

# Next generation web scanning New Zealand: A case study

First presented at KIWICON III 2009

By Andrew Horton  
aka urbanadventurer



# NZ Web Recon

Goal: To scan all of New Zealand's web-space to see what's there.

Requirements:

- Targets
- Scanning
- Analysis

Sounds easy, right?



# Targets



# Targets

What does 'NZ web-space' mean?

It could mean:

- Geographically within NZ regardless of the TLD
- The .nz TLD hosted anywhere
- All of the above

For this scan it means, IPs geographically within  
NZ

# Finding Targets

We need creative methods to find targets



# DNS Zone Transfer

```
:~$ host -al nz
nz AXFR record query refused by ns2.dns.net.nz
nz AXFR record query refused by ns3.dns.net.nz
nz AXFR record query refused by ns7.dns.net.nz
nz AXFR record query refused by ns4.dns.net.nz
nz AXFR record query refused by ns5.dns.net.nz
nz AXFR record query refused by ns1.dns.net.nz
nz AXFR record query refused by ns6.dns.net.nz
No nameservers for nz responded
:~$
:~$ dig nz axfr

; <=> DiG 9.5.1-P2 <=> nz axfr
;; global options:  printcmd
; Transfer failed.
```

# Find IP addresses on IRC and by resolving lots of NZ websites

WXNZ	58.*.*.*	Orcon	60.*.*.*	65.*.*.*	91.*.*.*
	110.*.*.*		111.*.*.*	113.*.*.*	114.*.*.*
	115.*.*.*		116.*.*.*	117.*.*.*	118.*.*.*
	119.*.*.*		120.*.*.*	121.*.*.*	122.*.*.*
SNAP	123.*.*.*		124.*.*.*	125.*.*.*	130.*.*.*
	131.*.*.*	canterbury uni	132.*.*.*	138.*.*.*	139.*.*.*
	143.*.*.*		144.*.*.*	146.*.*.*	150.*.*.*
	153.*.*.*	AUT	156.*.*.*	161.*.*.*	162.*.*.*
	163.*.*.*		165.*.*.*	166.*.*.*	167.*.*.*
Doc.govt.nz	192.*.*.*		198.*.*.*	202.*.*.*	203.*.*.*
	210.*.*.*		218.*.*.*	219.*.*.*	222.*.*.*

Handwritten notes and circled area:

- acsdatta
- Jetstream
- Telecom
- VUW otago uni
- Everything (circled around 202.\*.\*.\* and 203.\*.\*.\*)

729,580,500 IPs. More than we want to try.

# IP address blocks in the IANA IPv4 Address Space Registry

Prefix	Designation	Date	whois	Status [1]
-----	-----	----	-----	-----
000/8	IANA - Local Identification	1981-09		RESERVED
001/8	IANA			UNALLOCATED
002/8	RIPE NCC	2009-09	whois.ripe.net	ALLOCATED
003/8	General Electric Company	1994-05		LEGACY
201/8	LACNIC	2003-04	whois.lacnic.net	ALLOCATED
202/8	APNIC	1993-05	whois.apnic.net	ALLOCATED
203/8	APNIC	1993-05	whois.apnic.net	ALLOCATED
204/8	ARIN	1994-03	whois.arin.net	ALLOCATED
205/8	ARIN	1994-03	whois.arin.net	ALLOCATED
206/8	ARIN	1995-04	whois.arin.net	ALLOCATED
207/8	ARIN	1995-11	whois.arin.net	ALLOCATED
208/8	ARIN	1996-04	whois.arin.net	ALLOCATED
209/8	ARIN	1996-06	whois.arin.net	ALLOCATED
210/8	APNIC	1996-06	whois.apnic.net	ALLOCATED
211/8	APNIC	1996-06	whois.apnic.net	ALLOCATED

This list has 663,255,000 IPs. More than we want to try.



# Failed methods to find targets

- DNS Zone transfers from top level domain name servers
- Learn IP address ranges for well known national websites and networks
- All IP addresses allocated to APNIC (Asia Pacific NIC)

We need new methods to find IP addresses and website hostnames for New Zealand

# geoipgen and the MaxMind GeoIP database

Use MaxMind's free database of IP to Country allocations

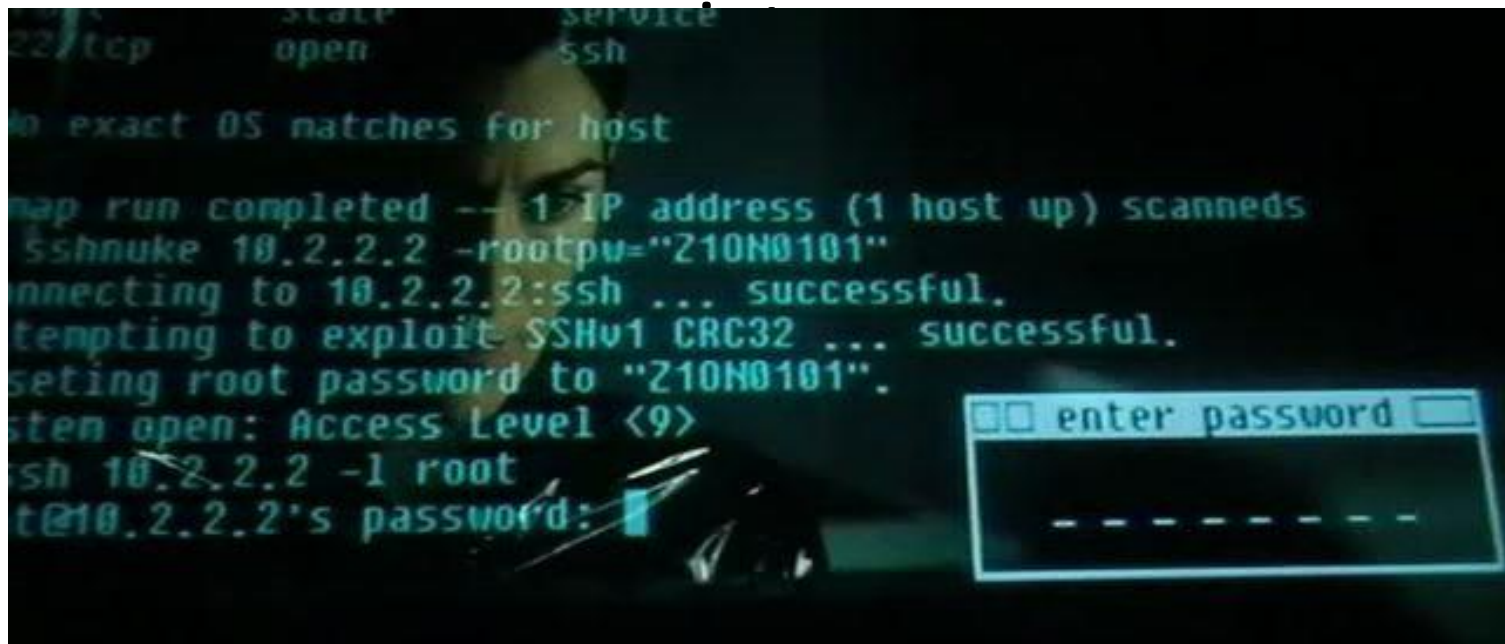
Homepage: <http://www.morningstarsecurity.com/research/geoipgen>

```
:~/projects/geoipgen-0.4$ ./geoipgen nz | head
116.93.136.27
118.90.173.125
160.4.198.233
125.238.89.114
166.83.49.86
202.160.56.150
192.86.12.9
118.149.255.218
130.217.121.198
150.206.23.55
```

Produces 6,319,348 New Zealand IP addresses

# Scanning for TCP Port 80 with nmap

Find the 75,964 web servers among 6 million IPs



```
nmap -i ./iplist -P0 -sT --open -n -p 80 -oG iplist.gnmap.log
```

# Reverse Resolving IP addresses

Use adns-tools for fast, asynchronous resolving

```
:~/projects/nzwide-whatweb$ cat iplist.port80.log | adnslogres | grep "[a-z]"  
122-57-247-79.jetstream.xtra.co.nz  
dbsys2.digiweb.net.nz  
222-152-235-159.jetstream.xtra.co.nz  
118-92-112-95.dsl.dyn.ihug.co.nz  
210-54-240-196.ipnets.xtra.co.nz  
vcenter.vmware.solarix.net.nz  
210-54-241-165.ipnets.xtra.co.nz  
118-92-189-178.dsl.dyn.ihug.co.nz  
60-234-220-15.bitstream.orcon.net.nz  
203-114-179-201.dsl.sta.inspire.net.nz  
125-239-232-161.jetstream.xtra.co.nz  
h241-245.catalyst.net.nz  
ns1.marketpulse.net.nz  
ip-118-90-29-161.xdsl.xnet.co.nz  
ip-119-47-113-133.cust.openhost.net.nz
```

31,973 IPs resolve to hostnames



```
:~/projects/nzwide-whatweb$ ./bing-ip2hosts
Usage: ./bing-ip2hosts <IP>
by Andrew Horton (urbanadventurer) www.morningstarsecurity.com
Resolve vhosts for the IP address using bing.com

:~/projects/nzwide-whatweb$ ./bing-ip2hosts 210.48.71.196
annaklekottka.com
demo.gymmaster.co.nz
dressfordialogue.com
dru.treshna.com
ignavus.net
kiwiorchid.com
newzealandtrademanual.com
nzbridgecongress.co.nz
nzcps.treshna.com
sizexchange.com
wainuipark.org
www.adrianmotel.co.nz
www.akaroabus.co.nz
www.annaklekottka.com
```



- Uses Bing search query IP parameter.
  - Example: ip:210.48.71.196
- Tested 75,964 NZ IPs found in the port scan
- Discovered 11,872 IPs are indexed by bing.com
- Found 89,265 virtual hostnames

Homepage: <http://www.morningstarsecurity.com/research/bing-ip2hosts>



```
:~/projects/nzwide-whatweb$ ./gggooglescan
Usage: ./gggooglescan [OPTION]... <QUERY>
by Andrew Horton (urbanadventurer)
-c=CC          Search within a country, eg. au, uk or nz
-d=NUM         Depth of results, 0 = 1st page, 1 = 2nd page. Default: 5
-g=IP          IP or hostname of a Google search appliance. Default: 210.55.180.157
-l=FILE        Log file, output is appended if the file already exists
-o            Only print hostnames, not urls
-v            Verbose output

:~/projects/nzwide-whatweb$ ./gggooglescan -c nz -d 2 -o kiwicon
wellington.geek.nz
wellington.geek.nz
computerworld.co.nz
computerworld.co.nz
atta.cked.me
pressf1.pcworld.co.nz
coffee.geek.nz
www.trademe.co.nz
pressf1.co.nz
www.geekzone.co.nz
```



There is a common misconception that Google scraping is no longer possible and is halted by Google's bot detection.

