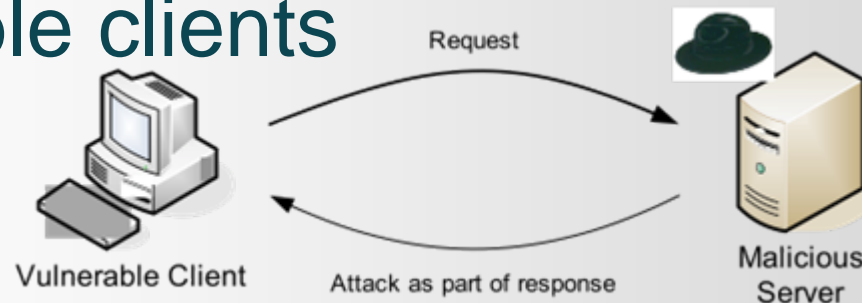


Scanning the .nz Domain for Drive-by-Downloads



Drive-by-Downloads

Attacks launched by servers that target vulnerable clients



Web server attacking web browser)

- Visiting a page is sufficient for exploit to be delivered
- Targets a specific vulnerability of the browser, plug-in or the operating system

Study Overview

Study undertaken by Victoria University of Wellington

Sponsored by InternetNZ

- Phases:

1. Assess threat posed by servers in the .nz domain compared to other English speaking domains (complete)
2. Analyse the entire .nz domain for the presence of malicious web servers (complete)
3. Re-run analysis monthly for six months and more often on URLs identified as malicious in tests (complete)



Study overview - cont

Methodology:

- Drive vulnerable clients (Windows XP SP2/Internet Explorer 6 SP2) to visit websites
- store interaction with the server and watch for anomalous system behaviour



Results – Phase 1

- Phase one:

- Determined prevalence of malicious web servers in .au, .com, .nz and .uk domains by inspecting a sample of 664,000 URLs
- Found the following malicious data (URLs/hosts):
.au (26/16), .com (1/1), .nz(3/3), .uk (8/7)



