Direction centrale de la sécurité des systèmes d'information
(DCSSI)

Sous-direction Opérations
(SDO)

Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques

(CERTA)

Complexité des programmes

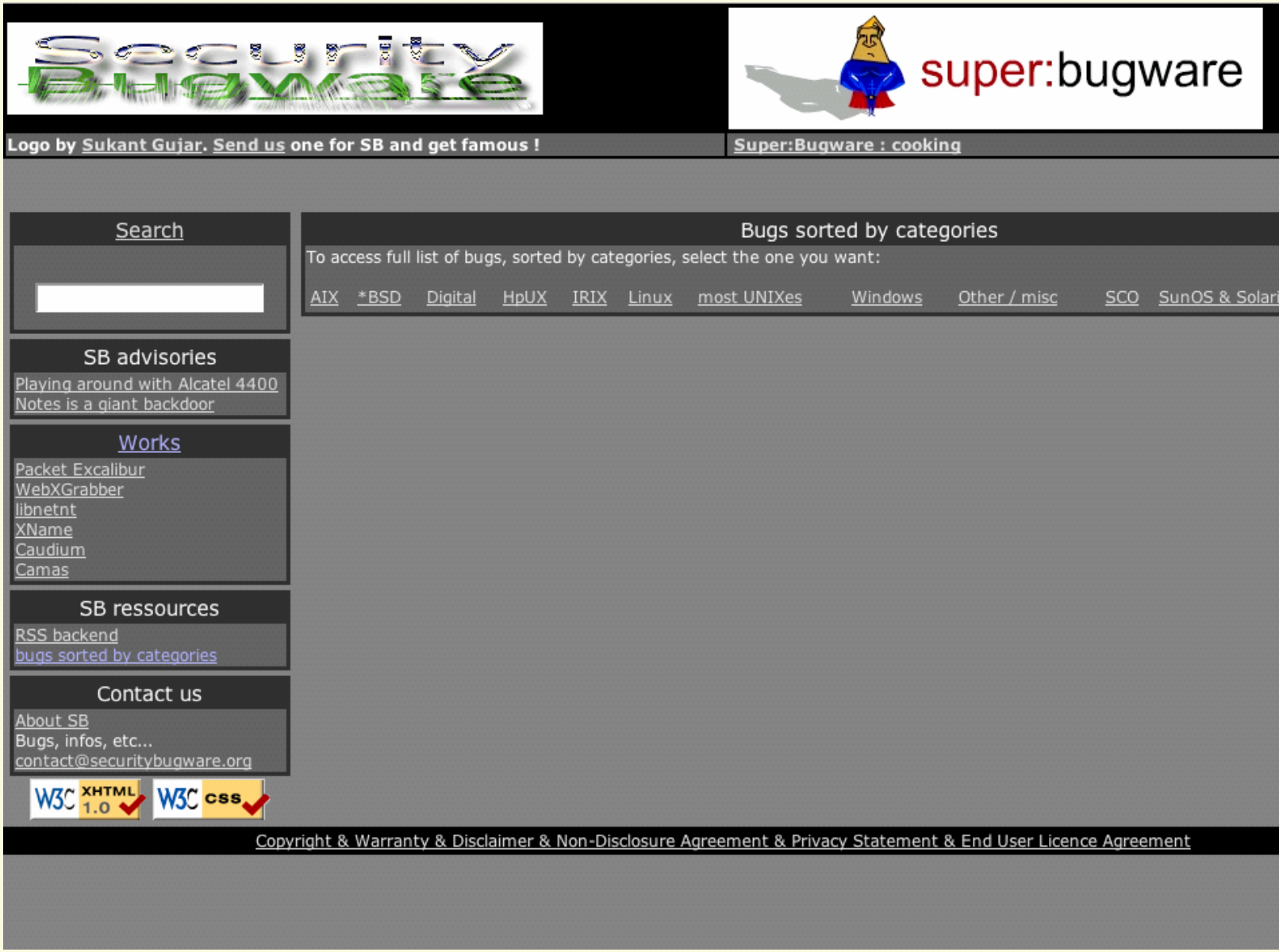
- Le niveau de sécurité d'un poste de travail est directement lié au nombre des vulnérabilités qu'il contient et à leur niveau de gravité.

- Le nombre des vulnérabilités résiduelles contenues dans un programme est directement proportionnel à son importance et à sa complexité. Bruce SCHNEIER cite dans un de ses livres (Secrets et mensonges) :

Système d'exploitation	*Année*	*Lignes de code*
Windows 3.1	1992	3 millions
Windows NT	1992	4 millions
Windows 95	1995	15 millions
Windows NT 4.0	1996	16,5 millions
Windows 98	1998	18 millions
Windows 2000	2000	35 à 60 millions

Les menaces

- Tout système d'exploitation et tout logiciel comportent des erreurs (volontaires ou involontaires).
- Il existe de nombreux sites permettant, en fonction d'un système d'exploitation ou du numéro de version d'un logiciel, de connaître les failles associées.
- On trouve également de nombreux sites qui proposent un ensemble d'outils permettant d'exploiter ces failles.


Security Bugware
super:bugware
Logo by Sukant Gujar. Send us one for SB and get famous !
Super:Bugware : cooking
Search
SB advisories
Playing around with Alcatel 4400
Notes is a giant backdoor
Works
Packet Excalibur
WebXGrabber
libnetnt
XName
Caudium
Camas
SB ressources
RSS backend
bugs sorted by categories
Contact us
About SB
Bugs, infos, etc...
contact@securitybugware.org
W3C XHTML 1.0
W3C CSS
Bugs sorted by categories
To access full list of bugs, sorted by categories, select the one you want:
AIX *BSD Digital HpUX IRIX Linux most UNIXes Windows Other / misc SCO SunOS & Solaris PalmOS
Copyright & Warranty & Disclaimer & Non-Disclosure Agreement & Privacy Statement & End User Licence Agreement

Logo by Sukant Gujar. Send us one for SB and get famous !

