

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-23

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-2005-ACT-023>

Gestion du document

Référence	CERTA-2005-ACT-023
Titre	Bulletin d'actualité n° 2005-23
Date de la première version	10 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 ainsi que la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constaté sur deux dispositifs de filtrage, entre le 26 mai et le 2 juin 2005.

1.2 Incidents traités

1.2.1 Défiguration de site web

le certa a traité un cas de défiguration d'un site web. L'étude est en cours mais la faille exploitée n'est pas encore connue.

1.2.2 Infections par MyTob

Un des correspondants du CERTA a informé de l'infection d'une trentaine de postes par le ver MyTob. Il s'agit d'une version différente de celle dont nous avons déjà parlé dans le bulletin d'actualité CERTA-2005-ACT-021, et qui avait fait l'objet de l'alerte CERTA-2005-ALE-004.

Alors que la première version de MyTob que nous avons rencontrée se caractérisait par des tentatives de connexion sur la machine `irc.blackcarder.net` sur le port 7000/tcp, cette nouvelle version effectuée des connexions vers la machine `195.13.58.92 (195-13-58-92.oxyd.net)` sur le port 6667/tcp.

Recommandation :

L'afflux de nouvelles versions montre bien que la défense ne peut pas reposer uniquement sur les antivirus, même mis à jour, car ces derniers seront tôt ou tard confrontés à une version qui ne sera pas reconnue. Un filtrage en sortie, en interdisant toutes les connexions sauf celles explicitement autorisées, est plus approprié pour empêcher le bon fonctionnement des chevaux de Troie véhiculés par les vers. Une lecture régulière des journaux des dispositifs de filtrage permet de repérer les machines infectées. Le CERTA peut vous assister dans cette analyse.

2 Utilisation du service d'affichage des messages 1026/udp et 1027/udp

Nous constatons régulièrement la présence des ports 1026/udp et 1027/udp dans les paquets le plus souvent rejetés par les équipements de filtrage. Ces deux ports correspondent à l'utilisation du *service d'affichage des messages*. Celui-ci permet l'envoi de messages instantanés apparaissant sur le bureau du destinataire sous forme d'une boîte de dialogue. Les messages les plus fréquemment rencontrés sont de type pourriel (spam). Cependant, il arrive que certains aient une autre finalité. En effet, des messages envoyés se présentant sous la forme de faux messages de sécurité incitent l'utilisateur à télécharger un correctif sur un site distant puis de l'exécuter. Or, ce pseudo-correctif n'est en fait qu'un cheval de Troie. L'utilisateur croyant rendre sa machine plus sûre vient en fait de la compromettre. Dans certains cas, le site distant indiqué dans le pourriel est un site de *phishing*.

Recommandation :

En premier lieu, il convient toujours d'interdire l'accès à ces ports depuis l'Internet. Il est également recommandé de désactiver ce service à moins qu'il ne soit d'une quelconque utilité. Enfin, lorsque vous effectuez une mise à jour de votre système d'exploitation ou d'un logiciel tiers, il est impératif de s'assurer dans la mesure du possible que ce correctif a bien pour origine l'éditeur du logiciel.

3 Rappel des avis et mises à jour émis

Durant la période du 27 mai au 3 juin 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-185 : Multiples vulnérabilités de Ipswitch Imail ;
- CERTA-2005-AVI-186 : Multiples vulnérabilités dans Mailutils ;
- CERTA-2005-AVI-187 : Vulnérabilité des routeurs Nortel ;
- CERTA-2005-AVI-188 : Vulnérabilité dans bzip2 ;
- CERTA-2005-AVI-189 : Vulnérabilité dans Apple Quicktime ;
- CERTA-2005-AVI-190 : Vulnérabilité de divers outils gérant le format ELF ;
- CERTA-2005-AVI-191 : Vulnérabilités dans HP Openview Gestion des applications RADIA.

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

- CERTA-2005-AVI-165-001 : Vulnérabilité dans Squid (ajout des références aux bulletins de sécurité FreeBSD et OpenBSD) ;
- CERTA-2004-AVI-034-007 : Multiples vulnérabilités de XFree86 et XSun (Nouveau titre. Ajout référence au bulletin de sécurité de Sun) ;
- CERTA-2005-AVI-003-007 : Multiples vulnérabilités de libtiff (ajout référence au bulletin de sécurité #57769 de Sun) ;
- CERTA-2005-AVI-124-003 : Multiples vulnérabilités dans le client Telnet (ajout de la référence au bulletin de sécurité Debian DSA-731) ;
- CERTA-2005-AVI-131-001 : Vulnérabilité de WU-FTPD (ajout référence au bulletin de sécurité de Sun) ;
- CERTA-2005-AVI-157-001 : Vulnérabilité dans Xine (ajout des bulletins de sécurités Mandriva et Novell) ;
- CERTA-2005-AVI-161-001 : Vulnérabilité dans phpBB (Ajout de la référence CVE CAN-2005-1193) ;
- CERTA-2005-AVI-163-001 : Multiples vulnérabilités de gaim (ajout des bulletins de sécurité pour OpenBSD et FreeBSD) ;
- CERTA-2005-AVI-166-001 : Multiples vulnérabilités dans PostgreSQL (ajout des références aux bulletins de sécurité Mandriva et RedHat) ;

- CERTA-2005-AVI-170-001 : Vulnérabilité dans FreeRADIUS (ajout du bulletin VuXML sur FreeBSD du 22 mai 2005) ;
- CERTA-2005-AVI-183-001 : Vulnérabilités dans gzip (ajout de la référence au bulletin de sécurité Mandriva) ;
- CERTA-2005-AVI-188-001 : Multiples vulnérabilités dans bzip2 (ajout d'une nouvelle vulnérabilité, de la référence CVE et des références aux bulletins de sécurité Mandriva et Debian).

