Submission to the House Standing Committee on Communications

Inquiry into Cyber Crime

David Jones
ThreatMetrix Pty Ltd
ThreatMetrix Inc.

Brief Biography of Submitter:

David Jones, CTO and VP of Engineering

Mr. Jones co-founded ThreatMetrix in 2005 – ThreatMetrix is now a leader in e-commerce fraud protection using next generation Device Intelligence that detects Botnets, compromised hosts and fraudulent users involved in e-commerce transactions.

Mr. Jones has more than 20 years experience in technical and management roles within the software industry and over 12 years dealing with Internet security issues.

He is an advisor to Encassa, an Australian company globally pioneering the fight against malicious password and credential stealing keyloggers and Trojans.

He is also a co-conceiver of SafeAndSurf an e-commerce protection application for iPhone users. SafeAndSurf is a project of the ThreatMetrix Labs –who recognized that the risks of fraud and safety don't stop at the PC but also extend to the new Internet enabled "smart" phones.

Prior to co-founding ThreatMetrix, he founded SpamMATTERS delivering technology used by the Australian Communications and Media Authority for tracking Phishing and Spamming operations. SpamMATTERS allowed Australian consumers to simply and swiftly report the presence of cybercrime impacting them. In 2009 SpamMATTERS remains a cornerstone of the nation's defence against spam and phishing.

From 2001-2004 At Surfcontrol, he was VP of Global Research, a leading Internet content filtering company that has most recently been acquired by WebSENSE. Among his major achievements at SurfControl was the management of the Email Filtering and flagship anti-spam solutions generating over 30% of company revenues.

Mr. Jones arrived at his position at SurfControl when EmUTech email filtering, another company he founded and operated as CEO, was acquired by SurfControl in 2001. Mr. Jones holds a B.E. in Electrical Engineering from the University of Technology, Sydney.

He can be contacted at:

Djones AT ThreatMetrix DOT com

Twitter: @djinoz

Phone: 0412 683 111

Terms of Reference:

Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans;

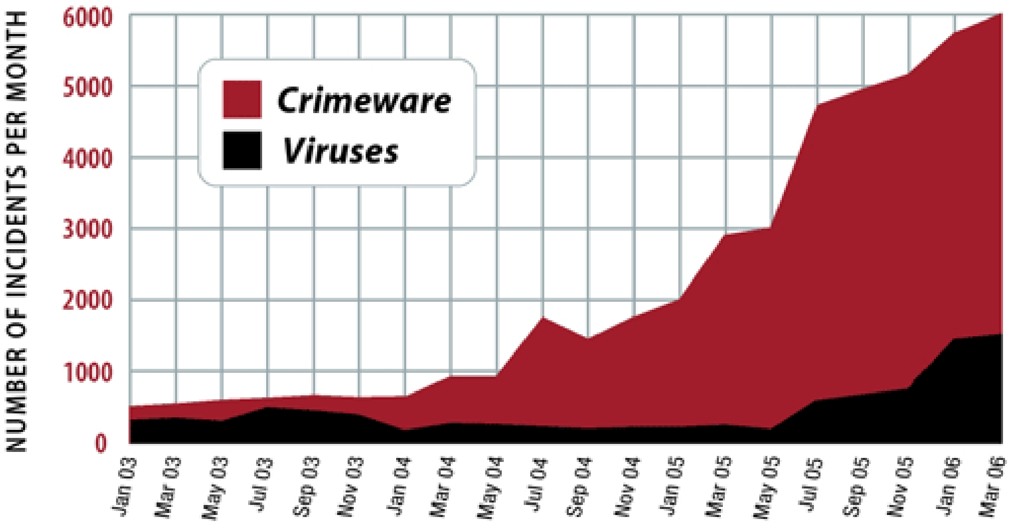
On 26 June 26, 2009, ThreatMetrix systems detected that approximately 205,000 IP addresses within Australian address space were displaying signs of possible infection in the last 7 days.

Most recent ABS statistics indicate 4.2million households have broadband access and making a general assumption of 1 IP address per household and accounting for enterprise and ISP space, **this equates to approximately 4% of computers infected in Australia on this date**.

In 1999, the first mass-email borne virus[1] was unleashed on the public. This virus was called "Melissa". In 2000 "LoveBug" virus launched with a more infectious DNA and proved that most modern computers were susceptible to this new threat. Growth of regularity and impact due to viruses and worms was steady over the period through 2003 as primarily a "nuisance" and something that 'geeks' would propagate for fame.

In 2003 with the delivery of the MigMaf Trojan it became apparent that malware (viruses, Trojans, worms etc) shifted from being an ego-driven enterprise to profit-driven. This was redefining malicious software into a new class of crimeware.

The following diagram illustrates that to 2006 that both viruses and "crimeware" have continued unabated with alarming increases in recent years. The trend has continued through to 2009.



Source: The Kaspersky Internet Security Lab

[1] More correctly considered a worm.

