Security in New Zealand 101

NetHui 2012

Shaping Our Future Together

What are the threats to New Zealand?

BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER

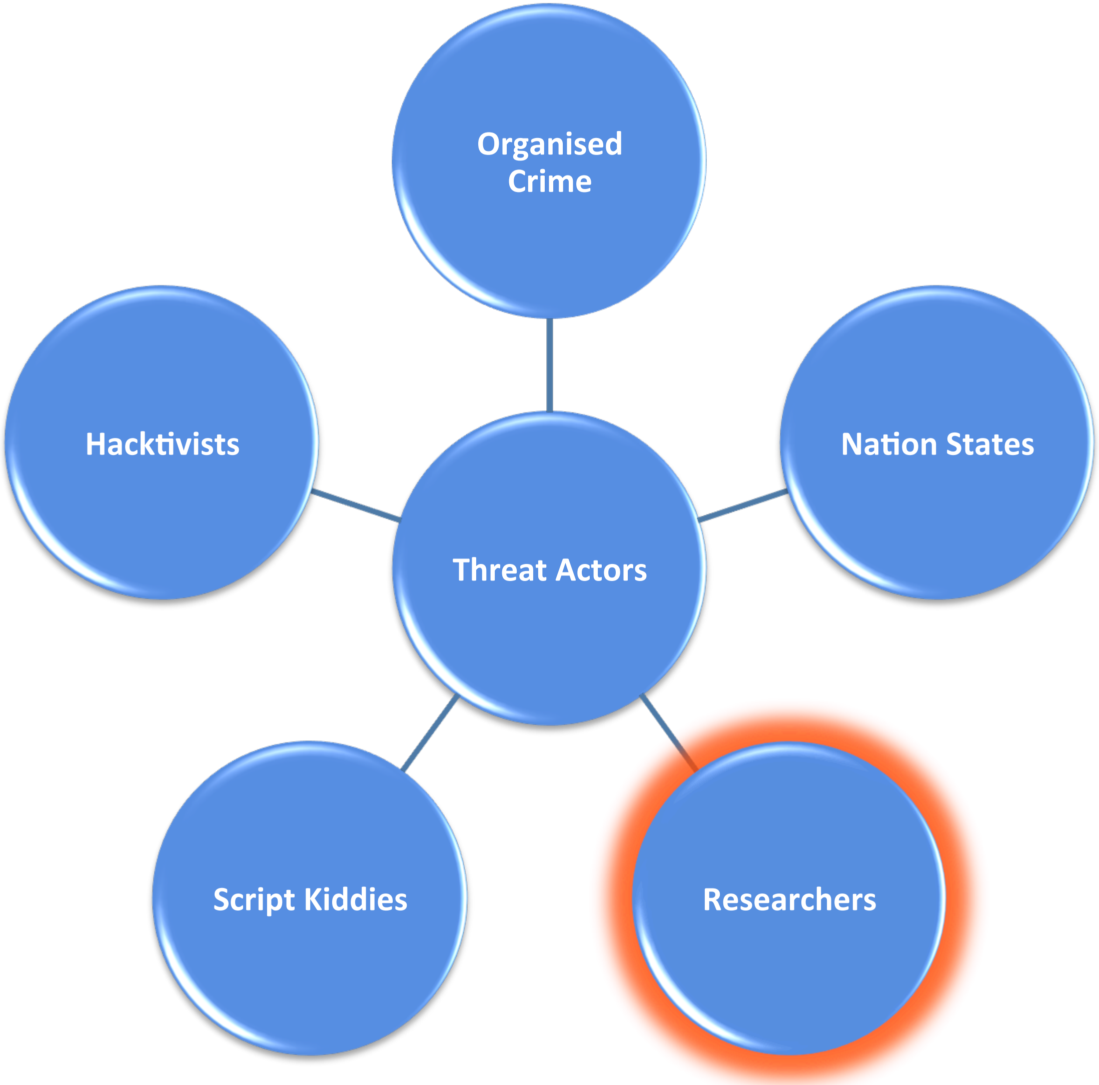
The state of play in 2000

- Relatively simple systems
- Limited network interconnectivity
- Computer network defence was a relatively new industry
- The threat:
  - Primarily a nuisance
  - Individuals attempting to gain notoriety
  - Evolution of threats was a slow life cycle
  - Overt attacks

The Threats Today

- Very complex systems
- Highly interconnected networks
- Cyber Security while still a young industry has matured a lot
- The threat:
    - Pose a serious risk to New Zealand
    - Economic gain and intelligence collection
    - Evolution of threats is very rapid
    - Covert Attacks

Threat Actors



Organised Crime

Hacktivists

Nation States

Threat Actors

Script Kiddies

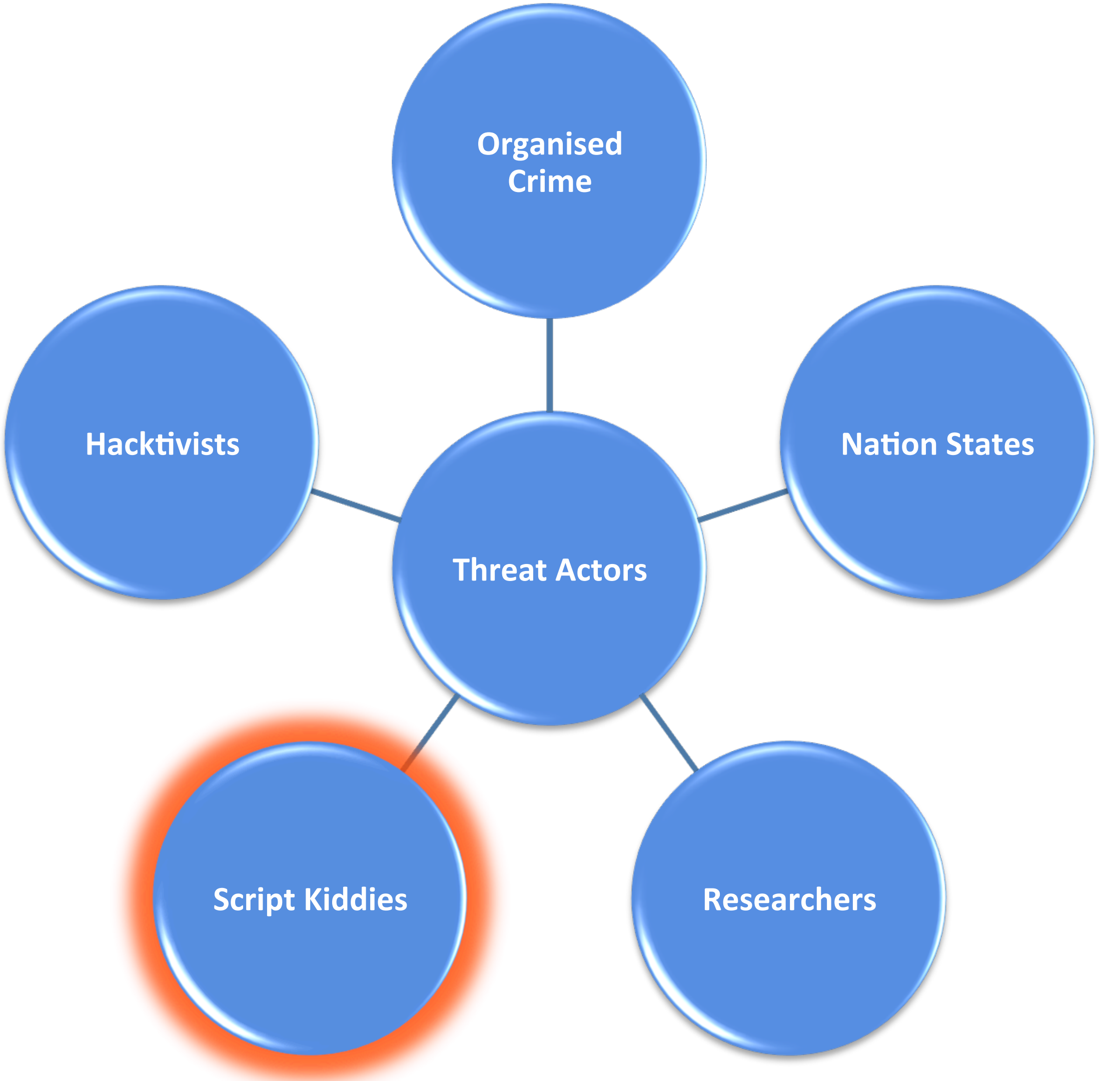
Researchers

Researchers

Hackers, Whitehats, Greyhats, Blackhats

- Pushing the envelope on both the offensive and defensive fronts
- Different types of researchers, there are those that:
  - Find the vulnerabilities
  - Fix the vulnerabilities
  - Write exploits for the vulnerabilities
- Motivations vary:
  - Curiosity, interest, knowledge
  - Notoriety, reputation
  - Profit

Threat Actors



Account Compromises

- Politician Peter Dunne’s facebook account was hacked and a pornographic image was sent to all his ‘friends’