It is possible to search for a wide set of search terms and to retrieve a shallow set of the each result, i.e. 3 pages.

searching aaa through to zzz found 58,602 hostnames

searching every word in /usr/share/dict/words found 116,052 hostnames

126,408 unique NZ hostnames found with Google

Homepage: <http://www.morningstarsecurity.com/research/>



# DNS Zone Transfers Revisited

```
; <<>> DiG 9.5.1-P2 <<>> @dns1.canterbury.ac.nz canterbury.ac.nz axfr
; (1 server found)
;; global options: printcmd
canterbury.ac.nz.      86400   IN      SOA     dns1.canterbury.ac.nz. soa.canterbury.ac.nz. 2009111001 1
0800 3600 604800 86400
canterbury.ac.nz.      86400   IN      NS      dns1.canterbury.ac.nz.
canterbury.ac.nz.      86400   IN      NS      dns2.canterbury.ac.nz.
canterbury.ac.nz.      86400   IN      NS      pubsec.domainz.net.nz.
canterbury.ac.nz.      86400   IN      MX      10 mx1.canterbury.ac.nz.
canterbury.ac.nz.      86400   IN      MX      10 mx2.canterbury.ac.nz.
canterbury.ac.nz.      86400   IN      TXT     "University of Canterbury, Christchurch."
!webmail.canterbury.ac.nz. 86400 IN CNAME   ucatmail2.canterbury.ac.nz.
*.canterbury.ac.nz.    86400   IN      MX      10 mx1.canterbury.ac.nz.
*.canterbury.ac.nz.    86400   IN      MX      10 mx2.canterbury.ac.nz.
_sipfederationtls._tcp.canterbury.ac.nz. 86400 IN SRV 10 10 5061 sip.canterbury.ac.nz.canterbury.ac.nz.
_sip._tls.canterbury.ac.nz. 86400 IN SRV 10 10 443 sip.canterbury.ac.nz.canterbury.ac.nz.
acad-hsm40.canterbury.ac.nz. 86400 IN A 132.181.223.83
acad-lv011.canterbury.ac.nz. 86400 IN A 132.181.223.146
access.canterbury.ac.nz. 86400 IN A 132.181.106.224
accom.canterbury.ac.nz. 86400 IN A 132.181.2.10
acis.canterbury.ac.nz. 86400 IN MX 10 mx1.canterbury.ac.nz.
acis.canterbury.ac.nz. 86400 IN MX 10 mx2.canterbury.ac.nz.
www.acis.canterbury.ac.nz. 86400 IN A 132.181.190.13
www.adulteducation.canterbury.ac.nz. 86400 IN A 132.181.153.124
afis.canterbury.ac.nz. 86400 IN A 132.181.190.1
afis.canterbury.ac.nz. 86400 IN MX 10 mx1.canterbury.ac.nz.
afis.canterbury.ac.nz. 86400 IN MX 10 mx2.canterbury.ac.nz.
student.afis.canterbury.ac.nz. 86400 IN A 132.181.190.1
```

# DNS Zone Transfers Revisited

## Extracting domainnames

```
~/projects/nzwide-whatweb$ ./basedomainname
basedomainname 0.1 by Andrew Horton (urbanadventurer) www.morningstarsecurity.com
Usage: basedomainname [-h|--help][--tld|--ext|--domain|--host] [-i <input-file>]
If input-file is not specified it reads from STDIN

Examples: --tld
www.wolves.mobi => mobi, www.panda.cn => cn
Examples: --ext
www.mice.co.uk => co.uk, k.iwi.nz => iwi.nz
Examples: --domain
www.dogs.co.nz => dogs.co.nz, dev12.wlg.cats.com => cats.com
Examples: --host
www.kangaroo.com.au => www, nose.shark.int => nose

~/projects/nzwide-whatweb$ cat hostnames_combined_nz.log | ./basedomainname --domain | more
e-xpert.co.nz
e-xpert.co.nz
e-xpert.co.nz
e-xpert.co.nz
007films.com
01b.co.nz
01.co.nz
01dev.co.nz
01.net.nz
021builder.co.nz
jordansurfshapes.co.nz
021extras.com
040trainsnmodels.co.nz
0508pizza.com
0508pizzas.com
```

# DNS Zone Transfers Revisited

## Results

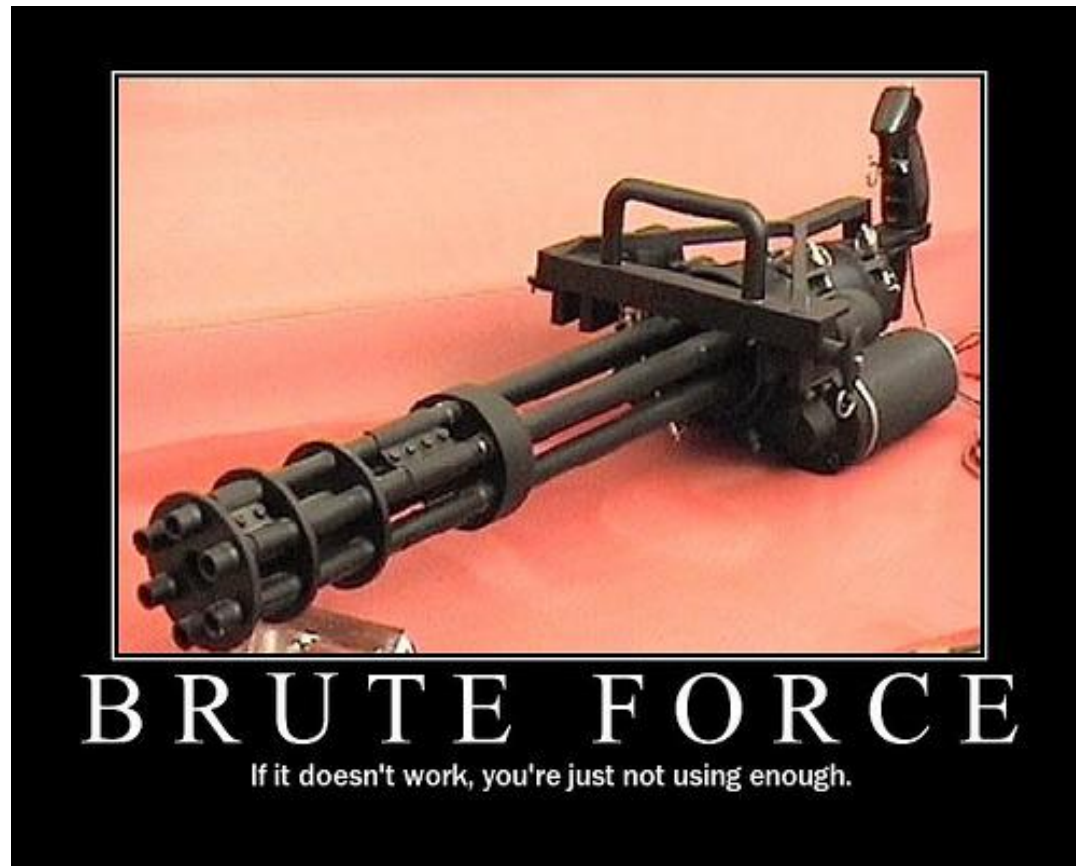
Attempt a DNS zone transfer for each domain

135,591 unique domain names were found with reverse resolving IPs, Bing, and Google scanning.

Tool: `dns-enum.pl`

Found 560,352 hosts in 70,475 domains.

# DNS Brute Forcing – Not Implemented



Guessing subdomains, eg. test.example.com,  
www2.example.com, intranet.example.com

# Final Target List

- 699,413 unique hostnames found with reverse resolving, Google, Bing and zone transfers
- Resolve the hostnames to IPs
- Keep only the hostnames with IPs in the port scanned list of 75,964 IPs found with nmap
- 75,964 IPs + 274,989 hostnames = 350,953 virtual hosts to test

# Scanning

- Targets
- Scanning
- Analysis



# Traditional Web Scanners

## Nikto and Nessus

- Time. Nikto takes too long because it guesses 1000s of URLs.
- Impolite. Nikto has a big footprint with 1000s of lines in each web servers logs and it increases web server load.
- Law. Some Nikto tests will attempt to exploit vulnerabilities so it is not suitable for use without permission.
- Information. Pretty good

## Nmap

- Time. Nmap is fast
- Impolite. Nmap is polite, it makes only a few connections
- Law. Unquestionable
- Information. Scarce

# WhatWeb

- Time. Fast
  - Polite. Doesn't trigger NIDS
  - Law. Unquestionable
  - Information. Rich
- 
- Instead of guessing URLs to identify systems, make better use of the information provided by the web server during an HTTP transaction.

