FUJITSU

THE POSSIBILITIES ARE INFINITE

SUBMISSION TO THE STANDING COMMITTEE ON COMMUNICATIONS

NEW INQUIRY INTO CYBER CRIME

26 JUNE 2009

Contact Details
Fujitsu Australia Limited
David Nockels, Principal Consultant
19-25 Moore Street
Turner ACT 2612
Phone: 02 6247 7677
Email: david.nockels@au.fujitsu.com

CONTENTS

Introduction

Fujitsu Australia and New Zealand Limited is pleased to provide this submission to the Standing Committee on Communications *New Inquiry into Cyber Crime* as detailed in the Media Release issued 18 May 2009.

What is the Current Threat Environment for Australia?

According to a 2008 survey by security vendor AVG[1], Australia has the highest incidence of cyber crime in the world. 1,000 users were canvassed in each of the following countries: Australia, U.S., France, Germany, Italy, Spain, Sweden, Brazil and the Czech Republic. Results showed that more than 39 per cent of Australians had been the victim of cyber crime, compared to 32 per cent in Italy, 28 per cent of Americans, and just 14 per cent in Sweden and Spain.

For the purpose of this report, Cyber crime is defined according to the broader international definition as an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offences and copyright offences. The technology utilised by cyber criminals is so flexible and advances at such a rapid pace that writing an adequate definition of the crime is part of the problem.

Further, perpetrators of these crimes are not bound by national boundaries. Attacks against Australian citizens can and do originate from servers based in Russia, China and even the U.S. Attributing attacks to specific individuals operating under the cover of proxy servers and Internet aliases require deep and consistent monitoring and penetration of black hat (criminal) hacker forums, IRC chat, Tencent QQ chat, Web sites and other hidden communities and communications mediums.

In summary, the nature of internet crime is transnational, engaged in by both novices and professionals and feeds an underground economy that has its own language, tradecraft, assets and resources.

Broad categories of internet crimes that impact Australian citizens and governments include but are not limited to:

- hacking
- denial of service
- data theft
- defacement
- espionage
- robbery.

1 http://www.crime-research.org/news/20.06.2008/3422/

The perpetrators of these crimes may include:

- Hacker unions or crews (domestic and foreign)
- Organised crime
- Foreign Intelligence Services
- Botnet operators
- Random individuals looking to take advantage of readily available black (underground) technologies.

Experience in conducting global investigations against many of these groups, suggests that a committed and ongoing exploratory effort to gain answers to the following questions as they pertain to Australia is required.

- Identify the role of organised crime (such as the Russian Business Network) and categorise its engagement in the Pacific region in general and Australia in particular.
- Identify the major sources of attacks on Australian government agencies, businesses and individuals.
- Identify whether or not there is collusion with foreign national entities or non-state hackers and Foreign Intelligence services.

Collection and Analysis on Cyber Criminal Actors

Experience of tracking non-state hackers engaged in internet crime and cyber warfare (including cyber espionage), has provided familiarity with the activities of hackers from Russia, China, the Middle East and Pakistan. This has provided a baseline from which to identify patterns of hacker behaviour.

Characteristics are similar across nationalities in that they each operate in the anonymous domain of the cyber underworld utilising a variety of forms of Malware ranging from simple Denial of Service kits to SQL Injection (SQLi) to Botnets.

Motivations vary, from religious to nationalistic to financial. The composition of hacker crews who choose to self-identify in online hacker communities and Web sites for the purpose of establishing their viability and hacker 'credentials' are frequently multi-national when motivated by money or nationalism, but share the same religious beliefs when motivated by religion.

By combining leading edge technologies, social network analysis with server level data, vendor and government organisations are able to track and identify hackers up to their alias and nationality, and, less frequently, to their real identity, place of employment, age and even physical address. It is vital for law enforcement and intelligence agencies to exploit these sources in order to track back and/or predict cyber crimes, attacks and incidents of espionage.

