



Who Said IT Security Was Boring

Garry Bentlin – Senior Information Security Advisor

PulseANZ2010

Meet the people who can help
advance your infrastructure





Introduction

- I work for IBM Security and Risk Management
 - Big Blue – not always what you may think !
 - No specifics, or they will have to ~~kill~~ censure me
- My History
 - 13 years in IBM, from the Sydney 2000 Olympics to global integrated accounts
 - Started at the bottom of the food chain
 - In 1989, no one could hear you scream (or really cared if a tape or cartridge went missing, except for the pain of recreating the data)
 - Manager of IBM's Computer Emergency Response Team
 - Security advisor to a multiple hundred million dollar account (now *that* is a lot of money)
 - Post-graduate degree in Intelligence and Counter-Terrorism



IBM's Computer Emergency Response Team

- IBM's Computer Emergency Response Team (CERT)
 - Forensic investigators/PI's
 - Malware reverse engineers
 - Ethical hackers
 - Security Operators in a 24x7 SOC
 - Oncall Engineers
 - Incident responders
 - Operations
- We do the 'fun stuff' at cert@au1.ibm.com



IBM's Computer Emergency Response Team

- Sometimes, its not so fun
 - 24 hour oncall, incident management
 - 36 hours straight opens your mind to all kinds of possibilities
 - You need a good lie down at that point
 - three straight weeks of packet capture in a data centre
- You see things you don't want to see sometimes
 - Personal computers have personal things on them, and are often scarier than the big bad Interweb
 - Sometimes you will have no option but to ring someone in Law Enforcement
 - Face to face interviews with suspects



Making a Difference

- Sometimes we see the results of our work on TV at 6pm
 - Hmmmm, I know you and your car collection
- My tried and true hiring discussion with prospective staff
 - These are people with families and kids and mums and dads
 - Be very very sure with your conclusion
- IBM's Computer Emergency Response Team (CERT)
 - Blaster/Slammer/DDoS attacks/Botnets
 - Zero-day exploits and vulnerabilities
 - Usual run of the mill background traffic of old worms bouncing off the nice crunchy exterior of the networks
 - Who's that trip-trapping across my network ?
 - Gold plated bullet-proof solutions



The face of the Enemy

The old



The new



The old days

- networks crashing due to zero day exploits
- Slammer/Sasser
- IBM Zurich labs designed a kill program
- We used it to BSOD systems off networks
- Eventually the owners of the systems who did not respond got the message





The fun stuff

- Exciting security 😊, its not always SOX or AUS810
- Plenty of cold data centre floors
 - See the world !
 - Standby for 9/11 ☹
 - Getting up close and personal with the outside of a 747-400 in a hangar on the concrete, instead of in a seat in the comfy comfy cabin
 - Inside data centres looking for a hole in the roof/wall because I have been locked in, when every man and their dog left (do I call a pizza guy to come let me out ??)
 - or do I try and bump the lock ?
 - Investigating international fraud, smuggling and money laundering




The fun stuff (continued, there is a lot of fun)

- Internship in the US, working for a dot-Com guru who got out at the right time (hence guru)
- Teaching and coaching security staff around the world
 - Gamut ranges from ‘not that way up, it goes this way up’ to ‘ooh can I borrow that idea thanks very much I won’t let the door hit me in the back kk thx cya bye !’
- That email you always wanted to send to the boss of the company, telling them how you would run things if you were them but you didn’t send it, you say ? (what, this one right here in free space on the hard drive ?)
- Pointing an antenna at a building from the 24th floor in Sydney CBD
 - And finding a Kingsford Smith Airport AP with line of sight
- Decoding IM logs discussing how to smuggle cash across a Customer inspection point, how much is ‘only’ a recorded conviction as opposed to a term of incarceration



The nasty stuff

- Investigations into fraud and theft
 - Partnering with local police agencies in a third country, whilst I am from the first country sitting in a second (IM logs are such a wonderful goldmine, especially when in clear text)
 - Sitting in an office, looking at a PGP encrypted hard disk
 - Mmm what next ? 
 - Let my fingers do the walking and tap in to the massive skill base of IBM, and call a world leading forensic researcher and published author for a 'chat'
- Things you don't want to see
 - Time to get up and walk away from the keyboard
- Personal safety concerns – in a glass fishbowl with any number of suspects watching you, solidarity and safety in numbers



Things to watch out for on some engagements

- Being advised your travel plans should include a budget allocation for an armed escort of at least three people plus driver





Things to watch out for on some engagements

- Sometimes you just have to say no, especially when there is a Government travel warning on the destination
- Being an 'uncomfortable shoulder' to cry on when a 'friend' betrays your client as you progress through an investigation
- Traipsing around buildings in the dark looking for a suspect's computer with a client executive peering over your shoulder 'is *this* the guy ?'



