Improving the cyber security posture of New Zealand

Members Trust Portal

Members click here to access the NZITF Trust Portal

Latest News

'Pay bitcoins or your network gets it' threats for New Zealand organisations.

The New Zealand Internet Task Force (NZITF) advises that an unknown international group has this week begun threatening New Zealand organisations with Distributed Denial of Service (DDoS) attacks.

NZITF releases disclosure guidelines

The New Zealand Internet Task Force (NZITF) has released guidelines on how New Zealanders and NZ companies can implement coordinated disclosure.

New Zealand websites named among Australasia’s most trustworthy

A quartet of New Zealand organisations have been recognised as among the most trustworthy in Australasia for their commitment to consumer safety, security and privacy online.

SHELL SHOCK CVE_2014_6271

A newly discovered vulnerability in the Bash command-line interpreter poses a critical security risk to Unix and Linux systems including Apple OSX.

GameOver Zeus P2P Malware

Information and advise for users relating to the GameOver Zeus P2P Malware

HeartBleed vulnerability - The Next Steps

The New Zealand Internet Task Force (NZITF) highlights what the next steps are your

organisation might consider in its management of the HeartBleed vulnerability.

HeartBleed vulnerability warning for website owners

The New Zealand Internet Task Force (NZITF) warns website owners that their site's security may have been breached and private information may have been stolen through the HeartBleed vulnerability.

Public Consultation on Responsible Disclosure Guidelines

The New Zealand Internet Task Force (NZITF) opens consultation on New Zealand responsible disclosure guidelines.

Responsible Disclosure Guidelines

The New Zealand Internet Task Force (NZITF) is currently working on New Zealand responsible disclosure guidelines.

Local group scoops top Australian security award

The New Zealand Internet Task Force (NZITF) has beaten the Australians at their own game, taking out the top prize in the prestigious AusCERT Awards.

NZITF Wins Best Security Initiative

The NZITF has been awarded the Best Security Initiative in the 2013 Australian Information Security Awards.

NZITF Finalist in 2013 Australian Information Security Awards

The NZITF has been announced as a finalist in the Best Security Initiative category in the 2013 Australian Information Security Awards.

Cyber Security Awareness Week

New Zealand's second annual Cyber Security Awareness Week(CSAW) will be held 27 - 31 May 2013.

NZITF Highly Commended in ANZIAs

The NZITF has received a Highly Commended recognition in the Security & Privacy category of 2012 Australia and New Zealand Internet Awards (the ANZIAs).

'Pay bitcoins or your network gets it' threats

for New Zealand organisations.

Media release – 7 May 2015

The New Zealand Internet Task Force (NZITF) advises that an unknown international group has this week begun threatening New Zealand organisations with Distributed Denial of Service (DDoS) attacks.

DDoS attacks are attempts to make an organisation's Internet links or network unavailable to its users for an extended length of time.

This latest DDoS threat appears as an email threatening to take down an organisation's Internet links unless substantial payments in the digital currency Bitcoin are made.

NZITF Chair Barry Brailey warns the threat is not an idle one and should be taken extremely seriously as the networks of some New Zealand organisations have already been targetted.

"The networks of at least four New Zealand organisations that NZITF knows of have been affected, so far. A number of Australian organisations have also been affected," he says.

This unknown group of criminals have been sending emails to a number of addresses within an organisation. Sometimes these are support or helpdesk addresses, other times they are directed at individuals.

The emails contain statements threatening DDoS, such as:

"Your site is going under attack unless you pay 25 Bitcoin."

"We are aware that you probably don't have 25 BTC at the moment, so we are giving you 24 hours."

"IMPORTANT: You don't even have to reply. Just pay 25 BTC to [bitcoin address] – we will know it's you and you will never hear from us again."

The emails may also provide links to news articles about other attacks the group has conducted.