Collection and Analysis on Tradecraft

While Phishing and Trojans are frequently employed against targets, by far the most threatening of these attacks is SQL Injection. A successful SQL Injection attack may result in a full data breach that an organisation will never recover from. This includes all backend storage, all user names and passwords, and it doesn't stop there. Once usernames and passwords have been obtained an aggressive hacker will leverage that information to continue finding additional access to personal accounts on well-known banking or social websites.

SQL Injection is an attack technique that takes advantage of poor secure application coding practices. If an application does not provide the correct validation for user supplied input parameters, an attacker could embed SQL commands within the parameters passed from the web application to the hacked database.

The result is that the attacker can execute arbitrary SQL queries and/or commands on the backend database server, using the web application as the delivery mechanism. SQL Injection is a CRITICAL application issue and typically results in the loss of all the data stored within the database and compromise of the system housing the database. Additional information on generic SQL Injection attacks can be found here: http://www.owasp.org/index.php/SQL_injection.

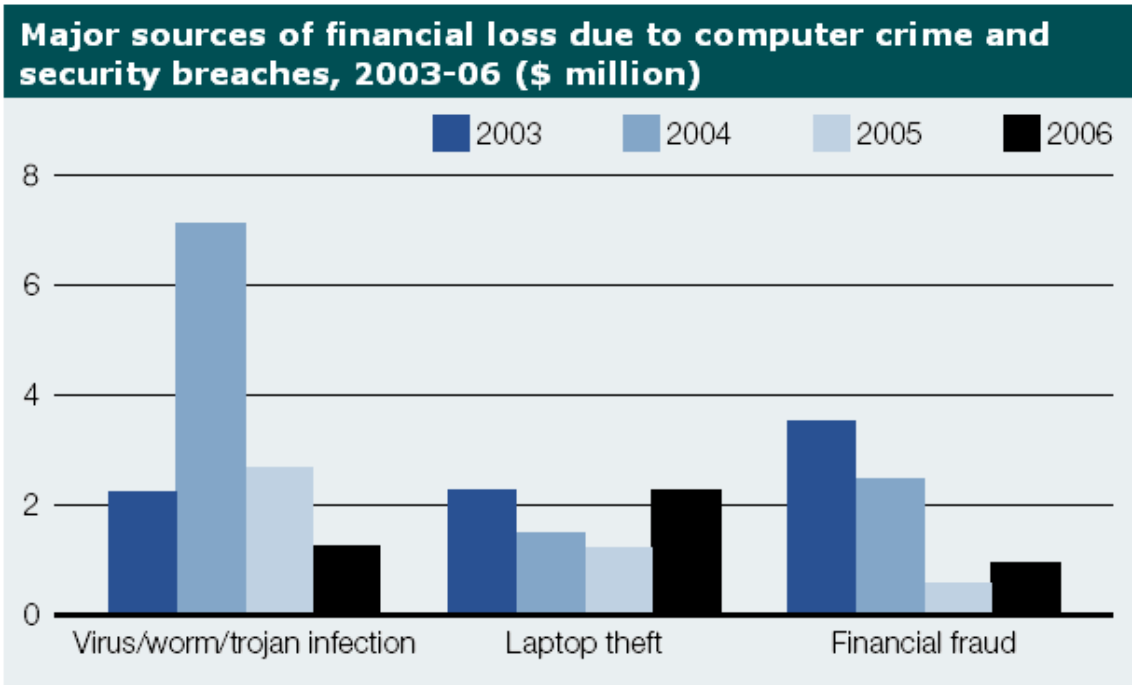
Recent conflicts have seen an upsurge in non-state hacker activities. Specific techniques used include a new twist on the typical SQL Injection vulnerability exploitation techniques. Attackers use SQL Injection vulnerabilities to call a CPU intensive task (built in crypto functions) for the backend database to execute hundreds of thousands of times. Cyber criminal and hacker activities, whether by State backed or non-state backed personnel, continue therefore to evolve.