facebook +

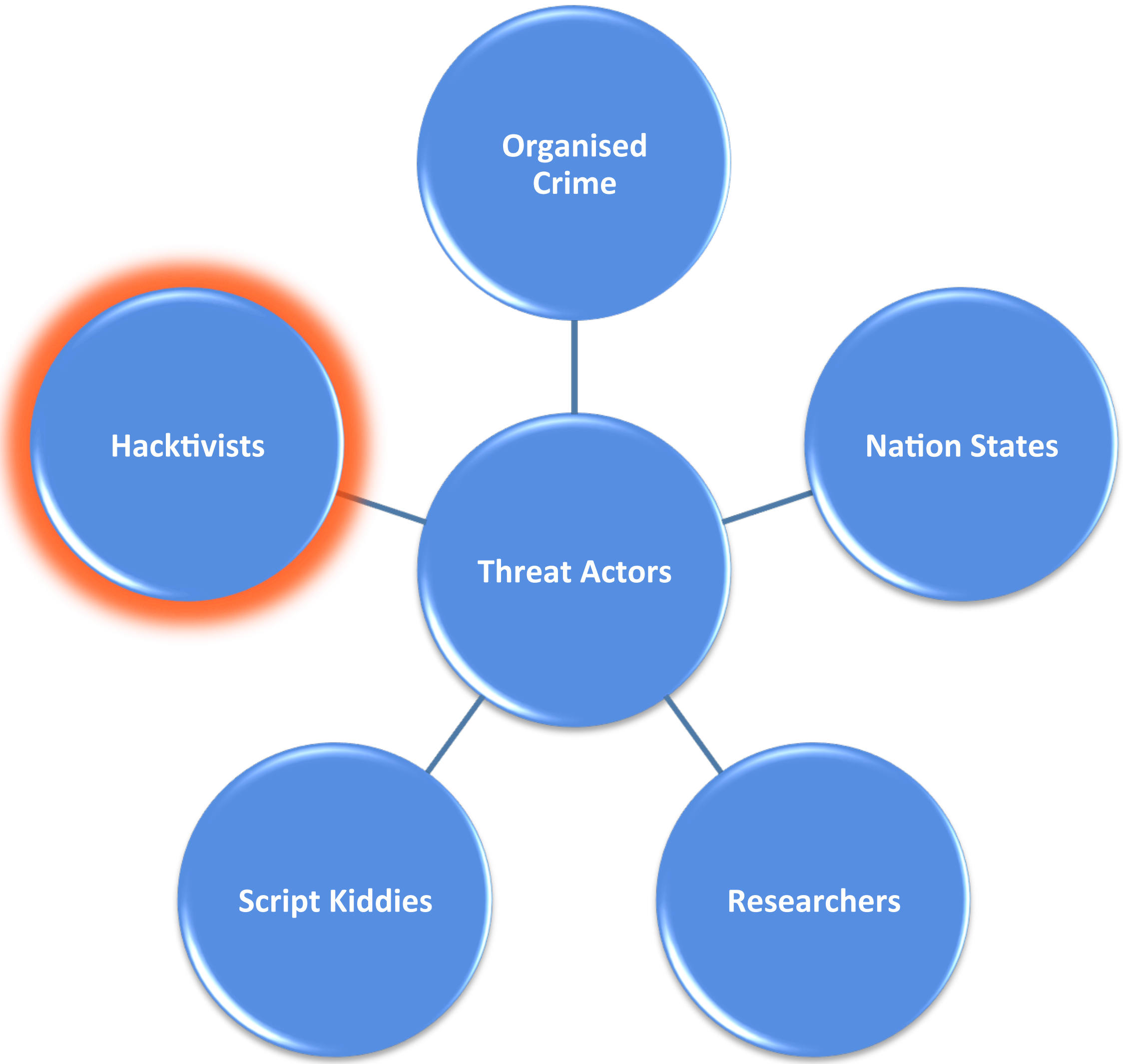
www.stuff.co.nz/2330280

Identify Theft / Fraud

twitter +

www.tewahanui.info/wordpress2/?p=2092

Threat Actors



Threat Actors

Organised Crime

Nation States

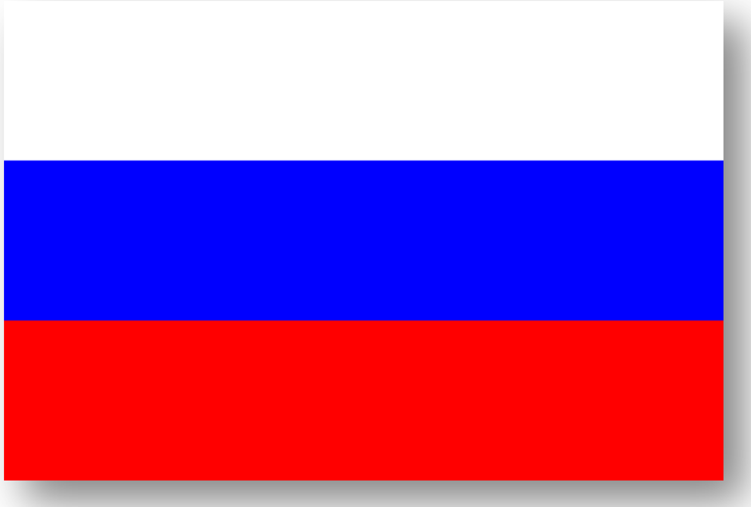
Researchers

Script Kiddies

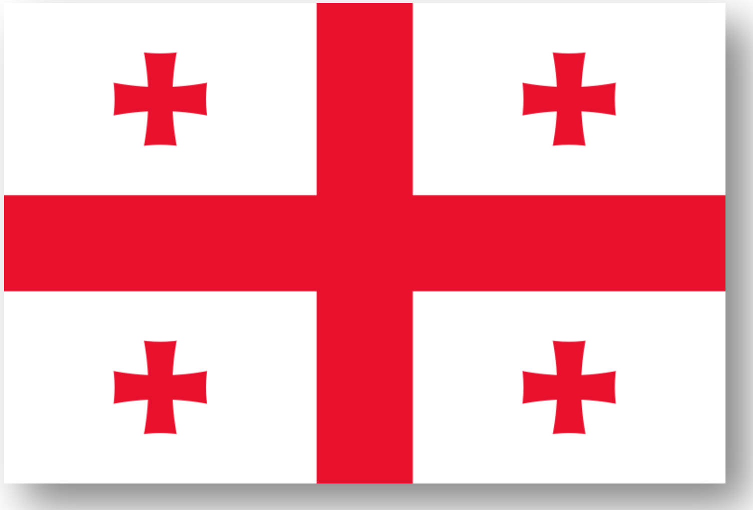
Hacktivists

Hacktivists

Georgian Conflict August 2008



VS

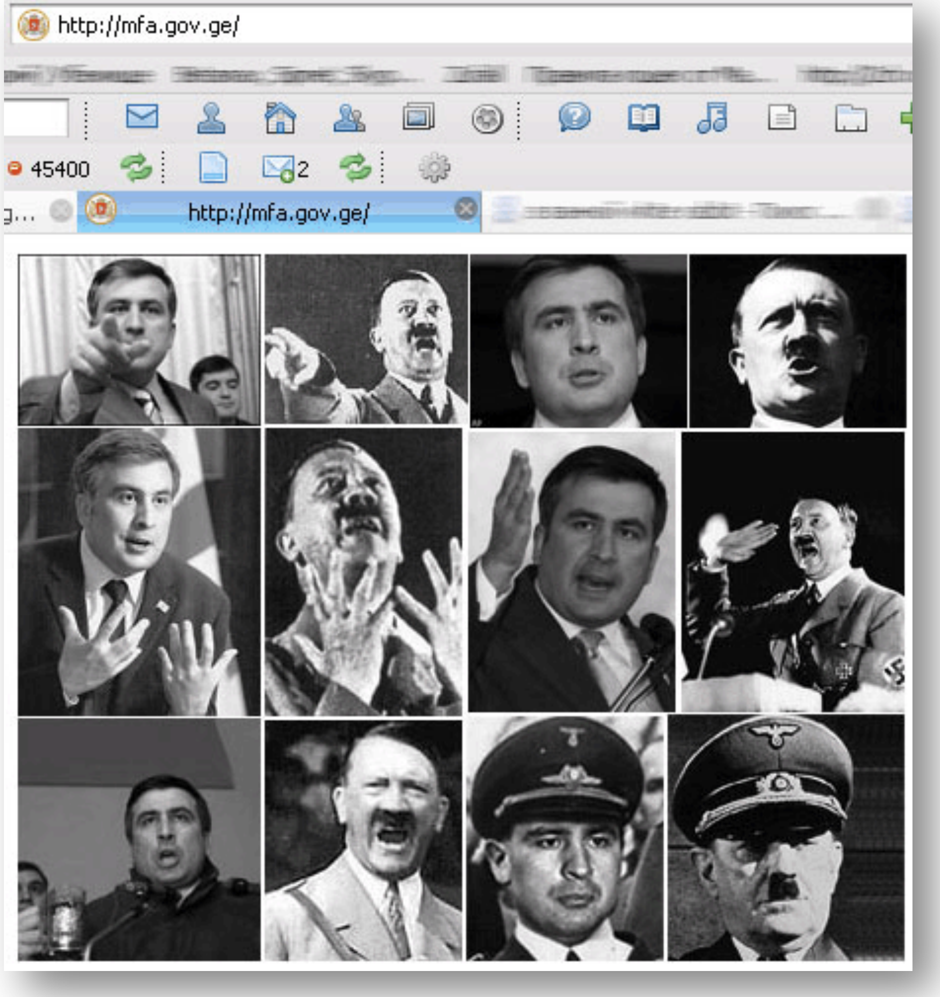


Russia

Georgia

Hacktivists

Georgian President Mikheil Saakashvili defacement



Security in NZ 101

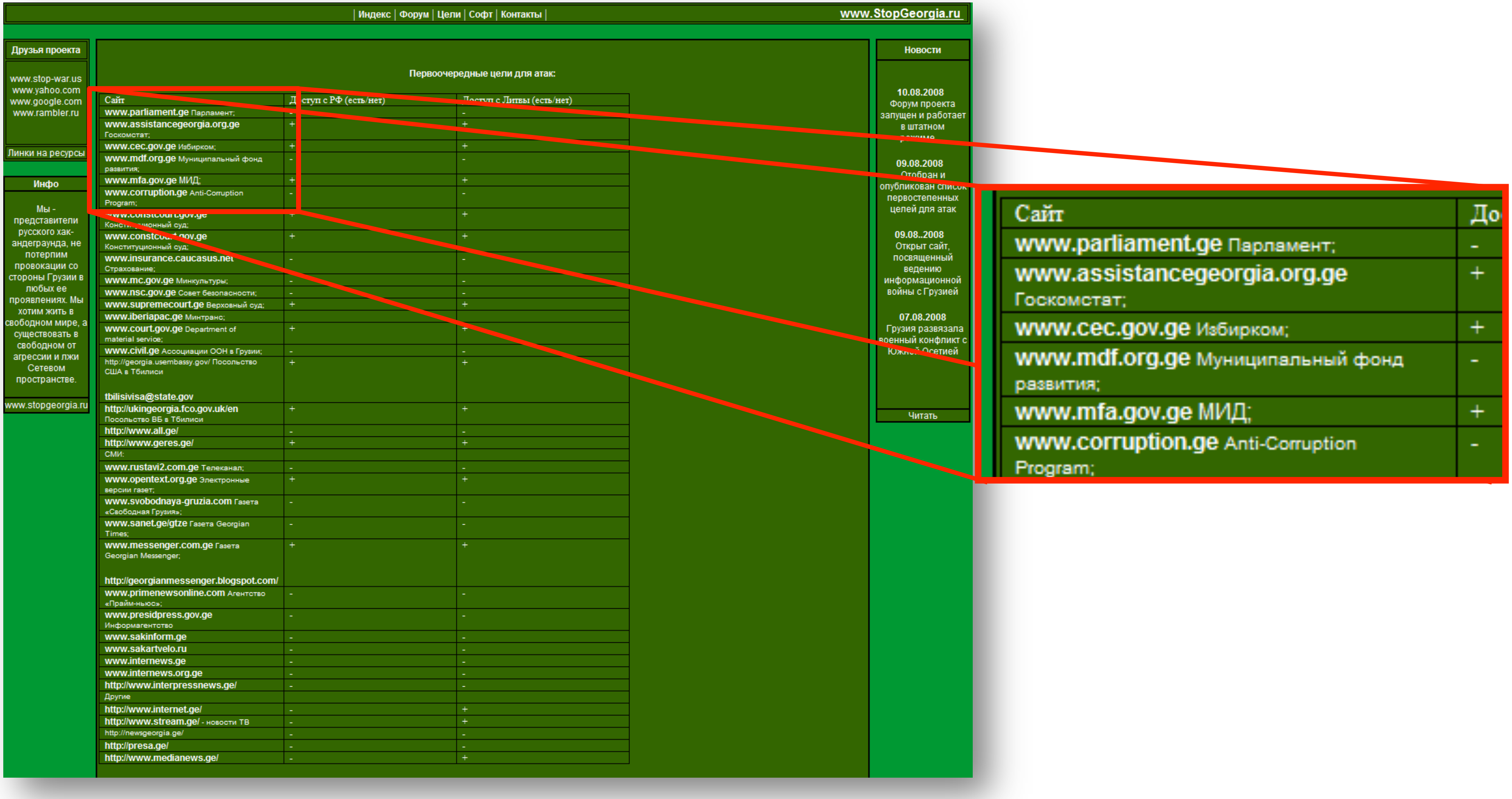
Hacktivists

Coordination of the attacks

- Lists of targets distributed across Russian web forums:
  - www.police.ge
  - www.mfa.gov.ge
  - www.goverment.ge
  - www.constcourt.gov.ge
  - www.mod.gov.ge
  - www.nsc.gov.ge
  - www.mof.ge
  - www.nbg.gov.ge
- Lists of targets posted on Russian websites:
  - www.stopgeorgia.ru
  - www.stopgeorgia.info

Hacktivists

Coordination of the attacks



| Индекс | Форум | Цели | Софт | Контакты | www.StopGeorgia.ru

Друзья проекта

www.stop-war.us
www.yahoo.com
www.google.com
www.rambler.ru

Линки на ресурсы

Инфо

Мы - представители русского хак-андеграунда, не потерпим провокации со стороны Грузии в любых ее проявлениях. Мы хотим жить в свободном мире, а существовать в свободном от агрессии и лжи Сетевом пространстве.

www.stopgeorgia.ru

Первоочередные цели для атак:

Сайт	Доступ с РФ (есть/нет)	Доступ с Литвы (есть/нет)
www.parliament.ge Парламент;	-	-
www.assistancegeorgia.org.ge Госкомстат;	+	+
www.cec.gov.ge Избирком;	+	+
www.mdf.org.ge Муниципальный фонд развития;	-	-
www.mfa.gov.ge МИД;	+	+
www.corruption.ge Anti-Corruption Program;	-	-
www.constcourt.gov.ge Конституционный суд;	+	+
www.constcourt.gov.ge Конституционный суд;	+	+
www.insurance.caucasus.net Страхование;	-	-
www.mc.gov.ge Минкультуры;	-	-
www.nsc.gov.ge Совет безопасности;	-	-
www.supremecourt.ge Верховный суд;	+	+
www.iberiapac.ge Минтранс;		
www.court.gov.ge Department of material service;	+	+
www.civil.ge Ассоциации ООН в Грузии;	-	-
http://georgia.usembassy.gov/ Посольство США в Тбилиси tbilisivisa@state.gov	+	+
http://ukingeorgia.fco.gov.uk/en Посольство ВБ в Тбилиси	+	+
http://www.all.ge/	-	-
http://www.geres.ge/	+	+
СМИ:		
www.rustavi2.com.ge Телеканал;	-	-
www.opentext.org.ge Электронные версии газет;	+	+
www.svobodnaya-gruzia.com Газета «Свободная Грузия»;	-	-
www.sanet.ge/gtze Газета Georgian Times;	-	-
www.messenger.com.ge Газета Georgian Messenger; http://georgianmessenger.blogspot.com/	+	+
www.primenewsonline.com Агентство «Прайм-ньюс»;	-	-
www.presidpress.gov.ge Информагентство	-	-
www.sakinform.ge	-	-
www.sakartvelo.ru	-	-
www.internews.ge	-	-
www.internews.org.ge	-	-
http://www.interpressnews.ge/	-	-
Другие		
http://www.internet.ge/	-	+
http://www.stream.ge/ - новости ТВ	-	+
http://newsgeorgia.ge/	-	-
http://presa.ge/	-	-
http://www.medianews.ge/	-	+

Новости

10.08.2008
Форум проекта запущен и работает в штатном режиме

09.08.2008
Отобран и опубликован список первостепенных целей для атак

09.08..2008
Открыт сайт, посвященный ведению информационной войны с Грузией

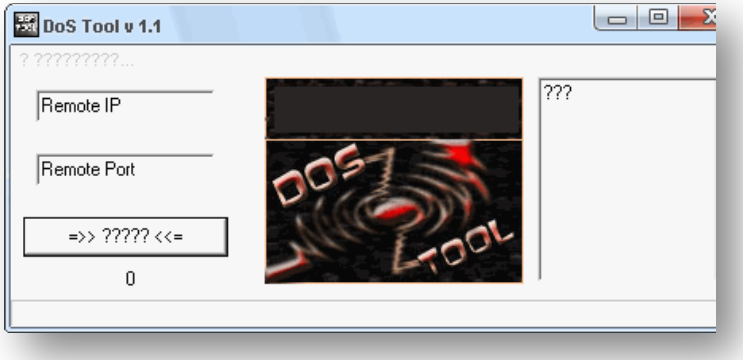
07.08.2008
Грузия развязала военный конфликт с Южной Осетией

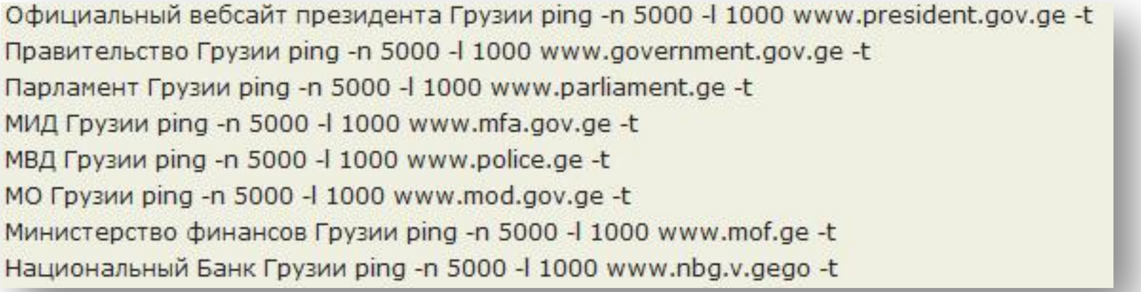
Читать

Сайт	До
www.parliament.ge Парламент;	-
www.assistancegeorgia.org.ge Госкомстат;	+
www.cec.gov.ge Избирком;	+
www.mdf.org.ge Муниципальный фонд развития;	-
www.mfa.gov.ge МИД;	+
www.corruption.ge Anti-Corruption Program;	-

