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

SecurityFocus™
Microsoft®

Internet Service Providers

Managers, Decision Makers

CISOs (Ministries, Bank, Critical networks…)

Webmaster, Network admin, developers,

Internet Community

Vulnerabilities, Exploit, 0days

Malwares, Botnets,…

Internet Service Providers

Mailing List, Web site, Data Base, Call Center

Certs, International Partners

CERT-TC (Computer Emergency Response Team - Tunisian Coordination Center)

CertIST
FIRST

Microsoft, CERT-TC

N.A.C.S
www.ansi.tn
cert-tcc@ansi.tn
Watch, Warning, Information & Alert

Investigation & Incident Response Team

Information Sharing and Analysis Center
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.
1000 Vulnerabilities published in 2007-2008
35 Malwares published in 2007-2008
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
• 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)
Internal Workflow Solutions

Chater (Smart in Arabic) شاطر

RSS Reader, Filter, Task Management

→ Free and Open Source

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:

- A CSIIRT team in charge of providing (free of charge) **Assistance for Incident Handling**
- Call-center, **available 24 Hours/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)
• Computer forensics
• Evidence analysis
• Investigation (Log, Hard Drive, memory dump, …)

On-site
• Incident handling process
• Evidence collection
Incident handling platform

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

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
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

Saher – Web: Tunisian Web Sites monitoring

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

SAHER–IDS: Massive attack detection

System developed based on a set of Open Source tools

Web defacement
- DoS Web
- Deterioration of web access

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

- Viral attack
- Intrusion
- DDoS
- ...

Computer Emergency Response Team - Tunisian Coordination Center
wwwansi.tncert-tcc@ansi.tn
Gathering and Filtering of large sets of network data to identify unauthorized and potentially malicious activity (Worms, attacks, scans ...).

Event Gathering Database

Corporate Networks → Intrusion Detection
IDCs → Anomaly Detection
ISP → Traffic Analysis
Darknet

Vuln. Exploit. Evaluation
Malw. Propag. Evaluation

Critical Node Monitoring (Integrity, Availability)

Web, Pop, SMTP, DNS

Log Correlation Server

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

Automatic Alert-Triggers
- Scripts for Traces Correlation.
- Trace Tools.
- Scripts for “Smart Honey-Potting”
- Technical proactive and Counter-measures.

National Reaction Plan

Alerting the Community
Safer – Web: Tunisian web sites monitoring

Liste des sites webs modifiés:

<table>
<thead>
<tr>
<th>Site</th>
<th>Débit (K/s)</th>
<th>Date de dernière initialisation</th>
<th>Date de dernière modification</th>
<th>Risque</th>
</tr>
</thead>
</table>

Liste des sites webs non initialisés:

<table>
<thead>
<tr>
<th>Site</th>
<th>Débit (K/s)</th>
<th>Date de dernière initialisation</th>
<th>Date de dernière modification</th>
<th>Risque</th>
</tr>
</thead>
</table>

Computer Emergency Response Team - Tunisian Coordination Center
SAHER–SRV: Internet services availability monitoring (server Mail, DNS,...)
Saher – IDS: Massive attack detection
- “Formal” **Global** Reaction Plan.

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

With CERT/TCC acting as a **coordinator** between them.
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)
Case Studies
- 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

- 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 Community (Media, Press...)
- Public Advisory
Receive Malware Spam

- Malware Analysis (static and dynamic analysis)
- Identify C&C Servers
- Identify Malicious Servers
- Identify Malware communication protocols

- 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 Community (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