The challenge for developing countries of acquiring cybersecurity capability ***today***

Benoît Morel

Carnegie Mellon University

Issues

- Multi-dimensional:
  - Cybercriminality (legal dimension)
  - Technical dimension (skill and competence are probably the MOST important feature of cybersecurity capacity)
  - Cost (The economics of cybersecurity can act as a hindrance)
- What template for developing countries:
  - US and advanced Western countries are not good examples.
  - Tunisia is a unique success story and it is of great relevance for developing countries which want to create national CERT
- Complexity of the threat

Complexity of the threat

- Cybersecurity is a vast world projecting an impression of arcane complexity.
- Most of the times cyber-attacks are “benign”, … but one should NOT rely on that when building cybersecurity capabilities: The serious threats should not be ignored and one should expect more of them in the future:
  - Examples of recent threat that foreshadow the future:
    - ghostnet,
    - agent.btz,
    - conficker
- Web applications, wireless are opening a new generation of vulnerabilities
- Developing countries can be targets and also used to facilitate attacks (for example by being pockets of infections)
- Large bandwidth connection will exacerbate this problem

Worldwide phenomenon

- The art of cyberattack improves faster than our ability to respond:
  - Conficker outsmarts our defense capabilities: Conficker working group, Conficker: the first application of MD6…
  - Agent.btz and the protection of data when even USB keys can propagate malware.
- Cyberattackers have the strategic edge
- Repository of knowledge:
  - The hackers are the most competent then come the security operators of institutions like banks, the private sector and academia (in that order).
- The governments (except China??) are far behind and has far more to learn than to teach…

US no template for developing countries

- US critical infra-structure far more computerized than in developing countries

- Cyberdefense in the US today is the result of 20 years of self-organization
- The US government is not good at securizing itself: FISMA: an unmitigated fiasco (NIST)
- The concept of private-public partnership means very different things in the US and in developing countries:
  - the private sector has the lead in the US
  - In developing countries, the situation should be the opposite

Tunisia as template

- CERT/Tcc (which became ANSI) was created in 2005
- Enjoys support from Government and parliament.
- Involved in:
  - Out-reach to protect children from the internet
  - Developing a tool (Saher) to monitor the national network for vulnerabilities and infections
  - Creating a system of audits which pro-actively makes the whole economy of Tunisia more resilient against cyberattacks
  - Organizing events to inform and sensitize the population of Tunisia

Technical dimension of the problem

- Lesson from the past:
  - Security should not be added retro-actively, but part of the original design
- Fundamental tension between functionality and security
- There is no known completely safe protocol:
  - One key is the **human factor** (NANOG, Security operators, etc..)
  - They explain why the system still works despite all its flaws and weaknesses …

Getting out of the "Pay today or pay tomorrow" dilemma

- Cybersecurity is not cheap, but ignoring it can cost dearly
- Security industry is (so far) our *only* line of defense but it is also for profit
- The extension of cybersecurity to the developing world also means revisiting some fundamentals of the economics of cybersecurity

- Free or open source security tools are not on a par with commercial tools, today, but could become so tomorrow…

A good idea for developing countries: Build National CERTs

- National CERT should be:
  - the centralized repository of knowledge for the country (should be able to advise the government as well as private interests)
  - Coordinate the establishment of the cyberdefense at the national level (regulation, monitor the distribution of security tools and their upgrade, being able to clean the equivalent of conficker infection,…)
  - Stay abreast with the fast changing world of cybersecurity (collaboration with nations in similar situations
- Does not need to start very large, as long as the nations organizes itself to have access to adequate technical expertise in case of emergency.
- Learning by doing an important component
- Ask the Tunisians…

