AusCERT
Australian Computer Emergency Response Team

Trends in Malware Enabled Identity Theft

Matthew McGlashan -
matthew@auscert.org.au
Computer Security Analyst, AusCERT

Outline

AusCERT
Australian Computer Emergency Response Team

- About AusCERT
- What AusCERT is doing to combat ID theft
- The Threat: Trojan Horse software
- Timelines: 2004 and 2005
- Hooks and Lures
- Installation
- Exploit timeline
- Logging: methods, trends, data, examples
- Recent developments
- Future directions
- Internal operational processes
- Operational response results
- Questions

About AusCERT

AusCERT
Australian Computer Emergency Response Team

- Australia's national CERT
  - Collect, monitor, advise on threats and vulnerabilities
  - Incident response coordination and assistance
- Independent, university-based, non-government
- Not-for-profit – revenue from service contracts and member subscriptions
- Chair of APCERT
- Close collaboration with the AHTCC
- Close collaboration with APACS
- "Other" collaborations (eg other CERTs)

AusCERT v ID Theft

AusCERT
Australian Computer Emergency Response Team

- Monitor threats, vulnerabilities, detect incidents
- Coordinate IR with UK and Germany
- Procedures to prioritise actions per AHTCC/AusCERT strategy
- Incident response:
  - closed hundreds of sites
  - submitted over 40 virus sample to AV vendors in 2004
- Request artefacts and logs to investigate impact
- Provided technical and threat analysis
- Encouraging analysis, information sharing between Australia, UK and Germany

AusCERT v ID Theft

AusCERT
Australian Computer Emergency Response Team

By arrangement with AHTCC, AusCERT is the central reporting point of contact in Australia for reporting incidents of on-line identity theft in the banking and finance sector (BFS)

- Provide first-line response to incidents of on-line identity theft:
  - Through CERT network, seek closure of sites overseas and retrieval of artefacts, logs
- Provide technical analysis of artefacts, techniques, trends to AHTCC and banks
- Issue alerts about new threats/vulnerabilities regarding on-line identity theft

