Spring 2009 – Security Update

noteworthy(?) things to do with security
in the past 6 months...

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Thanks

(input from & thanks to)

- Romain Wartel
- Sebastien Dellabella
- Sebastian Lopienski
- Djilali Mamouzi
- Stefan Lüders
- David Myers

" .. aw, that presentation is *so* easy. At least you always have *tons* of material to present.."

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Outline

- Windows
- MacOS
- Linux
- Cross-platform, Web, Mail
- Grid
- Controls
- Mobile
- Misc.

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

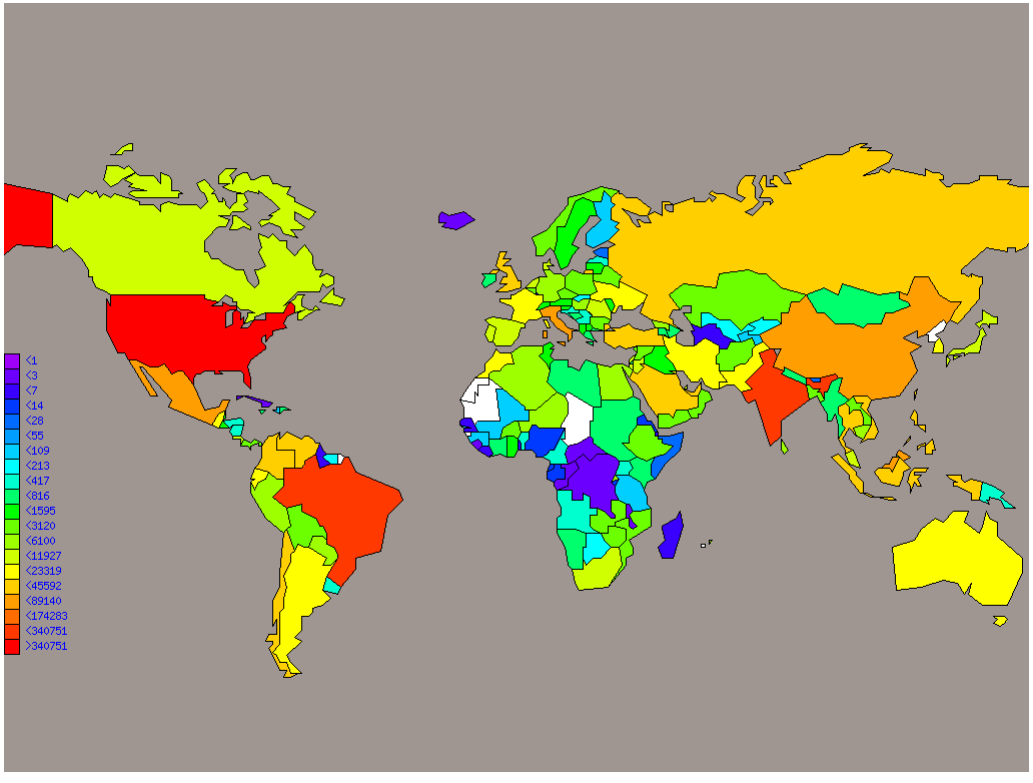
Windows - Conficker/Downadup

- out-of-band patch from Microsoft in Oct 2008; infects “Windows Server” service, spreads via net/shares/USB-autorun/local admin passwords/..)
- “millions” of infected machines, but many cleaned afterwards (the worm was victim of its own success)
- versions A and B contacted each some of 250 domains, different everyday; for version C it is a (small) subset of 50000, changing daily
- version C activated on Apr 1st, but nothing happened. Big media scare.
- eventually used for sending SPAM...
- the hype has resulted in many fake (malware) Conficker-removal tools..

Department Infrastructure
CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Conficker (cont.)

