CERT-TCC

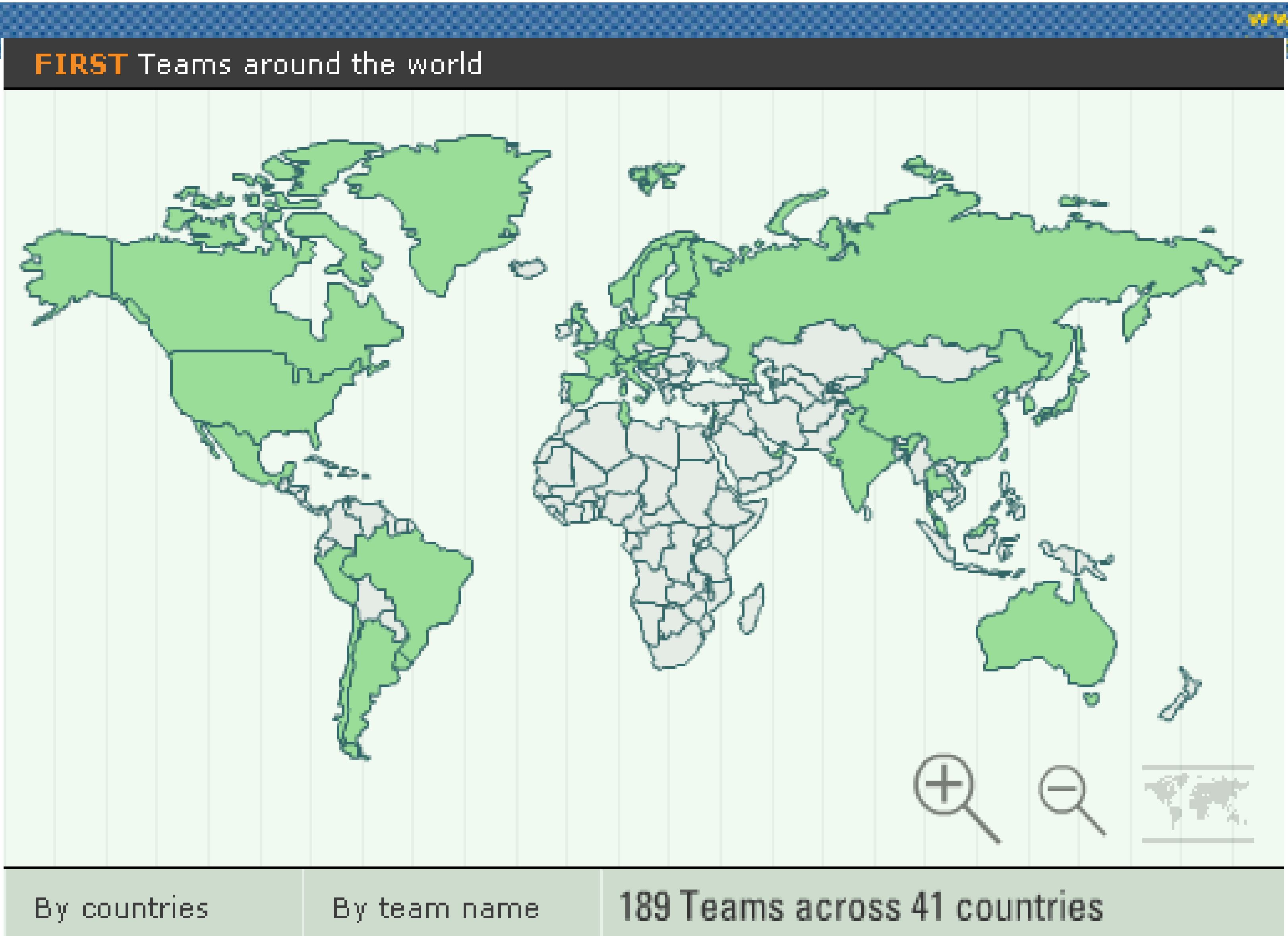
Computer Emergency Response Team- Tunisian Coordination Center

