Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 janvier 2006
N° CERTA-2006-ACT-002

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-02

Gestion du document

Référence	CERTA-2006-ACT-002
Titre	Bulletin d'actualité 2006-02
Date de la première version	13 janvier 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-002.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-002/

1 Activité en cours

1.1 Incidents traités

1.1.1 Modifications de page web

Le CERTA a récemment traité deux cas de modifications de page web :

– Dans le premier cas, la faille exploitée n'est pas connue. Plusieurs pages d'accueil de sites web hébergés sur la même machine ont été modifiées, mais l'attaque ne s'est pas limitée à ces actions puisqu'un intrus a ajouté un proxy pour faire de l'`irc` (`bouncer`).
– Dans le second cas, la faille exploitée est probablement une vulnérabilité d'un forum phpBB qui n'était pas mis à jour.

1.1.2 Mise en liste noire

Un de nos correspondants nous a informés que ses serveurs de messagerie avaient été mis en liste noire (`blacklist`) par un organisme suite à l'infection de quelques postes par un code malveillant qui émettaient des messages non sollicités (`spams`). L'organisme gérant la liste noire exige qu'un montant d'au moins 50 dollars

soit versé à une association caritative avant de retirer qui que ce soit de cette liste. Le CERTA traite actuellement cet incident. Si vous avez aussi été mis en liste noire, veuillez nous contacter afin que nous vous aidions à en sortir.

1.1.3 Fichier au format WMF malveillant

Un de nos correspondants nous a signalés l'infection de quelques postes sous Windows suite à l'exploitation de la vulnérabilité décrite dans l'alerte CERTA-2005-ALE-019. Il s'agit pour le moment du premier cas porté à notre connaissance. Nous rappelons que Microsoft a mis à disposition un correctif concernant cette vulnérabilité (voir avis CERTA-2006-AVI-011). Toutefois, ce correctif ne résoud pas tous les problèmes liés aux fichiers au format WMF. Il subsiste quelques vulnérabilités qui sont connues et ont été rendues publiques, mais selon Microsoft, l'impact de celles-ci se limitent à des problèmes de stabilité d'application (voir le message posté sur http://blogs.technet.com/msrc/archive/2006/01/09/417198.aspx).

1.1.4 Infections par Sober

Le CERTA a été informé de multiples infections par le ver `Sober`. L'activité liée à ce ver se caractérise par de nombreuses tentatives vers les sites :

- people.freenet.de
- scifi.pages.at
- free.pages.at
- home.pages.at
- home.arcor.de

Recommandation :

L'examen des journaux des éventuels proxies permet de découvrir facilement ces infections. Le but des connexions vers les sites mentionnées ci-dessus est de télécharger des exécutables. Les machines infectées peuvent donc par la suite adopter un comportement imprévisible.

2 Correctifs de Microsoft

En marge du correctif concernant les fichiers WMF, Microsoft a émis deux bulletins ce mois-ci concernant des failles critiques relatives à l'affichage des polices web et au format TNEF dans les messages. Cette dernière (avis CERTA-2006-AVI-018) peut faire l'objet d'un ver. Il est important d'appliquer ces correctifs (conformément à votre politique de sécurité).

2.1 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 29 décembre 2005 et le 05 janvier 2006.

3 Liens utiles

- Mémento sur les virus ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-MEM-001.pdf
- 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
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien)
  http://www.auscert.org.au/render.html?it=1935

4 Rappel des avis et mises à jour émis

Durant la période du 06 au 12 janvier 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-011 : Disponibilité du correctif sur la vulnérabilité Microsoft diffusée par l'alerte CERTA-2005-ALE-019
- CERTA-2006-AVI-012 : Vulnérabilité dans ClamAV
- CERTA-2006-AVI-013 : Vulnérabilité du module mod_ssl dans Apache 2
- CERTA-2006-AVI-014 : Multiples vulnérabilités dans postgreSQL
- CERTA-2006-AVI-015 : Vulnérabilité dans auth_ldap pour Apache
- CERTA-2006-AVI-016 : Vulnérabilité dans uucp et uustat sous Solaris
- CERTA-2006-AVI-017 : Vulnérabilité dans Microsoft Windows
- CERTA-2006-AVI-018 : Vulnérabilité dans Microsoft Outlook et Exchange
- CERTA-2006-AVI-019 : Vulnérabilités dans QuickTime
- CERTA-2006-AVI-020 : Vulnérabilité dans mod_auth_pgsql pour Apache
- CERTA-2006-AVI-021 : Vulnérabilité du système de filtrage ipfw de FreeBSD
- CERTA-2006-AVI-022 : Vulnérabilité de Symantec Norton Protected Recycle Bin
- CERTA-2006-AVI-023 : Vulnérabilité dans Cisco CS-MARS