NZITF urges all New Zealand firms and organisations to be on the alert and consider the:

· **Don't pay**. Even if this stops a current attack, it makes your organisation a likely target for future exploitation as you have a history of making payments.

· Educate all staff to be on the lookout for any emails matching the descriptions above. Have them alert appropriate security personnel within the organisation as soon as possible.

· Establish points of contact with your Internet Service Providers (ISP) in the event that you need them to perform traffic filtering. Defense against many attack types is most effective when performed before it reaches your network. To date NZITF has had reports of organizations being able to handle these attacks effectively through collaboration with their ISPs.

· Establish a baseline of normal activity on your internal network to determine uncharacteristic levels of Internet traffic in the event of an attack. Report any attack to the appropriate authorities.

For more tech savvy organisations here are some additional steps to consider:

· Make use of DDoS mitigation services or content delivery networks to serve Web content. Solutions that specialize in protecting Web content may be more cost effective and, given the limited types of traffic that should be allowed, might be able to more aggressively drop malicious traffic.

· For DDoS attacks conducted over non-critical services (esp., SSDP and NTP), blocking the relevant ports may provide temporary mitigation.

For more information contact:

Barry Brailey
Chair
New Zealand Internet Task Force (NZITF)
021 798 418

About the New Zealand Internet Task Force (NZITF)

The New Zealand Internet Task Force (NZITF) is a non-profit with the mission of improving the cyber security posture of New Zealand. It is a forum based on mutual trust for debate, networking, information sharing, and collaboration on matters relating to the cyber security of New Zealand.

www.nzitf.org.nz

NZITF releases disclosure guidelines

Media release – 10 December 2014

The New Zealand Internet Task Force (NZITF) has released guidelines on how New Zealanders and NZ companies can implement coordinated disclosure. These guidelines will help security researchers and organisations to work together when disclosing and addressing vulnerabilities in ICT systems.

New Zealand businesses and organisations do not want to have ICT systems (such as websites) with vulnerabilities in them. Security researchers want to be able to notify organisations of vulnerabilities they come across without fear of legal action or negative publicity. It is important that we are all clear about what is expected of us when disclosing a vulnerability or when someone contacts us with a vulnerability.

Because the NZITF has a broad membership of security professionals we have designed these guidelines to give people an easy to use introduction to coordinated

disclosure. Barry Brailey, the NZITF's Chair said "I hope the guidelines set some clear boundaries and ultimately make it easier for security professionals to work together and help improve New Zealand's cyber security posture."

You can download a copy of the coordinated disclosure guidelines from the NZITF's website here

To contact us about a vulnerability email us at disclosure@nzitf.org.nz.
Our PGP details are:
Key ID: 06A8A214
Fingerprint: DBBD 4DE3 5FDD CCC0 175C 03B4 6451 0C5E 06A8 A214

New Zealand websites named among Australasia's most trustworthy

New Zealand websites named among Australasia's most trustworthy A quartet of New Zealand organisations have been recognised as among the most trustworthy in Australasia for their commitment to consumer safety, security and privacy online.

The websites of Marlborough-based HealthPost, online auction giant Trade Me, New Zealand Post and accounting software firm Xero earned the honour in the just-completed 2014 Australia and New Zealand (A/NZ) Online Trust Audit.

Two of the companies - Trade Me and Xero - are members of the New Zealand Internet Task Force (NZITF) - a non-profit group of Internet security professionals tasked with improving the cyber security posture of New Zealand.

NZITF Chair Barry Brailey congratulates Health Post, Trade Me, New Zealand Post and Xero for their success in the 2014 Online Trust Audit, saying their website security, data protection and privacy policies serve as an exemplar that other New Zealand companies should look to emulate.

"It's pleasing to see these four local companies leading the way in securing and protecting their customers' personal data. When organisations like these commit to best practice data protection and privacy, it helps instil tremendous trust and confidence in their online services.

"We strongly encourage other New Zealand businesses to learn from their example."