Homepage <http://www.morningstarsecurity.com/research/whatweb>



# WhatWeb

Discover what powers websites by identifying:

- content management systems (CMS)
  - blogging platforms
  - stats/analytics packages
  - javascript libraries
  - HTTP servers
- 
- Written in Ruby for Linux
  - OpenSource License
  - Plugin architecture

# WhatWeb

- Passive and aggressive plugins
- Passive plugins use information from:
  - The HTML page
  - HTTP headers
  - Cookies
  - URL
- Lightweight like a search engine crawler
- A single GET / HTTP/1.0 request

# WhatWeb

- Aggressive plugins use information from:
  - Testing for URLs and identifying patterns in the HTML
  - Testing for URLs and recognising the MD5 hash of the response
  - Testing for URLs and simply noting they exist or return an HTTP status 200 code.
- Can return an exact version of a CMS, can discover installed modules or plugins
- Uses multiple HTTP requests

# WhatWeb

```
:~/projects/whatweb$ ./whatweb
WhatWeb - Discover what powers websites.
Version 0.3 by urbanadventurer (Andrew Horton)
Usage: whatweb [options] <URLs>

--input-file=FILE, -i    Identify URLs found in FILE
--aggression, -a         1 passive - on-page
                        2 polite - follow on-page links if in the extra-urls list (default)
                        3 impolite - try extra-urls when plugin matches (smart, guess a few urls)
                        4 aggressive - try extra-urls for every plugin (guess a lot of urls)
--recursion, -r          Follow links recursively. Only follows links under the path (default: off)
--depth, -d              Maximum recursion depth (default: 3)
--max-links, -m           Maximum number of links to follow on one page (default: 25)
--list-plugins, -l        List the plugins
--run-plugins, -p         Run comma delimited list of plugins. Default is to run all
--info-plugins, -I        Display information about a comma delimited list of plugins. Default is all
--example-urls, -e        Add example urls for each plugin to the target list
--colour=[WHEN],          control whether colour is used. WHEN may be `never', `always', or `auto'
--color=[WHEN]
--log-full=FILE           Log verbose output
--log-brief=FILE          Log brief, one-line output
--user-agent, -U          Identify as user-agent instead of WhatWeb/VERSION.
--max-threads, -t         Number of simultaneous threads identifying websites in parallel (CPU intensive).
Default is 5.
--help, -h                This help
--verbose, -v             Increase verbosity (recommended), use twice for debugging.
```

# WhatWeb Examples

```
:~/projects/whatweb$ ./whatweb research.elabs.govt.nz
http://research.elabs.govt.nz [200] JQuery, WordPress[2.5.1], md5[440dcb
a8246faa8a17de13d57789cc90], meta-generator[WordPress 2.5.1], server-hea
der[Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny3 with Suhosin-Patch mod_ssl/
2.2.9 OpenSSL/0.9.8g], title[Research e-Labs &raquo; web trends, open
source and technology in government], uncommon-headers[x-pingback], x-p
owered-by-header[PHP/5.2.6-1+lenny3]
```

# Passive & Aggressive Tests

```
:~/projects/whatweb$ ./whatweb www.ardentcreative.co.nz
http://www.ardentcreative.co.nz [200] Google-Analytics-GA[791888], Joomla[1.5], md5[fcb3ec0dfafae53dfdef2e991a24f1c1], meta-generator[Joomla! 1.5 - Open Source Content Management], server-header[Apache], title[Ardent Creative, Christchurch Web Design]
:~/projects/whatweb$
:~/projects/whatweb$ ./whatweb -a 3 www.ardentcreative.co.nz
http://www.ardentcreative.co.nz [200] Google-Analytics-GA[791888], Joomla[1.5,1.5.13 - 1.5.14], md5[fcb3ec0dfafae53dfdef2e991a24f1c1], meta-generator[Joomla! 1.5 - Open Source Content Management], server-header[Apache], title[Ardent Creative, Christchurch Web Design]
:~/projects/whatweb$
```

With aggressive tests it identifies the Joomla CMS version by retrieving a handful of URLs and recognising the MD5 hashes

# Aggressive Tests

## phpBB forum

```
:~/projects/whatweb$ ./whatweb forum.letterboxer.org.nz
http://forum.letterboxer.org.nz [200] md5[9cfae166b2b4dba6c6aac8e9da9613ee], phpBB[3], server-header[Apache], title[forum.letterboxer.org.nz &bull; Index page]
:~/projects/whatweb$
:~/projects/whatweb$ ./whatweb -a 3 forum.letterboxer.org.nz
http://forum.letterboxer.org.nz [200] md5[336067e5c258b61448244632b14972e7], phpBB[3,3.0.4], server-header[Apache], title[forum.letterboxer.org.nz &bull; Index page]
:~/projects/whatweb$
```

/docs/CHANGELOG.html

# Plugins available

Acclipse	Advanced-Guestbook	BlogSmithMedia	Blogger	DiBos
Drupal	EarlyImpact-ProductCart	Echo	GoAhead-Webs	Google-Analytics-GA
Google-Analytics-urchin	IIS-SiteNotFound	IIS-UnderConstruction	ISP-Config	Jquery
Joomla	Lightbox	Mailto	Mambo	Minify
Moodle	MovableType	NovellGroupwise	OSCommerce	Oce
Plesk	Plone	Prototype	Quantcast	Scriptaculous
Siemens-SpeedStream-Router	TypePad	VSNS-Lemon	Windows-SBS	WordPress
WordPressSpamFree	Antiboard	apache-default	asp-nuke	belkin-modem
bing-searchengine	citrix-metaframe	Comersus	Coppermine	Cpanel
Formmail	index-of	invision-power-board	ispCP-omega	mailsite-express
Md5	meta-generator	mnoGoSearch	oki-pbx	php-cake
phpBB	redirect-location	server-header	snom-phone	Title
toshiba-printer	uncommon-headers	Vbulletin	vp-asp	Webguard
x-aspnet-version-header	x-powered-by-header	xtra-business-hosting		



# Making Plugins is Easy

```
Plugin.define "Plone" do
  author "Andrew Horton"
  version "0.1"
  description "CMS http://plone.org"
  examples %w| www.norden.org www.trolltech.com www.plone.net www.smeal.psu.edu|

  matches [
    {:name=>"meta generator tag",
     :probability=>100,
     :regexp=>=>/<meta name="generator" content="[^>]*http:\\\\plone.org" \\/>/},

    {:name=>"plone css",
     :probability=>100,
     :regexp=>=>/(@import url|text\\css)[^>]*portal_css\\/. *plone.*css(\\|")\\/},

    {:name=>"plone javascript",
     :probability=>100,
     :regexp=>=>/src="[^"]*ploneScripts[0-9]+.js"/},

    {:name=>"div class=\"visualIcon contenttype-plone-site\"",
     :probability=>100,
     :regexp=>=>/<div class="visualIcon contenttype-plone-site"/>/},

    {:name=>"div tag, visual-portal-wrapper",
     :probability=>75,
     :regexp=>=>/<div id="visual-portal-wrapper"/>/},
  ]
end

def passive
  m=[]
  #X-Caching-Rule-Id: plone-content-types
  #X-Cache-Rule: plone-content-types
  m << {:name=>"X-Caching-Rule-Id: plone-content-types", :probability=>100 } if @meta["x-caching-rule-id"] =~ /plone-content-types/i
  m << {:name=>"X-Cache-Rule: plone-content-types", :probability=>100 } if @meta["x-cache-rule"] =~ /plone-content-types/i
  m
end

end
```



