NATIONAL CONGRESS

23 – 25 NOVEMBER 2016

GRAND HYATT MELBOURNE

Event Partner:

Reckon

IPA INSTITUTE OF PUBLIC ACCOUNTANTS®

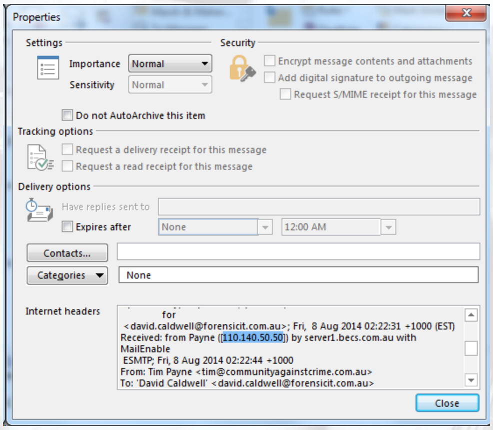
Internet Investigations
Theft of Intellectual Property
Spear Phishing
Ransomware
Payroll Compromise

Internet based investigations – IP Addresses

IP Address (Internet Protocol)

An IP address is a unique numeric value assigned to any computer on the internet

203.122.145.110



Properties

Settings

Importance: Normal

Sensitivity: Normal

□ Do not AutoArchive this item

Security

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request S/MIME receipt for this message

Tracking options

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Delivery options

Have replies sent to

□ Expires after: None 12:00 AM

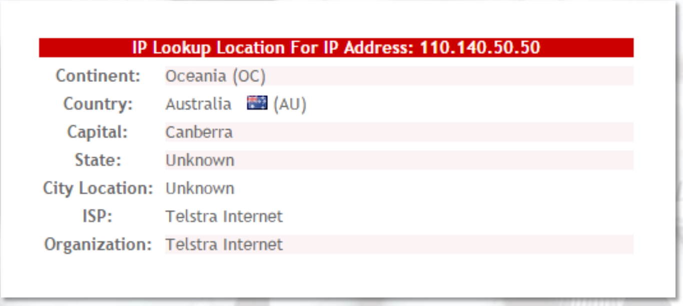
Contacts...

Categories: None

Internet headers

```
          for
 <david.caldwell@forensicit.com.au>; Fri,  8 Aug 2014 02:22:31 +1000 (EST)
Received: from Payne ([110.140.50.50]) by server1.becs.com.au with
MailEnable
 ESMTP; Fri, 8 Aug 2014 02:22:44 +1000
From: Tim Payne <tim@communityagainstcrime.com.au>
To: 'David Caldwell' <david.caldwell@forensicit.com.au>
```

www.ip-tracker.org/



IP Lookup Location For IP Address: 110.140.50.50

Continent:	Oceania (OC)
Country:	Australia (AU)
Capital:	Canberra
State:	Unknown
City Location:	Unknown
ISP:	Telstra Internet
Organization:	Telstra Internet

What does the IP address tell us?

The identity of the Internet Service Provider (ISP) who was used.

From the ISP we can find out the name, address and billing information of the owner of the Internet Access Account.

Madeline Pulver- Mosman Collar Bomb Hoax

On 3 August 2011 in the mid-afternoon Peters walked through the front door of the home wearing a rainbow balaclava and carrying a baseball bat and a backpack.
He confronted Ms Pulver and then told her: "I'm not going to hurt you."
He then removed a black box from the backpack and tied it around his victim's throat with a USB stick and a two-page letter.

Read more: http://www.smh.com.au/nsw/maddie-pulver-bomb-hoax-pictures-released-20121019-27von.html#ixzz3BTTTKc5a

Nightmare in Mosman
August, 2011
• Attacker straps teen in collar 'bomb'
• She endures 10-hour ordeal
• Hoax sparks massive police operation
• FBI SWAT team arrests man in US
MOSMAN
SYDNEY CBD

- "Powerful new technology plastic explosives are located inside…... The case is booby trapped. …………………………..I am a former special forces Green Beret Munitions specialist, and have constructed such devices over 20 years…….you will inadvertently trigger a tragically avoidable explosion ... You will be provided with detailed remittance instructions to transfer a Defined Sum…………….. If remittance instructions are executed CORRECTLY … I will immediately provide you with: 1) The combination that can open the case without triggering a **Brian Douglas Wells** event and 2) An internal key to completely disable the explosive mechanism embedded inside ... "

Read more: http://www.smh.com.au/nsw/count-to-200--ill-be-back--if-you-move-i-can-see-you-details-of-maddie-collar-bomb-revealed-20120308-1ulir.html#ixzz3BTWJRJ6M

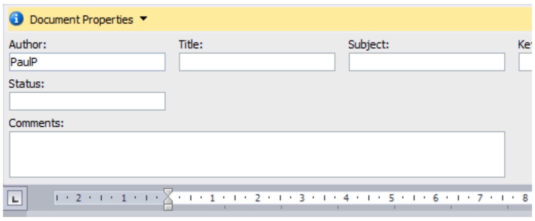
http://en.wikipedia.org/wiki/Brian_Douglas_Wells

Sources of Evidence & Info

- Two primary sources of evidence
- USB placed around Madeline’s neck containing a ransom demand
- Gmail account – dirkstruan1840@gmail.com from the ransom demand

USB Device

- Contained a ransom demand in a Word document
- Metadata



Document Properties

Author: PaulP

Title:

Subject:

Status:

Comments:

- Deleted: Two previous versions of demand
- Deleted: Draft letter of demand addressed to the "Trustee of the James M.Cox Estate Trust".