More information about the 2014 Australia and New Zealand (A/NZ) Online Trust Audit is available at www.otalliance.org. For more information about the New Zealand Internet Task Force (NZITF) visit www.nzitf.org.nz

Contact:

Barry Brailey
Chair, NZITF

"SHELL SHOCK" Bash vulnerability

Advice for Businesses and End Users

What can we do now?

Businesses and other Website Owners

1) Patch fast, patch often.

Keep a close watch on the website of your software vendors. There isn't likely to be a 'one big fix' patch for a number of days. There may however be multiple smaller patches which fix individual aspects of the vulnerability. It's better to apply patches even if they only provide partial fixes

2) Reduce your 'attack surface'

Identify business critical systems and less critical, consider shutting down less critical systems to reduce your attack surface until a patch is released. For vunerable business critical services, ensure they are located behind some form of border protection and that you have a regular, verified method of data backup and recovery. Placing services behind Web Application Firewalls (as opposed to a network firewall) which have been tuned to detect this attack will provide some protection.

3) Monitor Logs

Increase the frequency with which you monitor you logs. Keep an eye on anything which looks out of the ordinary and take steps to investigate. You will want to keep an eye on your webserver access logs in particular to see if there is anything strange showing up. We have had some reports of administrators using the following 'grep' string to search through web server access logs to see if there have been any exploit attempts:

```
grep '() {'
```

4) Educate yourself

Information about the vulnerability is presented on the NZITF website (further down this page). This is an evolving issue. Make sure that you check back on this page regularly as we will be adding more information as it comes to hand. There is also a very well written write up here: http://www.troyhunt.com/2014/09/everything-you-need-to-know-about.html

5) Test your servers:

There are a number of vulnerabilities being tracked at present (CVE-2014-6271 and CVE-2014-7169).

To test if your version of Bash is vulnerable to the CVE-2014-6271 issue, run the following command:

```
$ env x='() { :;}; echo vulnerable'  bash -c "echo this is a test"
```

If the output of the above command looks as follows:

```
vulnerable
this is a test
```

you are using a vulnerable version of Bash. The patch used to fix this issue ensures that no code is allowed after the end of a Bash function. Thus, if you run the above example with the patched version of Bash, you should get an output similar to:

```
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x`;
this is a test
```

There are also a number of experimental tools which attempt to get your website to demonstrate if they are vulnerable. These are not a fool proof way of testing and can give a false result in a large number of cases. We would advise businesses to test using the bash code above, and if a server is vulnerable and runs a service that accepts traffic on the internet, assume that it is able to be exploited. Use the services below at your own risk and on your own servers only.

- http://www.shellshocktest.com/
- http://shellshock.brandonpotter.com/

End Users:

1) Patch fast, patch often.

Make sure that you have automatic updates turned on for your operating system. In general apply vendor patches as soon as they are available.

For users on Apple Mac computers running OSX, you should ensure that you check on the App Store for Operating System updates atleast once a day until this vulnerability is resolved.

For more advanced users, if you manage your own home network. Don't forget to

ensure that your router/DSL modem software is upto date and any administration webpage is not accessable from the Internet.

2) Be extra vigilant of malware and scams over the next few weeks.

If there is an increase in the number of websites being compromised, these could be used to launch malware or scams. Make sure that you keep your paranoid filter on high for the next little while.

This may show up as more people calling you during dinner to offer to help you 'fix' your computer. These are almost always scams. Be extra wary of clicking on links in emails or social media sites from people you don't trust

3) Educate yourself

Check back often. This is an emerging issue. If there is more we think you can do, we'll post it here, so check back.

If you're interested in learning some more about this, there is some more information further down this page. There is also a very well written write up here:

http://www.troyhunt.com/2014/09/everything-you-need-to-know-about.html

SHELL SHOCK - CVE-2014-6271

CVE-2014-6271 "SHELL SHOCK"

Bash Code Injection Vulnerability

Overview

A critical vulnerability has been discovered in the Bourne again shell, commonly known as *bash* and present in most Linux and UNIX distributions, including Mac OS X. Administrators are urged to patch immediately.

