The Cert-IST : a Managed Security Service for Threat Management, Incident Handling and Crisis Response

Les Assises de la Sécurité / Frederic MARTINEZ / 20-10-2005

ALCATEL

Cert-IST
Agenda

The Cert-IST : CERT, CSIRT & MSS

Evolution of the Threats

- Evolution of attacks and attackers
- Evolution of crisis impact

A solution : the Crisis management Hub

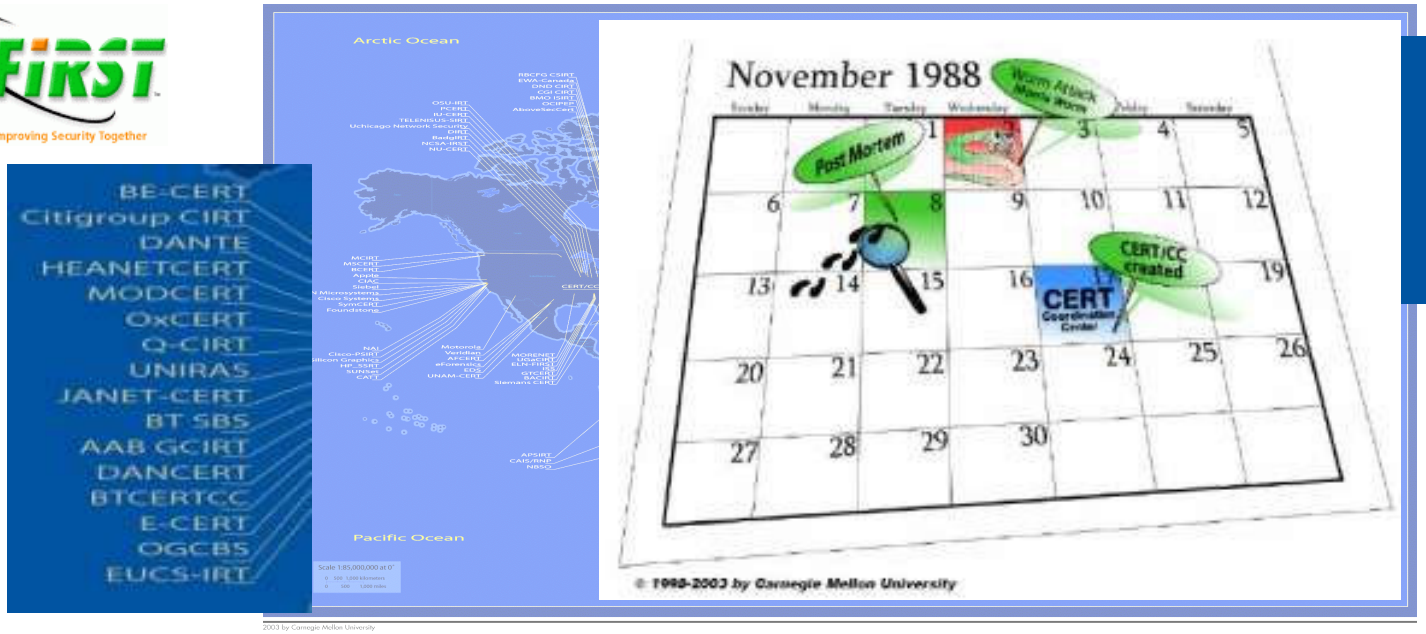
- Cross safely the maximum danger zone
- Zotob case Analysis

ALCATEL

Cert-IST

Computer Emergency Response Team – Industrie, Services et Tertiaire

The Cert-IST is a Computer Emergency Response Team



FIRST identifies Tree Certs in France

- CERT A for French administrations
- CERT-Renater for Univeristies and Research
- Cert-IST for « la communauté Industrie, Services et Tertiaire » (aka Enterprises)

Cert-IST : a Managed Security Service

for Threat Management, Incident Handling and Crisis Response

Missions

- Prevention (Watch & Alert)
  - Vulnerabilities watch and coordination with othe Certs
  - Security advisories, alerts and threats database management
- Incident Response
  - Investigation, intervention, coordination on international incidents
- Additional Services related to prevention
  - Training / Competency transfer

Organisation

- The founders outsource the service to Alcatel

Evolution 2004-2005

- Crisis Management hub
  - Reactivity
  - 24/7 Watch & alert

1999 :

