Country Case Study on Incident Management Capabilities

CERT-TCC, Tunisia

Helmi Rais

CERT-TCC Team Manager

National Agency for Computer Security, Tunisia

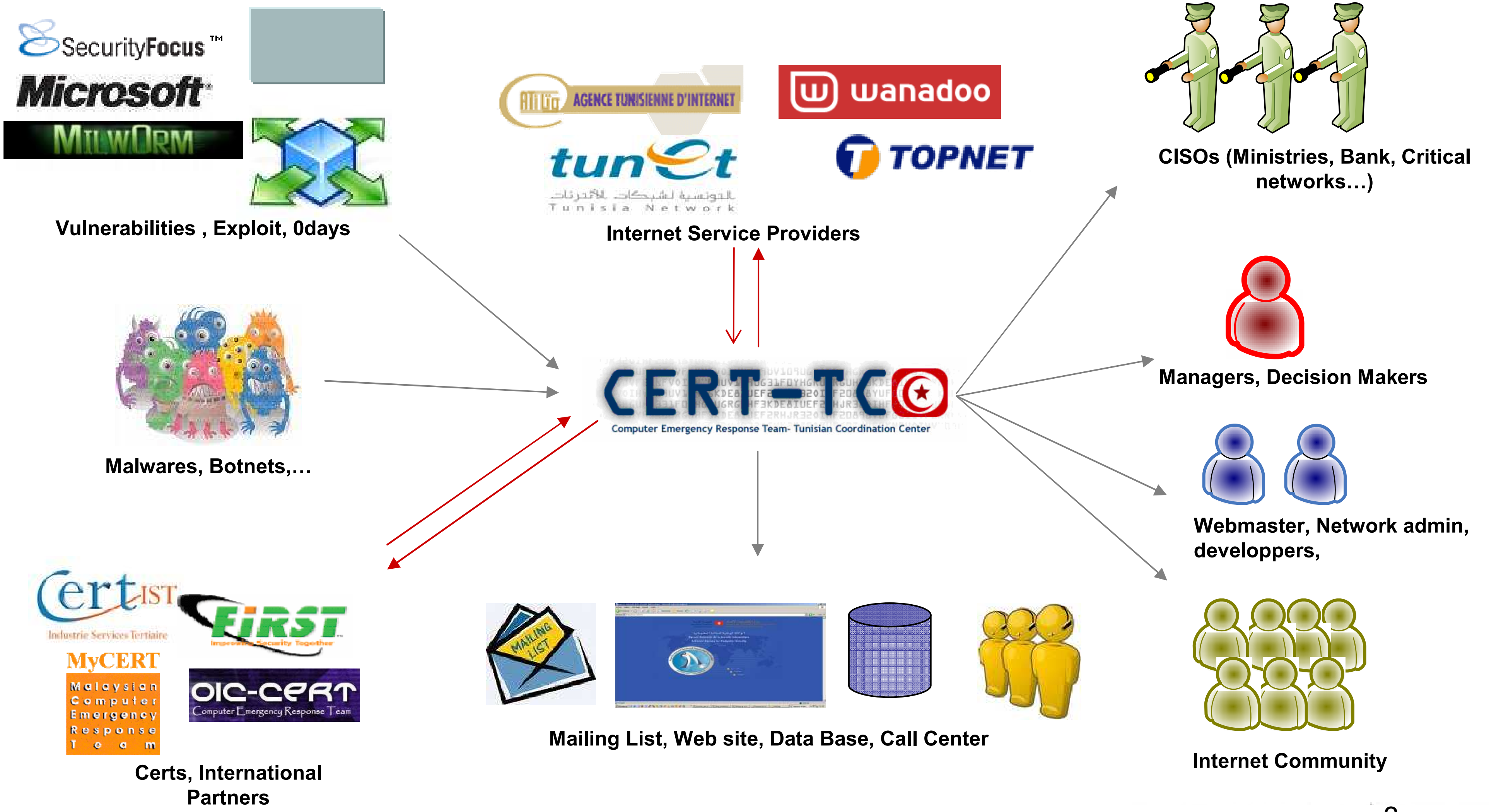
helmi.rais@ansi.tn helmi.rais@gmail.com

Framework

CERT-TCC Collaboration Network

N.A.C.S

www.ansi.tn
cert-tcc@ansi.tn


SecurityFocus
Microsoft
MILW0RM
AGENCE TUNISIENNE D'INTERNET
tunet
Tunisia Network
wanadoo
TOPNET
CERT-TCC
Computer Emergency Response Team- Tunisian Coordination Center
CertIST
Industrie Services Tertiaire
FIRST
Improving Security Together
MyCERT
Malaysian Computer Emergency Response Team
OIC-CERT
Computer Emergency Response Team
MAILING LIST

Vulnerabilities , Exploit, 0days

Internet Service Providers

CISOs (Ministries, Bank, Critical networks…)

Managers, Decision Makers

Malwares, Botnets,…

Webmaster, Network admin, developpers,

Certs, International Partners

Mailing List, Web site, Data Base, Call Center

Internet Community

Watch, Warning, Information & Alert

Investigation & Incident Response Team

Information Sharing and Analysis Center

Watch, Warning, Information & Alert

Investigation & Incident Response Team

Information Sharing and Analysis Center

CERT-TCC Watch Center (24/7)

Information and Alert

Threat alert :

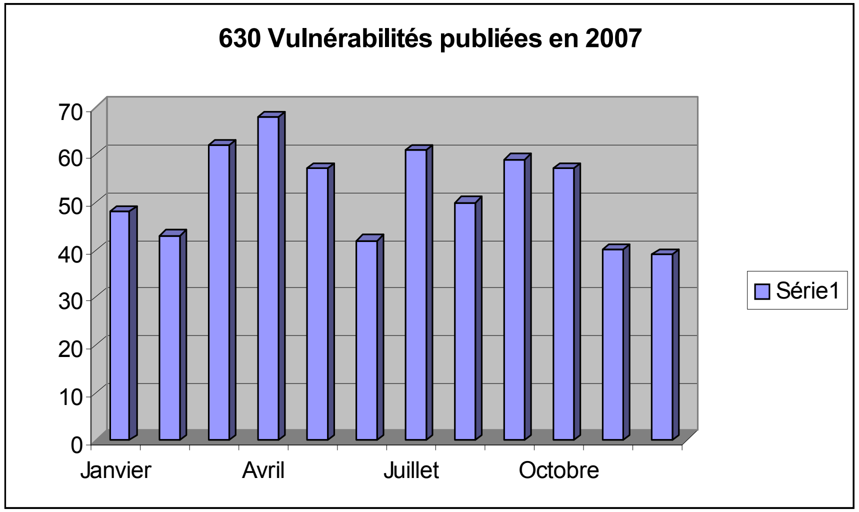
• Analyse the state of Internet security and convey that information to the system administrators, network managers, and wide public in the Internet community.