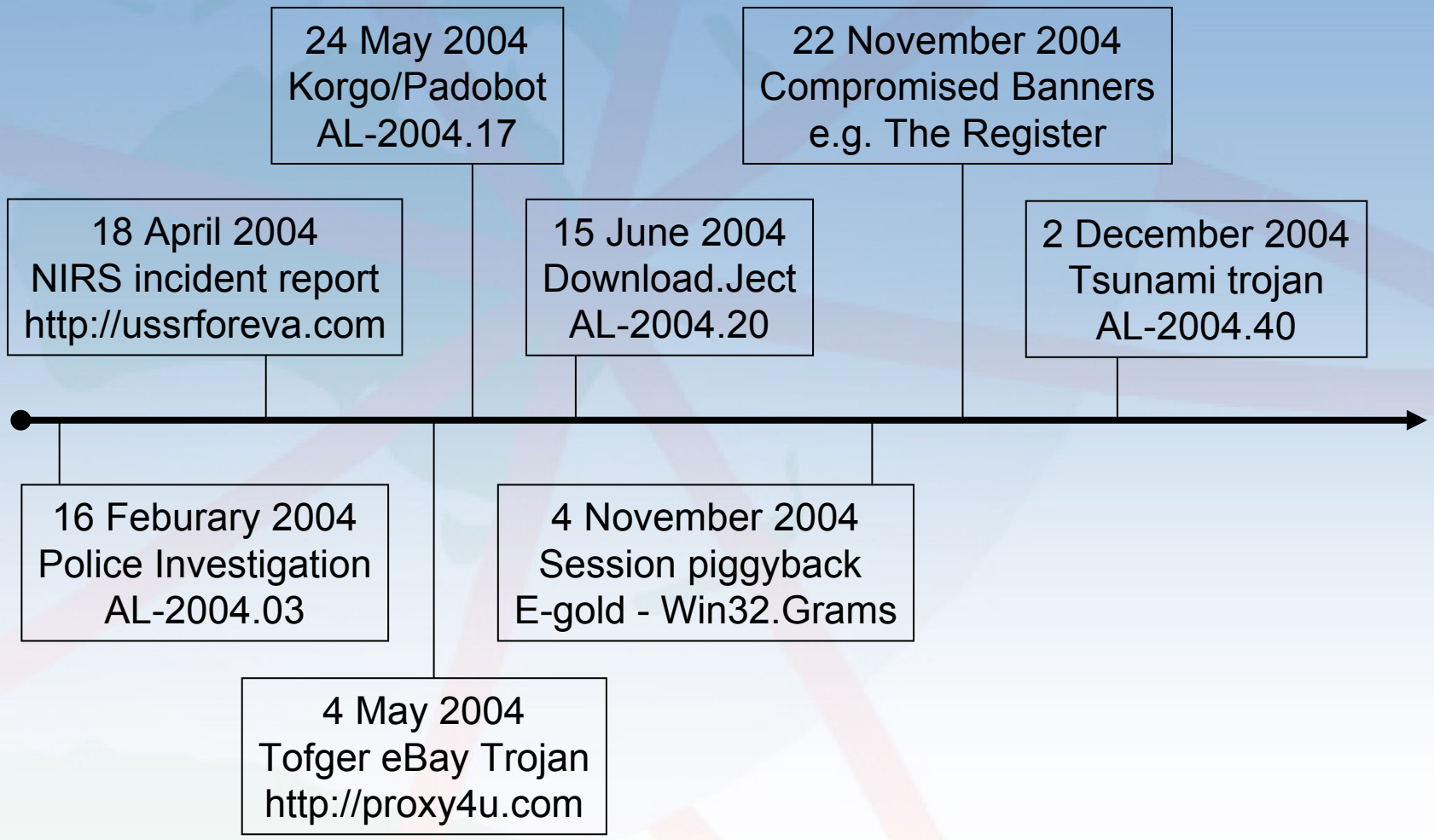
Trojan Horses

AusCERT
Australian Computer Emergency Response Team

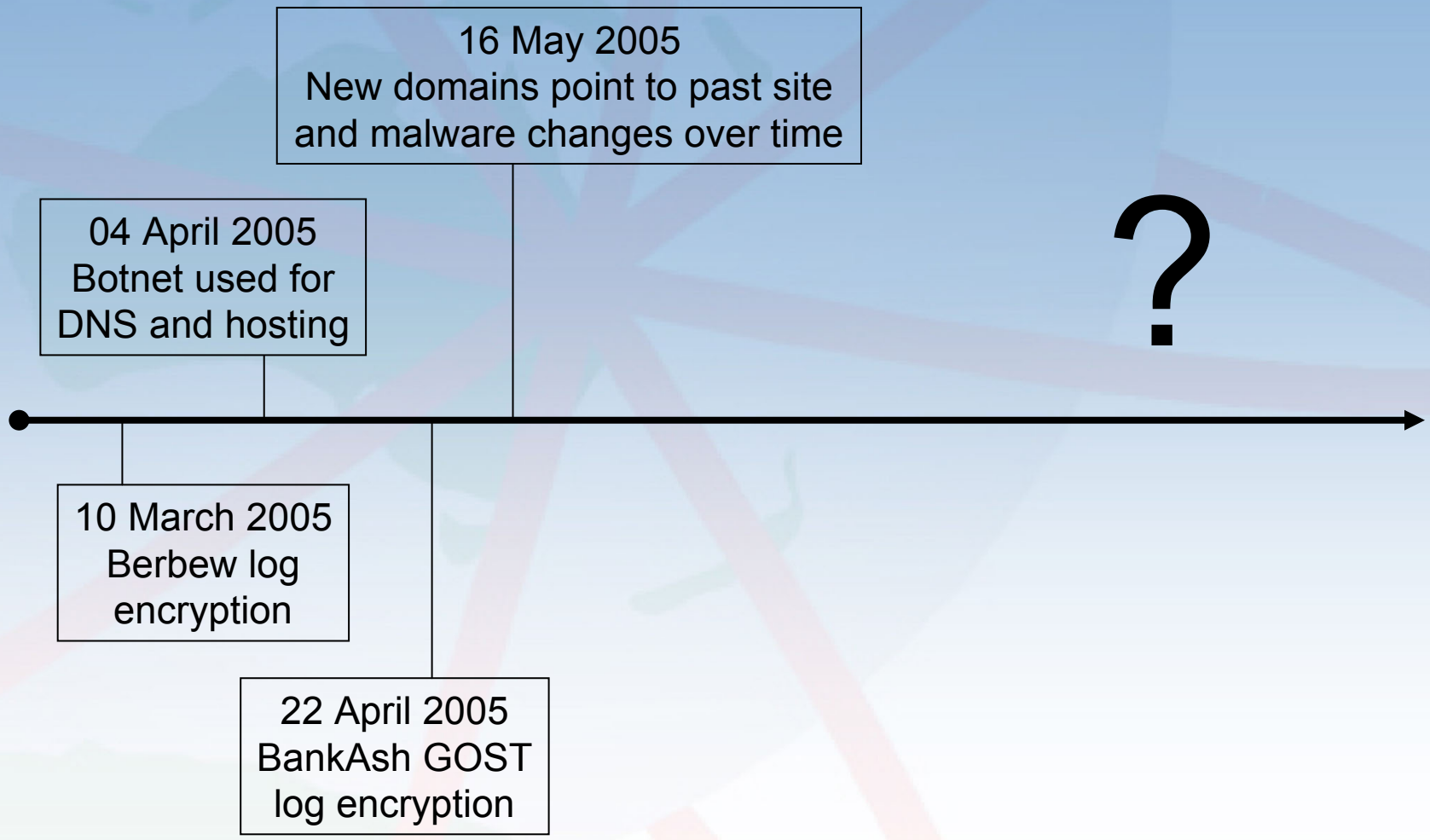
- Attackers motivation: financial gain
- Method:
  - Compromise online banking credentials
    - “Phishing” (fraudulent web sites) since 2003
    - DNS corruption (“Pharming”)
    - Trojan horse software - early 2004
  - Move money from compromised accounts to “mules”
  - Mules take a cut and transfer the rest overseas via Western Union
- Why are Trojans effective? ….

Timeline 2004

AusCERT
Australian Computer Emergency Response Team



Timeline 2005



Hooks

AusCERT
Australian Computer Emergency Response Team

- Spam
  - Hard to detect and rarely reported
  - No malicious code, but URLs to malicious sites
  - Unrelated to the targeted institution
- Variations on spamming
  - Posts to bulletin boards
  - Instant messaging
- Other
  - Padobot (aka: Korgo) – LSASS vulnerability
  - Download.Ject – Vulnerable IIS serving berbew
  - Compromised banner ads (e.g. The Register)
  - Cross site scripting

Lures

AusCERT
Australian Computer Emergency Response Team

- Spam – social engineering:
  - June 04 and prior: “RE: Question for seller -- Item #845269116”
  - Aug 04: “Act of terrorism at The Opening Ceremony of the ATHENS 2004 Olympic Games”
  - Aug 04: “Customerhelpcentre, Your ID was stolen” d-reports.org
  - Sep 04: “Osama Found Hanged”
  - Sep 04: “George Bush sniper-rifle shot!”
  - Nov 04: “Huge ocean wave!” http://www.tsunamidanger.com
  - Feb 05: “I sent Sent You an E-Card From AOL E-Cards powered by BlueMountainCards.com.au”
  - Mar 05: “SENSATION! It's happened again! White house orgie!”
  - May 05: “You've been sent money”

Installation

AusCERT
Australian Computer Emergency Response Team

- Browser (IE particularly based) exploits
  - IFrame vulnerability
  - Drag and Drop vulnerabilities
  - ITS protocol handlers and CHM
  - Java classloader vulnerability
  - plus others…
- Weak browser settings
- Pure social engineering
  - “Update your windows machine” (AL-2005.07)
  - “Pick up sticks” game
  - “Paypal Safety Bar”

