

UNCLASSIFIED



AFP

AUSTRALIAN FEDERAL POLICE

Cybercrime Operations

AIPI Meeting - 19 August 2016

Federal Agent Scott MELLIS



UNCLASSIFIED

Federal Agent Scott Mellis

- Started in AFP Computer Crime in 1995
- Current Team Leader of AFP Cybercrime Operations in Melbourne
- Former Team Leader of Cybercrime Intelligence in Australian High Tech Crime Centre in Canberra
- 13 years in Cybercrime

Impact?

“The global cost of cybercrime is greater than the combined effect on the global economy of trafficking in marijuana, heroin and cocaine... the straight-up financial costs of cyber attacks worldwide at \$114bn, with time lost dealing with the crime adding the remaining \$274bn, while the global black market in the three drugs costs \$288bn”

Norton Cybercrime Report - September 2011

UNCLASSIFIED

"...the likely annual cost of cybercrime to the global economy is more than 400 billion dollars."

Mark Rutte, Prime Minister of The Netherlands – April 2015

UNCLASSIFIED

"Cyber threat is one of the most serious economic and national security challenges American faces as a nation...America's economic prosperity in the 21st century depends on cyber security."

US President Barack Obama

The truth!

**Cybercrime is mainstream
crime....**

NOT unusual

NOT the exception

NOT niche

UNCLASSIFIED

What I am talking about?

- Our role
- Evolution
- Case studies
- Current trends



UNCLASSIFIED

The Internet is a headache

- Ease of access
- Lack of regulation
- Global audience
- Anonymous
- Instantaneous
- Deniable



What **is** Cybercrime?

- Denial of Service Attacks
- Hacking (unauthorised access, modification, impairment)
- Possessing malware with intent
- Deploying malicious software (malware)

What **isn't** Cybercrime?

- Selling drugs/guns online
- Sending threatening emails
- Running online scams (i.e romance scams)
- Cyber bullying
- Cyber stalking

Evolution

2006

- Locals compromising/impairing local systems

2016

- Overseas organised crime groups compromising systems worldwide with sophisticated malware

Desirable outcomes?

- Prosecution
- Disruption
- Mitigation
- Prevention
- Diversion
- Displacement



Our key partners

- CERT Australia
- *White hat* hacking groups
- ACMA
- Private security researchers
- NCFTA Pittsburgh USA
- FBI Cyber Division



Five Cybercrime Teams

- Canberra x 2
- Canberra (ACSC)
- Sydney
- Melbourne
 - The teams, until recently, had different remits because of differing skill sets
 - Locations reflect need for victim liaison

UNCLASSIFIED

Case studies

Operation Cappella

- In 2009 posts found online in carding forum revealing sextortion of 13yo.
- Communications resolved to POI in Brisbane
- Monitoring of POI online activities instigated
- Search warrant executed, suspect arrested
- Technically difficult case
- Trial in 2013, unique defences raised
- Convicted and sentenced to 12 years to serve 6 years

UNCLASSIFIED

Operation Cappella

Online predator Luan Muharrem Tahiraj sentenced to 12 years' jail for grooming lonely teen

RENEE VIELLARIS LEGAL AFFAIRS THE COURIER-MAIL AUGUST 21, 2013 12:00AM

SHARE



SAVE THIS STORY



FOR THE FIRST 12 WEEKS, CONDITIONS

Can
THE

SCRATCH

Citadel

- Late 2012/early 2013 C2 server in Melbourne
- *Citadel* malware (Zeus variant) campaign
- Monitoring of C2 commenced
- Supporting IT infrastructure located in Germany, NZ, US
- A\$587 million in valid Australian bank account/credit card credentials seized
- Russian based gang identified

Operation Trove

- Worldwide IRC network trading stolen credit card credentials, many Australian
- Node identified in Perth, then Canberra
- Node moves to Vietnam, so we followed
- Vietnam Police conduct investigation
- Data fast tracked to AFP for analysis
- A\$88 million in valid Australian credit card credentials identified and shut down

Gameover Zeus (GOZ)

- Sophisticated P2P malware from Russia
- AFP received briefings in 2013 in Pittsburgh
- Vulnerability found in GOZ in early 2014
- Asked AFP to help
- Consultation over several months with ISPs
- Global takedown on 29/30 May 2014
- Most Australian infected PCs were disinfected

UNCLASSIFIED

NEWS 

LOCATION:  Melbourne, Vic [Change](#)

[Home](#) [Just In](#) [Australia](#) [World](#) [Business](#) [Sport](#) [Analysis & Opinion](#) [Fact Check](#) [Programs](#)

[Print](#) [Email](#) [Facebook](#) [Twitter](#) [More](#)

Cyber scams Gameover Zeus, Cryptolocker dismantled; AFP helps crush botnet over theft of \$100m

By North America correspondent [Lisa Millar](#), wires
Updated 3 Jun 2014, 11:56am

The Australian Federal Police (AFP) has helped the United States and 10 other countries dismantle a global computer hacker network that used a sophisticated computer virus to steal more than \$100 million from companies and consumers.

Gameover Zeus, which first appeared in September 2011, stole bank information and other confidential details from victims, the US Justice Department said.

RELATED STORY: [Hackers break into eBay database, steal customer data](#)

RELATED STORY: [Chinese companies in hacking row 'have Australian links'](#)

MAP: [United States](#)

What's good about working in Cybercrime?

- Challenging work
- Good networking
- Upskilling/personal development
- Travel



What's bad?

- Don't get out much!
- Challenging/frustrating
- Non-traditional policing
- Nature of the work is often misunderstood
- Outcomes of work are often misunderstood



Current Cybercrime trends

- Business Email Compromise
- Attacks on non-traditional financial platforms (superannuation, payroll)
- Unprecedented cashout levels via money mules
- Ransomware
- State based intrusion



UNCLASSIFIED

Tips when investigating Cybercrime

- Preservation, preservation
- Data integrity
- Networking
- Don't assume anything, it's Cybercrime!



UNCLASSIFIED

BRINGING CIVILIZATION TO ITS KNEES...

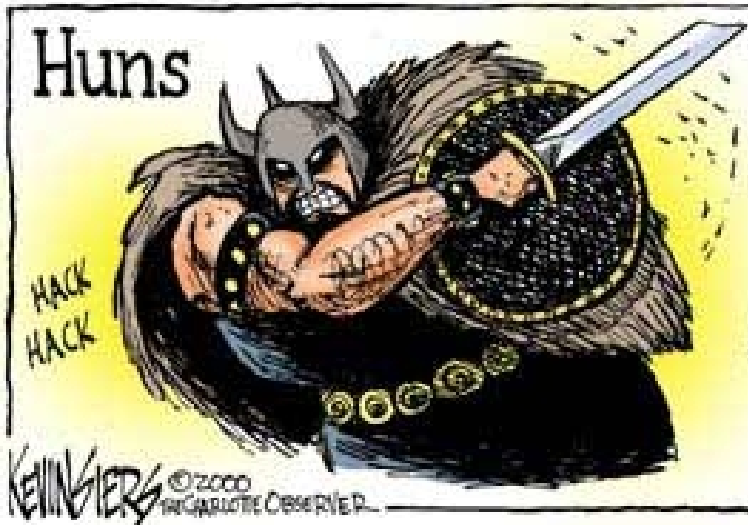
Goths



Vandals



Huns



Geeks



UNCLASSIFIED



AFP

AUSTRALIAN FEDERAL POLICE

