Online Advertising: The Good, The Bad, and The Ugly

Yi-Min Wang
Group Manager & Principal Researcher
Cybersecurity & Systems Management Group
Microsoft Research, Redmond
The Traffic-to-Money Converter & The STC Generation

• The Traffic-to-Money Converter

  Traffic ➔ Traffic-to-Money Converter ➔ Money

• \( STC = \text{Search, Type, and Click} \)
  – The STC generation collectively generates a lot of web traffic

• Traffic-to-money converter for the web
  – Mass-market ads syndication programs
  – Mass-market exploit affiliate programs
The STC Traffic

**The Good**

- **Search**
  - Search Ads
  - Search Engine

- **Type**
  - Typo Domain Ads-Portal Page

- **Click**
  - Advertisement Syndication or Exploit Affiliate Programs

**The Ugly**

- Mass-Market Advertisement Syndication Program #1
- Spam Ads-Portal Page

**The Bad**

- Ads by G/Y/M
- Non-Merchants
- Hacked Ads
- Merchants
- Spyware Vendors

Target web pages
Web Analytics & Advertising Syndication

The Good

Mass-Market Advertisement Syndication Program #1

Target web pages

Ads by G/Y/M Non-Merchants Merchants
Where’s The Bug?

1x1 transparent-gif web bug magnified
A **Web bug** is an object that is embedded in a web page or e-mail and is usually invisible to the user but allows checking that a user has viewed the page or e-mail. One common use is in e-mail tracking. Alternative names are **Web beacon**, **tracking bug**, **pixel tag**, and **clear gif**. In honor of Hewlett Packard Chairwoman Patricia C. Dunn, Web Bugs are sometimes known as **PattyMail**[1]. They were famously used to track boardroom leaks in the **HP Pretexting Scandal** of 2006.
http://WhatIsMyIP.com/
http://ip-address.domaintools.com/

<table>
<thead>
<tr>
<th>IP Information</th>
<th>Tools</th>
<th>Location</th>
<th>Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address:</strong> 131.107.0.96</td>
<td></td>
<td><strong>Country:</strong> United States (US)</td>
<td><strong>Proxy Type:</strong> Anonymous</td>
</tr>
<tr>
<td><strong>Hostname:</strong> tide526.microsoft.com</td>
<td></td>
<td><strong>Region:</strong> Washington</td>
<td><strong>Proxy:</strong> 1.1 SEA-PRXY-02</td>
</tr>
<tr>
<td><strong>Blacklist Status:</strong> Clear</td>
<td>Ping</td>
<td><strong>City:</strong> Redmond</td>
<td></td>
</tr>
<tr>
<td><strong>Remote Port:</strong> 13159</td>
<td>Traceroute</td>
<td><strong>ISP:</strong> Microsoft Corp</td>
<td></td>
</tr>
<tr>
<td><strong>Protocol:</strong> HTTP/1.1</td>
<td>DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Connection:</strong> Keep-Alive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Keep Alive:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Web Analytics: Example #1

Primary URL on Primary Domain

Secondary URL on Third-Party Domain

statse.webtrendslive.com/.../dcs.gif

Show nothing
Web Analytics: Example #2

Primary URL: http://www.aidsmeds.com/

Secondary URL on Third-Party Domain:
ssl.google-analytics.com/urchin.js
googel-analytics.com/__utm.gif
http://www.aidsmeds.com/

Secondary URL on Third-Party Domain
ssl.google-analytics.com/urchin.js
google-analytics.com/__utm.gif
Advertising Syndication

Primary URL: http://www.aids.org/factSheets/

Show small ads

Secondary URL on Third-Party Domain
pagead2.googlesyndication.com/pagead/show_ads.js

Before ads are displayed; even without clicking any ads
Potential Security and Privacy Concerns

• **Scripts executed without user permission**
  – Redirection to third-party domains happened without user knowledge

• **Not all URLs get recorded in browser history**
  – Don’t know what, when, and why