Super:Bugware : cooking

Search

SB advisories
- Playing around with Alcatel 4400
- Notes is a giant backdoor

Works
- Packet Excalibur
- WebXGrabber
- libnetnt
- XName
- Caudium
- Camas

SB ressources
- RSS backend
- bugs sorted by categories

Contact us
- About SB

Bugs, infos, etc...
contact@securitybugware.org

W3C XHTML 1.0 W3C CSS

NTBug List Page

Apr 16th	new	win2k.sys - NT - Windows 2003 win2k.sys vulnerability
Apr 16th	new	veritas backupExec - NT - Veritas BackupExec 9.0 is vulnerable to Slammer worm
Apr 11th	new	Microsoft VM - NT - Microsoft Virtual Machine Bytecode Verifier Vulnerability
Apr 10th	new	Hyperion FTP Server - NT - Hyperion FTP Server Buffer Overflow (DoS & remote access)
Apr 10th	new	Microsoft Proxy Server / Internet Security and Acceleration Server - NT - Microsoft Proxy Server and Internet Security and Acceleration Server DoS
Apr 10th	new	Portable Executable (PE) File Format For Win32 - NT - Portable Executable (PE) File Format For Win32 analysis and vulnerabilities
Apr 9th	new	mIRC - NT - mIRC dcc filename spoofing
Apr 6th	new	QuickTime - NT - Buffer Overflow in Windows QuickTime Player
Apr 6th	new	kernel - NT - Microsoft Windows XP Redirector Local Buffer Overflow Vulnerability
Mar 26th	new	JWALK - NT - JWALK application server Directory Traversal Vulnerability
Mar 26th	new	Emule - NT - Emule 0.27b remote crash
Mar 26th	new	Symantec - NT - Symantec Enterprise Firewall (SEF) HTTP URL pattern evasion issue
Mar 18th	update	kernel - NT - IIS remote buffer overflow due to WebDAV/ntdll.dll
Mar 9th	update	MAILsweeper - NT - MAILsweeper MIME attachment evasion
Mar 18th	update	kernel - NT - IIS remote buffer overflow due to WebDAV/ntdll.dll
Mar 22th	new	ActiveSync - NT - ActiveSync DoS
Mar 22th	new	kernel - NT - NT Service Killer
Mar 18th	update	kernel - NT - IIS remote buffer overflow due to WebDAV/ntdll.dll
Mar 20th	new	ISA - NT - ISA Server DNS Intrusion DoS
Sep 26th	new	Internet Explorer - NT - Microsoft Internet Explorer Still Download And Execute ANY Program Automatically
Sep 26th	new	IIS - NT - Special device access and DoS in Internet Exporer/Outlook Express/Outlook
Sep 26th	new	Opera - NT - Opera we browser javascript protocol permit to read cookies/filesystem/cache
Sep 26th	new	Office - NT - A variant of "Word Mail Merge" vulnerability
Sep 26th	new	Messenger - NT - MSN Messenger OCX Buffer Overflow
Sep 26th	new	4D - NT - 4D webserver buffer overflow
Sep 26th	new	Flash - NT - Macromedia Flash IE plugin (flash.ocx) buffer overflow

6th Apr 2003 [SBWID-6107]

COMMAND

Microsoft Windows XP Redirector Local Buffer Overflow Vulnerability

SYSTEMS AFFECTED

Microsoft Windows XP
Microsoft Windows XP SP1

PROBLEM

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

NSFOCUS Security Advisory(SA2003-01)

Topic: Microsoft Windows XP Redirector Local Buffer Overflow Vulnerability

Release Date: 2003-3-27

CVE CAN ID: CAN-2003-0004

Affected system:

- - Microsoft Windows XP
- - Microsoft Windows XP SP1

Summary:

NSFOCUS Security Team has found a buffer overflow vulnerability in Microsoft Windows XP Redirector. Exploiting the vulnerability local attackers could crash the system or gain local system privilege by carefully crafted code.

Description:

The Windows Redirector is used to access files, whether local or remote.It is used to access network shares by net use command.

A security vulnerability exists in the Windows Redirector on Windows XP.An unchecked length in handling the received parameter information causes a buffer overflow vulnerability. Exploiting the vulnerability a non-privileged user could cause system blue screen and reboot. If the code was carefully crafted, attackers could execute arbitrary command in system privilege. At present no remote exploitation method has been found.

packet storm | Archives | Forums | search | /// Switch Mirror Site | go

about | forums | assessment | defense | papers | magazines | miscellaneous | links

Section: .. / DoS /

Denial of Service tools are for use when testing your own machines only - If you use them against other people you are very lame. Also be aware that many windows binaries in this section are flagged by AV software because they have "offensive" capabilities. Only run these programs on test machines against test machines. Use of these tools on a test network is essential to stress testing a stable environment.

Page 1 of 11

<< **1** 2 3 4 5 6 7 8 9 10 11 >>

Files 1 - 25 of 265

Currently sorted by: File Name

Sort By: Last Modified, File Size

/// File Name:	6tunneldos.c
Description:	IPV6 connection flooder which also works as a DoS for 6tunnel.
Author:	Awayzzz
File Size:	2816
Last Modified:	Oct 25 08:26:32 2001
MD5 Checksum:	1d8c93ed83ec40ff9aa443bc1e0d0166

/// File Name:	7plagues.pl
Description:	7plagues.pl is a threaded 7-headed Denial of Service, which should be used to test/audit the TCP/IP stack stability on your different Operating Systems, under extreme network conditions. The seven different DoS implemented there (1 over udp, 2 over icmp, 2 over igmp, 1 over tcp and 1 using random protocol numbers) exploit some known bugs of various networking proto stacks. Requires Net::RawIP.
Author:	51
File Size:	11561
Last Modified:	May 22 01:54:27 2001
MD5 Checksum:	3cbae956a1f1b3b5b50be77027a6793c

/// File Name:	ACME-localdos.c
Description:	Local linux denial of service attack tested on Slackware 8.1 and 9.1, Redhat 7.2, and OpenBSD 3.2. Uses fork() and LD_PRELOAD.
Author:	Acme
File Size:	765
Last Modified:	Nov 8 03:23:44 2003
MD5 Checksum:	c096201996222a58fc56350c3bdf885f

/// File Name:	aimrape.tar.gz

/// Last 10 Files

:· 042004.txt
:· msxml3dll.txt
:· 2425ouch.txt
:· sa11590.txt
:· monit41.pl
:· sasserftpd.c
:· paxdos.c
:· phpshop_29-04-04.txt
:· getlvcb.c
:· hatsquad.txt

[Last 20 | Last 50 | Last 100]