Computer Security just isn't important, it's all virtual

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
 - Last weeks unpatched Stuxnet Microsoft Windows shortcut file (.LNK) vulnerability (CVE-2010-2568)
 - issued Advisory ICESA-10-201-01 indicating that they "confirmed the malware installs a Trojan that interacts with installed SIMATIC WinCC or SIMATIC Siemens STEP 7 software and then makes queries to any discovered SIMATIC databases."
 - Simatic S5 PLC is an automation system based on Programmable Logic Controllers commonly used in SCADA environments



Computer Security just isn't important, it's all virtual

- The "*Aurora Generator Test*" was conducted in March 2007 by the U.S. Department of Homeland Security and involved the remote accessing of a generator control station. It resulted in the partial destruction of a \$1 million dollar large diesel-electric generator
- This test conducted at Idaho National Labs showed it is possible to exploit remote access to send commands to large generators to cause them to damage or destroy themselves.



Computer Security just isn't important, its all virtual

- Researchers were able to remotely change the operating cycle of the generator, sending it out of control. A video of the incident shows that the target generator shakes, emits smokes, and then stops. A simple analogy would be to consider the effect of randomly changing the firing order of spark pugs in your car – the engine would soon render itself nonoperational.





Hacking sewerage

- 2000-1 the traditional disgruntled *potential* (?!) employee
- After monitoring and recording all transmitted signals and messages, they concluded that someone was deliberately hacking into the control system to cause the disruptions. After three months, the culprit was arrested,
- not before a million litres of raw sewage was released into local waterways, parks, and even the grounds of a Hyatt Regency hotel
- \$50,000 spent cleaning it up.
- 49-year-old Vitek Boden's revenge for failing to get a job with the Maroochy council in Queensland
- He made 46 attempts to take control of the sewage system. On 23 April, police who pulled over his car found radio and computer equipment
- Boden was sentenced to two years imprisonment



Extreme wireless hacking

- Israel displayed significant cyber-warfare capability in a purported airstrike on a Syrian site in 2007.
- It was reported that Israeli used modified luxury aircraft (Gulfstream G550's) with onboard technology that enabled them to hack into the Syrian integrated air defence (IAD) computer network and shut down components of their anti-air defence capability.





Extreme wireless hacking

- They carried out the cyber-attack in mid-air
- Modifying the attack as they flew through Syrian airspace to identify and attack the command and control network.
- The electronic attack aircraft transmitted data streams directly into Syrian antennas and then monitored passively to ensure that the attack had had the desired effect of neutralising the Russian-built air defences.
- This attack enabled non-stealthy F-15 aircraft to enter the Syrian airspace undetected and deliver an explosive payload to a targeted building at Dayr az-Zawr.





More Extreme Wireless Hacking

- Kosovo Conflict in 1997
- The US was more circumspect than the Israeli operation in Syria and no overt confirmation of the capability has been made public.
- Yugoslavia's air defences included Soviet-made surface to air missile (SAM) installations equipped with thousands of missiles,
- It has been asserted that "some means may have been used to distort the images that the Serbian integrated air defence systems were generating".
- These efforts remain classified but it seems that they were able to manipulate data to protect NATO aircraft, generating false images on radar.



Activities 2006-2009





What do Anonymous do ?

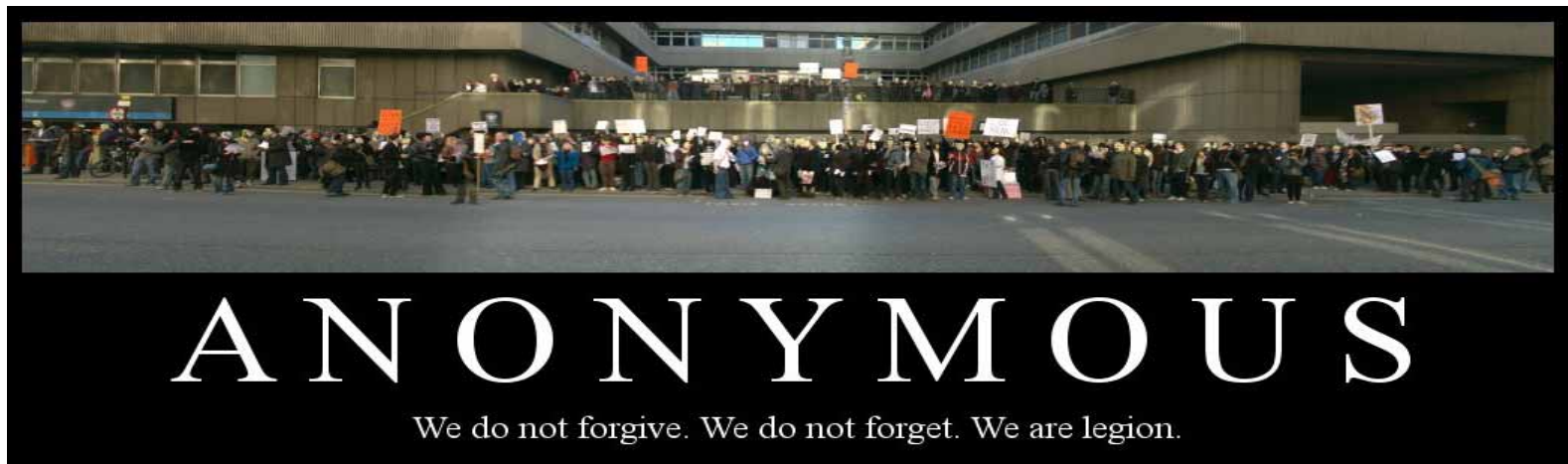
- Hello, Leaders of Scientology. We are Anonymous. Over the years, we have been watching you. Your campaigns of misinformation; your suppression of dissent; your litigious nature, all of these things have caught our eye”
- Scientology.org were subjected to heavy attacks over the Internet starting on the 16th of January 2008
- Scientology call centres were subjected to the music of Rick Astley. Pizzas and taxis arrived at Scientology buildings around the world.