The Gmail Account – dirkstruan1840@gmail.com

Information from Google:

- Created on 30 May 2011
- IP address – Chicago airport
- Airline passenger list

On the day of the assault on Madeline Pulver the account was accessed three times. Tracing the IP addresses identified:

- 1 - public internet terminal at Kincumber Library
- 2 & 3 – Avoca Beach Video

Credit Cards & CCTV

Credit card records:

- Purchase of a USB device and a purple lanyard from Officeworks in West Gosford on July 4
- Purchase of a black aluminium softball bat from Rebel Sport at Erina Fair on July 16

CCTV footage:

- Erina Fair shopping centre – Baseball bat
- Kincumber Library – Gmail account access
- Avoca Beach video shop - Gmail account access
- Sydney airport – flight to USA
- Purchase of items to assemble the homemade "explosive" device

IP Address Logs & Data Retention Laws

- "Data retention" describes the retention of metadata by telecommunication services providers (BigPond/Optus etc) for all customers for a legislated period of time.
- That data is then available for law enforcement agencies to use in their investigations.

What is Metadata?

Metadata is widely understood by government officials to include the following:

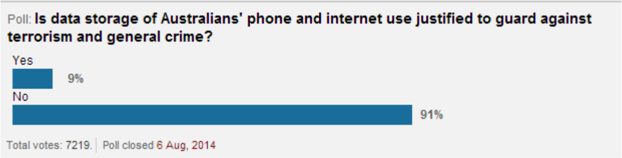
1. Telephone numbers
2. The IP addresses of computers from which messages are received or sent
3. Location of parties making phone calls/communications
4. To and from email addresses on emails
5. Logs of visitors to chat rooms online
6. Chat aliases or identifiers (the name a person uses in a chat room online)
7. Start and finish times of internet sessions

Metadata is not:

1. Content of a phone call or an email
2. Subject line of an email
3. What is said in a chat room online
4. Content of a SMS
5. Attachments to emails
6. Web camera transmissions
7. Websites a person visits (i.e. browsing histories)
8. Names of websites

Is this a new thing?

- Agencies accessed metadata 330,640 times in 2012-13 - an 11 per cent increase in a year and a jump of 31 per cent over two years.
- ASIO is not included in the figures as it is exempt from having to report the number of requests it makes
- Something similar proposed about 2 years ago….which wasn't popular with most.



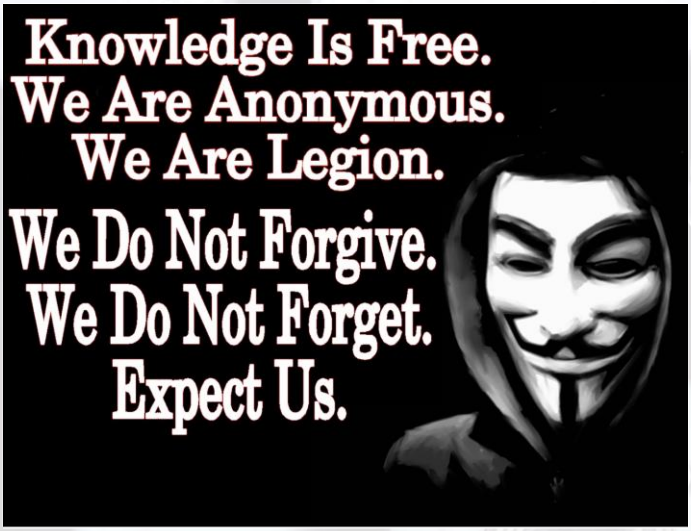
Poll: **Is data storage of Australians' phone and internet use justified to guard against terrorism and general crime?**

Yes 9%

No 91%

Total votes: 7219. Poll closed 6 Aug, 2014

- Even 'anonymous' weren't happy with the Australian Government's idea!



Hackers cripple ASIO site to protest web spy plan

Over the past week Anonymous' Australian Twitter account has been boasting it will attack the ASIO website and that of Defence Signals Directorate. "The anonymous Operation Australia hackers have today again been busy with further attacks on the ASIO and DSD website," Anonymous Australia wrote on Wednesday.

ASIO's website was down for at least half an hour this morning and now either works, loads slowly or doesn't work at all.

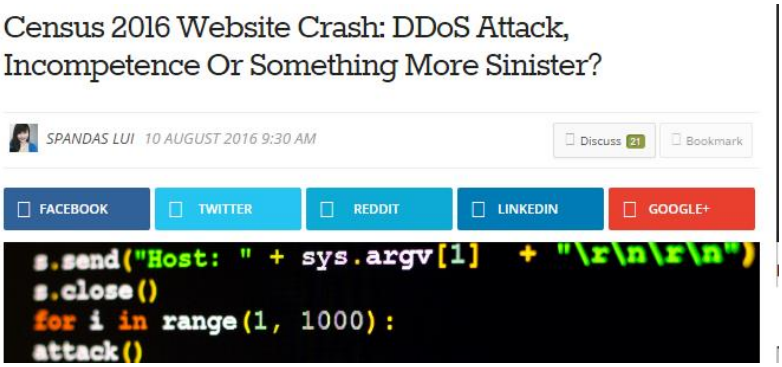
2010 PayPal DDoS Attack

- PayPal pulled support for Wikileaks, which had dumped 250,000 classified US State Department cables.
- PayPal said the move was in response to "a violation of the PayPal Acceptable Use Policy" because Wikileaks "was encouraging sources to release classified material."
- Anonymous DDoS attacks PayPal, Amazon, Visa, and MasterCard websites
- DoJ arrest 16 people for Anonymous-related DDoS attacks
- Claiming to support transparency and counter-censorship.