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

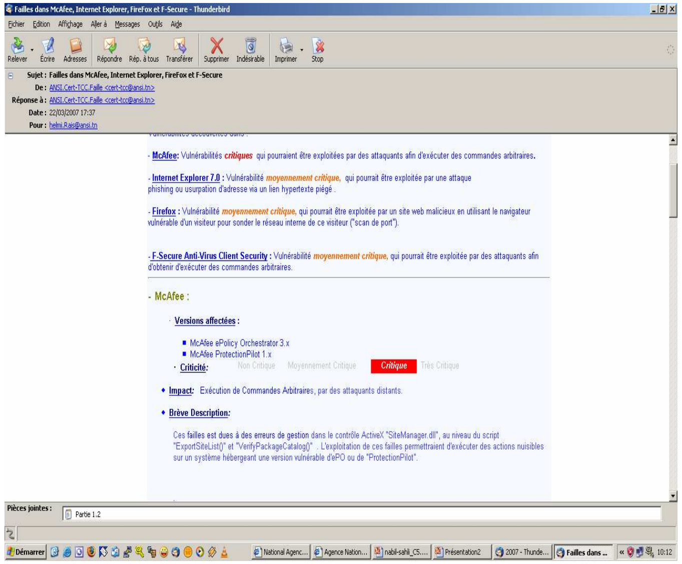
• We analyze the potential vulnerability and try to work with other CERTs and technology producers to track the solutions to these problems. We also make vulnerability information widely available through a vulnerability database.

Information and Alert

- 1000 Vulnerabilities published in 2007-2008
- 35 Malwares published in 2007-2008



630 Vulnérabilités publiées en 2007



Failles dans McAfee, Internet Explorer, FireFox et F-Secure - Thunderbird
Fichier Edition Affichage Aller à Messages Outils Aide
Relever Écrire Adresses Répondre Rép. à tous Transférer Supprimer Indésirable Imprimer Stop
Démarrer National Agenc... Agence Nation... nabil-sahli_C5.... Présentation2 2007 - Thunde... Failles dans ... 10:12

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

- **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

Information and Alert

15 Minor Alerts in 2007-2008

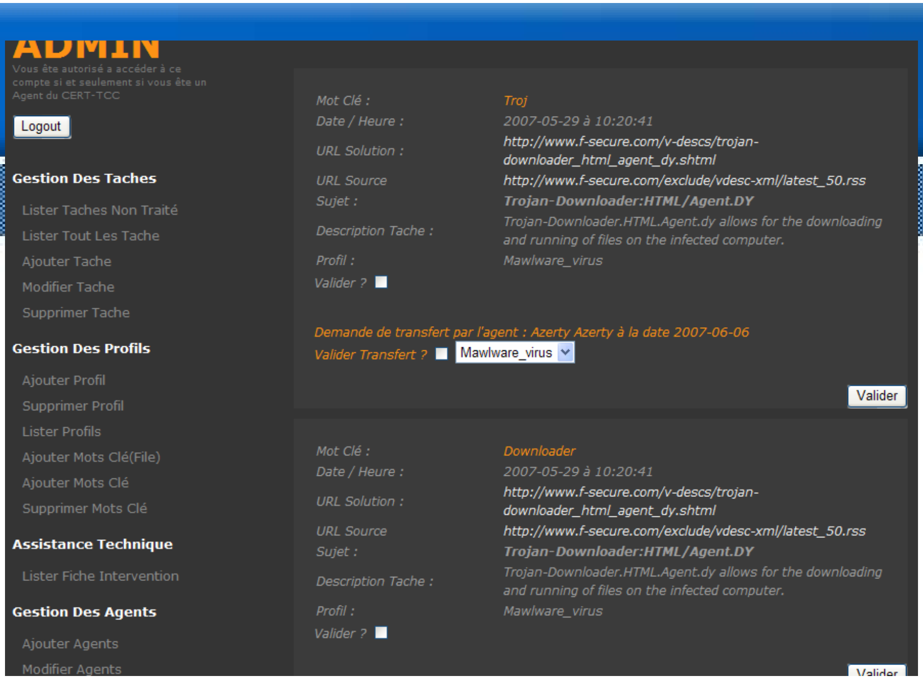
- Microsoft Word 0day **(CERT-TCC/Vuln.2007-045)**
- Sun Solaris Worm **(CERT-TCC/Vuln.2007-66)**
- Microsoft Windows DNS Service **(CERT-TCC/Vuln.2007-190)**
- Firefox et Netscape Navigator 0day **(CERT-TCC/Vuln.2007-368)**
- Propagation of "Storm Worm" "Zhelatin.LJ **(CERT-TCC/MAL-2007-009)**
- *RSTP QuickTime* Vulnerability **(CERT-TCC/Vuln.2007-577)**
- Asprox Botnet Propagation (**CERT-TCC / MAL-2008-011)**
- Exploits of Adobe Reader Vulnerabilities **(CERT-TCC/Vuln.2008-081)**
- Kaminisky DNS vulnerability **(CERT-TCC/Vuln.2008-330)**

- *Netmonster* : *The First Virus « made in Tunisia »* **(CERT-TCC/Malw.2007-023)**
- *Other Alerts on Scams/SPAMS and Hoaxes*

Information and Alert

- More than **8000** ***Voluntary*** subscribers
- More than **600** calls Monthly served (Call Center 24/7 + Green Number)
- More than **800** Advisories sent Since 2005
  - Vulnerabilities
  - Malwares
  - Spam &Hoax
  - Open Source
  - Books
  - Tools
  - Announces

Inscription is free: a@ansi.tn **(FR)**



ADMIN

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

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

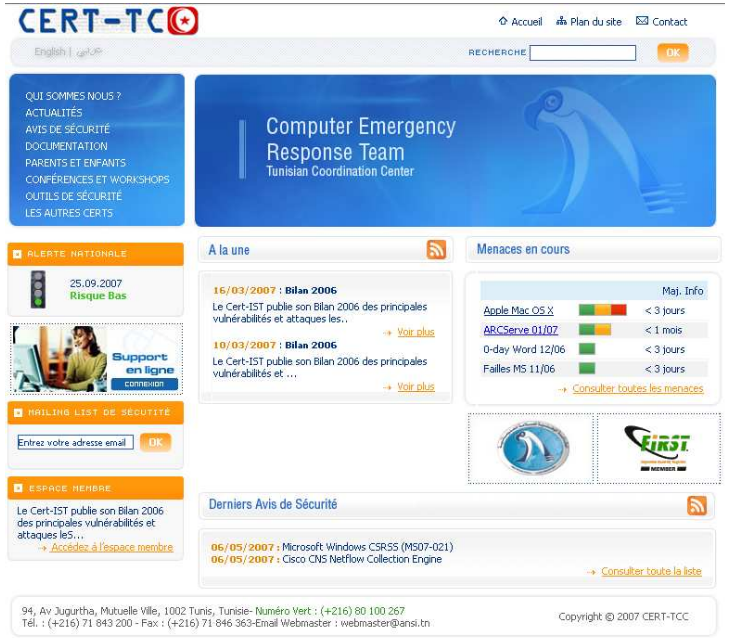
Mot Clé : Downloader
Date / Heure : 2007-05-29 à 10:20:41
URL Solution : http://www.f-secure.com/v-descs/trojan-downloader_html_agent_dy.shtml
URL Source http://www.f-secure.com/exclude/vdesc-xml/latest_50.rss
Sujet : Trojan-Downloader:HTML/Agent.DY
Description Tache : Trojan-Downloader.HTML.Agent.dy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

