Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 juin 2005
N° CERTA-2005-ACT-025

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-25

Gestion du document

Référence	CERTA-2005-ACT-025
Titre	Bulletin d'actualité n° 2005-25
Date de la première version	24 juin 2005
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.

1 Activité en cours

1.1 Ports observés

Le tableau 3 montre les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 09 et le 16 juin 2005.

1.2 Activité sur le port 139/tcp

Le trafic sur le port 139/tcp continue d'augmenter. Il est désormais en tête des rejets. Le CERTA ne sait toujours pas à quoi correspond ce type de trafic, mais constate qu'il est souvent accompagné de tentatives sur le port 80/tcp.

Recommandation :
Il est fortement recommandé de filtrer le port 139/tcp au niveau du pare-feu.

2 Publication d'un outil exploitant une vulnérabilité de SMB dans Microsoft Windows

Un outil exploitant une vulnérabilité du client SMB de Microsoft Windows a été récemment publié. Cette vulnérabilité avait fait l'objet de l'avis CERTA-2005-AVI-058 le 09 février 2005. Il s'agit d'une vulnérabilité du client SMB, c'est-à-dire qu'un utilisateur mal intentionné doit inciter sa victime à se connecter sur un serveur

malveillant, ce qui peut être fait au moyen de liens de type `file://` insérés dans des messages électroniques par exemple.

D'autre part, une vulnérabilité affectant le serveur SMB a récemment été publiée (avis CERTA-2005-AVI-213), permettant l'exécution de code arbitraire à distance (avis CERTA-2005-AVI-213).

Recommandation :

Il est conseillé d'appliquer sans délai les correctifs indiqués dans les avis CERTA-2005-AVI-058 et CERTA-2005-AVI-213 concernant le client et le serveur SMB :

http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-058/index.html

http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-213/index.html

Par ailleurs, il est recommandé de filtrer les ports 139/tcp et 445/tcp en entrée et en **sortie** (pour empêcher la connexion vers des serveurs malveillants).

3 Rappel des avis et mises à jour émis

Durant la période du 13 au 17 juin 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-202 : Multiples vulnérabilités de Gaim
- CERTA-2005-AVI-203 : Vulnérabilité d'ImageMagick et GraphicsMagick
- CERTA-2005-AVI-204 : Vulnérabilité dans Symantec pcAnywhere
- CERTA-2005-AVI-205 : Vulnérabilité dans les produits Macromedia
- CERTA-2005-AVI-206 : Vulnérabilité de produits Adobe
- CERTA-2005-AVI-207 : Vulnérabilité de GNU wget
- CERTA-2005-AVI-208 : Vulnérabilités de Novell iManager et Novell eDirectory
- CERTA-2005-AVI-209 : Vulnérabilités des versions Sun de Java 2 Standard Edition
- CERTA-2005-AVI-210 : Vulnérabilité dans Microsoft Outlook Express
- CERTA-2005-AVI-211 : Vulnérabilité de Outlook Web Access pour Microsoft Exchange Serveur 5.5
- CERTA-2005-AVI-212 : Vulnérabilité dans l'aide HTML de Windows
- CERTA-2005-AVI-213 : Vulnérabilité dans SMB de Microsoft
- CERTA-2005-AVI-214 : Vulnérabilité du client Telnet Microsoft
- CERTA-2005-AVI-215 : Vulnérabilité de Microsoft ISA Server 2000
- CERTA-2005-AVI-216 : Vulnérabilité des systèmes Microsoft Windows
- CERTA-2005-AVI-217 : Vulnérabilité des systèmes Microsoft Windows
- CERTA-2005-AVI-218 : Vulnérabilités dans Internet Explorer
- CERTA-2005-AVI-219 : Vulnérabilité dans le service WebClient de Microsoft
- CERTA-2005-AVI-220 : Vulnérabilité dans Acrobat et Reader d'Adobe
- CERTA-2005-AVI-221 : Vulnérabilité de gedit
- CERTA-2005-AVI-222 : Vulnérabilité de lpadmin sous Solaris
- CERTA-2005-AVI-223 : Vulnérabilité de Opera
- CERTA-2005-AVI-224 : Vulnérabilité de SquirrelMail
- CERTA-2005-AVI-225 : Vulnérabilité dans SpamAssassin