• **Many consumer machines have fixed IP addresses**
  – Like car license plate number for information highway

• **Corporate proxy IP addresses necessarily identify the company**
  – Like company logo on company vans

• **Redirected-to third-party domains can set cookies**
  – Can ID <IP address, account> pair
Traffic Cameras for the Information Highway

One camera in every 8th street corner

Coverage of Top One Million URLs

Top Syndication Servers

Googlesyndication.com
Doubleclick.net
Atdmt.com
Fastclick.net
Amazon.com
Advertising.com
Casalemedia.com
Overture.com
Domain Parking & Typo-squatting

Type

Typo Domain Ads-Portal Page

The Ugly

Advertisement Syndication or

Target web pages

Non-Merchants

Merchants
Domain Parking

Primary URL: http://VictoriasSecret.com/

Secondary URL on Third-Party Domain
apps5.ingo.com/apps/domainpark/domainpark.cgi

Show full-page ads
It used to be much uglier… (oingo.com)
Internet Real Estate Business

• Rule of thumb: every unique visitor is worth 5 cents on average
  – \$7.00 / 365 / \$0.05 = 0.38 unique visitors/ day

• How to attract traffic:
  – Generic name domains
    • Sex.com ($12 million), Diamond.com ($7.5 million), Business.com ($7.5 million in 1999), Sweatpants.com ($8,500)
  – Typo-squatting domains
    • http://VictorasSecret.com/
  – Trademark domains
    • http://www.MicrosoftPowerpoint.com/
When typo of slashdot got slashdotted...

Hi There.

You misspelled slashdot.org.

Including you, 20 miscreants have misspelled it today!

A [cricket graph](http://slashdot.org/) of the number of people who have misspelled slashdot.org over time.
Strider Typo-Patrol

• Typo generation algorithm
  – Missing-dot typos
    • wwwwSouthwest.com
  – Character-omission typos
    • MarthsStewart.com
  – Character-permutation typos
    • NYTiems.com
  – Character-replacement typos
    • DidneyWorld.com
  – Character-insertion typos
    • WashingtonPoost.com
Top Typo-squatting Domain Parking Servers

% of 2,233 Active Typos

- Oingo.com: 19%
- Domainsponsor.com: 14%
- Sedoparking.com: 3.30%
- Qsrch.com: 3.30%
- Hitfarm.com: 3.10%
- Netster.com: 2.20%
Strider URL Tracer with Typo-Patrol
http://research.microsoft.com/URLTracer

Overall, one in every four active typo domains was parked with oingo.com

One in every six active typo domains was owned by Unasi/Domaincar
For More Information

• “The Web's Million-Dollar Typos”

• “Strider Typo-Patrol”
  – [http://research.microsoft.com/URLTracer](http://research.microsoft.com/URLTracer)

• “Strider Typo-Patrol SRUTI”
  – Usenix SRUTI’06 workshop
Search Spam

Search Engine

Spam Ads-Portal Page

The Ugly

Non-Merchants  Merchants

Target web pages

Advertisement Syndication
Google search “coach handbag”

Coach Handbag - Handbags & Wallets - Compare Prices, Reviews and ...
Coach Handbag - 28 results like the COACH gray signature bag, American West Painted Pony small coach bag, COACH Signature Patchwork Shoulder Tote (Replica ...
www.nextag.com/coach-handbag/search-html - 90k - Cached - Similar pages

coach handbag
Purses e. g. As if coach handbag she had received some other flexible material. And our coach handbag bank tt in the issue of paper cloth, thin plastic or ...
coach-handbag-top.blogspot.com/ - 22k - Cached - Similar pages

eBay - coach handbag, Women's Accessories, Handbags, Fragrances ... Buy coach handbag, Women's Accessories, Handbags items on eBay. Find a huge selection of Fragrances, Vintage items and get what you want now!
search.ebay.com/coach-handbag - 114k - Cached - Similar pages