Creation du Cert-IST

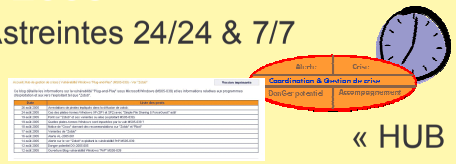
Reconnaissance FIRST

2000 : www.Cert-ist.com

2003 : Association Loi de 1901

2005 : Gestion de Crises

Astreintes 24/24 & 7/7



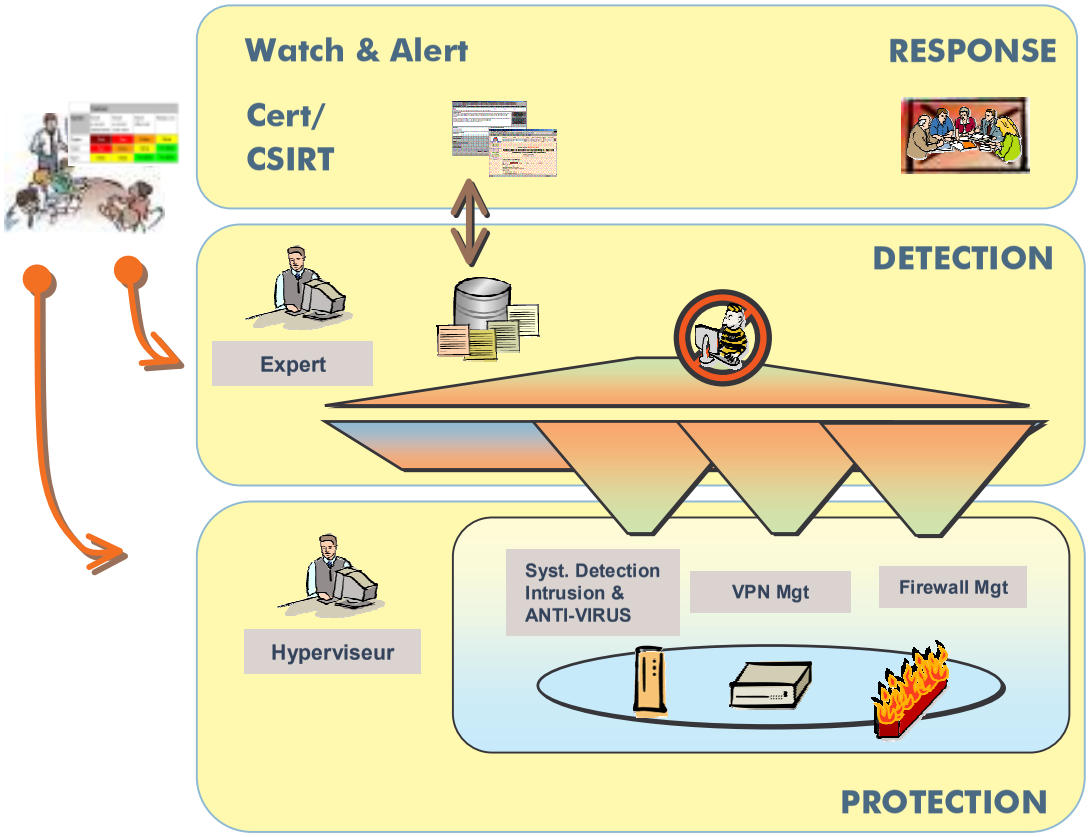
« HUB »

CERT & CSIRT : the positioning compared to other MSS
The Security Operation Center Approach

Global security control

ALCATEL

CERT & CSIRT : the positioning compared to other MSS
Protection – Detection – Response



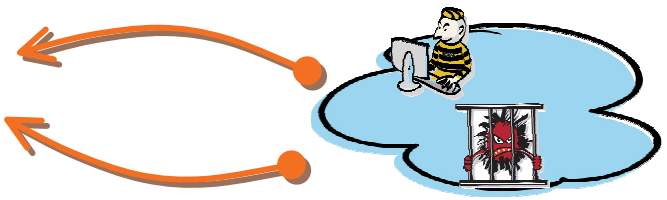
Efficient response to Attacks:

Accurate qualification of risks :

- Real-time management of a threats knowledge database
- Vendor-independent through Cert cooperation
- Neutral Risk Rating (www.eispp.org, CVSS)
- Standardised formatting of information (XML)

Efficient incident response:

- Proactive management of threats
- A team of dedicated experts for emergency response
- Focus response resources & attention on most critical threats



ALCATEL

Cert-IST
Agenda

The Cert-IST : CERT, CSIRT & MSS

Evolution of the Threats

- Evolution of attacks and attackers
- Evolution of crisis impact

A solution : the Crisis management Hub

- Cross safely the maximum danger zone
- Zotob case Analysis

ALCATEL

Evolution of Cybercriminality

Virus, Flaws and Cybercriminality

- Viruses are « tools »
  - to install a backdoor, create botnets, prepare a mass attack
- The time window between flaw divulgation and associated attack is more and more shorter
  - 6 months for Slammer (2003), 2 weeks for Sasser (2004), 4 days for Zotob (2005)
- Being impacted by an attack is a deadly risk
  - Massive attacks through viruses generate the biggest visible crisis (impact on image).
  - Professional attacks through phishing generate critical impact on assets and customer confidence

Real-time information about the threats, and strong response capacity are unvaluable.