Browser Exploit

AusCERT
Australian Computer Emergency Response Team

- Example: “Drag and Drop” Vulnerability (CAN-2004-0839)
  - 19 Aug 2004: Initial post to Full Disclosure by “http-equiv”
  - 24 Aug 2004: More effective POC released by “mikx”
  - 24 Aug 2004: AL-2004.024 released by AusCERT
  - 31 Aug 2004: Akak Trojan, analysis by LURHQ
  - 07 Sep 2004: AusCERT Incident report, active exploitation for financial fraud
  - 12 Oct 2004: Patch released by Microsoft
  - 19 Oct 2004: A variation of this vulnerability not fixed by the patch posted to Full Disclosure by “http-equiv”

Logging Methods

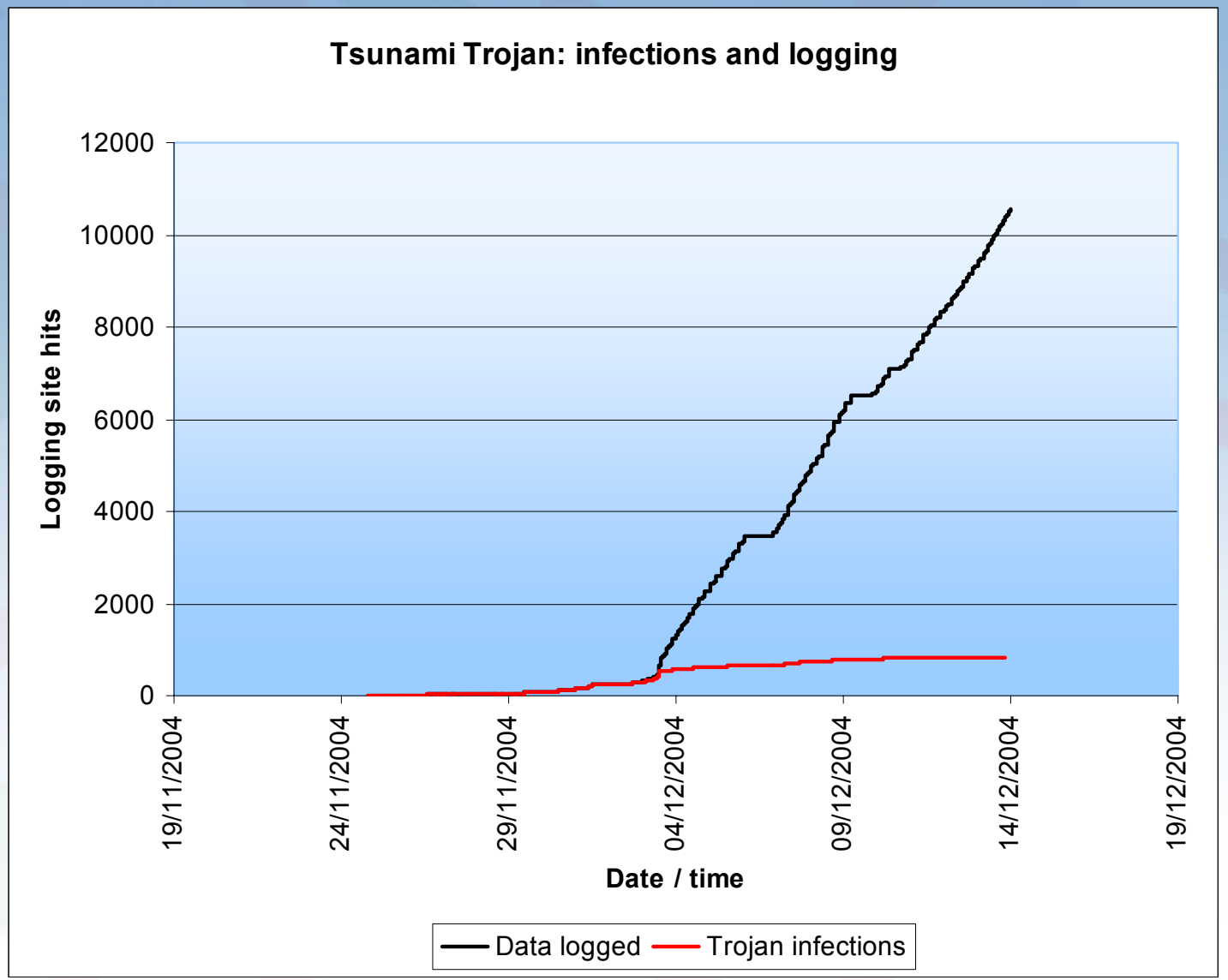
AusCERT
Australian Computer Emergency Response Team