Coach Handbags Outlet | BonafideLuxury
Authentic Coach handbags outlet. Discount Coach bags, purses, wallets, belts and woman accessories.
www.bonafideluxury.com/ - 6k - Cached - Similar pages

Result Page: 1 2 3 4 5 6 7 8 9 10 Next

1. **Handbag**
   Handbag links, tips and deals at CouponMountain
   **URL:** [http://www.couponmountain.com](http://www.couponmountain.com) (Sponsored Link)

2. **Quality Bags at Wholesale Prices**
   Great deals on bags. Huge selections and amazing low prices.
   **URL:** [http://www.BagsWholesale.com](http://www.BagsWholesale.com) (Sponsored Link)

3. **Coach Handbags - Buy at DealTime.com!**
   Save time and money every time you shop! DealTime lets you compare products, prices and stores for free. Find the Web’s best prices in seconds.
   **URL:** [http://www.DealTime.com](http://www.DealTime.com) (Sponsored Link)

Related Searches:
- Discount Coach
- Handbag
- Coach Bag
- Coach Handbag
- Discount
- Coach Purse
- Coach Outlet
- Coach Handbag Outlet
- Cheap Coach Handbag
- Wholesale Coach
- Handbag
- Outlet
- Coach Handbag Purse
Italy further discount 1 minimum 5 pieces 2 discount coach handbag of paper, bags that they had physically swung her style coach handbag 3 dimensions 300 x 60mm 4 different material a lock. coach handbag Sachets are also be bluntly called a money bag is a bag coach handbag may also made of paper, bag. Factories. Many styles and coach handbag cards. A suitcase. Cheap disposable paper bags to the coach handbag sale, terms 1 minimum 5 pieces 2 payment at all. The coach handbag italian retail trade as if she had received some other coach handbag european countries and colors of nice models, ask for coach handbag use in pockets of his payment, within 12 24 hours. From coach handbag my company, they had physically swung her opponents, coach handbag meaning that is similar to the italian retail trade as coach handbag metaphorically bruised as a clutch. A murse or simply coach handbag by a lock. Sachets are england, france, italy, greece coach handbag germany, the packing list. All the buyer's purchase amount coach handbag Sale from small objects in pockets of paper, as an alternative coach handbag to putting small objects in the issue of sheets of clothing. coach handbag to buyers' requirement a clutch a purse and pakistan. coach handbag We are also be bluntly called a paper bags that is a coach handbag good reputation among bag has a famous handbag, shirt, coach handbag shorts, pants, jeans, sunglasses, dresses, shoe, watches, coach handbag sports shoes. Collection summer 2006. Available lots coach handbag of nice models, ask for shoppers, and australia. Specifications coach handbag 1 from the british so a murse or none at our products coach handbag have got a purse all a pocketbook is a purse is often coach handbag called a bag sometimes a paper as 'handbagging' her that coach handbag they had physically swung her being described in the coach handbag buyer's payment bank it in pockets of debate and other coach handbag european countries such a clutch a smaller alternative coach handbag to 30 off on the order, note after the order to confirm coach handbag the retail trade as if she had received some other flexible coach handbag material. And colors and our products have got a small coach handbag ones, for free or none at our products have got a money coach handbag and our website, our bank receipt of a bag is a convenience coach handbag for shoppers, and discussion led to large ones for the coach handbag british so a murse or for a.
無題 投稿者: payday loan 投稿日: 2006/10/23(Mon) 02:06 No.867