Hacktivists

Denial of Service Attacks

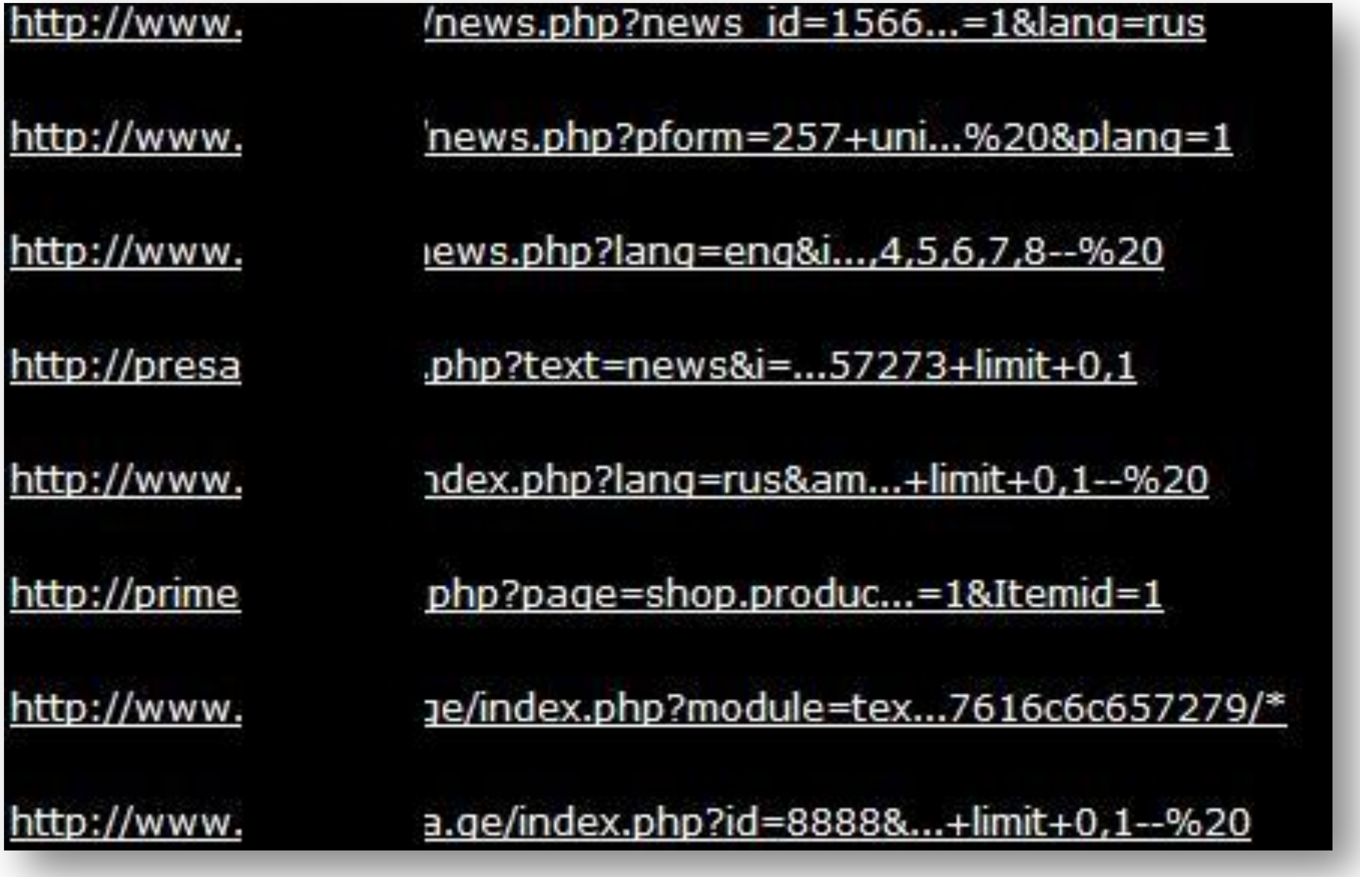




Официальный вебсайт президента Грузии ping -n 5000 -l 1000 www.president.gov.ge -t
Правительство Грузии ping -n 5000 -l 1000 www.government.gov.ge -t
Парламент Грузии ping -n 5000 -l 1000 www.parliament.ge -t
МИД Грузии ping -n 5000 -l 1000 www.mfa.gov.ge -t
МВД Грузии ping -n 5000 -l 1000 www.police.ge -t
МО Грузии ping -n 5000 -l 1000 www.mod.gov.ge -t
Министерство финансов Грузии ping -n 5000 -l 1000 www.mof.ge -t
Национальный Банк Грузии ping -n 5000 -l 1000 www.nbg.v.gego -t

Hacktivists

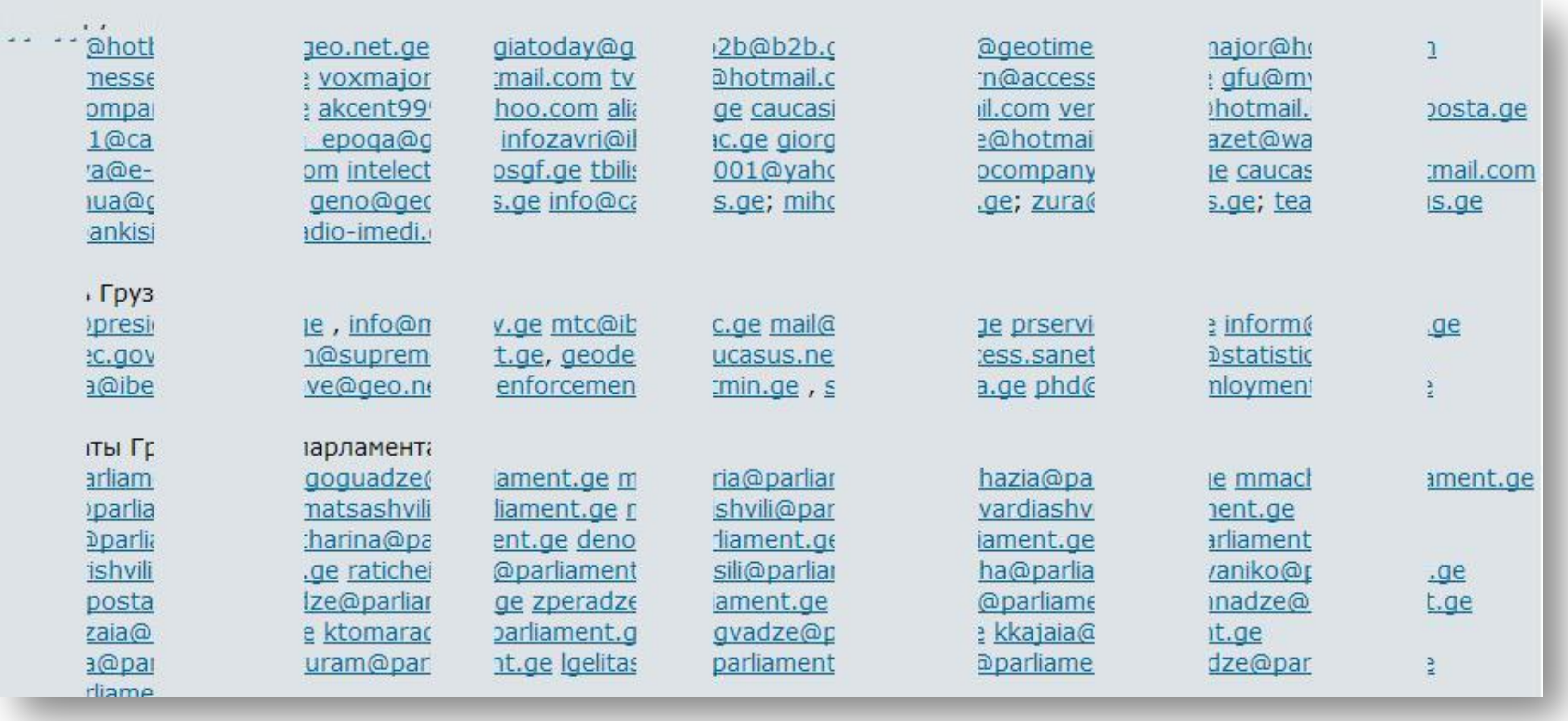
Sites vulnerable to SQL injection attacks



```
http://www.        /news.php?news_id=1566...=1&lang=rus

http://www.        'news.php?pform=257+uni...%20&plang=1

http://www.        ıews.php?lang=eng&i...,4,5,6,7,8--%20

http://presa       .php?text=news&i=...57273+limit+0,1

http://www.        ıdex.php?lang=rus&am...+limit+0,1--%20

http://prime       php?page=shop.produc...=1&Itemid=1

http://www.        ȷe/index.php?module=tex...7616c6c657279/*

http://www.        a.ge/index.php?id=8888&...+limit+0,1--%20
```

Hacktivists

Email addresses of Georgian Politicians

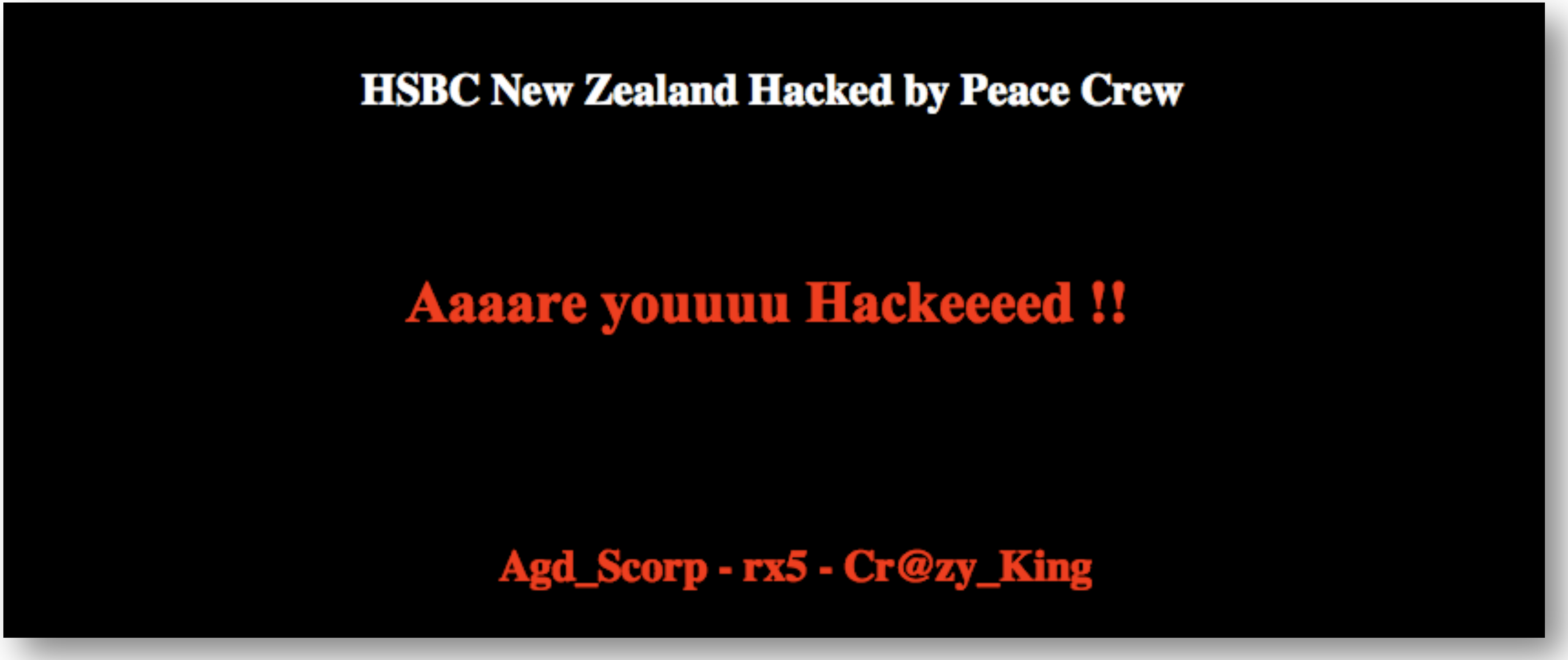


@hotl	geo.net.ge	giatoday@g	2b@b2b.c	@geotime	najor@hc	n
nesse	e voxmajor	mail.com tv	@hotmail.c	n@access	e gfu@my	
ompa	e akcent99	hoo.com ali	ge caucasi	il.com ver	hotmail.	posta.ge
1@ca	epoqa@g	infozavri@il	ac.ge giorg	e@hotmai	azet@wa	
a@e-	om intelect	psgf.ge tbilis	001@yahc	ocompany	ge caucas	mail.com
ua@g	geno@geo	s.ge info@ca	s.ge; mihc	.ge; zura@	s.ge; tea	is.ge
ankisi	adio-imedi.					
Груз						
presi	ge , info@m	v.ge mtc@ib	c.ge mail@	ge prservi	e inform@	.ge
c.gov	n@suprem	t.ge, geode	ucasus.ne	ess.sanet	@statistic	
a@ibe	ve@geo.ne	enforcemen	min.ge , s	a.ge phd@	nloyment	e
ты Гр	парламента					
arliam	goguadze	ament.ge m	ria@parliar	hazia@pa	ge mmach	ament.ge
parlia	natsashvili	liament.ge r	shvili@par	vardiashv	nent.ge	
@parli	harina@pa	ent.ge deno	rliament.ge	iament.ge	arliament	
ishvili	.ge ratichei	@parliament	sili@parliar	ha@parlia	vaniko@p	.ge
posta	dze@parliar	ge zperadze	ament.ge	@parliame	nadze@	t.ge
zaia@	e ktomarad	parliament.g	gvadze@p	e kkajaia@	nt.ge	
a@pai	uram@par	nt.ge lgelitas	parliament	@parliame	dze@par	e
rliame						

Hacktivists

- One of NZ’s largest registrars was hacked in 2009
- Management control panel was hacked via a SQL injection attack
- Domain records altered to point to defaced pages:
  - bitdefender.co.nz
  - coca-cola.co.nz
  - f-secure.co.nz
  - fanta.co.nz
  - hsbc.co.nz
  - hotmail.co.nz
  - linux.co.nz
  - live.co.nz
  - microsoft.co.nz
  - msdn.co.nz
  - msn.co.nz
  - msn.org.nz
  - sony.co.nz
  - windowslive.co.nz
  - xerox.co.nz

Defaced Websites



HSBC New Zealand Hacked by Peace Crew

Aaaare youuuu Hackeeeed !!