Fast overview about the CERT-TCC

Helmi Rais

CERT-TCC Team Manager

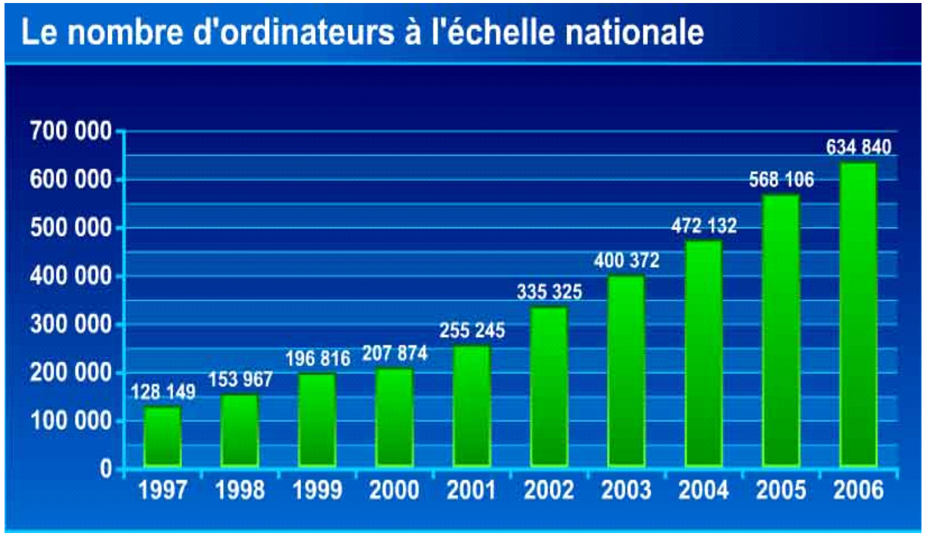
Helmi.rais@ansi.tn

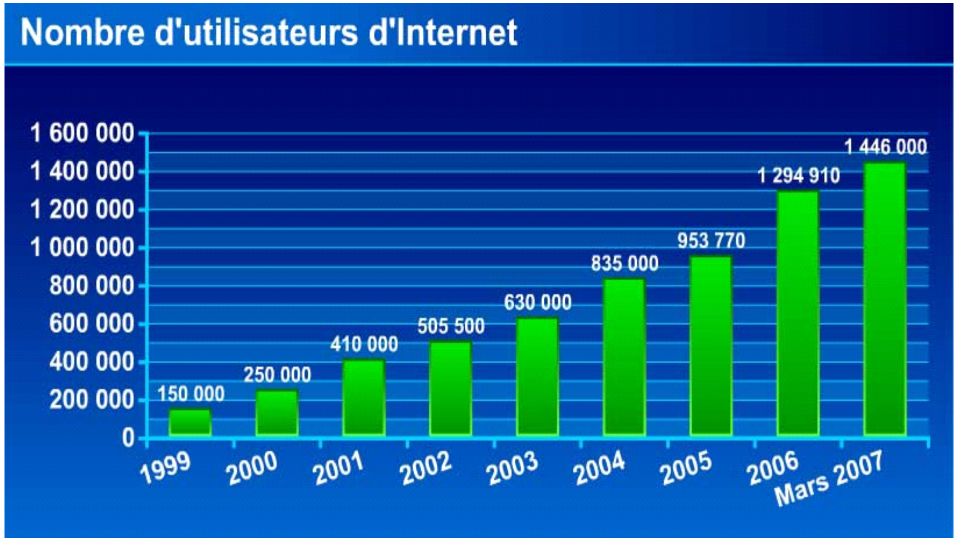


FIRST Teams around the world

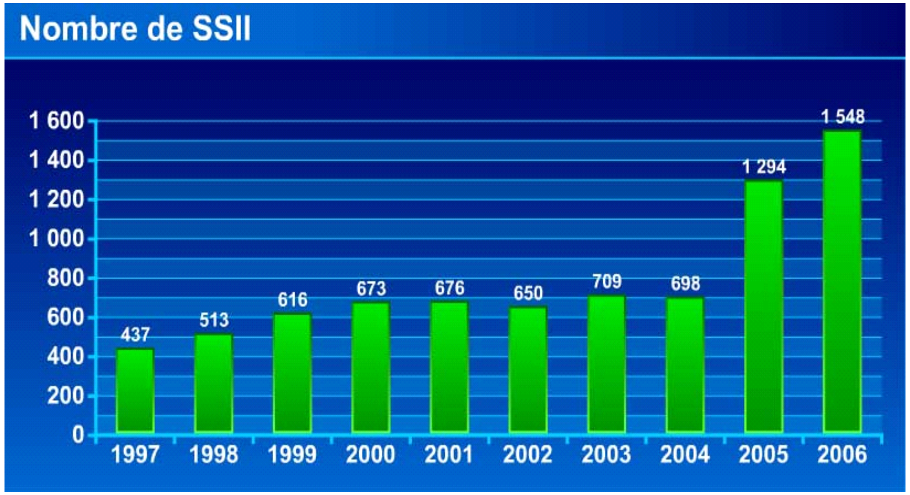
189 Teams across 41 countries

Les IT en Tunisie: Quelques Statistiques

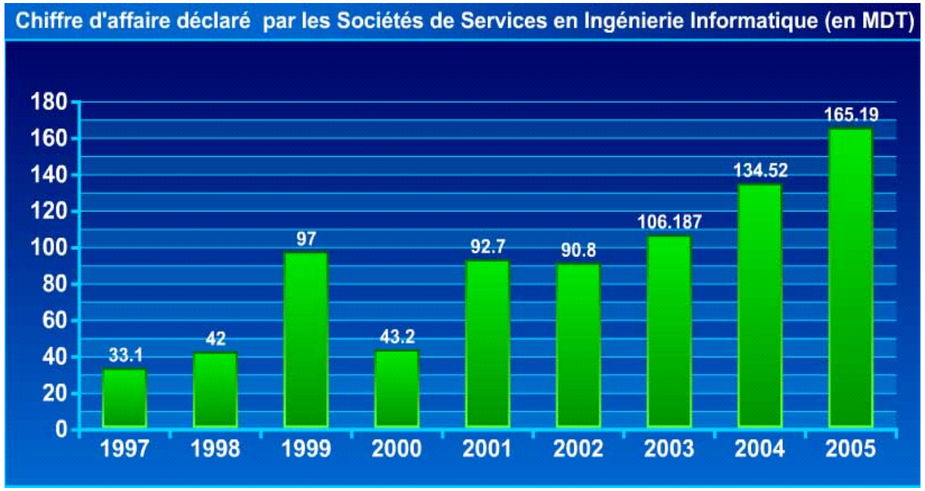

Le nombre d'ordinateurs à l'échelle nationale


Nombre d'utilisateurs d'Internet

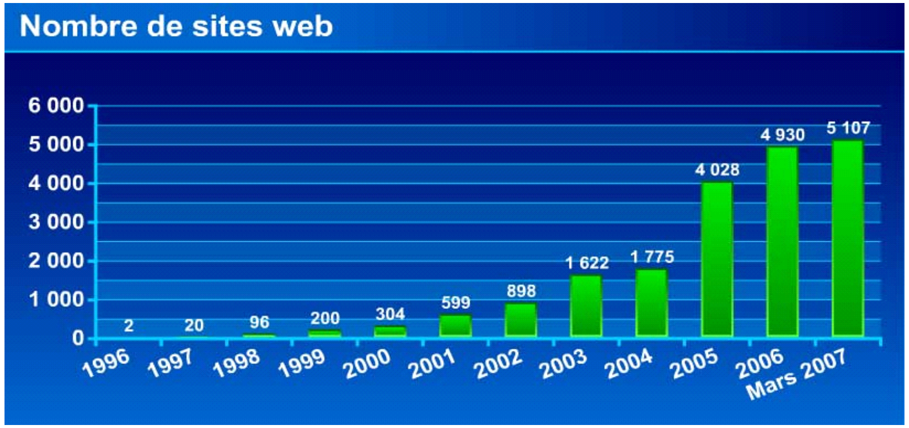
Les IT en Tunisie: Quelques Statistiques



Nombre de SSII



Chiffre d'affaire déclaré par les Sociétés de Services en Ingénierie Informatique (en MDT)



Nombre de sites web

a fast Historical Overview

❑ end **<u>1999 :</u>** Launch of a **<u>UNIT (a "Micro-CERT")</u>** , specialized in IT Security

Objective :

- **sensitize policy-makers and Technical staff about security issues**.
- Assists in Monitoring the security of highly critical national applications and infrastructures..

+ ***creates a first Task-force of Tunisian Experts in IT Security***

❑ From **<u>End 2002</u>** (" **certification of the role of IT security as a pillar of the « Information Society** ») **<u>:</u>**

➢ The unit starts the establishment of a **strategy** and of a **National Plan** in IT Security

(**national survey** , for fixing: priorities, volume of actions, needed logistic, supporting tools, .).

❑ **January 2003 :**

- **Decision of the Council of Ministers, headed by the President, and dedicated to informatics and IT Security , of :**

❑ The creation of a National Agency, specialized in IT Security

(The Tool for the execution of the national strategy and plan)

❑ The Introduction of Mandatory and Periodic Security audits

(Pillar of our strategy)

❑ The creation of a "body of certified Auditors" in IT Security

+ A lot of accompanying measures (launch of masters in IT security, …)

In addition of existent Laws :

Ø Law on protection of **Privacy and Personal data** **(Law n° 2004-63)**
Ø Law on **Electronic Signature and e-commerce** **(Law N° 2000-83)**
Ø Law **Against Cyber-Crimes** **(Law N° 1999-89, Art 199)**
Ø **Law on consumer protection and respect of Intellectual property** **(Law N°1994-36)**

✓ February **2004** : **Promulgation of an "*original*" LAW,** on **computer security**
(Law N° 5-2004 ***and 3 relatives decrees***) :

Obligation for national companies (ALL public + "big" and sensitive private ones) to do **Periodic (Now annually) Security audits of their IS.**

➢ **Organization of the field of Security audits**

→ Audits are Made by **CERTIFIED auditors** ***(from the private sector***),
→ *definition of the process of certification of auditors*
→ *definition of the auditing missions and process of follow-up (***ISO 1 77 99***)*

➢ *Creation and definition of the Missions of the* **National Agency for Computer Security (which does not deal with National Security & Defense issues)**
(created under the **Ministry of Communication Technologies)**

➢ **Obligation to declare** security Incidents (Viral, mass hacking attacks, ..) that could affect **others** IS, with guarantee of **confidentiality**, by law.