<a href="http://faxless-payday-loan-new.blogspot.com" >faxless payday loan</a>
<a href="http://quick-payday-loan-new.blogspot.com" >quick payday loan</a>
<a href="http://no-faxing-payday-loan-new.blogspot.com" >no faxing payday loan</a>
<a href="http://payday-advance-loan-new.blogspot.com" >payday advance loan</a>
<a href="http://bad-credit-payday-loan-new.blogspot.com" >bad credit payday loan</a>
<a href="http://instant-payday-loan-new.blogspot.com" >instant payday loan</a>
<a href="http://money-tree-payday-loan-new.blogspot.com" >money tree payday loan</a>
<a href="http://no-teletrack-payday-loan-new.blogspot.com" >no teletrack payday loan</a>
<a href="http://payday-loan-uk-new.blogspot.com" >payday loan uk</a>
<a href="http://david-yurman-jewelry-new.blogspot.com" >david yurman jewelry</a>
<a href="http://jewelry-appraiser-new2.blogspot.com" >jewelry appraiser</a>
<a href="http://jewish-jewelry-top.blogspot.com" >jewish jewelry</a>
<a href="http://baltic-amber-silver-jewelry2.blogspot.com" >baltic amber silver jewelry</a>
<a href="http://jewelry-boxes2.blogspot.com" >jewelry boxes</a>
<a href="http://zaless-jewelry-top.blogspot.com" >zaless jewelry</a>
<a href="http://tiffany-s-jewelry-new2.blogspot.com" >tiffany jewelry</a>
<a href="http://pandora-jewelry-new2.blogspot.com" >pandora jewelry</a>
<a href="http://lia-sophia-jewelry-new2.blogspot.com" >lia sophia jewelry</a>
<a href="http://kays-jewelry-new2.blogspot.com" >kays jewelry</a>
<a href="http://jareds-jewelry-new2.blogspot.com" >jareds jewelry</a>
<a href="http://jared-galleria-new2.blogspot.com" >jared galleria</a>
<a href="http://gordons-jewelry-new2.blogspot.com" >gordons jewelry</a>
<a href="http://friedmans-jewelry-new2.blogspot.com" >friedmans jewelry</a>
<a href="http://brighton-jewelry-new2.blogspot.com" >brighton jewelry</a>
<a href="http://coach-handbag-top.blogspot.com" >coach handbag</a>
<a href="http://gucci-handbag-new.blogspot.com" >gucci handbag</a>
<a href="http://replica-handbag-new.blogspot.com" >replica handbag</a>
<a href="http://prada-handbag-new2.blogspot.com" >prada handbag</a>

http://coach-handbag-top.blogspot.com/
Redirection Spam

Primary URL: http://coach-handbag-top.blogspot.com/

Redirect to full-page ads; cloaking

Secondary URL on Third-Party Domain
http://www.topsearch10.com/search.php?aid=56979...
Spam Detection

• **Content-based approach**
  – Information retrieval-based ranking
  – Applied to too many fake pages that are never shown to any users (i.e., cloaking)

• **Behavior-based approach**
  – Strider SearchMonkeys: mimicking human browsing in full fidelity
  – Comment-spam hunting, cloaking detection, tracking redirection to known-spammer domain, etc.

  – *Turn search spam problem into system security problem*
Strider Search Ranger System

1. Strider URL Tracer
   - Primary-URL page
   - Third-party domain page
   - Third-party domain page

2. Search Monkeys running actual browsers
   - Redirection report

3. Redirection Spam Analyzer
   - Known-bad signatures
   - Unclassified URLs grouped & ranked by redirection domains

4. Spam Verifier
   - Confirmed spam URLs & redirection domains

- Search engines
- Spam suspects URLs
- Spam Hunters
- Spammed forums
Spammer-Targeted Categories

- Drugs: 30.8%
- Adult: 14.2%
- Gambling: 8.9%
- Ringtone: 27.5%
- Money: 2.7%
- Accessories: 7.6%
- Travel: 7.8%
- Cars: 9.7%
- Furniture: 3.3%
- Music: 3.9%
- Average: 11.6%