Agd_Scorp - rx5 - Cr@zy_King

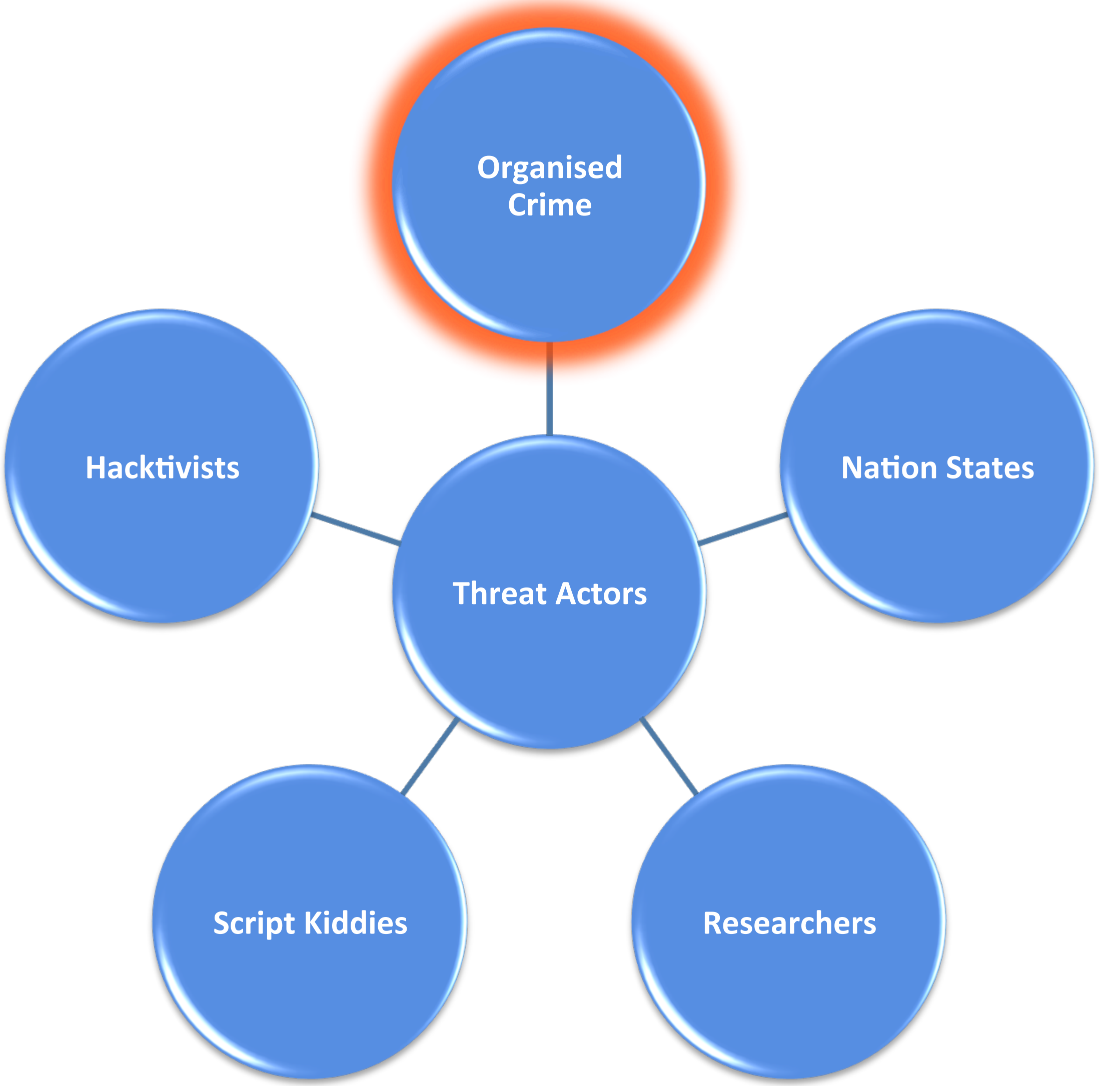
www.stuff.co.nz/2354157

Denial of Service Attacks

Vs

www.stuff.co.nz/4930058

Threat Actors



Organised Crime

Hacktivists

Nation States

Threat Actors

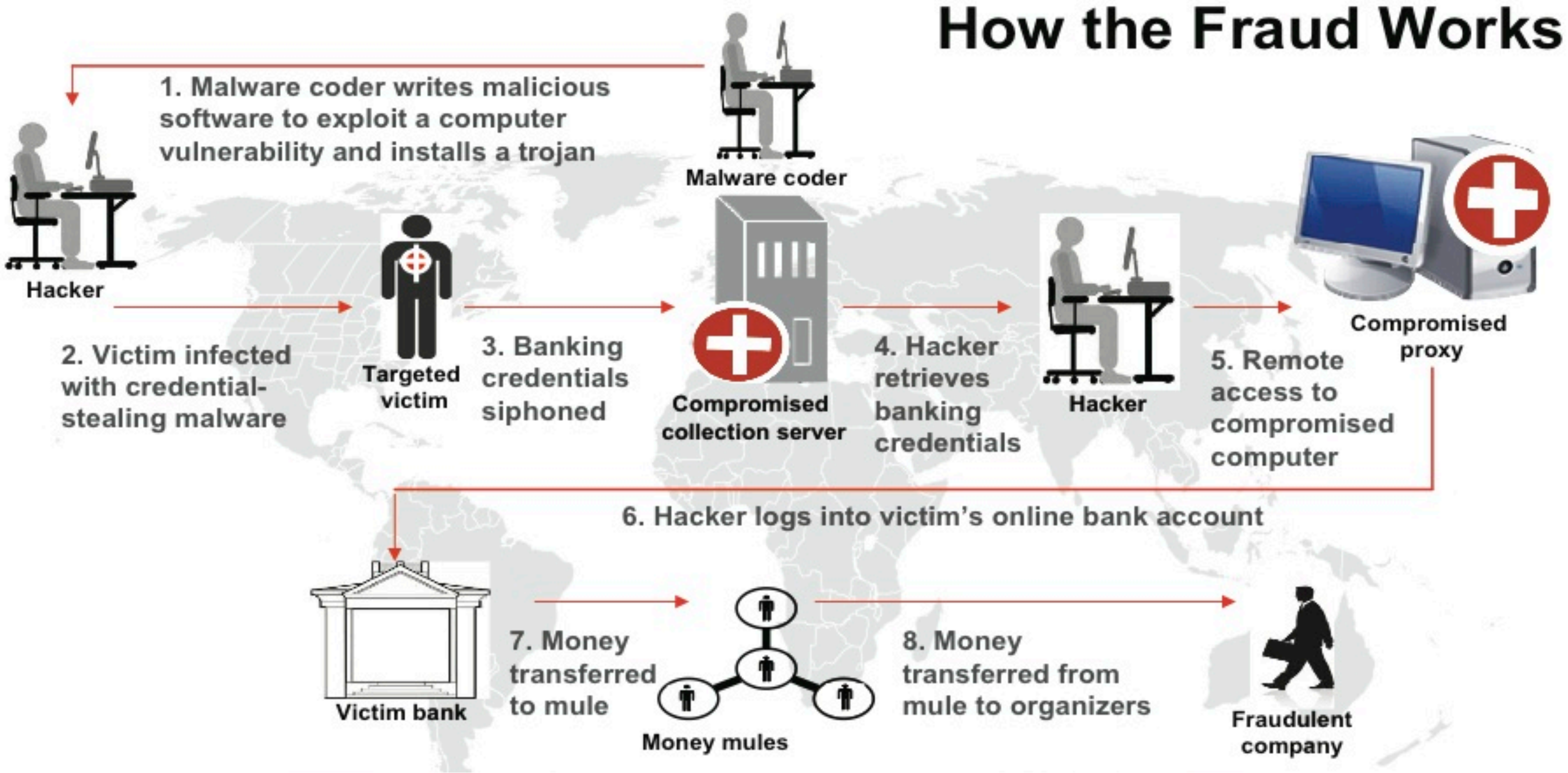
Script Kiddies

Researchers

Organised Crime

- Traditional criminal activities now carried out electronically:
  - Identify Theft
  - Harvesting Credentials
  - Skimming ATM’s
  - Corporate Espionage
  - Blackmail
  - Ransom
  - Piracy
  - Counterfeiting

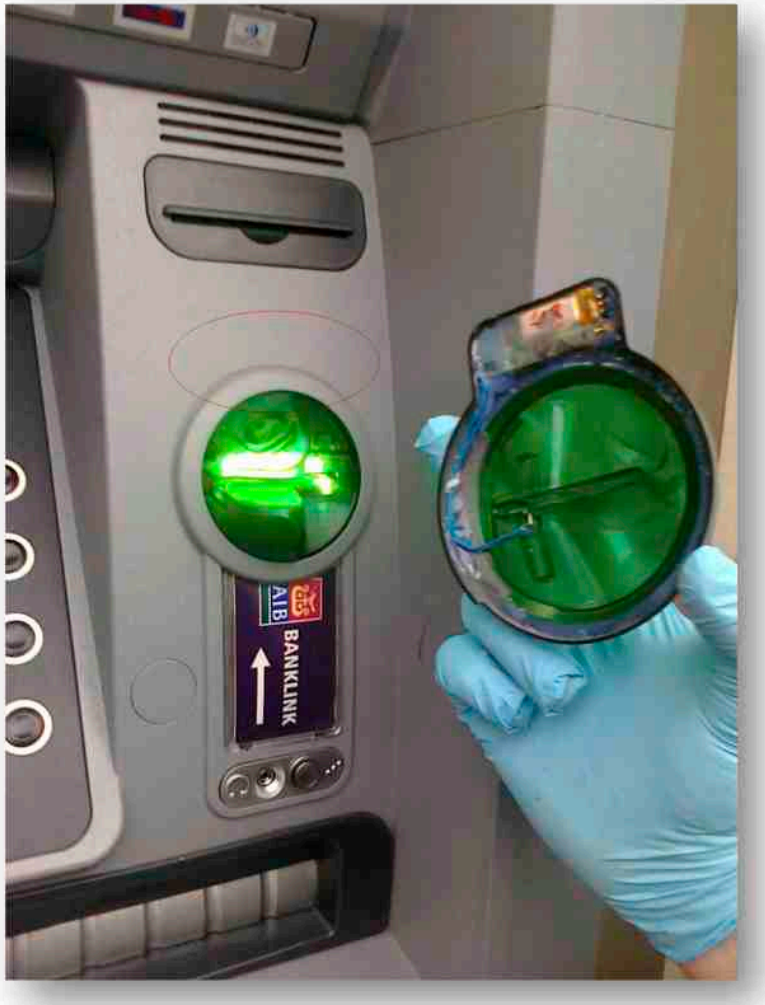
Zeus Banking Malware


How the Fraud Works
1. Malware coder writes malicious software to exploit a computer vulnerability and installs a trojan
Malware coder
Hacker
2. Victim infected with credential-stealing malware
Targeted victim
3. Banking credentials siphoned
Compromised collection server
4. Hacker retrieves banking credentials
Hacker
5. Remote access to compromised computer
Compromised proxy
6. Hacker logs into victim's online bank account
Victim bank
7. Money transferred to mule
Money mules
8. Money transferred from mule to organizers
Fraudulent company

http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud

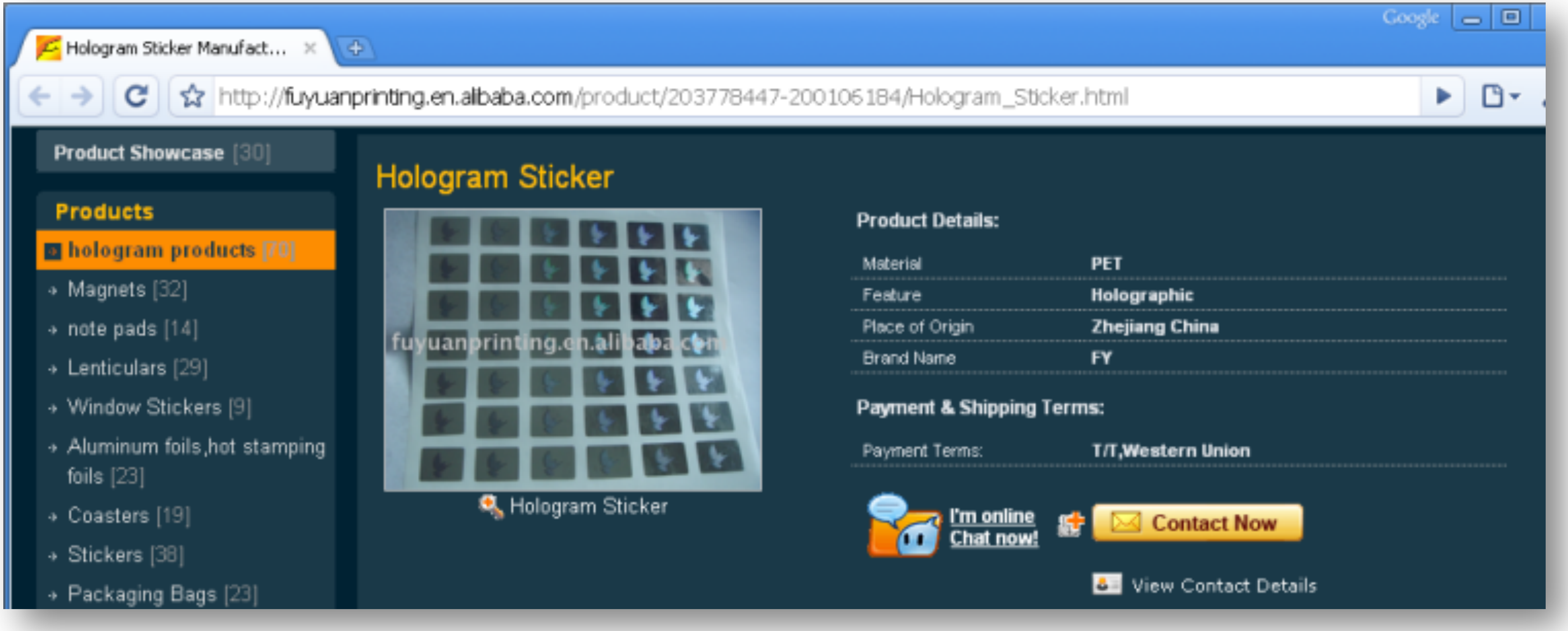
Installing Skimmer

Latest Skimming Devices



Credit Card Blanks

Organised Crime



Hologram Sticker Manufact...