Internal Workflow Solutions

Chater (Smart in Arabic) شاطر

RSS Reader , Filter, Task Management

→ Free and Open Source



ALERTE NATIONALE

25.09.2007
Risque Bas

MAILING LIST DE SÉCUTITÉ

Entrez votre adresse email OK

ESPACE MEMBRE

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

Watch, Warning , Information & Alert

Investigation & Incident Response Team

Information Sharing and Analysis Center

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**

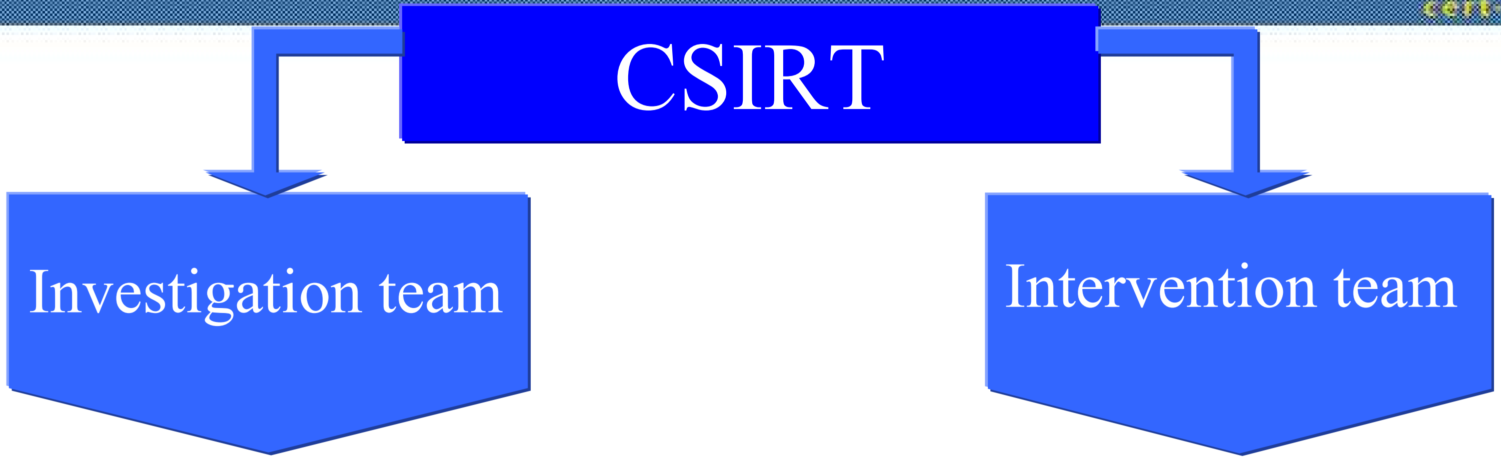
Article 10 of the Law No. 2004-5 relative to IT security
(Public & Private institutions, must inform the National Agency for Computer Security about any Incident, which can affect other Information Systems)

Article 9 of the Law No. 2004-5 relative to IT security Stipulate that
The employees of the National Computer Security Agency and security auditors are Responsible about the preservation of confidentiality 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)



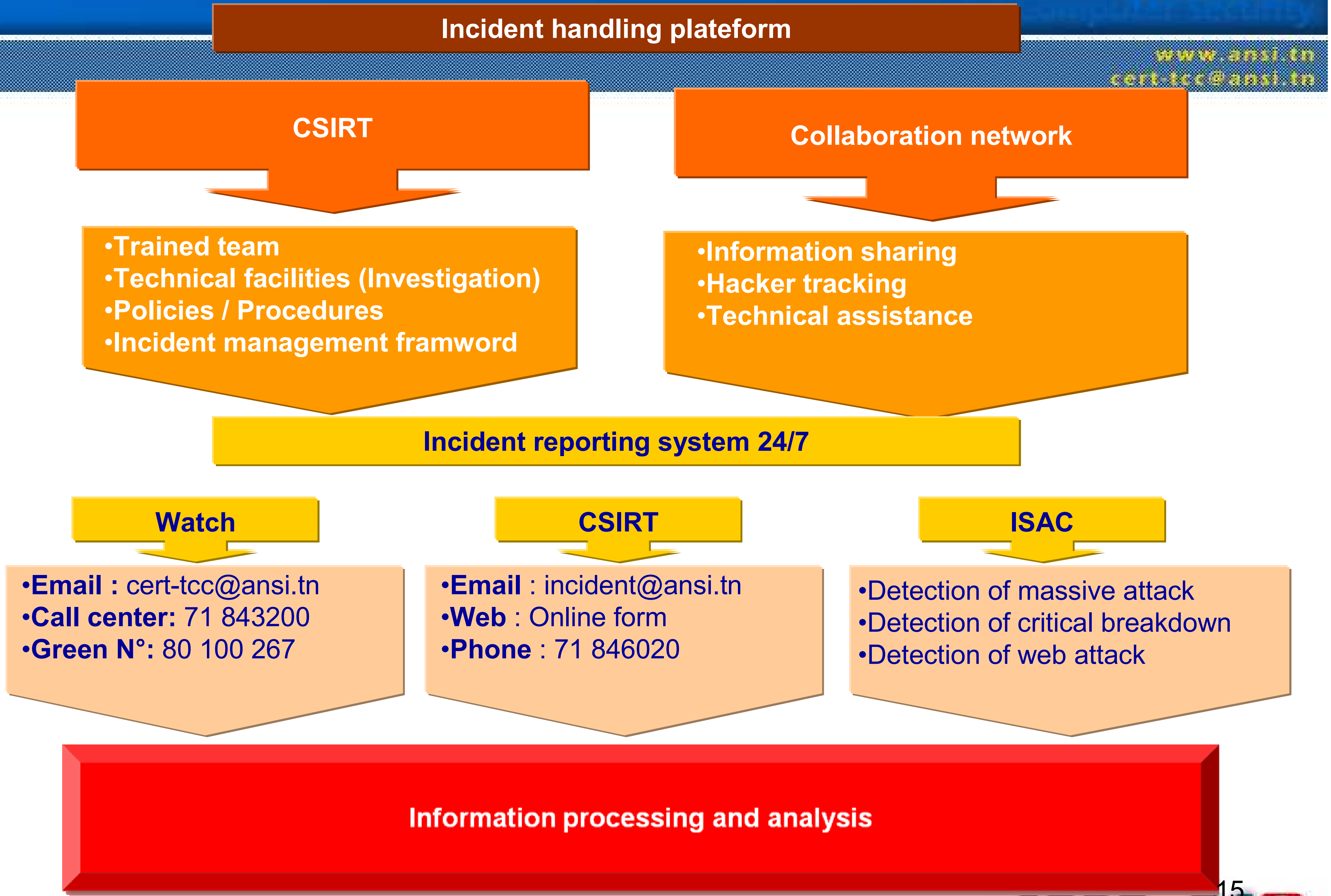
CSIRT

Investigation team

Intervention team

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

- On-site
- Incident handling process
- Evidence collection



Incident handling plateform

CSIRT

- Trained team
- Technical facilities (Investigation)
- Policies / Procedures
- Incident management framword

Collaboration network

- Information sharing
- Hacker tracking
- Technical assistance

Incident reporting system 24/7

Watch

- **Email :** cert-tcc@ansi.tn
- **Call center:** 71 843200
- **Green N°:** 80 100 267

CSIRT

- **Email** : incident@ansi.tn
- **Web** : Online form
- **Phone** : 71 846020

ISAC

- Detection of massive attack
- Detection of critical breakdown
- Detection of web attack

Information processing and analysis

Most relevant cases

- Web defacement
- Phishing
- Sabotage
- Identity theft
- Massive virus infection
- Denial of service

Watch, Warning, Information & Alert

Investigation & Incident Response Team

Information Sharing and Analysis Center

ISAC “Saher”