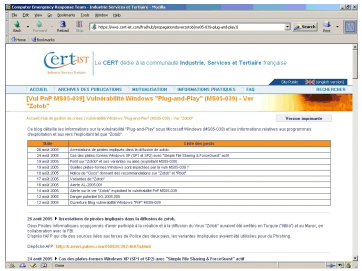

Le Monde

Les créateurs de virus informatiques deviennent des mercenaires

Le nombre de codes malicieux mis en circulation sur Internet augmente considérablement. Les spécialistes de sécurité des systèmes d'information suspectent, notamment, des collusions entre émetteurs de courriels non sollicités et auteurs de programmes malins

CERTIST Industrie Services Tertiaire

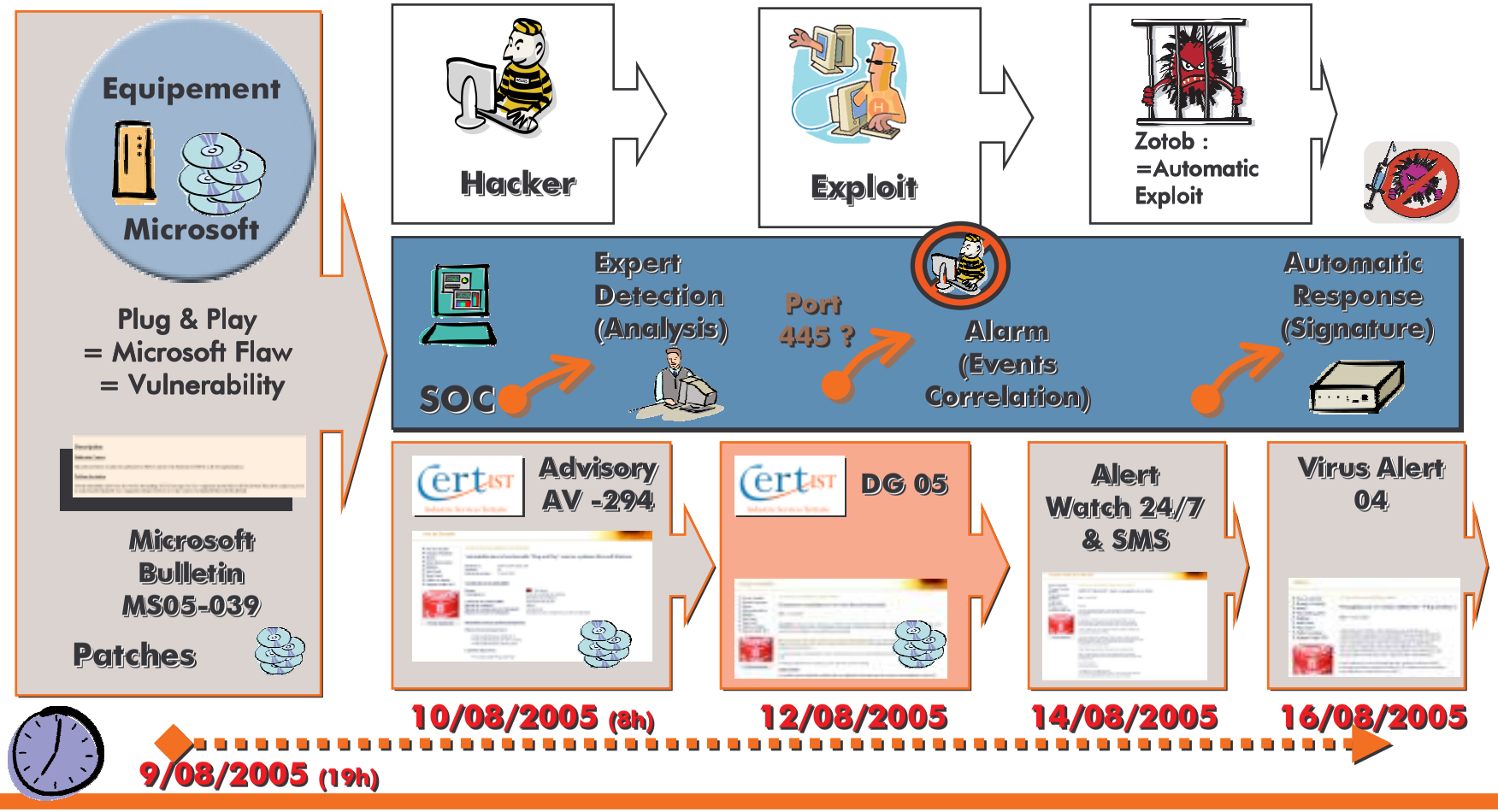
CTUSE



ALCATEL

The threats watch & response race : Zotob case

Viruses & Hacking start from a Vulnerability



Can you afford to lose that race ? The impact of Sarbanes-Oxley

« Public Company Accounting Reform and Investor Protection Act of 2002 », better known as Sarbanes-Oxley

- Sarbanes-Oxley sets requirements for new standards with regard to corporate accountability.

Section 404, titled "Management Assessment of Internal Controls".

- This section essentially requires companies (and their IT executives) to assess any risk associated with information technology or internal process that may impact the accurate and timely reporting of financial information.