# The Scan

```
http://www.raroadeer.co.nz [200] Google-Analytics-GA[1855496], md5[427a3708cc4ebf15935c7be216a16466], server-header[Microsoft-IIS/6.0], title[Home, Raroa Red Deer -], x-powered-by-header[ASP.NET]
```

```
http://keystonecars.co.nz [200] md5[ca3fb523a65a4c4eba6fc659e9adfc9d], server-header[Microsoft-IIS/6.0], title[01博 000000000000000000000000Keystone Cars], x-powered-by-header[ASP.NET]
```

```
http://sis-ltd.co.nz [200] md5[2ac95de5ccbacc29c7388a34cdae0f01e], server-header[Apache/2.2.11 Unix) mod_ssl/2.2.11 OpenSSL/0.9.7a mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/4.4.9], title[Security Installation Services Ltd]
```

```
http://saltdesign.co.nz [200] Google-Analytics-urchin[2393723], md5[4866964c747b25b5d03e8a92e8d4f043], server-header[Apache/2.2.8 (CentOS)], title[[ : salt design : print motion interactive : ] Interactive Agency, Online Advertising, Design, Flash, Experiential, Website Design & Dvelopment - Salt Design], x-powered-by-header[PHP/5.2.8]
```

```
http://www.squirrel.co.nz [200] Google-Analytics-GA[3441576], JQuery[1.2.6], Mailto, WordPress[2.7.1], md5[1df40bcbcd85a848df6d1a99ab992fc1], meta-generator[WordPress 2.7.1], server-header[Apache/2.2.3 (Fedora)], title[Squirrel Mortgage Brokers], uncommon-headers[x-pingback], x-powered-by-header[PHP/5.2.5]
```

```
http://mail1.parkcitychurch.org.nz [200] Google-Analytics-GA[5512734], Joomla[1.0], md5[20b4445eaae00e79acdd017c9b841b99], meta-generator[Joomla! - Copyright (C) 2005 - 2007 Open Source Matters. All rights reserved.], server-header[Apache/2.2.3 (Debian) PHP/4.4.4-8+etch6], title[Park City Church - Home], x-powered-by-header[PHP/4.4.4-8+etch6]
```

```
http://www.vectorelectricity.co.nz [200] Drupal, Google-Analytics-GA[5501775], md5[011c447c73abd5bccb22ff2ec8327278], server-header[Apache], title[Auckland's Electricity Network Company - Vector Electricity]
```

```
http://125.236.210.63 [403] md5[6a2826a05dec7e657540cbfac2646285], server-header[Microsoft-IIS/6.0], title[You are not authorized to view this page], uncommon-headers[microsoftofficewebservr], x-powered-by-header[ASP.NET]
```

```
http://webmail.ezyqc.co.nz [302] md5[d41d8cd98f00b204e9800998ecf8427e], redirect-location[http://webmail.ezyqc.co.nz/login.php?Horde3=7c8491ad4277d5c73edce1938a8d3cab], server-header[Apache/2.0.46 (CentOS)], x-powered-by-header[PHP/4.4.8]
```

```
http://webmail.ezyqc.co.nz/login.php?Horde3=7c8491ad4277d5c73edce1938a8d3cab [302] md5[d41d8cd98f00b204e9800998ecf8427e], redirect-location[http://webmail.ezyqc.co.nz/imp/login.php?Horde3=8b303f25a56324b62fdf22ee5404d140], server-header[Apache/2.0.46 (CentOS)], x-powered-by-header[PHP/4.4.8]
```

```
http://webmail.ezyqc.co.nz/imp/login.php?Horde3=8b303f25a56324b62fdf22ee5404d140 [200] md5[797a
```

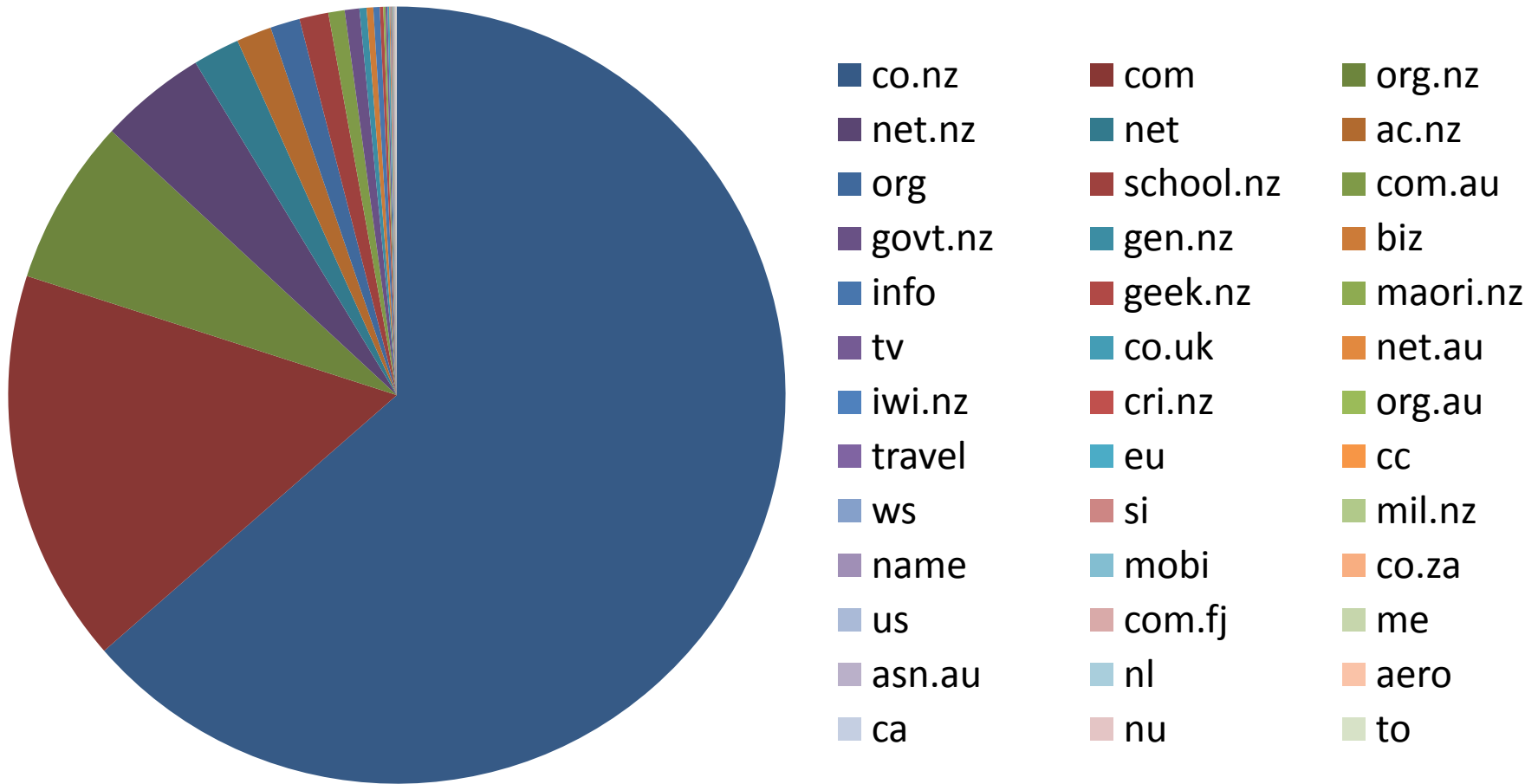
# Analysis – What did I find?