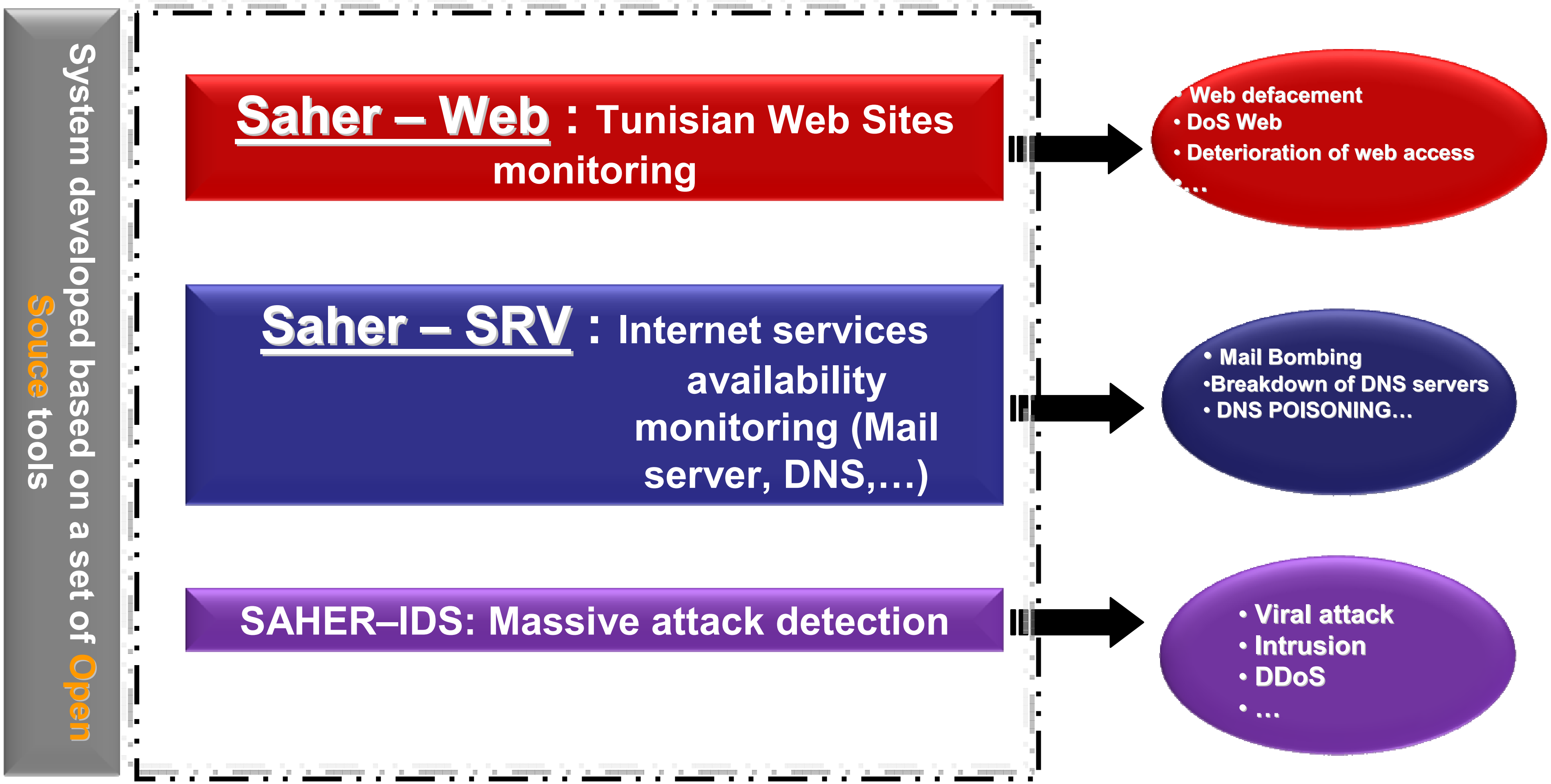
A **Watch- center** (based on **open-source solutions),** which permits to monitor the National Cyber-Space security in **Real time,**

→ **Early Detection of Mass attacks, D-Dos Attacks (Estonia 2007, Georgia 2008)**

→ 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 evaluation**

« Saher » Architecture



System developed based on a set of Open Souce tools

Saher – Web : Tunisian Web Sites monitoring

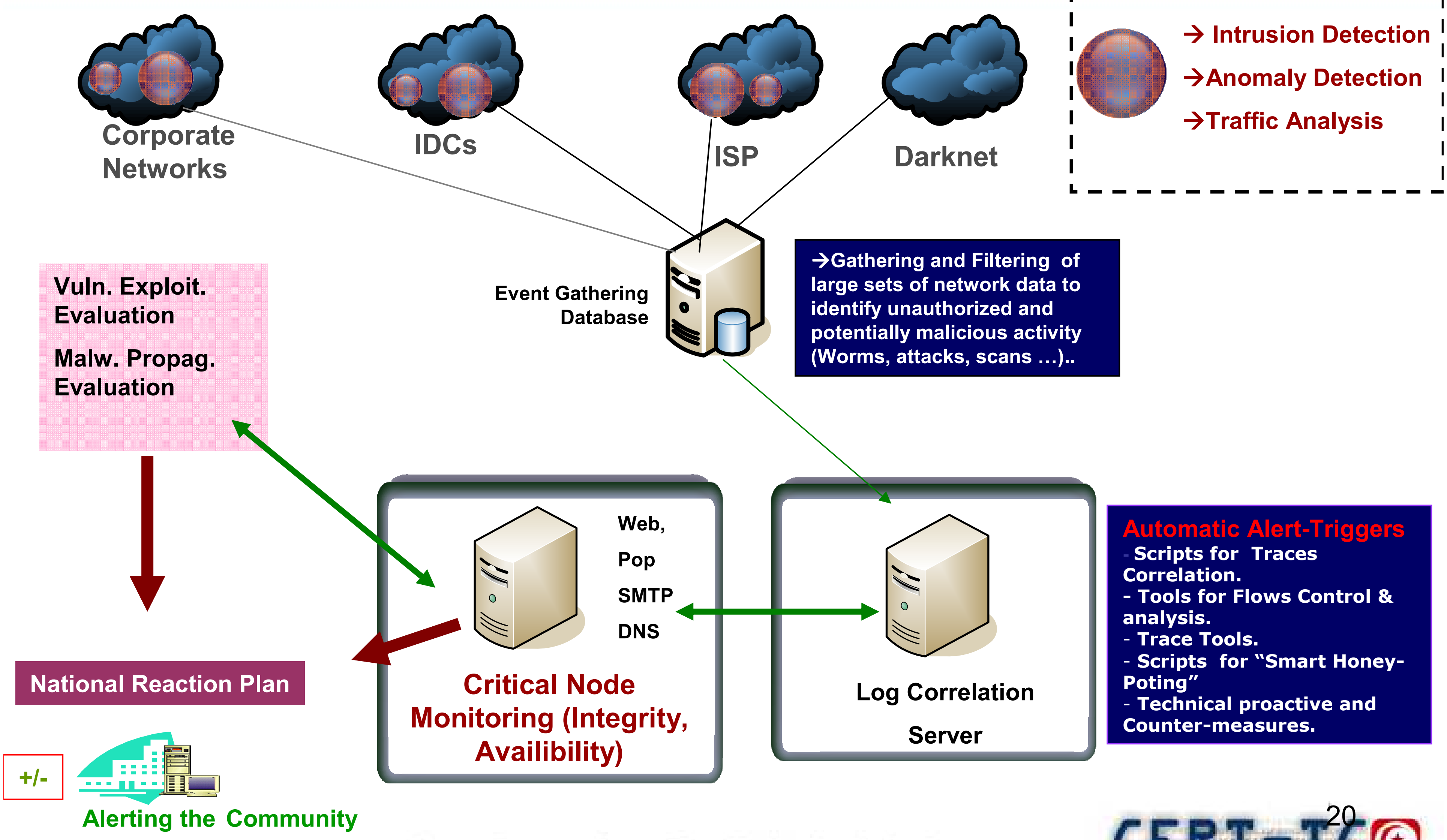
- Web defacement
- DoS Web
- Deterioration of web access
- …