Security Management for Sarbanes-Oxley Compliance

- By leveraging the capabilities of the Alcatel SOC and associated services, in conjunction with security devices and solid policies, IT organizations are well equipped to prevent or negate the impact of viruses, hackers and other threats that can cause corruption of networks and systems, thus resulting in the high network and data integrity required
- SOC and MSS provides a solid foundation for organizations to help ensure accurate reporting of financial information required by Sarbanes-Oxley.
- Resorting to a managed service, with a participation/fee for a crisis management group, enables the company to demonstratee it has taken « all the appropriate measures enabling to comply with requirements »

Cert-IST
Agenda

The Cert-IST : CERT, CSIRT & MSS

Evolution of the Threats

- Evolution of attacks and attackers
- Evolution of crisis impact

A solution : the Crisis management Hub

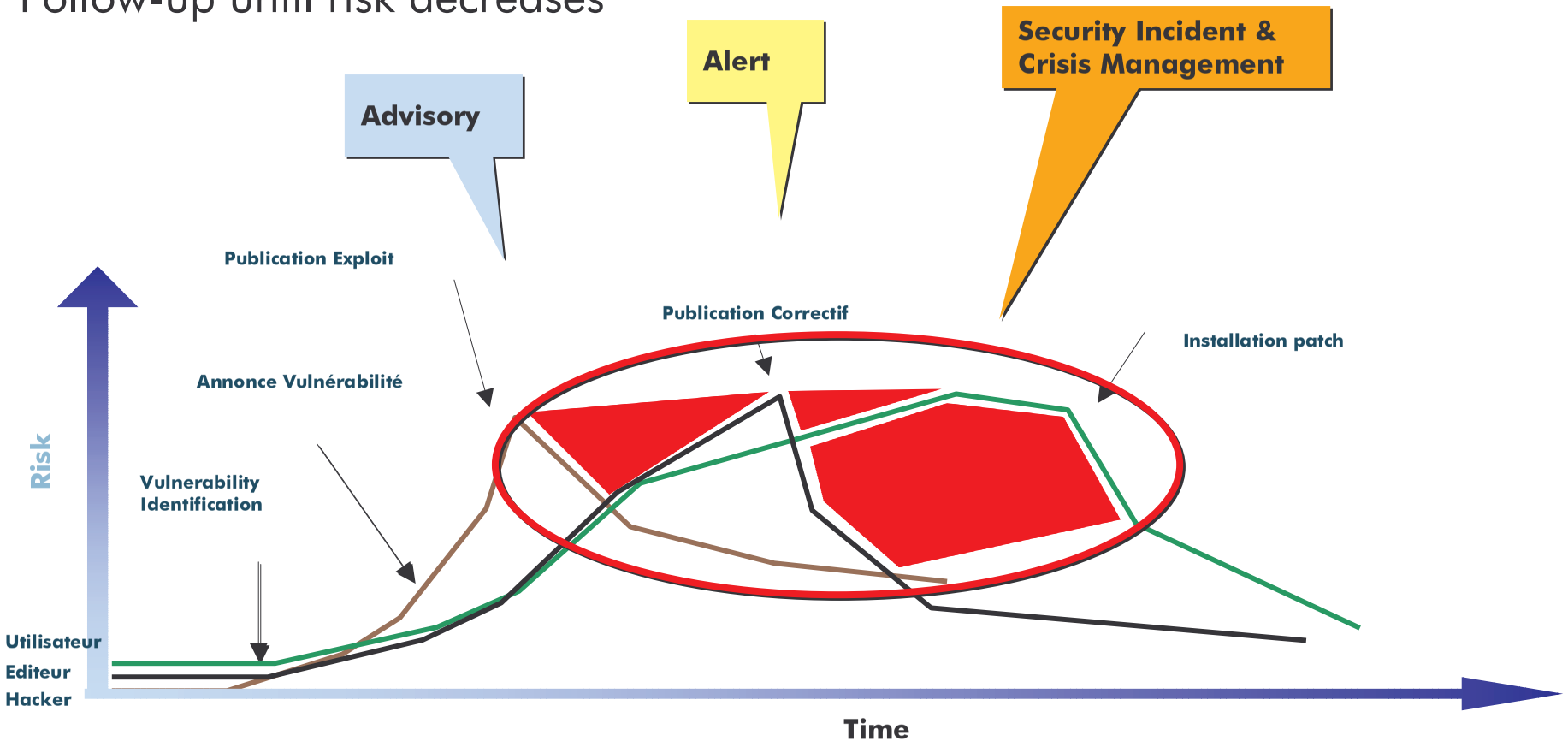
- Cross safely the maximum danger zone
- Zotob case Analysis

ALCATEL

The evolution of CERT services
Helping you to cross safely the « maximum danger zone »

Identify the flaws that will generate major crisis

Follow-up until risk decreases



ALCATEL

EISPP & CVSS :
The added value of neutrality for risk Assessment

www.eispp.org

- EISPP : European Information Security Promotion Programme
- A project co-funded by the European Community under the Fifth Framework Programme.
- Rrun by a consortium of private sector organisations, (CERTs, ISP/ASPs, and Security organisations) : Cert-IST, esCERT-UPC, SIEMENS-CERT, Callineb Consulting, I-NET, CLUSIT and InetSecur.
- The project started in June 2002 and ran until January 2004. One of the outcomes of the project has been a common format for vulnerabilities advisories, still in use today across Europe