The term “crimeware” is a general grouping for malicious software in the form of:

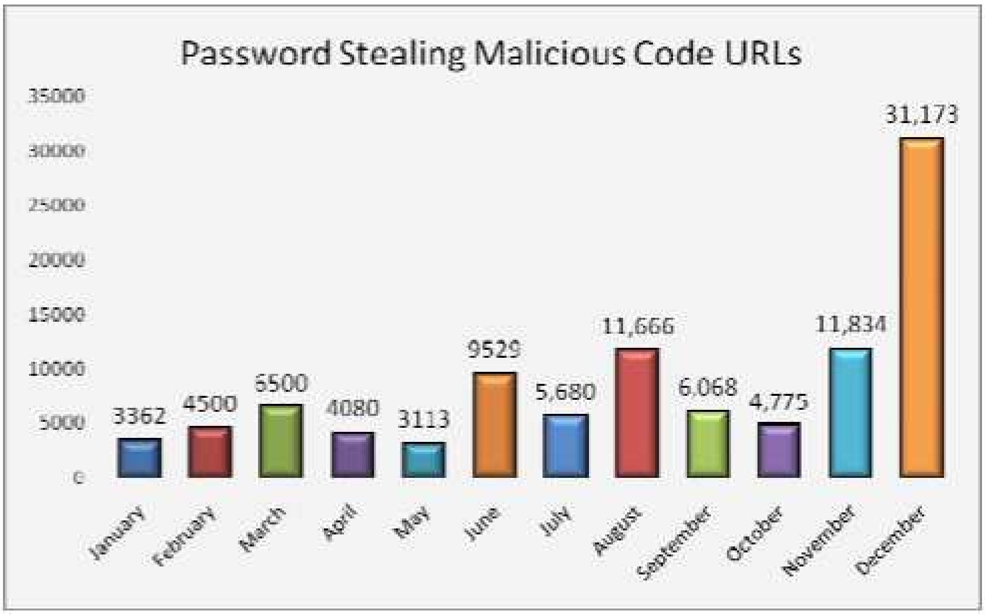
- Trojans
- Keyloggers
- Spyware
- Scareware (rogue anti-malware programs)

Each class of malware was created for the specific goal of executing “identity theft” or financial deception. Identity Theft is the practise of stealing information including but not limited to:

- user logins and passwords
- banking logins and PINs
- credit card details (such as PAN, expiry date, CVV and cardholder address)
- other personal information such as tax information, health identifiers etc

Whilst not limited to computers, identity theft has expanded rapidly due to the ease of stealing data from compromised computers or users.

Year-end Number of Crimeware Sites Surges in Largest Jump Ever in Dec. 2008

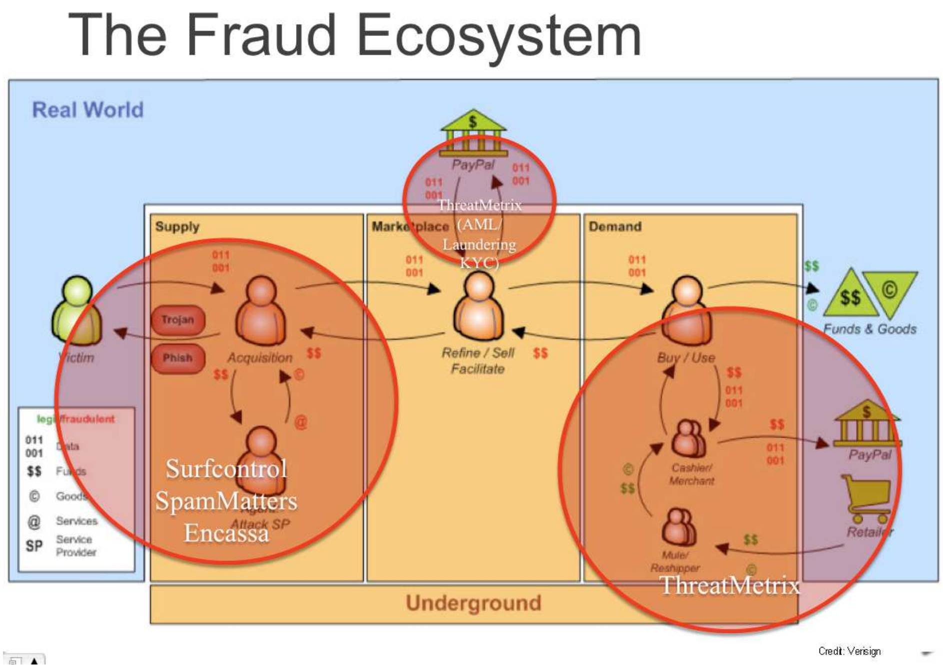


The number of crimeware-spreading sites infecting PCs with password-stealing crimeware reached an all time high of 31,173 in December, an 827 percent increase from January of 2008. See

As can be seen above[2], the trend is that crimeware is increasing more dramatically than “normal” spam and virus spreading malware. To be explicit: **<u>the cybercriminals have focussed their energies on high profit activities. They are abandoning the old techniques of selling “Viagra” and “enlargement” products via spam to simply stealing money and identities from consumers</u>**.

But this is not an accident or co-incidence, I have had the privilege to be in forums with US enforcement officers and our worst fears are confirmed that malicious software provides an essential component of organized crime activities. Consider this quote from a leading antifraud specialist from RSA security:

> *Moloney said: “Fundamentally what we’re seeing is a commercialization of the fraud industry at a level really greater than what we’ve ever seen before.*
>
> *“The barrier for entry, if you’re a non-technical kind of person, has been significantly lowered.”*
>
> *This was seen with ‘fraud-as-a-service’, which meant that people didn’t need technical expertise to infect a machine with a trojan or other type of attack, as they could simply buy what they needed.*
>
> *Fraud-as-a-service has the potential to be a game-changer in favor of online fraudsters and against those conducting legitimate business on the worldwide web. The worldwide volume of account logins, new accounts, and online credit card purchases (CNP) increases year after year—and thanks to fraud-as-a-service the number of people willing and able to commit online fraud is likely to grow at a faster rate.*


The Fraud Ecosystem

Credit: Verisign

[2] Source: Antiphishing workgroup

The submitter/author's experience is shown in this diagram, the "Fraud as a Service" ecosystem is multifaceted and on most fronts we are losing the battle. Our enforcement personal do not have the tools, resources or international support to mount a credible defence.

