A larger role for RIR's in cybersecurity?

BenoîtMorel
Carnegie Mellon University

Ghostnet: simple and deadly…

- What made ghostnet deadly were two things:
  - it allowed the attackers to spy on the email of networks such as embassies, government etc…
  - It was difficult to the victims to realize they were spied upon
- What made ghostnet simple were two other things:

A Virus Total screen capture of a malware infected email attachment

Antivirus	Version	Last Update	Result
AntiVir	-	-	EXP/Word.Dropper.Gen
Authentium	-	-	CVE-2006-2492
Avast	-	-	MW97:CVE-2006-2492
eTrust-Vet	-	-	W97M/SmartTags!exploit
F-Prot	-	-	CVE-2006-2492
Fortinet	-	-	MSWord/ObjPointer.A!exploit.M20062492
GData	-	-	MW97:CVE-2006-2492
Ikarus	-	-	Virus.MW97.CVE.2006.2492
Microsoft	-	-	Exploit:Win32/Wordjmp.gen
Sophos	-	-	Troj/MalDoc-Fam
Webwasher-Gateway	-	-	Exploit.Word.Dropper.Gen

11 out of 34…

Example of social engineering used by ghostnet

From: "campaigns@freetibet.org" <campaigns@freetibet.org>
Date: 25 July 2008
Subject: Translation of Freedom Movement ID Book for Tibetans in Exile

Translation of Freedom Movement ID Book for Tibetans in Exile.

Front Cover

Emblem of the Tibetan government in Exile

Script: Voluntary Contribution into common fund for Tibetan Freedom Movement

Inside Cover

Resolution was passed in the preliminary general body meeting of the Tibetan Freedom Movement held on July 30, 1972 that the Tibetan refugees in exile would promise for each individual,Äôs share of the voluntary contribution into the Tibetan Freedom Movement Receipt book. This resolution was later reaffirmed by the 11th Tibetan People,Äôs Deputies and passed into the law on April 01, 1992 (Tibetan King Year 2119)

Until the last page of this book is used, the book stands valid until August 15, 2012