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 inexplicables 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.

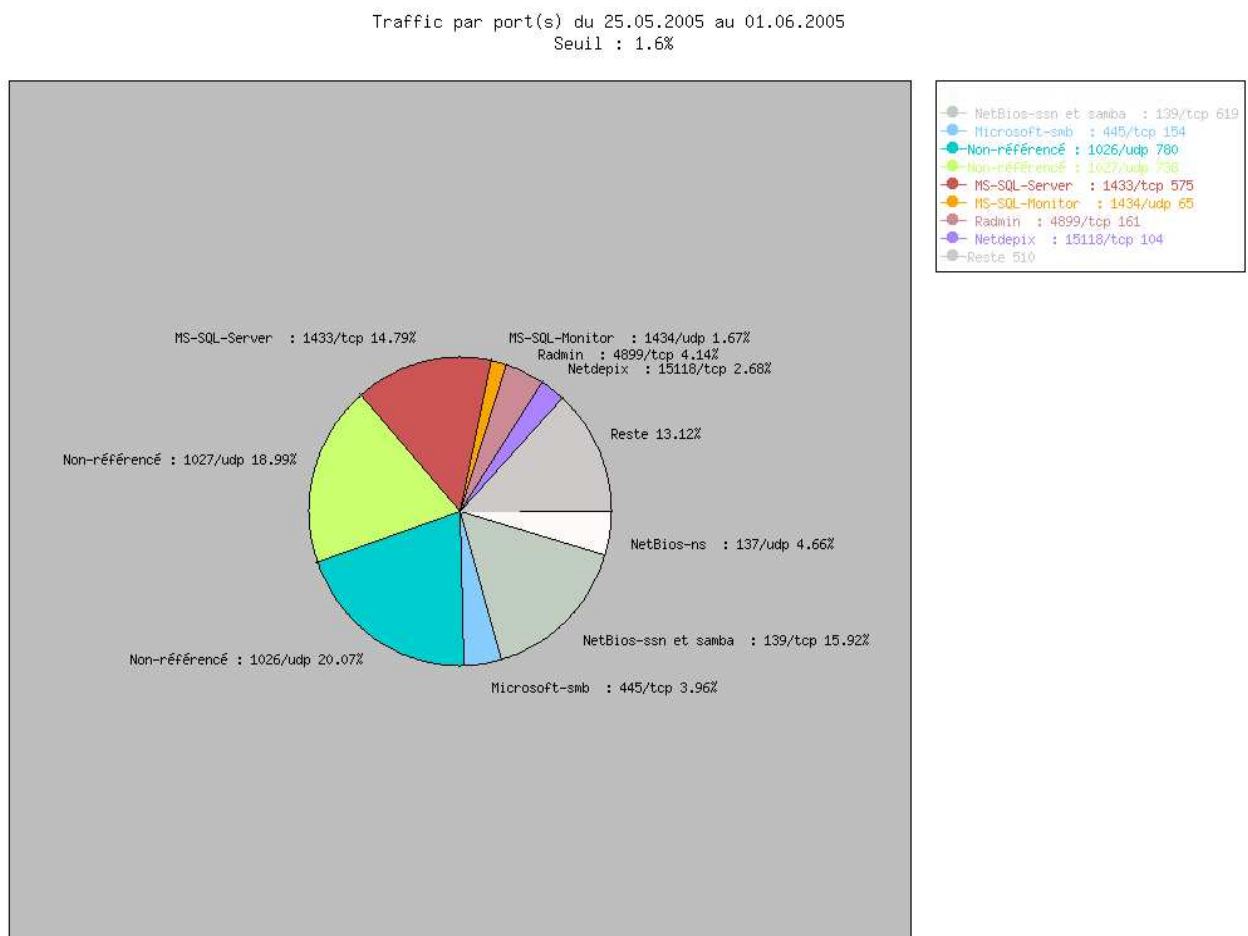


FIG. 1 – Répartition relative des ports

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	5
3	Paquets rejetés	6

Gestion détaillée du document

03 juin 2005 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2004-AVI-066 CERTA-2004-AVI-064 CERTA-2003-AVI-132
22	TCP	SSH	–	CERTA-2003-AVI-152
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	–	CERTA-2005-AVI-133
42	TCP	WINS	–	CERTA-2004-AVI-384
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214
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
1026/udp	27,03
1027/udp	17,99
139/tcp	14,14
1433/tcp	14,05
137/udp	6,40
4899/tcp	3,92
1434/udp	3,08
445/tcp	2,89
15118/tcp	2,74
5554/tcp	1,46
9898/tcp	0,95
1080/tcp	0,93
22/tcp	0,64
2745/tcp	0,52
25/tcp	0,43
3306/tcp	0,29
443/tcp	0,28
80/tcp	0,26
2100/tcp	0,26
5000/tcp	0,22
6129/tcp	0,22
3127/tcp	0,21
23/tcp	0,21
11768/tcp	0,21
21/tcp	0,15
6101/tcp	0,15
42/tcp	0,14
1023/tcp	0,12
111/tcp	0,10
3389/tcp	0,02

TAB. 3 – Paquets rejetés