Where do Anonymous operate ?

- Protests were held on 10 February, the birthday of Lisa McPherson who died whilst under the care of the Scientologists.
- Over 9,000 protesters participated worldwide in real life, not just over the Internet
- "The actions of Anonymous will not interrupt the church's normal activities serving its parishioners and the community, and the church is working in co-ordination with local authorities to minimize the negative impact of this mask-wearing, cyber-terrorist group."





Total Protestors in Australia

Estimates by city	10.5.08		12.4.08		15.3.08		10.2.08	
	Min	Max	Min	Max	Min	Max	Min	Max
Adelaide	60	60	70	70	200	230	150	150
Brisbane	65	80	60	60	100	165	40	100
Canberra					10	10	4	4
Melbourne	60	100	115	125	200	200	150	200
Perth	60	60	75	75	100	100	60	100
Sydney	150	150	200	200	150	200	150	300
Australia Total	395	450	520	530	760	905	554	854



Caught and Sentenced

- Dmitriy Guzner plead guilty and was sentenced to one year for launching distributed denial of service attacks against websites of the Church of Scientology in January 2008
- According to the prosecutors Guzner's attacks were acts of hacktivism. In October 2008, the hacker became the first Anonymous member ever to be charged in connection with the group's actions.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILED

2008 OCT 17 AM 11:41
U.S. DISTRICT COURT
CENTRAL DISTRICT OF CALIF.
LOS ANGELES

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,)	CR No. 08-08-01224
Plaintiff,)	INFORMATION
v.)	[18 U.S.C. § 1030(a)(5)(A)(i),
DMITRIY GUZNER,)	(B)(i): Unauthorized
Defendant.)	Impairment Of A Protected
)	Computer]
)	
)	

The United States Attorney charges:

Between January 17, 2008, and January 18, 2008, in Los Angeles County, within the Central District of California, and elsewhere, defendant DMITRIY GUZNER knowingly caused the transmission of information, codes, and commands, and as a result of such conduct, intentionally and without authorization caused damage by impairing the integrity and availability of data, a program, a system, and information on a computer system that was used in interstate and foreign commerce and communications, specifically websites belonging to the Church of Scientology,

///

WLH:wlh
W



Why ?

- “Hello, Kevin Rudd. We are Anonymous. We have been watching you. It wasn't very long ago since you were elected, was it?”
- The Australian Government’s Internet filter proposal by Minister Stephen Conroy is the catalyst. This is mandatory filtering of website access from all Australian ISP’s. It also includes issuing take-down notices to websites operating in Australia, and requires Google to remove offending sites from search results
- Australian Communications and Media Authority (ACMA) maintains a blacklist, which leaked in March 2009 to wikileaks.org and other sites
- The attack was initially planned for 27/6/2009



Do you ever wonder where all your tax money is going to? Well I'll tell you what \$44 MILLION has been budgeted to so far: CENSORSHIP! The Rudd government is implementing a plan to censor the internet at the Service Provider level, whether you want it or not. Whether the content is illegal or not. Even the BBC, Sun and Times, British NEWS sites are already on the blacklist. If you still think filtering is a good idea, consider that the trial was worked around by a 15 year old. This wont stop anyone who wants to get around it, but it will slow EVERYONE down and begin a new Big Brother mentality in the government.