Anonymous Targets Trump

Back in early March, hackers affiliated with Anonymous tried to reboot their Operation Trump campaign by calling for everyone to take down Trump's websites in a coordinated effort on April 1. Almost immediately, the initiative was criticized by people within Anonymous as irresponsible and "cringeworthy," but a dedicated group apparently moved on with the plan

Census DDoS Attack



Census 2016 Website Crash: DDoS Attack, Incompetence Or Something More Sinister?

SPANDAS LUI 10 AUGUST 2016 9:30 AM

```
s.send("Host: " + sys.argv[1]  + "\r\n\r\n")
s.close()
for i in range(1, 1000):
attack()
```

Theft of IP

The Most Common Scenario

Employee moving on – what have they taken?

- Client lists
- Research data
- Financial info
- Project info
- Templates
- Presentation information

Case examples

- Wilson v Secure
- Utilities company – external hard drive
- Property Development company – Keylogging

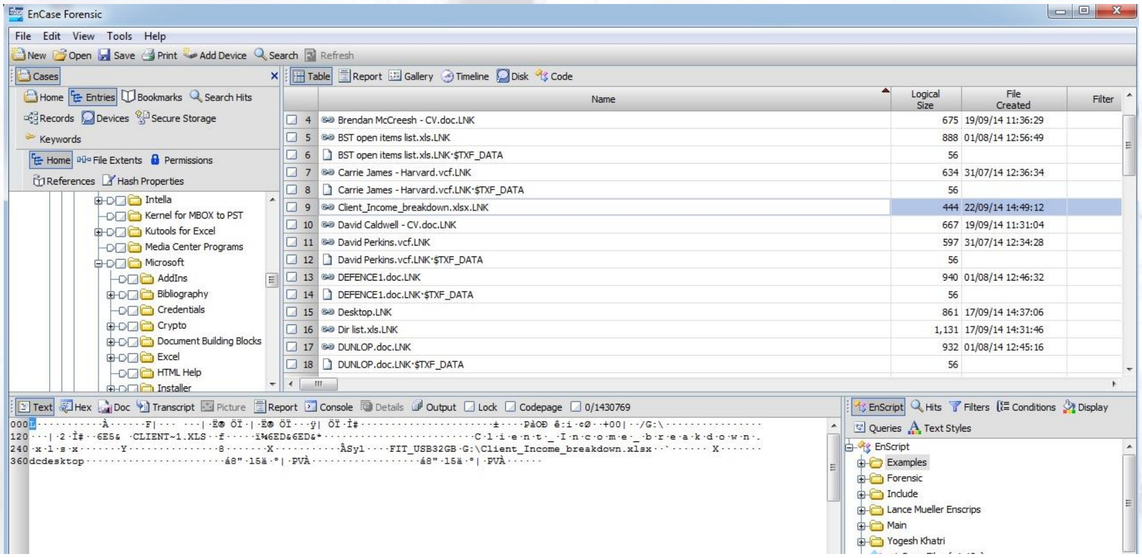
What do we examine?

- Employee's desktop/laptop/iPad/phone:
  - Link files
  - Deletion
  - Webmail
  - External storage (USB) devices
  - Discussions with other employees
  - Social Media: Facebook/Twitter/LinkedIn
  - Registration of business names
  - Lease of Premises

Chronology

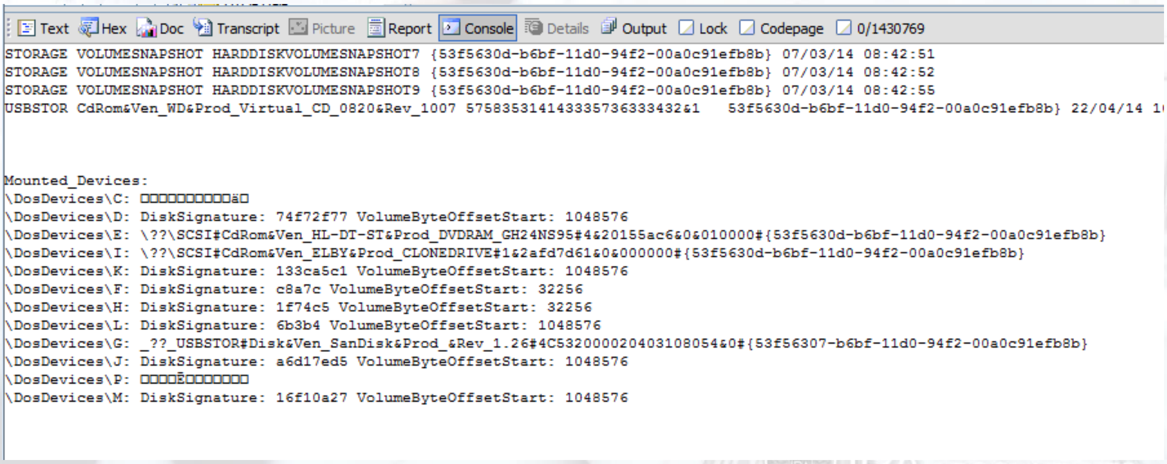
- Analyse the time leading up to departure
- Evidence of USB device insertion on computer
- Power off command to USB device?
- What documents have been accessed immediately before or after the USB?
- Do link files show source of document as a USB device?
- What documents have been sent off to a personal webmail account?