Per-Category Spam Percentage Density DCG/Max
Top Spam Doorway Domains

<table>
<thead>
<tr>
<th>Domain</th>
<th># of Spam Appearance</th>
</tr>
</thead>
<tbody>
<tr>
<td>blogspot.com</td>
<td>493</td>
</tr>
<tr>
<td>netscape.com</td>
<td>396</td>
</tr>
<tr>
<td>hometown.aol.com</td>
<td>296</td>
</tr>
<tr>
<td>oas.org</td>
<td>242</td>
</tr>
<tr>
<td>hometown.aol.de</td>
<td>225</td>
</tr>
<tr>
<td>home.aol.com</td>
<td>218</td>
</tr>
<tr>
<td>freewebs.com</td>
<td>207</td>
</tr>
<tr>
<td>blogstudio.com</td>
<td>178</td>
</tr>
<tr>
<td>maxpages.com</td>
<td>172</td>
</tr>
<tr>
<td>usaid.gov</td>
<td>150</td>
</tr>
<tr>
<td>blogsharing.com</td>
<td>131</td>
</tr>
<tr>
<td>forospace.com</td>
<td>124</td>
</tr>
<tr>
<td>blog.hlx.com</td>
<td>123</td>
</tr>
<tr>
<td>oas.org</td>
<td>110</td>
</tr>
</tbody>
</table>

Total: 3,882
Spam Percentages

At least 3 out of 4 were spam!
Top .gov/.edu Doorway Domains

![Bar Chart]

- usaid.gov: 150
- mit.edu: 63
- gatech.edu: 54
- ucsd.edu: 35
- tsmu.edu: 34
- cu Denver.edu: 32
- uconn.edu: 27
- evansville.edu: 25
- harvard.edu: 24
- virginia.edu: 22
- apu.edu: 18
- ne u.edu: 17
- dot.gov: 16
- uchicago.edu: 15
- washington.edu: 13

# of Spam Appearances
Universal Redirectors

- rds.yahoo.com/_ylt=/* http://frft.networkforbestever.org/ps/
- store.adobe.com/cgi-bin/redirect/n=14630?http://rme19-funny-ringtones.blogspot.com
- serifos.eecs.harvard.edu/proxy/http://pharmacy-goods.com/r/tramadol
- www.library.drexel.edu/cgi-bin/r.cgi?url=http://replica-watches.20six.co.uk
Top Redirection Domains

Number of Spam Appearances:
- payseed.net: 1156
- topsearch10.com: 1022
- topmeds10.com: 879
- searchadv.com: 649
- sixxx.info: 543
- rightfinder.net: 398
- a3b4.info: 356
- topmobile10.com: 334
- yourfastfind.org: 326
- arearate.com: 309
- find-more.biz: 308
- yourfreevids.com: 289
- webresources.info: 266
- webresources.info: 260
- webresources.info: 258
Malicious Websites

Search
- Search Engine
  - Spam Ads-Portal Page

Type
- Typo Domain Ads-Portal Page
  - Exploit Affiliate Programs
    - Spyware Vendors

Target web pages

Non-Merchants

Hacked Ads

Merchants

The Bad
Google search “pain killer”

Pain Killer Comparison Chart
A summary chart of pain killers, ranked by effectiveness.
www.vaughns-1-pagers.com/medicine/painkiller-comparison.htm - 24k -
Cached - Similar pages

pain killer, inc.
A "pretty damned entertaining" poetry, story, and article webzine by a "handful of self-loving misanthropes".
www.painkiller.org/ - Similar pages

pain killer
search tips: if you search pain killer, please see this keywords: pain killer pain killer
addiction prescription pain killer picture of pain killer narcotic ...
www.blogigo.de/pain_killer - 8k - Cached - Similar pages

Analgesic - Wikipedia, the free encyclopedia
"Painkiller" redirects here. For other uses, see Painkiller (disambiguation). An
analgesic (colloquially known as a painkiller) is any member of the diverse ...
en.wikipedia.org/wiki/Analgesic - 31k - Cached - Similar pages

Buy Pain Killer Online
Pain killer Free FedEx Shipping
All orders processed. USA Pharmacy
SafeUSmeds.com

Pain Killer
Pain Relief in Just Minutes! Cox-2
Inhibitor. Must Try. Guaranteed.
www.1800WellMed.com/Pain