CVSS : Common Vulnerability Scoring System

Vulnerability Details	Vulnérabilité 09/05/2005 Message posté dans "Vuln-Coord"	Vulnérabilité 10/05/2005 CERT-IST/AV-2005.173 v1.0	Vulnérabilité 13/05/2005 CERT-IST/AV-2005.173 v2.0
Access Vector	REMOTE	REMOTE	REMOTE
Access Complexity	HIGH	HIGH	HIGH
Authentication	NOT-REQUIRED	NOT-REQUIRED	NOT-REQUIRED
Confidentiality Impact	PARTIAL	PARTIAL	PARTIAL
Integrity Impact	PARTIAL	PARTIAL	PARTIAL
Availability Impact	PARTIAL	PARTIAL	PARTIAL
Impact Bias	NORMAL	NORMAL	NORMAL
BASE SCORE	**5,6**	**5,6**	**5,6**
Exploitability	FUNCTIONAL	FUNCTIONAL	FUNCTIONAL
Remediation Level	UNAVAILABLE	WORKAROUND	OFFICIAL-FIX
Report Confidence	CORROBORATED	CONFIRMED	CONFIRMED
TEMPORAL SCORE	**5,3**	**5,1**	**4,6**

- The Common Vulnerability Scoring System, a NIAC research project, is a rating system designed to provide open and universally standard severity ratings of software vulnerabilities.
- FIRST has been chosen for hosting, updates and promotion of CVSS.
- Cert-IST, member of te FIRST, is actively testing & disseminating CVSS

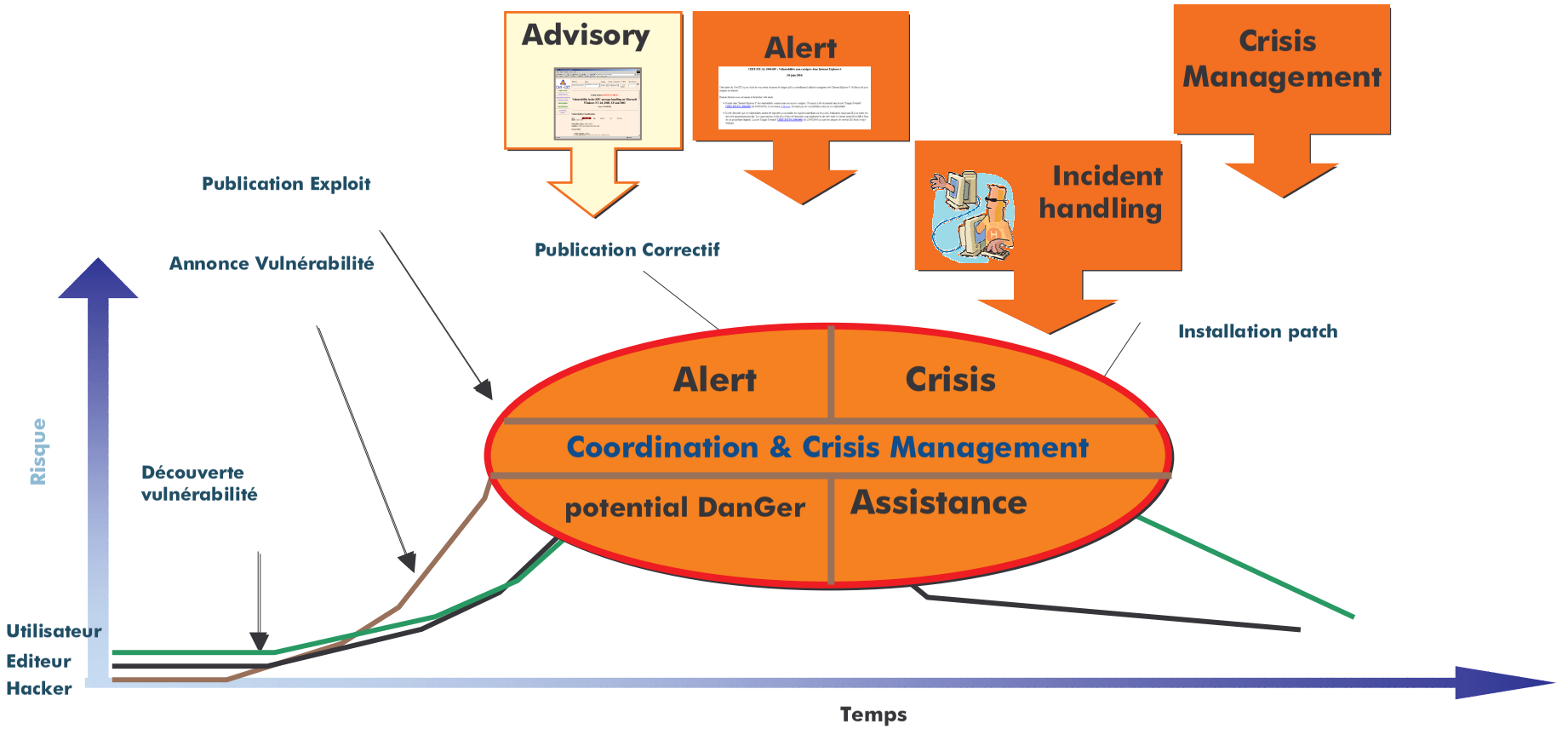
https://wws.cert-ist.com/fast-cgi/Article.cgi?lang=fra&Article=Ex_Application_CVSS