IPUTER SECURITY REPORT CARD

March 16, 2006

GOVERNMENTWIDE GRADE 2005: D+

	2005	2004		2005	2004
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+	A+	DEPARTMENT OF COMMERCE	D+	F
DEPARTMENT OF LABOR	A+	B-	DEPARTMENT OF JUSTICE	D	B-
SOCIAL SECURITY ADMINISTRATION	A+	B	NUCLEAR REGULATORY COMMISSION	D-	B+
OFFICE OF PERSONNEL MANAGEMENT	A+	C-	DEPARTMENT OF TREASURY	D-	D+
ENVIRONMENTAL PROTECTION AGENCY	A+	B	DEPARTMENT OF ENERGY	F	F
NATIONAL SCIENCE FOUNDATION	A	C+	DEPARTMENT OF VETERANS AFAIRS	F	F
GENERAL SERVICES ADMINISTRATION	A-	C+	DEPARTMENT OF HEALTH AND HUMAN SERVICES	F	F
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	B-	D-	DEPARTMENT OF THE INTERIOR	F	C+
SMALL BUSINESS ADMINISTRATION	C+	D-	DEPARTMENT OF DEFENSE	F	D
DEPARTMENT OF TRANSPORTATION	C-	A-	DEPARTMENT OF STATE	F	D+