Nationally, it is a common scenario where a public servant develops a level of expertise where their skills are valuable in private industry at a significant increase to their salary. Therefore these staff serves their apprenticeship in public service then migrate to private industry – it is a common pattern. Therefore, the public service cannot retain skills in the face of an extremely sophisticated and profitable enemy.

At the same time, consumers pay for technology to protect themselves – but this technology is not providing adequate protection. In this study (http://secunia.com/gfx/Secunia_Exploit-vs-AV_test-Oct-2008.pdf) only one antivirus vendor tested was able to detect greater than **3%** of 300 exploits of which 126 were considered critical.

The report generated much debate about the methodology used in the study but illustrates that no current antivirus solution is perfect. Because the malicious software is extremely sophisticated, consumers often misconstrue that by purchasing antivirus software they are completely (100%) protected – this is not the case.

Such naivety may result in some consumers being blasé in regard to opening malicious attachments or visiting malicious websites – misplaced belief of 100% protection leaves these consumers vulnerable to infection.

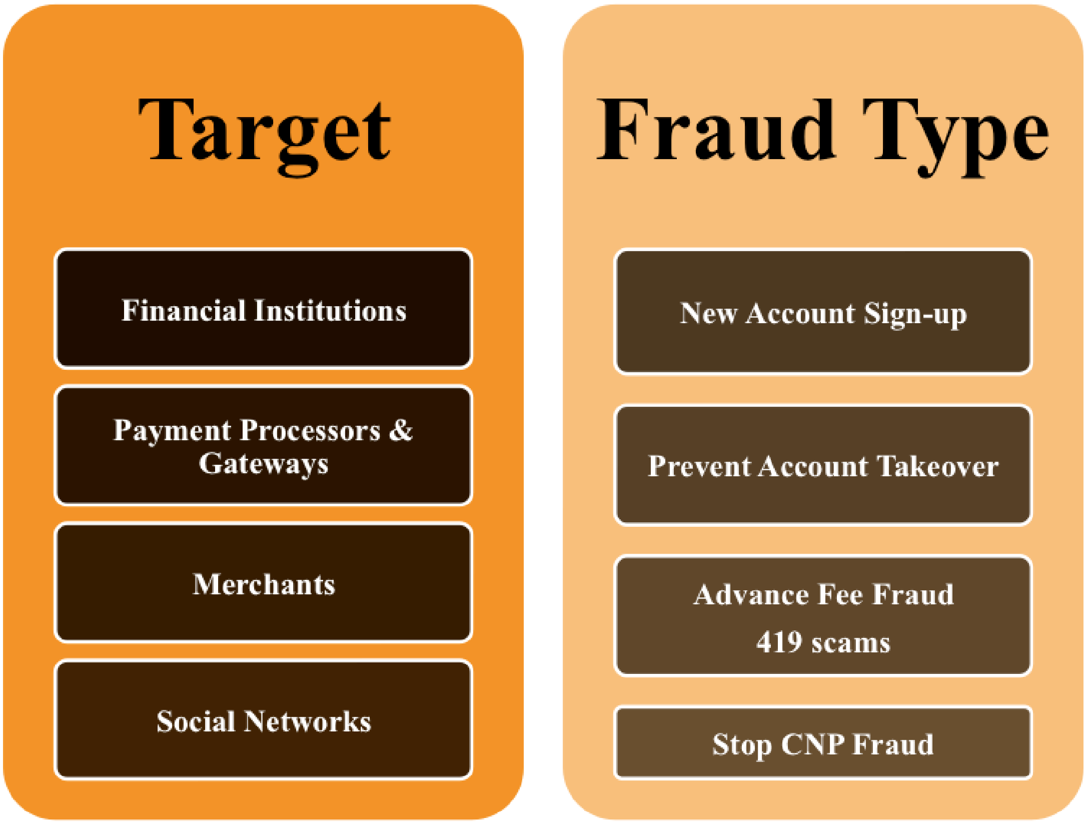
Social Engineering

Whilst not related to malicious software, the use of social engineering remains a common method enticing users to infection. Users of Linux or Apple OS/X operating systems can commonly have the misconception that their systems are impervious to infection – however there are Trojans that perform Keylogging for identity theft.

More on Social Engineering in section c, d.

b) The implications of these risks on the wider economy, including growing economic and security impact of botnets.

Fraud online is everywhere that e-commerce flows. ThreatMetrix encounters the following daily:



<u>It should be noted that in this diagram (that whilst not listed), consumers are also the targets and victims.</u>

It is common to find Advance Fee Fraud (419 scams) in dating and personal websites, fraud is not purely about banking and credit card transactions.

This is one of the topics under discussion at the High Tech Crime Symposium in July organised by Queensland Police.