This vulnerability allows attackers to compromise systems remotely, including systems used as web servers. It is as least as severe as the recent Heartbleed exploit and affects a large number of Internet-facing systems.

Details

The bash command shell processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code.

This is a high severity remote code execution vulnerability that potentially affects any system with bash installed, **even if bash is not used interactively on that system.** Exploits have been demonstrated that reach vulnerable bash versions via sshd, Apache, and dhclient, and common utilities such as procmail are believed to be vulnerable as well.

All mainstream linux distributions and Mac OS X are vulnerable, and should be patched immediately. In addition, affected systems should be repeatedly repatched as new patches become available.

Detecting vulnerable versions

To test if your version of Bash is vulnerable to this issue, run the following command:

```
$ env x='() { :;}; echo vulnerable'  bash -c "echo this is a test"
```

If the output of the above command looks as follows:

```
vulnerable
this is a test
```

you are using a vulnerable version of Bash. The patch used to fix this issue ensures that no code is allowed after the end of a Bash function. Thus, if you run the above example with the patched version of Bash, you should get an output similar to:

```
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x`;
this is a test
```

Currently available patches are an early mitigation, and further tests and patches may be added later.

Platform advisories

Ubuntu

http://www.ubuntu.com/usn/usn-2362-1/

Debian

https://www.debian.org/security/2014/dsa-3032

RedHat Linux

https://access.redhat.com/articles/1200223

Novell/SUSE

http://support.novell.com/security/cve/CVE-2014-6271.html

Mac OS X

No vendor-provided patch or advisory is available at this time. Advanced users may address the vulnerability by compiling a patched version of bash and replacing the system bash binary.

You may also like to follow these instuctions to ensure that your local firewall is blocking incoming connections

http://nzitf.org.nz/files/MacFirewall-BlockingConnections.pdf

Further information

Initial disclosure:

http://seclists.org/oss-sec/2014/q3/650

NIST/CVE vulnerability listing:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

RedHat severity discussion:

https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/

GameOver Zeus P2P Malware

Posted: 3 June 2014

Content courtesy of US-CERT

Overview

GameOver Zeus (GOZ), a peer-to-peer (P2P) variant of the Zeus family of bank credential-stealing malware identified in September 2011, uses a decentralized network infrastructure of compromised personal computers and web servers to execute command-and-control. The United States Department of Homeland Security (DHS), in collaboration with the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ), is releasing this Technical Alert to provide further information about the GameOver Zeus botnet.

Description

GOZ, which is often propagated through spam and phishing messages, is primarily used by cybercriminals to harvest banking information, such as login credentials, from a victim's computer. Infected systems can also be used to engage in other malicious activities, such as sending spam or participating in distributed denial-of-service (DDoS) attacks.

Prior variants of the Zeus malware utilized a centralized command and control (C2) botnet infrastructure to execute commands. Centralized C2 servers are routinely tracked and blocked by the security community. GOZ, however, utilizes a P2P network of infected hosts to communicate and distribute data, and employs encryption to evade detection. These peers act as a massive proxy network that is used to propagate binary updates, distribute configuration files, and to send stolen data. Without a single point of failure, the resiliency of GOZ's P2P infrastructure makes takedown efforts more difficult.

Impact

A system infected with GOZ may be employed to send spam, participate in DDoS attacks, and harvest users' credentials for online services, including banking services.