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

- CERTA-2005-AVI-082-005 : Vulnérabilité de gFTP
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-163-002 : Multiples vulnérabilités de gaim
  (ajout des références aux bulletins de sécurité SUSE et RedHat RHSA-2005:432)
- CERTA-2005-AVI-164-002 : Multiples vulnérabilités dans tcpdump
  (ajout des références aux bulletins de sécurité Gentoo et RedHat RHSA-2005:505. Ajout de la référence CVE CAN-2005-1267. Modification de la référence au bulletin de sécurité Mandriva)
- CERTA-2005-AVI-174-002 : Multiples failles des noyaux Linux
  (ajout du bulletin de sécurité Novell SUSE-SA:2005:029)
- CERTA-2005-AVI-183-002 : Vulnérabiltés dans gzip
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:357)

- CERTA-2005-AVI-188-002 : Multiples vulnérabilités dans bzip2
  (ajout de la référence au bulletin de sécurité SUSE SUSE-SR:2005:015)
- CERTA-2004-AVI-308-002 : Vulnérabilité dans OpenSSH
  (ajout références aux bulletins de sécurité RHSA-2005-495 de Red Hat et MDKSA-2005:100 de Mandriva)
- CERTA-2005-AVI-165-002 : Vulnérabilité dans Squid
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-183-003 : Vulnérabiltés dans gzip
  (ajout de la référence au bulletin de sécurité freeBSD SA-05:11)
- CERTA-2005-AVI-202-001 : Multiples vulnérabilités de Gaim
  (ajout référence au bulletin de sécurité Mandriva)
- CERTA-2005-AVI-164-003 : Multiples vulnérabilités dans tcpdump
  (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:101. Correction des références CVE)
- CERTA-2005-AVI-188-003 : Multiples vulnérabilités dans bzip2
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:474)
- CERTA-2005-AVI-202-002 : Multiples vulnérabilités de Gaim
  (ajout référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-212-001 : Vulnérabilité dans l'aide HTML de Windows
  (mise à jour des systèmes affectés (ajout de Microsoft Windows 2000 SP4)
- CERTA-2005-AVI-213-001 : Vulnérabilité dans SMB de Microsoft
  (mise à jour des systèmes affectés (ajout de Microsoft Windows 2000 SP4)
- CERTA-2005-AVI-081-002 : Vulnérabilité de Midnight Commander
  (ajout des références aux bulletins de sécurité Debian DSA-639, Debian DSA-698 et RedHat RHSA-2005:512. Ajout des références CVE CAN-2004-1009, CAN-2004-1090, CAN-2004-1091, CAN-2004-1093, CAN-2004-1174, CAN-2004-1175 et CVE CAN-2005-0763)
- CERTA-2005-AVI-114-004 : Multiples vulnérabilités de xli
  (ajout du bulletin de sécurité Avaya ASA-2005-134)
- CERTA-2005-AVI-124-004 : Multiples vulnérabilités dans le client Telnet
  (ajout du bulletin de sécurité Avaya ASA-2005-132)
- CERTA-2005-AVI-126-002 : Multiples vulnérabilités dans PHP
  (ajout du bulletin de sécurité Avaya ASA-2005-136)
- CERTA-2005-AVI-131-002 : Vulnérabilité de WU-FTPD
  (ajout bulletin de sécurité Avaya ASA-2005-126)
- CERTA-2005-AVI-164-004 : Multiples vulnérabilités dans tcpdump
  (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:101. Correction des références CVE. Ajout du bulletin de sécurité Avaya ASA-2005-137)
- CERTA-2005-AVI-174-003 : Multiples failles des noyaux Linux
  (ajout du bulletin de sécurité Avaya ASA-2005-120)
- CERTA-2005-AVI-178-002 : Multiples vulnérabilités d'Ethereal
  (ajout du bulletin de sécurité Avaya ASA-2005-131)

4 Actions suggérées

4.1 Respecter la politique de sécurité

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.

4.2 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.

4.3 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.

4.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiat. 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.

4.5 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.

4.6 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 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.

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 6
3 Paquets rejetés 7

Gestion détaillée du document

24 juin 2005 version initiale.