DEPARTMENT OF EDUCATION	C-	C	DEPARTMENT OF HOMELAND SECURITY	F	F
HOUSING AND URBAN DEVELOPMENT	D+	F	DEPARTMENT OF AGRICULTURE	F	F

In fact does not mean what it seems. It reflects the failure of an approach which turned into a paperwork exercise.

Pentagon attack

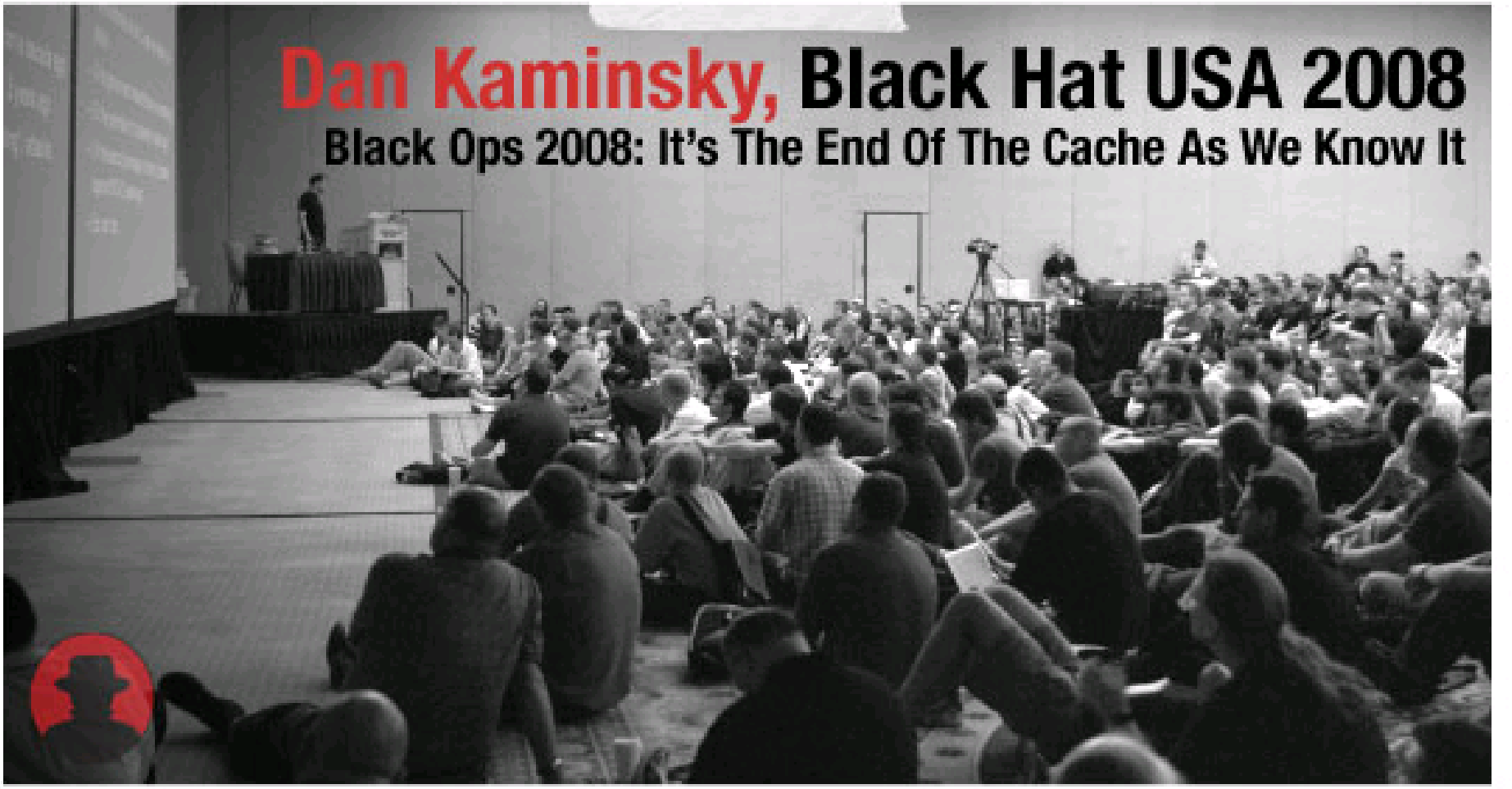
- Copy of a memo sent out last week (November 14 2008) to an Army division warning of the cyber attack:
  - "Due to the presence of commercial malware, CDR USSTRATCOM has banned the use of removable media (thumb drives, CDRs/DVDRs, floppy disks) on all DoD networks and computers effective immediately.“
- The GIG is a system of 17 million computers, many of which house classified or sensitive information.
- The problem, according to a second Army e-mail, was prompted by a "virus called Agent.btz." It is a known Trojan dropper.