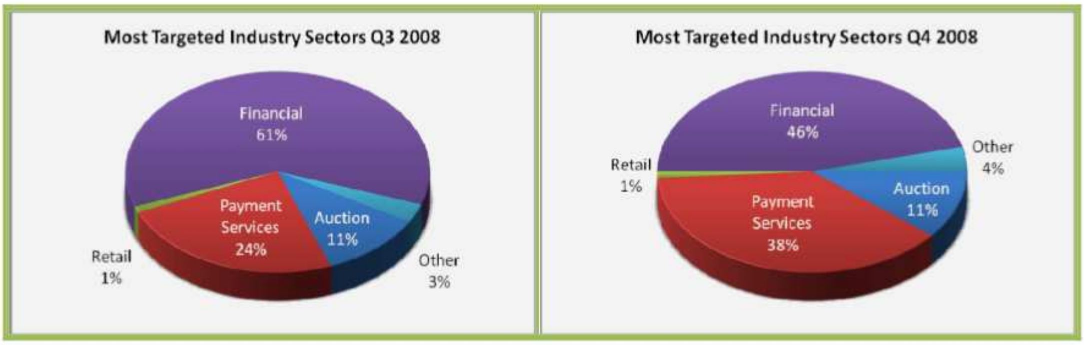
http://www.police.qld.gov.au/News+and+Alerts/campaigns/synergy/hitechsymp/default.htm

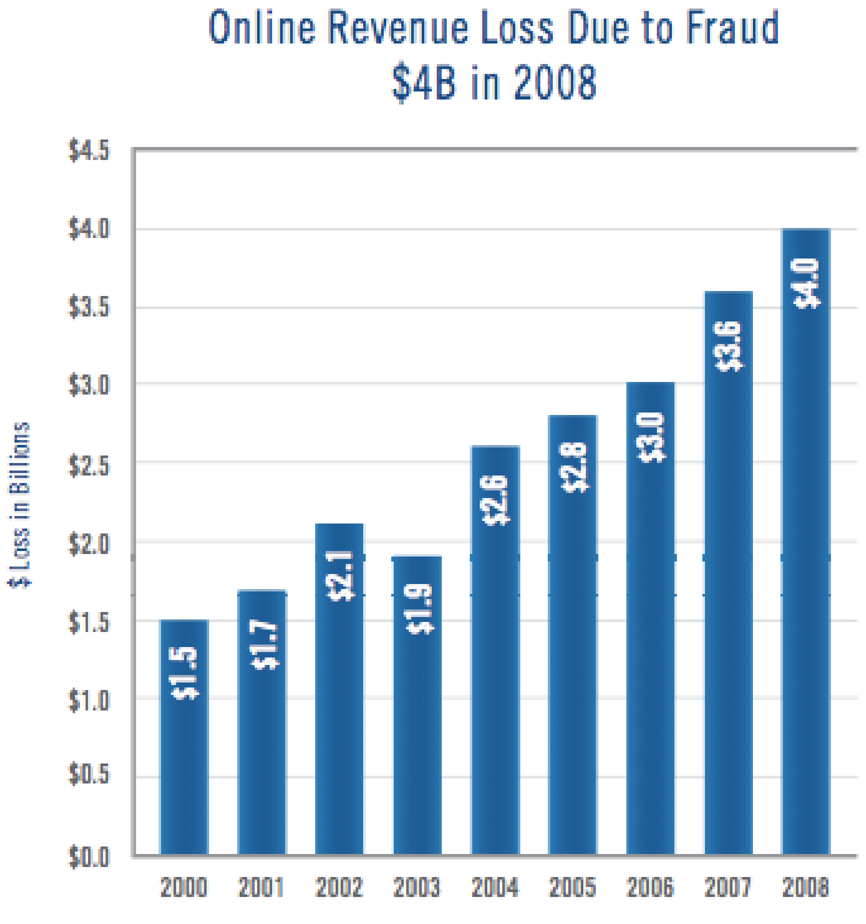
Fraud Statistics

It is challenging to obtain indicative figures from banking organisations about fraud losses – banks are quite opaque on this matter – this is not unexpected; a key element of a bank's value is its credibility as safe and trustworthy institution. (Not withstanding sub-prime meltdown and Australian banking fees).

The absence or opacity of such information in the public domain is problematic - any figures published are like an iceberg; the true (much larger) measure is hidden beneath the surface.

However, there are more freely shared statistics that indicate the true import of the problem. This diagram[3] represents incidents of "Account takeover"





This statistic[4] shows that "card not present" (Credit Card Fraud) losses in the US have been progressively growing. Other statistics have shown similar figures in Europe. It is reasonable to project that Australian online (cybercrime) losses are no less than "10's of millions".

[3] Source: Antiphishing workgroup

[4] Source: Cybersource

In 2007 Australian Payments Clearing Association reported that fraud in credit card transactions was over AU$84million. In 2009, the same entity reported a 47% increase in this statistic

> *David Bell, Chief Executive of the ABA, said: "We have seen an increase in credit card fraud rates. Fraud on credit card transactions, in particular card-not-present transactions, such as those made online or via telephone, has increased, as well as fraud committed by criminals skimming the card information and creating counterfeit cards."*

The trend is clear – online commerce affords cybercriminals anonymity and refuge from detection and incarceration.