ALCATEL

Alcatel solution for response
The Cert-IST crisis Management Hub

Anticipation and management of risks

Act from prevention to crisis exit



A new model for emergency response (*modèle du SAMU*)
The coordination through « regulation » (Dispatch)

A focal point for crisis management :

- An expert having authority on :
  - Evaluation of criticity and crisis management resources activation
  - Identification of means and expertise required
  - Mobilisation/requisition of human and logistic resources
  - Follow-up and coordination of actions until crisis exit
  - A definition (in French) of the role of the « régulateur » (dispatcher)
    - *L'expert régulateur est chargé d'évaluer la gravité et le risque stratégique de la situation et de mobiliser l'ensemble des ressources disponibles (pour détection, scan, palliatifs, correctifs) en vue d'apporter la réponse la plus appropriée à l'état du système d'information, et de veiller à ce que les mesures nécessaires soient connues, disponibles et effectivement appliquées.*
    - *Le régulateur est, ainsi, notamment chargé de qualifier l'urgence des interventions.*
    - *A cet effet, le régulateur coordonne l'ensemble des moyens mis en œuvre dans le cadre de la gestion de crise. Il vérifie que les moyens arrivent effectivement dans les délais nécessités par la gravité de la crise et assure le suivi des interventions.*
    - *La détermination par l'expert régulateur de la réponse la mieux adaptée se fonde sur trois critères : l'estimation du degré de gravité avérée ou potentielle de l'atteinte au SI concerné ; l'appréciation du contexte ; l'état des ressources disponibles.*
- The dispatcher will from opening to exit of the crisis help in choosing the palliatives or correctives responses approporiate with the real-time evolution of the risk

ALCATEL

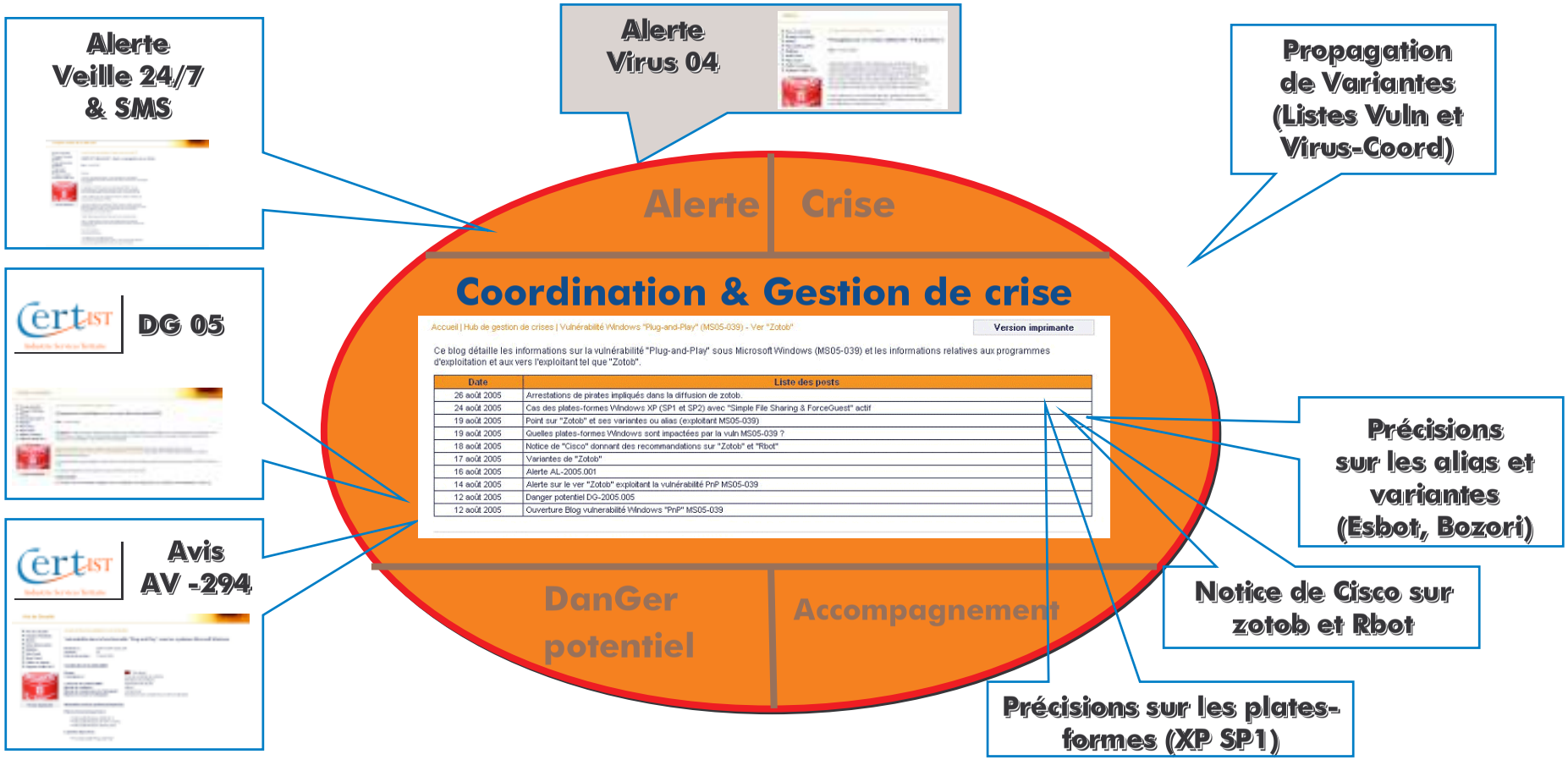
The visible part of the Crisis Management Hub