Date: August 16, 2008
Emblem of the Tibetan Government in Exile

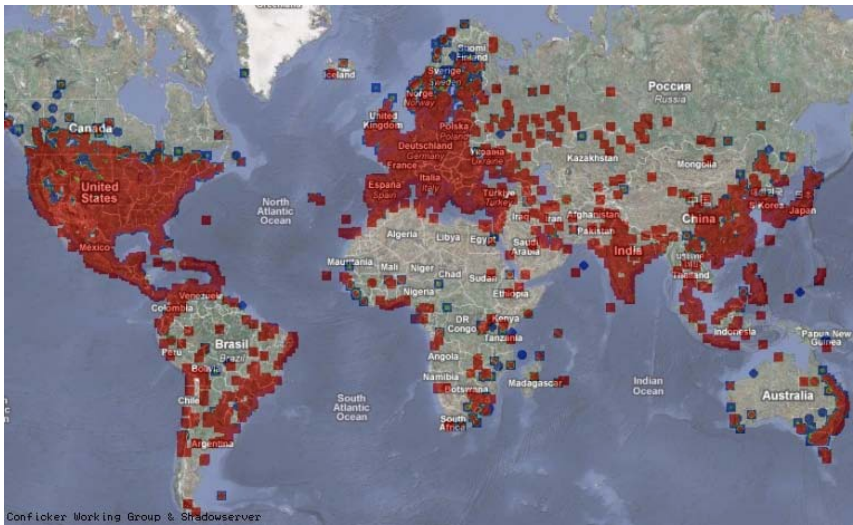
Official Signature

Attachment: Translation of Freedom Movement ID Book for Tibetans in Exile.doc

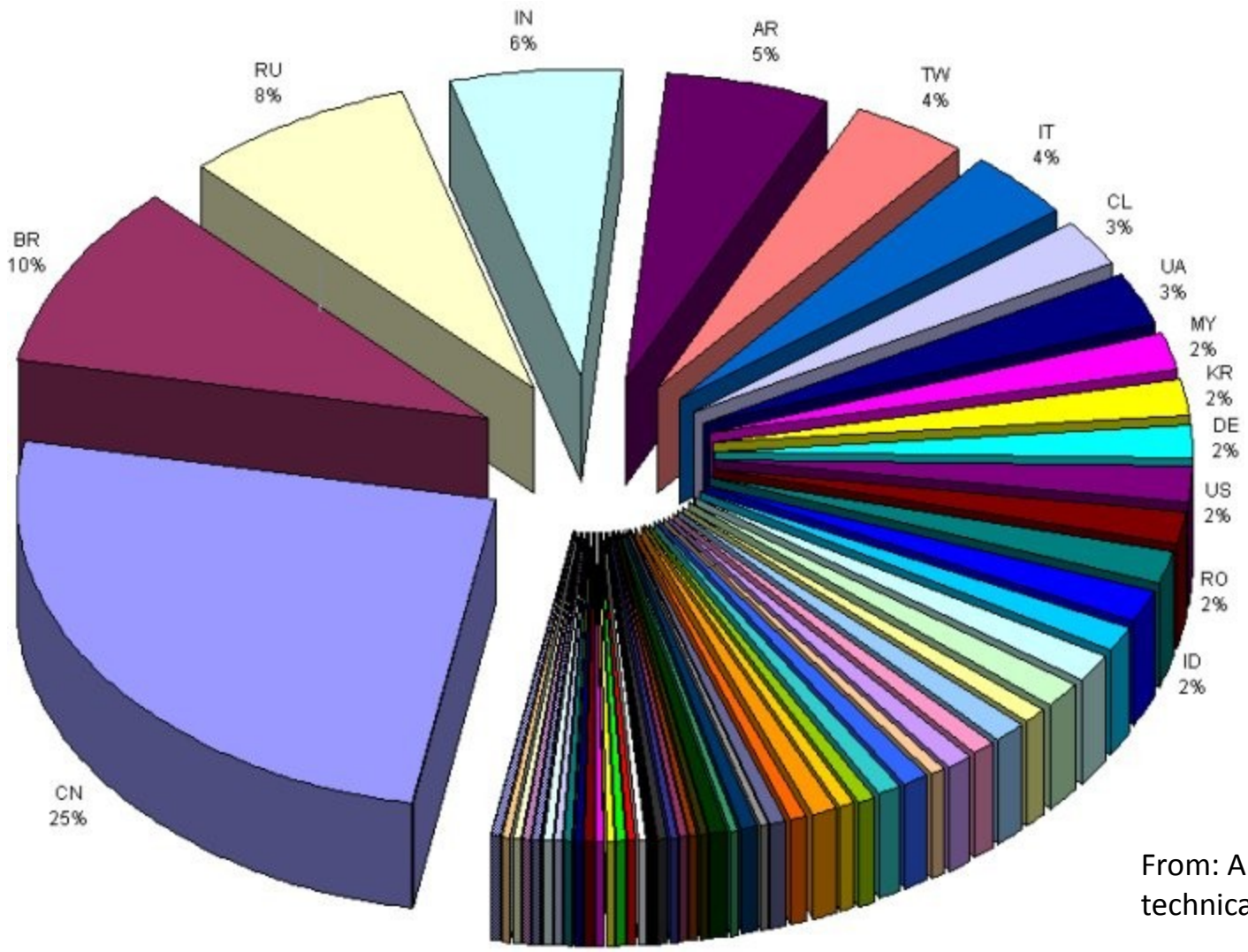
Conficker

- The existence of the Conficker working group: evidence that C. ushered us in a new era…
- Where is the repository on knowledge in cybersecurity?

- Who are those guys?



Early distribution of conficker



From: An analysis of Conficker, SRI technical report , 2009

Lessons from Conficker

- Containment was made successfully: it did not do any damage (not yet…)
- It defeated annihilation or eradication
  - A botnet is dynamic
  - Removal of the malware is slow
- Command and Control architecture are not known
- Its system of updating was brilliant (but not good enough)

The Internet's Leading Banking Trojan

- Zeus (also known as Zbot, PRG, Wsnpoem, Gorhax and Kneber) is considered the most trusted and robust malware platform for online banking fraud,
  - Zeus is (was -> 2010) a family of toolkits, which can be purchased for as little as $700 (if sold from a reseller) and up to $15,000 for the newest version with all new available features
  - **It has been licensed by numerous criminal organizations to launch targeted attacks against specific bank's customers**.