Solution

Users are recommended to take the following actions to remediate GOZ infections:

- *Use and maintain anti-virus software* - Anti-virus software recognizes and protects your computer against most known viruses. It is important to keep your anti-virus software up-to-date (see Understanding Anti-Virus Software for more information).
- *Change your passwords* - Your original passwords may have been compromised during the infection, so you should change them (see Choosing and Protecting Passwords for more information).
- *Keep your operating system and application software up-to-date* - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it (see Understanding Patches for more information).
- *Use anti-malware tools* - Using a legitimate program that identifies and removes malware can help eliminate an infection. Users can consider employing a remediation tool (examples below) that will help with the removal of GOZ from your system.

  F-Secure

  http://www.f-secure.com/en/web/home_global/online-scanner (Windows Vista, 7 and 8)

  http://www.f-secure.com/en/web/labs_global/removal-tools/-/carousel/view/142 (Windows XP)

  Heimdal

  http://goz.heimdalsecurity.com/ (Microsoft Windows XP, Vista, 7, 8 and 8.1)

  Microsoft

  http://www.microsoft.com/security/scanner/en-us/default.aspx (Windows 8.1, Windows 8, Windows 7, Windows Vista, and Windows XP)

Sophos

http://www.sophos.com/VirusRemoval (Windows XP (SP2) and above)

Symantec

http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network (Windows XP, Windows Vista and Windows 7)

Trend Micro

http://www.trendmicro.com/threatdetector (Windows XP, Windows Vista, Windows 7, Windows 8/8.1, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2)

The above are examples only and do not constitute an exhaustive list. The U.S. Government does not endorse or support any particular product or vendor.

- GOZ has been associated with the CryptoLocker malware. For more information on this malware, please visit the CryptoLocker Ransomware Infections page.

HeartBleed vulnerability - The Next Steps

Posted: 14 April 2014

The NZITF has produced a document outlining the next steps that organisations can take as they work to protect themselves against he HeartBleed vulnerability.

In addition to the immediate 3 steps outlined in previous advisories, 3 new steps have been highlighted.

- 1. Establish if your site’ s servers are vulnerable.
- 2. Patch the vulnerable servers.
- 3. Revoke/reissue certificates.
- 4. Prepare a Public Statement
- 5. Conduct a Security Risk Assessment
- 6. Recommend Password Resets

The detailed guidelines are available for download at:
http://nzitf.org.nz/files/NZITF-HeartBleed-TheNextSteps.pdf

HeartBleed vulnerability warning for OpenSSL users

Posted: 9 April 2014

New Zealand Internet Task Force is warning website owners and IT managers that their SSL certificate based security may have been breached and private information may have been stolen after the HeartBleed vulnerability was identified.

Individual web users do not have to do anything however website owners and IT managers are advised to check their website, Mail severs and VPN servers and patch them where required.

The vulnerability in OpenSSL software, commonly used to secure web sites, is easy to exploit and virtually impossible to detect when it has been exploited. Any web site, Mail server or VPN server using a vulnerable version of OpenSSL may have been attacked by criminals stealing data or eavesdropping on communications to and from the site. Now that this vulnerability is widely known the likelihood of criminals using this exploit are significantly higher."

To fix the vulnerability, you are advised to follow the below list in the order provided:

- 1. Establish if your site’ s servers are vulnerable.
- 2. Patch the vulnerable servers.
- 3. Revoke/reissue certificates.

1. Establishing if your site is vulnerable

There are a number of online tools available which website owners can use to establish if their site is vulnerable to this exploit:

- https://www.ssllabs.com/ssltest/

2. Patching vulnerable servers.

Once all vulnerable servers have been identified, website owners should take all vendor specified steps to ensure that the vulnerability is patched. Below are some resources for different operating systems that describe patching procedures:

- Ubuntu USN-2165-1: OpenSSL vulnerabilities
- Ubuntu CVE-2014-0160 detailed information per release
- Debian DSA-2896-1 openssl – security update
- Red Hat RHSA-2014:0376-1 Red Hat Enterprise Linux 6
- Red Hat RHSA-2014:0377-1 Red Hat Storage Native Client for Red Hat Enterprise Linux
- CentOS 6 CVE-2014-0160 CentOS 6 openssl heartbleed workaround
- Gentoo glsa-201404-07 OpenSSL: Information Disclosure
- Novell/Suse SUSE Linux Enterprise Server 11 and older versions with openssl 0.9.8 are not affected. Only openSUSE 12.3 and 13.1 are shipping affected versions currently.
- Tor components affected by OpenSSL bug CVE-2014-016