- CERT-TCC is a sub-structure of the National Agency for Computer Security

- CERT-TCC is the Gov Tunisian CERT

CERT-TCC

Watch, Warning & Awarness Team

Investigation & Incident Response Team

Information Sharing and Analysis Center

CERT-TCC

Watch, Warning & Awarness Team

Investigation & Incident Response Team

Information Sharing and Analysis Center

Services Provided

- Information and alert
- Education and awareness
- Enterprise support (security self-assessment)
- Electronic Surveys on security and Participation in International organizations
- Training

Services Provided

Information and Alert

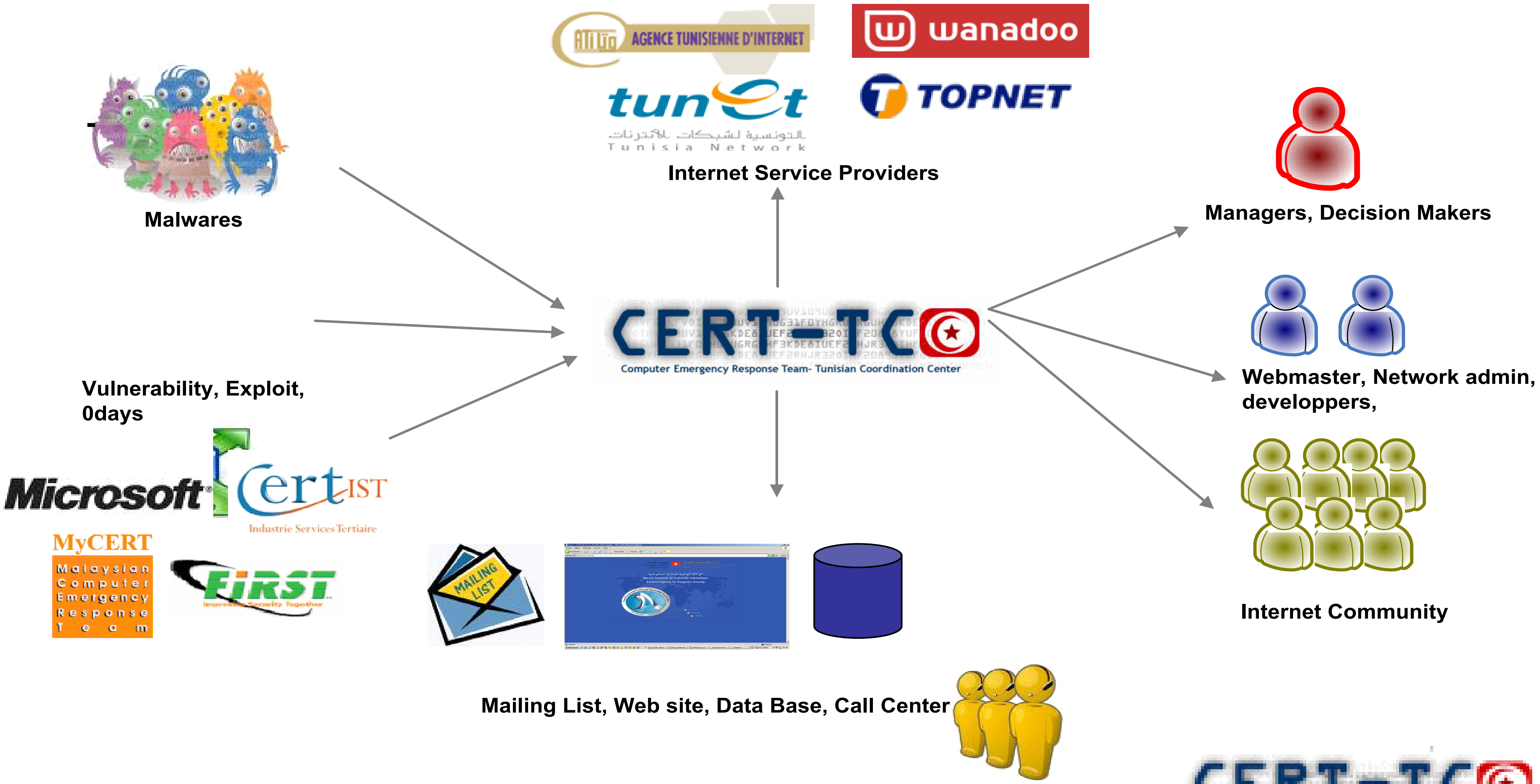
Threat alert :

• Analyse the state of Internet security and convey that information to the system administrators, network managers, and wide public in the Internet community.

• Monitor sources of vulnerability information and regularly sends reports and alerts on those vulnerabilities (mailing-lists, publication on the web site).

• We analyze the potential vulnerability and try to work with other CERTs and technology producers to track the solutions to these problems. We also make vulnerability information widely available through a vulnerability database.

Information & Alert


AGENCE TUNISIENNE D'INTERNET
wanadoo
tunet
التونسية لشبكات الأنترنات
Tunisia Network
TOPNET
CERT-TCC
Computer Emergency Response Team- Tunisian Coordination Center
Microsoft
CertIST
Industrie Services Tertiaire
MyCERT
Malaysian Computer Emergency Response Team
FIRST
Improving Security Together
MAILING LIST