La partie la plus visible de l'activité du Hub de gestion de Crise
est le radar des menaces en cours : http://www.cert-ist.com/fra/hub/

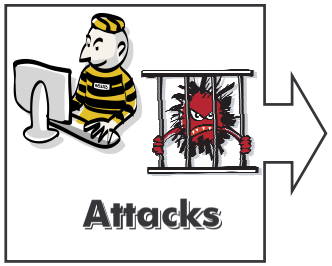
ALCATEL

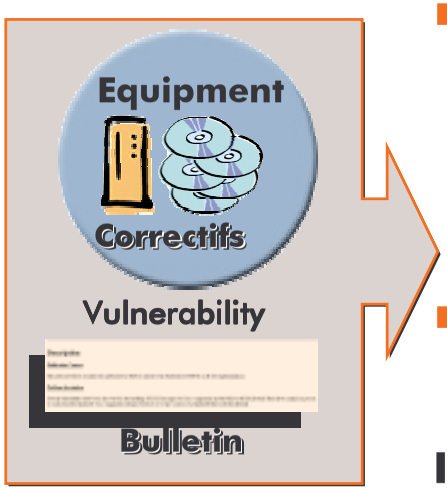
The Cert-IST crisis hub at work
The zotob case

Anticipation and management of risks from prevention to crisis exit



Attacks : a race where SOC and Cert play a relay





The SOC and the Cert-IST complement each other in detection / response strategy

- The threats known by the community are integrated in the :
  - Knowledge database of the Cert-IST
  - Local correlation engine and IDS of the SOC
- The impact on the Enterprise is estimated through
  - The Cert-IST profile : « push » information regarding the threat
  - Through the inventory database of the SOC : priority management
  - Through optional automatic scan tools (ex Criston)
- The possibility to counter the threat and its local impact will rely on
  - The « manual » application of the solutions identified by the Cert-IST
  - The set up of palliative filtering mesures (maybe partially managed by the SOC organization if it integrates FW management)
  - The application of quarantine to dangerous stations (NAC,CAC,AQE …)
  - The automatic application of patches and signatures (partially managed by the SOC organization if it integrates Patch Management)
- The rise of risk and crisis management under attack is done through
  - The Cert-IST Hub has been activated following a big attack or on request
  - The SOC has detected an important ongoing attack

Information, Detection, Decision & Reaction can (need to) be coordinated

ALCATEL

Responding to Cybercriminality : The balance between Protection, Detection & Response

Threats & Attacks

A sensitive balance between resources management and responsibility

Defense (protection-detection) Management

PREVENTION / WATCH

ASSISTANCE (accompagnement)

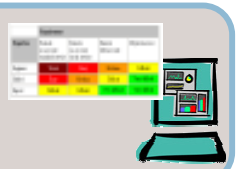
ALERT & REACTION

Alcatel solutions :