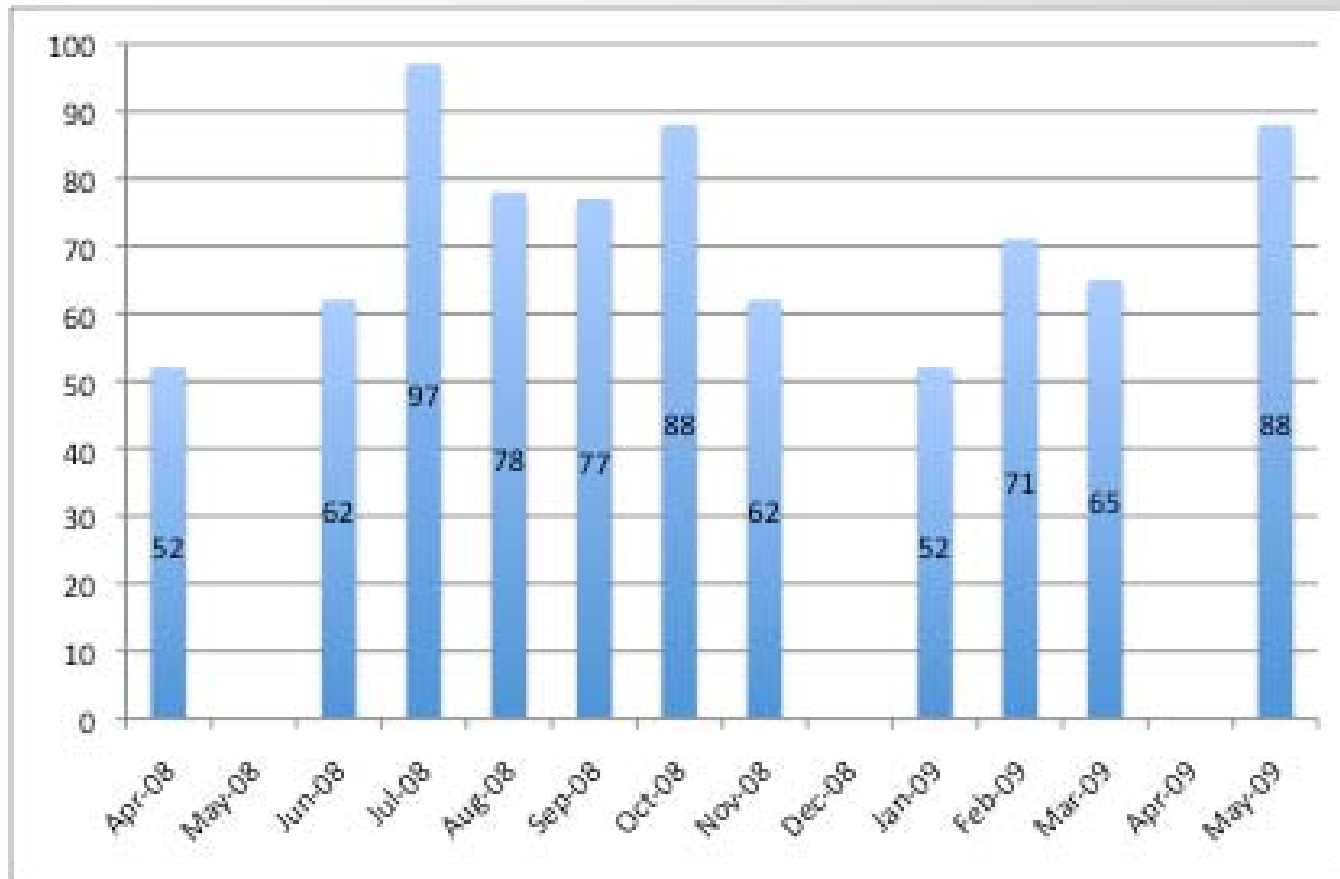
Results – Phase 2

- Phase two:

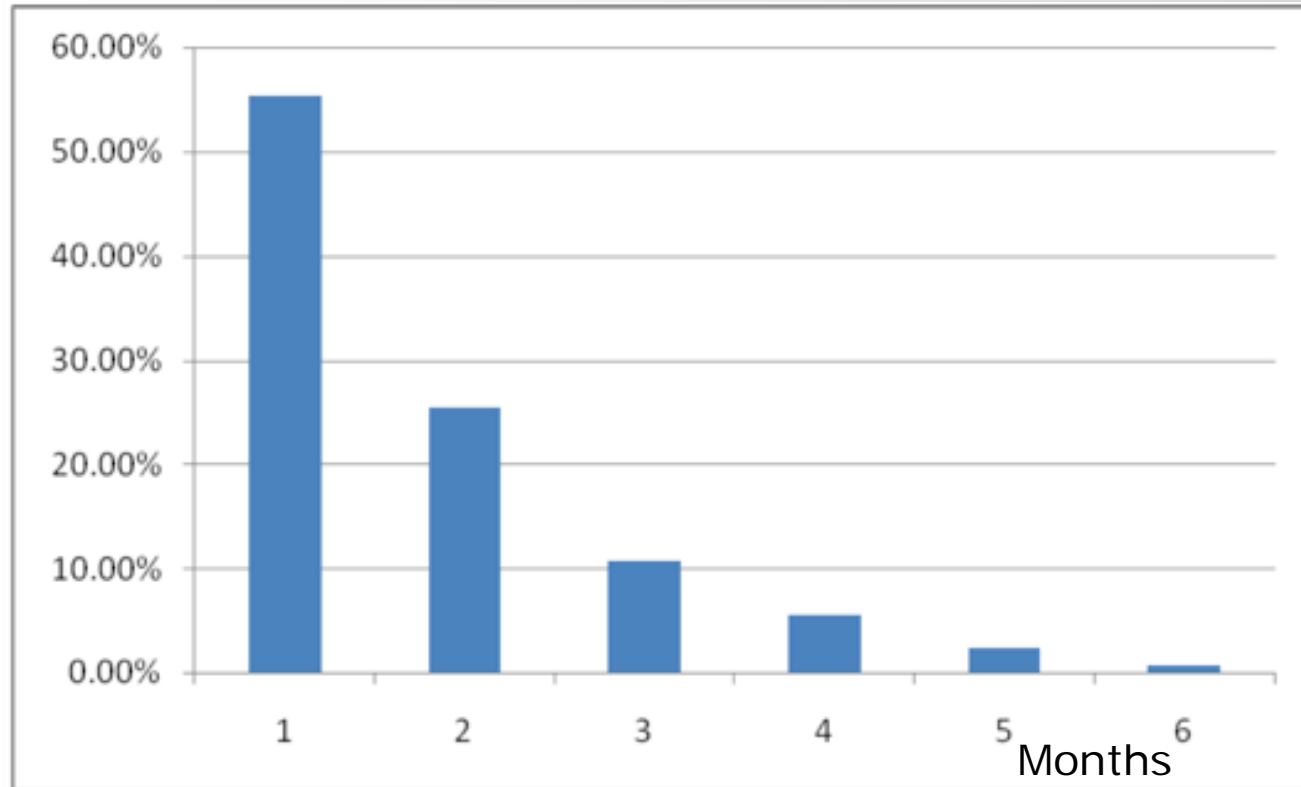
- Visited front page of all .nz web servers identified from zone file (247,198 hosts) in April 2008
- Found 52 web servers with malicious response or content
- Malicious servers located in USA, UK, Australia & NZ
- **Exploit servers** located in China, Russia, Germany, UK, USA, South America