Internet Service Providers

Malwares

Vulnerability, Exploit, 0days

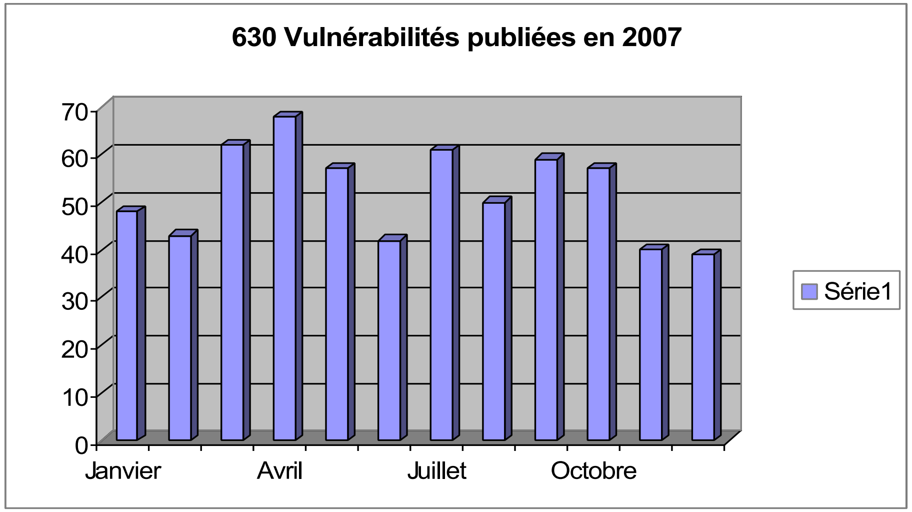
Managers, Decision Makers

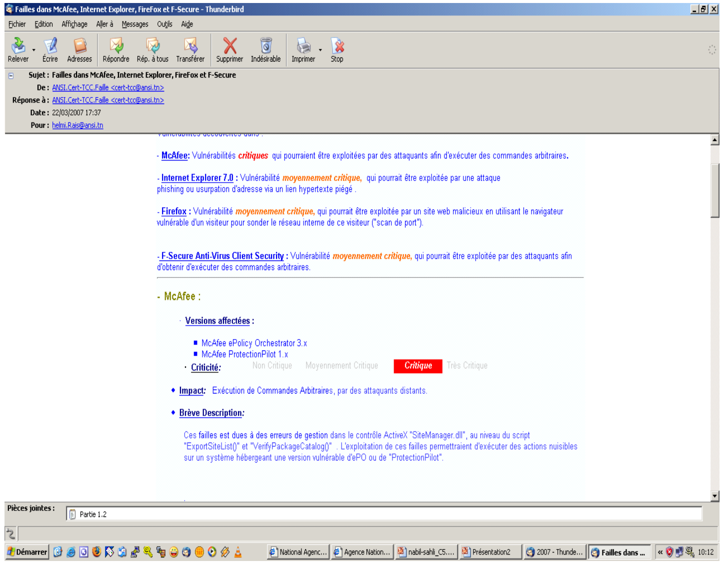
Webmaster, Network admin, developpers,

Internet Community

Mailing List, Web site, Data Base, Call Center

- 630 Vulnerabilities published in 2007
- 25 Malwares published in 2007





Sujet : Failles dans McAfee, Internet Explorer, FireFox et F-Secure
De : ANSI.Cert-TCC.Faille <cert-tcc@ansi.tn>
Réponse à : ANSI.Cert-TCC.Faille <cert-tcc@ansi.tn>
Date : 22/03/2007 17:37
Pour : helmi.Rais@ansi.tn

Vulnérabilités découvertes dans :

- **McAfee:** Vulnérabilités ***critiques*** qui pourraient être exploitées par des attaquants afin d'exécuter des commandes arbitraires.

- **Internet Explorer 7.0 :** Vulnérabilité ***moyennement critique,*** qui pourrait être exploitée par une attaque phishing ou usurpation d'adresse via un lien hypertexte piégé .

- **Firefox :** Vulnérabilité ***moyennement critique,*** qui pourrait être exploitée par un site web malicieux en utilisant le navigateur vulnérable d'un visiteur pour sonder le réseau interne de ce visiteur ("scan de port").

- **F-Secure Anti-Virus Client Security :** Vulnérabilité ***moyennement critique,*** qui pourrait être exploitée par des attaquants afin d'obtenir d'exécuter des commandes arbitraires.

- McAfee :

- **Versions affectées :**
  - McAfee ePolicy Orchestrator 3.x
  - McAfee ProtectionPilot 1.x
- **Criticité:** Non Critique Moyennement Critique ***Critique*** Très Critique
- **Impact:** Exécution de Commandes Arbitraires, par des attaquants distants.
- **Brève Description:**

Ces failles est dues à des erreurs de gestion dans le contrôle ActiveX "SiteManager.dll", au niveau du script "ExportSiteList()" et "VerifyPackageCatalog()" . L'exploitation de ces failles permettraient d'exécuter des actions nuisibles sur un système hébergeant une version vulnérable d'ePO ou de "ProtectionPilot".

Pièces jointes : Partie 1.2

13 Minor Alerts in 2007

- Microsoft Word 0day **(CERT-TCC/Vuln.2007-045)**
- Sun Solaris Worm **(CERT-TCC/Vuln.2007-66)**
- Microsoft Windows DNS Service **(CERT-TCC/Vuln.2007-190)**
- Firefox et Netscape Navigator 0day **(CERT-TCC/Vuln.2007-368)**
- Propagation of "Storm Worm" "Zhelatin.LJ **(CERT-TCC/MAL-2007-009)**
- *RSTP QuickTime* Vulnerability **(CERT-TCC/Vuln.2007-577)**

- *Netmonster* : *The First Virus « made in Tunisia »* **(CERT-TCC/Malw.2007-023)**

- More than **7000 _Voluntary_** subscribers
- More than **800** calls Monthly served
- More than **600** e-mails sent Since 2005
  - Vulnerabilities
  - Malwares
  - Spam &Hoax
  - Open Source
  - Books
  - Tools
  - Announces

Services Provided

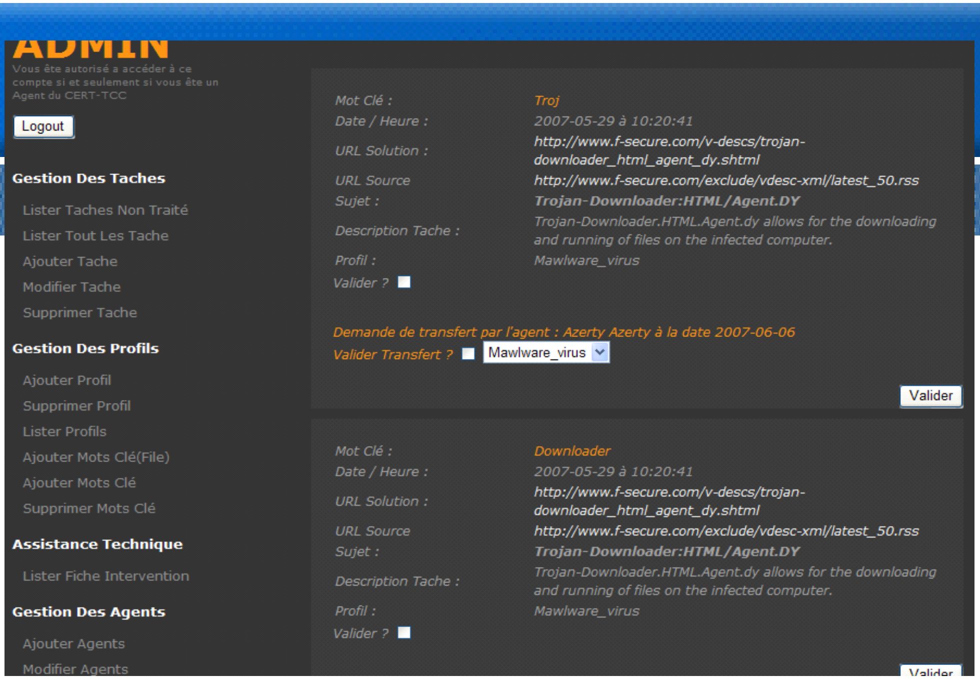
Information and Alert

Information :

To increase awareness of security issues and help organizations to improve the security of their systems, we collect and disseminate information through multiple channels (mailing-lists, World Wide Web site, brochures and Knowledge bases, News).

More than 30 Guides and Manuals

Home Users
Open Source Solutions
Best Practices
Security Policy
Security Chart
Technical Documents / Tips
Technical specification models for security solution acquisitions
Tender of offers for Security Audit Missions



ADMIN

Vous être autorisé à accéder à ce compte si et seulement si vous ête un Agent du CERT-TCC

Logout

Gestion Des Taches

- Lister Taches Non Traité
- Lister Tout Les Tache
- Ajouter Tache
- Modifier Tache
- Supprimer Tache

Gestion Des Profils

- Ajouter Profil
- Supprimer Profil
- Lister Profils
- Ajouter Mots Clé(File)
- Ajouter Mots Clé
- Supprimer Mots Clé

Assistance Technique

- Lister Fiche Intervention

Gestion Des Agents

- Ajouter Agents
- Modifier Agents

Mot Clé : Troj
Date / Heure : 2007-05-29 à 10:20:41
URL Solution : http://www.f-secure.com/v-descs/trojan-downloader_html_agent_dy.shtml
URL Source http://www.f-secure.com/exclude/vdesc-xml/latest_50.rss
Sujet : ***Trojan-Downloader:HTML/Agent.DY***
Description Tache : Trojan-Downloader.HTML.Agent.dy allows for the downloading and running of files on the infected computer.
Profil : Mawlware_virus
Valider ? □