Link files


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Search Hits
Records Devices Secure Storage
Keywords
Home File Extents Permissions
References Hash Properties
Intella
Kernel for MBOX to PST
Kutools for Excel
Media Center Programs
Microsoft
AddIns
Bibliography
Credentials
Crypto
Document Building Blocks
Excel
HTML Help
Installer
Table Report Gallery Timeline Disk Code
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/1430769
EnScript Hits Filters Conditions Display
Queries Text Styles
EnScript
Examples
Forensic
Include
Lance Mueller Enscrips
Main
Yogesh Khatri

	Name	Logical Size	File Created	Filter
4	Brendan McCreesh - CV.doc.LNK	675	19/09/14 11:36:29	
5	BST open items list.xls.LNK	888	01/08/14 12:56:49	
6	BST open items list.xls.LNK·$TXF_DATA	56		
7	Carrie James - Harvard.vcf.LNK	634	31/07/14 12:36:34	
8	Carrie James - Harvard.vcf.LNK·$TXF_DATA	56		
9	Client_Income_breakdown.xlsx.LNK	444	22/09/14 14:49:12	
10	David Caldwell - CV.doc.LNK	667	19/09/14 11:31:04	
11	David Perkins.vcf.LNK	597	31/07/14 12:34:28	
12	David Perkins.vcf.LNK·$TXF_DATA	56		
13	DEFENCE1.doc.LNK	940	01/08/14 12:46:32	
14	DEFENCE1.doc.LNK·$TXF_DATA	56		
15	Desktop.LNK	861	17/09/14 14:37:06	
16	Dir list.xls.LNK	1,131	17/09/14 14:31:46	
17	DUNLOP.doc.LNK	932	01/08/14 12:45:16	
18	DUNLOP.doc.LNK·$TXF_DATA	56		

```
000L···········À······F|···  ···|·Ë® ÖÏ·|·Ë® ÖÏ···ÿ| ÖÏ·Ì‡·······················±····PàOÐ ê:i·¢Ø··+00|··/G:\················
120···|·2·Ì‡··6E5&  CLIENT~1.XLS··f·····ï¾6ED&6ED&*·························C·l·i·e·n·t·_·I·n·c·o·m·e·_·b·r·e·a·k·d·o·w·n·.
240·x·l·s·x·······Y···············8·······X···········ÅSyl····FIT_USB32GB·G:\Client_Income_breakdown.xlsx··`······ X·······
360dcdesktop·······················á8"·15ä·°|·PVÀ··················á8"·15ä·°|·PVÀ······
```


Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/1430769

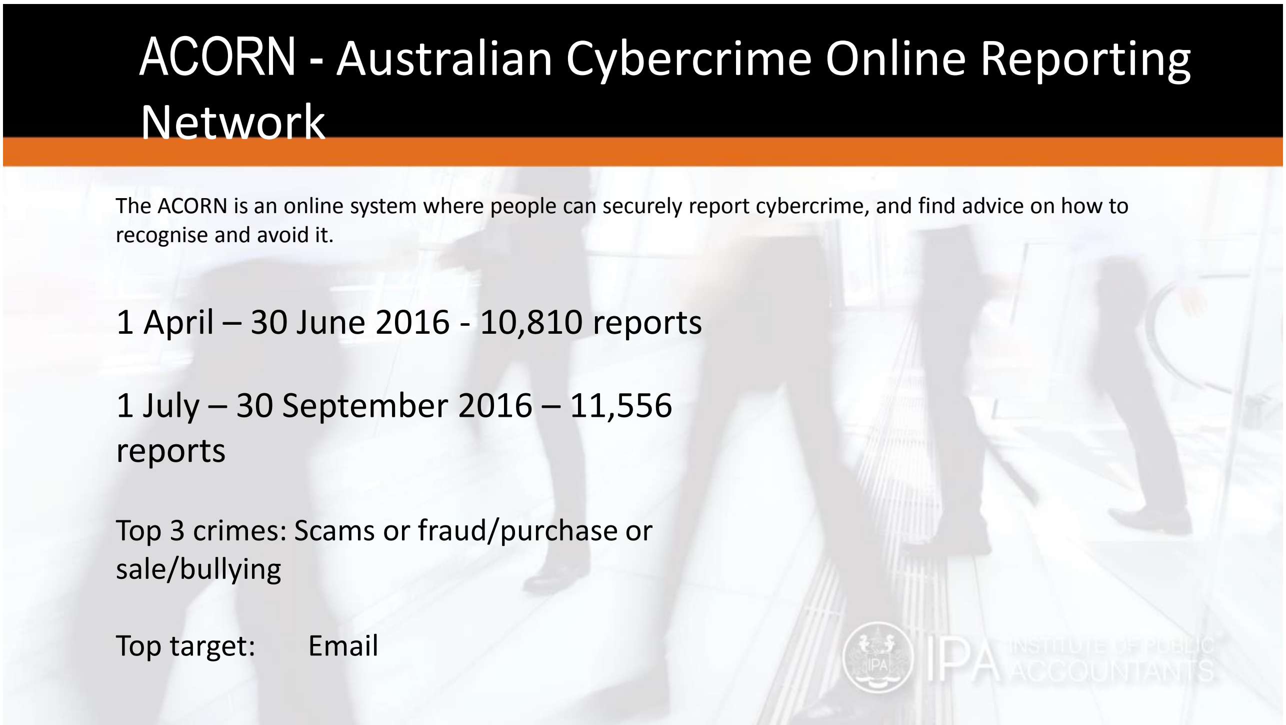
```
STORAGE VOLUMESNAPSHOT HARDDISKVOLUMESNAPSHOT7 {53f5630d-b6bf-11d0-94f2-00a0c91efb8b} 07/03/14 08:42:51
STORAGE VOLUMESNAPSHOT HARDDISKVOLUMESNAPSHOT8 {53f5630d-b6bf-11d0-94f2-00a0c91efb8b} 07/03/14 08:42:52
STORAGE VOLUMESNAPSHOT HARDDISKVOLUMESNAPSHOT9 {53f5630d-b6bf-11d0-94f2-00a0c91efb8b} 07/03/14 08:42:55
USBSTOR CdRom&Ven_WD&Prod_Virtual_CD_0820&Rev_1007 575835314143335736333432&1   53f5630d-b6bf-11d0-94f2-00a0c91efb8b} 22/04/14 1


Mounted_Devices:
\DosDevices\C: □□□□□□□□□□□ä□
\DosDevices\D: DiskSignature: 74f72f77 VolumeByteOffsetStart: 1048576
\DosDevices\E: \??\SCSI#CdRom&Ven_HL-DT-ST&Prod_DVDRAM_GH24NS95#4&20155ac6&0&010000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
\DosDevices\I: \??\SCSI#CdRom&Ven_ELBY&Prod_CLONEDRIVE#1&2afd7d61&0&000000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
\DosDevices\K: DiskSignature: 133ca5c1 VolumeByteOffsetStart: 1048576
\DosDevices\F: DiskSignature: c8a7c VolumeByteOffsetStart: 32256
\DosDevices\H: DiskSignature: 1f74c5 VolumeByteOffsetStart: 32256
\DosDevices\L: DiskSignature: 6b3b4 VolumeByteOffsetStart: 1048576
\DosDevices\G: _??_USBSTOR#Disk&Ven_SanDisk&Prod_&Rev_1.26#4C532000020403108054&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
\DosDevices\J: DiskSignature: a6d17ed5 VolumeByteOffsetStart: 1048576
\DosDevices\P: □□□□Ē□□□□□□□□
\DosDevices\M: DiskSignature: 16f10a27 VolumeByteOffsetStart: 1048576
```