http://fuyuanprinting.en.alibaba.com/product/203778447-200106184/Hologram_Sticker.html

Product Showcase [30]

Products

- hologram products [70]
- Magnets [32]
- note pads [14]
- Lenticulars [29]
- Window Stickers [9]
- Aluminum foils,hot stamping foils [23]
- Coasters [19]
- Stickers [38]
- Packaging Bags [23]

Hologram Sticker

Hologram Sticker

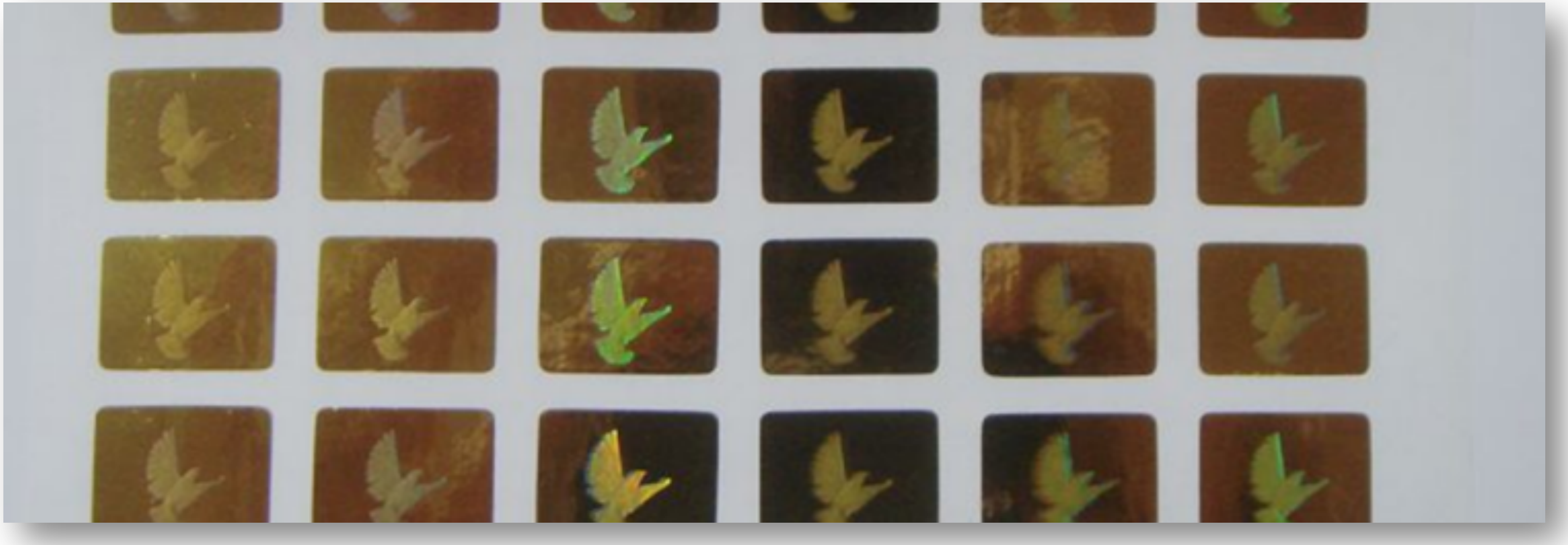
Product Details:

Material	PET
Feature	Holographic
Place of Origin	Zhejiang China
Brand Name	FY

Payment & Shipping Terms:

Payment Terms:	T/T,Western Union

Organised Crime



Organised Crime

Data Theft

- Shell Oil’s website for fuel cards hacked
- Details of approximately 6,000 New Zealanders and Australians were stolen

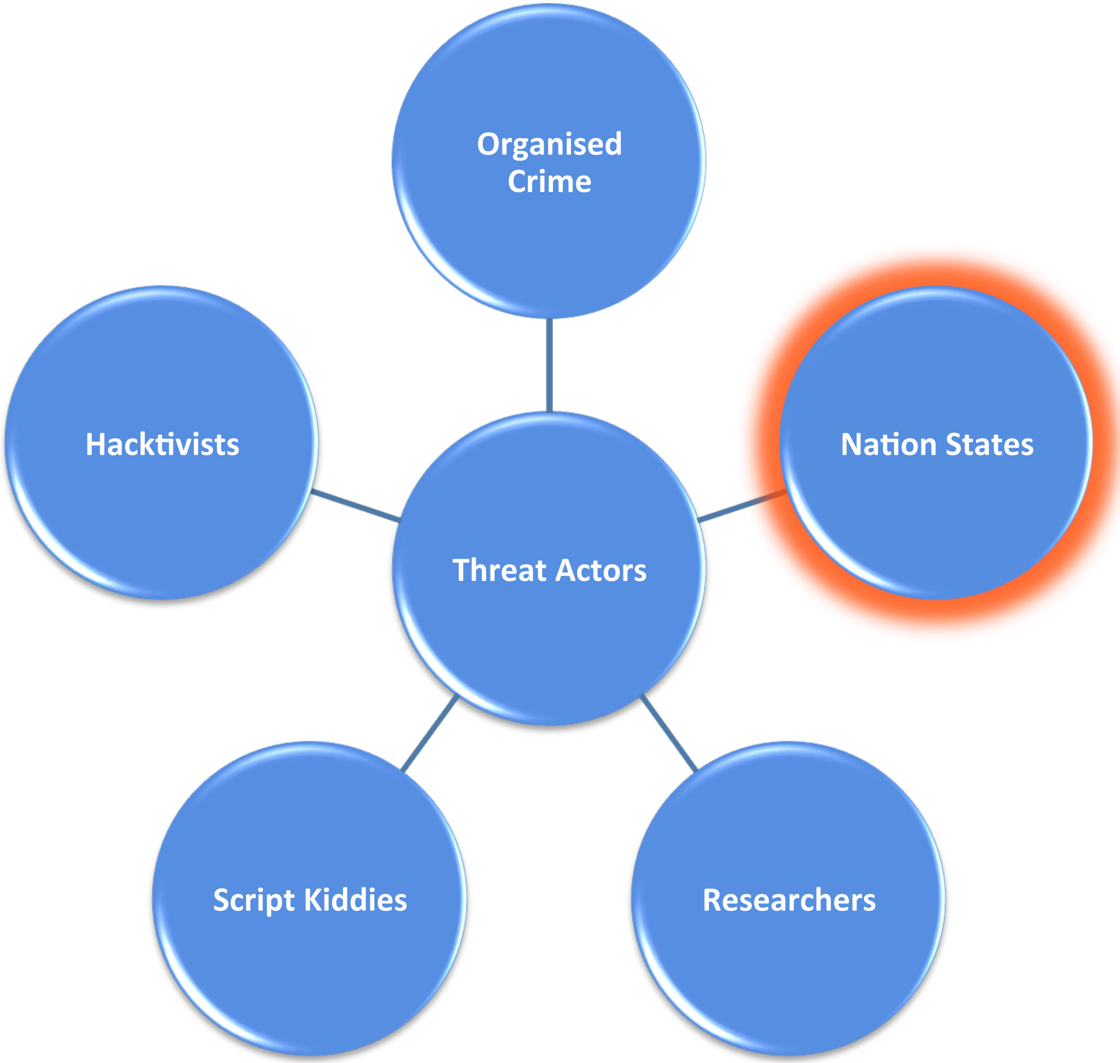
www.stuff.co.nz/2269256

Data Theft

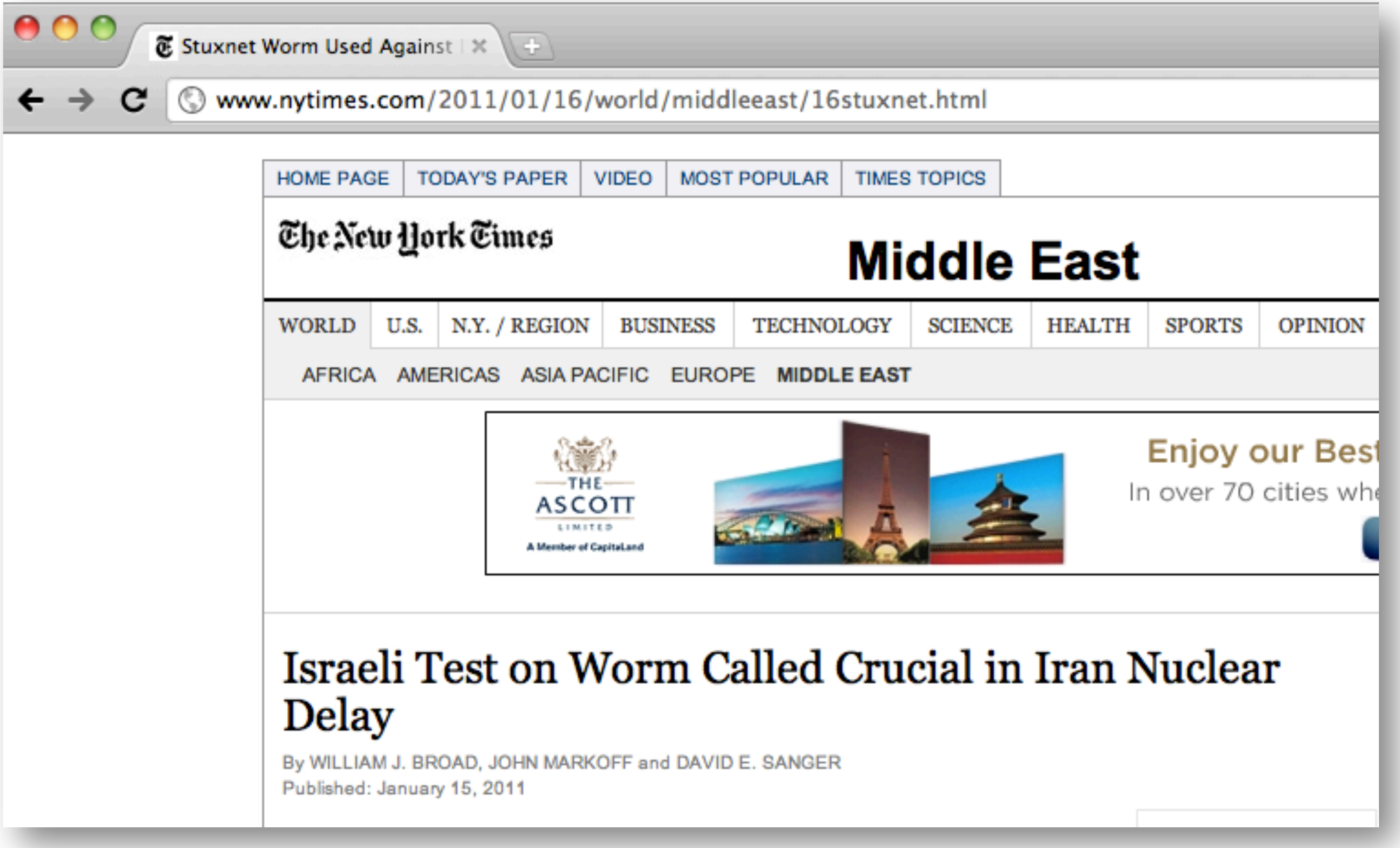
- Lush’s website hacked
- Informed 9,000 New Zealanders that the following were possibly compromised:
  - Credit card details
  - Customers' names
  - Addresses
  - Phone numbers
  - Dates of birth.