Demande de transfert par l'agent : Azerty Azerty à la date 2007-06-06
Valider Transfert ? □ Mawlware_virus

Valider

Mot Clé : Downloader
Date / Heure : 2007-05-29 à 10:20:41
URL Solution : http://www.f-secure.com/v-descs/trojan-downloader_html_agent_dy.shtml
URL Source http://www.f-secure.com/exclude/vdesc-xml/latest_50.rss
Sujet : ***Trojan-Downloader:HTML/Agent.DY***
Description Tache : Trojan-Downloader.HTML.Agent.dy allows for the downloading and running of files on the infected computer.
Profil : Mawlware_virus
Valider ? □

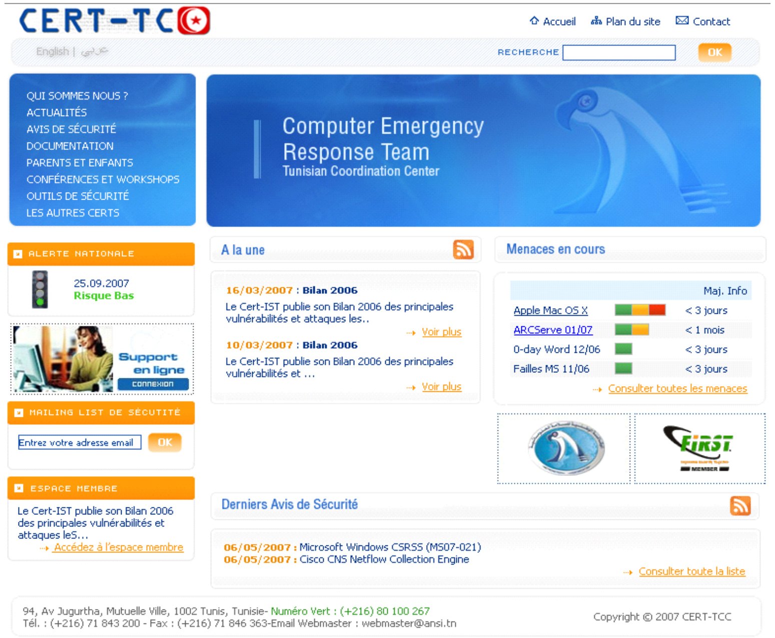
Valider

Internal Workflow Solutions

Chater (Smart in Arabic) شاطر

RSS Reader , Filter, Task Management

→ Free and Open Source



25.09.2007
Risque Bas

Le Cert-IST publie son Bilan 2006 des principales vulnérabilités et attaques leS…
Accédez à l'espace membre

A la une

16/03/2007 : Bilan 2006
Le Cert-IST publie son Bilan 2006 des principales vulnérabilités et attaques les..
Voir plus

10/03/2007 : Bilan 2006
Le Cert-IST publie son Bilan 2006 des principales vulnérabilités et …
Voir plus

Menaces en cours

		Maj. Info
Apple Mac OS X	🟩🟧🟥	< 3 jours
ARCServe 01/07	🟩🟧	< 1 mois
0-day Word 12/06	🟩	< 3 jours
Failles MS 11/06	🟩	< 3 jours

Consulter toutes les menaces

Derniers Avis de Sécurité

06/05/2007 : Microsoft Windows CSRSS (MS07-021)
06/05/2007 : Cisco CNS Netflow Collection Engine
Consulter toute la liste

94, Av Jugurtha, Mutuelle Ville, 1002 Tunis, Tunisie- Numéro Vert : (+216) 80 100 267
Tél. : (+216) 71 843 200 - Fax : (+216) 71 846 363-Email Webmaster : webmaster@ansi.tn

Copyright © 2007 CERT-TCC

Vulnerability and Malwrae Database into CERT-TCC Back Office Website

Services Provided

Awareness Activities

- Decision Makers
- CSOs
- Professionals
- Technicians / Engineer
- Trainers
- Students
- Tunisian Cyber Community
- Home Users
- Journalists
- Jurists

Hacking Simulation

Trojans

Vulnerability Exploits

Phishing attacks

XSS

SQL Injection

Password Sniff

Services Provided

Awareness

- ***Publications :*** we also reproduce or develop and publish free electronic publications (guides, ..), to show administrators how to protect systems and networks against malicious and inadvertent compromise.

- ***Media information :*** We also work with the news media, and give them the necessary information material and support to raise the awareness of a broad population to the risks they face on the Internet and steps they can take to protect themselves.

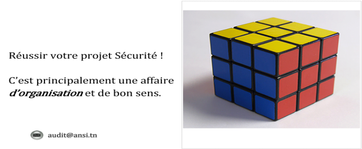
- ***Presentations :*** We organize and regularly give presentations at conferences, workshops, and meetings, as an excellent way to help attendees to learn more in the area of network information system security.

Weekly participation in 8 National Radios and

1 TV Program

Agence Nationale de la Sécurité Informatique
CERT-TCC
Computer Emergency Response Team
Tunisian Coordination Center

4 AW cdroms



Réussir votre projet Sécurité !

C'est principalement une affaire *d'organisation* et de bon sens.

audit@ansi.tn

2008 Calendar

8 aw booklets

Services Provided

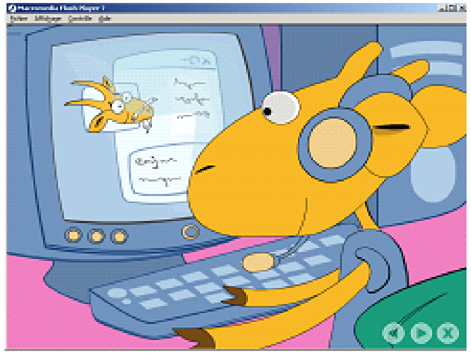
Youth and Parents Awareness

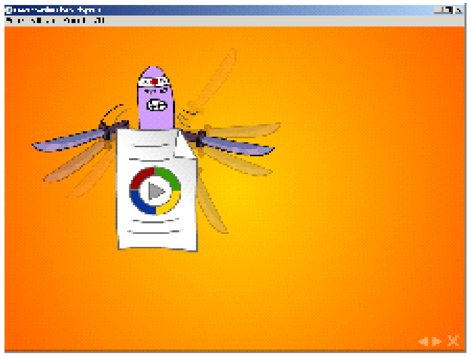
- Acts for raising **Youth and parents awareness ,**In Collaboration with specialized centers and associations :

  - Preparation of a first pack of short (awareness) courses for Primary school.
  - Starts the Development of special pedagogical material for childrens&parents : 3 “Cartoons”, Quizs

- Development of a special rubric in the Web site and Inclusion of a special Mailing-List rubric for parents **(**Parental control tools, risks, ..)

- ***Development of special awareness tools (Cdroms, Cartoons, Games, Booklets…)***





- Acting in **Raising awareness about the benefits (&limits) of the deployment of open-source tools.**

- Formulation (funds) of **4 projects for the development of security tools (from open-source**) for the **private sector** (including improvement of the system “Saher”).