- Targets
- Scanning
- **Analysis**



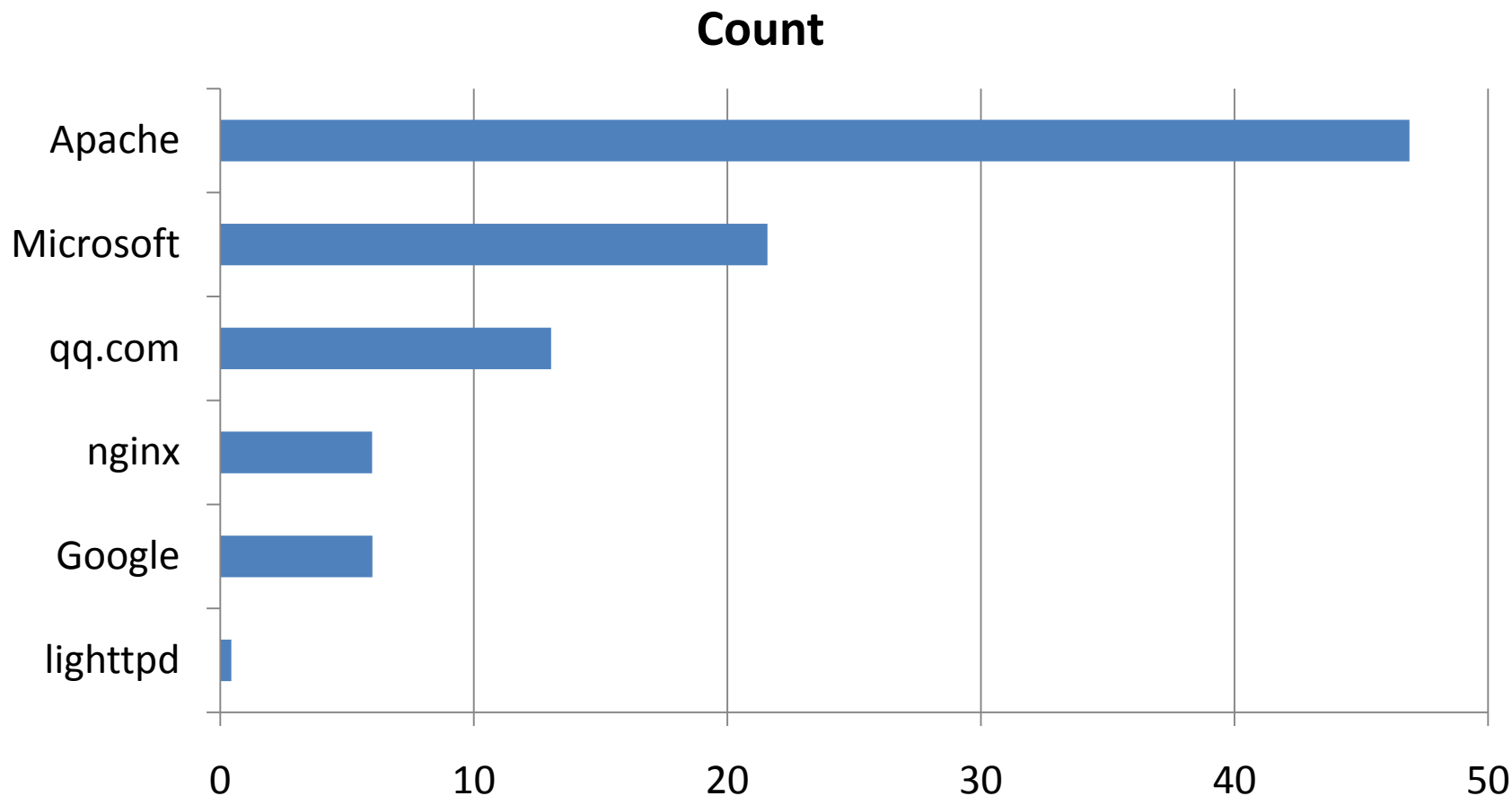
# TLDs & SLDs hosted within NZ

Extn



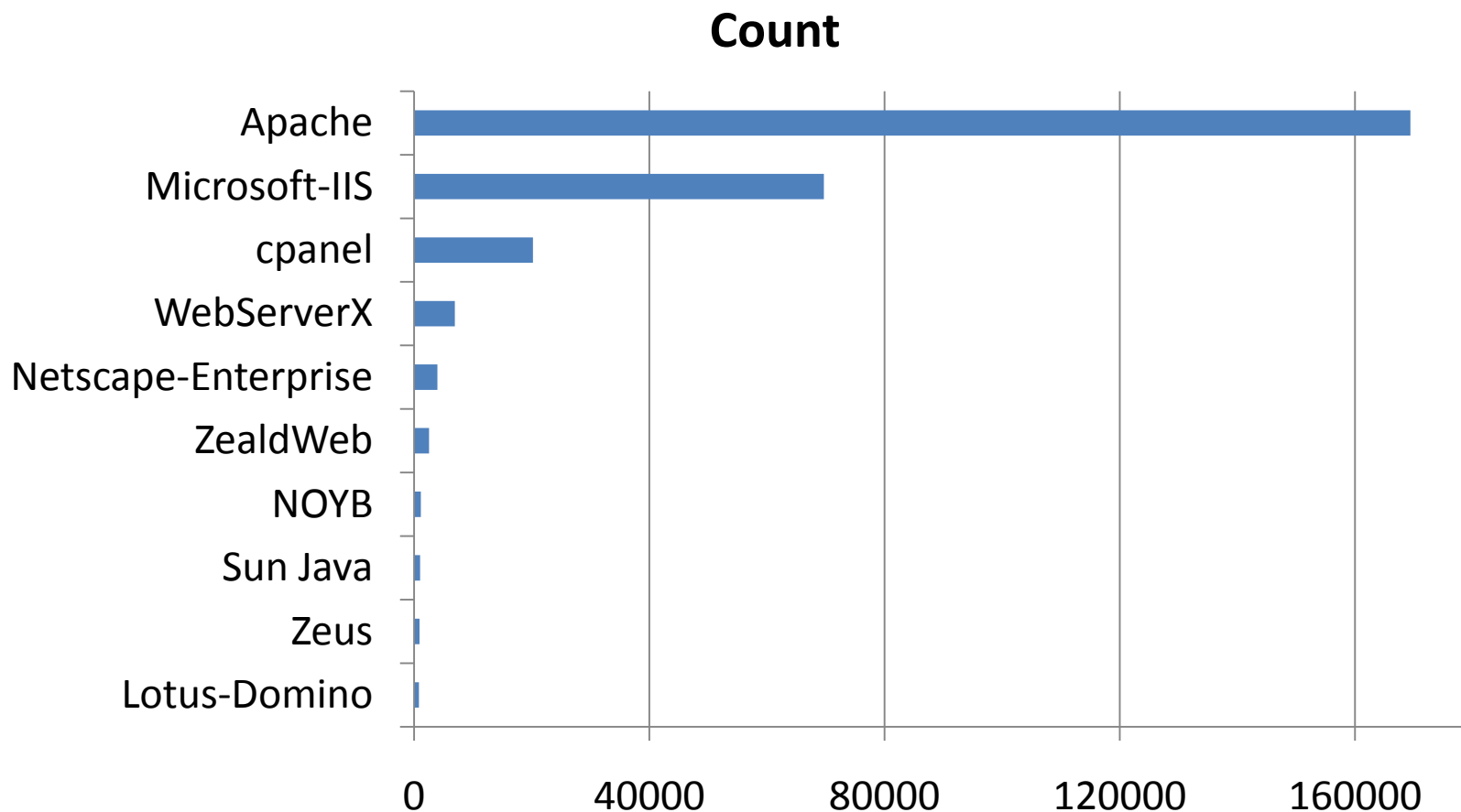
# NetCraft's Top HTTP Servers

## What I expected to find



# Top 10 HTTP Server Versions

## What I found



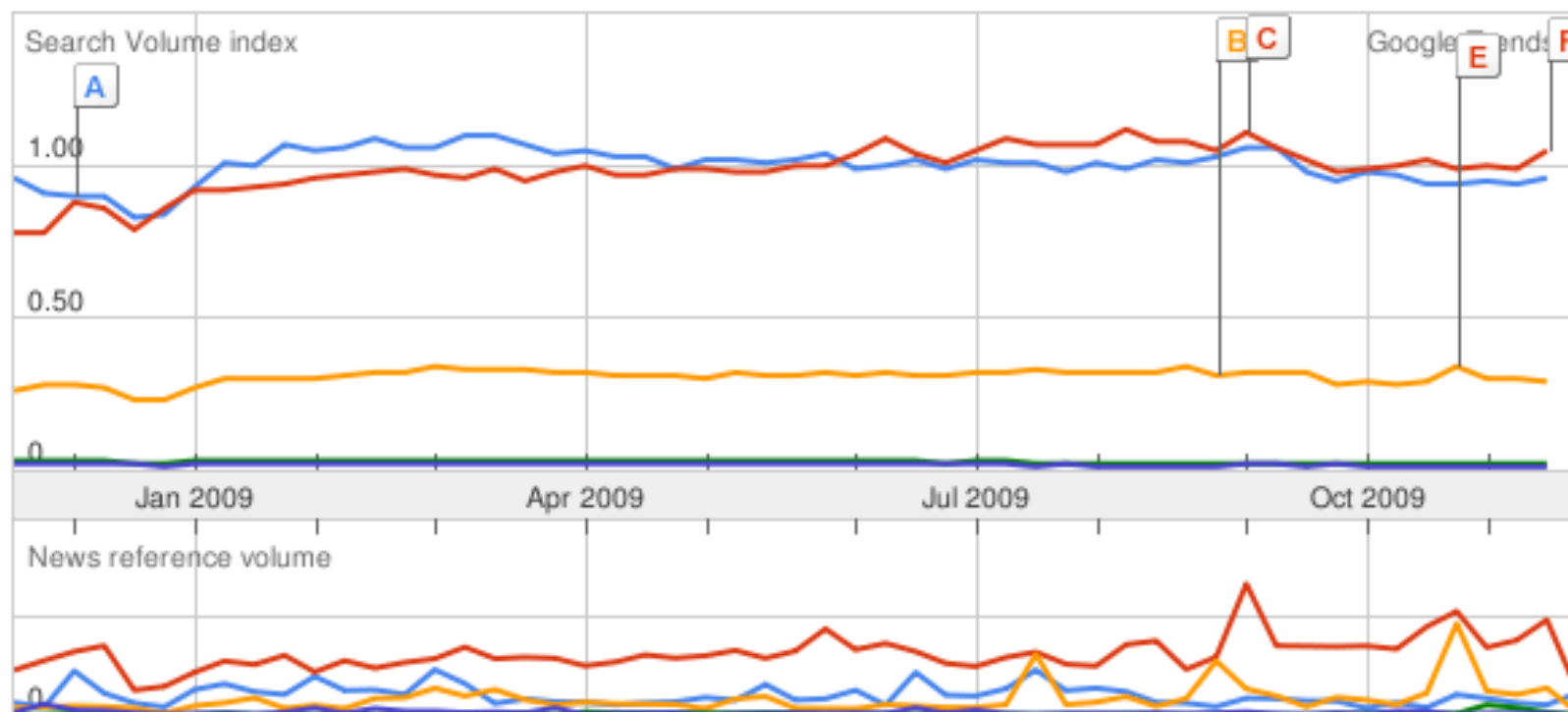
Apache, Microsoft-IIS, cpsrvd, WebServerX, cPanel, Netscape-Enterprise, ZealWeb, Apache-Coyote, Apache (FreeBSD) mod\_perl, NOYB, Sun Java System Application Server 9.1, Zeus, Lotus-Domino, cisco-IOS, nginx, UserLand Frontier, squid, Zope, RomPager, lighttpd, Roxen, Apache-AdvancedExtranetServer, Microsoft-HTTPAPI, Virata-EmWeb, Boa, WindWeb, NetPort Software 1.1, IceWarp, WDaemon, GoAhead-Webs, AkamaiGHost, EZproxy, Apache Coyote, Unknown, 2wire Gateway, GeoHttpServer, BigIP, Sun-ONE-Web-Server, This server is configured to not send version information, Resin, SonicWALL, micro\_httpd, Allegro-Software-RomPager, 4D\_WebSTAR\_S, CommuniGatePro, GFE, IBM\_HTTP\_Server, gws, Lasso, httpd, webserver, Cougar, ATR-HTTP-Server, fnord, Jetty, Oracle-Application-Server-10g, Mbedthis-Appweb, mini\_httpd, Mongrel 1.1.4, glass, Abyss, JRun Web Server, OwnServer1.0, Alpha Five Application Server, Mongrel 1.1.5, BarracudaHTTP 1.00, Web, W3MFC, Mirapoint, WebSTAR, SonicWALL SSL-VPN Web Server, sw-cp-server, EksosM, KFWebServer, thttpd, IP\_SHARER WEB 1.0, DMZGlobal Web Server 20040625 2.1, Nucleus, Apache Tomcat, Kerio MailServer 6.7.2, DirectAdmin Daemon v1.34.0 Registered to Hosting Direct Ltd - YourHOST, Clear Enterprise, Citrix Web PN Server, DManager, Web Server, Provoke Solutions Web, AV-TECH AV787 Video Web Server, AppleDiskServer-1F3010, Kerio MailServer 6.3.1, Caudium, AOLserver, SAMBAR, DPS EFT 1.5, Rumpus, Kerio MailServer 6.6.2, ExperForms 4.5 build 103, Mongrel 1.1.3, Microsoft-WinCE, Sun GlassFish Enterprise Server v2.1, Alkaline Search Engine, 4D\_WebStar\_D, Oversee Turing v1.0.0, LiteSpeed, Ili 100, HTTP Proxy, Foundry Networks, Kerio MailServer 6.7.0 patch 1, Hikvision-Webs, Sun-Java-System-Web-Server, QuasiM0d0V9.5, HTTPd-WASD, Grandstream, FileMakerPro, ADH-Web, VajraJavaWebApplicationServer, unknown, SQ-WEBCAM, SonicWALL SSL-VPN Web Server., Kerio MailServer 6.7.1, Jetty(6.1.5), Indy, FM Web Publishing, Agranat-EmWeb, WebSEAL, Viavideo-Web, PWS, Jetty(6.1.20), ghs, best-of-perl-server-1.0, WWW Server, WN, webfs, t-rex (10.2.0 release-0.0 [BuildId 11252]), RWAPM X-Server Apache, Purveyor Encrypt Export, IBM\_HTTP\_SERVER, http server 1.0, Cisco AWARE 2.0, CherryPy, Atlas, Xitami, WEB602, M5830S-HTTP-Server, DvrHttpd, Web-Server, WebGUI, VPOP3 Mail Http Server, Upkeep Http, Sun Java System Application Server 9.1\_01, Sun-Java-System, Serv-U, PicLan-IP 2.0.0 (build 151), Oracle HTTP Server Powered by Apache, netTRUST-GCN HTTPd, MS-MFC-HttpSvr, ListManagerWeb, Lancam Server, Kerio MailServer 6.5.1, Jetty(EAServer, Jetty(6.1.9), Jetty(6.1.18), DMZGlobal, Cougar 4.1.0.3930, CAMEO-httpd, A-Web, XVR Http Server, WEBrick, Sumerian202, Squeegit, RAC\_ONE\_HTTP 1.0, PRTG, Polycom SoundPoint IP Telephone HTTPd, Orion, hi, debut, YTS, Webserver Faster Higher, Webserver, UltiDev Cassini, uc-httpd 1.0.0, Twisted, Techno Vision Security System Ver. 2.0, Sun-Java-System-Web-Proxy-Server, Stronghold, Strategi HTTPD V1R9M6, PasteWSGIServer, OpenCms, Noelios-Restlet-Engine, Niagara Web Server, Kerio MailServer 6.7.0, Kerio MailServer 6.5.0 patch 1, Kerio MailServer 6.4.1 patch 1, Jetty(6.1.x), IWeb, Ipswitch-IMail, InetPowerServer, igfe, HyNetOS, http server, Hiawatha v6.10, GXC, FTGate 6.2.003, FirstClass, eHTTP v2.0, dynamic.wellingtonnz.com, dynamic.beehive.govt.nz, DSLG