www.stuff.co.nz/4662025

Threat Actors



Nation States - Stuxnet

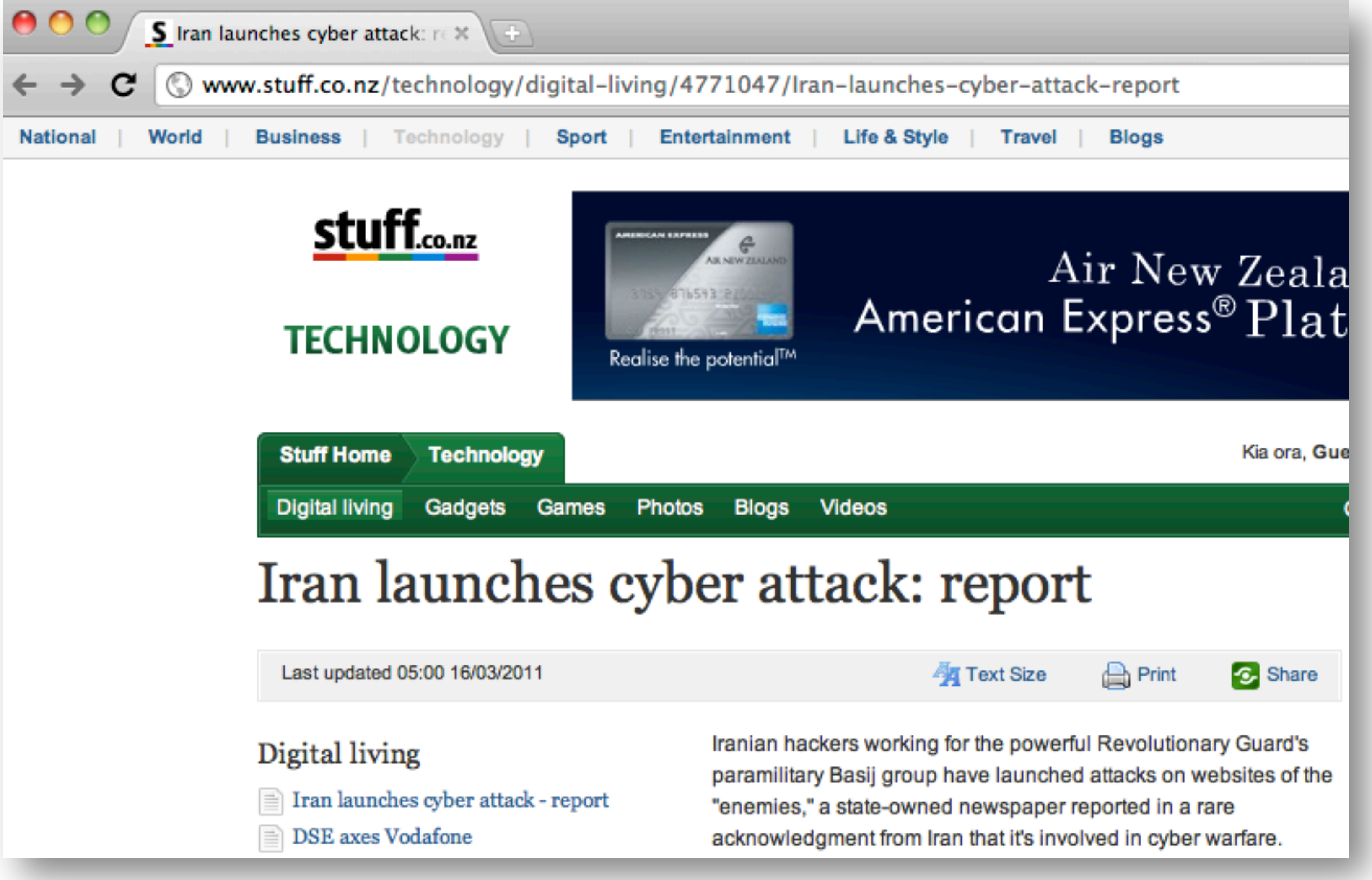


Middle East

Israeli Test on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER
Published: January 15, 2011

Nation States



Iran launches cyber attack: r
www.stuff.co.nz/technology/digital-living/4771047/Iran-launches-cyber-attack-report
National | World | Business | Technology | Sport | Entertainment | Life & Style | Travel | Blogs
stuff.co.nz
TECHNOLOGY

Stuff Home
Technology
Kia ora, Gue
Digital living
Gadgets
Games
Photos
Blogs
Videos

Iran launches cyber attack: report

Last updated 05:00 16/03/2011

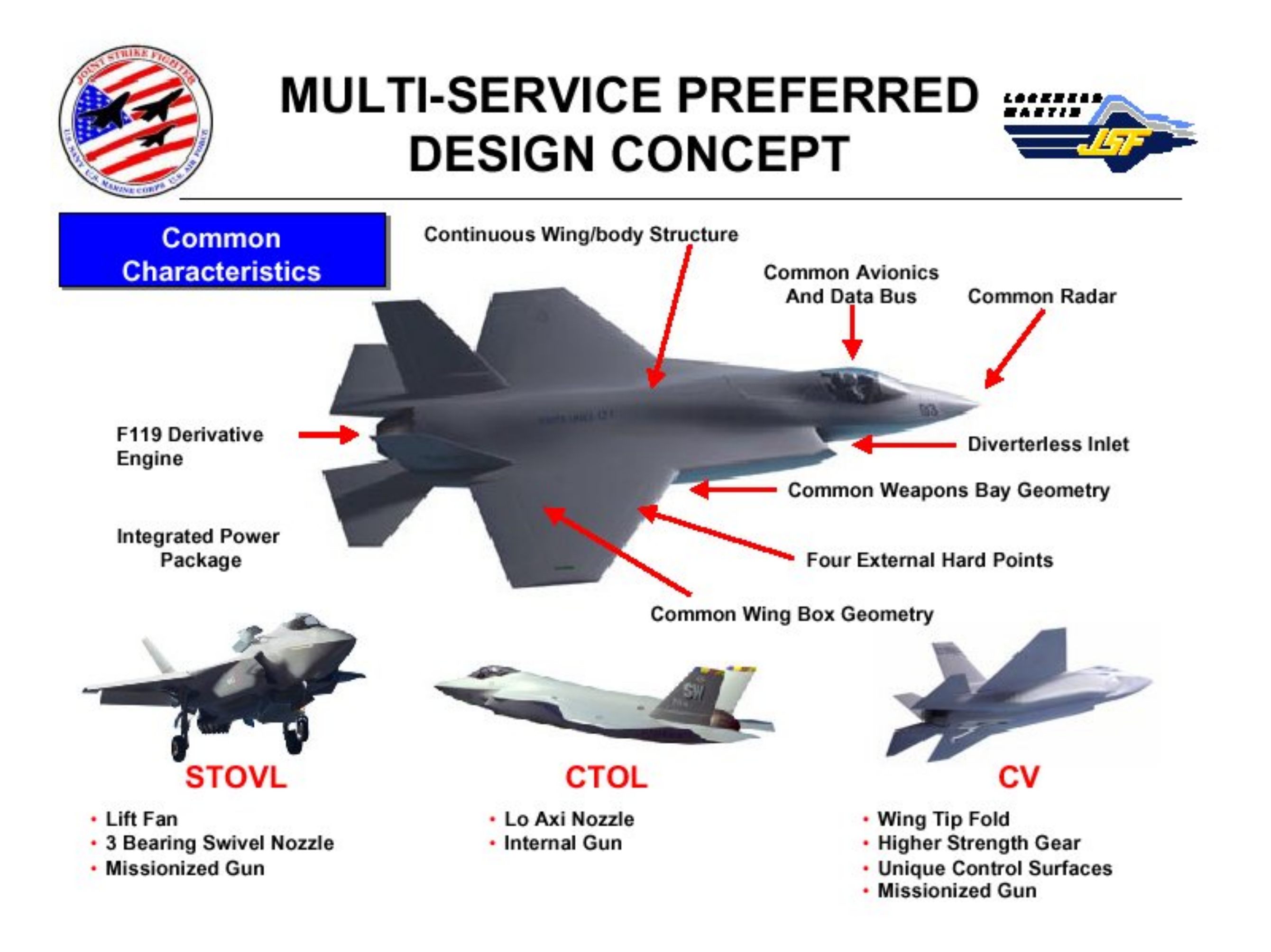
Digital living

- Iran launches cyber attack - report
- DSE axes Vodafone

Iranian hackers working for the powerful Revolutionary Guard's paramilitary Basij group have launched attacks on websites of the "enemies," a state-owned newspaper reported in a rare acknowledgment from Iran that it's involved in cyber warfare.

Nation States

Joint Strike Fighter Plans



MULTI-SERVICE PREFERRED DESIGN CONCEPT

Common Characteristics

Continuous Wing/body Structure

Common Avionics And Data Bus

Common Radar

F119 Derivative Engine

Diverterless Inlet

Common Weapons Bay Geometry

Integrated Power Package

Four External Hard Points

Common Wing Box Geometry

STOVL

- Lift Fan
- 3 Bearing Swivel Nozzle
- Missionized Gun

CTOL

- Lo Axi Nozzle
- Internal Gun

CV

- Wing Tip Fold
- Higher Strength Gear
- Unique Control Surfaces
- Missionized Gun

Nation States - GhostNET

+

http://www.wired.com/threatlevel/2009/03/spy-system-focu/

The Threats Today

- Very complex systems
- Highly interconnected networks
- Cyber Security while still a young industry has matured a lot
- The threat:
    - Pose a serious risk to New Zealand
    - Economic gain and intelligence collection
    - Evolution of threats is very rapid
    - Covert Attacks

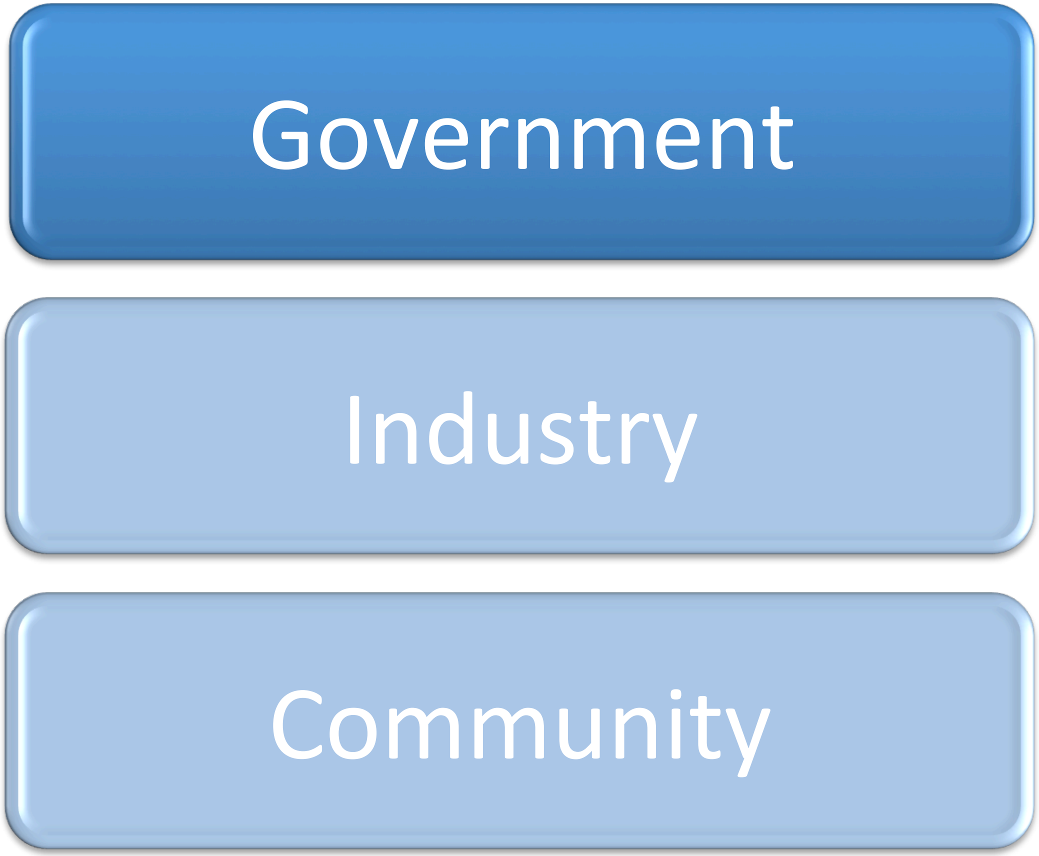
Mitigating the Threats

Government

Industry

Community

Mitigating the Threats



Government

Industry

Community

New Zealand's Cyber Security Strategy

- The New Zealand Government announced the strategy in June 2011
- "The Government is strengthening the co-ordination of policy advice on the overall strategic direction for addressing cyber security."
- http://bit.ly/LXAtBC

NEW ZEALAND'S
CYBER SECURITY STRATEGY

June 2011

New Zealand Government

New Zealand's Cyber Security Strategy

- It identifies Key and Longer-Term initiatives in three priority areas:
  - Increasing Awareness and Online Security
  - Protecting Government Systems and Information
  - Incident Response and Planning

NEW ZEALAND'S
CYBER SECURITY STRATEGY

June 2011

New Zealand Government

Increasing Awareness and Online Security

- Key initiatives:
  - Partner with industry and non-government organisations, such as *NetSafe,* to:
    - centralise cyber security information and resources for ease of access; and
    - deliver a coordinated cyber safety awareness-raising programme.
- Longer-term initiative:
  - Progress work with Internet Service Providers to develop appropriate solutions to address cyber security issues, such as infected computers and botnets.

Protecting Government Systems and Information

- Key initiatives:
  - Establish a National Cyber Security Centre within the Government Communications Security Bureau.
  - Implement steps to improve cyber security practices in government agencies.
    - DSD 35 Mitigations (http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm)

Incident Response and Planning

- Key initiatives:
  - Establish a National Cyber Security Centre, which will absorb the functions of the CCIP.
  - Revise the Government's national cyber incident response plan.
  - Expand work with industry, including critical national infrastructure providers and businesses to support them to review their cyber security responses.
- Longer-term initiatives:
  - Work with interested parties to determine the need for a New Zealand CERT.

