



ICTs for strengthening the economic development

経済発展を強化するための情報通信の技術

Belhassen ZOUARI

General Director, National Agency for Computer Security, Tunisia
Head of the Tunisian Cert (tunCERT),

E-mail : b.zouari@ansi.tn

The Arab-Japan Economic Forum- Tunis, 12 december 2010



Economy, ICTs & Cyber security

- World economies would not survive without adopting ICTs
- Human being activities are more & more ***dependent*** on ICTs (e-commerce, e-gov, social networks, ...)
- *Quality* of ICT products and services would lead to a better life (economic, social)
- *Cyber security* is viewed as a major component of the Quality of ICT products/services



How to ensure an efficient use of ICTs

- Cyber security is a prerequisite to build trust and confidence in e-services
- Cyber security must be addressed globally
- Politics have to be aware of that
- Cyber security Strategy reflects political willing
- Politics have to :
 - Define a National Strategy
 - Provide necessary resources to its implementation



National Strategy Components

- Defining Legal Cyber security Framework
- Cyberspace protection
- Training & Education
- R & D (controlling technologies)
- Awareness
- International Cooperation
- Creating Execution & Implementation mechanisms (Agencies, CERTs, Task force, etc.)



World situation

➤ Need for operational Cybersecurity Centers

FIRST Teams around the world



By countries

By team name

230 Teams across 48 countries



Tunisian Cyber Security Strategy

General objective:

Raising the Security level of Tunisian Information Systems.

Main Axes:

- Updating Legal Cyber Security Framework
- Setting up operational tools to evaluate and to follow up cyber security processes of public and private institutions
- Protecting national cyber space (Coordination, Assistance, etc.)
- Developing a “know-how” in IT Security (training, R&D, open source skills)
- Raising Awareness



Presentation of the Tunisian CERT

tunCERT (formerly CERT-TCC) is a national CERT acting to provide incident management services.

Target users :

Government, Public and Private Sector, Banks, Professionals, Home users, ...

Missions :

- A centralized coordination for IT security issues (Trusted Point of Contact).
- Centralized and specialized unit for **incident response**
- Technology and security **watch**
- Cyberspace **monitoring**
- The expertise to support and assist to quickly **recover** from security incidents.
- Awareness of all categories of users



Watch



Publication of vulnerabilities, exploits, 0days



Collaboration program



Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil



Watch professionals



Collaboration network

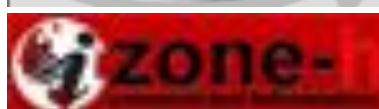


TREND MICRO

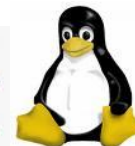
Antivirus suppliers



Professional community



Trend indicators



Equipments constructors



Tunisian Computer Emergency Response Team



Alert & warning process

Collect information

Evaluation

Identification

Classification

Metric

Severity

Distribution

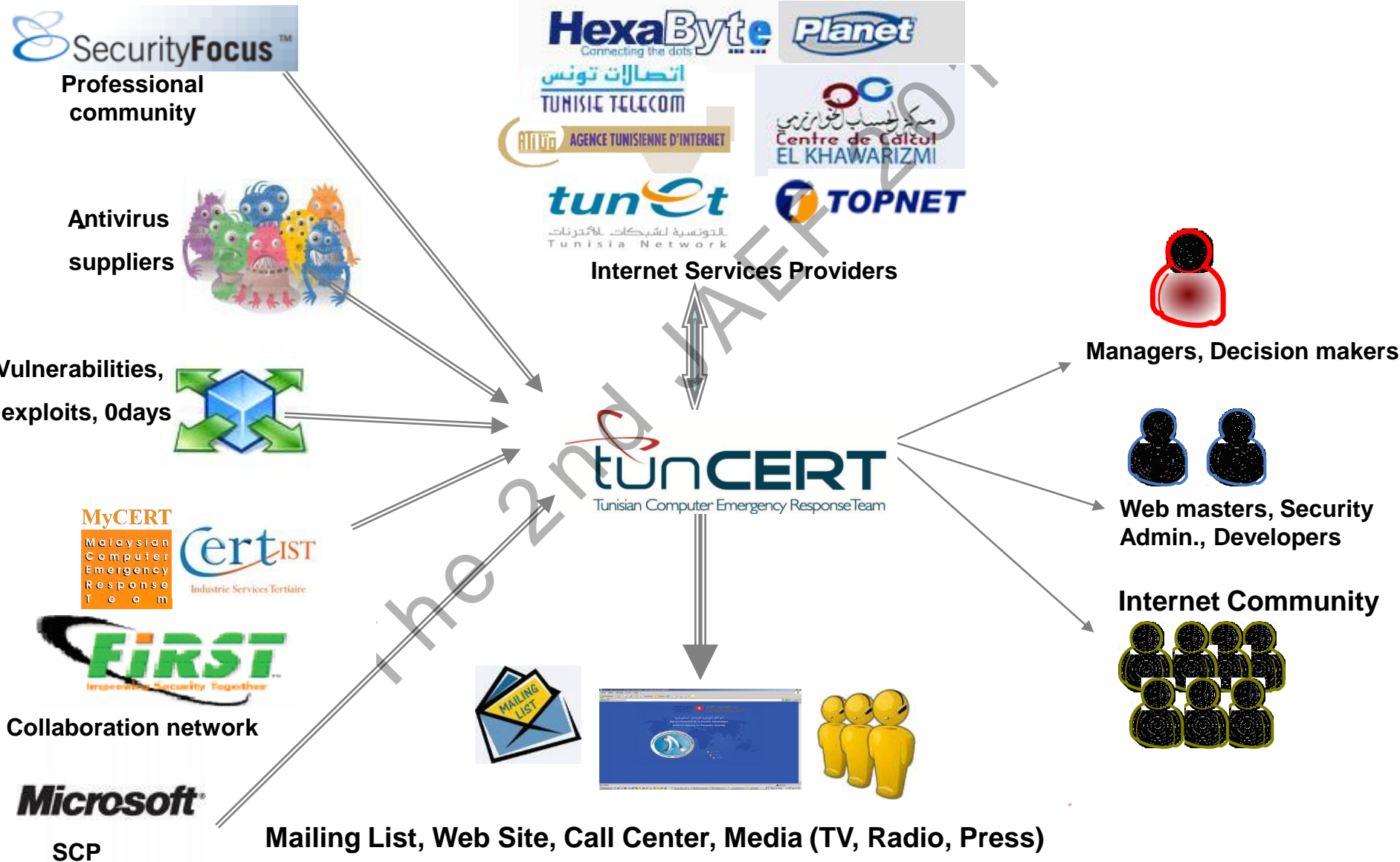
- Public website
- Closed member area on the website
- Mailing lists
- Personalised e-mail
- Phone / Fax
- SMS
- Monthly or annual reports
- Media