- Three main methods:
  - HTTP: posting via php forms
  - FTP: username/password encoded into the trojan
  - Email: Sending email to a hard coded email address

- In the majority of networks, this traffic would be considered OK unless there was content inspection.

Logging Trends

AusCERT
Australian Computer Emergency Response Team



Logged Data

AusCERT
Australian Computer Emergency Response Team

- centrelink.gov.au
- ebay.com.au
- etradeaustralia.com.au
- gu.edu.au
- iinet.net.au
- melbourneit.com.au
- myob.com.au
- optusnet.com.au
- qantas.com.au
- sa.gov.au
- thrifty.com.au

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

- “Question for seller”
- 8.7 Gb of text
- Bitmap screenshots
- 1652 unique IPs
- 1130 domains

- **Not just the banks…**

Logging Example

AusCERT
Australian Computer Emergency Response Team

- **The following slides show data from a recent incident: TrojanSpy.Win32.Banker.jj**

UID: {3C24AAB7-F462-4472-BD0B-AAAAAAAAAAAA}
IP: x.x.220.245
Country: United Kingdom
Language: English
OS: Windows 2000 Service Pack 3 (Build 2195)
IE: Internet Explorer 5.01 SP3 (Windows 2000 SP3 only)

Installed apps:
…
Windows 2000 Hotfix - KB823980, version: 20030705.101654
LiveReg (Symantec Corporation), version: 2.2.5.1678
LiveUpdate 2.6 (Symantec Corporation), version: 2.6.14.0
Spybot - Search & Destroy 1.3, version: 1.3
Norton Internet Security, version: 6.0.2.0
…

Active processes:
…
\SystemRoot\System32\smss.exe
C:\WINNT\system32\services.exe
C:\WINNT\system32\spoolsv.exe
C:\Program Files\Common Files\Symantec Shared\ccEvtMgr.exe
C:\Program Files\Norton Internet Security\NISUM.EXE
C:\Program Files\Norton Internet Security\ccPxySvc.exe
C:\WINNT\Explorer.EXE
C:\WINNT\process.exe
…
--
Created on Monday 14th of February 2005 07:58:42 AM

Logging Example

AusCERT
Australian Computer Emergency Response Team

-- Saved Forms --

URL (Form): http://lc1.law13.hotmail.passport.com/cgi-bin/login
User/Pass: <username>:

URL (Form): http://signin.ebay.co.uk/aw-cgi/eBayISAPI.dll
User/Pass: <username>:<password> (Modified: 09/07/2004 14:00)

URL (Form): http://webmail.businessserve.co.uk/index.php
User/Pass: <username>:<password> (Modified: 16/06/2004 16:42)

URL (Form): http://www.viewdata.net/login.asp
User/Pass: <username>:<password> (Modified: 19/01/2004 12:07)
User/Pass: <username>:<password> (Modified: 19/01/2004 12:07)

-- Outlook Passwords --

SMTP Email Address: sales@<domain>.co.uk
POP3 User Name: <username>
POP3 Password2: <password>
POP3 Server: pop.businessserve.co.uk