Prevention

- Monitor the business environment
- Have a departure process
- Understand who the ‘key’ employees are
- Real time alerts based on risk profile
  - USB device use
  - Document access
  - Document copying
  - Emailing documents to personal accounts

Criminal Law – Is theft of data an offence

- ***Oxford v Moss*** (1979): Student stole an exam result paper and was charged with theft.
- The court ruled that information was not property within the definition of the Crimes Act and therefore was incapable of being stolen.
- Definition of property: “property includes money and all other property real or personal including things in action and other intangible property.”
- Crown appealed – dismissed.
- R v George



ACORN - Australian Cybercrime Online Reporting Network

The ACORN is an online system where people can securely report cybercrime, and find advice on how to recognise and avoid it.

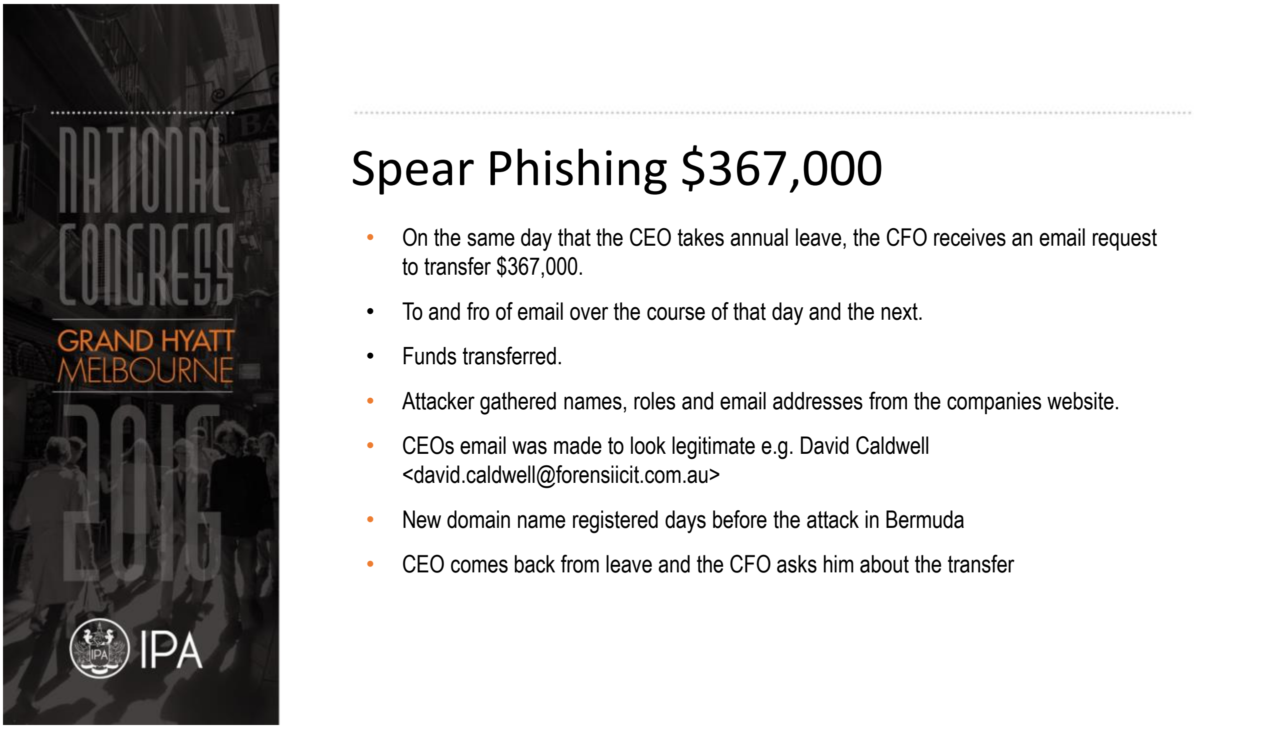
1 April – 30 June 2016 - 10,810 reports

1 July – 30 September 2016 – 11,556 reports

Top 3 crimes: Scams or fraud/purchase or sale/bullying

Top target: Email

IPA INSTITUTE OF PUBLIC ACCOUNTANTS



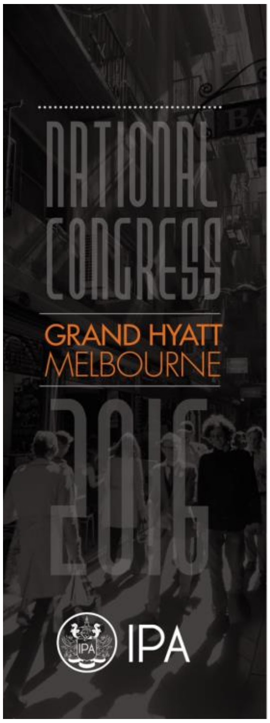
NATIONAL CONGRESS
GRAND HYATT MELBOURNE
2016
IPA

Spear Phishing $367,000

- On the same day that the CEO takes annual leave, the CFO receives an email request to transfer $367,000.
- To and fro of email over the course of that day and the next.
- Funds transferred.
- Attacker gathered names, roles and email addresses from the companies website.