What is the Current Defensive Posture of the Australian Economy and Consumer?

Analysis of total cost to the Australian economy/consumer from cyber crime

The following table is provided from the Australian Institute of Criminology 2007 report into financial loss from cyber crime and shows the amount in $millions lost through cyber crime activities.

Figure 1: Major sources of financial loss due to computer crime and security breaches, 2003-06



Another survey was conducted by AusCERT - the *2005 Australian computer crime and security survey*[2]. AusCERT grouped cyber crimes and the costs associated with them. For instance, the most costly cybercrime was 'Denial of Service attack', which reported a total lost of $8.9 million followed by virus/worm/trojan infection with $2.7 million and computer system abuse with $2.4 million.

The survey further reported that the cost of computer crimes experienced by 110 of the organisations surveyed produced a total lost of $16.9 million in Australia.

AUSCERT provides the following information from research conducted in 2005[3]. Clearly, the number of incidents has increased significantly from that period to 2009 moving Australia to the world's top position in victims of computer crime.[4]

- The most common cybercrime in Australia during 2005, accounting for over 63%, was in the category of virus/worm/trojan infection.
- Laptop theft constituted the second largest category with almost 58%.
- Denial of Service attack was the third top cyber crime with about 22% of the cases.
- The fourth in the list of cybercrimes was the so-called 'degradation of network performance associated with heavy scanning,' which accounted for 21% of the cases reported.
- Following this line of cybercrime cases, the fifth most common cybercrime in Australia during 2005 was 'theft of computer hardware or devices'.

'Unauthorized access to privileged information by insider' accounted for 19% of the cases; following by 'theft/breach of proprietary or confidential information' (18%); 'computer system abused' by insiders (about 9%); identity theft (9%); website defacement (8%); theft of hand-held computers (7%); outsider system penetration (6%); financial fraud (5%); sabotage of data networks (4%); telecommunications fraud (3%) and the last in the list is 'interception of telecommunications ' with 1% of the reported cases.

It could be inferred from this information that in Australia damage to computer systems and computer theft are the predominant cybercrimes contrasting with privacy and identity theft cyber crimes common in the United States.

NOTE: A major concern that the authors have is that due to the fact that Australian businesses are not legally required to report cyber crimes nor are many of them technically capable of determining if their networks have been penetrated, the statistics that have been collected and reported on by the ABACUS survey, for example, may be grossly under-represented.[5].

2 https://www.auscert.org.au/render.html?it=4579

3 http://www.ibls.com/internet_law_news_portal_view.aspx?id=1646&s=latestnews

4 http://www.crime-research.org/news/20.06.2008/3422/

5 http://www.aic.gov.au/publications/tbp/tbp032.html

Analysis of the current defensive posture of the Australian econony/consumer

Problems specific to Australia, its companies and its current laws include the following.