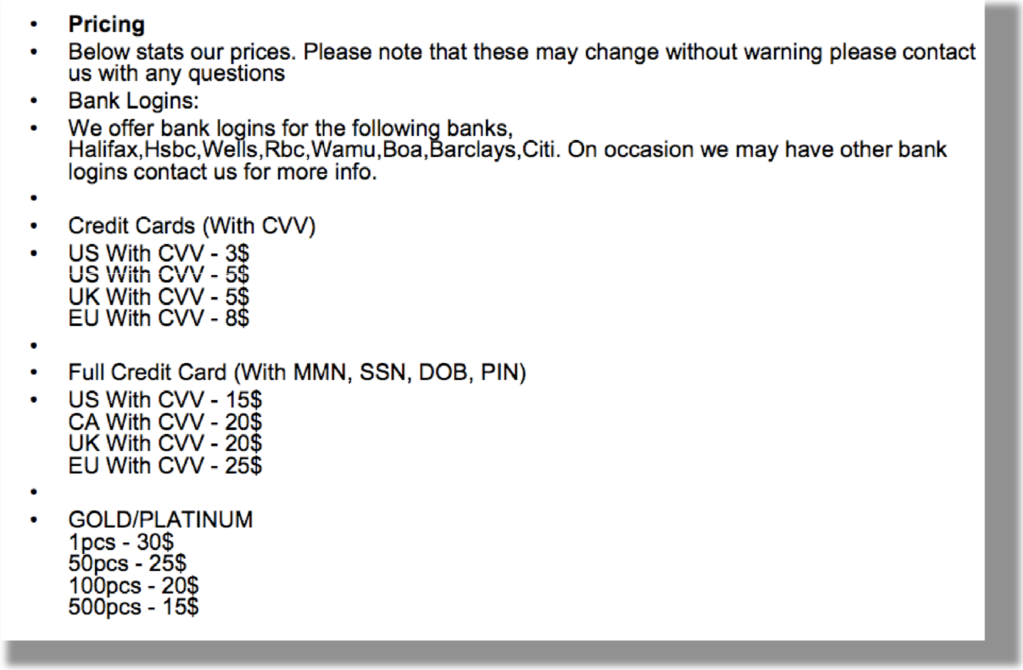
I don't have statistics on consumer confidence but most people I speak with (who are outside the internet security industry) are simply confused about whether they can trust their computer for conducting banking and purchases.

Some numbers do exist globally for stolen identities (credit cards and purchaser information) based on large security breaches, here are some examples:

- TJX had over 45 million credit cards stolen
- Heartland payment process had over 100 million credit cards were stolen
- 220 financial institutions were affected by the Heartland breach
- The TJX hacker spent $75,000 on a birthday party for himself and once complained that he had to manually count $340,000 in pilfered $20 bills because his counting machine broke.

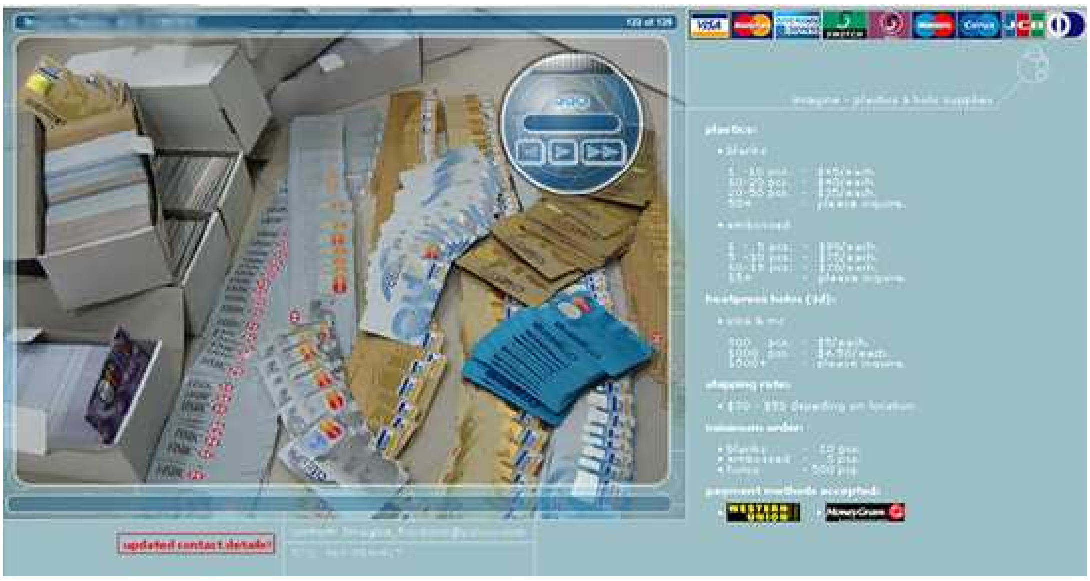
This has a devastating impact to the growth of online commerce and is ultimately bad for economy, for business and for taxation revenues.

As shown in my "Fraud Ecosystem" diagram, there is a market place for selling or exchanging stolen identity data. Here is a posting on a "carders" forum promoting stolen credit cards for just a few dollars. This is extremely common if you know where to look.