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

- CERTA-2005-AVI-483-003 : Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées (ajout des références aux bulletins de sécurité Mandriva)
- CERTA-2006-AVI-011-001 : Disponibilité du correctif sur la vulnérabilité (ajout de la référence au bulletin de sécurité Avaya)
- CERTA-2005-AVI-490-002 : Vulnérabilité sur le module mod_imap d'Apache (ajout du bulletin de sécurité Mandriva)
- CERTA-2005-AVI-483-004 : Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées (ajout des références aux bulletins de sécurité Debian)
- CERTA-2005-AVI-483-005 : Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées (remplacement de l'avis Fedora FEDORA-2005-1122 par l'avis FEDORA-2005-027 du 11 janvier 2006, remplacement des avis RedHat RHSA-2005-867 et RHSA-2005-878 par respectivement les avis RHSA-2006-0163 et RHSA-2006-0177 du 11 janvier 2006 ; ajout des avis Ubuntu USN-236-1 et USN-236-2, SuSE SUSE-SA:2006:001, Mandriva MDKSA-2006:010 et MDKSA-2006:011, Debian DSA-936 et DSA-937, des références CVE CAN-2005-3624 à CAN-2005-3628 et du bulletin sécurité de Chris Evans)
- CERTA-2006-AVI-006-001 : Vulnérabilité dans cpio (ajout des références aux bulletins de sécurité FreeBSD et Mandriva)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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

6 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.

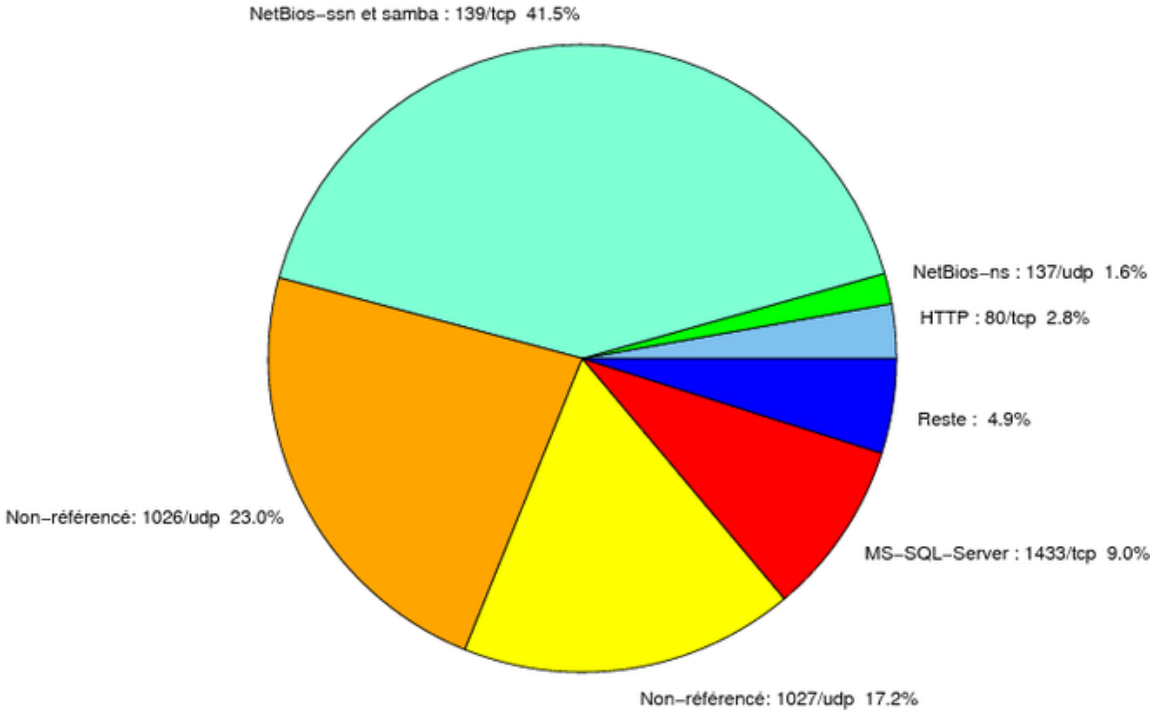

FIG. 1: Répartition relative des ports pour la semaine du 05.12.2005 au 12.01.2006

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
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/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CER
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

port	pourcentage
139/tcp	41,49
1026/udp	23,03
1027/udp	17,22
1433/tcp	8,99
80/tcp	2,79
137/udp	1,57
4899/tcp	0,79
1080/tcp	0,71
1434/udp	0,57
3128/tcp	0,33
15118/tcp	0,3
10000/tcp	0,27
143/tcp	0,2
3127/tcp	0,19
9898/tcp	0,15
5554/tcp	0,1
2100/tcp	0,07
5000/tcp	0,06
111/tcp	0,05
6129/tcp	0,04
25/tcp	0,03
11768/tcp	0,01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

13 décembre 2006 version initiale.