- Still: spreading at 50k hosts/day?
- (Symantec blog):
  main spread in US,
  Brazil, India



- CERN:
  - (only) two cases detected at CERN (so far)
  - detection at CERN: by looking for Conficker domains in CERN DNS query logs, now also with nmap

Department Infrastructure
CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Linux

- Continued SSH-borne intrusions & *phalanx2* installs in the HEP community – roving between sites.
  - Communication suboptimal, but difficult to balance
- "udevd" vulnerability also claimed some victims:
  - Apr 8 : obscure git commit in libudev
  - Apr 9: Red Hat bug open
  - Apr 16: "exploit" blog entry; various vendor releases
  - Apr 16: timestamp of exploit found on LXPLUS... (wasn't vulnerable, SLC4).
- Philip Gabriel Pettersson 'Stakkato' (2005 NASA/HEP/US intrusions..) finally charged in US. Over Cisco SW.

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Mac OS

- Backdoored “pirated” iWork 2009, Photoshop in January (fully functional)
- CanSecWest 2009 (link)
  - 1 local root exploit (HFS-Diskimages), 5 DoSes.., 0-day for Safari..
  - Pwn2own:
    - Mac gone in <10sec.
    - “*Exploit writing on the Mac is fun. Exploit writing on Windows Vista is hard work.*” (quote)
    - “[..] *The bug does affect Windows but, honestly, it’s way harder to get the code to run reliably on Windows. That’s the reason I did my Firefox attack on the Mac.* “ (quote)

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Cross-platform

- Adobe Acrobat Reader: non-JavaScript exploit (JBIG2) “in the wild” (and 2 others - “partial fix” only) http://secunia.com/advisories/33901/
- Firefox-3: 10 advisories since October.. (mozilla.org)
  - CanSecWest 2009: exploits for MS-IE, Firefox, Safari – by “Nils”. Chrome survived... (Tipping Point)
- Google Chrome: 5 vulns in 2009... (Google blog)
- Adobe Flash: 3 updates.. (Secunia)

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

The InterWebs

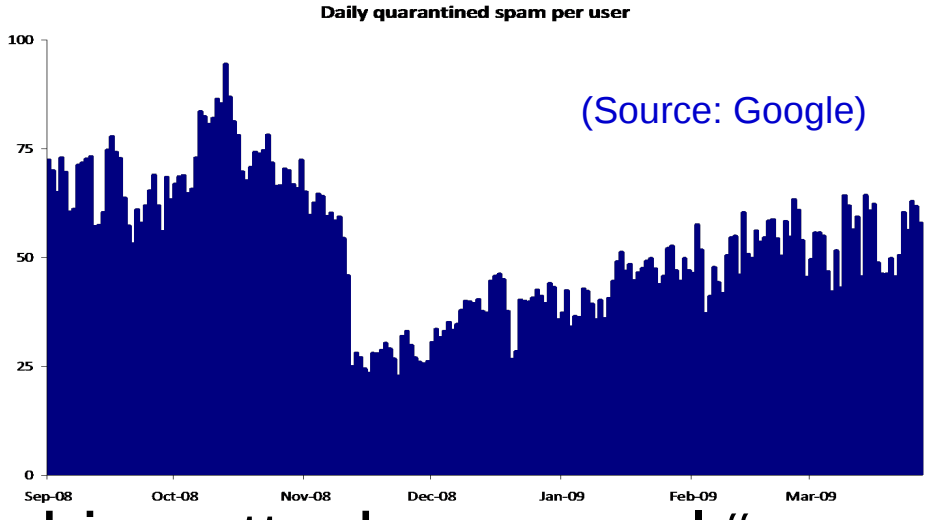
- more malware distributed via social networking
  - scenarios: a "friend" sends a video link that needs an *“updated”* Adobe Flash Player (proposed update is malware). In some cases, non-Windows users are redirected to a real YouTube video..
  - Twitter worms (StalkDaily: 100's of accounts?, JavaScript..)
  - online poker sites are a common target for attackers

- at CERN: Web application security project started.
  - Goal: to minimize number of vulnerabilities in Web applications, mainly by using vulnerability scanners (opensource+commercial).