- CEOs email was made to look legitimate e.g. David Caldwell <david.caldwell@forensiicit.com.au>
- New domain name registered days before the attack in Bermuda
- CEO comes back from leave and the CFO asks him about the transfer

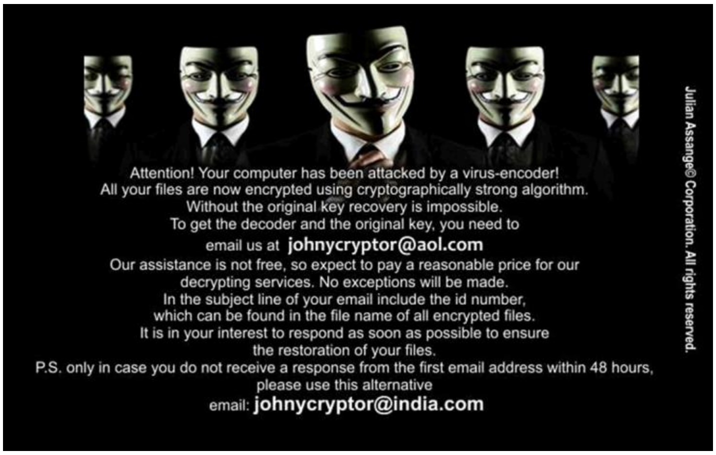
Spear Phishing $35,000

- Financial Controller receives an email from the MD
- Requests transfer of funds $35,000
- Grammar slightly different
- Checks with MD by phone
- Investigation shows that email address used was compromised in LinkedIn hack in 2012.



Ransomware

- Engaged in a matter where the network has been encrypted and there is a 'dispute' taking place between the business and the IT outsourcers.

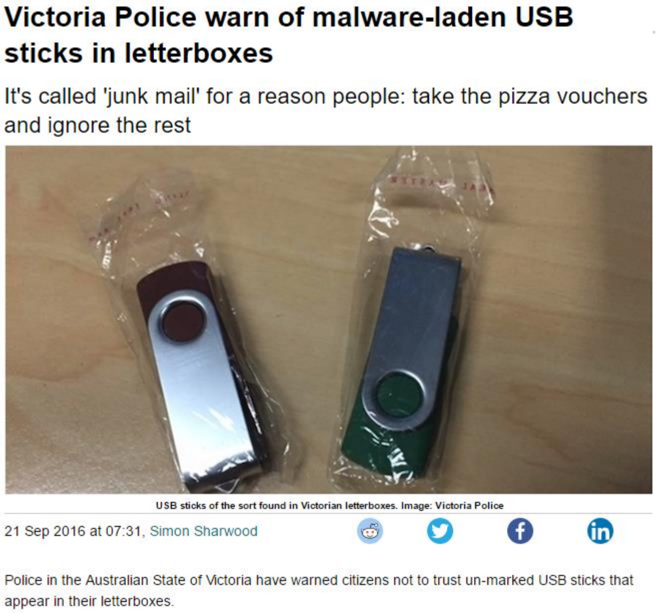


Attention! Your computer has been attacked by a virus-encoder!
All your files are now encrypted using cryptographically strong algorithm.
Without the original key recovery is impossible.
To get the decoder and the original key, you need to
email us at **johnycryptor@aol.com**
Our assistance is not free, so expect to pay a reasonable price for our
decrypting services. No exceptions will be made.
In the subject line of your email include the id number,
which can be found in the file name of all encrypted files.
It is in your interest to respond as soon as possible to ensure
the restoration of your files.
P.S. only in case you do not receive a response from the first email address within 48 hours,
please use this alternative
email: **johnycryptor@india.com**

Julian Assange© Corporation. All rights reserved.