3. Revoking/Reissuing Keys and Certificates

If you have had a vulnerable server for any length of time at all, it is imperative, that

you revoke your website certificate and have it reissued using new crypto keys. The mechanisms around how to do this are outside the scope of this document, but you should immediately engage with your trusted IT security advisor to ensure these steps are taken. Patching alone will reduce your risk of future data compromise, but cannot fix protect any data that has already been captured through this method. This could include the cryptographic keys used to protect the data, as well as user IDs and passwords. You should carry out a risk assessment to determine what the implications are and what to address. Individuals should have separate passwords for different web services, and we recommend changing those passwords frequently.

Consultation open on Responsible Disclosure Guidelines

Posted: 8 November 2013

Today the New Zealand Internet Task Force (the NZITF) has released draft guidelines on responsible disclosure. These guidelines will help security researchers and organisations that operate ICT systems to work together to identify, understand and fix security vulnerabilities in New Zealand websites and ICT systems.

We are seeking your views on these draft guidelines to make sure that they are high quality and provide useful guidance on the aspects of responsible disclosure that need covering.

We welcome any comments or suggestions that you have on how the guidelines could be improved. We would also like to hear from you if your organisation is interesting in being named as a third party for finders to contact and act as an intermediary between them and the ICT owners that they deal with.

The guidelines are available for download at
http://nzitf.org.nz/files/NZITF_Draft_Responsible_Disclosure_Guidelines.pdf

Submissions should be sent, by email, to consult@nzitf.org.nz by Sunday 22 December (please include the words "guidelines submission" in the subject header).

Responsible Disclosure Guidelines

Posted: 3 September 2013

Media release – 3 September 2013

The New Zealand Internet Task Force (NZITF) is currently working on responsible disclosure guidelines. These guidelines will help security researchers and organisations to work together when disclosing and addressing vulnerabilities in ICT systems.

New Zealand businesses and organisations do not want to have ICT systems (such as websites) with vulnerabilities in them. Security researchers want to be able to notify organisations of vulnerabilities they come across without fear of legal action or negative publicity. It is important that we are all clear about what is expected of us when disclosing a vulnerability or when someone contacts us with a vulnerability.

Because the NZITF has a broad membership of security professionals we think that we

can provide guidance that will add value, set some clear boundaries and ultimately make it easier for security professionals to work together and help improve New Zealand's cyber security posture. The NZITF is intending to hold a public consultation on the guidelines later this year.

Local group scoops top Australian security award

Posted: 7 June 2013

Media release – 7 June 2013

The New Zealand Internet Task Force (NZITF) has beaten the Australians at their own game, taking out the top prize in the prestigious AusCERT Awards.

Winner of the 'Best Security Initiative,' the NZITF was recognised last month for its bringing together of security experts from across the country's government and private sector security communities.

New Zealand Internet Task Force Chair Mike Seddon says members of the NZITF are delighted to have been recognised on Australian soil, with the AusCERT win testament to the strength and effectiveness of the Task Force's proactive cyber security activities.

A volunteer group of security professionals across government, law enforcement, academia, information security and private sector industries, the NZITF works collaboratively to improve the cyber security posture of New Zealand in defending against and mitigating cyber based threats.

Seddon says the comprehensive make-up of the NZITF affords it a unique view of the opportunities and threats across the entire spectrum of IT security and risk.

"Our approach is grounded in collaboration and trust. In sharing amongst ourselves our knowledge and experience, the general delivery and state of IT security and risk management in New Zealand is significantly improved.
"We are a rather unique outfit in a global sense and that is why the benefits we have and will continue to deliver are a key contributor as to why New Zealand could be considered world leading in this arena."