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
- …



→ Intrusion Detection

→Anomaly Detection

→Traffic Analysis

→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

National Reaction Plan

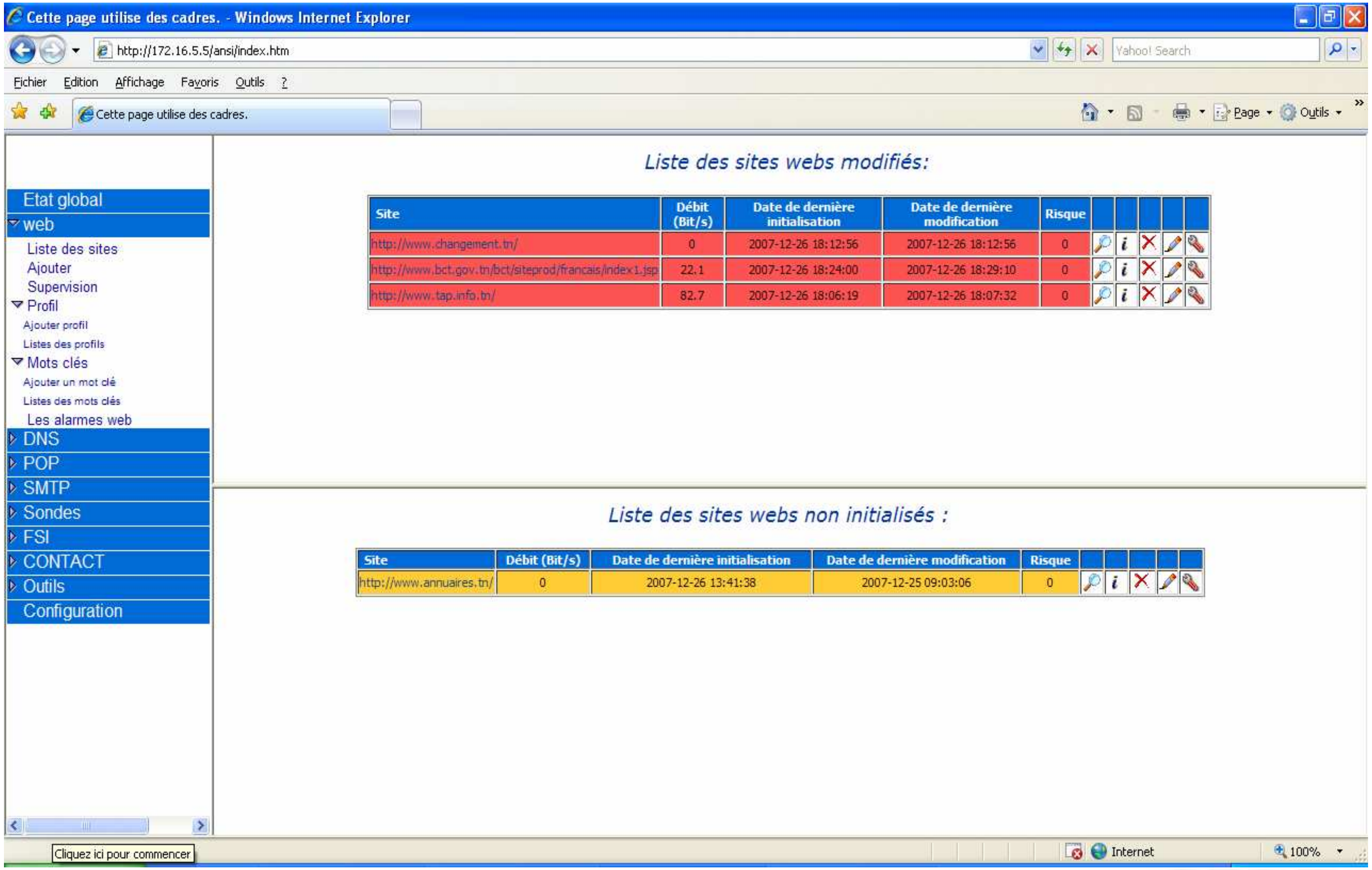
Critical Node Monitoring (Integrity, Availibility)

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.

Saher – Web : Tunisian web sites monitoring



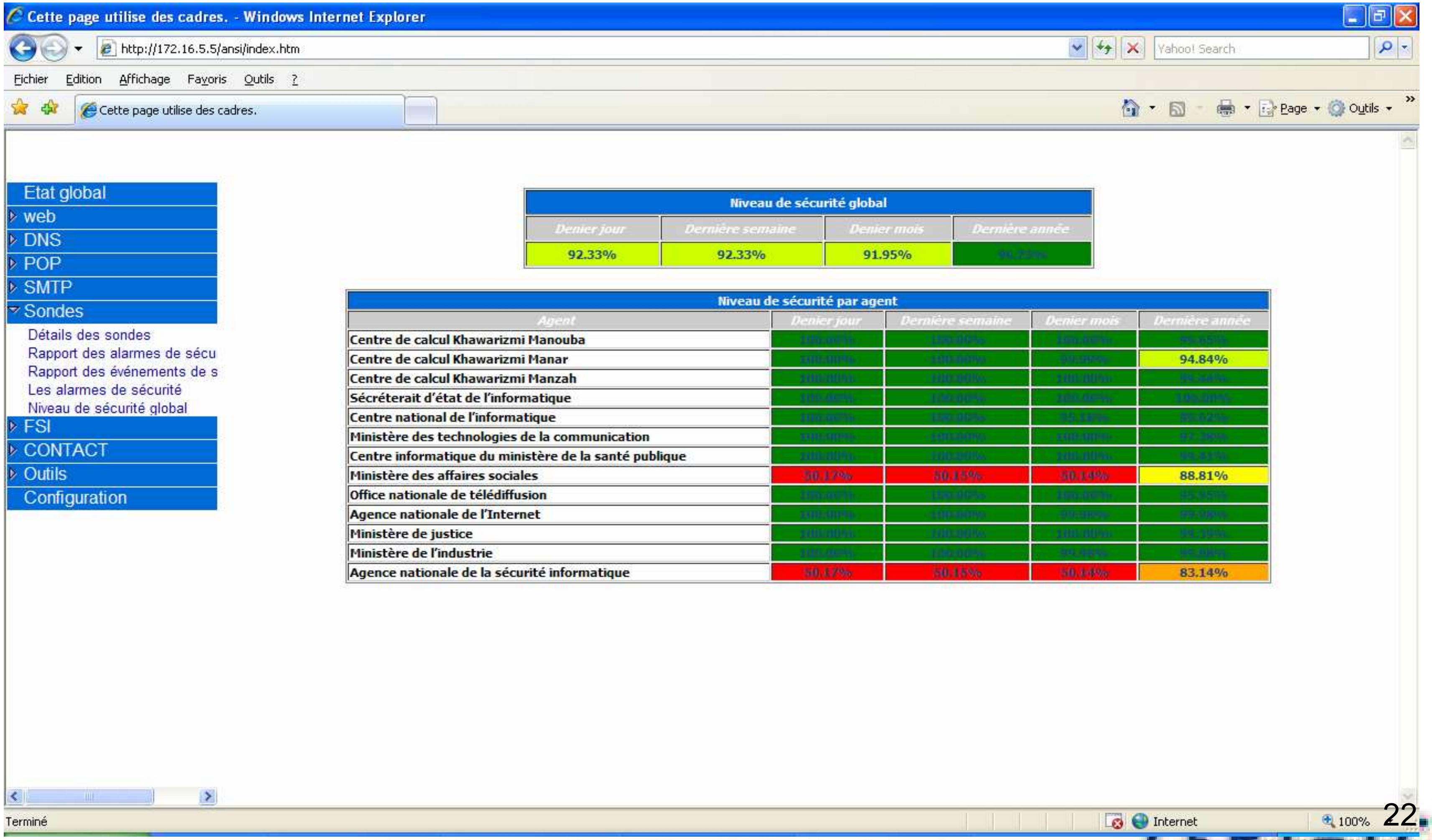
Liste des sites webs modifiés:

Site	Débit (Bit/s)	Date de dernière initialisation	Date de dernière modification	Risque					
http://www.changement.tn/	0	2007-12-26 18:12:56	2007-12-26 18:12:56	0	🔍	i	✕	✎	🔧
http://www.bct.gov.tn/bct/siteprod/francais/index1.jsp	22.1	2007-12-26 18:24:00	2007-12-26 18:29:10	0	🔍	i	✕	✎	🔧
http://www.tap.info.tn/	82.7	2007-12-26 18:06:19	2007-12-26 18:07:32	0	🔍	i	✕	✎	🔧

Liste des sites webs non initialisés :

Site	Débit (Bit/s)	Date de dernière initialisation	Date de dernière modification	Risque					
http://www.annuaires.tn/	0	2007-12-26 13:41:38	2007-12-25 09:03:06	0	🔍	i	✕	✎	🔧

SAHER–SRV: Internet services availability monitoring (server Mail, DNS,…)



Cette page utilise des cadres. - Windows Internet Explorer
http://172.16.5.5/ansi/index.htm
Yahoo! Search
Fichier Edition Affichage Favoris Outils ?
Cette page utilise des cadres.
Page
Outils
Etat global
web
DNS
POP
SMTP
Sondes
Détails des sondes
Rapport des alarmes de sécu
Rapport des événements de s
Les alarmes de sécurité
Niveau de sécurité global
FSI
CONTACT
Outils
Configuration
Terminé
Internet
100%

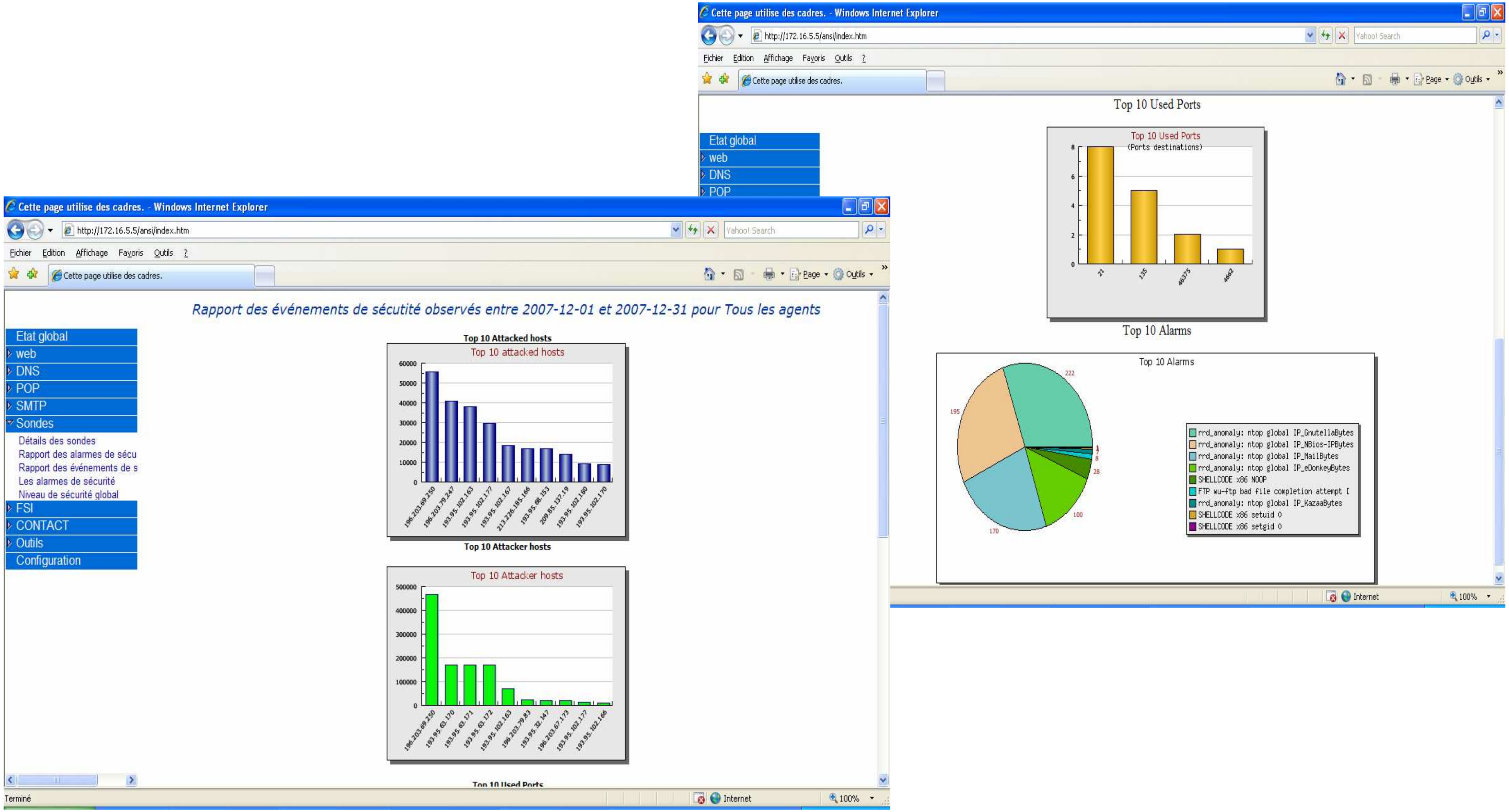
Niveau de sécurité global

Denier jour	Dernière semaine	Denier mois	Dernière année
92.33%	92.33%	91.95%	96.72%

Niveau de sécurité par agent

Agent	Denier jour	Dernière semaine	Denier mois	Dernière année
Centre de calcul Khawarizmi Manouba	100.00%	100.00%	100.00%	99.65%
Centre de calcul Khawarizmi Manar	100.00%	100.00%	99.09%	94.84%
Centre de calcul Khawarizmi Manzah	100.00%	100.00%	100.00%	99.44%
Sécréterait d'état de l'informatique	100.00%	100.00%	100.00%	100.00%
Centre national de l'informatique	100.00%	100.00%	95.16%	99.62%
Ministère des technologies de la communication	100.00%	100.00%	100.00%	97.26%
Centre informatique du ministère de la santé publique	100.00%	100.00%	100.00%	99.41%
Ministère des affaires sociales	50.17%	50.15%	50.14%	88.81%
Office nationale de télédiffusion	100.00%	100.00%	100.00%	95.95%
Agence nationale de l'Internet	100.00%	100.00%	99.98%	99.98%
Ministère de justice	100.00%	100.00%	100.00%	99.39%
Ministère de l'industrie	100.00%	100.00%	99.94%	99.88%
Agence nationale de la sécurité informatique	50.17%	50.15%	50.14%	83.14%