/// Last 10 Advisories

:· 042004.txt
:· msxml3dll.txt
:· 2425ouch.txt
:· sa11590.txt
:· phpshop_29-04-04.txt
:· hatsquad.txt
:· 1242.html
:· sa11567.txt
:· 57555.html
:· efFingerD.txt

[Last 20 | Last 50 | Last 100]

/// Last 10 Exploits

:· monit41.pl
:· sasserftpd.c
:· paxdos.c
:· getlvcb.c
:· emule042e.pl
:· auxploit-1.0.tgz
:· 305-pound.c
:· WFBE.txt
:· win_msrpc_lsass_ms04-11_Ex.c
:· waraxe-2004-SA028.txt

[Last 20 | Last 50 | Last 100]

packet storm | Archives | Forums | search | /// Switch Mirror Site | go

about | forums | assessment | defense | papers | magazines | miscellaneous | links

Section: .. / Last 20 Exploit Files /

/// File Name:	monit41.pl
Description:	Remote exploit for Monit 4.1 that uses connect back shellcode. This exploit makes use of a buffer overrun when an overly long username is passed to the server.
Author:	Shadowinteger
Related File:	monit.txt
File Size:	7042
Last Modified:	May 11 19:23:39 2004
MD5 Checksum:	25f80041bd01686cdfe6e4a1c1287a64

/// File Name:	sasserftpd.c
Description:	Remote exploit for the Sasser worm ftpd server that spawns on port 5554.Targets included for Windows XP and 2000. Note: To use this against Sasser.e, change the port to 1023.
Author:	mandragore
Related Exploit:	win_msrpc_lsass_ms04-11_Ex.c
File Size:	8033
Related CVE(s):	CAN-2003-0533
Last Modified:	May 11 19:18:52 2004
MD5 Checksum:	be9399c6c8b87c60bab1a07bd359570a

/// File Name:	paxdos.c
Description:	PaX with CONFIG_PAX_RANDMMAP for Linux 2.6 denial of service proof of concept exploit the send the kernel into an infinite loop. Originally discovered by ChrisR.
Author:	Shadowinteger
File Size:	3178
Last Modified:	May 11 06:45:27 2004
MD5 Checksum:	001c4ea7efedf19d582a2e5969a9939b

/// File Name:	getlvcb.c
Description:	Local exploit for IBM AIX versions 4.3.3, 5.1 and 5.2 which are vulnerable to a buffer overflow. The overflow is caused by improper bounds checking via the getlvcb and putlvcb utilities. By supplying a long command line option, a local attacker, with root group privileges, could overflow a buffer and gain root privileges on the system.
Author:	matt0x
Homepage:	http://www.secnetops.com

/// Last 10 Files

- 042004.txt
- msxml3dll.txt
- 2425ouch.txt
- sa11590.txt
- monit41.pl
- sasserftpd.c
- paxdos.c
- phpshop_29-04-04.txt
- getlvcb.c
- hatsquad.txt

[Last 20 | Last 50 | Last 100]

/// Last 10 Advisories

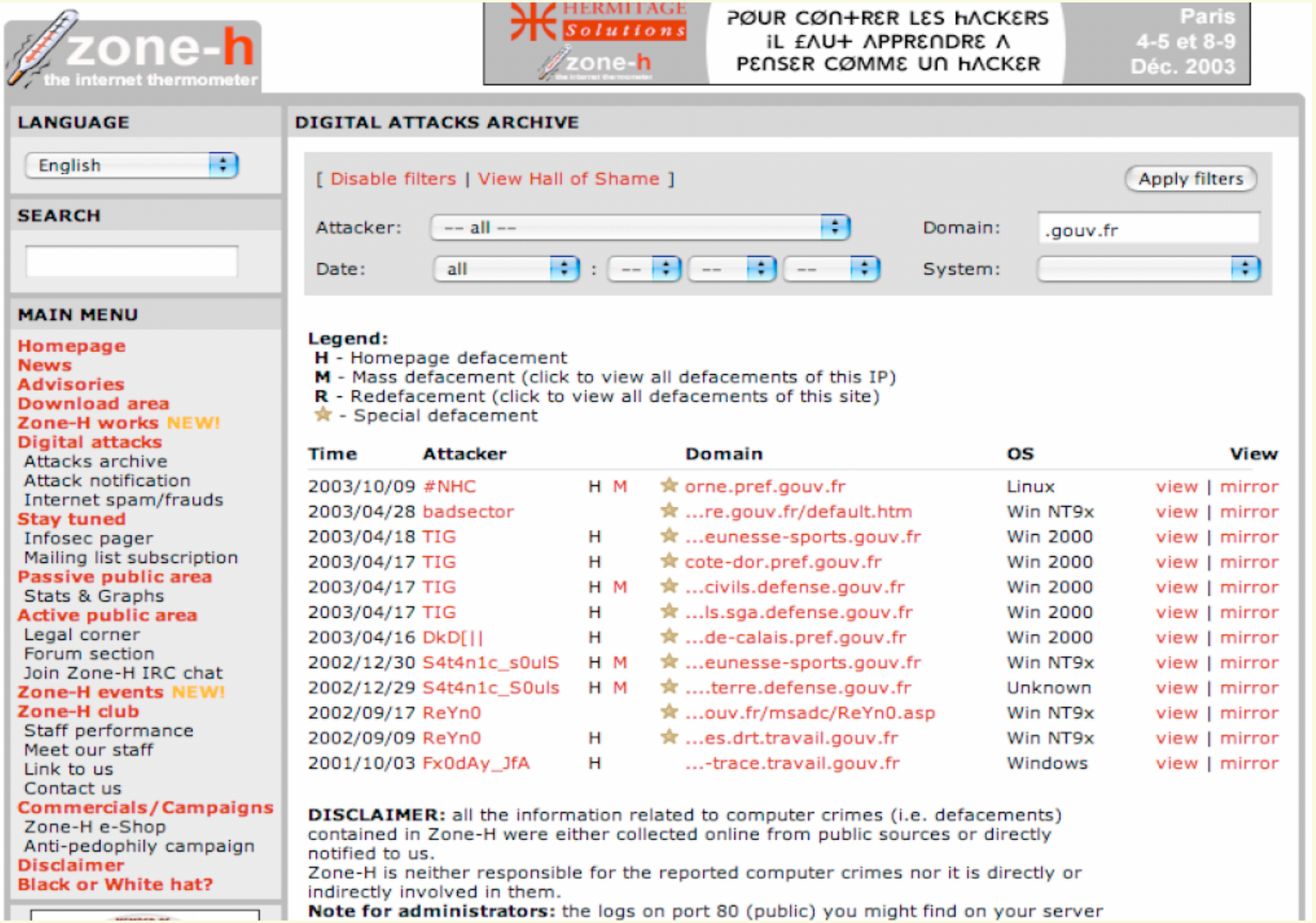
- 042004.txt
- msxml3dll.txt
- 2425ouch.txt
- sa11590.txt
- phpshop_29-04-04.txt
- hatsquad.txt
- 1242.html
- sa11567.txt
- 57555.html
- efFingerD.txt