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Mail

- SPAM drop after McColo shutdown (last fall, 70%) only temporary :-(



(Source: Google)

- CERN: targeted phishing attacks, several “waves” - compromised accounts ultimately used to send SPAM via authenticated SMTP.
  - “Mailbox size” mail +link to phishing site:
    - 1500 mails received,>= 109 devices contacted site, >=30 users disclosed password (and only 5 noticed immediately)
  - Users are being trained to recognize them
    - And now start reporting them, so we get 10s of notifications..

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Phishing Example 1 -english


```
Subject: EMAIL ACCOUNT UPDATE
From: "costomerservice@@cern.ch" <costomerservice@@cern.ch>
Date: Wed, 29 Apr 2009 19:55:21 +0200
To: Undisclosed recipients <Undisclosed recipients:;>

The CERN WEBMAIL SERVICE WEBSITE WISH TO INFORM YOU
THAT WE HAVE SOME PROBLEMS ABOUT EACH CUSTOMER ACCOUNT EMAIL. DUE TO
ERROR CODE 334409. WE DISCOVERD THAT IN FEW DAYS FROM NOW EACH
CUSTOMER WILL NOT BE ABLE TO ACCESS HIS OR HER EMAIL ACCOUNT.

IN THAT REGARD,YOU ARE REQUIRED TO SEND YOUR EMAIL ADDRESS AND
PASSWORD FOR A NEW ACCOUNT UPDATE.

YOU ARE ADVISED TO IMMEDIATELY SEND US THE REQUIRED INFORMATION SO AS
TO ENABLE US IMMEDIATELY UPDATE YOUR ACCOUNT.YOU ARE TO SEND US THIS
INFORMATION VIA EMAIL TO
account_update@sify.com

Note:You have to understand that the reason why we are not sending
this message from our own private account.This is due to some
technical problem we are having right now.
Thanks for your understanding.
BELOW IS THE INFORMATION REQUIRED FOR ACCOUNT UPDATE

1)Full Email Address:
2)password:
3)country:
4)First name/Last name:
```

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Phishing Example 2 - French

CERN IT Department

```
Subject: COMPTE DE MISE À JOUR DE COURRIEL
Date: Wed, 29 Apr 2009 11:22:23 -0700
From: helpdesk@cern.ch <helpdesk@cern.ch>
Reply-To: <account_update@sify.com>
To: Undisclosed recipients:;

CERN SERVICE DU SITE WEB tiens à vous informer
QUE nous pose quelques problèmes sur chaque compte client EMAIL. DUE TO
ERREUR CODE 334409. WE découvert que dans quelques jours, CHAQUE
Client de ne pas pouvoir accéder à ses compte de messagerie.

A CET EGARD, vous êtes tenu de vous ENVOYEZ VOTRE ADRESSE EMAIL ET
MOT DE PASSE DE COMPTE D'UNE NOUVELLE MISE À JOUR.

Il vous est conseillé d'envoyer immédiatement les informations requises
US FACON
POUR PERMETTRE US IMMEDIATEMENT METTRE À JOUR VOTRE ACCOUNT.YOU SONT A
ENVOYER CE
Informations par courrier électronique à
account_update@sify.com

Note: Vous devez comprendre que la raison pour laquelle nous ne sommes
pas d'envoi
ce message de notre propre account.This est due à une
problème technique que nous avons maintenant.
Merci pour votre compréhension.
VOUS TROUVEREZ CI-DESSOUS DE L'INFORMATION REQUISE POUR COMPTE DE MISE À
JOUR

1) adresse e-mail:
2) le mot de passe:
3) pays:
4) Prénom / nom:

Copyright CERN 2008 - Web Communications, DSU-CO
```