- The lack of legislation forcing companies to report breaches of their computers/networks that have caused customer data or financial loss.
- The lack of a central reporting point for security breaches. There is difficulty therefore in data gathering, information sharing and gathering and disseminating intelligence on cyber crime activities within Australia.
- Existing penalties for system and network intrusions should be reviewed for adequacy. This could include the possibility of enacting new legislation which specifies different penalty rates based on the financial damage caused as well as penalties for denial of service attacks and running a Botnet.
- There appears to be no legislation in place that addresses the criminal underground economy, the people involved therein, and the tools which they use or write (Malware).
- Law enforcement agencies are currently restricted in the deployment of offensive tools (i.e., exploiting software vulnerabilities to identify suspects where it is not known where the suspect is physically located).
- Internet service providers are not sufficiently invested in assuring their customers' security. Internet service providers should be legally required to take reasonable action when notified of a security breach on one of their customer's systems. This may include notification of the infected customer or blocking of certain traffic to the customer's system.
- Neither companies nor individuals who hold the personal data of others are legally obligated to report breaches that have compromised or potentially may have compromised such data.
- Even if companies were so inclined to report such a breach, there is no clear-cut procedure detailing how and where such reporting should occur.
- Information silos within Federal and State based agencies exist. Information silos have proven to be counterproductive in virtually every nation in the world. Data sharing between agencies is a requirement for any successful cyber crime strategy.
- Cracking anonymous Internet aliases is currently burdened by bureaucratic obstacles within Australian law enforcement. For example, if a police officer were to deploy an exploit against a target for the purpose of ascertaining the targets physical location, a senior police officer would need to sign a 'Controlled Operations Certificate' first, which is only valid for Australian-based targets. This ignores the global nature of this threat and is counterproductive to solving Australia's Internet crime problem.
- There is no database upon which to build identifying factors and attach them to individual Internet aliases. Instead, current law enforcement investigations stop at the alias only.
- No Australian agency (law enforcement or otherwise) has the legislation to offensively target the infrastructure of cyber criminals. The ability to conduct these activities should be considered.
- Currently there is no legislation allowing any Australian agency to deploy a technical capability to remove virus/trojans/malware from victims in Australia. Historically, this has proven to be an effective way to eliminate the threat of large Botnets like Storm. In that case, European researchers discovered a vulnerability in the Storm Botnet source code and released a program onto the internet than scanned for victim PCs and removed the Storm infection.

What New Technologies are required to Improve Australian Security?

While all parts of the cyber crime environment are of concern, Denial of Service threats are particularly serious since they can shut down entire networks, company-wide or nation-wide. Mitigation comes down to several areas of targeted protection within three general groups; ISP, customer networks and CERT-Type agencies.

Internet Service Provider

Threats

Threats in this area include Bandwidth consumption, Hosted Web server resource exhaustion and Hosted DNS server resource exhaustion.

Protection of ISP Infrastructure

Mitigation Techniques used in this area include the following.

- Real Time Black Hole Filtering.
- Detection of Denial of Service through traffic flow analysis using available technology with a flow analyser tool.
- Use of application recognition techniques to create rate limiting access lists or route maps to drop the Denial of Service traffic at peering edge routers.
- Use of a high speed Intrusion Protection System to deny malicious traffic.
- Use of packet shaping appliances to rate limit all kinds of traffic but in this case malicious Denial of Service traffic.

Protection of Hosted Servers

Techniques used in this area include the following.

- Real Time Black Hole Filtering.
- Detection of Denial of Service through traffic flow analysis using available technology with a flow analyser tool.
- Implement reverse proxy technology, which limits connections and caches connections to the protected web hosts.
- Implement DNS protection, which limits and caches DNS requests to the hosted servers.

Protection of the Customer 'Last Kilometre'

Techniques used in this area include the following.

- Real Time Black Hole Filtering.
- Use of a high speed Intrusion Protection System to deny malicious traffic.
- Use of packet shaping appliances to rate limit all kinds of traffic and preserve quality of service (QoS).
- Use of application recognition techniques to create rate limiting access lists or route maps to drop the Denial of Service traffic at peering edge routers or create QoS configurations to preserve bandwidth for other applications.

Customer Networks

Threats

Threats in this area include Bandwidth consumption, Hosted Web server resource exhaustion, and internal worm, virus or compromise.

Protection of Internal Servers and Network Infrastructure

Mitigation Techniques used in this area.

- Detection of Denial of Service through traffic flow analysis using available technology with a flow analyser tool.
- Use of application recognition techniques to create rate limiting access lists or route maps to drop the Denial of Service traffic at customer edge routers.
- Use of a high speed Intrusion Protection System to deny malicious traffic.
- Use of packet shaping appliances to rate limit all kinds of traffic but in this case malicious Denial of Service packets.
- Create a 'denial all' permit by exception firewall rule set to limit target ports for Denial of Service.
- Harden server and network infrastructure.
- Create High Availability/Disaster Recovery Plans.
- Have an agreement with a 'clean pipe' provider to move traffic in case of a serious attack.
- Develop internal incident response procedures.

