Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 janvier 2006
N° CERTA-2006-ACT-004

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-04

Gestion du document

Référence	CERTA-2006-ACT-004
Titre	Bulletin d'actualité 2006-04
Date de la première version	27 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-004.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-004/

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 29 décembre 2005 et le 05 janvier 2006.

1.1.1 Activité sur le port 106/tcp

Nous avons reçu encore de nombreuses remontées concernant le port 106/tcp qui est largement sondé. Les adresses IP à l'origine de ce trafic semblent peu nombreuses.

Recommandation :

Nous vous conseillons de filtrer le port 106/tcp si vous ne l'utilisez pas et nous vous demandons de nous informer si vous aviez un service en écoute sur ce port.

2 Codes malveillants

2.1 CME-24

Un code malveillant connu sous la référence CME-24 (`Common Malware Enumeration`) et portant différents noms selon les éditeurs d'antivirus (Kama Sutra, BlackWorm, Blackmal, MyWife, Nyxem, ...) se propage depuis plusieurs jours par les vecteurs classiques : message électronique comportant un fichier attaché et partage de fichiers. Ce code malveillant est conçu pour détruire sur les machines infectées les fichiers ayant pour extension `.doc`, `.xls`, `.mdb`, `.mde`, `.ppt`, `.pps`, `.zip`, `.rar`, `.pdf`, `.psd` et `.dmp`. Cette destruction est prévue pour le 03 de chaque mois (attention donc au 03 février prochain).

Les codes malveillants analysés par les éditeurs d'antivirus ajoutent la clé de registre suivante :