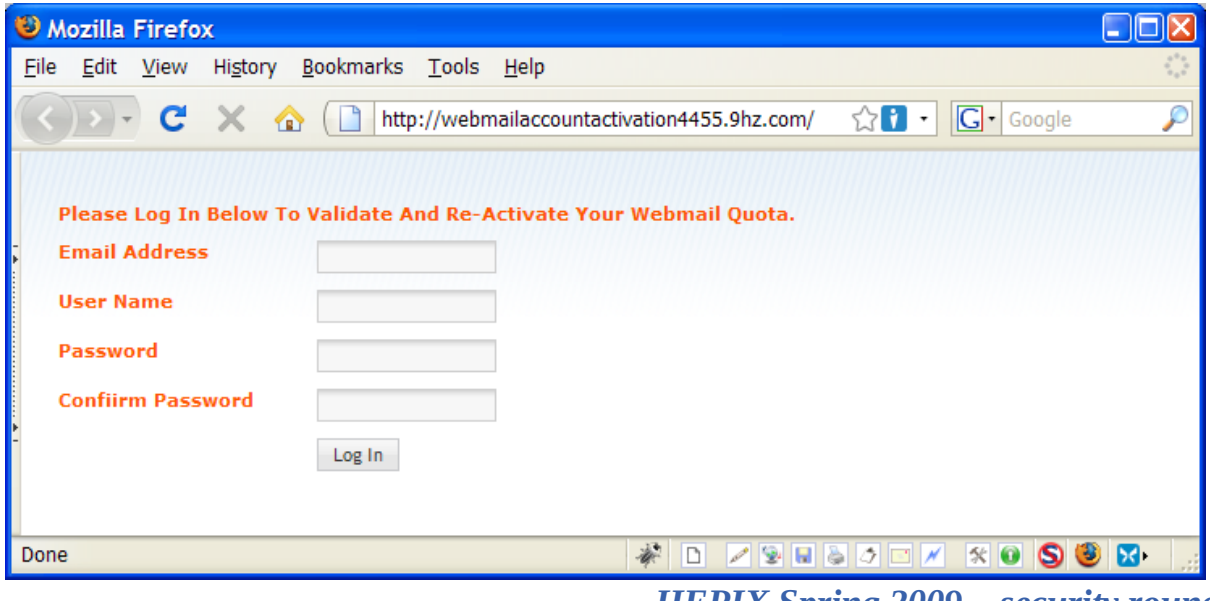
Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Phish via web

CERN IT Department

```
Subject:  YOUR WEBMAIL MEMORY HAS EXCEEDED THE SET LIMIT
Date:     Mon, 4 May 2009 01:09:51 -0700
From:     ithelp@cern.ch <ithelp@cern.ch>
Reply-To: <account_update@sify.com>
To:  Undisclosed recipients:;

YOUR WEBMAIL ACCOUNT HAS EXCEEDED THE SE QUOTA OF 20GB.YOU ARE NOW USING 20.7GB.

PLEASE CLICK THE LINK BELOW TO RE-ACTIVATE YOUR WEBMAIL ACCOUNT AND BOOST YOUR WEBMAIL QUOTA

http://webmailaccountactivation4455.9hz.com/

FAILURE TO CLICK THIS LINK MAY RESULT IN LIMIED ACCESS TO YOUR WEBMAIL ACCOUNT.

THANKS
LOCALHOST
WARNING!!! PLEASE DO NOT SEND YOUR WEBMAIL ACCOUNT AND PASSWORD TO ANYONE VIA EMAIL
```



CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

GRIDs

- JSPG – currently drafting several policy updates
  - "Security Incident Response Policy" (link)
  - "VO Portal Policy" (link)

- EGEE Tier-0/1 security service challenge
  - Same procedure / "incident" as last year:
    - "Consider any activity from the following user as malicious. DN: ...."
    - pre-announced
  - Overall: gradual improvements, details on GDB slides (link)