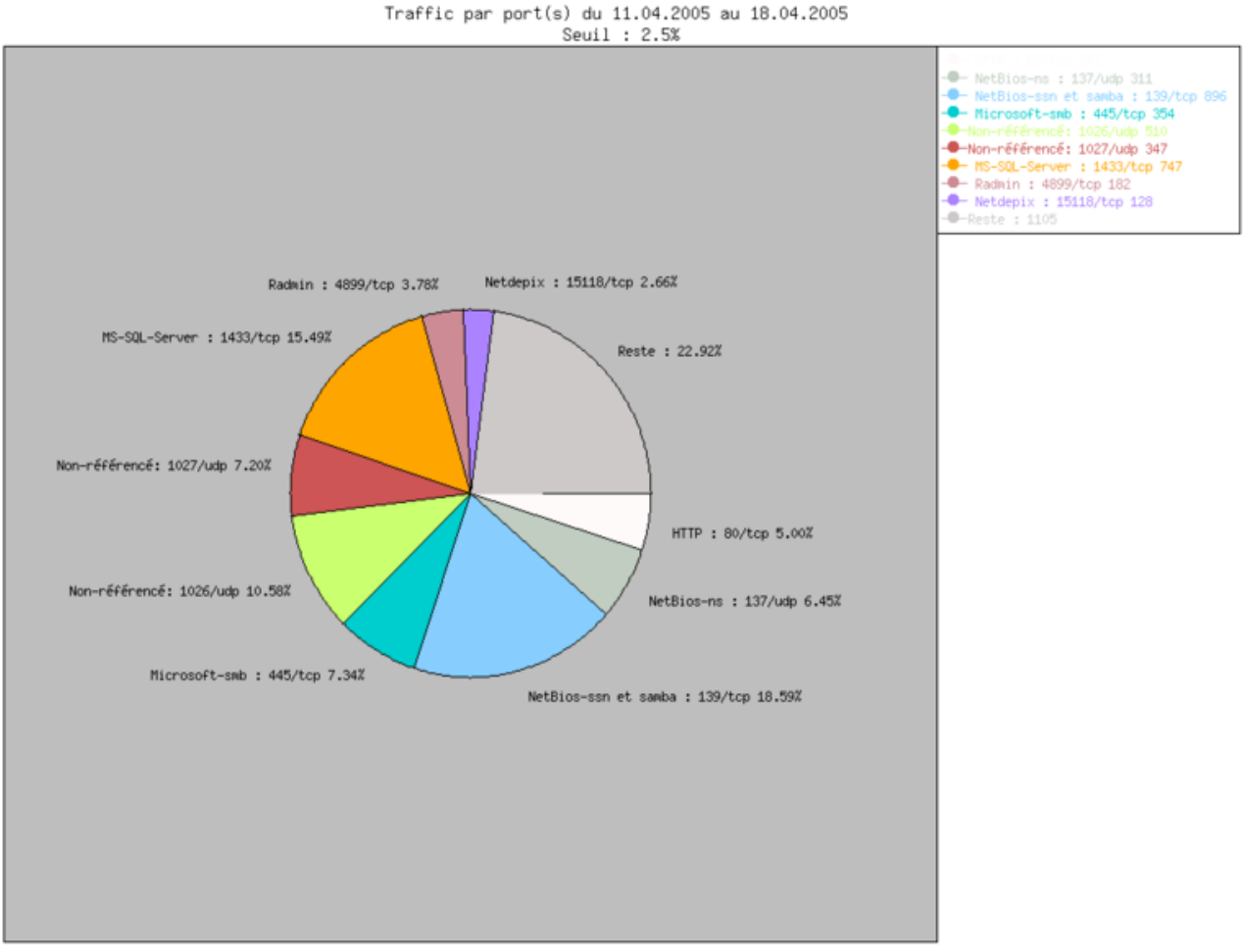

FIG. 1: Répartition relative des ports

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-20 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-13
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-38
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-19 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-23
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-05
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-00 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-11 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-03
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-36 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-16 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-21
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-18
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-00 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-24 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-05
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-00
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-15
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-ALE-00
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-18 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-21
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-16
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-02
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-00
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-21
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

port	pourcentage
139/tcp	34,37
1026/udp	20,83
1027/udp	14,31
80/tcp	13,78
1433/tcp	6,40
137/udp	2,73
4899/tcp	1,58
1434/udp	0,91
445/tcp	0,85
15118/tcp	0,80
1080/tcp	0,47
6129/tcp	0,42
9898/tcp	0,37
5554/tcp	0,36
23/tcp	0,29
22/tcp	0,22
21/tcp	0,19
2745/tcp	0,19
2100/tcp	0,16
443/tcp	0,13
6101/tcp	0,13
25/tcp	0,12
3306/tcp	0,10
111/tcp	0,06
3127/tcp	0,04
3128/tcp	0,04
143/tcp	0,04
11768/tcp	0,04
5000/tcp	0,02
10080/tcp	0,02
42/tcp	0,02
1023/tcp	0,01

TAB. 3: Paquets rejetés