- **Pricing**
- Below stats our prices. Please note that these may change without warning please contact us with any questions
- Bank Logins:
- We offer bank logins for the following banks, Halifax,Hsbc,Wells,Rbc,Wamu,Boa,Barclays,Citi. On occasion we may have other bank logins contact us for more info.
-
- Credit Cards (With CVV)
- US With CVV - 3$
  US With CVV - 5$
  UK With CVV - 5$
  EU With CVV - 8$
-
- Full Credit Card (With MMN, SSN, DOB, PIN)
- US With CVV - 15$
  CA With CVV - 20$
  UK With CVV - 20$
  EU With CVV - 25$
-
- GOLD/PLATINUM
  1pcs - 30$
  50pcs - 25$
  100pcs - 20$
  500pcs - 15$

I've seen in other online marketplaces Australian credit cards for sale typically about US$3 per card. Once someone purchases these credit cards, they can use these for online (CNP) transactions or they can do the following:



This diagram shows the availability of blank credit cards impersonating many globally recognized banks:

```
Stolen Identities + Embossed Credit cards = Offline Fraud
```

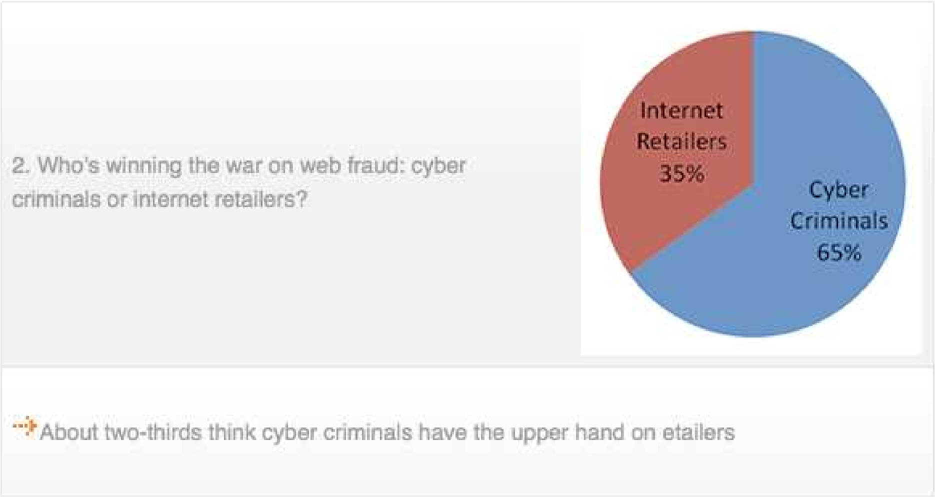
This simple equation shows that cybercrime feeds back to real-world credit card fraud. As the MasterCard advertisements say….**"Priceless"**.

Whilst the comment is flippant the reality is that proceeds of identity theft from the internet can now be used by fraudsters for physical world goods and services

– this is damaging to the community at large. Often such proceeds are used for gambling, substance abuse and subsistence. But more sinister is the conjecture it is used to fund terrorist activities. Austrac would have more authoritative information on that.

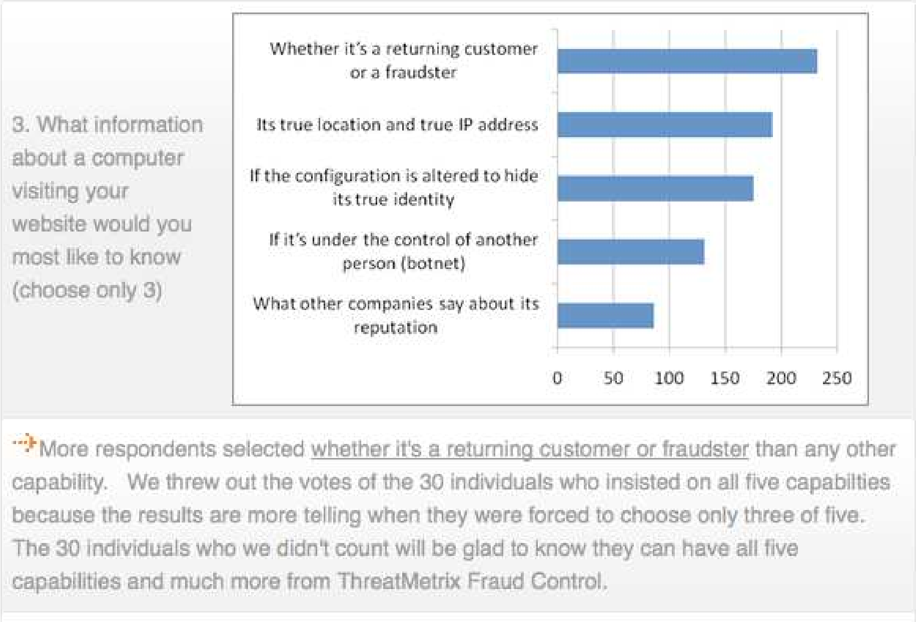
Impact on SME Merchants

In ThreatMetrix's own survey of online merchants they revealed a disturbing fact – that the criminals are winning:



2. Who's winning the war on web fraud: cyber criminals or internet retailers?

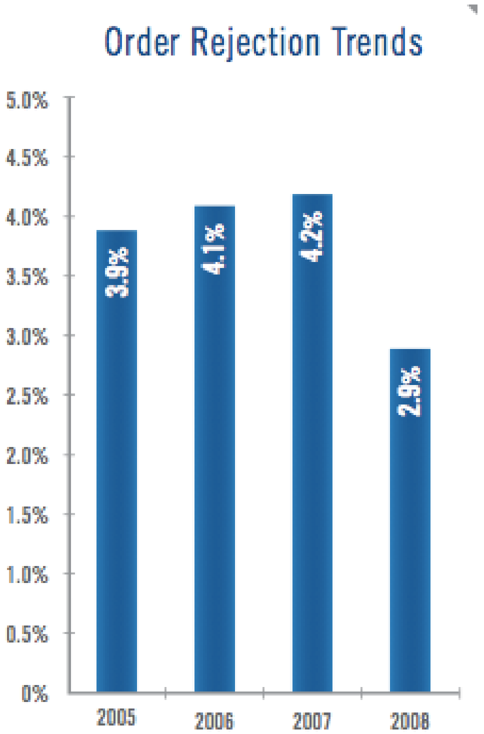
⇢ About two-thirds think cyber criminals have the upper hand on etailers



3. What information about a computer visiting your website would you most like to know (choose only 3)

⇢ More respondents selected whether it's a returning customer or fraudster than any other capability. We threw out the votes of the 30 individuals who insisted on all five capabilties because the results are more telling when they were forced to choose only three of five. The 30 individuals who we didn't count will be glad to know they can have all five capabilities and much more from ThreatMetrix Fraud Control.