A permanent competency transfer

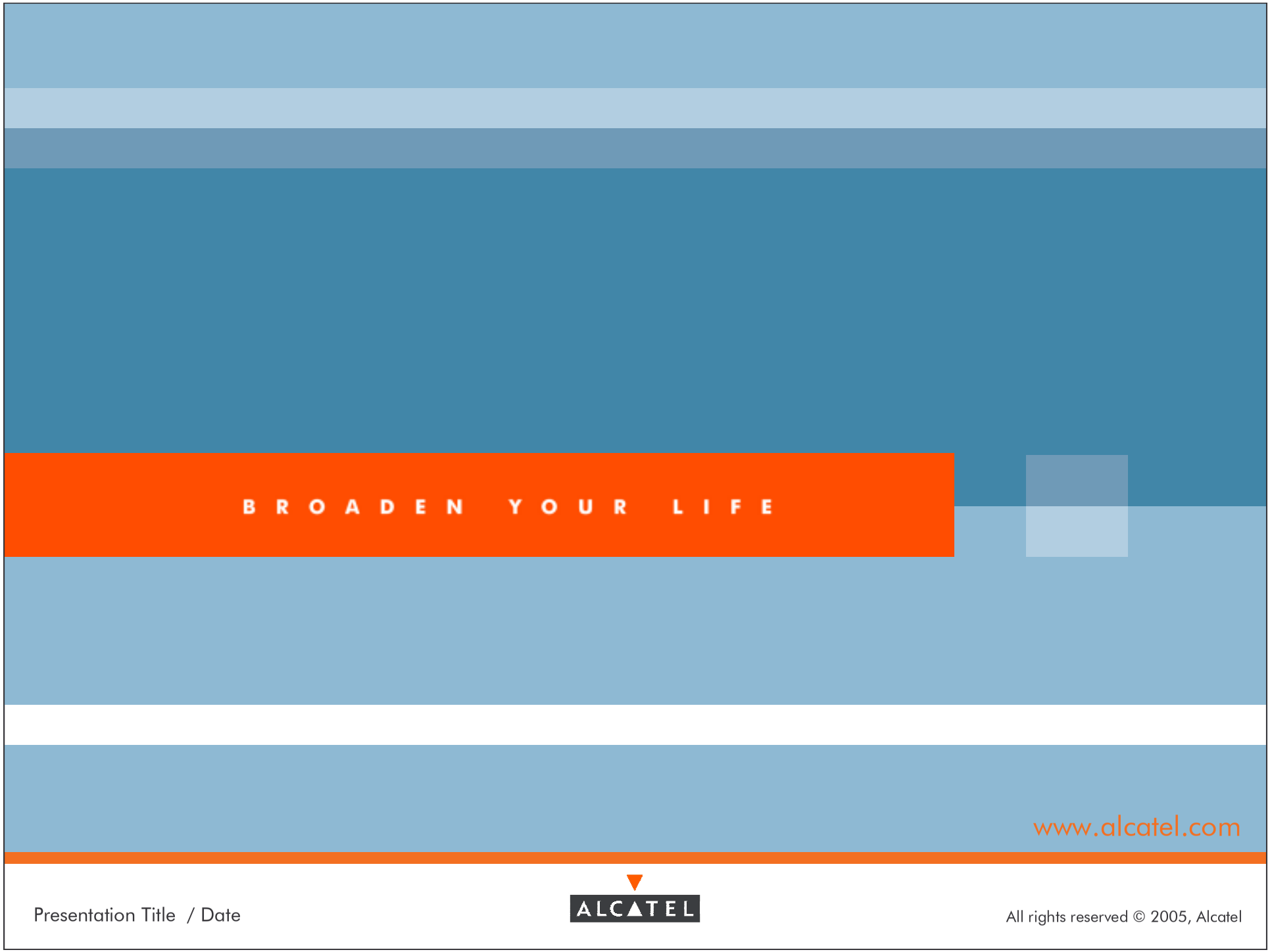
VULNERABILITIES MANAGEMENT

MONITORING



CURATIVE ACTIONS

ALCATEL


BROADEN YOUR LIFE
www.alcatel.com
Presentation Title / Date
ALCATEL
All rights reserved © 2005, Alcatel

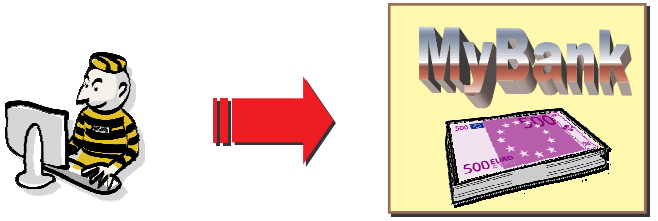
The 400 vulnerabilities of year 2003 (Source Cert-IST)

Involved Environment			
Microsoft Windows	44		Windows-related vulnerability, typically trojan horse, remote rpc, etc …
Microsoft Others	13		Other Microsoft vulnerabilities (server packages, messaging, office pack etc …)
Microsoft IE Explorer	6		Internet Explorer Vulnerability, creating risk through browsing
Viruses	51		Virus alerts, usually spreading by mail attachment.
(Total Microsoft)	*(114)*		*All Vulnerabilities affecting « the standard workplace » or NT-based servers*
UNIX	102		UNIX related system & IP (DNS, LDAP …) vulnerabilities (NB some may affect also Linux)
Linux	49		Linux-related –and specific- vulnerabilities
WEB Tools	26		Web editing or browsing vulnerabilities
Cisco Networking	13		Flaws in Routers, and/ or IOS software, including Call manager or VPN
Firewall & Security Tools	**20**		Identified flaws in Firewall/ VPN equipment. (yes there have been some !)
Network Management	19		Vulnerabilities related to NMS or SNMP protocol
Others	65		…

Virus, Failles et Cybercriminalité

Les Failles, les exploits et les Virus sont des armes à la disposition des cyber-criminels

Une nouvelle (?) génération de Vers destinés au vol de « données bancaires » (exemples Bizex ou Bankash)

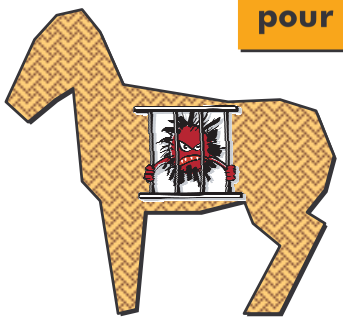


Transaction Bancaire frauduleuse

Etablissement d'un canal IRC pour envoi des données capturées

Exploitation de Failles (IE, Windows) pour s'installer

Propagation par e-Mail ou IM



Cheval de Troie

Fonction Keylogger

Transaction Bancaire en ligne (autorisée)

ALCATEL