Educating Staff

- Phishing education software
- Security education
- Training employees on identifying spoofed emails
- How to respond/report
- Testing ongoing through internal phishing campaign



Victoria Police warn of malware-laden USB sticks in letterboxes

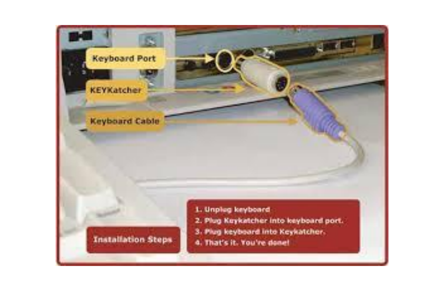
It's called 'junk mail' for a reason people: take the pizza vouchers and ignore the rest

USB sticks of the sort found in Victorian letterboxes. Image: Victoria Police

21 Sep 2016 at 07:31, Simon Sharwood

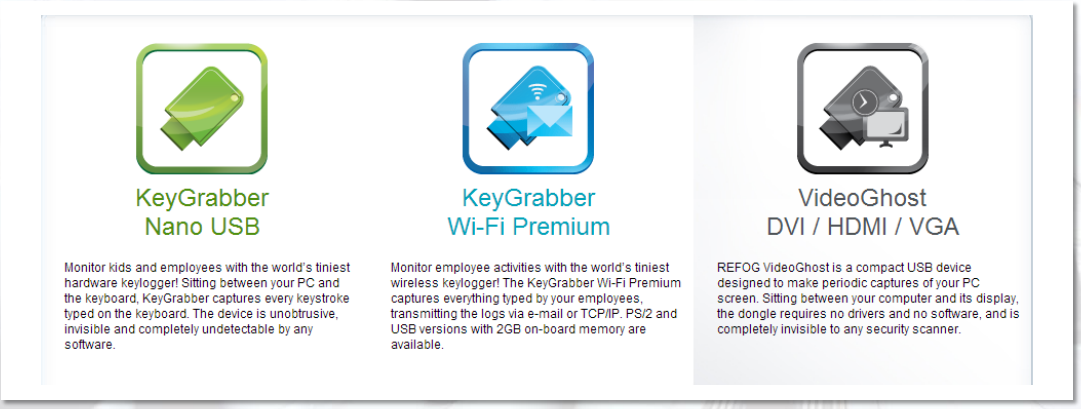
Police in the Australian State of Victoria have warned citizens not to trust un-marked USB sticks that appear in their letterboxes.

Key Logging (Computer Monitoring)



Installation Steps

1. Unplug keyboard
2. Plug Keykatcher into keyboard port.
3. Plug keyboard into Keykatcher.
4. That's it. You're done!



KeyGrabber Nano USB

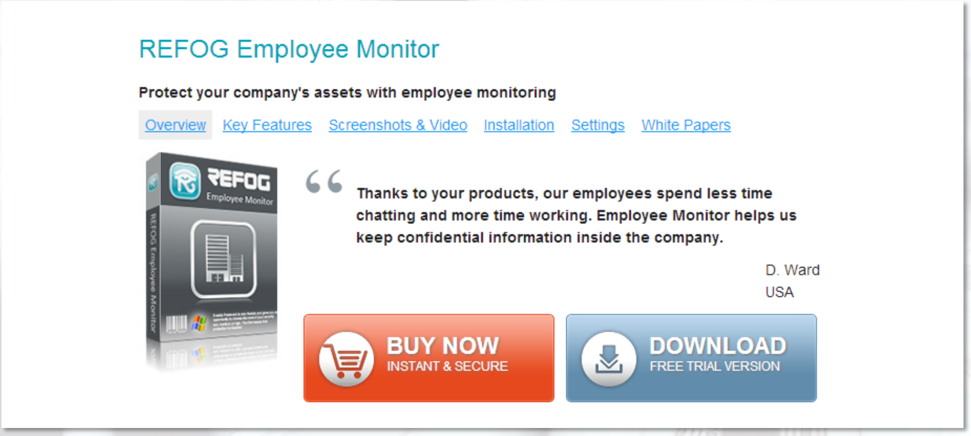
Monitor kids and employees with the world's tiniest hardware keylogger! Sitting between your PC and the keyboard, KeyGrabber captures every keystroke typed on the keyboard. The device is unobtrusive, invisible and completely undetectable by any software.

KeyGrabber Wi-Fi Premium

Monitor employee activities with the world's tiniest wireless keylogger! The KeyGrabber Wi-Fi Premium captures everything typed by your employees, transmitting the logs via e-mail or TCP/IP. PS/2 and USB versions with 2GB on-board memory are available.

VideoGhost DVI / HDMI / VGA

REFOG VideoGhost is a compact USB device designed to make periodic captures of your PC screen. Sitting between your computer and its display, the dongle requires no drivers and no software, and is completely invisible to any security scanner.



REFOG Employee Monitor

Protect your company's assets with employee monitoring

> Thanks to your products, our employees spend less time chatting and more time working. Employee Monitor helps us keep confidential information inside the company.
>
> D. Ward
> USA

Key Logging - Software

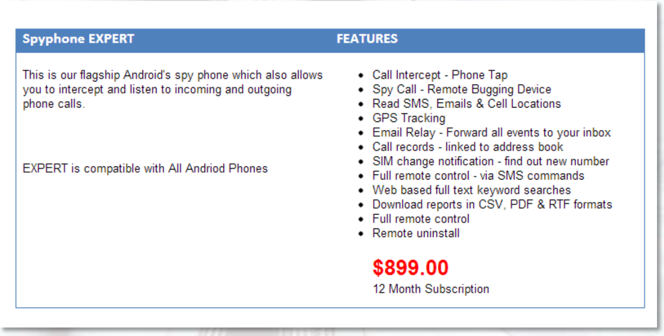
Smartphone Spy App

Wonder where your kids went last night? Can't reach them by the phone? Learn where your kids are (and were) with Hoverwatch Cell Phone Spy! Hoverwatch is meant to help you protect and supervise your kids, giving you the ability to track their location, discover their daily routes, listen to their calls and read their text messages.