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

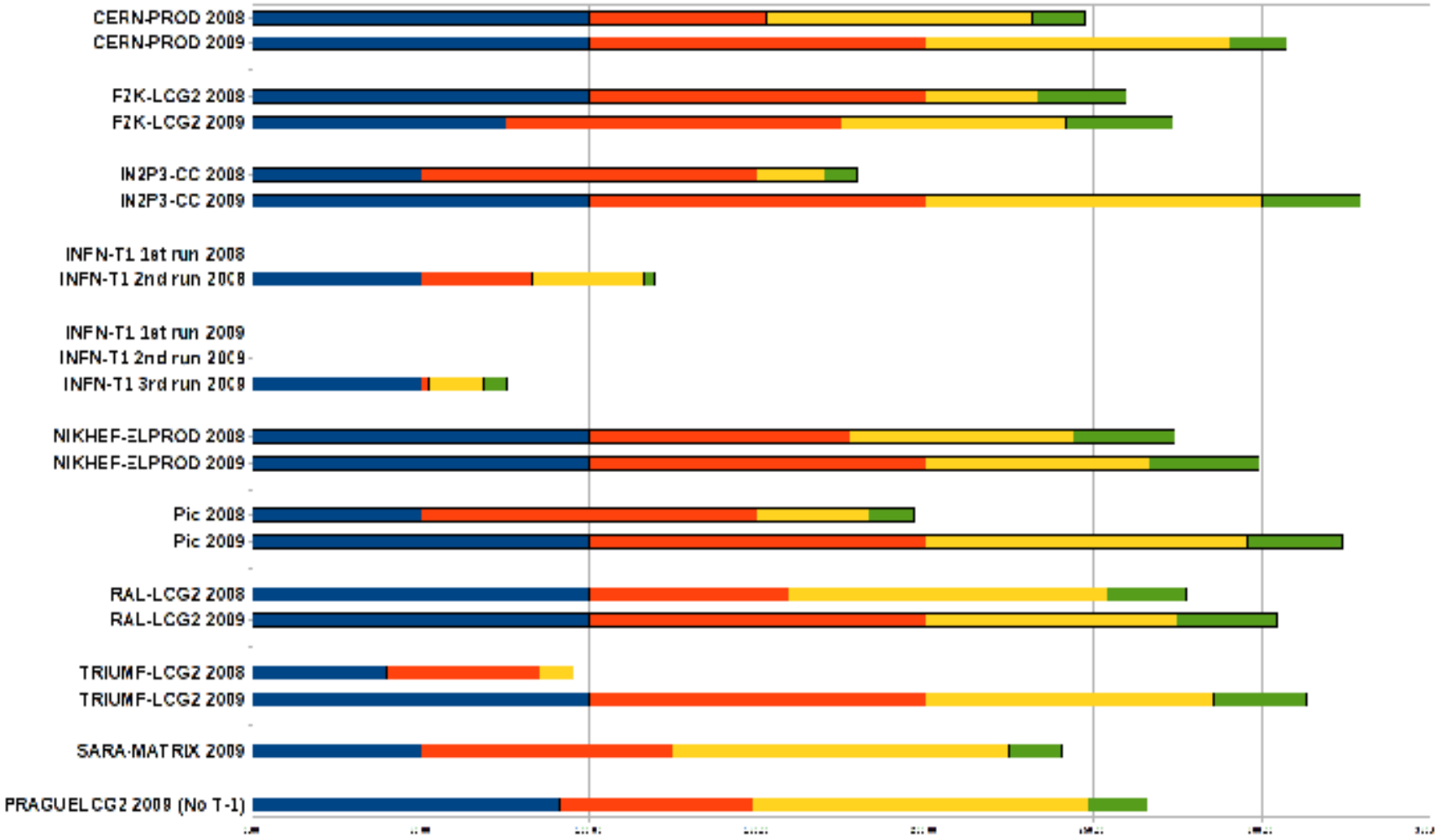
The Task / Evaluation

Evaluation, 3 areas -Time Matters: Bonus Points for fast reactions/pre-reports.

