spammer ausserdem noch Javascript um ihre Mails schwerer bzw. unlesbar für Email-Programme zu machen.

Scriptschreiber

Bei dieser Methode ist die Mail bis sie geöffnet wird durch eine einzige Variable verschlüsselt. Hierbei hofft der Spammer, dass der Filter nicht dem Link folgt und die Mail somit auch nicht als Spam erkennt.

WYSI nicht WYG (what you see is not what you get)

Ein weiterer Javascript Trick ist mit dem Verschleiern von URLs verwandt. Hierbei wird der Text, der in der Statusbar erscheint sobald der Mauszeiger über dem Link ist ausgetauscht (siehe Listing 6).

Der Empfänger glaubt eine bestimmte Seite zu öffnen, während er eine vollkommen andere besucht.

Ironie der ganzen Sache

Die Ironie hierbei liegt in der Tatsache, dass, je mehr ein Spammer versucht eine Mail so zu verändern, dass sie nicht mehr von Filtern als Spam erkannt wird, desto eher sie als solcher identifizierbar ist. Denn, welcher normale User versendet schon eine Mail unter Benutzung solcher Sachen wie dem *Schwarzen Loch*, *unsichtbarer Tinte* oder dem *Microdot*? ■

URLs verschleiern

Hier die vier oben schon erwähnten Methoden:

- Erstens: Herausfinden der IP-Adresse der Website (z.B. mit dem Kommando `host`), danach umwandeln in eine Dezimalzahl mit Hilfe der Formel: (X3*256^3) + (X2*256^2) + (X1*256) + X0, wobei die IP-Adresse X3.X2.X1.X0 ist.
- Zweitens: Umwandeln der durch die erste Methode ermittelten Zahl ins Hexadezimalformat, danach ein `0x` voranstellen.
- Drittens: Umwandeln der einzelnen Elemente ins Oktalsystem, dann jedem Element eine `0` voranstellen.
- Viertens: Mit Hilfe der ASCII-Tabelle den Wert jedes einzelnen Zeichens herausfinden, danach umwandeln ins Hexadezimalsystem und anschliessend ein `%` voranstellen und in eine Lückenlose Zeichenkette schreiben.