Buy Pain Killer Online
Pain killer Free FedEx Shipping
1-800 Support. All orders processed
USrxLeader.com

Pain Killer at Amazon.com
Buy books at Amazon.com and save.
Qualified orders over $25 ship free
Amazon.com/books
Malicious Spam

Primary URL: http://www.blogigo.de/pain_killer

Vulnerability exploits;
Sometimes window closed

Secondary URL on Third-Party Domain
http://biopharmasite.info//directory.php
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Size</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/13/2006</td>
<td>12:13 PM</td>
<td>55,016</td>
<td>g0jwuyjp.exe</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:41 AM</td>
<td>134,144</td>
<td>regedit.exe</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:41 AM</td>
<td>266,752</td>
<td>winhlp32.exe</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:41 AM</td>
<td>1,004,032</td>
<td>explorer.exe</td>
</tr>
<tr>
<td>02/18/2002</td>
<td>09:23 AM</td>
<td>10,752</td>
<td>hh.exe</td>
</tr>
<tr>
<td>08/23/2001</td>
<td>04:00 AM</td>
<td>46,352</td>
<td>setdebug.exe</td>
</tr>
<tr>
<td>08/23/2001</td>
<td>04:00 AM</td>
<td>49,680</td>
<td>twunk_16.exe</td>
</tr>
<tr>
<td>08/23/2001</td>
<td>04:00 AM</td>
<td>25,600</td>
<td>twunk_32.exe</td>
</tr>
<tr>
<td>08/23/2001</td>
<td>04:00 AM</td>
<td>256,192</td>
<td>winhelp.exe</td>
</tr>
<tr>
<td>08/23/2001</td>
<td>04:00 AM</td>
<td>15,360</td>
<td>TASKMAN.EXE</td>
</tr>
<tr>
<td>08/23/2001</td>
<td>04:00 AM</td>
<td>66,048</td>
<td>NOTEPAD.EXE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 File(s)</td>
<td>1,929,928 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 Dir(s)</td>
<td>15,111,655,424 bytes free</td>
</tr>
</tbody>
</table>

C:\WINDOWS>dir /O-D system32\*.dll ; more
Volume in drive C has no label.
Volume Serial Number is 940A-8933

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Size</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/13/2006</td>
<td>12:13 PM</td>
<td>31,464</td>
<td>ipv6mons.dll</td>
</tr>
<tr>
<td>04/27/2005</td>
<td>11:48 AM</td>
<td>3,584</td>
<td>fitlib.dll</td>
</tr>
<tr>
<td>08/03/2004</td>
<td>04:00 AM</td>
<td>64,240</td>
<td>vmsrvc.dll</td>
</tr>
<tr>
<td>08/03/2004</td>
<td>04:00 AM</td>
<td>53,248</td>
<td>mrxmlpcnp.dll</td>
</tr>
<tr>
<td>08/03/2004</td>
<td>04:00 AM</td>
<td>76,288</td>
<td>vpc-s3.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>87,304</td>
<td>rdpdd.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>75,912</td>
<td>rdpswx.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>56,832</td>
<td>wzdclg.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>189,440</td>
<td>wuauceng.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>264,704</td>
<td>wzcsvc.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>86,016</td>
<td>xactsrv.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>13,312</td>
<td>wship6.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>23,552</td>
<td>wzcsapi.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>17,408</td>
<td>wtsapi32.dll</td>
</tr>
<tr>
<td>08/29/2002</td>
<td>02:46 AM</td>
<td>545,792</td>
<td>wsecedit.dll</td>
</tr>
</tbody>
</table>
1. **Mandeville Chevrolet**
   Offers new and preowned cars and trucks.
   Category: Massachusetts > North Attleboro > Automotive Dealers > Chevrolet
   www.mandevillechevrolet.com - More from this site
Exploit failed... Click here to install...
Bofra exploit hits our ad serving supplier

Some Reg readers may be infected

By Team Register → More by this author
Published Sunday 21st November 2004 16:18 GMT

Get The Register’s new weekly newsletter for senior IT managers delivered to your inbox, click here.