[Last 20 | Last 50 | Last 100]

/// Last 10 Exploits

- monit41.pl
- sasserftpd.c
- paxdos.c
- getlvcb.c
- emule042e.pl
- auxploit-1.0.tgz
- 305-pound.c
- WFBE.txt
- win_msrpc_lsass_ms04-11_Ex.c
- waraxe-2004-SA028.txt

[Last 20 | Last 50 | Last 100]



zone-h
the internet thermometer

HERMITAGE Solutions
zone-h
PØUR CØN+RER LES hACKERS
iL £AU+ APPRENDRE A
PENSER CØMME UN hACKER
Paris
4-5 et 8-9
Déc. 2003

LANGUAGE
English

SEARCH

MAIN MENU
Homepage
News
Advisories
Download area
Zone-H works NEW!
Digital attacks
Attacks archive
Attack notification
Internet spam/frauds
Stay tuned
Infosec pager
Mailing list subscription
Passive public area
Stats & Graphs
Active public area
Legal corner
Forum section
Join Zone-H IRC chat
Zone-H events NEW!
Zone-H club
Staff performance
Meet our staff
Link to us
Contact us
Commercials/Campaigns
Zone-H e-Shop
Anti-pedophily campaign
Disclaimer
Black or White hat?

DIGITAL ATTACKS ARCHIVE

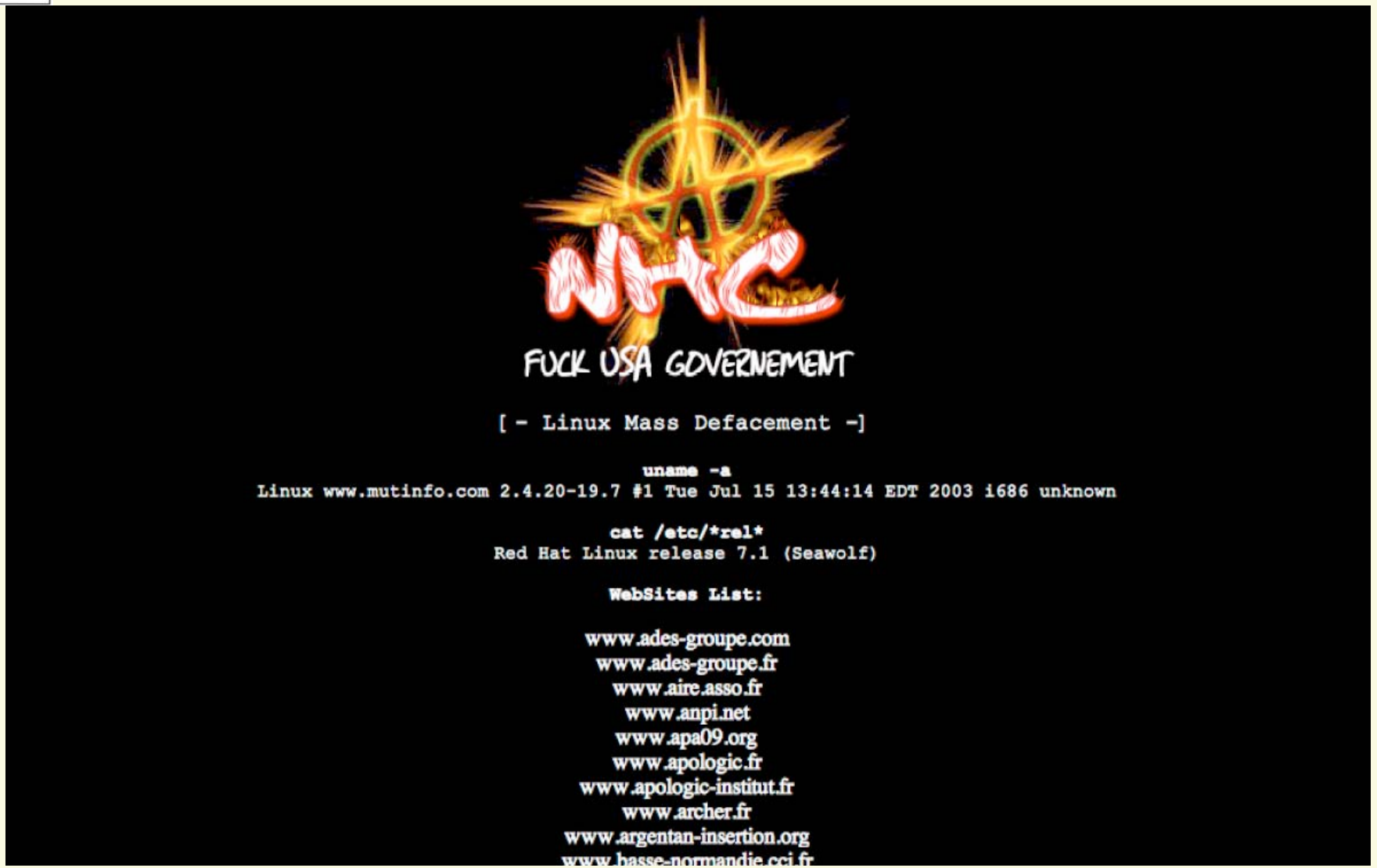
[Disable filters | View Hall of Shame] Apply filters

Attacker: -- all -- Domain: .gouv.fr
Date: all : -- -- -- System:

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
☆ - Special defacement

Time	Attacker			Domain	OS	View
2003/10/09	#NHC	H	M	☆ orne.pref.gouv.fr	Linux	view | mirror
2003/04/28	badsector			☆ ...re.gouv.fr/default.htm	Win NT9x	view | mirror
2003/04/18	TIG	H		☆ ...eunesse-sports.gouv.fr	Win 2000	view | mirror
2003/04/17	TIG	H		☆ cote-dor.pref.gouv.fr	Win 2000	view | mirror
2003/04/17	TIG	H	M	☆ ...civils.defense.gouv.fr	Win 2000	view | mirror
2003/04/17	TIG	H		☆ ...ls.sga.defense.gouv.fr	Win 2000	view | mirror
2003/04/16	DkD[|]	H		☆ ...de-calais.pref.gouv.fr	Win 2000	view | mirror
2002/12/30	S4t4n1c_s0ulS	H	M	☆ ...eunesse-sports.gouv.fr	Win NT9x	view | mirror
2002/12/29	S4t4n1c_S0uls	H	M	☆ ....terre.defense.gouv.fr	Unknown	view | mirror
2002/09/17	ReYn0			☆ ...ouv.fr/msadc/ReYn0.asp	Win NT9x	view | mirror
2002/09/09	ReYn0	H		☆ ...es.drt.travail.gouv.fr	Win NT9x	view | mirror
2001/10/03	Fx0dAy_JfA	H		...-trace.travail.gouv.fr	Windows	view | mirror

DISCLAIMER: all the information related to computer crimes (i.e. defacements) contained in Zone-H were either collected online from public sources or directly notified to us.
Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved in them.
Note for administrators: the logs on port 80 (public) you might find on your server


FUCK USA GOVERNEMENT
[- Linux Mass Defacement -]
uname -a
Linux www.mutinfo.com 2.4.20-19.7 #1 Tue Jul 15 13:44:14 EDT 2003 i686 unknown
cat /etc/*rel*
Red Hat Linux release 7.1 (Seawolf)
WebSites List:
www.ades-groupe.com
www.ades-groupe.fr
www.aire.asso.fr
www.anpi.net
www.apa09.org
www.apologic.fr
www.apologic-institut.fr
www.archer.fr
www.argentan-insertion.org

Les parades

- Connaître parfaitement l'état de son parc informatique :
  - qu'est-ce qui est installé sur chaque machine ;
  - quelles sont les versions du système d'exploitation et des logiciels installés.
- Suivre les *avis* et *alertes* publiant les failles découvertes et les parades associées et appliquer les correctifs proposés.
- Ne pas installer une machine avec l'*installation par défaut* mais installer uniquement les processus strictement nécessaires et les configurer en fonction des besoins.
- Sensibiliser l'ensemble du personnel à la SSI.

Qu'est-ce qu'un CSIRT ?

- Le ***CERT/CC*** (*Computer Emergency Response Team - Coordination Center*) a été créé, fin 1988, en réponse au *« ver Internet »* de novembre 1988.
- Les deux principaux objectifs d'un ***CSIRT*** (*Computer Security Incident Response Team*) sont d'assurer :
  - la détection et la résolution des incidents concernant la SSI ;
  - le conseil pour la mise en place de moyens permettant de prévenir et de se prémunir contre de futurs incidents.

Coopération internationale : FIRST

http://www.first.org

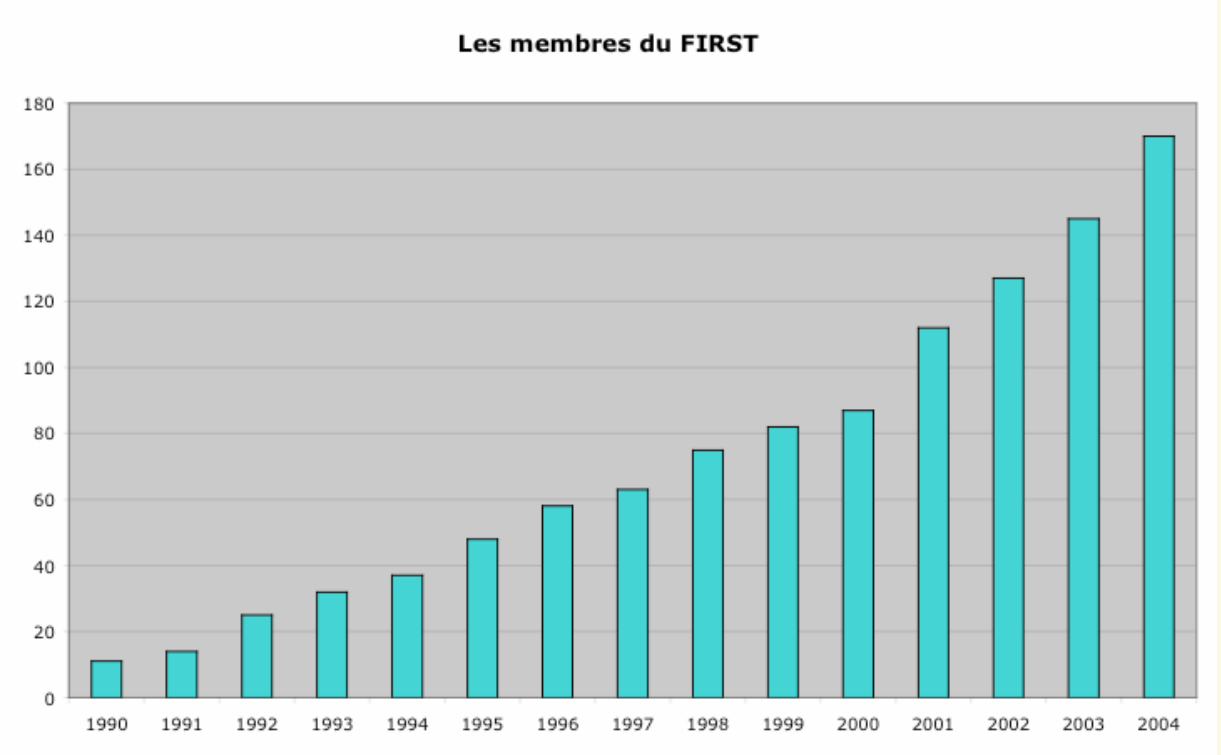
- Le ***FIRST*** (*Forum of Incident Response and Security Teams*) a été créé en 1990 pour fédérer l'ensemble des équipes de réaction aux incidents concernant la sécurité des systèmes d'information.