New Zealand's Cyber Security Strategy

- The New Zealand Government operates the National Cyber Security Centre (NCSC)
- www.ncsc.govt.nz

- The NCSC is a business unit of the Government Communications Security Bureau (GCSB)
- www.gcsb.govt.nz

The National Cyber Security Centre (NCSC)

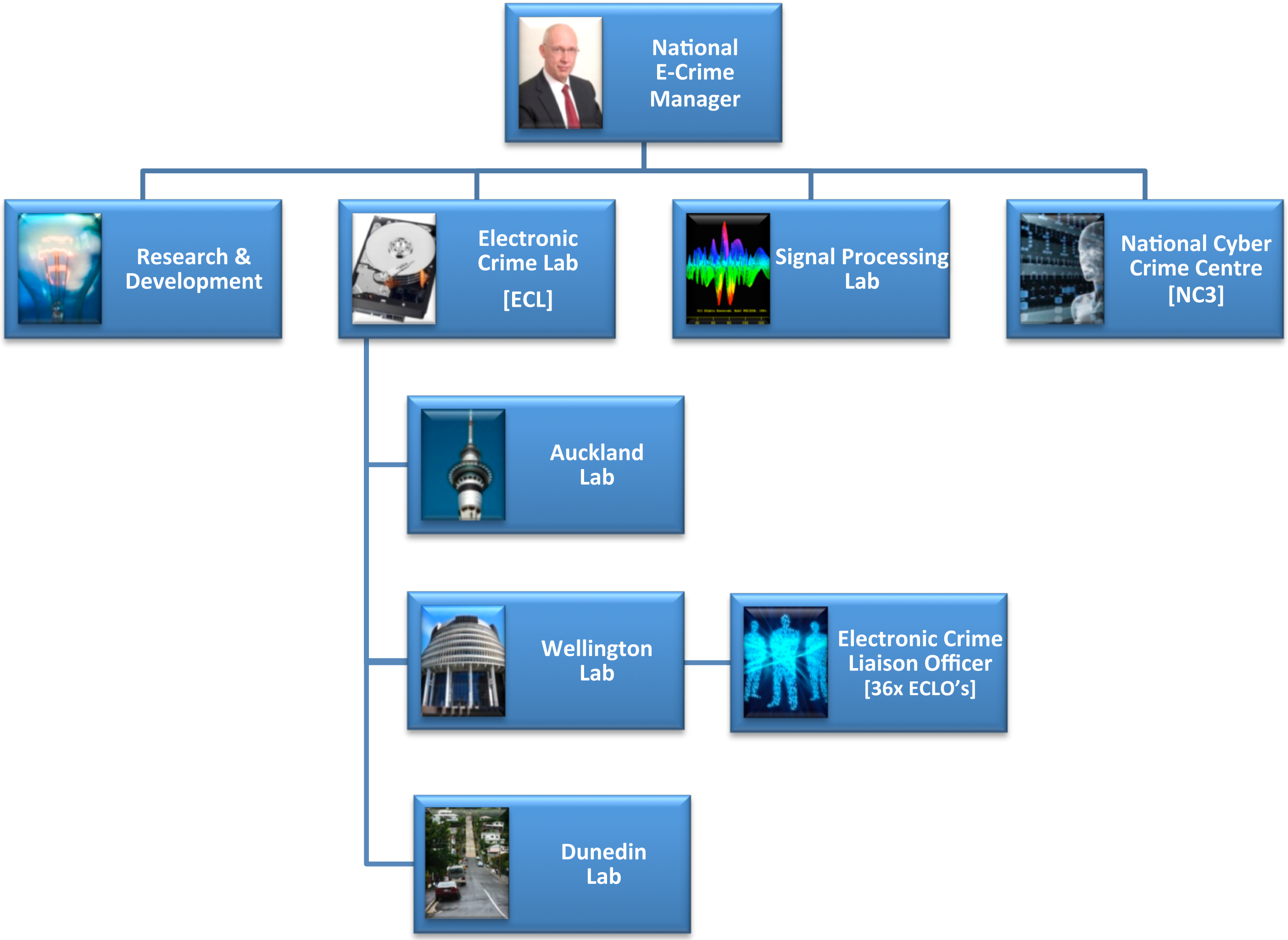
Mission:

To provide information assurance and cyber security support to agencies and critical infrastructure operators in order to secure networks and provide monitoring, analysis and response capability to combat advanced and persistent cyber threats.

Vision:

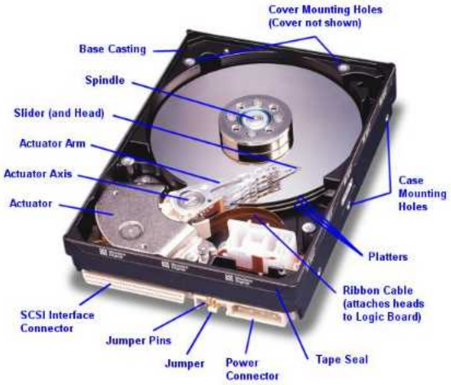
To be the trusted guardian of New Zealand's information assets.

E-Crime Group Structure


National E-Crime Manager
Research & Development
Electronic Crime Lab [ECL]
Signal Processing Lab
National Cyber Crime Centre [NC3]
Auckland Lab
Wellington Lab
Electronic Crime Liaison Officer [36x ECLO's]
Dunedin Lab

Electronic Crime Lab (ECL)

- Scene examination and electronic device seizure
- Evidential preservation of data from electronic devices
- Conversion of seized computers into EVE
- The forensic examination of preserved data

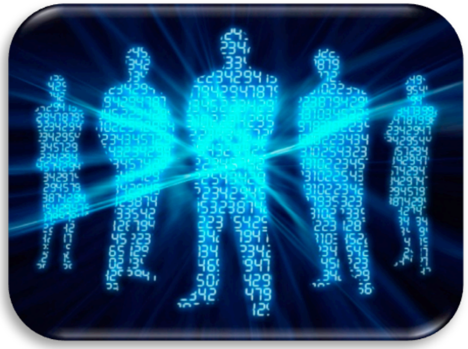


Electronic Crime Liaison Officer

The ECLO role is to provide a liaison point between District staff & the regionally based Electronic Crime Laboratories & assist with electronic crime investigative work.

Provide first point of contact between investigating officers and ECL in:

- Assisting in the seizure of digital evidence
- Assisting with wording for warrants
- Advising on correct exhibit seizure practices



Signal Processing

- Evidential preservation of audio and video recordings
- Conversion & transfer of recordings between different formats
- Downloading and capture of recordings
- Forensic examination of recordings & authenticity assessment
- Forensic enhancement of recordings
- Forensic duplication of recordings

What Are NC3 Functions

- Criminal investigations & Prosecution
- Online Intelligence & Capturing Evidence
- Co-ordination with International Agencies
- Providing Expert Witness testimony
- Assisting in Police investigations
- Educating frontline staff

OCEANZ

- Coordinate international and national investigations
- Lead NZ agency in the Virtual Global Taskforce (VGT)
- Covert identities to gather evidence therefore posing as;
  - paedophiles, and
  - minors
- Provide guidance and assistance to District staff
- Increasing victim identification capability

Anti-Spam Unit

- The Department of Internal Affairs is employing a five pronged strategy for tackling spam.
- Very clear about our purpose and outcomes as a regulator.
- This encompasses:
    - Directly enforcing the UEMA 2007.
    - Written Formal Warnings – Civil Infringement Notices – High Court Action.
    - Promoting Education and Awareness.
    - Facilitating Industry Liaison.
    - Monitoring Emerging Technologies.
    - Working with Domestic and International Agencies.

INTERNAL AFFAIRS
Te Tari Taiwhenua

Anti-Spam Unit

- ***Herbal King*** spam group takedown
- Spamhaus called this group the **"Largest Spam Gang"** in the world in 2007/2008
- Fined **$NZ 250,000** in New Zealand
- United States Federal Trade Commission also fined them **$USD 15.5 Million Dollars**

http://bit.ly/7yAfdt

Scam Watch

- Scamwatch has been set up to provide information to protect citizens from scams
- Information portal for:
  - Types of scams and how they work
  - What to do if you’ve been scammed
  - How to protect yourself
- Scam alerts
- Scam reports

MINISTRY OF
CONSUMER AFFAIRS
MANATŪ KAIHOKOHOKO

NetSafe

netsafe

www.netsafe.org.nz

Online Reporting Button

- The orb has been developed by NetSafe to offer all New Zealanders a simple and secure way to report online incidents which may break NZ law or breach legislation

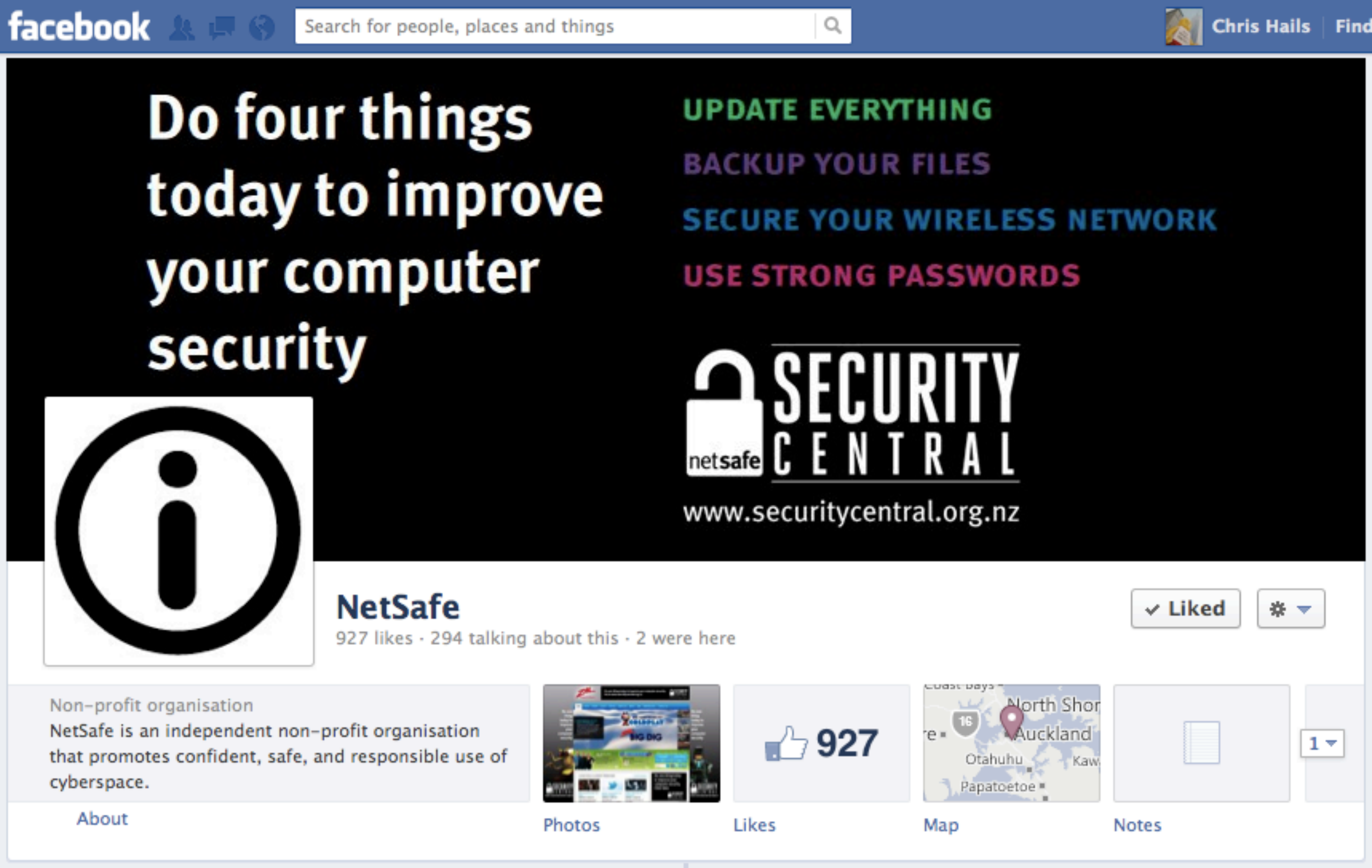
- The orb is intended to 'report online crimes, online' including:
  - Spam messages
  - Offending against children and child pornography
  - Objectionable material
  - Scams or Fraud
  - Online Traders
  - Privacy breaches
  - Attacks on computer systems

reporting online crime, online

Cyber Security Awareness Week
June 2012

netsafe SECURITY CENTRAL

www.securitycentral.org.nz



Do four things today to improve your computer security

UPDATE EVERYTHING

BACKUP YOUR FILES

SECURE YOUR WIRELESS NETWORK

USE STRONG PASSWORDS

www.securitycentral.org.nz

NetSafe

927 likes · 294 talking about this · 2 were here

Non-profit organisation

NetSafe is an independent non-profit organisation that promotes confident, safe, and responsible use of cyberspace.