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
ScanRegistry = "scanregw.exe /scan"
```

et ajoutent les fichiers suivants :

- `%Root%\Temp.htt`
- `%System%\scanregw.exe`
- `%System%\Update.exe`
- `%System%\Winzip.exe`
- `%System%\WINZIP_TMP.EXE`
- `%Windows%\Rundll16.exe`
- `%Windows%\WINZIP_TMP.EXE`

Les machines infectées sont censées incrémenter un compteur situé sur un serveur web (`webstats.web.rcn.net`).

Des informations complémentaires concernant ce code malveillant sont accessibles depuis le lien suivant :
http://cme.mitre.org/data/list.html#24

Recommandation :

Il est conseillé de filtrer le trafic HTTP à destination de la page `webstats.web.rcn.net/cgi-bin/Count.cgi` et d'examiner les machines à l'origine de cette activité puisque ceci peut être la conséquence d'une infection par ce code malveillant. La plupart des antivirus reconnaissent aujourd'hui ce code malveillant. Toutefois, il est tout à fait possible que de nouvelles versions de ce code malveillant se propagent prochainement sur l'Internet, avec une activité caractéristique différente.

2.2 Expéditeur usurpant une adresse d'un ministère

Un code malveillant se propage par messagerie électronique avec un nom d'expéditeur usurpant le nom de domaine d'un ministère. Le ministère en question n'est en rien responsable de l'envoi de ce message.

Le code malveillant est un fichier avec une extension `.scr` dans une archive `.zip`. L'infection se caractérise par des connexions POP3 vers le serveur `mail.tut.by`.

Recommandation :

Il est conseillé de filtrer le trafic POP3 (port 110/tcp) à destination du serveur `mail.tut.by`, et d'analyser toute machine qui aurait été à l'origine d'un tel trafic.

2.3 Enseignements

Ces deux codes malveillants ne sont pas nouveaux par leur mode de propagation : il s'agit, dans les deux cas, d'inciter un utilisateur à exécuter une pièce jointe. Il ne s'agit donc pas de problèmes techniques, mais de problèmes humains : il est important de sensibiliser les utilisateurs sur les dangers de la messagerie. Les informations concernant l'expéditeur des messages ne constituent pas une donnée fiable. Le CERTA a publié un mémento sur les virus, disponible à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-MEM-001.pdf

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
- 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

4 Rappel des avis et mises à jour émis

Durant la période du 20 au 26 janvier 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-038 : Vulnérabilités dans EMC Legato NetWorker
- CERTA-2006-AVI-039 : Vulnérabilité dans KDE
- CERTA-2006-AVI-040 : Vulnérabilité de ftpd dans HP-UX
- CERTA-2006-AVI-041 : Multiples vulnérabilités dans Cisco Call Manager
- CERTA-2006-AVI-042 : Vulnérabilité d'un composant DM Deployment de Computer Associates
- CERTA-2006-AVI-043 : Vulnérabilité de fetchmail

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

- CERTA-2005-AVI-483-007 : Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2006:0160)
- CERTA-2005-AVI-495-001 : Vulnérabilité de Sudo
  (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2006-AVI-012-003 : Vulnérabilité dans ClamAV
  (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2006-AVI-015-001 : Vulnérabilité dans auth_ldap pour Apache
  (ajout de la référence au bulletin de sécurité Mandriva et à la référence CVE)
- CERTA-2005-AVI-483-008 : Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées
  (ajout de la référence au bulletin de sécurité Debian DSA-950)
- CERTA-2005-AVI-495-002 : Vulnérabilité de Sudo
  (ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2006-AVI-015-002 : Vulnérabilité dans auth_ldap pour Apache
  (ajout des références aux bulletins de sécurité RedHat et Debian)
- CERTA-2006-AVI-039-001 : Vulnérabilité dans KDE
  (ajout des références aux bulletins de sécurité KDE, Mandriva et Gentoo)
- CERTA-2006-AVI-043-001 : Vulnérabilité de fetchmail
  (ajout de la référence au bulletin de sécurité FreeBSD)

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.

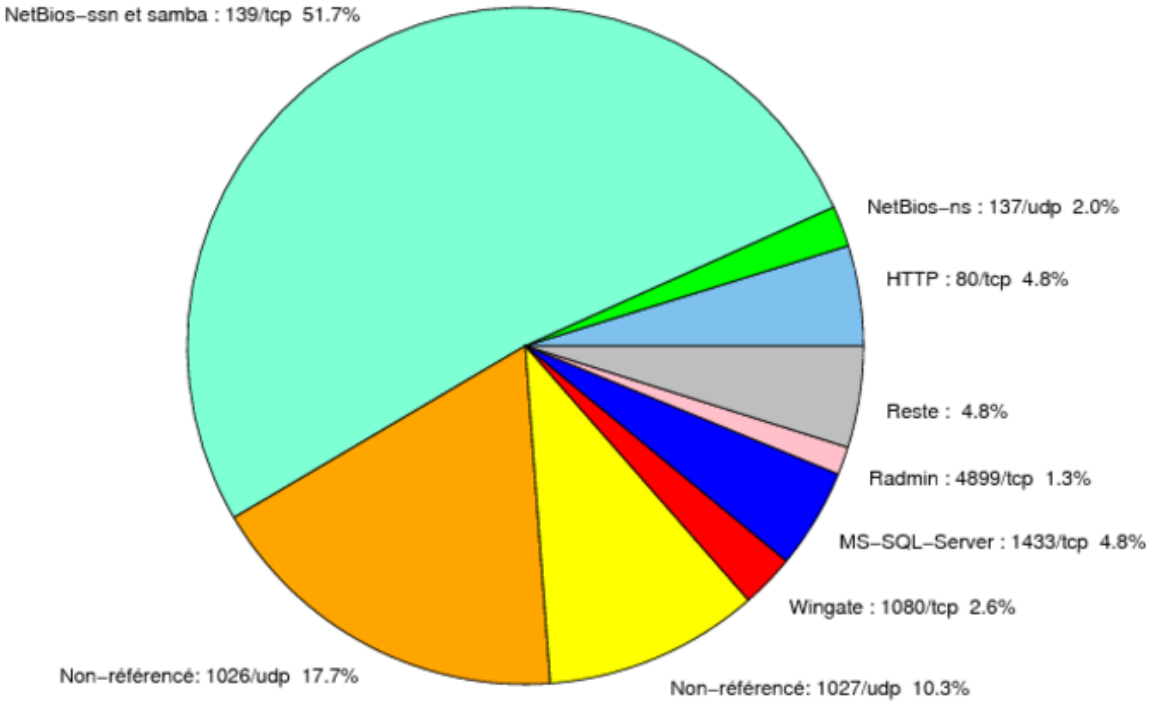

FIG. 1: Répartition relative des ports pour la semaine du 19.12.2005 au 26.01.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER

139	TCP	NetBios-ssn et samba	–	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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
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	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
15118	TCP	–	Netdepix	–

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

port	pourcentage
139/tcp	51,74
1026/udp	17,7
1027/udp	10,29
1433/tcp	4,77
1080/tcp	2,56
137/udp	1,95
4899/tcp	1,33
1434/udp	0,73
3128/tcp	0,61
10000/tcp	0,51
22/tcp	0,42
443/tcp	0,35
9898/tcp	0,3
3127/tcp	0,26
15118/tcp	0,25
5554/tcp	0,2
5000/tcp	0,19
143/tcp	0,16
106/tcp	0,11
1023/tcp	0,1
10080/tcp	0,08
3306/tcp	0,06
25/tcp	0,05
42/tcp	0,03
6101/tcp	0,02
3389/tcp	0,01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

27 janvier 2006 version initiale.