Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 03 mars 2006
N° CERTA-2006-ACT-009

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-09

Conditions d'utilisation de ce document : `http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document : `http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-009`

Gestion du document

Référence	CERTA-2006-ACT-009
Titre	Bulletin d'actualité 2006-09
Date de la première version	03 mars 2006
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-009.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-009/

1 Activité en cours

1.1 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 23 février et le 02 mars 2006.

2 Attaque par SSH

Le CERTA a récemment traité un cas de compromission par exploitation d'un mot de passe faible pour le compte `root`. Ce type d'incidents est fréquent, mais il peut être limité en suivant les conseils ci-dessous :

– Il est possible de désactiver les connexions avec le compte `root` dans la configuration du serveur SSH. Toute connexion se fait dès lors avec un compte sans privilège. L'administration de la machine reste possible après utilisation de la commande `su` ou `sudo` (nous recommandons dans ce cas de ne pas mettre de commandes sans mot de passe dans le fichier de configuration de `sudo`).

– Les mots de passe utilisés doivent être forts. Il existe de nombreux outils gratuits disponibles sur l'Internet permettant de tester la robustesse des mots de passe. Par ailleurs, la lecture de la note d'information CERTA-2005-INF-001 est recommandée.
– La surveillance régulière des journaux des serveurs met généralement en évidence ce type d'attaques. En particulier, les administrateurs peuvent suivre de près les connexions SSH réussies (par exemple avec la commande `grep -i accepted /var/log/secure`).

3 Noms de domaine tombés en désuétude

Les noms de domaine se réservent auprès des registres (`registrar`) pour une durée déterminée (souvent un an). À l'issue de cette période de bail, les propriétaires des noms de domaine doivent effectuer un renouvellement. Si cette action n'est pas effectuée, le nom retournera dans le domaine public, et pourra ainsi être réservé par d'autres personnes.

Il arrive que les propriétaires de noms de domaine ne les renouvellent pas par oubli ou les abandonnent volontairement. Ce phénomène peut poser quelques problèmes avec les référencements des sites web. En effet, certains placés dans des domaines tombés en désuétude peuvent être référencés par d'autres sites où dans divers documents. Le problème survient lorsque ces domaines sont rachetés par la suite par des personnes mal intentionnées. Celles-ci peuvent dès lors installer des serveurs web hébergeant du code malveillant ou du contenu pouvant porter atteinte à l'image d'une organisation. Il est ainsi possible de voir des sites gouvernementaux référençant des sites à caractère pornographique.

L'abandon d'un nom de domaine doit faire l'objet d'une information au grand public et aux webmestres afin que les liens vers ces anciens domaines soient modifiés ou supprimés.

4 Liens utiles

– Mémento sur les virus ;
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
– Note d'information sur l'acquisition de correctifs ;
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
– Note d'information pour sur les systèmes obsolètes ;
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
– Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé ;
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
– Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien)
http://www.auscert.org.au/render.html?it=1935

5 Rappel des avis et mises à jour émis

Durant la période du 24 février au 02 mars 2006, le CERTA a émis les avis suivants :

– CERTA-2006-AVI-090 : Vulnérabilité de phplib
– CERTA-2006-AVI-091 : Vulnérabilité de Mambo
– CERTA-2006-AVI-092 : Vulnérabilité de GNU tar
– CERTA-2006-AVI-093 : Vulnérabilité dans Winamp
– CERTA-2006-AVI-094 : Vulnérabilité de unzip
– CERTA-2006-AVI-095 : Multiples vulnérabilités dans Squirrelmail
– CERTA-2006-AVI-096 : Mises à jour de sécurité Mac OS X

Pendant cette même période, les mises à jour suivantes ont été publiées :

– CERTA-2005-AVI-221-003 : Vulnérabilité de gedit
(ajout de la référence au bulletin de sécurité FreeBSD)
– CERTA-2006-AVI-067-001 : Vulnérabilité sur OpenSSH
(ajout de la référence au site Internet OpenSSH et des références aux bulletins de sécurité OpenBSD, SUSE et Ubuntu)

- CERTA-2006-AVI-067-002 : Vulnérabilité sur OpenSSH
  (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2005-AVI-195-004 : Vulnérabilité de libtiff
  (ajout de la référence au bulletin de sécurité Mandriva)
- CERTA-2006-AVI-049-001 : Vulnérabilité de ImageMagick
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2006-AVI-050-001 : Vulnérabilité du package nfs-server
  (changement du titre et ajout de la référence au bulletin de sécurité Debian DSA-975)
- CERTA-2006-AVI-083-001 : Vulnérabilité du logiciel ImageMagick
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2006-AVI-086-001 : Vulnérabilité de GnuPG
  (ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2005-AVI-487-005 : Vulnérabilité de Ethereal
  (ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2005-AVI-490-004 : Vulnérabilité sur le module mod_imap d'Apache
  (ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2006-AVI-013-001 : Vulnérabilité du module mod_ssl dans Apache 2
  (ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2005-AVI-486-004 : Vulnérabilité de Perl
  (ajout de la référence au bulletin de sécurité Solaris)
- CERTA-2006-AVI-086-002 : Vulnérabilité de GnuPG
  (ajout de la référence au bulletin de sécurité SUSE SUSE-SA:2006:013)
- CERTA-2006-AVI-092-001 : Vulnérabilité de GNU tar
  (ajout des références aux bulletins de sécurité Mandriva, Ubuntu et RedHat)