In response to cybercrime threats, online merchants are reacting by accidentally rejecting good orders as well as fraudulent orders – for them, the risk of financial loss is too great to take chances. This translates directly to lost revenue and reductions in commerce in general. In security terms, this is referred to as a "False Positive".



The above diagram shows that in 2008 merchants are rejecting slightly lower percentages of online orders but this is largely accountable to more sophisticated merchants implementing fraud detection systems such as ThreatMetrix. Areas such as online electronics merchants (cameras, computers etc) typically experience high fraudulent order rates, as the goods can be "fenced" online though popular auction sites.

The problem remains that less mature business do not have the sophisticated tools and experience to fight this crime easily or cost effectively. This becomes an onerous "cost of doing business".

b) Level of understanding and awareness of e-security risks within the Australian community;

ThreatMetrix has participated in the Internet Industry Association activities such as "ZombieWeek" - an awareness campaign about botnets and fraud. In past years ThreatMetrix has also provided information and support for e-security week.

Senator Conroy in his recent 2009 e-security week opening stated:

> *"In fact, our key message is that being more secure online can be as easy as strengthening your password.*
>
> *It is important that people understand the steps they can take to improve their e-security and we all have a role to ensure the right information is available.*
>
> *The messages are simple but salient.*
>
> *Ensuring people understand how to avoid losing bank details to criminals, how to avoid online scams and how to protect their personal information goes a long way to ensuring online confidence."*

This captures the state of sophistication of our countries online community, we need to reach the most vulnerable as they will be easy targets. Without any educational expertise I would commend such initiatives as:

- http://www.staysmartonline.gov.au particularly thing like budd:e but I don't know of equivalent programs for seniors
- http://www.childsafe.org.au

However, I would caution that even experienced users will be susceptible. For example as discussed in (b) – Advanced Fee/Nigerian/419 fraud has massive personal impact on individuals. Education is required for seniors and people who have savings that can be scammed. Information exists at:

http://www.scamwatch.gov.au/content/index.phtml/tag/Nigerian419Scams

http://www.scamwatch.gov.au/content/index.phtml/tag/UpfrontPaymentScams

But I am sceptical if this information is illustrative enough of what actually happens. I would recommend role-playing and tests that people can actually engage in. A few years ago I saw a company deliver an online phishing simulation, this allowed people to test their skills and develop awareness.

With the availability of media tools such as youtube, education can be more visceral, entertaining and understandable and can also direct users to educational media reports such as this from a US TV network http://www.youtube.com/watch?v=2-wFhy0ouzI&feature=related

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:

- Education initiatives

- Legislative and regulatory initiatives

- Cross-portfolio and inter-jurisdictional coordination

- International co-operation.

In 2004 I participated in the OECD Taskforce against Spam and also ITU WSIS Thematic Meeting on Countering Spam.

http://www.oecd.org/document/7/0,3343,en_2649_34487_33656711_1_1_1_1,00.html

http://www.itu.int/osg/spu/spam/

At the time, the Australian Government presented a leadership position in both legislation and practical enforcement. This led to MOUs being signed with Korea, US, UK and others for joint co-operation and inter-jurisdictional coordination. I am not privy to know if these foundations allowed for practical outcomes but I applaud the initial leadership efforts – this should be continued.

I believe the actions taken at that time still keep Australia in a better condition than most other countries in regard to spam and phishing.

e) Future initiatives that will further mitigate the e-security risks to Australian internet users.

It is my belief that the government should focus on five key areas:

1. Education and awareness for the community at large
2. Legislation – a refresh/review of cybercrime laws is required to respond to the current environment of botnets, compromised hosts and stolen identities.
3. Enforcement – particularly international co-operation and inter-jurisdictional information flow and coordination. There must be credible proof of a country's ability to enforce laws – it needs to be an effective deterrent to crime otherwise the impact will be nil.
4. Support to innovation and services of e-security in Australia. Companies like ThreatMetrix and Encassa employ staff and produce products that ultimately benefit the community at large. Continued incubation and commercialisation grant support is pivotal to such innovation.

a. The Rudd government discontinued the AusIndustry **Commercial Ready grant** system and has not delivered an adequate replacement.

b. Contrast with Israel who leads the world in security innovation with such companies as Checkpoint being started in Israel but graduating to a global company (with a US$4.9B market cap on 26th June 2009)

c. The National Broadband Network is a large commitment. However, committed, detailed considerations of the security implications are not clear to this submitter from following normal press reports. In the early 2000, Korea deployed massive broadband and rapidly grew to being a world leader in Botnet hosts (not an enviable position). The Korean government responded and supported a number of national Internet security initiatives and ultimately wrestled the Botnet problem to a much-reduced level.

d. The government should seek to partner with industry to build a permanent set of skills and tools for analytics, intelligence and enforcement that give the government and public service resilience against loss of knowledgeable staff to private industry, matters of e-security are simply too important to be secondary to market forces for skills.

