# The Snooping Dragon – Social-malware Surveillance of the Tibetan Movement

Shishir Nagaraja
(University of Illiinois at Urbana-Champaign)

Ross Anderson
(Computer Lab, Cambridge University)

# Case study – the Office of His Holiness the Dalai Lama (OHHDL)

- Several dozen people, mostly monks, support his political / religious activity
- Simple attacks reported since early 2007 – from directed spam to simple targeted stuff
- Things seemed to get worse from July 2008 (the run-up to the Peking Olympics)
- Manifest security failure led to our being called in September 2008

# Computing infrastructure

- ‘Unclassified, ‘Confidential’ and ‘Secret’ material, if NATO rules had been applied
- A web server – mostly for publishing talks by His Holiness
- A linux-based email server – 50 or so accounts
- Filesystems holding project and meeting documents – schools, community halls
- A refugee database on a Windows machine (now disconnected from the network)

# Attack vector

- Hijack social trust
  - Steal an email with an attachment
  - Embed malware in the attachment
  - Resend the email to the target
- Initial break not clear
  - Probably social malware constructed with public information
  - Not enough unsuccessful log entries for a dictionary attack
  - A much smaller number of successful log entries from IP addresses in China

# Sample subverted email

Subject: Kalon Tripa Succession
From: "Pema Rinzin" <prinzintibet@yahoo.com>
Date: Thu, September 18, 2008 8:14 am
To: choejor@dalailama.com

---

Dear Sir,

Attached please find the final Tibetan translation of my English announcement for the Kalon Tripa succession initiative. Response to my press release on September 2nd has been very positive and I have been receiving lots of email and phone messages from Tibetans everywhere.

I am trying to get someone to translate the Kalon Tripa Hochoe into English, but if you already have it translated, please send it to me.

Any advice from you in this initiative of mine would be greatly appreciated.

Yours sincerely,

Pema Rinzin
President
TAC

Official Photographer/webmaster
Office of His Holiness the Dalai Lama
Thekchen Choeling
P/O Mcleod ganj 176219
Dharamsala (H.P.)
India

# Malware and payload

- Pdftools used to analyse documents, Wireshark and python to analyse network traces
- Malware exploited a known buffer overflow vulnerability in the PDF sandbox
- Payload did:
  - key-logging
  - file search and transfer
  - “I am alive” beacons
  - custom HTTP-based protocol
- Mostly communicated with three control servers located in Sichuan Province

# Attacker's operational security

- Tor – not used
- Dynaweb – some use once we started cleanup
- Grave operational security error gave the game away – sigint used for minor tactical advantage with no plausible deniability
- However, UKUSA opsec rules took a long time to develop and embed!

# Targeted attacks

- ‘Dragon Bytes: Chinese Information-War Theory and Practice’, Timothy Thomas, 2004
- 2008 annual report of the US – China Economic Security Review Commission
- WSJ articles on control systems etc
- AV industry: occasional similar attacks, rising from 1 in 2004–5 to 40 this year
- ‘What the Chinese spooks did in 2008, Russian crooks will be doing in 2010’

# Attribution – Alternative1

- Private enterprise by a hacker group.
- Against:
  - Chinese infowar doctrine of using hacker groups as auxiliaries – see ‘Dragon Bytes’
  - Coordinated pattern of activity from multiple locations in China associated with identified Chinese state organs
  - Use of intelligence product by Chinese diplomats