- Les buts du FIRST sont les suivants :
  - favoriser la coopération entre les équipes ;
  - fournir un moyen de communication commun ;
  - aider au développement des activités des membres ;
  - faciliter le partage des informations relatives à la SSI (outils, méthodes et techniques).

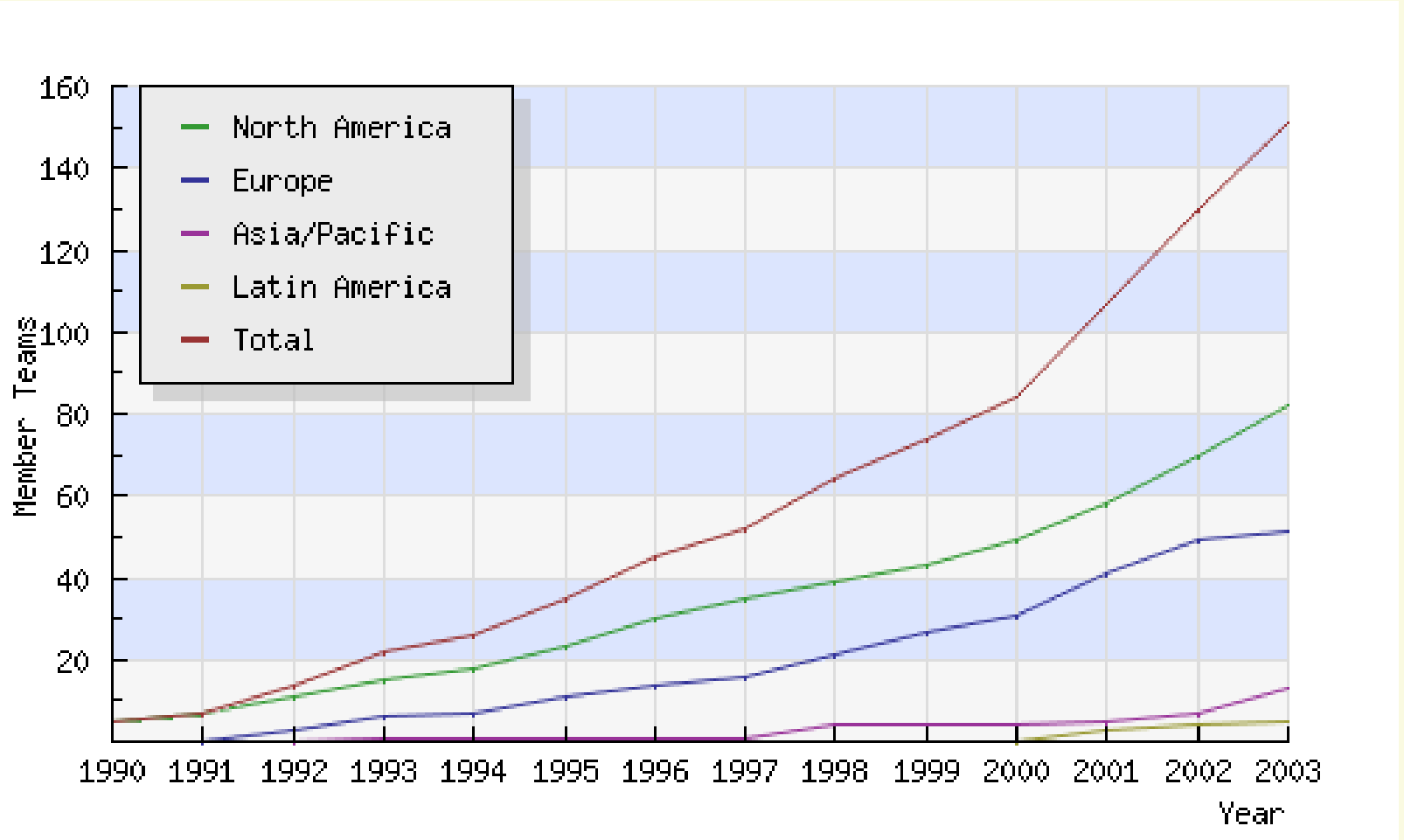
- ***Le CERTA est membre du FIRST depuis le 12 septembre 2000.***

Les membres du FIRST

- Au 27 octobre 2004, le FIRST compte **170** membres (**160** équipes et **10** liaisons).



Les membres du FIRST



Collaboration européenne

Les CSIRTs en Europe : bref historique

1988 : Création du CERT/CC (Etats-Unis)

1990 : Création du FIRST :
(11 membres dont 1 seul européen : *SPAN France*)

1990-1996 : Développement de nombreux CSIRTs en Europe :
Réflexions sur une coopération accrue en Europe,
15 CSIRTs européens membres du FIRST en 1996 (essentiellement « enseignement-recherche »)

1997-1999 : Projet **EuroCERT**
But : créer un « CERT-CC » européen => *échec*

1999-(2002) : **TF-CSIRT**, nombreuses réussites

TF-CSIRT – Première phase : 1999-2002

- Mise en place d'un modèle européen « *d'assurance du niveau de confiance* » (Trusted Introducer).
- Création d'un modèle permettant de définir un incident : IODEF (Incident Object Definition Exchange Format).
- Mise en place d'un « *contact sécurité* » (IRT Object) dans la base RIPE.
- Définition d'outils communs.
- Élaboration d'un programme de formation pour les nouveaux CSIRTs.
- Aide à la création de nouveaux CSIRTs en Europe.