- Communication
  - Acknowledge/Heads-up report sent to the CSIRT list (Target 4h).
  - Alert sent to the affected VO Manager (Target 24 h).
  - Verify the responsible CA has been notified (Target 144 h).
  - Close-out report sent to the CSIRT list (Target 144 h).
- Containment
  - Found the malicious job and killed it (Target 4h).
  - Suspended the user at the site (Target 4h).
- Forensics
  - Discovery of initiating site (UI) and established contact with that site's CERT (Target 24h).
  - Found evidence of malicious network traffic (Target 48h).
  - Some analysis of the submitted binaries was performed (Target 48h).

Preliminary Results

SSC3 – overall results



Recent Developments in Controls

Cracked road-sign with open wireless access

THE WALL STREET JOURNAL. | TECH

Europe Edition ▾ | Today's Paper • Video • Columns • Blogs • Graphics • Journal Com

Home | World | Business | Markets | Market Data | Tech | Life & Style

Digits | Personal Technology

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

U.S. electrical grid in jeopardy (April 2009)

Congress > Legislation > 2009-2010 (111th Congress) > S. 773

ShareThis

Text of S. 773: Cybersecurity Act of 2009

Show this version:
Introduced in Senate
Download PDF
Full Text on THOMAS
Go to Bill Status

Compare to this version:
None

GovTrack's bill text viewer has been recently updated. While we work out the kinks in the new viewer, archival legislative text may not be available. Your comments and suggestions for the new viewer are welcome.

This version: Introduced in Senate. This is the original text of the bill as it was written by its sponsor and submitted to the Senate for consideration. This is the latest version of the bill available on this website.

S 773 IS

111th CONGRESS

SEC. 2. FINDINGS.

The Congress finds the following:

(1) America's failure to protect cyberspace is one of the most urgent national security problems facing the country.

U.S. congress faces this Wind of Change !

At CERN: Lot's of consolidation of controls networks & PCs

Mobile:

- Redirect phone data services via “operator” SMS (DNS, proxy servers etc) (link)
- SymbianOS “SexyView” (Yxe.A) - first SMS-borne worm? (social engineering – website+spread via contact list; signed with valid (leaked) cert = minimal interaction)

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

The GhostNet

- Tibetan government in exile suspected infiltration of computers, called investigators in 2008
- Investigators from Canada and the U.K. discovered cyber-espionage malware infecting targeted machines:
  - penetrated Tibetan computer systems, extracting sensitive documents from the private office of the Dalai Lama
  - stealing e-mail correspondence, other data
  - remote control
  - video and audio recording

  (investigation results published in March 2009)