**To learn more go to
nocleanfeed.com**



Targets

- Australians protestors were advised to not participate in the attack online, as they would be able to be prosecuted by Australian LEA's
- Instead they were requested to
 - /efg/ in person and print out fliers and cards and distribute them
 - blackfax i.e. use white-on-black messages such as Information Is Free, the links, NO CENSORSHIP etc.
 - *"I've been fax DDoSing with black pieces of paper taped together creating an infinite loop but they've recently blocked them from coming through"*
 - Call in repeatedly. Fax and phone numbers provided included:
 - +61 2 6271 1901 [Department of Broadband, Communications & the Digital Economy]
 - +61 2 6273 4154 [Stephen Conroy, Parliamentary Office]
 - +61 3 9650 3251 [Stephen Conroy, Ministerial Office]
 - +61 3 9408 0194 [Stephen Conroy, Electorate Office]
 - +61 2 6219 5353 [ACMA Office, Canberra]
 - +61 3 9963 6899 [ACMA Office, Melbourne]
 - +61 2 9334 7799 [ACMA Office, Sydney]



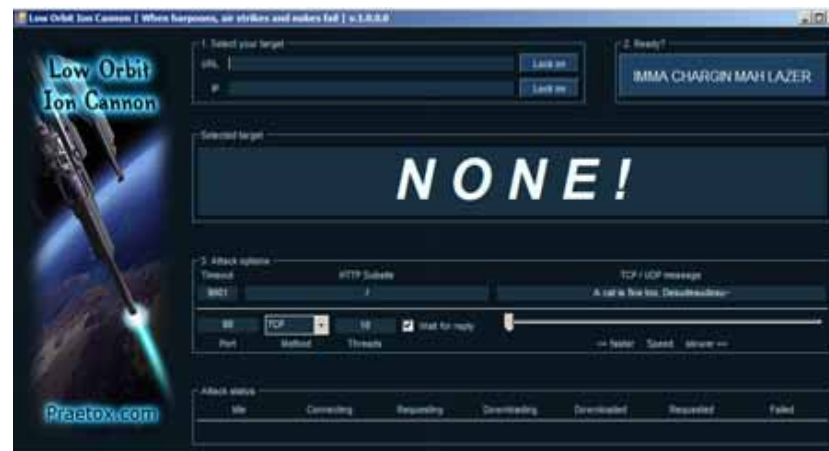
Generating Media Hype

- To influence the media Anonymous created programs to automatically promote their cause via search engine manipulation. They also provided manual instructions for those less-technical members
- Anonymous provided lists and times of talk back radio shows and hosts.
 - Station : [2GB](#) Number : 131 873
 - Station: [4BC](#) Number: 13 13 32
 - Station: [Triple J HACK](#) Number :1300 0555 36
 - Station: [96.5fm](#) [Talking life with Peter Janetzki 8-10pm Sundays]
Number:1300 85 13 14
 - Station: [NOVA 969](#) Number: 13 24 10
 - Station: [Vega 953](#) News room - 02 9564 9800 The studio: 13 25 10
 - Some Melbourne stations:
 - 3AW - 693kHz AM - 03 96 900 693 or 131 332
 - ABC - 774kHz AM - 1300 222 774
 - Vega - 91.5 MHz FM - 13 25 10
 - SYN - 90.7 MHz FM - 03 9925 9907



Outcome

- "In two minutes from when I type this, Anonymous is declaring war on the Australian Government over its decision to implement Draconian internet censorship,"
"Tick tick tick."
"7:18pm pm.gov.au DOWN!"
"7:21pm Kevin Rudd's page is down completely. Strike one to Anonymous."
- They used a program called Low Orbit Ion Cannon
- Minister Stephen Conroy described the attack as "juvenile"
- Media coverage was extensive, including print, television and Internet





IBM – a security company

- Note: this is not the ‘Sell’ part of my presentation, this is just why I personally like the company I work for
- IBM bought ISS a few years ago, adding a massive intelligence capacity and some very nice protection technologies that I had already happened to be using
- I can tap into this massive amount of intelligence
- XFORCE research network, meeting some very very smart people and confirming the theory that there is always someone smarter than you (and realising to my detriment that there a lot of them in that room with you right about then)
- Knowing your customer is protected, and feeling somewhat complacent instead of waking up at 3am thinking
 - ‘Crap!’
- Sometimes finding out that you cannot protect your customer against themselves
 - ‘No DON’T click on the link in the email that susie@iloveyou.com sent AGAIN !)
 - And then finding someone in 400,000 people in the company who can provide a solution to protect them from themselves



My personal payoff in security

- So why ?
- I make a difference
- My evidence assisted to put someone in jail
- Or get them fired
- Or get them exonerated
- Save a customer money, reputation, integrity, intellectual property
- Stop them from doing something stupid
- Or tell them they are being stupid and why
- I help people, none of this white/grey/black hat stuff



Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© IBM Corporation 1994-2010. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at <http://www.ibm.com/legal/copytrade.shtml>.