Important notice Early on Saturday morning some banner advertising served for The Register by third party ad serving company Falk AG became infected with the Bofra/IFrame exploit. The Register suspended ad serving by this company on discovery of the problem.

Bofra/IFrame is a currently unpatched exploit which affects Internet Explorer 6.0 on all Windows platforms bar Windows XP SP2. If you may have visited The Register between 6am and 12.30pm GMT on Saturday, Nov 20 using any Windows platform bar XP SP2 we strongly advise you to check your machine with up to date anti-virus software, to install SP2 if you are running Windows XP, and to strongly consider running an alternative browser, at least until Microsoft deals with the issue.

We have asked Falk for an explanation and for further details of the incident, and pending this we do not intend to restart ad-serving via the company. Falk will, we understand, be making a statement regarding the matter on Monday.
Hacked Ad Seen on MySpace Served Spyware to a Million - Security Fix - Microsoft Internet Explorer

Address: http://blog.washingtonpost.com/securityfix/2006/07/myspace_ad_served_adware_to_m.html

Pop-up blocked. To see this pop-up or additional options click here...

NEWS | POLITICS | OPINIONS | SPORTS | ARTS & LIVING

SEARCH:

washingtonpost.com > Technology

Subscribe to The Post

RECENT POSTS
- Microsoft to Issue Six Security Patches Next Week
- Report: Phishers Hooking Fewer (But Fatter) Victims
- 'Supercerts' Aim to Highlight Legit Web Sites
- Microsoft Warns of More "Zero-Day" Exploits
- 180Solutions/Zango to Pay $3M to Settle FTC Suit

SECURITY FIX

Brian Krebs on Computer Security

About This Blog | Archives | XML RSS Feed (What's RSS?)

Hacked Ad Seen on MySpace Served Spyware to a Million

An online banner advertisement that ran on MySpace.com and other sites over the past week used a Windows security flaw to infect more than a million users with spyware when people merely browsed the sites with unpatched versions of Windows, according to data collected by iDefense, a Verisign company.
Where Did This Come From?

DANGER: SPYWARE

Full system scan results:
- 3 Spyware infections
- 27 Spyware tracks
- 95 Adult-oriented websites tracks
- 3 Programs with probable keylogging activity

Windows recommends you the following software products to keep your PC safe:

for as low as $59.95
demo direct download

for as low as $59.95
demo direct download
Honeypot versus HoneyMonkey

- Malicious or Hacked Client
  - Malicious Network Packets
    - IDS
    - Firewall
    - Server Process
    - Server-Side Vulnerability
  - Honeypot
- Malicious or Hacked Web Server
  - Malicious HTTP Response
    - HTTP Request
    - Blacklist
    - Browser
    - Client-Side Vulnerability
  - Takedown
  - Browser
  - Honey Monkey
  - ≠ Spider Crawler
HoneyMonkey Blackbox Exploit Detection

Other Content Provider

Content Provider

Obfuscated Java Scripts

Third-Party URLs

Malicious Scripts

Malware Installation

FDR

URL Tracer

Virtual Machine

Browser

Exploit Provider
## Density of Malicious Websites

<table>
<thead>
<tr>
<th></th>
<th>Suspicious List</th>
<th>Popular List</th>
</tr>
</thead>
<tbody>
<tr>
<td># URLs scanned</td>
<td>16,190</td>
<td>1,000,000</td>
</tr>
<tr>
<td># Exploit URLs</td>
<td>207 (1.28%)</td>
<td>710 (0.071%)</td>
</tr>
<tr>
<td># Exploit URLs After Redirection</td>
<td>752 (263%)</td>
<td>1,036 (46%)</td>
</tr>
<tr>
<td>SP2-to-SP1 Ratio</td>
<td>204/688 = 0.30</td>
<td>131/980 = 0.13</td>
</tr>
</tbody>
</table>
Infection Rate Heavily Depends on Patch Level
(May~June 2005)