Saher – IDS : Massive attack detection



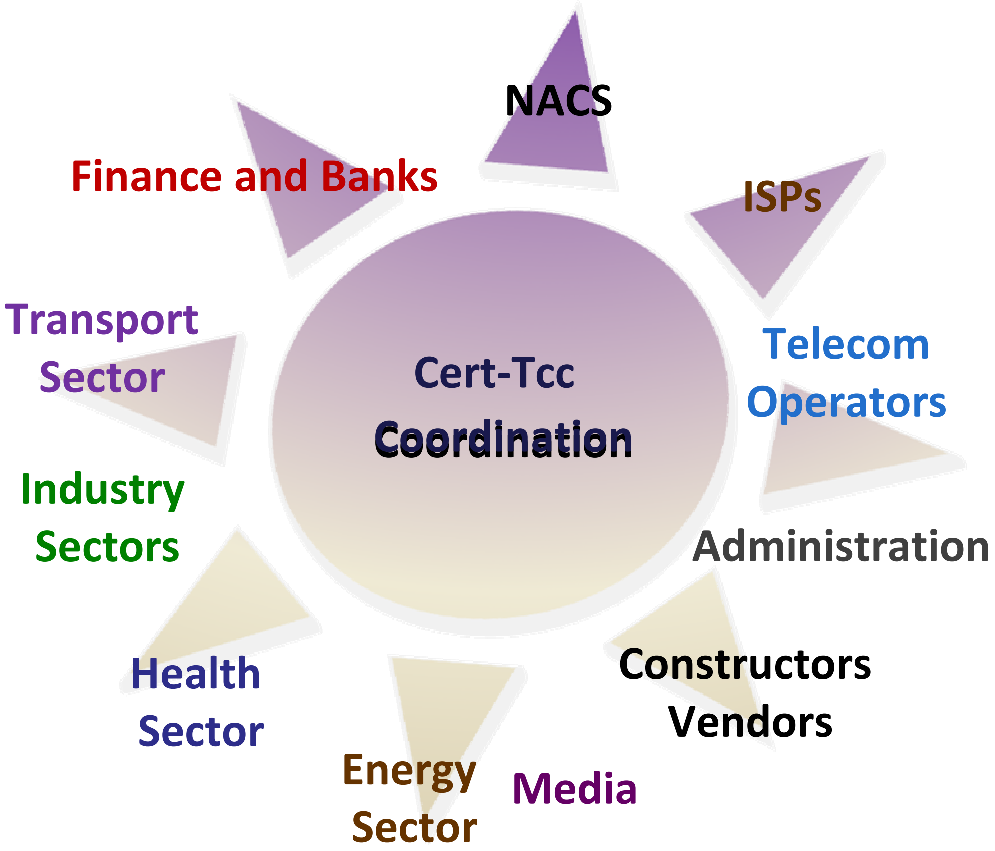
Rapport des événements de sécutité observés entre 2007-12-01 et 2007-12-31 pour Tous les agents

NRP: National Reaction Plan

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

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

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



NRP: National Reaction Plan

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)

ONU Conference about Terrorism

Case Studies

Kaminsky DNS Vulnerability

- In July 2008, Kaminsky had discovered a fundamental flaw in the DNS protocol. ("Most overhyped security vulnerability")

-The flaw could allow attackers to easily perform cache poisoning attacks on any nameserver

-All internet protocols (HTTP, FTP, Email…)are affected

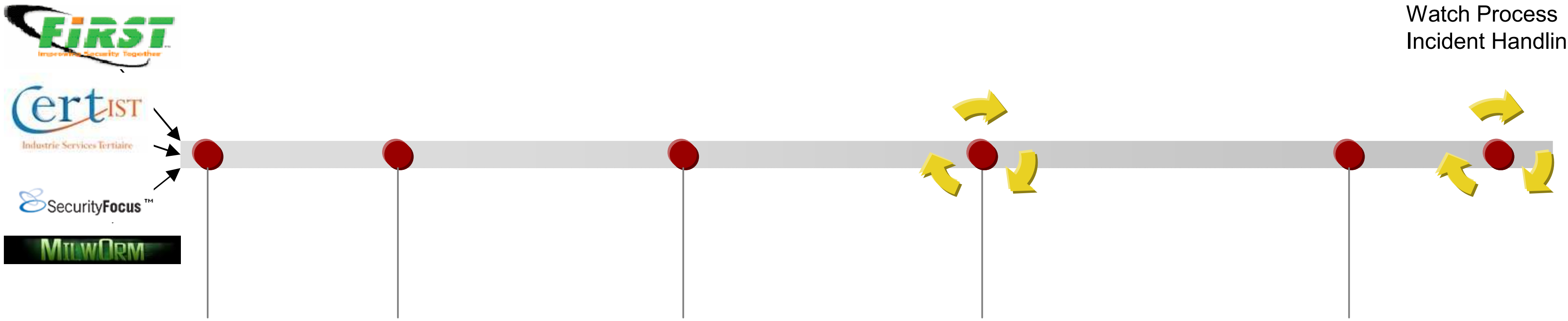
- Kaminsky informed DNS vendors in secret to develop a patch to make exploiting the vulnerability more difficult, which was released on July 8, 2008

-Kaminsky had intended not to publicize details of the attack until 30 days after the release of the patch, but it was accidentally leaked on July 21, 2008

- DNS Exploits has been published + Reverse Engineering on released patches

- Kaminisky had published more information about the vulnerability on August 8, 2008 at Black Hat 2008

Kaminsky DNS Vulnerability



Watch Process &
Incident Handling

- Information Collection
  Test and Analysis

- Identify Affected Tunisian Servers
- Inform Concerned parts

- Crisis Cell
- Inform ISPs
- Inform CiSOs
- Technical Advisories (Patches, workarounds,

- Watch Process on DNS resolutions for Tunisian Servers (for the 10 most visited websites in Tunisia)