Logging Example

AusCERT
Australian Computer Emergency Response Team

(!) URL: https://online.lloydstsb.co.uk/logon.ibc

Form action: https://online.lloydstsb.co.uk/logon.ibc
Form method: post
Java (hidden): On
Key (hidden): 01-000001111111177471100000000000
LOGONPAGE (hidden): LOGONPAGE
UserId1 (text): <username>
Password (password): <password>

Recent Developments

AusCERT
Australian Computer Emergency Response Team

- Increase in the number of organisations targeted
- Domain names and hosting:
  - Several domain names registered, multiple IP changes as ISPs respond
  - Botnets used to host phishing sites so the host serving the site changes every 30 minutes
- Captured account details
  - Encoding and private key encryption
  - More detailed, better organised and compressed
- Malware:
  - Root-kit techniques for hiding presence
  - Session piggybacking (e-gold Win32.Grams / GETGOLD.A)
  - Downloadable (dynamic) configuration

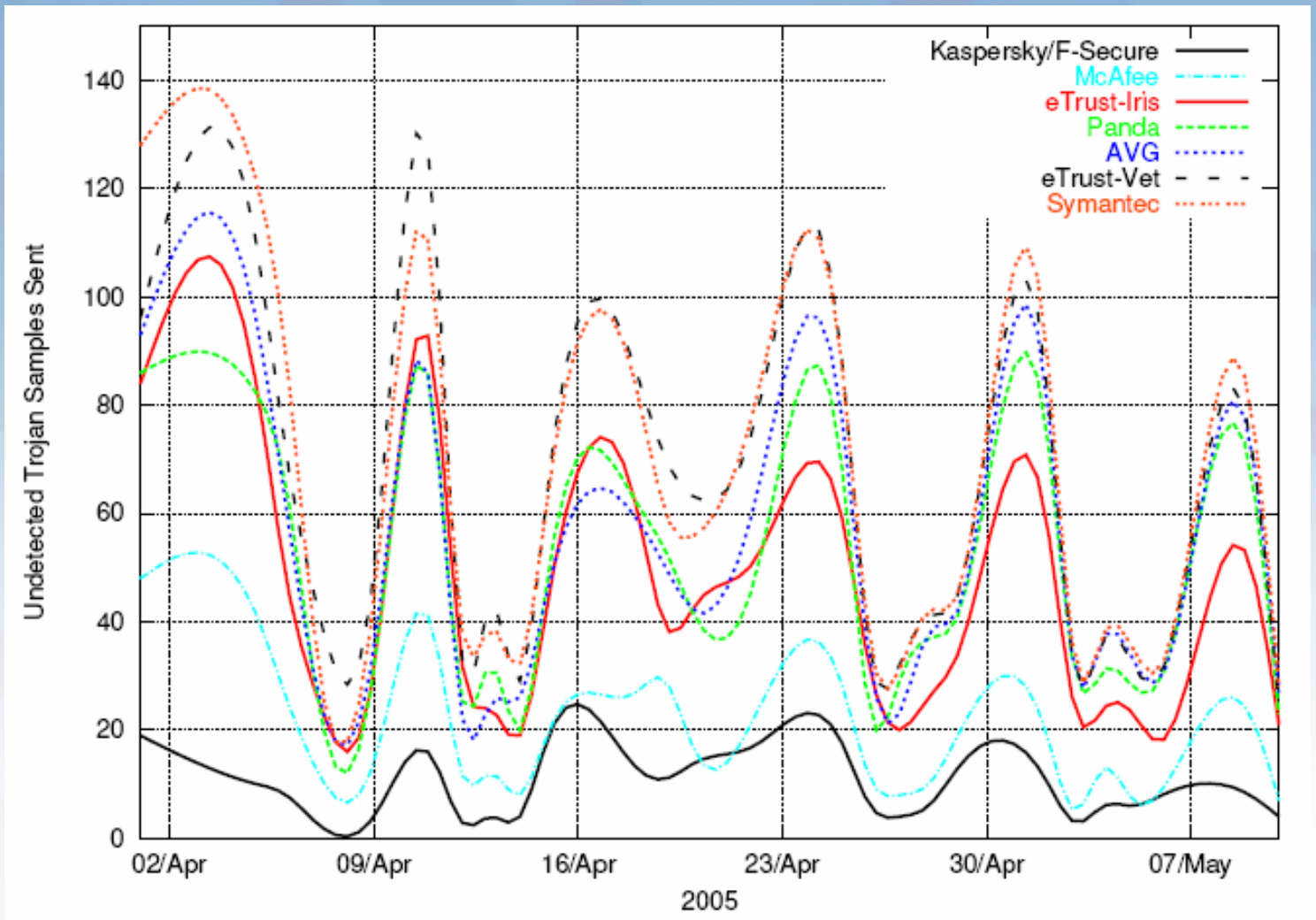
Future Directions

AusCERT
Australian Computer Emergency Response Team

- Domain names and hosting:
  - Botnets for hosting, as for phishing
  - Exploits of browsers other than Internet Explorer
- Captured account details
  - Strong (public key) encryption
- Malware:
  - More root-kit technology
  - Binary armouring, obfuscation and other anti-analysis techniques
  - Session piggybacking for other organisations. Subverting 2 factor authentication
  - Improved and encrypted dynamic configuration and updates

Future Directions

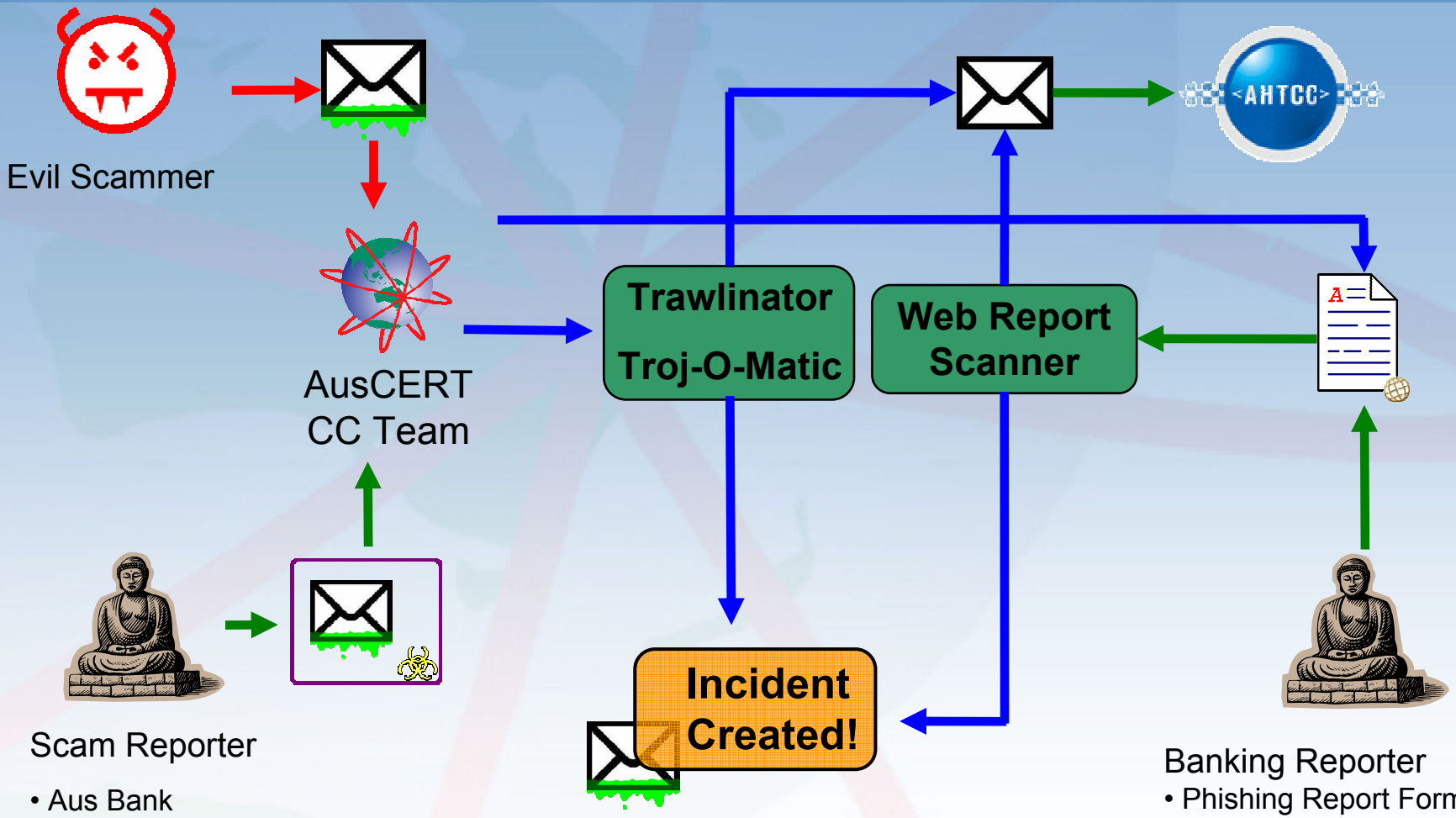
AusCERT
Australian Computer Emergency Response Team