Not allowing Computers to be Part of the Problem

This requires the implementation of prudent security practices. Mitigation techniques used in this area include the following.

- Detection of compromised internal hosts through available traffic flow analysis technology with a flow analyser tool.
- Use of application recognition techniques to create QoS/rate limiting rules that allow the rest of the business to operate in the event of an attack.
- Use of a high speed Intrusion Protection System to deny malicious traffic.
- Use of packet shaping appliances to rate limit all kinds of traffic or deny malicious traffic.
- Create a 'denial all' permit by exception firewall rule set to limit outbound ports for Denial of Service; use proxy servers for most applications if port filtering is not possible.
- Have an agreement with a 'clean pipe' provider to move traffic in case of a serious attack.
- Develop internal incident response procedures to identify compromised machines.
- Deploy end point protection such as a desktop firewall, to quickly contain a compromised host.

CERT or General Industry Observations

Awareness should be created around Denial of Service as a tool for cyber warfare. Similar to spear-phishing attacks, Denial of Service occurs often around politically-motivated or world events – the public and private industry should be aware of this trend and be trained on defence against it.

Summary

The challenge is significant and will continue to evolve. Cyber criminals will continue to seek new methods of exploiting weak spots, be they technology or human, in an attempt to defeat implemented counter technologies and strategies. This will prove particularly so as technology itself evolves. It is improbable and impractical to believe that all cyber crime activities can be detected and defeated. Decreeing the problem as too vast however is not an option as the security, financial and political implications of cyber crime in all of its forms is potentially damaging on a massive scale and is already likely growing at an exponential rate.

Government must closely interact with industry (security experts and technology vendors) at all levels to collaboratively determine effective policies and strategies as well as to drive anti-cyber crime technology that will assist in thwarting cyber crime as much as possible. This will require a commitment of resources and funding on an ongoing basis as well as continual vigilance backed by sound and up to date legislation to meet evolving cyber crime threats.

Fujitsu would be pleased to provide additional information or clarification if required.

ABOUT FUJITSU

Fujitsu Australia and New Zealand Capabilities Statement

Fujitsu Australia and New Zealand is a leading service provider of business, information technology and communications solutions. Throughout Australia and New Zealand we partner with our customers to consult, design, build, operate and support business solutions. From strategic consulting to application and infrastructure solutions and services, Fujitsu Australia and New Zealand has earned a reputation as the supplier of choice for leading corporate and government organisations.

ICT makes up a $1.2 trillion plus industry. Fujitsu is the third largest IT Company in the world with annual revenues of $62 billion, more than 5000 employees in Australia and more than 160 000 employees globally. Fujitsu was established in 1935 in Japan and has been in Australia since 1972. We partner with our customers to consult, design, build, operate and support business solutions. For over 30 years Fujitsu Australia and New Zealand has been helping our customers become more effective through leveraging their investment in technology. We've done this through hiring the best people; looking after them and helping them grow just as we have. Fujitsu invests over US$2.5 billion in research and development annually so that our customers have all the advantage of emerging technologies and the smart thinking behind them.

Fujitsu Australia Limited and Fujitsu New Zealand Limited are wholly owned subsidiaries of Fujitsu Limited (TSE: 6702). For further information email askus@au.fujitsu.com or askus@nz.fujitsu.com or visit: **au.fujitsu.com** or **nz.fujitsu.com**.

Acknowledgement

Fujitsu wishes to acknowledge the expert advice provided to it in compiling this submission by Mr Jeffrey Carr, Principal of GreyLogic Inc. Jeff Carr is highly regarded and respected within the international anti-cyber crime community and specialises in the investigation of cyber attacks against governments and infrastructure by State and Non-state hackers, activists and criminals. He is a sought after expert resource and most recently presented at the NATO Conference on Cyber Warfare in Tallinn, Estonia in June 2009.