Polymorphic malware

- Antivirus detection of Zeus has a poor track record.
  - In a 2009 report based on information gathered from 3 million desktops in North America and the UK Trusteer found that the majority of Zeus infections occur on antivirus protected machines.
  - It is estimated that in average the rate of detection by AV is about 23%...
- Zeus 1.4 was specifically crafted to avoid antivirus detection and uses advanced *polymorphic techniques*, which make antivirus technologies completely blind to it.
- Outwardly, a ZEUS infected PC will show no

Stuxnet and the vulnerability of modern critical infra-structures

The control center of the Bushehr nuclear power plant

Enrichment centrifuge cascades

SIEMENS

Siemens S7 Programmable Logic Controller (PLC)

What Stuxnet accomplished and did not…

- 4 zero-day attacks + MS08-067
- 2 rogue certificates
- Malware which speaks to control system
- Penetrated highly protected networks
- But it leaked out
- It setback the nuclear program of Iran, but by a few years at most

More recent attacks

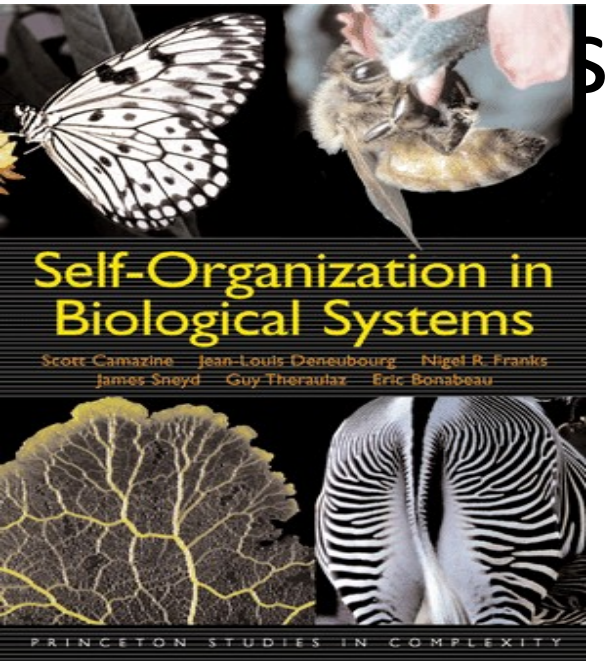
- Night Dragons (target energy)
- DigiNotar (certificates)
- DuQu (copied Stuxnet to produce a spyware)
- ShadyRAT (Anew version of Ghostnet?)
- The water pump in Illinois (Maroochy)

One message of the history of cyberattacks is that each new technology seems to open the door to a new kind of attack

- Still the more significant progress in cyberattacks is in the art of designing new attacks
- Many of the the concepts used are by and large similar to what was used before, but they are exploited more shrewdly:
  - Buffer overflows have been there for decades and are still there. What has “improved” is the art of writing exploits.
    - Our defense has not improved in a commensurate way
  - Vulnerabilities which were thought to be not exploitable, turned out to be

- Sheldon Whitehouse (Sen, RI): Whatever its form —copying source code, industrial espionage of military product designs, identity theft, online piracy or outright theft from banks —cybercrime cripples innovation, kills jobs, undermines our economic security and violates individual privacy.”

Cybersecurity as an instantiation of self-organization



- No planned architecture or any design underlies the present form of cybersecurity: it is a result of pure self organization…

- But this is work in progress and there are challenges…
- The threat and challenges are increasing,
  - Some because the attackers are getting better
  - Some as a result of web and other innovations…
- For the future we need to be better at defense, **far better!**

A global cybersecurity response?

- There is a difference between state actors and non-state actors, in what they do and represent as threat.
- State actors tend to spy
- Non-state actors?
- Who cost more to the world economy?
- Needed today: containing the threat from non-state actors

How?

- Nations' sovereignty stops at their border.
- When it comes to bots, ISPs see best
- There may not be silver bullets, but cooperation among ISPs could go a long way in improving the tracking of malicious traffic a basic condition to fight it.
- There is some need of some form of governance of the internet.

There is not real relevant authority or governance
A new role for the RIR's??