Identity Theft - Australian Response

Jamie Gillespie
jamie@auscert.org.au
Senior Security Analyst, AusCERT

Overview

• Scope of Identity Theft in Australia
• AusCERT’s Role
  – Local IR
  – International IR
  – Analysis
• Response Procedures
• Trends (Present and Future)
Scope of Australian ID theft

- **Primary instances:**
  - Target: Financial Institutions
  - Methods: Phishing web sites and Trojan malware
  - Perpetrators: evidence to suggest non-Australian based organised crime

- Other (incl. Government) systems have been “collateral damage” in attacks targeting financial institutions

- Smaller local incidents of identity theft

- Evidence of more targeted attacks against Australian (and other) government sites
Scope of Australian ID Theft

- centrelink.gov.au
  - Government social services
- ebay.com.au
- etradeaustralia.com.au
- gu.edu.au
  - University
- iinet.net.au
  - ISP
- melbourneit.com.au
- myob.com.au
- optusnet.com.au
- qantas.com.au
  - Airline
- sa.gov.au
- thrifty.com.au
  - Car rental company

- .gov.au
- .gov.uk
- .gov
- .mil

- “Question for seller”
- 8.7 MB of text
- Bitmap screenshots
- 1652 unique IP addresses
- 1130 domains

- Not just the banks...

Scope of Australian ID Theft

**Tsunami Trojan: Infections and Logging**

![Diagram showing data logged and Tsunami Trojan infections over time]
AusCERT’s Role: Local

- Local response arrangements
  - Strong co-operation with the Australian High Tech Crime Centre (AHTCC)
  - Banking and Financial Sector information sharing and threat/incident analysis
  - AusCERT members and the general public
  - Australian ISPs
  - Local law enforcement mailing lists (local forensics groups)

AusCERT’s Role: International

- APCERT teams – excellent assistance in the rapid closure of sites within their constituencies
- CERTs, AV vendors and other security researches providing reverse engineering and analysis
- CERT.br (Brazil) – future trends due to advanced local ID theft
- Other national CERTs assisting with site closure
AusCERT’s Role: International

- APACS and BFK – sharing incident response with AusCERT enabling (limited) 24 hour coverage
- Closed mailing lists: APWG, FIRST, APCERT, AVIEN, others
- ISPs and registrars (e.g. YesNIC)

AusCERT’s Role: Analysis

- Analysis
  - Mailing lists to share information and intelligence between banks and AusCERT
  - Crime survey
  - Threat analysis
  - Monitoring vulnerabilities, PoCs and exploit activity
Response Procedures

Evil Scammer → AusCERT CC Team

Scam Reporter → AusCERT CC Team
- Aus Bank
- UK Bank
- All Bank

Trawlinator Troj-O-Matic → Web Report Scanner

Incident Created!

Banking Reporter → Phishing Report Form
- Trojan Report Form

Offending Website → Scamalizer

DNS/Whois and Contacts

AHTCC Template

APACS Template

Virus-Submit Template

Local CERT Template

ISP/Registrant Template

AusCERT CC Team → Local CERT

Copyright © 2005 AusCERT
Questions or comments?