

New Zealand Internet Task Force



Improving the cyber security posture of New Zealand

A bottom up approach to improving the contries cyber security posture

Barry Brailey

NZITF Vice Chair & Manager, Security Policy at .nz DNC

Programme

- Introduction
- Background
- The Birth of a Trust Group
- .nz Role
- The Way We Work
- Working Groups and Initiatives
- Q&A

Who Am I?

.nz
DOMAIN
NAME
COMMISSION

- Manager, Security Policy - .nz DNC



- Vice Chair – NZITF

What is the NZITF?

The New Zealand Internet Task Force is a non-profit with the mission of **improving the cyber security posture of New Zealand**

It is a **collaborative effort** based on **mutual trust** of it's members

New Zealand (Middle Earth)



NZ is excellent for many reasons!



NZ Gov't Cyber Security.....



- 2002 - Centre for Critical Infrastructure Protection



- 2011 – Cyber Security Strategy
(fairly brief)



- 2012 – National Cyber Security Centre

The Security Landscape

- The rise of ‘Worms and Trojans’ (Blaster, Welchia etc)
- NASA & other ‘hacks’
- Estonia Attacks
- Georgia Attacks
- Ghostnet (Cyber espionage)
- Conficker
- Rise of the ‘Botnets’
- Stuxnet

The Birth of a Trust Group



- Following BTF7, Conficker Working Group and Cyber Storm II in 2008 the NZ Botnet Task Force was formed
- Renamed NZITF early 2009 as the focus evolved and membership expanded

.nz Role

- DNC, NZRS and InternetNZ were very engaged in the NZ Conficker Working Group
- Formalised this support in 2009
- Ongoing support
 - Membership & Participation
 - Financial administration and facilities (InternetNZ)
- This also influences our internal Group Security Forum

The Early Days

- NZITF started small without any big fanfare
- ‘Coordinated by CCIP’ around other meetings
- Shoulder taps and introductions
- Increasing activity levels of NZITF required the need for a Steering Committee to be established in 2009



Growing Up

- Formally Incorporated in 2011
- Membership fee structure introduced
- First advertised public event



NZITF Board

- Telecom NZ, Mike Seddon (Chair)
- .nz DNC, Barry Brailey (Vice Chair)
- Bank of New Zealand, Chester Holmes (Secretary)
- Independent Consultant, Dean Pemberton (Treasurer)
- Dept. Internal Affairs, Toni Demetriou
- Vodafone, Steve Martin
- PwC, Adrian van Hest

The Way We Work

- Members are nominated and vouched on
- Traffic Light Protocol
- Meetings
- Training
- Working Groups



What has the NZITF done?

- Coordinating technical training
 - Targeted Threat Workshop
 - Security Architecture training
 - Wireless Security Training course
 - Team Cymru Botnet Forensics
 - Honeynet Project and Shadowsever Botnet Defense/Offence courses
 - CSIRT introduction
 - Open Source Intelligence
 - Windows Reverse Engineering



What has the NZITF done?

- Support industry and community initiatives
- Graduate secondments into industry
- Support research initiatives



NZITF Initiatives

- Some NZITF working groups:
 - CREST NZ
 - Cyber Exercising Framework
 - Botnet/Malware Data
 - Responsible Disclosure



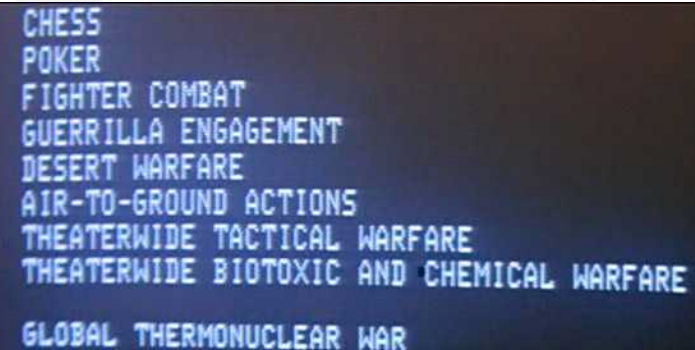
CREST NZ

- The NZITF set up working group to establish CREST NZ Council of Registered Ethical Security Testers
- No professional voice or representation for the penetration testing industry
- Lack of education and training courses
- Skill set shortage in New Zealand
- Growing international certification
- CREST Australia is now up and running



Cyber Exercising Framework

- Exercising tests and improves the levels of preparedness for a significant cyber incident
- Develop a framework and schedule for conducting cyber exercises:
 - Communications Checks
 - Scenario Discussions
- Table Top Exercises (TTX)
- National and International Full Play Exercises



```
CHES  
POKER  
FIGHTER COMBAT  
GUERRILLA ENGAGEMENT  
DESERT WARFARE  
AIR-TO-GROUND ACTIONS  
THEATERWIDE TACTICAL WARFARE  
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE  
  
GLOBAL THERMONUCLEAR WAR
```

Botnet/Malware Data

- Assess current NZ infection rates
- Identify data sources of botnet infections & compromised New Zealand websites
- Recommend potential mitigations that could be effective in New Zealand and the stakeholders for each
- Identify possible technical and policy based mitigations



Vulnerability Disclosure Example

- Researcher finds potential flaw on MoJ website
- Researcher informs opposition MP
- Opposition give about 24hours notice and go to media
- Justice Minister responds:

“The ministry and I do not deal with hackers and we do not deal with burglars.”

Hon JUDITH COLLINS

Highlighted an issue in NZ

- Report a security vulnerability to a New Zealand website - probably have a 50% chance of being reported to the Police
- The other 50% - spend a large amount of time trying to explain why it's an issue
- Hence, while vulnerabilities are being found every day - they are never being reported or fixed

We had to do better!

- NZITF WG drafted 'Responsible Disclosure Guidelines'
- Released for public consultation last year
- Consulted at OWASP and Kiwicon in NZ
- Final version will be released this year
- Hope that it will help improve 'maturity' amongst website owners and businesses
 - NZRS has already adopted a great example

Q&A



info@nzitf.org.nz

misp@dnc.org.nz



Improving the cyber security posture of New Zealand