- Definition of **5 federative projects of Research&Development** for **academic laboratories** (under the supervision of the **Ministry of Scientific Research**)

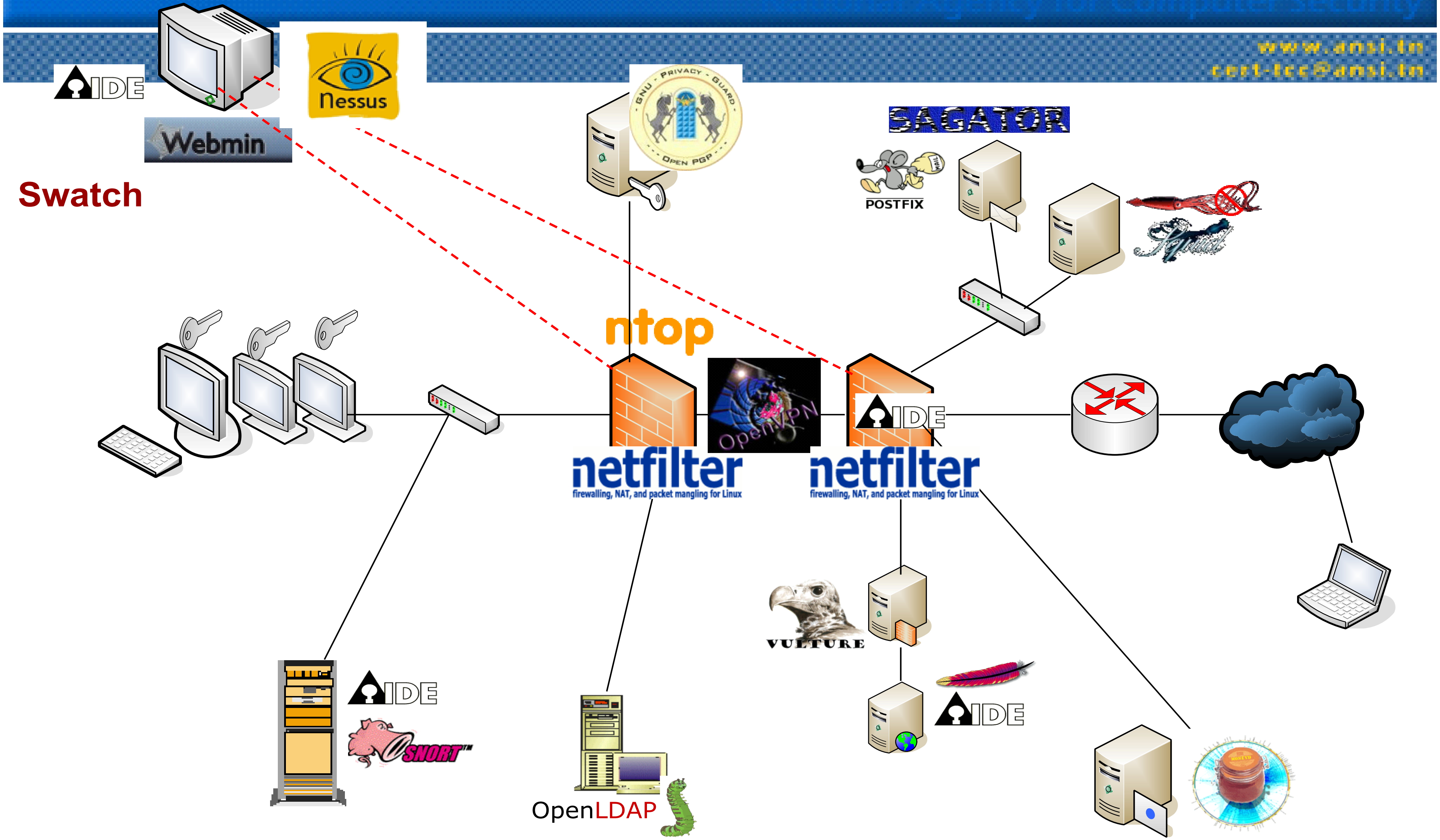
- Collaboration, with the university for the launch of a **Research laboratory** specialized in open-source security tools (Loan from the World Bank).

CERT/TCC is Acting for sensitizing young investors (by providing “Markets”),to:

First Step : Provides support for open-source tools deployment (installation, training, “maintenance”)

Then → Customization of open-source solutions (for clients specific needs)

End → Launch of real Research/Development activities


AIDE
Webmin
Nessus
Swatch
GNU Privacy Guard
Open PGP
SAGATOR
POSTFIX
Squid
ntop
OpenVPN
AIDE
netfilter
firewalling, NAT, and packet mangling for Linux
netfilter
firewalling, NAT, and packet mangling for Linux
VULTURE
AIDE
AIDE
SNORT
OpenLDAP

Services Provided

Training

Our urgent and big problem is the present lack of specialized experts and trainers in the various fields of information system security. This CERT is first concentrated on the organization of trainings (in Tunisia and in International institutes) for trainers in the field of specialized Information systems security trends and also for the judicial and investigation staff.

Afterwards, we organize very specialized training courses in Tunisia (and some in foreign centers) for technical staff and managers of computer security incident response teams as well as for system administrators of highly critical systems.

Services Provided

Training

- Network perimeter security technics (Secure architectures, Firewalls, IDS, secure dial-up servers, content gateways and proxies, ..) .
- Internal Network security organization and technics (security policy development, security plan development, tools : Distributed firewalls, Anti-virus gateways, PKI, ..).
- Technical basis for intrusion prevention (identifying and preventing intrusions and security flaws).
- Fundamentals of Incident Handling and overview of a Computer Security Incident Response Team
- Creating and Managing a Computer Security Incident Response Team
- Methodologies of security self-assessment.
- ISO 17799 and ISO 27000 Families.
- Wireless Security
- CBK Security
- Open Source Solutions
- Intergrating Security into SDLC
- Specialized courses for judicial and investigation staff

CERT-TCC

Watch, Warning & Awarness Team

Investigation & Incident Response Team

Information Sharing and Analysis Center

Services Provided

Incident handling and assistance

CERT/TCC provides :

o **A CSIRT team** in charge of providing (free of charge) **Assistance for Incident Handling**
o Call-center, **available 24Hours/24 and 7 days/week**