Phase 3: Confirmed malicious servers



Phase 3: Persistence of Malicious Servers



Discussion

- Results of the .nz scan indicate a slight upward trend in malicious server deployment overall
 - High variability month by month
 - 43% are newly malicious on monthly scans
 - Malicious servers redirect to an exploit server located outside the .nz domain



Discussion – cont.

Many sites remain malicious for long periods before system administrators detect and nullify malicious behaviour

–Over 53% remain malicious for 1 month or more

–<http://www.internetnz.net.nz/workstreams/honeypot>



Further Information

- Technology
- Phase 1 results
- Phase 2 results



Technology

- Using software platform initially developed by Christian Seifert and a team of research assistants at Victoria University of Wellington.
- Software is released as open source (GPL-ed) and hosted by the international HoneyNet Project
- Capture-HPC (a high interaction honeyclient) is obtainable from:
 - <https://projects.honeynet.org/capture-hpc/>

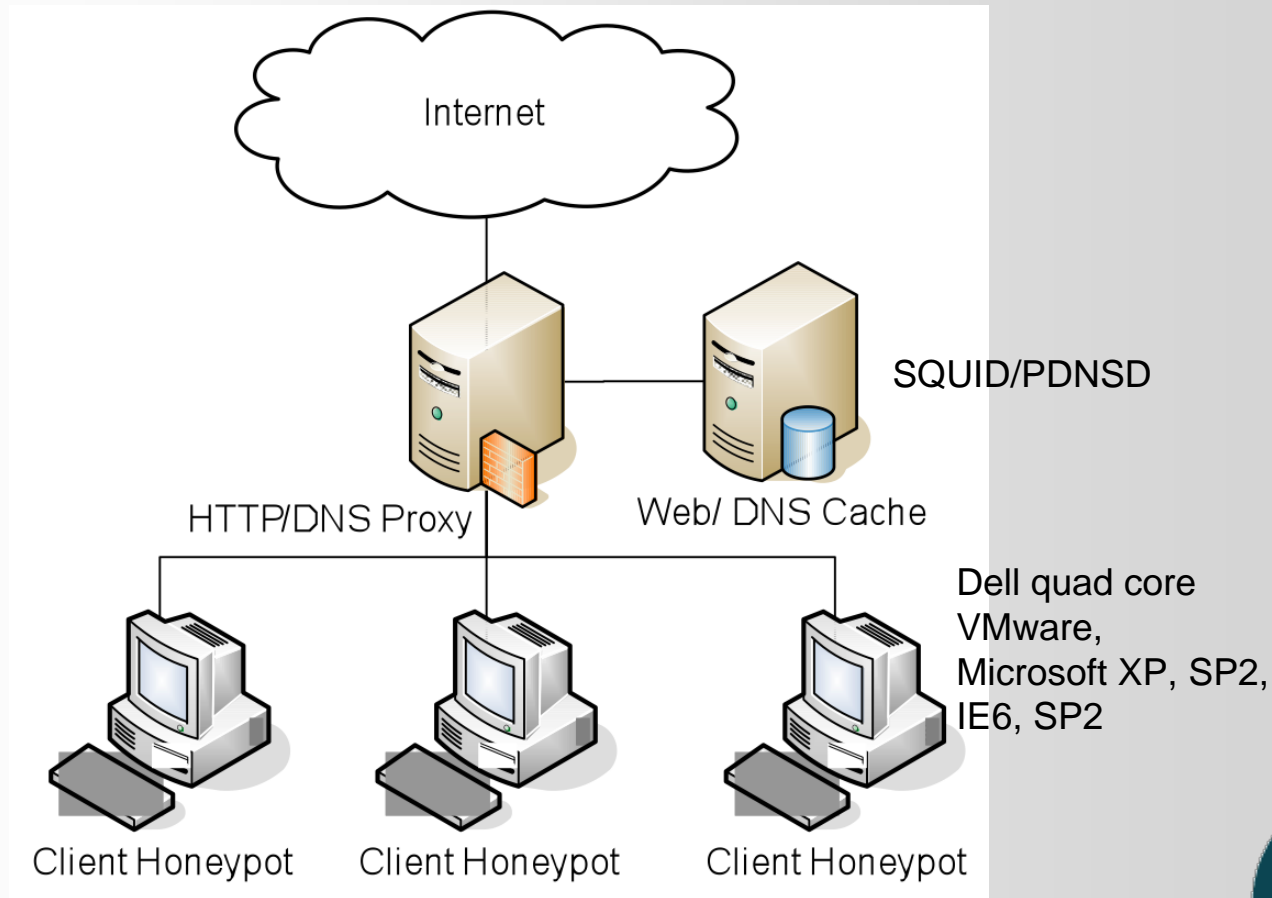


Technology Update

- Capture-HPC 2.5.1 (released 8th September 2008)
 - Faster detection, more options
- New release expected in beta testing (8/2009)
 - More network monitoring support
 - Database support
 - Visualisation of data and reports
 - Enhanced documentation for systems admin and developers