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

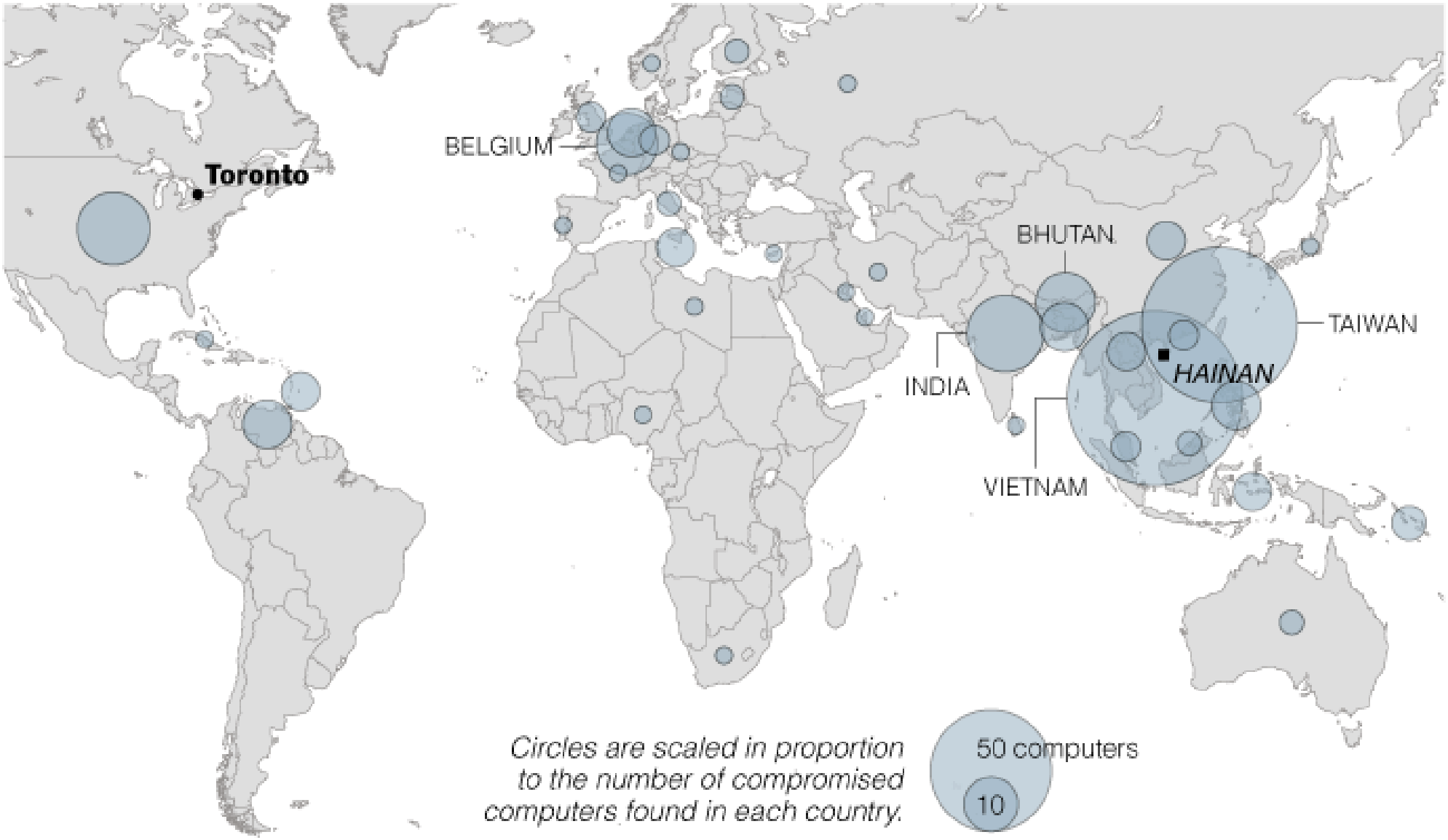
The GhostNet

- ~1300 compromised systems in ~100 countries:
  - embassies and governments of many countries, mostly Asian (India, South Korea, Indonesia, Iran, Philippines, Thailand, Taiwan, Pakistan, Laos), but also Portugal and Germany
- China involved?
  - network controlled from servers located mainly in China
  - University of Cambridge researchers believe that the Chinese government is behind these intrusions
  - no strong evidence; China denies any involvement
  - but some actions of Chinese government officials corresponded with the information obtained via GhostNet

(more: http://en.wikipedia.org/wiki/GhostNet)

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

The GhostNet



DarkMarket

- http://www.darkmarket.ws – an online criminal forum
  - trading stolen identities & credit cards, attacks tools & services etc.

from F-Secure.com

- … taken over and run from Nov 2006 until Oct 2008 by an undercover FBI agent Keith Mularski
- *"56 arrests worldwide; $70 million loss prevented"*

(more http://www.wired.com/threatlevel/2008/10/56-arrested-in/)

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

national “cybersecurity”

- Various reports unhappy about US inter-agency mess (National Strategy to Secure Cyberspace Feb 03, CSIS Dec 08, ..)
- “turf war” between NSA & DHS?
  - NSA widely seen a technically capable but untrusted
  - DHS: “National Cybersecurity Center” unfunded, boss quits ..
- DOD/military also would like “cyber command” (link)
- FBI-led Joint Inter-Agency Cyber Task Force (link) since April 08
- France (link), Germany (link) armies setting up “cyber” units, including offensive capacity.

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it