French Airforce grounded

- Apparently, in the past two weeks (Preceding February 10), some French fighter planes were grounded because the military *had failed to take sufficient action* (even though Microsoft had sent advance warning) to prevent the spread of a Windows-transmitted virus Conficker…

Not only the French being affected though, the UK Ministry of Defence also reported that some of its major systems were also affected, spreading across admin offices, Royal Navy Warships and Submarines. It has even infected over 800 Hospital computers in Sheffield! Does anyone else find this somewhat concerning?

DNS


Dan Kaminsky, Black Hat USA 2008
Black Ops 2008: It's The End Of The Cache As We Know It

Ghostnet Report

Quote from the report: “A disturbing picture

- At the time of writing, these organizations are almost certainly oblivious to the compromised situation in which they find themselves.
- The computers of diplomats, military attachés, private assistants, secretaries to Prime Ministers, journalists and others are under the concealed control of unknown assailant(s).
- Almost certainly, documents are being removed without the targets’ knowledge, keystrokes logged, web cameras are being silently triggered, and audio inputs surreptitiously activated.
- This raises the question,
  - how many illegal transactions have been facilitated by information harvested through *GhostNet*?
  - Worst of all, how many people may have been put at risk?”

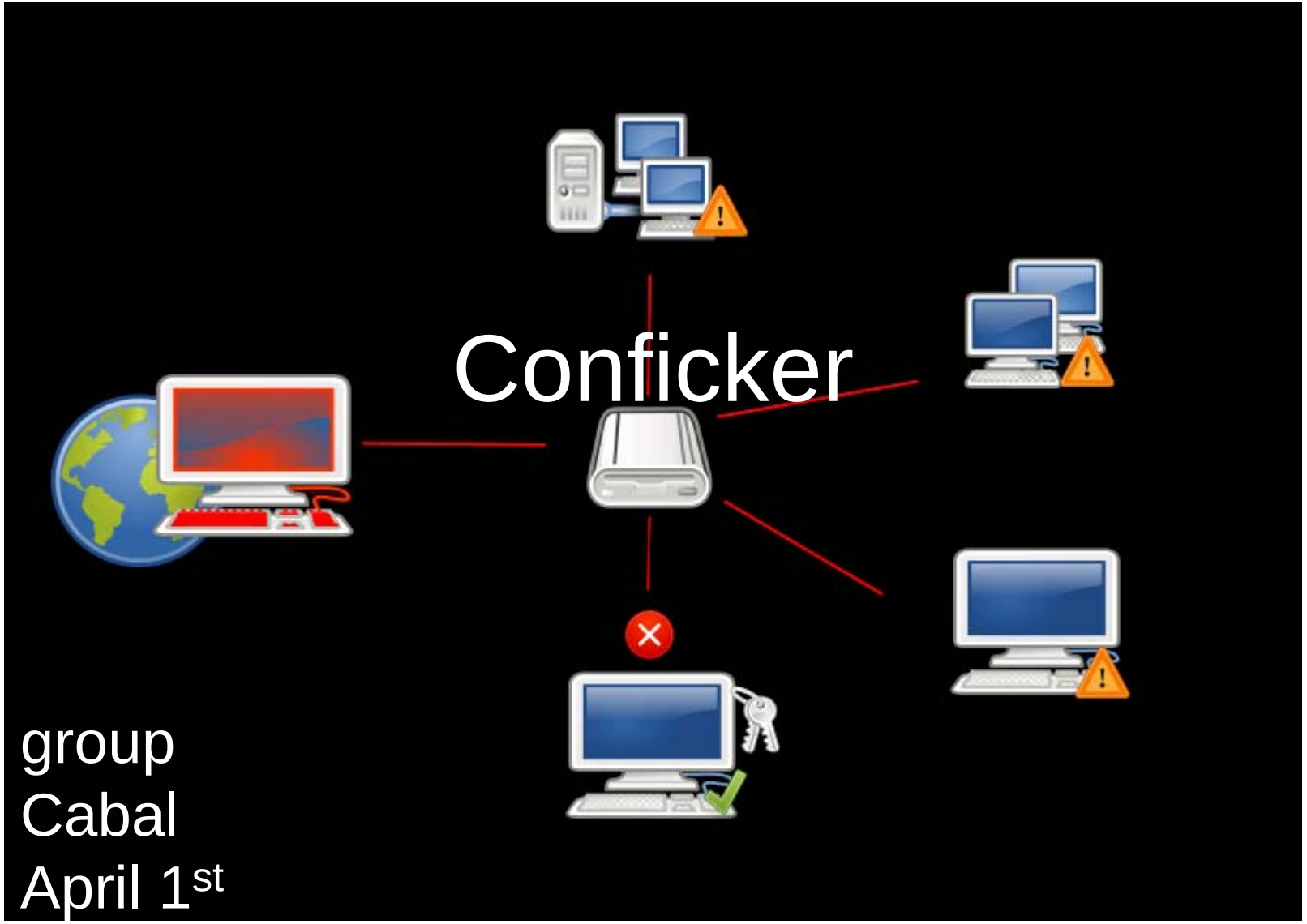
Remarks

- The Trojan used in that case was not detected by the major antivirus software
- A new Trojan can be made specifically for such an attack and be completely invisible to antivirus software
- Only skillful administrators could detect its presence early