- Home user
- Professional
- Customer
- CSO
- Manager
- Webmaster
- Programmer
- Administrator
- etc

Vulnerability, Malware, Attack



Alert & Warning Actors





SAHER : The technical platform

System developed based on a set of Open Source tools

Saher – Web: DotTN Web Sites monitoring

- Web defacement
- DoS Web
- Deterioration of web access
- ...

Saher – SRV: Internet services availability monitoring (Mail server, DNS,...)

- Mail Bombing
- Breakdown of DNS servers
- DNS POISONING...

SAHER-IDS: Massive attack detection

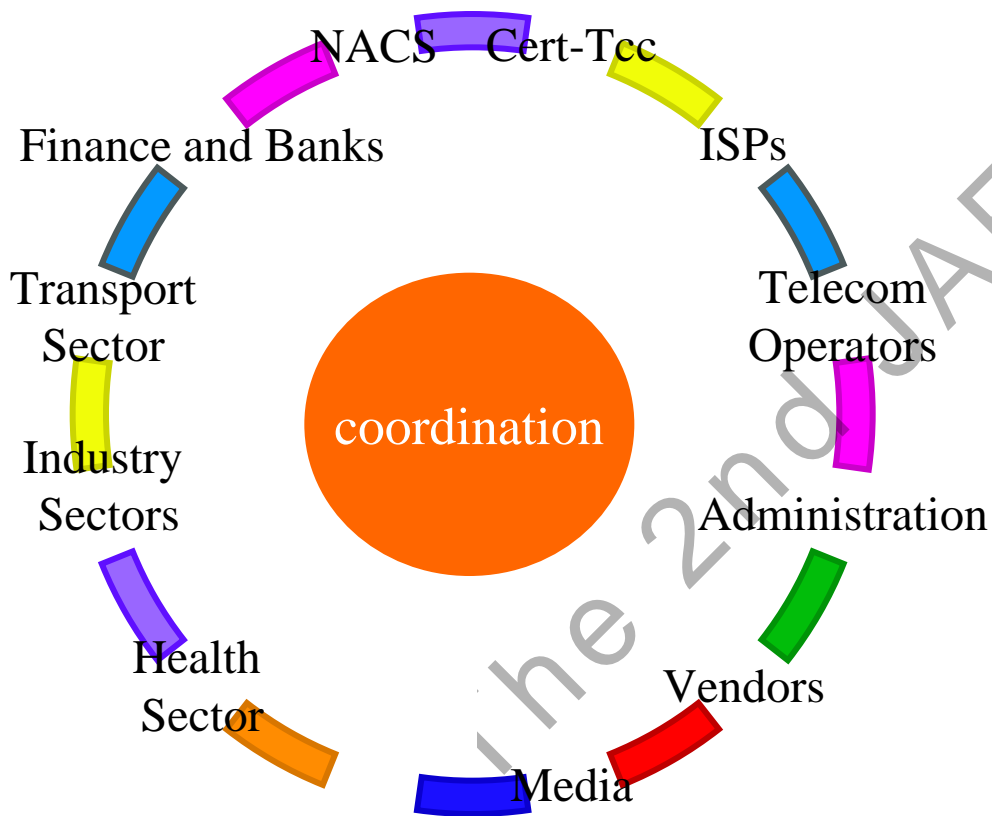
- Viral attack
- Intrusion
- DDoS
- ...

SAHER-HONEYNET: Malware gathering

- Viral attack
- Scan
- Possible attacks



National Reaction Plan



- “Formal” **Global** Reaction Plan.
- Establishment of **Coordinating Crisis Cells** (ISPs, IDCs, Access Providers).

With tunCERT acting as a **coordinator** between them

Deployed several times:

- 2004: African Football Cup
- 2004: 5+5 summit
- 2004: Sasser & MyDoom worms
- 2004: Presidential election
- 2005: Suspicious hacking activity 2005
- 2005: WSIS
- 2005: Arab League Meeting
- 2006 : Hand Ball World Cup
- 2009: Conficker



Other Missions

- NACS acts as a Security Expert for the government. It is involved in the main national IT projects.
- Training and Support in the fields of Cyber Security.
- Rising Awareness
(Decision makers, Professionals, Teachers, Students, Home users, Journalists, Lawyers, Customers, etc.)

Flyers, Posters, Emails, Radio Emission, Cartoon, Video Spot, Attack Simulation Guide



Thank you

The 2nd JAERT 2011