WEB SERVER, CPWS, Caplin Liberator, Bomgar, BIG-IP, AllegroServe, WYM, WhatsUp, Ipswitch 1.0, WebSphere Application Server, Web Crossing, Vivotek Network Camera, Video server, VB, Varnish, Uicom, TwistedWeb, Sun ONE Web Server, Sun-ILOM-Web-Server, Sametime Server (Meeting Services) 1.6, nzarnginx, NetApp, Mongrel 1.1.1, Fastream IQ Web, Easy File Sharing Web Server v4.6s, dynamic.stardeals.co.nz, dynamic.staging.stardeals.co.nz, D-Link Internet Camera, DirectAdmin Daemon v1.34.4 Registered to Ben Simpson, CERN, ABWS, ZyXEL-RomPager, Xerver, WinGate Engine, WatchGuard Firewall, Vivotek Video Server, VideoDR-S, Ultraseek, TRMB, tncdn, thin 1.0.0 codename That, Sun Java System Application Server 9.1\_02, Strategi HTTPD V1R9M3, Squid, SpatialMedia, SolusVM, snom embedded, Slinger, Sawmill, Redirector, Rapid Logic, PrHTTPD Ver1.0, PicLan-IP 2.0.0 (build 177), PicLan-IP 2.0.0 (build 159), NZACU, Nucleus WebServ, NS8.0.55.3, No-server-here, NetZoom, Network Camera, NetworkActiv-Web-Server, NetCloak, MoxaHttp, Mongrel 1.1, Mongrel 1.0.4, Mongrel 1.0.1, Mathopd, LiveStats Reporting Server, Kerio MailServer 6.6.1, iTP WebServer, IP\*Works! Web Server, Ipswitch 1.0, InterMapper, HTTP, HPWB, HP-ChaiSOE, Henry, Gordian Embedded1.0, Google Frontend, gateway, FlashCom, FCS-1040 P, Embedded HTTP Server., E-Government Server, e, DirectAdmin Daemon v1.34.3 Registered to Hosting Direct Ltd, dhhttpd, Debut, CrackHead, Clw, CCProxy, Camera Web Server, BarracudaHTTP 2.0, Asterisk, AssetWebServer101, ArGoSoft Mail Server Pro for WinNT, AppleShareIP, AppleDiskServer-1F3009, 4D\_v11\_SQL, 2.2.5.5, 2.2.5.2, yxorp-x.x, Yaws, xLightweb, Webserver (Windows), Web Crossing(r) Unix-v6.0 built Nov 25 2008 09:02:42 (source:1190 2008-11-13 09:33:19 - 0800), Visualware MyConnection Server Professional Edition 8.6d, Verint-Webs, UPnP, Upkeep Httpd, Unknown Web Server, TMS320V5000, TinyWeb, thin 1.2.2 codename I Find Your Lack of Sauce Disturbing, Sunny WebBox, sun.net, Summary, Snap Appliance, Inc., Server, Savant, RTMC\_WebServer v2.6.48.0 (Win32), Rolleston Community Church (HWS149), Rogatkin, RMC Webserver 1.0, RealVNC, Power-Sockets, Pi3Web, OracleAS-Web-Cache-10g, Oracle Application Server Containers for J2EE 10g (9.0.4.1.0), Oracle9iAS, OpenSA, OmniSecure, NS\_6.1, NewsBoss Wires 4.6d, NetWare-Enterprise-Web-Server, NETLAB, NetBox Version 2.8 Build 4128, NET+ARM Web Server, Mongrel 1.1.2, Ministry of Womens Affairs Server, MiniServ, Mikrotik HttpProxy, Micro-Web, Microsoft-Cassini, Mbedthis-AppWeb, ManageUPSnet Web Server, MagnoWare, MacHTTP, LPC Http Server, LiveServer, LightTPD, Lanswitch - V100R003 HttpServer 1.1, KiwiServers, jToolkitHTTP, JC-HTTPD, iTP Secure WebServer, IPWEBS, IPConsult HTTP Server 1.9.19.1, ioLogik Web Server, Intoto Http Server v1.0, Ili 150, ICT, HttpServer, HTTP-Redirect.sh, HP-ChaiServer, HomeSeer, HI, HFS 2.2f, HFS 2.2d, HFS 2.2a, GWS, GoAhead, FX-EWB-Compatible, FWS, FSPMS, FriendFeedServer, FortiWeb-2.2.0, ExpressWay, eRez Imaging Server, EPSON-HTTP, ePipe 2242, Entrust, eHTTP v1.0, Easy File Sharing Web Server v4.8s, dynamic.dev.topshelfmedia.co.nz, DCS-6620G, DCS-6620, DCS-3220, DCS-2120, Dart WebServer Tool, CoyotePoint L7 Load Balancer, Cleo LexiCom, Cherokee, CarelDataServer, Cardax Embedded Interface, CANON HTTP Server Ver2.30, Canon Http Server 2.11, Canon Http Server 2.10, BWS, Blueliris-HTTP, AWC86 MicroRTOS, Aragorn, Apache 3, AKCP Embedded Web Server, Adaptive Security Appliance HTTP, 3Com

Searches Websites

All regions

Scale is based on the average worldwide traffic of **joomla** in the last 12 months. [Learn more](#)