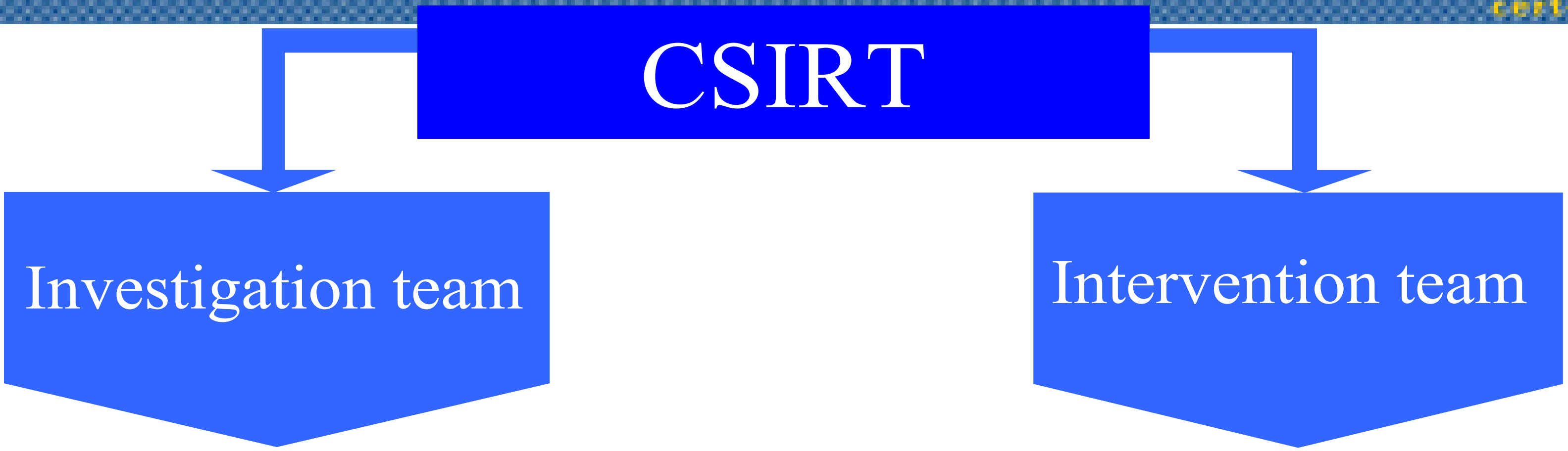
<u>Article 10</u> of the Law No. 2004-5 relative to IT security
(Public & Private institutions, <u>must</u> inform the National Agency for Computer Security about any Incident, which can affect other Information Systems)

<u>Article 9</u> of the Law No. 2004-5 relative to IT security Stipulate that
The employees of the National Computer Security Agency and security auditors <u>are Responsible about the preservation of confidentiality</u> and are liable to penal sanctions

→ Private and public organizations should **trust** the CERT/TCC
→ **Call for assistance**

- A "**Citizen's assistance service** ", To which Home users can bring their PC to solve security problems or install security tools (anti-virus, PC firewall, anti-spam, ..), free for domestic use.

- Acting for the emergence of corporate CSIRT in some sensitive sectors (E-gov, E-Banking → Energy, Transportation, Health)



CSIRT

Investigation team

- Computer forensics
- Evidence analysis
- Investigation (Log, Hard Drive, memory dump, …)

Intervention team

- On-site
- Incident handling process
- Evidence collection

CERT-TCC

Watch, Warning & Awarness Team

Investigation & Incident Response Team

Information Sharing and Analysis Center

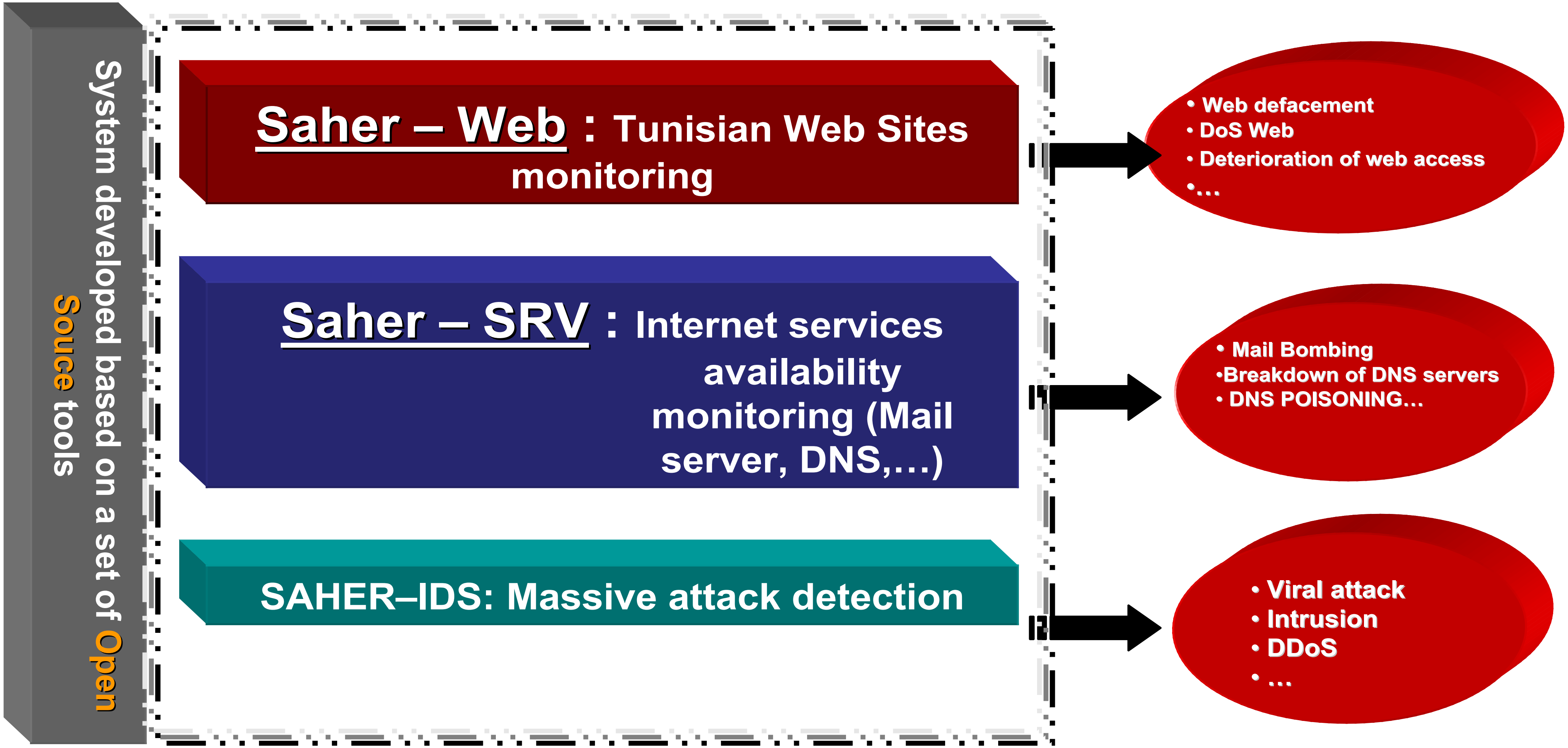
ISAC “Saher”

A **Watch- center** (based on **open-source solutions),** which permits to monitor the National Cyber-Space security in **Real time**

→ For the early Detection of **potential** threats and evaluation of their impact.
(First prototype, deployed at the level of ISP, during phase 2 of WSIS)