Trusted Introducer

- ***Trusted Introducer*** : un modèle européen « *d'assurance du niveau de confiance* ». Entre autres : *engagements sur la protection des informations*.
- Trois niveaux :
  - « ***Listed*** » *(Level 0)*
  - « ***Accreditation Candidate*** » *(Level 1)*
  - « ***Accredited*** » *(Level 2)*
- Au 27 octobre 2004, il y a :
  - 90 CSIRTs « ***Listed*** »
  - 2 CSIRTs « ***Accreditation Candidate*** »
  - 40 CSIRTs « ***Accredited*** »

registered by TRUSTED Introducer The European CSIRT Directory

*Le CERTA participe à la TF-CSIRT depuis sa création (« **Listed** » depuis le 21 septembre 2000, « **Accreditation Candidate** » depuis le 4 janvier 2002, et « **Accredited** » depuis le 25 mars 2002).*

Trusted Introducer

- Au 27 octobre 2004, la TF-CSIRT regroupe **86** CSIRTs qui se répartissent sur **30** pays :

Allemagne (15), **Autriche** (1), **Belgique** (1), **Chypre** (1), **Croatie** (1), **Danemark** (3), **Espagne** (3), **Finlande** (2), **France** (4), **Grèce** (2), **Hongrie** (2), **Irlande** (1), **Islande** (1), **Israël** (1), **Italie** (2), **Lituanie** (1), **Luxembourg** (1), **Malte** (1), **Norvège** (1), **Pays-Bas** (10), **Pologne** (3), **Portugal** (1), **République Tchèque** (1), **Royaume-Uni** (13), **Russie** (2), **Scandinavie** (1), **Slovénie** (1), **Suède** (4), **Suisse** (5) et **Turquie** (1).

Auxquels s'ajoute quatre CSIRTs « *européens* » (appartenant à des sociétés internationales) : **CISCO**, **ESA**, **IBM** et **SUN**.

Les CSIRTs en France

- Quatre CSIRTs en France (membres du FIRST et/ou TF-CSIRT):
  - *CERTA* (*Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques*)
  - *CERT-IST* (Industrie Services et Tertiaire), CSIRT commercial créé fin 1998, (quatre partenaires: ALCATEL, CNES, ELF et France Télécom)
  - *CERT-RENATER*, partie du GIP RENATER (réseau académique) (*Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche*)
  - *LEXSI*, CSIRT commercial

Statistiques du CERT-RENATER

(juillet à décembre 2000)

- Plus de 600 sites raccordés avec plusieurs millions d'utilisateurs.
- Sur environ 3000 incidents :
  - « *scans* » 77,6 %
  - compromissions 10,7 %
  - relais de « *spam* » 7,2 %
  - déni de service 2,1 %
  - *divers* 1,5 %
  - « *warez* » 0,9 %

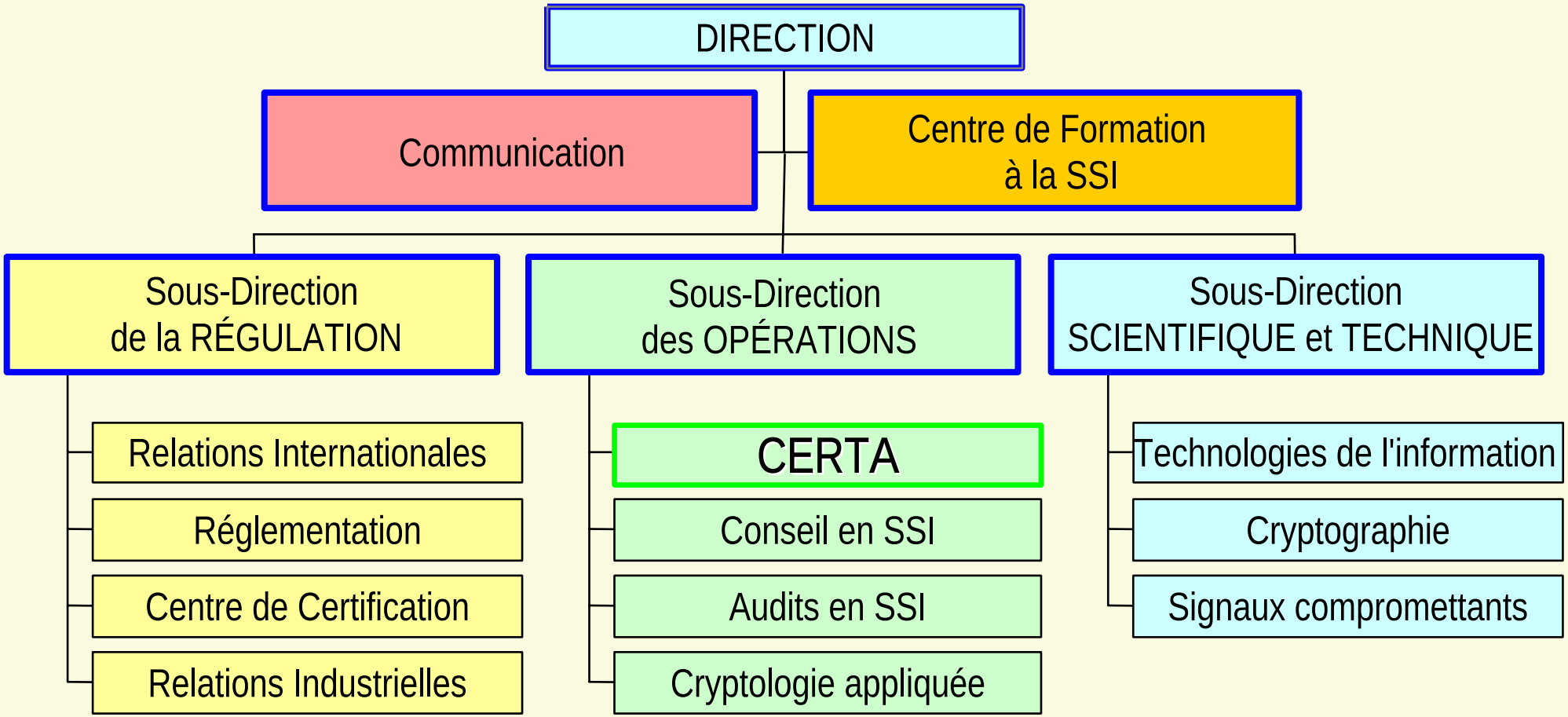
Création du CERTA

- Décision du Comité Interministériel pour la Société de l'Information (CISI) du 19 janvier 1999 :

> *« Renforcer la protection des réseaux de l'État contre les attaques*
>
> *Afin de renforcer et de coordonner la lutte contre les intrusions dans les systèmes informatiques des administrations de l'État, le Gouvernement décide la création d'une structure d'alerte et d'assistance sur l'Internet, chargée d'une mission de veille et de réponse aux attaques informatiques. Placée auprès du Secrétariat Général de la Défense Nationale elle travaillera en réseau avec les services chargés de la sécurité de l'information dans l'ensemble des administrations de l'État. Elle participera au réseau mondial des CERT (Computer Emergency Response Team). »*

Premier ministre
Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information



Les missions du CERTA

(Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques)

- Informer sur les différents types de vulnérabilités ainsi que sur les parades associées, grâce à une activité permanente de recherche, d'analyse et de traitement des failles informatiques.
- Lors d'un incident sur un Système d'Information *et sur demande de l'autorité hiérarchique ou fonctionnelle*, d'aider celle-ci à la compréhension, puis à la résolution de cet incident.
- Dans le cas d'incidents à grande échelle, de réagir sans délai en analysant la nature de l'événement, en identifiant des actions de prévention, protection puis de réparation en diffusant largement cette information vers les cibles atteintes ou potentielles.