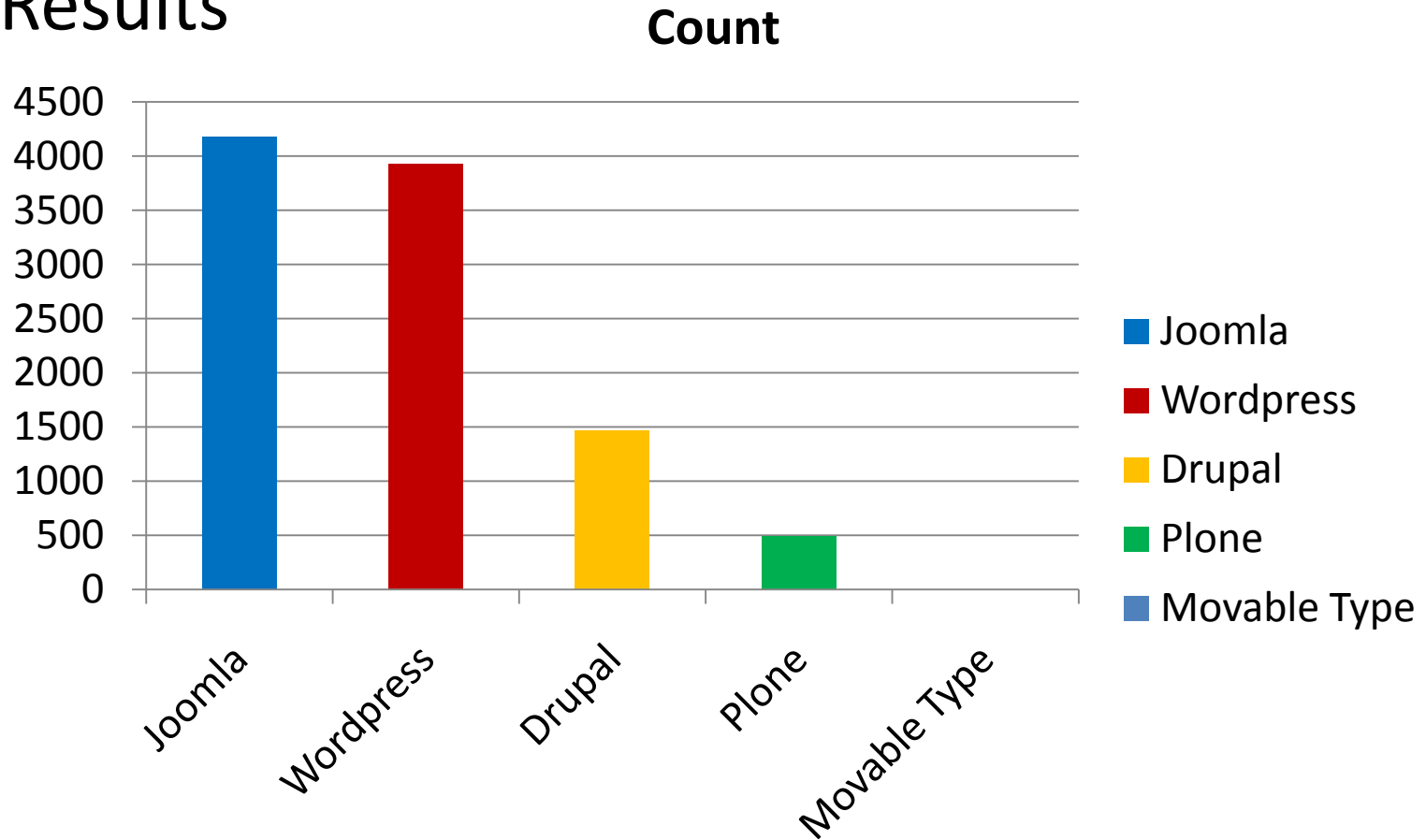
**joomla** 1.00 **wordpress** 0.99 **drupal** 0.31 **plone** 0.03  
**movable type** 0.02



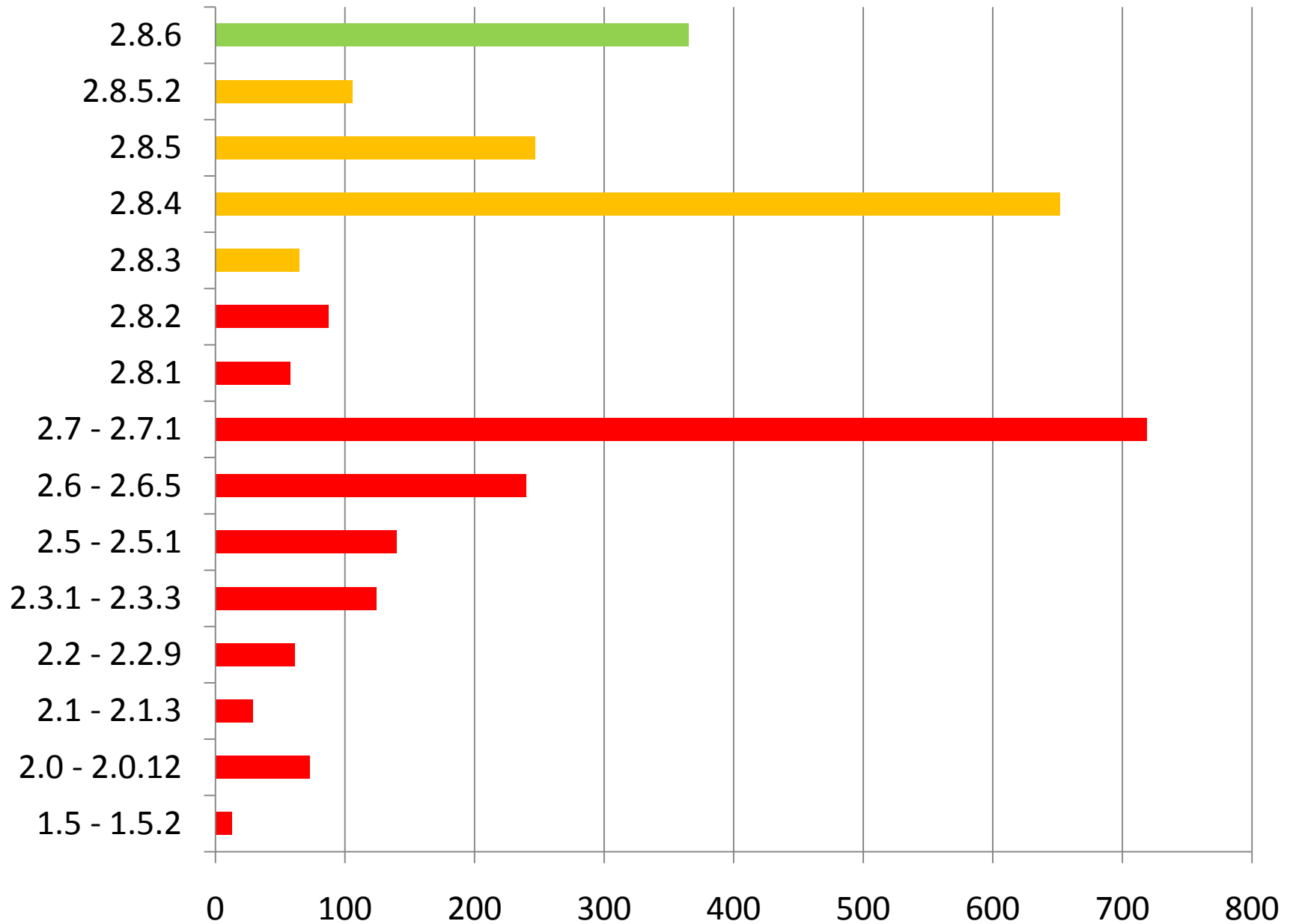


# CMS Showdown

## NZ Results



# WordPress Versions



# WordPress

- Is WordPress representative of other CMS's?
- 89% are not patched and up to date. < 2.8.6
- 53% are at high risk of exploitation. <= 2.8.2
- An internet worm is currently exploiting WordPress installations with versions of 2.8.2 and prior.  
<http://www.securityfocus.com/bid/27669/info>

# What else is on the web?

- Websites but not as you know them
- Web interfaces to cameras, printers, phones, etc.
- Many of these devices should not be available through websites on public, internet IP addresses
- Insecure vs Unsecured. Many devices are not protected by any authentication mechanism
- This presentation contains a subset of the screenshots in the full presentation

# Cameras



Digital Disk Recorder

WJ-HD220

Main  
Control Panel

Alarm List

Camera Select



Multiscreen Select



LIVE SEQUENCE

ALARM RESET

TIME & DATE SEARCH

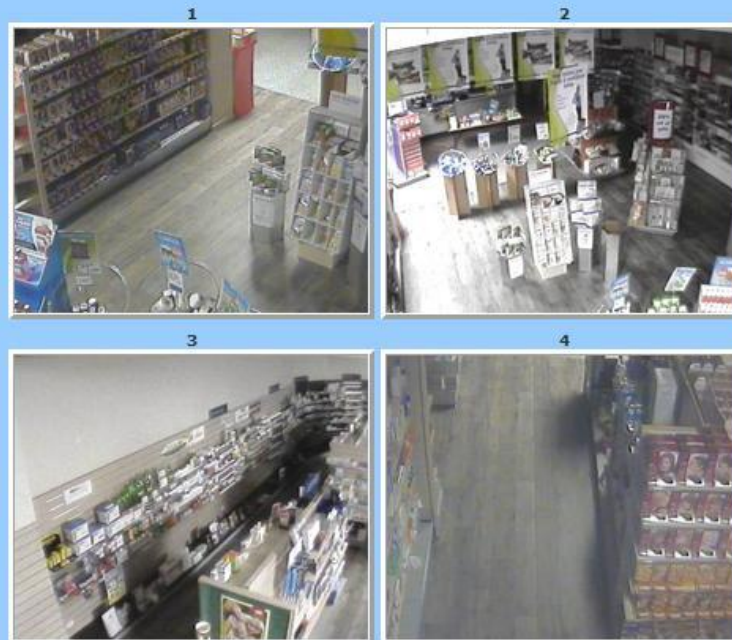
CAMERA CONTROL VIEW

SETUP MENU

LIVE CH1-CH4 [1 ]

REC

24/Nov/2009 01:54:17



TO OLDEST

REW

REV PLAY

PLAY

FF

TO LATEST

PREV FRAME

PAUSE

STOP

NEXT FRAME

# Printers

Xerox 9700 [1977]





HP LaserJet P1505n 192.168.15.102

Information Settings Networking

IPv4 Configuration IPv6 Configuration Advanced Bonjour Password SNMP Network Summary

## IPv4 Configuration

[Shop for Supplies](#) [Support](#)

**Warning: A change in the IP Address will result in loss of connectivity to the browser.**

IP Configured By: DHCP

Host Name: NPI7B7699

Domain Name:

### IP Address Configuration

☒ Automatic IP ☐ Manual IP

☒ DHCP ☐ BootP ☒ AutoIP

Manual IP Address: 192.168.15.102

IP Subnet Mask: 255.255.255.0

Manual Default Gateway: 192.168.15.254



# Phones



Polycom - SoundStation ... x Sipura SPA Configuration x

http:// 'coreConf.htm

**POLYCOM** SoundStation IP Configuration

Home General Network SIP Line

**General Configuration Parameters:**

User Preferences	Time	Audio Processing
Sampled Audio	Microbrowser	Logging

**User Preferences**

Headset Memory Mode	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Use Directory Names	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
One Touch Voice Mail	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Bypass Instant Message	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Welcome Sound (All Boot)	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Welcome Sound (Warm Boot)	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
top	Submit

**Time**

**Synchronization**

SNTP Server	
GMT Offset	-12
SNTP Resync Period	86400

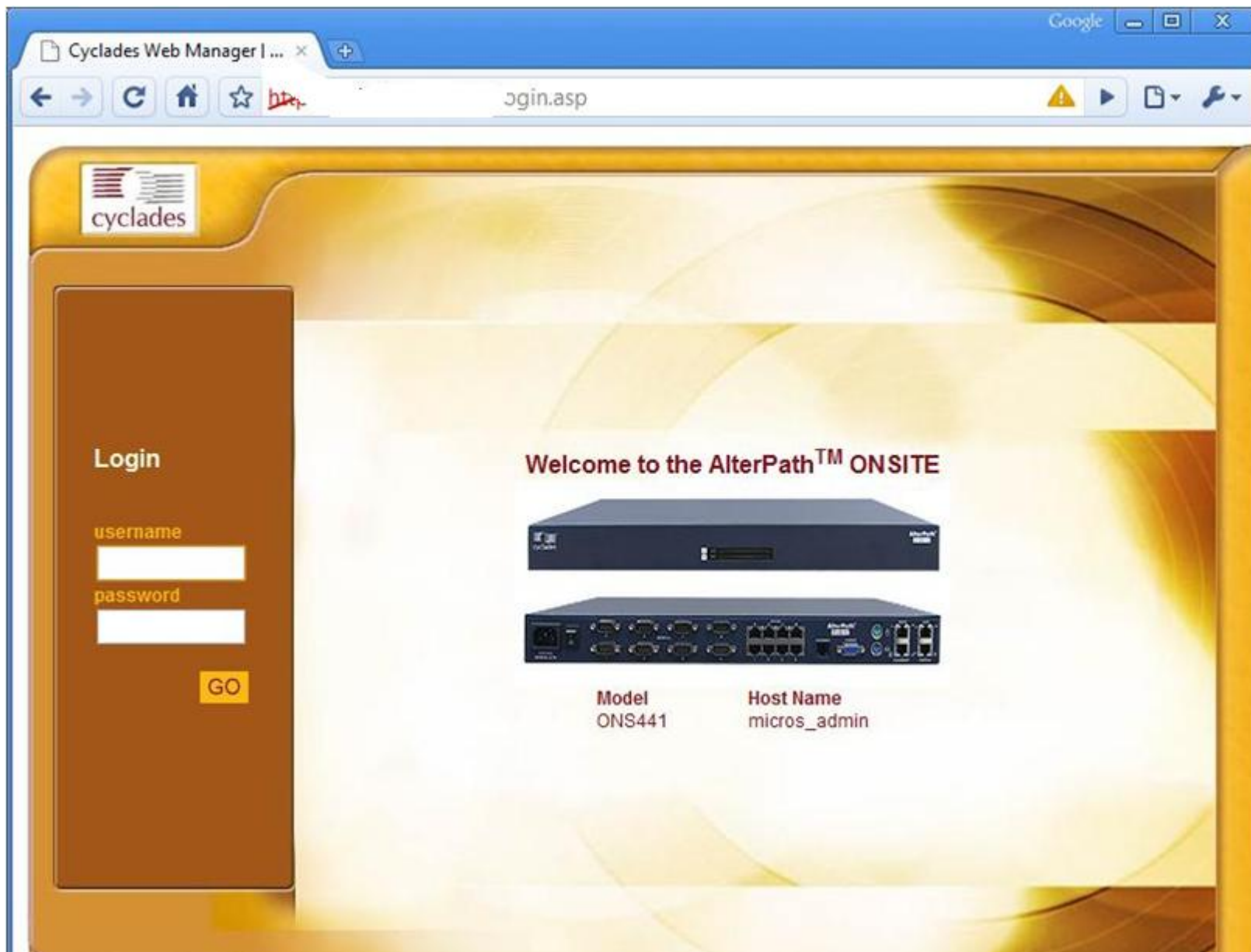
# TV devices





# GoAhead

- Don't judge a website by it's HTTP Server Name
- Many different types of devices are powered by the GoAhead embedded HTTP server.
- *Most* of the following devices are shown to display the variation of devices, not because they have a lack of authentication.









8647 - Leica GRX1200 GG ...

http://.../index.asp

**Leica Geosystems**

Instrument ID: 8647	Uptime: 70 days 16:53 h	Logging: Off	GPS:  SBAS 
Receiver type: GRX1200 GG Pro	Memory: 83% (25.30 MB)	RTK: Off	GLONASS:  Oscillator
IP address: 10.0.0.2	Power:  100% 	Ring buffer: Off	GALILEO:  02:11:29 2009-11-24

Home | Status | Configuration | Help | Support


**GRX1200 GG Pro** Start Start RB

**Status**

- System Information
- Power & Memory
- Position
- Satellites
- Antenna
- Message Log
- Interfaces
- Port summary
- CF Card (via FTP)

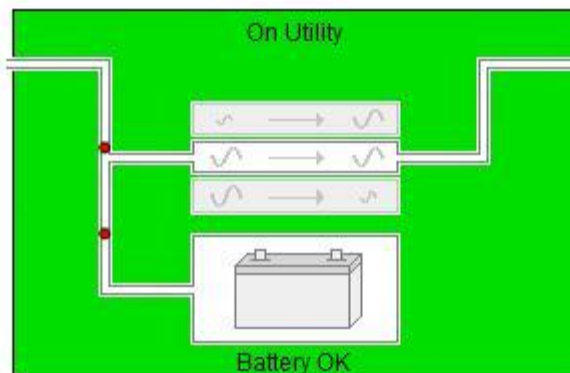
**GRX1200 GG Pro - Web Interface** ?

Welcome to the web interface for the GRX1200 GG Pro



[Home](#)[Logs](#)[Setup](#)[Help](#)[Logout](#)[Overview](#)[Alarms](#)[Identification](#)[Parameters](#)[Attached Devices](#)[Power Fail](#)[Shutdown Events](#)[Event Settings](#)[Manual Control](#)[Settings](#)

## Overview

[Help](#)[UPS Animation](#)[Alarms \( 0 \)](#)

Critical

Warning

Normal



# Heavy Equipment

- Air conditioning
- Industrial process sensors
- Data centres



[monitor](#)[control](#)[configure](#)[support](#)

Device:  
ProcessCooler1



Device Status:  
[Check Device Status](#)

#### Device Information:

- Summary
- Active Alarms
- System

#### Summary:

Updated: November 23, 2009 11:27:04PM

##### Return Air

Temperature 20.4° C  
Setpoint 19° C  
Humidity 42.8 %  
Setpoint 41 %

##### Supply Air

Temperature 0° C  
Setpoint 16° C  
Humidity 90 %

##### Unit 1 Status Info



Cooling Output % 100  
Heating Output % 0

##### Run Timer (hours)

Active Total	37766
Cool Mode	37229
Heat Mode	268
Humidify Mode	13058
De-Humidify Mode	1381
Humidify Operation	11825
Humidifier Service	0
Cool 1 Operation	37228
Cool 2 Operation	35407
Cool Service	613
Heat 1 Operation	268
Heat 2 Operation	79
Fan Operation	37761
Filter Service	613

#### Active Alarms:

General Alarm Status

# Analysis Notes

- A high percentage of content management system websites are insecure due to poor updating. 53% are at high risk.
- Unsecured devices discovered include cameras, printers, phones, TV units, intranets (not shown in this version of the slides), air conditioning systems and industrial process sensors. These should be behind a firewall or secured with a password.

# Tools Used

- Geoipgen – IP generator
  - Used to produce a near complete set of IP addresses in New Zealand. This is a MorningStar Security tool.
  - <http://www.morningstarsecurity.com/research/geoipgen>
- Nmap – Network scanner.
  - Used to port scan to test IPs for web servers on TCP port 80
  - <http://www.nmap.org>
- Dnsenum – DNS enumeration
  - Used to execute zone transfers
  - <http://code.google.com/p/dnsenum/>
- adns-tools
  - Used for fast reverse DNS resolving
  - <http://www.chiark.greenend.org.uk/~ian/adns/>

# New Tools Developed

- WhatWeb
  - Used to identify websites with a light scan
  - Homepage <http://www.morningstarsecurity.com/research/whatweb>
- Gggooglescan
  - Find website hostnames by searching with Google.
  - Scan wide and shallow.
  - Homepage <http://www.morningstarsecurity.com/research/>
- bing-ip2hosts
  - Find all websites indexed by Bing on NZ IP addresses
  - Homepage <http://www.morningstarsecurity.com/research/bing-ip2hosts>
- Basedomainname
  - Used to extract the domainnames of hostnames
  - Homepage <http://www.morningstarsecurity.com/research/>

# 53% at high risk of exploitation. WTF?

Check out [www.morningstarsecurity.com](http://www.morningstarsecurity.com) for your freshest blend of IT security news each morning