Source: NBSO - NIC BR Security Office - Brazilian Computer Emergency Response Team

Internal Operational Processes

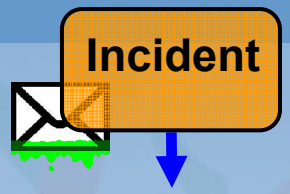
AusCERT
Australian Computer Emergency Response Team



Internal Operational Processes

AusCERT
Australian Computer Emergency Response Team

DNS/WHOIS
and Contacts



Scamalizer

Offending
Website

AHTCC Template | APACS Template | Virus-Submit Template | Local CERT Template | ISP/Registrant Template

AusCERT
CC Team

Virus-Submit

APACS

Local CERT

ISP/Registrant

Internal Operational Processes

AusCERT
Australian Computer Emergency Response Team

```
matthew@app <~> url_report
2005-05-13, beginning
2005-05-19, end
Check http://mywebpage.netscape.com/fotos110bbb5/fotos.exe...
Check http://313731.com/humortadela.scr...
...

AusCERT banking fraud reports, Fri May 13 2005 to Thu May 19 2005
================================================================
Report for 19/05/2005
=====================
AUSCERT#20059ab75
    Reported:           Thu May 19 11:00:34 2005
    Type:               trojans
    Org:                not_selected
    Subject:            Você recebeu uma piada animada do Humortadela
    URL:                http://313731.com/humortadela.scr
    Incident status:    not_looked_at
    HTTP Status:        200
    Title:

...
```

Operational Response Results

AusCERT
Australian Computer Emergency Response Team

Developed capability to analyse and respond to incidents and share information

Allowed

- Better coordination of IR (better use of scare resources)
  - Incident tracking numbers - better coordination and less duplication
  - Procedures in place to follow most appropriate course of action, in order of priority
  - We have helped close down around 100 sites, collect artefacts and logs to allow post-incident investigation to occur.

Operational Response Results

AusCERT
Australian Computer Emergency Response Team

Allowed

- Sharing of information and analysis
  - aus_bank, uk_bank, all_bank mailing lists managed by AusCERT and used by authorised Aus and UK banks
  - Other written assessments produced by AusCERT on restricted access basis
  - virus-submit and virus-submit-reply mailing lists
  - Contribute and benefit from other related projects eg Darknet, ISI, Honeynet, various sensor networks
  - Antiphishing Working Group, AVIEN, other closed lists
- Provides technical analysis for the benefit of the AHTCC investigations

Questions

AusCERT
Australian Computer Emergency Response Team

Questions or comments ?

Matthew McGlashan
matthew@auscert.org.au
Computer Security Analyst

AusCERT - www.auscert.org.au
auscert@auscert.org.au