Veille technologique

- C'est la base technique du CERTA. Afin de l'assurer correctement, il est nécessaire :
  - de surveiller le plus grand nombre possible de sources d'information ;
  - de recouper ces différentes informations afin de s'assurer de l'existence réelle d'une faille et ne pas propager des rumeurs ;
  - de reproduire éventuellement cette faille sur une plate-forme de test pour en comprendre le mécanisme et les limites ;
  - d'élaborer ou tester la ou les parades associées ;
  - de diffuser un *bulletin d'alerte* expliquant la faille et les moyens de s'en prémunir ;
  - d'inscrire cette faille et l'ensemble des éléments associés dans une base de connaissance pour en conserver la trace et faire croître le niveau d'expertise.

Résolution d'incident

- Pour qu'un incident puisse être résolu le plus rapidement possible, il est nécessaire :
  - d'être prévenu d'un incident dès sa détection ;
  - de réunir l'ensemble des éléments significatifs permettant de résoudre cet incident ;
  - d'estimer la portée de l'incident afin d'informer et/ou de travailler avec les autres CSIRTs à la résolution de cet incident ;
  - d'élaborer avec le *correspondant* une solution, qui sera ensuite appliquée par celui-ci pour traiter l'incident ;
  - d'alimenter la base de connaissance avec les éléments de l'incident.

Réseau de confiance

- Pour qu'un CSIRT soit efficace, il est nécessaire que l'information circule de manière sûre : il doit donc utiliser des moyens de communications de confiance avec ses correspondants. Il existe au moins deux flux d'information entre le CERTA et ses correspondants qui sont de natures très différentes :
  - le sens CERTA vers administration ;
  - le sens administration vers CERTA.

CERTA vers administration

- Ce flux correspond essentiellement aux informations techniques qui sont produites par le CERTA (*bulletin d'alerte*, *note d'information*, ...). Pour que cette information soit exploitée le plus efficacement possible, il est nécessaire :
  - qu'elle arrive le plus rapidement possible aux personnes concernées ;
  - qu'elle soit largement diffusée ;
  - que l'on puisse facilement authentifier l'émetteur et vérifier l'intégrité du message.

⇒ *messagerie Internet avec signature des messages*.

CERTA vers administration

- Deux modes de diffusion de ces informations sont possibles :
  - le CERTA dispose de la liste des correspondants ;
  - le CERTA transmet ces informations vers un correspondant unique, à charge pour celui-ci de les redistribuer dans son entité.

Administration vers CERTA

- Ce flux correspond essentiellement aux informations de type *incident* qui sont déclarées au CERTA. Pour que ces informations soient traitées rapidement et efficacement, il est nécessaire :
  - qu'elles soient validées ;
  - qu'elles soient de *même nature* : besoin de formats et d'outils *normalisés* ;
  - qu'il y ait une garantie sur le traitement confidentiel de ces informations.

⇒ *utilisation d'un chemin sûr*.

Type des documents émis par le CERTA

- Le CERTA émet quatre types de documents :
  - Les AVIS donnent une brève description de la vulnérabilité concernée, de ses conséquences et de la manière de s'en protéger (généralement un *correctif* « *patch* » publié par l'éditeur).
  - Les ALERTES sont des *avis* pour lesquels le moyen de se protéger n'a pas encore été publié (c'est au site de mettre en place les moyens de protection spécifiques à son architecture) ou qui demandent à être traités en urgence.
  - Les NOTES D'INFORMATION sont plus documentées que les simples *avis* ou *alertes* et donnent une explication complète d'un mécanisme.
  - Les RECOMMANDATIONS concernent plus particulièrement des mesures et des méthodes d'organisation.

Documents émis par le CERTA

	2000[1]	2001	2002	2003	2004[2]
ALE (Alertes)	16	23	7	11	20
AVI (Avis)	100	186	346	329	669
INF (Notes d'information)	6	5	3	1	0
REC (Recommandations)	2	1	2	0	0
	124	**215**	**358**	**341**	**689**

[1] 8 mois (1 mai au 31 décembre)
[2] 9 mois (1 janvier au 30 septembre)

Conclusion

- *Plus le CERTA sera informé des incidents, plus le CERTA pourra faire profiter l'ensemble de l'administration (après banalisation des incidents) de l'expérience acquise.*

Comment joindre le CERTA

- *Téléphone* : **01 71 75 84 50**
- *Télécopie* : **01 71 75 84 70**
- *Messagerie* : **CERTA-svp@CERTA.ssi.gouv.fr**
- *Site web* : **http://www.certa.ssi.gouv.fr**

Un incident type …

- Le 23 juin 2000, une faille concernant le serveur *WU-FTPd* est publiée ainsi que l'outil permettant d'exploiter cette faille ;
- Le 10 juillet 2000, installation d'un serveur (*« par défaut »*) ;
- Le 16 juillet 2000, l'administrateur de ce serveur constate un très grand nombre de requêtes de type `finger` ;
- Après analyse du serveur : les *traces* avaient été partiellement effacées, un `root-kit` et un *scanner* avaient été installés.
  Dans les traces du scanner, on trouve les résultats d'une analyse de tous les serveurs FTP de deux classes B ;

Un incident type …

- Résultats :
  - en 2 ou 3 jours, le *scanner* a analysé (au moins) 68539 machines ;
  - parmi ces 68539 machines, 2013 (environ 3%) utilisaient un serveur WU-FTPd ;
  - parmi les 2013 serveurs WU-FTPd, 296 avaient appliqué le correctif nécessaire.

85% des serveurs WU-FTPd étaient vulnérables !
(1717 machines)