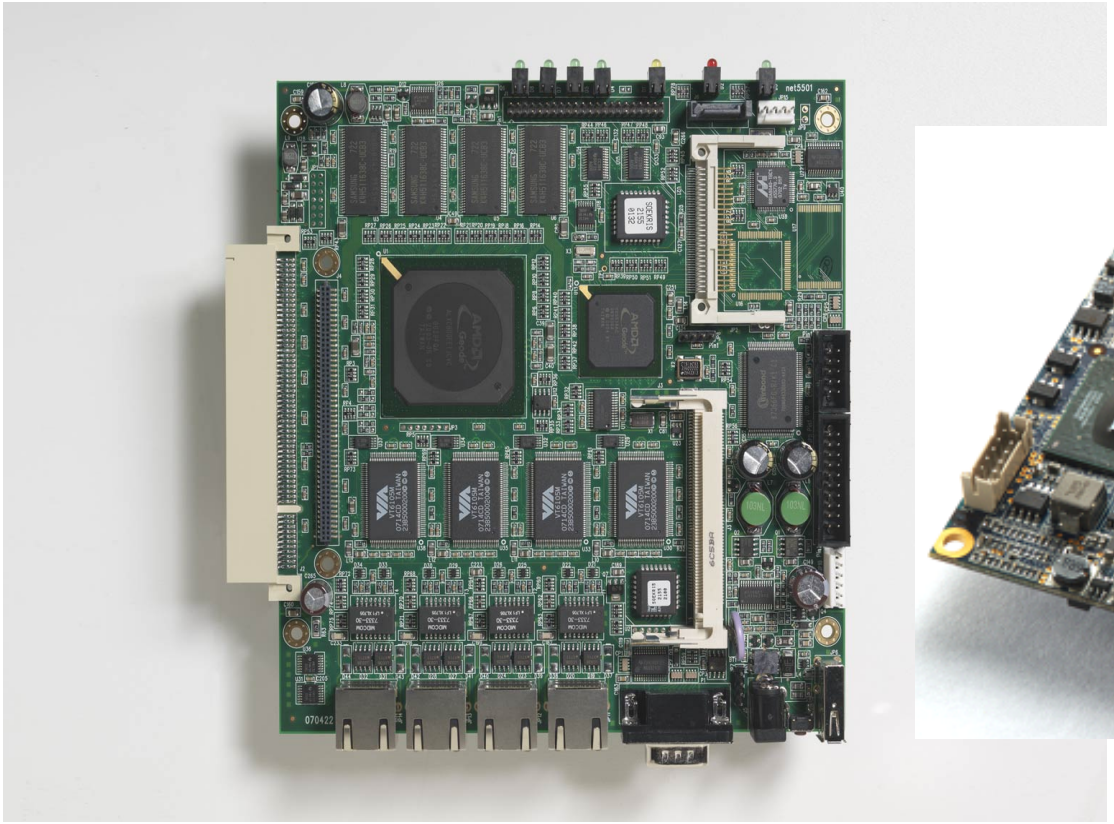
# Attribution – alternative 2

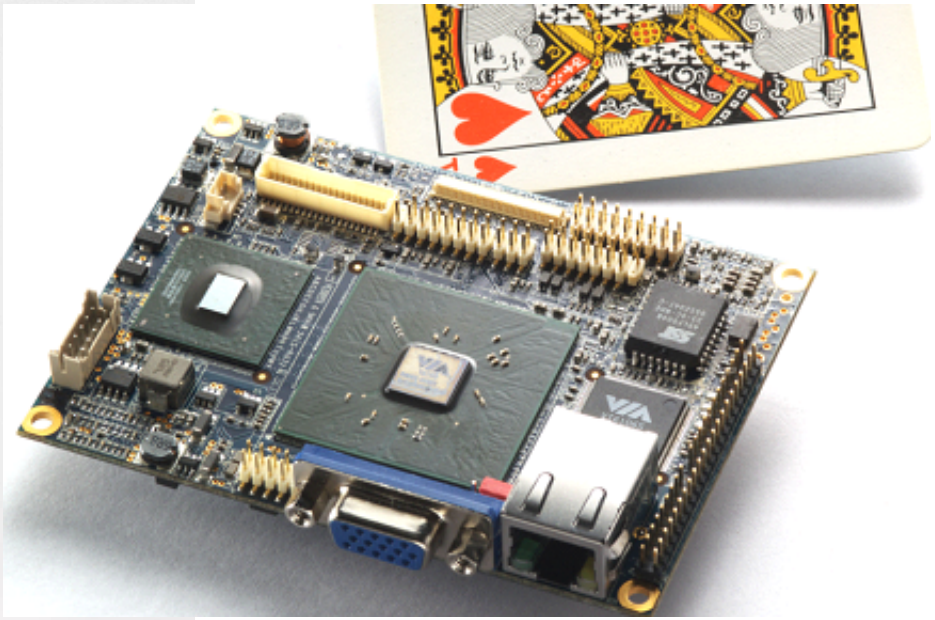
- An operation by the CIA, the FSB, etc using compromised machines in China
- Against:
  - USA, Russia not interested in Dalai Lama
  - pattern of activity from China much more complex than needed for deniability
  - pattern of intelligence priorities disclosed by Canadian compromise of the Chinese control server

# Countermeasures

- What can NGOs do to defend themselves?
- Well, how do the big powers do it?
  - Mandatory access control: BLP, labeling, mail guards, …
  - Heavy-duty operational security
- Can this work for OHHDL?
  - BLP engineering and opsec costs would not be sustainable
  - Middle way: train sysadmins, take all the Secret stuff offline
  - Application firewalls

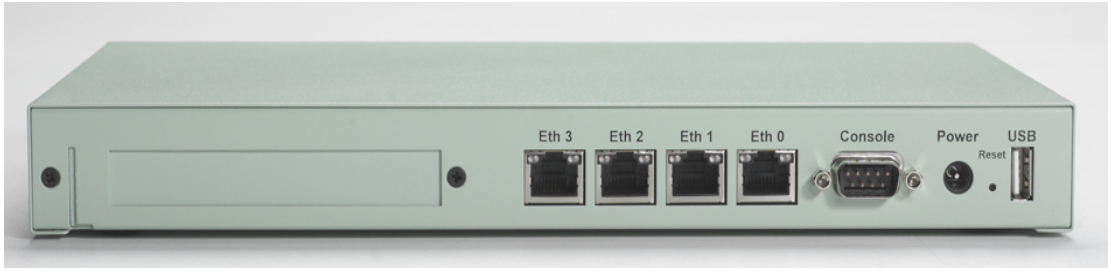
# Application firewalls: Step 0





VIA pico-tx

source: http://www.via.com




Soekris Net5501 source: http://www.soekris.com

# Countermeasures for companies

- How do you prevent input of false data?
- Accounting systems assume a single dishonest insider
- Social malware will change that!
- A firm might lock down the three machines that authorise bank payments
- But what about industrial control systems?

# Likely Future Developments

- What does security economics tell us?
- Banks and accounting system providers will dump the risk on their customers
- Auditing firms will follow old formulae until something compels change
- But should the government regulate (as in the USA, with NERC/FERC) or facilitate (as in the UK)?
- It might be best if the law prevented liability dumping

# Conclusions

- Social malware – the use of social engineering to install malware – is extremely powerful
- It looks like it's coming soon
- Protection is really hard – what accountants now tell companies to do is all but useless
- Lost-cost defences that can be fielded in companies and NGOs are urgently required
- The critical infrastructure community will have to think a bit more broadly