Protect and Supervise Your Kids

Cell Spy is made to help you supervise your kids, turning their Android phone into a spying device. With this program, you'll always stand behind their back and know when they need your help or protection. Cell Spy will constantly track their location recording their every step, and watch closely who they speak with and what they talk about.

Android Phones



Spyphone EXPERT

This is our flagship Android's spy phone which also allows you to intercept and listen to incoming and outgoing phone calls.

EXPERT is compatible with All Andriod Phones

FEATURES

- Call Intercept - Phone Tap
- Spy Call - Remote Bugging Device
- Read SMS, Emails & Cell Locations
- GPS Tracking
- Email Relay - Forward all events to your inbox
- Call records - linked to address book
- SIM change notification - find out new number
- Full remote control - via SMS commands
- Web based full text keyword searches
- Download reports in CSV, PDF & RTF formats
- Full remote control
- Remote uninstall

$899.00
12 Month Subscription

Stupid is as stupid does. No 1

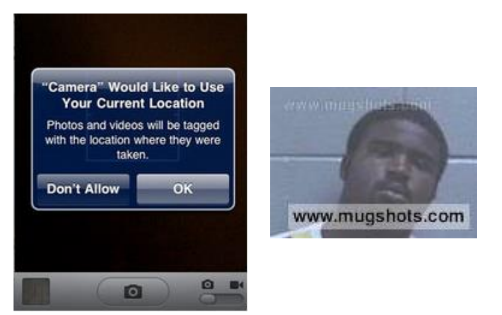
Theft suspect found and arrested after using stolen iPhone with geotagging

A man who took photos of himself holding a stolen iPhone then attempted to email them to friends using the stolen phone was arrested after the phone's owner found the photos on her email account.

Police arrested Marquise Tyronne Smith, 18, of Rialt0, Friday morning.

The owner of an iPhone stolen during an armed robbery a week earlier found pictures of Smith with her phone in her "sent" email folder. Smith had apparently attempted to email the pictures from the victim's account, which was connected to the phone.

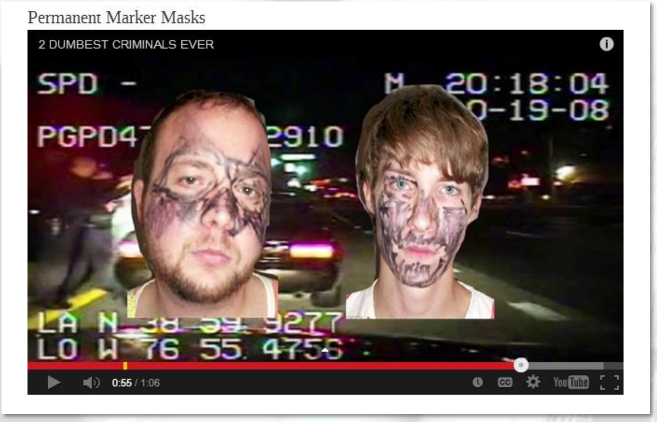
The iPhone's geo-tagging feature pinpointed the location where the photos were taken, leading investigators to Smith's address.



"Camera" Would Like to Use Your Current Location

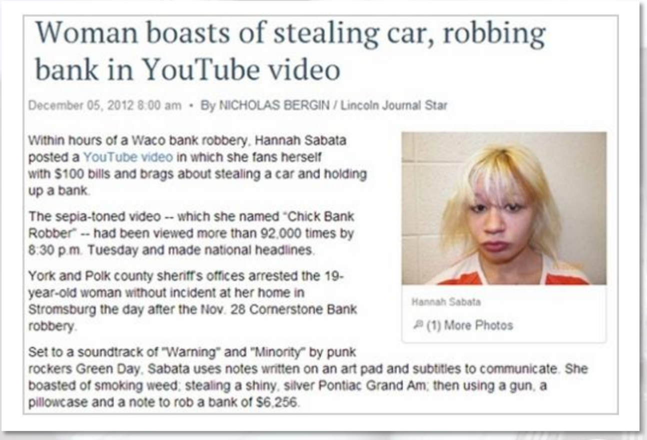
Photos and videos will be tagged with the location where they were taken.

Stupid is as stupid does. No 2



Permanent Marker Masks

Stupid is as stupid does. No 3



Woman boasts of stealing car, robbing bank in YouTube video

December 05, 2012 8:00 am • By NICHOLAS BERGIN / Lincoln Journal Star

Within hours of a Waco bank robbery, Hannah Sabata posted a YouTube video in which she fans herself with $100 bills and brags about stealing a car and holding up a bank.

The sepia-toned video -- which she named "Chick Bank Robber" -- had been viewed more than 92,000 times by 8:30 p.m. Tuesday and made national headlines.

York and Polk county sheriff's offices arrested the 19-year-old woman without incident at her home in Stromsburg the day after the Nov. 28 Cornerstone Bank robbery.

Hannah Sabata

(1) More Photos

Set to a soundtrack of "Warning" and "Minority" by punk rockers Green Day, Sabata uses notes written on an art pad and subtitles to communicate. She boasted of smoking weed; stealing a shiny, silver Pontiac Grand Am; then using a gun, a pillowcase and a note to rob a bank of $6,256.

Takeaway: Manage your Environment

- Backups
- Segregation of data based on role etc
- Monitor what's happening on the systems (Carbon Black etc)
- Retention of deleted email
- Staff departure process
- Regular security audit
- Educate your employees

NATIONAL CONGRESS

23 – 25 NOVEMBER 2016

GRAND HYATT MELBOURNE

IPA INSTITUTE OF PUBLIC ACCOUNTANTS

THANK YOU

for joining us

Reckon