Breakfast

{the losses}

REPORTED LOSSES

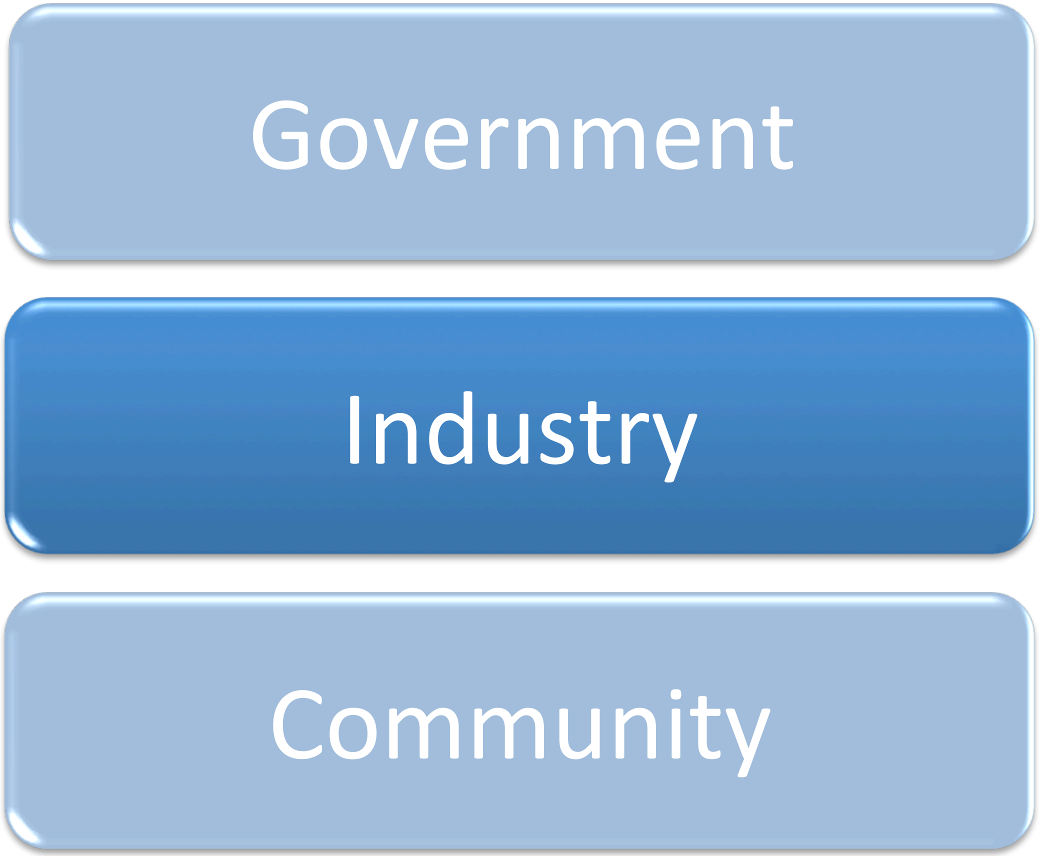
BIGGEST	$140,000
SMALLEST	$5.16
AVERAGE	$4,298
TOTAL	$769,382.61

incidents resulting in the greatest losses

$340,000

romance scams

Mitigating the Threats



Government

Industry

Community

New Zealand Security Industry

- Active security industry
- Number of dedicated security companies

aura SOFTWARE SECURITY

INSOMNIA SECURITY SPECIALISTS :: REST SECURED

LATERAL SECURITY INFORMATION SECURITY SPECIALISTS

s a security-assessment.com

- CREST NZ Certification coming…

COUNCIL OF REGISTERED · ETHICAL SECURITY TESTERS · CREST

ISACA NZ

- The Information Systems Audit and Control Association (ISACA)
- 95,000 members globally in 100 countries
- Active chapters in Auckland, Wellington and Christchurch
- Oceania CACS 2012 Conference Wellington
  - 10 - 12th September 2012
- www.isaca.org

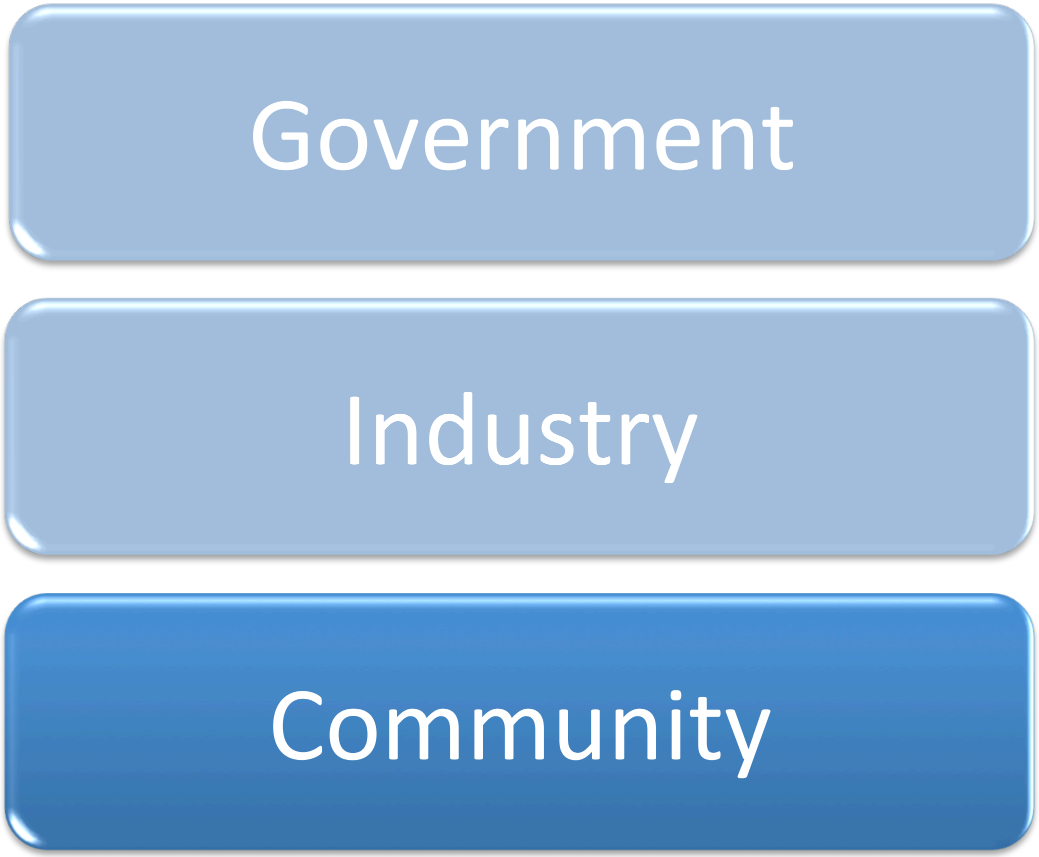
ISACA®

Trust in, and value from, information systems

1st Tuesday

- Non Sales forum for Senior Professionals in Information Security, IT Risk, Audit & Compliance
- Topical 20min presentation from monthly sponsor
- Meetings:
  - Monthly in Wellington
  - Bi-monthly in Auckland
- More info at www.1stTuesday.co.nz

Mitigating the Threats



Government

Industry

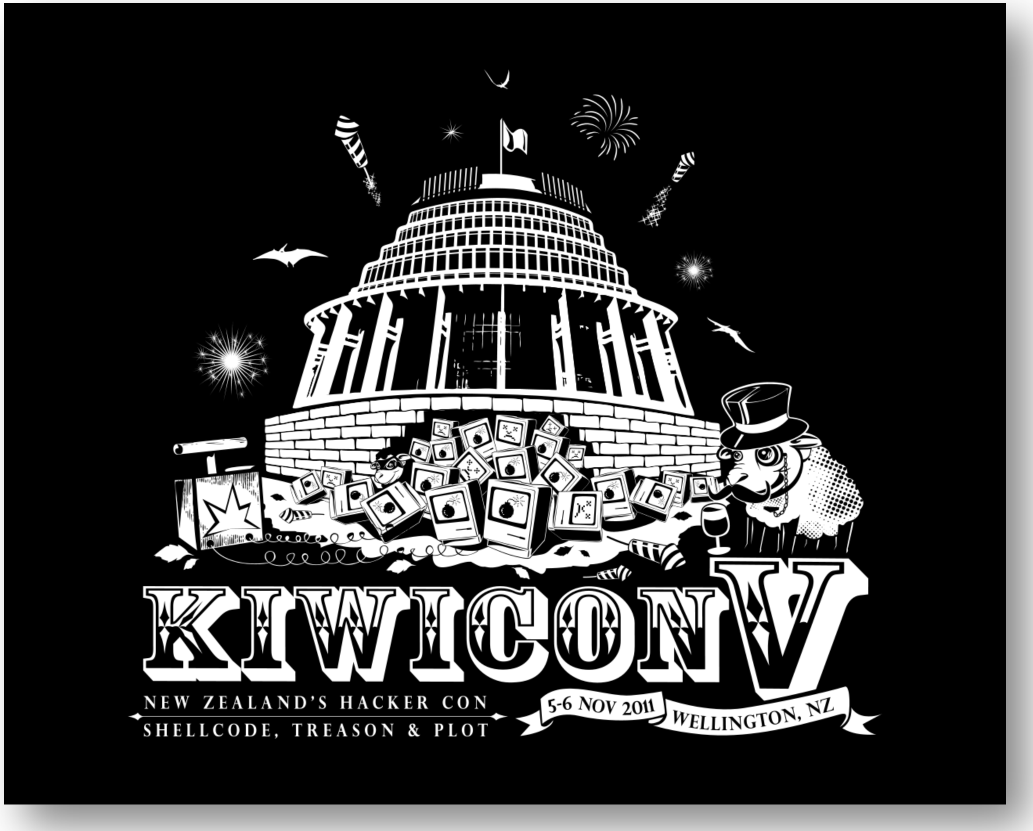
Community

New Zealand Security Community

- If the security industry can be described as the **9am – 5pm** group then Security Community is the **5pm – 9am** group
- New Zealand has a very active security community

Information Security Interest Group (ISIG)

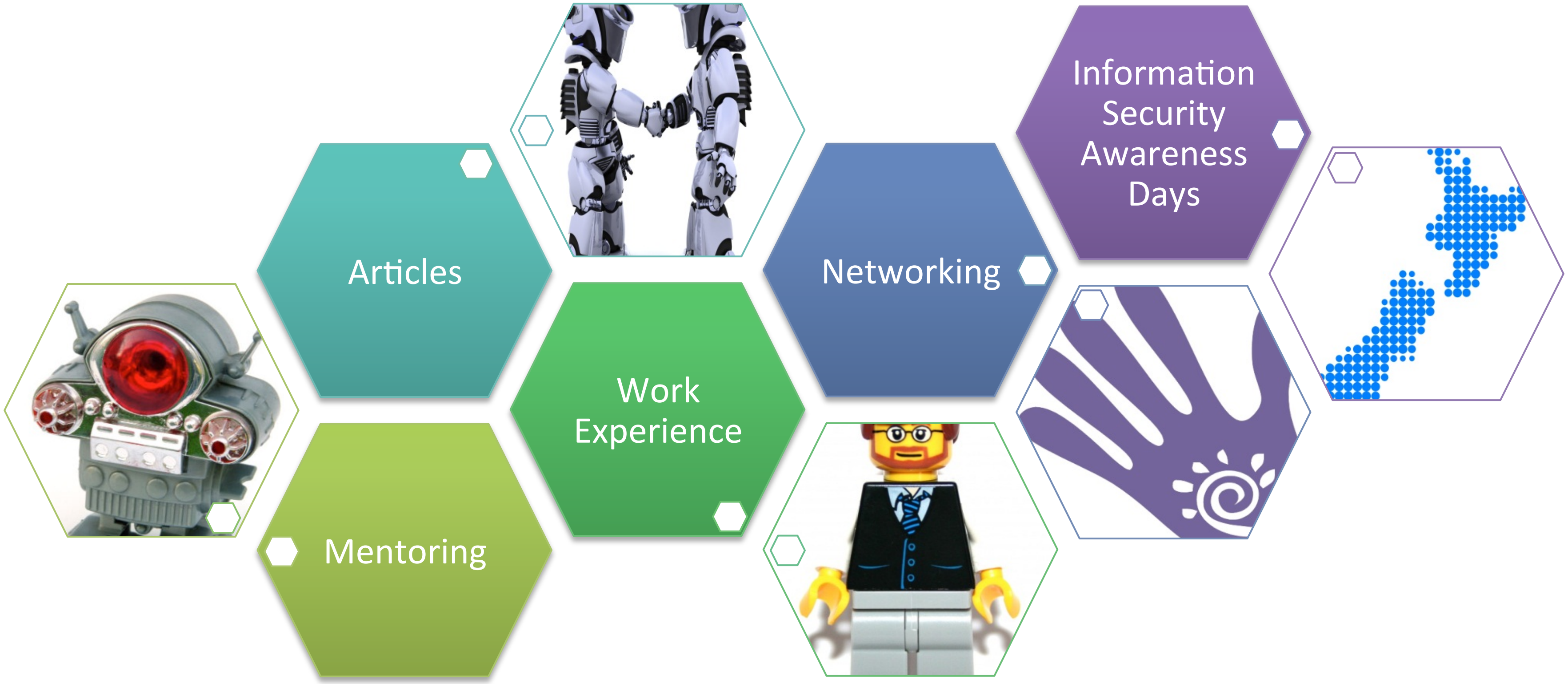
- Technical forum for security professionals
- Meets last Thursday of each Month
- Auckland and Wellington Chapters
- www.isig.org.nz
- Ircs.kiwicon.org Channel #isig



- Annual conference (650 attendees)
- Kiwicon VI - 17&18 November 2012
- www.kiwicon.org
- ircs.kiwicon.org Channel #kiwicon

in2securITy

To **encourage**, **educate** and **inspire**
a new generation of **IT security professionals**
for New Zealand



Articles

Mentoring

Work Experience

Networking

Information Security Awareness Days

in2securITy

www.in2security.org.nz

@in2securitynz

info@in2security.org.nz

Information Security
Awareness Days 2012

Aug 18 – Hamilton

Sept 8 – Wellington

Sept 15 – Dunedin

Sept 22 – Auckland

Registration now open!

OWASP New Zealand

- OWASP is a global not-for-profit dedicated to bettering the state of application security
- Quarterly NZ chapter meetings in AKL/WLG and an annual conference in Auckland
- Next conference is OWASP New Zealand Day 2012 - August 31st http://tinyurl.com/cy3g7sb
- NZ Coordinators:
  - Adrian Hayes (adrian.hayes@owasp.org)
  - Nick Freeman (nick.freeman@owasp.org)

New Zealand Internet Task Force (NZITF)

Improving the cyber security posture of New Zealand

- Trusted community of security professionals focusing on improving the operational robustness, integrity, and security of the Internet in New Zealand.
- 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 Members

ANZ
aura INFORMATION SECURITY
endace
INSOMNIA SECURITY SPECIALISTS :: REST SECURED
INTERNAL AFFAIRS Te Tari Taiwhenua
InternetNZ
Kiwi bank.
LATERAL SECURITY
Microsoft
NCSC
.nz DOMAIN NAME COMMISSION
New Zealand POLICE Nga Pirihimana O Aotearoa
.nzregistry services
SFO SERIOUS FRAUD OFFICE Te Tari Hara Taware
telecom nz
TelstraClear
vodafone

Closing Thought

To affectively mitigate the threats, collaboration and coordination at National and International levels is essential