Current Experimental Setup



Phase 2 Results

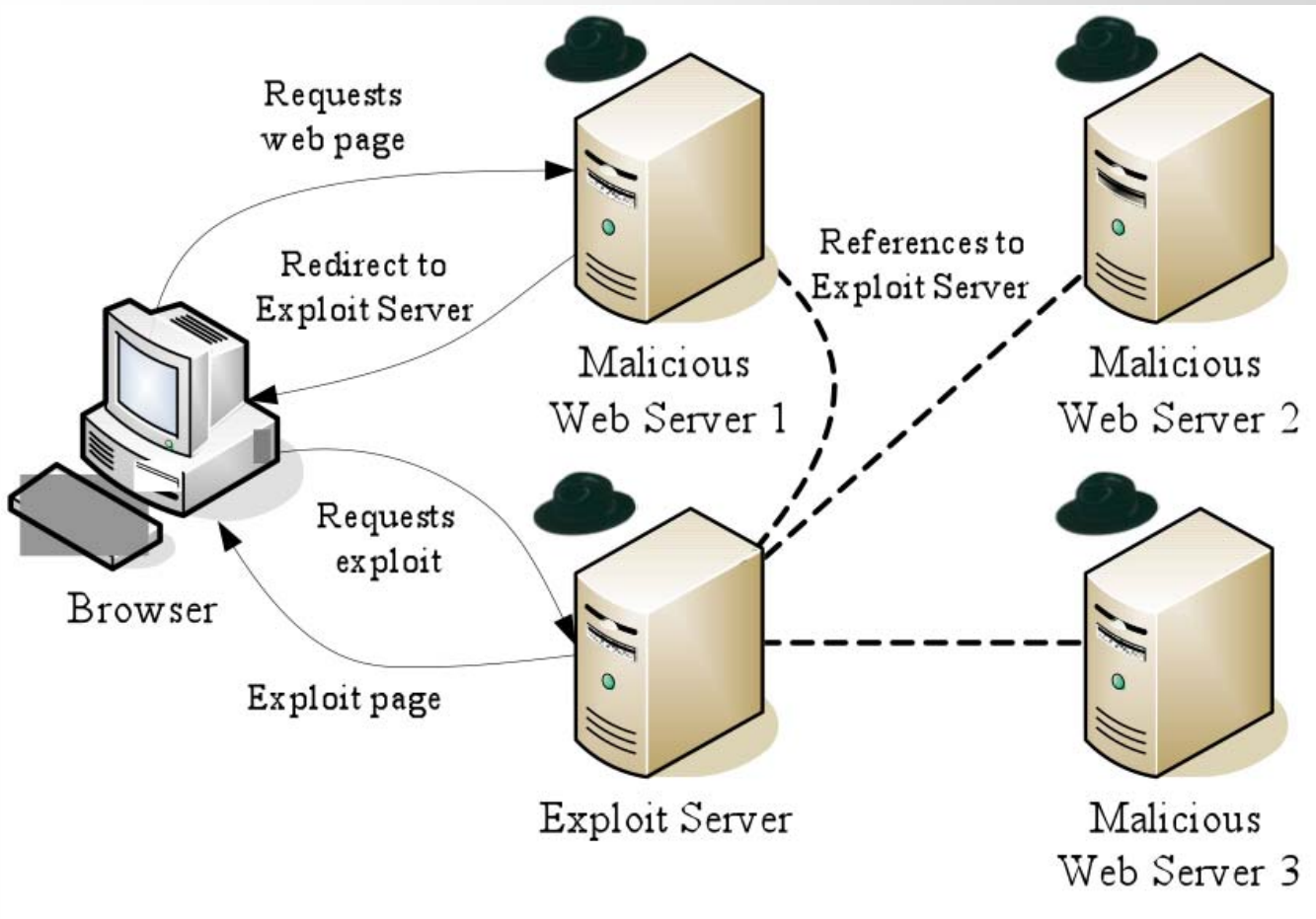
- Found 52 web servers with malicious response or content in .nz
- The malicious servers are located in USA, UK, Australia & NZ
- **Actual Exploit servers** located in:
 - China, Russia, Germany, UK, USA, South America
 - Redirected from compromised .nz web servers



Phase 2 Results: Map of Detected Malicious Servers (April 08)



But not the whole picture...



Phase 2 results: Map of Actual Exploit Servers



Further Analysis

- Revisited web site with fully patched system – all attacks were foiled
- Assessed popularity of compromised sites using Alexa, Google Toolbar and SiteAdvisor
 - 17 sites not known to ranking sites, 2 sites were rated “medium”, others “low”
 - Minor threat posed



Further Analysis – cont.

- Cross-checked site against Google's Safe Browsing API, McAfee SiteAdvisor and HauteSecure plugin
 - 9 out of 52 sites were tagged as malicious by Google, Stopbadware.com and SiteAdvisor (April 09)
 - Haute Secure did better (40 out of 52)



Table of Data – Malicious Servers .nz

Month	Diff malicious from prev month	New malicious	Total Malicious	% diff	% new
April			51		
June	29	29	62	46.8	46.8
July	77	75	97	79.4	77.3
August	60	43	78	76.9	55.1
September	55	34	77	71.4	44.2
October	47	38	88	53.4	43.2
Average	53.6	43.8	75.5	65.6	53.3