6 Actions suggérées

6.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

6.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

6.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

6.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

6.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

6.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexpliqués et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

6.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

7 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT

23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERT
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERT
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERT
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERT
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070 6101	TCP TCP	BrightStor ARCserve/Enterprise Backup Veritas Backup Exec	– –	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERT
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT

8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CERT
15118	TCP	–	Netdepix	–

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

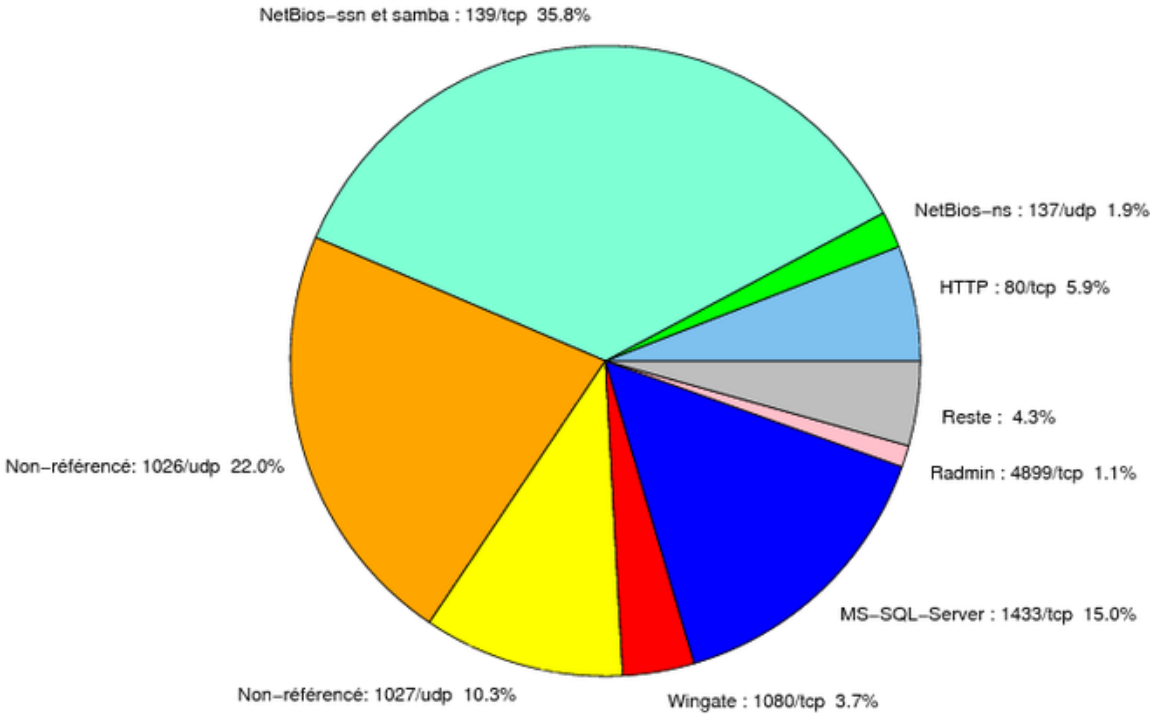

FIG. 1: Répartition relative des ports pour la semaine du 23.02.2006 au 02.03.2006

Liste des tableaux

Gestion détaillée du document

03 mars 2006 version initiale.

port	pourcentage
139/tcp	35,81
1026/udp	21,97
1433/tcp	14,99
1027/udp	10,31
80/tcp	5,91
1080/tcp	3,67
137/udp	1,86
4899/tcp	1,11
1434/udp	0,93
22/tcp	0,49
3128/tcp	0,34
15118/tcp	0,3
10000/tcp	0,28
9898/tcp	0,27
443/tcp	0,19
3306/tcp	0,17
42/tcp	0,14
3127/tcp	0,13
5554/tcp	0,12
2100/tcp	0,11
1023/tcp	0,09
106/tcp	0,08
5000/tcp	0,06
25/tcp	0,05
10080/tcp	0,03
2745/tcp	0,02
6112/tcp	0,01

TAB. 3: Paquets rejetés