For more information contact:

Mike Seddon
ChairNZ Internet Task Force
mike.seddon@nzitf.org.nz

NZITF wins Australian Information Security award

Posted: 23 May 2013

The New Zealand Internet Task Force has won the Award for Best Security Initiative in

the 2013 Australian Information Security Awards. The awards were held at the 2013 AusCERT Information Security Conference, and are run in conjunctions with SC Magazine.

The Best Security Initiative is presented to an individual or organisation who has developed solutions to security threats, and will build trust and confidence in the online environment.

NZITF finalist in 2013 Australian Information Security Awards

Posted: 10 May 2013

The New Zealand Internet Task Force has been announced as a finalist in the Best Security Initiative category in the 2013 Australian Information Security Awards. The award for Best Security Initiative is presented to an individual or organisation who has developed solutions to security threats.

The 2013 Australian Information Security Awards will be held at the 2013 AusCERT Information Security Conference.

Cyber Security Awareness Week 2013

Posted: 27 March 2013

New Zealand's second annual Cyber Security Awareness Week(CSAW) will be held 27 - 31 May 2013. CSAW is coordinated by NetSafe. You can find out more about CSAW at Security Central

NZITF Highly Commended in ANZIAs

Posted: 10 October 2012

The NZITF has received a Highly Commended recognition in the Security & Privacy category at the 2012 Australia and New Zealand Internet Awards (the ANZIAs). The ANZIAs judges agreed that the NZITF:

"contributes to a safer online environment for New Zealand businesses and individuals, through its' initiatives to enhance the capabilities of the security community".

The NZITF Board would like to extend it's congratulations to Aura Information Security, a member of the NZITF, who won the Security and Product category for thier RedEye Security product.

NZITF finalist in ANZIAs

Posted: 14 August 2012

The NZITF has been announced as a finalist in the Security & Privacy category at the 2012 Australia and New Zealand Internet Awards(the ANZIAs). Aura Information Security, a member of the NZITF, has also been nominated for its RedEye Security product.

The ANZIAs are a collaboration between auDA and InternetNZ, and an annual event celebrating the achievements of organisations, businesses and individuals that have made significant contributions to the development and use of the Internet in Australia and New Zealand. ANZIA winners receive recognition as industry leaders, for setting new standards in making the Internet a more inclusive, accessible and safe place. The ANZIAs category winners will be announced on October 12, 2012, for more details please visit the ANZIA website.

Cyber Security Awareness Week

Posted: 1 June 2012

New Zealand is holding it's inaugural Cyber Security Awareness Week, CSAW, 11-15 June 2012. CSAW is being coordinated by NetSafe. You can follow the weeks events via NetSafe's facebook page.

DNSChanger Diagnostic Check

Posted: 1 May 2012

Over 1000 New Zealand computers are believed to be infected with the DNSChanger malware, on 9 July it is likely that these infected machines will no longer be able to connected to the Internet.

To check if your machine is infected, and to find out how to fix this please visit the DNSChanger Diagnostic website. This website is a joint initiative between NetSafe, the New Zealand National Cyber Security Centre, and the Ministry of Economic Development.

Bruce Schneier Public Event

Posted: 2 April 2012

The NZITF is proud to annouce a public lecture by Bruce Schneier, Liars and Outliers, Tuesday 1 May 2012. This is event is free to attend but RSVP's are essential. More info...

NZ Lawyer Magazine Article

Posted: 23 March 2012

An article has been recently published in the NZ Lawyer magazine provides some useful suggestions for organisations that are looking to improve their online security. (Article)

SC Magazine Article

Posted: 9 March 2012

A recent article in SC Magazine Australia looks at the effort in New Zealand and Australia to establish a certification for the penetration testing industry. (Article)