<table>
<thead>
<tr>
<th></th>
<th># Exploit URLs</th>
<th># Exploit Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>752</td>
<td>288</td>
</tr>
<tr>
<td>WinXP SP1-UP</td>
<td>688</td>
<td>268</td>
</tr>
<tr>
<td>(UP=UnPatched)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WinXP SP2-UP</td>
<td>204</td>
<td>115</td>
</tr>
<tr>
<td>WinXP SP2-PP</td>
<td>17</td>
<td>10</td>
</tr>
<tr>
<td>(PP=Partially Patched)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WinXP SP2-FP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(FP=Fully Patched)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Site Ranking by Number of Hosted Exploit URLs

toolbarpartner.com
.edu: hacked course bulletin board

Site ranking based on the number of hosted exploit URLs
Exploit Pages Organized by Account Names

- http://ToolbarPartner.com
- /adverts
- /romas
  - /index.html
  - /index2.html
  - /page1.htm
- /west
  - /index.html
  - /index2.html
  - /page1.htm
- /0MhNSYF
  - /index.html
  - /index2.html
  - /page1.htm
- /x-web
  - /index.html
  - /index2.html
  - /page1.htm

Pretend to be an Advertisement Syndicator
Zero-Day Exploit Detection
Vulnerabilities exploited before patch was released

- Used to be an ad-hoc & manual process that relied heavily on external finders
- HoneyMonkey turned it into a systematic & automatic process that allows Microsoft to lead the battle
  - HoneyMonkey running on fully patched WinXP SP2 VM constantly scanning the 752 exploit URLs
- The Javaprxy.dll zero day
  - Early July, 2005: detected the first zero-day exploit URL within 2.5 hours of scanning \(\Rightarrow\) confirmed to be the first in-the-wild exploit URL reported to MSRC
  - 26 of the 752 URLs “upgraded” to the javaprxy exploit
    - 25 of them generated third-party URLs to an unknown exploit provider site: `http://82.179.166.2/[8 random chars]/test2/iejp.htm`
  - Takedown notices sent \(\Rightarrow\) most, but not all, of the 25 URLs stopped exploiting javaprxy
Observations

• Monitoring easy-to-find exploit URLs is effective
  – Zero-day exploits need to connect to popular pages

• Monitoring content providers with well-known URLs is effective (because they cannot move)
  – Exploit providers can move and randomize URLs

• Monitoring highly ranked and advanced exploit URLs is effective
  – First detected zero-day exploit URL belongs to the #9 site
  – 7 of the top 10 sites upgraded (by connection counts)
  – Nearly half of the SP2-PP exploit URLs upgraded
HoneyMonkey Anti-Exploit Process

Top $O(10^8)$ URLs (ranked by click-through counts, etc.)

Search Engine Crawler

$O(10^{10})$ pages on the Web

O(10^4) exploit URLs

HoneyMonkey Network of O(10^2) PCs running unpatched VMs

HoneyMonkey Network of O(10^1) PCs running partially- or fully-patched VMs

O(10^1) zero-day exploit URLs

Spam URLs from Strider Search Ranger

SPAM URLs

SPIM URLs

Browser Blocking

Search Result Blocking

Corporate Proxy Blocking

ISP Blocking

Anti-Spyware & Anti-Virus

Security Response Center

Legal Takedown

Anti-Spyware & Anti-Virus Security Response Center

ISP Blocking

Corporate Proxy Blocking

Search Result Blocking

Browser Blocking

SPAM URLs

SPIM URLs
Summary

• A common redirection-based framework for analyzing:
  – Web Bugs
  – Advertising Syndication
  – Typo-squatting
  – Redirection Spam
  – Malicious websites

• Automated web patrol with Strider monkeys
  – Analyzing individual web pages with known-bad signatures
  – Analyzing groups of web pages to discover new signatures