5. Support and strategy for a number of national initiatives on digital identity and transaction authentication. As opposed to some previous initiatives, consumers should be able to opt-in and opt-out of such models where they have privacy concerns but may apply this authentication to transactions where they seek to ensure security and prove their identity for their own protection. I am not proposing an ill-considered implementation but a formation of a national strategy.

Each of these five areas cannot be addressed or solved by market forces alone.

f) Emerging technologies to combat these risks.

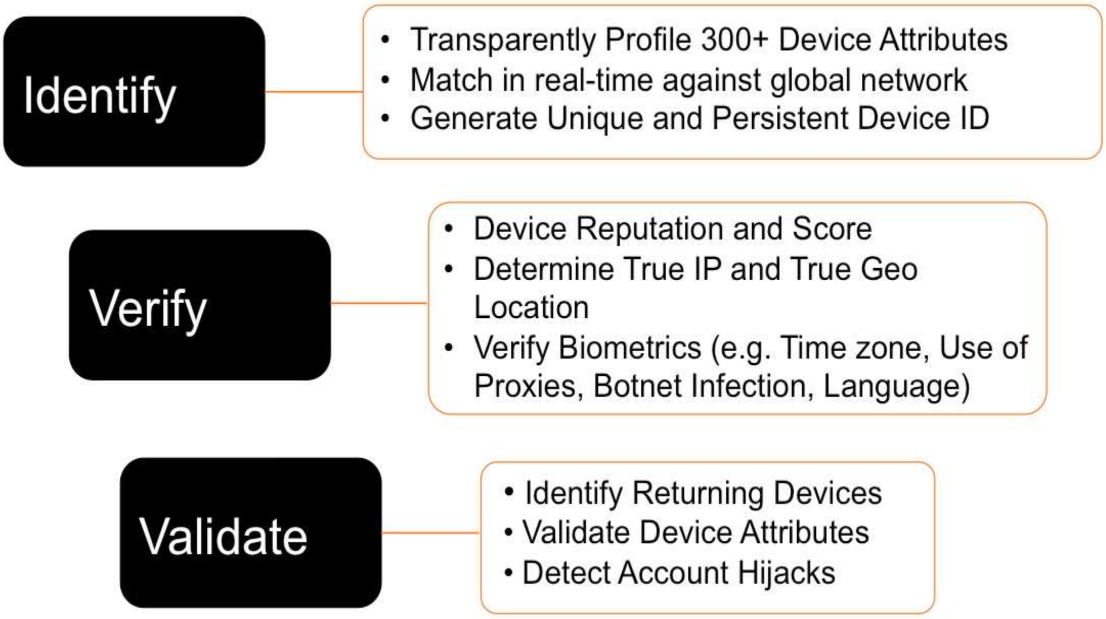
To date, there does not appear to be a practical and commercially viable "silver bullet" for these threats.

For this reason there are many technologies that attempt to address different elements of the problem – as illustrated in the "Fraud Ecosystem" diagram. The following are examples the author/submitter has involvement.

e-commerce transaction protection

Technologies such as ThreatMetrix were designed to assist in fraud mitigation in environments where it is assumed the consumer's PC has been infected and is either a Botnet host or compromised in some other way that a fraudster may be controlling the machine.

The purpose is to protect e-commerce entities because in most countries these (often SMEs) carry the risk of the transaction and have to repay money when fraud occurs on a consumer's credit card – this is called a "chargeback".


Identify
• Transparently Profile 300+ Device Attributes
• Match in real-time against global network
• Generate Unique and Persistent Device ID
Verify
• Device Reputation and Score
• Determine True IP and True Geo Location
• Verify Biometrics (e.g. Time zone, Use of Proxies, Botnet Infection, Language)
Validate
• Identify Returning Devices
• Validate Device Attributes
• Detect Account Hijacks

ThreatMetrix can be deployed in e-commerce application that needs increased protection from fraudulent logins, account hijack, account creation or fraudulent transactions.

With the emergence of Man-in-the-Browser attacks (MITB) and Man-in-the-middle (MITM), Device Intelligence can also provide risk assessment for transactions exploited by such techniques.

Desktop protection

Innovative desktop (consumer PC) solutions such as Encassa function on the premise that a computer can/will be easily infected and the user is not aware of it.

Encassa creates a "safe zone" within the infected PC, where the user can conduct transactions and be protected from "identity theft". Encassa achieves this by installing itself prior to rootkits and then encrypting keystrokes that would normally be logged by keystroke loggers and identity theft malware.

Similar technologies provide a completely "disposable" virtual machine for either transactions or visiting un-trusted sites. The underlying computer hardware and operating system remains untouched (ideally).

Inexpensive or free multi-factor authentication

With the emergence of iPhones and other smart phone technologies, it is expected that existing 2-factor or multi-factor cryptographic technology will be deployable without additional cost. In the past, digital identity solutions that relied on hardware "tokens" have generally proven to be unattractive to consumer facing e-commerce entities to deploy because of the per unit hardware cost and overall cost-of-ownership. By using smart-phones that are considered to be "sand-boxed" or immune to compromise, the hardware deployment cost is driven to zero.

It should be noted that these solutions do not solve problems such as some MITM types or MITB.