Encryption

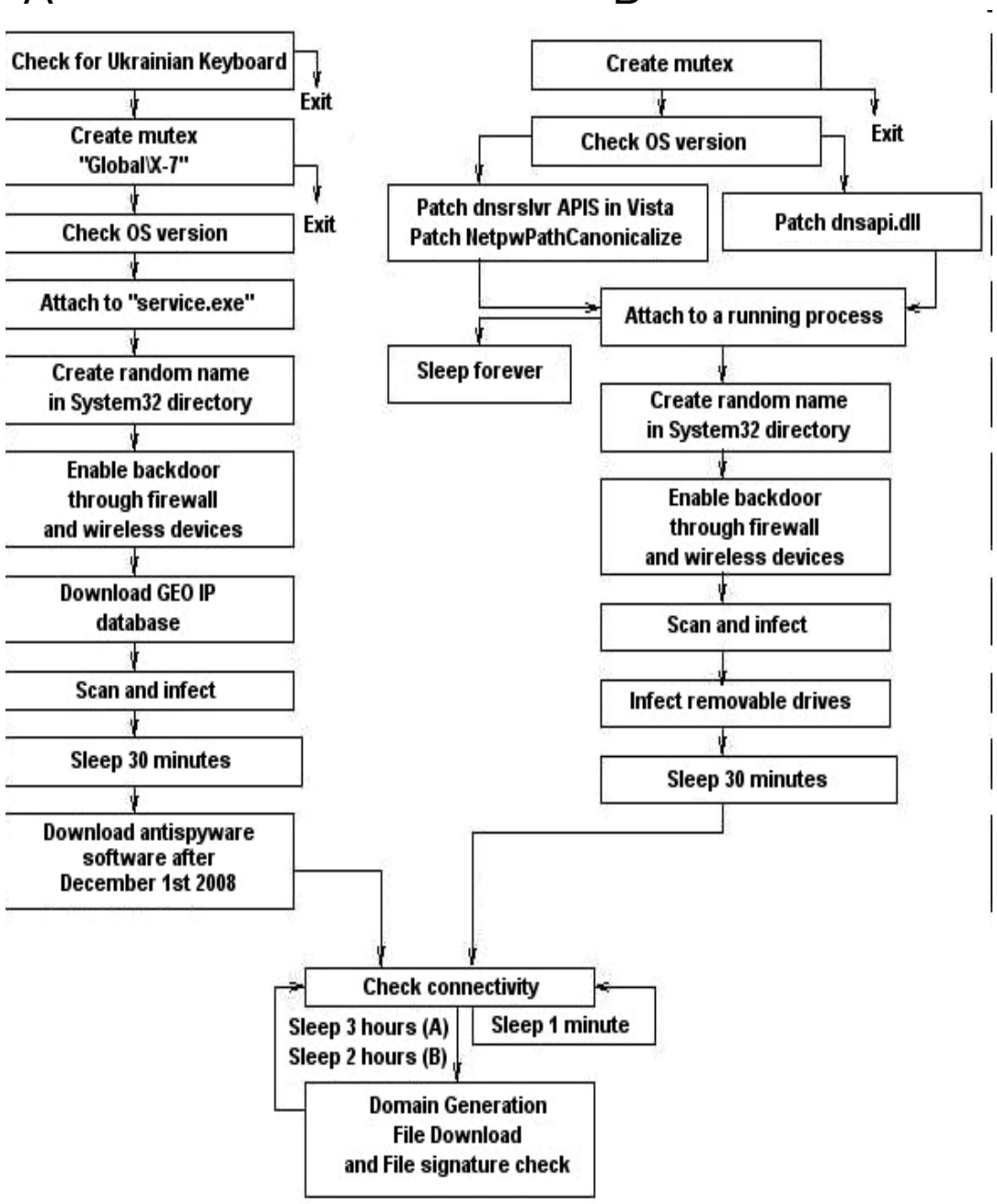
One interesting and minimally explored aspect of Conficker is its early and sophisticated adoption of binary encryption, digital signatures, and advanced hash algorithms to prevent third-party hijacking of the infected population.

- In evaluating this mechanism, we find that the Conficker authors have devised a sophisticated encryption protocol that is generally robust to direct attack.
  - All three crypto-systems employed by Conficker's authors (RC4, RSA, and MD-6) also have one underlying commonality. They were all produced by Dr. Ron Rivest of MIT.
- Furthermore, the use of MD-6 is a particularly unusual algorithm selection, as it represents the latest encryption hash algorithm produced to date.
  - The discovery of MD-6 in Conficker B is indeed highly unusual given Conficker's own development time line.
- We date the creation of Conficker A to have occurred in October 2008, roughly the same time frame that MD-6 had been publicly released by Dr. Rivest (http://groups.csail.mit.edu/cis/md6)
-



group
Cabal
April 1st

Sophistication (dll malware) using sophisticated encryption



For both Conficker, the agent is distributed and run as a dynamically linked library. Its base code has been compiled as a DLL and its DLLMain function initiates the main thread represented by the diagram.

The agent code proceeds by first checking the Windows version, and based on this result creates a remote thread in processes such as svchost.exe.

This is done by invoking LoadLibrary, where the copy of the DLL is passed as an argument.

The malicious library then copies itself in the system root directory under a random file name.

Summit Members

- Paul Vixie
- David Dagon
  - Georgia Tech – thanks for the net/compute nodes
- Florian Weimer
- Wouter Wijngaards
- Andreas Gustaffon
- Microsoft
- Nominum
- OpenDNS
- ISC
- Neustar
- CERT

What about the US government?

D. Kaminski unveiled a critical vulnerability in a critical infra-structure and the summit was organized in a private company (Microsoft) with private professional proposing a fix to be deployed world wide.

Is that OK?