→ **For Vulnerabilities exploitation and malwares propagation evals**

« Saher » Architecture



System developed based on a set of Open Souce tools

Saher – Web : Tunisian Web Sites monitoring

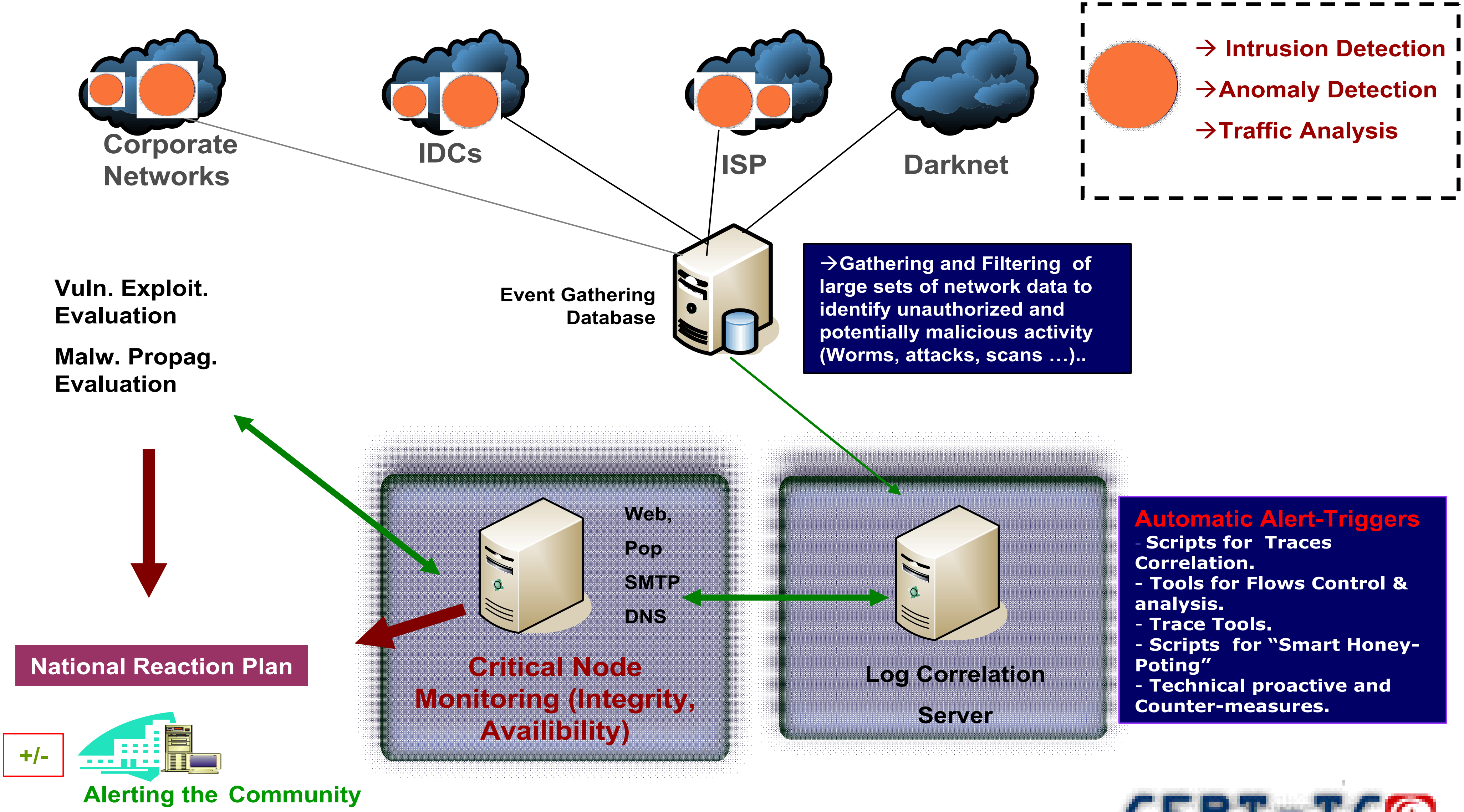
- Web defacement
- DoS Web
- Deterioration of web access
- …

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
- …



Corporate Networks

IDCs

ISP

Darknet

→ Intrusion Detection

→Anomaly Detection

→Traffic Analysis

Event Gathering Database

→Gathering and Filtering of large sets of network data to identify unauthorized and potentially malicious activity (Worms, attacks, scans …)..

Vuln. Exploit. Evaluation

Malw. Propag. Evaluation

Web,

Pop

SMTP

DNS

Critical Node Monitoring (Integrity, Availibility)

Log Correlation Server

Automatic Alert-Triggers

- Scripts for Traces Correlation.
- Tools for Flows Control & analysis.
- Trace Tools.
- Scripts for "Smart Honey-Poting"
- Technical proactive and Counter-measures.

National Reaction Plan

+/-

Alerting the Community

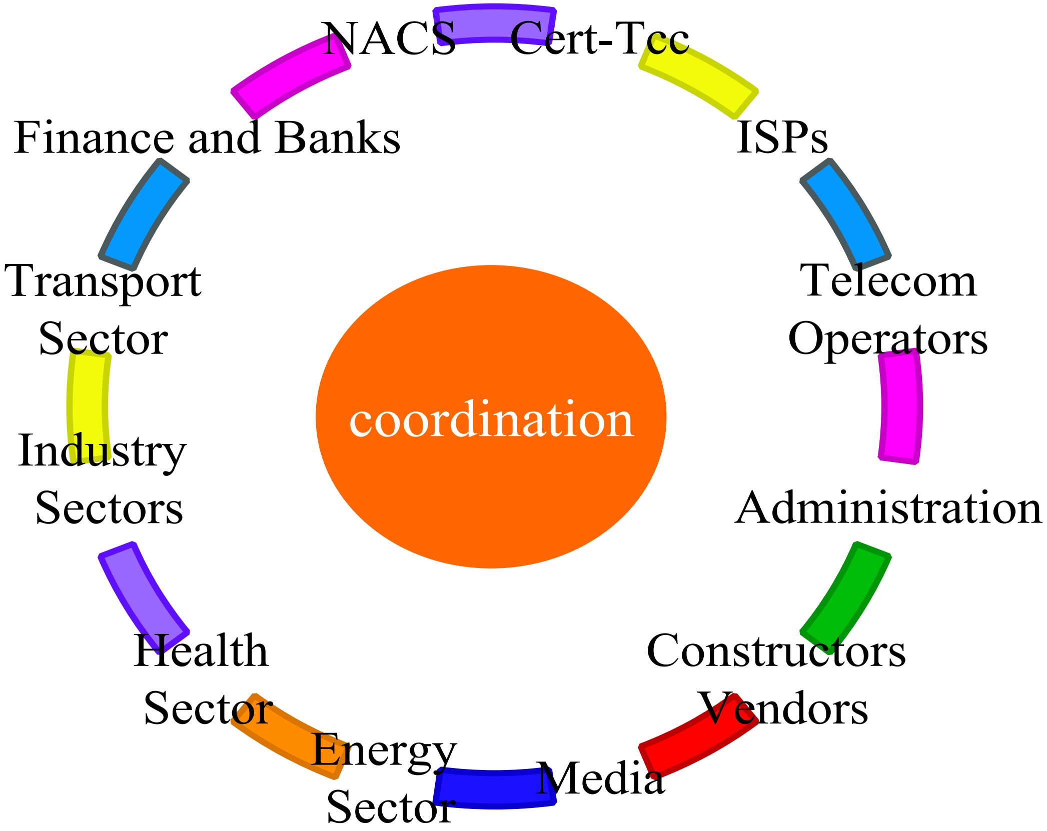
NRP
National Reaction Plan

Alert Handling Plan "Amen"

- "Formal" **Global** Reaction Plan.

- Establishment of **Coordinating Crisis Cells** (ISPs, IDCs, Acess Providers).

With CERT/TCC acting as a **coordinator** between them



NACS

Cert-Tcc

ISPs

Telecom Operators

Administration

Constructors Vendors

Media

Energy Sector

Health Sector

Industry Sectors

Transport Sector

Finance and Banks

coordination

was deployed 7 times,

During Sasser& MyDoom worms attack, during suspicious hacking activity and, proactively, during big events hosted by Tunisia (only with ISPs and telecommunication operator)

sommet mondial sur
la société de l'information
Genève 2003 - Tunis 2005

ONU Conference about Terrorism