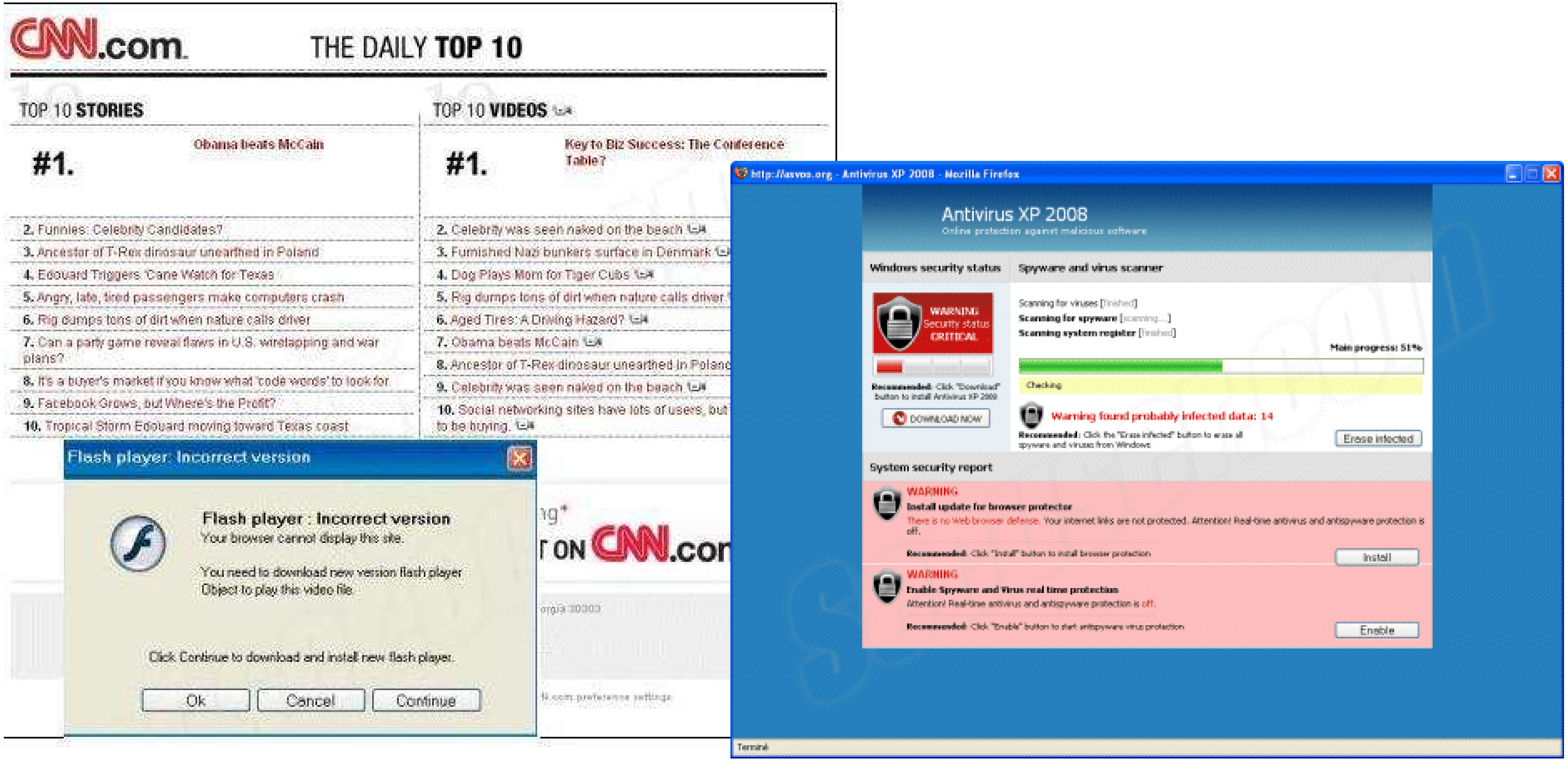
- Add Snort Signatures in SAHER system

- Intrusion detection Monitoring with SAHER system (attack tentative)

- Share Blacklist IPs with ISPs

- Inform Tunisian Internet Communuty (Media, Press,..)
  Public Advisory

Exchanger. JT (August 2008)



CNN.com THE DAILY TOP 10

TOP 10 STORIES

#1. Obama beats McCain

2. Funnies: Celebrity Candidates?
3. Ancestor of T-Rex dinosaur unearthed in Poland
4. Edouard Triggers 'Cane Watch for Texas
5. Angry, late, tired passengers make computers crash
6. Rig dumps tons of dirt when nature calls driver
7. Can a party game reveal flaws in U.S. wiretapping and war plans?
8. It's a buyer's market if you know what 'code words' to look for
9. Facebook Grows, but Where's the Profit?
10. Tropical Storm Edouard moving toward Texas coast

TOP 10 VIDEOS

#1. Key to Biz Success: The Conference Table?

2. Celebrity was seen naked on the beach
3. Furnished Nazi bunkers surface in Denmark
4. Dog Plays Mom for Tiger Cubs
5. Rig dumps tons of dirt when nature calls driver
6. Aged Tires: A Driving Hazard?
7. Obama beats McCain
8. Ancestor of T-Rex dinosaur unearthed in Poland
9. Celebrity was seen naked on the beach
10. Social networking sites have lots of users, but to be buying.

ng*
T ON CNN.com
orgia 30303
N.com preference settings

Flash player: Incorrect version

Flash player : Incorrect version
Your browser cannot display this site.

You need to download new version flash player Object to play this video file.

Click Continue to download and install new flash player.

http://asvos.org - Antivirus XP 2008 - Mozilla Firefox

Antivirus XP 2008
Online protection against malicious software

Windows security status

WARNING Security status CRITICAL

Recommended: Click "Download" button to install Antivirus XP 2008

Spyware and virus scanner

Scanning for viruses [finished]
Scanning for spyware [scanning...]
Scanning system register [finished]

Main progress: 51%

Checking

Warning found probably infected data: 14

Recommended: Click the "Erase infected" button to erase all spyware and viruses from Windows

System security report

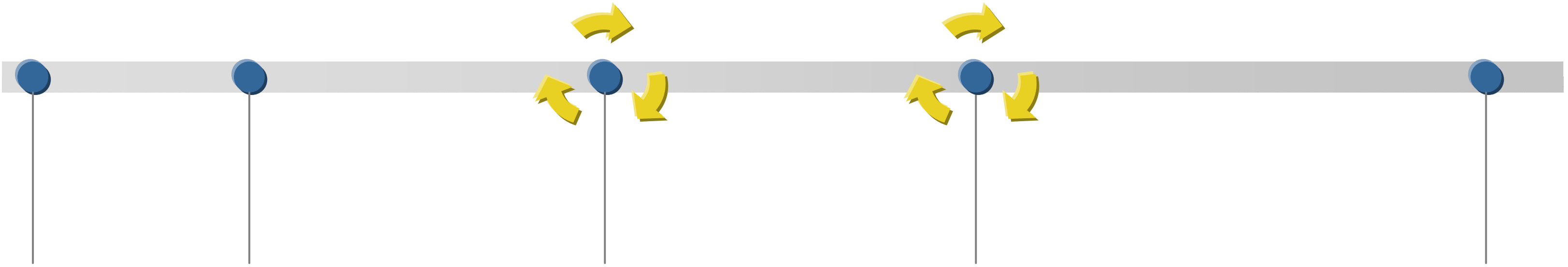
WARNING
Install update for browser protector
There is no Web browser defense. Your internet links are not protected. Attention! Real-time antivirus and antispyware protection is off.

Recommended: Click "Install" button to install browser protection

WARNING
Enable Spyware and Virus real time protection
Attention! Real-time antivirus and antispyware protection is off.

Recommended: Click "Enable" button to start antispyware virus protection

Exchanger. JT (August 2008)



Recieve
Malware
Spam

- Malware Analysis (static and dynamic anysis)
- Identify C&C Servers
- Identifiy Malicious Servers
- Identify Malware communication protocls

- Coordinate with ISPs
- Coordinate with International Partners and CERTs
- Stop Bad URLs
- Share Black List IPs

- Test Malware propagation in the Tunisian Cyber Space with SAHER System (Snort Signatures)

- Intrusion detection Monitoring with SAHER system (attack tentative)

- Share Blacklist IPs with ISPs

- Public Advisory for Tunisian Internet Communuty (Media, Press,..)

Projects in progress

- National Backup Center
- National Security Policy
- Tunisian Honeynet Project
- IT Security Labs: Forensics, Malware Analysis, Code Auditing, Software Assurance
- Assistance to set up Security and CERT/ CSIRT Cells in Ministries, GOV Establishments and also Private CERTs/CSIRTs for industrial sectors (Banks,…)
- Assistance to set up CERTs & Cyber Security Centers in Africa

Thank you for your attention