

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-50

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-050>

Gestion du document

Référence	CERTA-2005-ACT-050
Titre	Bulletin d'actualité n° 2005-50
Date de la première version	16 décembre 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 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 08 et le 15 décembre 2005.

2 Support de Windows NT4 Server

Ce bulletin d'actualité est l'occasion d'un rappel concernant les systèmes d'exploitation Microsoft Windows NT 4.0 Workstation et Microsoft Windows NT 4.0 Server.

Microsoft ne fournit plus de correctifs de sécurité pour Windows NT 4.0 Workstation depuis le 30 juin 2004 et depuis le 31 décembre 2004 pour Windows NT 4.0 Server.

Cependant, un support payant est encore possible sur demande auprès de Microsoft.

Recommandations :

Dans tous les cas, il est impératif de migrer rapidement vers un système d'exploitation alternatif disposant de mises à jour de sécurité. Pour ceux ne disposant pas des correctifs de sécurité via le programme payant, il est impératif de le faire dans les plus brefs délais. En effet, il existe à ce jour plusieurs vulnérabilités critiques impactant

Windows NT 4.0 Workstation et Server, qui sont connues, exploitables à distance (avec du code disponible sur Internet). En l'absence de support payant auprès de Microsoft, de tels systèmes sont hautement à risque.

Pour les cycles de vie des autres systèmes et logiciels, on pourra se reporter à notre note CERTA-2005-INF-003 relative aux systèmes et aux logiciels obsolètes.

3 Les cartes de vœux électroniques

En ces périodes de fêtes, il devient courant de recevoir ou d'envoyer des cartes de vœux électroniques. Nous attirons cependant votre attention sur la provenance des cartes que vous seriez amenés à recevoir. Celles-ci sont souvent au format HTML et contiennent des images ou des animations. De ce fait, il est tout à fait possible à une personne mal intentionnée d'insérer dans ce message du code malveillant destiné à compromettre la machine de la victime.

Recommandations :

De manière générale et plus particulièrement dans le cas des cartes de vœux, il convient de toujours vérifier la provenance des messages électroniques (même si ce n'est pas une garantie absolue) et de configurer votre logiciel de gestion de courrier pour qu'il n'affiche pas le contenu en HTML des messages ou les images en pièces jointes afin d'éviter une infection automatique. Dans tous les cas, si vous recevez un message suspect de ce type, veuillez en informer le CERTA.

4 Le ver Dasher

La presse s'est fait très largement l'écho de la propagation actuelle d'un code malveillant dénommé « dasher ». De façon très classique, ce code se propage en utilisant une vulnérabilité d'un service réseau de Microsoft. Cette vulnérabilité dispose d'un correctif depuis octobre 2005 (publication du CERTA le 24 octobre 2005 : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-403/CERTA-2005-AVI-403.html>).

Ce code malveillant reconnu par des antivirus à jour, installé sur la machine de la victime un outil permettant d'enregistrer toutes les saisies faites sur le clavier (« keylogger »). Par ailleurs, pour conduire l'attaque, le code malveillant doit se connecter sur un site situé en Chine. Il est donc relativement facile de filtrer le trafic afin de rendre le code malveillant inactif.

Concrètement, l'activité du ver sur une machine compromise se traduit par des tentatives de connexions provenant de celle-ci vers l'adresse IP : 222.240.219.143 sur les ports 5262/tcp pour la variante A ou 53/tcp pour la variante B.

En termes de défense en profondeur cette propagation permet de rappeler les éléments fondamentaux suivants :

- la première protection demeure la mise à jour du système : véritable action de prévention ;
- la seconde protection consiste à disposer d'un garde barrière permettant de filtrer les activités réseau ;
- la troisième protection est l'analyse des journaux : observation d'un comportement anormal ;
- la quatrième protection est l'antivirus : action de réaction. Il est intéressant de remarquer que si les antivirus réagissent relativement rapidement pour la mise à jour de leurs bases de signature, ils n'interviennent (pour « dasher ») dans le processus de défense que deux mois après la disponibilité du correctif.

Si vous constataz une activité de ce type sur une machine de votre parc informatique, veuillez en avvertir le CERTA.

5 Liens utiles

- Note d'information pour sur les systèmes obsolètes ;
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html>
- Note d'information pour limiter l'impact du SPAM ;
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/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>

6 Rappel des avis et mises à jour émis

Durant la période du 09 au 15 décembre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-485 : Vulnérabilité sur AIX
- CERTA-2005-AVI-486 : Vulnérabilité de Perl
- CERTA-2005-AVI-487 : Vulnérabilité de Ethereal
- CERTA-2005-AVI-488 : Vulnérabilité du noyau Microsoft Windows
- CERTA-2005-AVI-489 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2005-AVI-490 : Vulnérabilité sur le module mod_ldap d'Apache

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

- CERTA-2005-AVI-407-003 : Vulnérabilité dans la bibliothèque libcurl
(ajout des références aux bulletins de sécurité Debian DSA-919 et RedHat RHSA-2005:812.)
- CERTA-2005-AVI-482-001 : Vulnérabilité de cURL/libcurl
(ajout des références aux bulletins de sécurité Debian, Mandriva et FreeBSD et ajout de la référence CVE)
- CERTA-2005-AVI-484-001 : Vulnérabilité dans phpMyAdmin
(ajout de la référence au bulletin de sécurité Hardened-PHP, ajout des références aux bulletins de sécurité phpMyAdmin PMASA-2005-8 et PMASA-2005-9, ajout des références aux bulletins de sécurité Gentoo GLSA 200512-03 et FreeBSD et ajout des références CVE CAN-2005-3665 et CAN-2005-4079)
- CERTA-2005-AVI-486-001 : Vulnérabilité de Perl
(ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:225)
- CERTA-2005-AVI-489-001 : Multiples vulnérabilités dans Internet Explorer
(ajout de la référence au bulletin d'alerte CERTA-2005-ALE-017 mis à jour le 14 décembre 2005)
- CERTA-2005-AVI-428-002 : Multiples vulnérabilités dans PHP
(ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2005-AVI-487-001 : Vulnérabilité de Ethereal
(ajout des références aux bulletins de sécurité Mandriva et Gentoo)

7 Actions suggérées

7.1 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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme 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 réglementaire, 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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>

8 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	–	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 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398
143	TCP	IMAP	-	CERTA-2005-AVI-185
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 CERTA-2005-AVI-302
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	-
6070	TCP	BrightStor ARCserve/Enterprise Backup	-	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	-	CERTA-2005-AVI-024
6112	TCP	Dtspcd	-	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	-	CERTA-2003-AVI-214 CERTA-2005-AVI-326
8866	TCP	-	Porte dérobée Bagle.B	-

9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

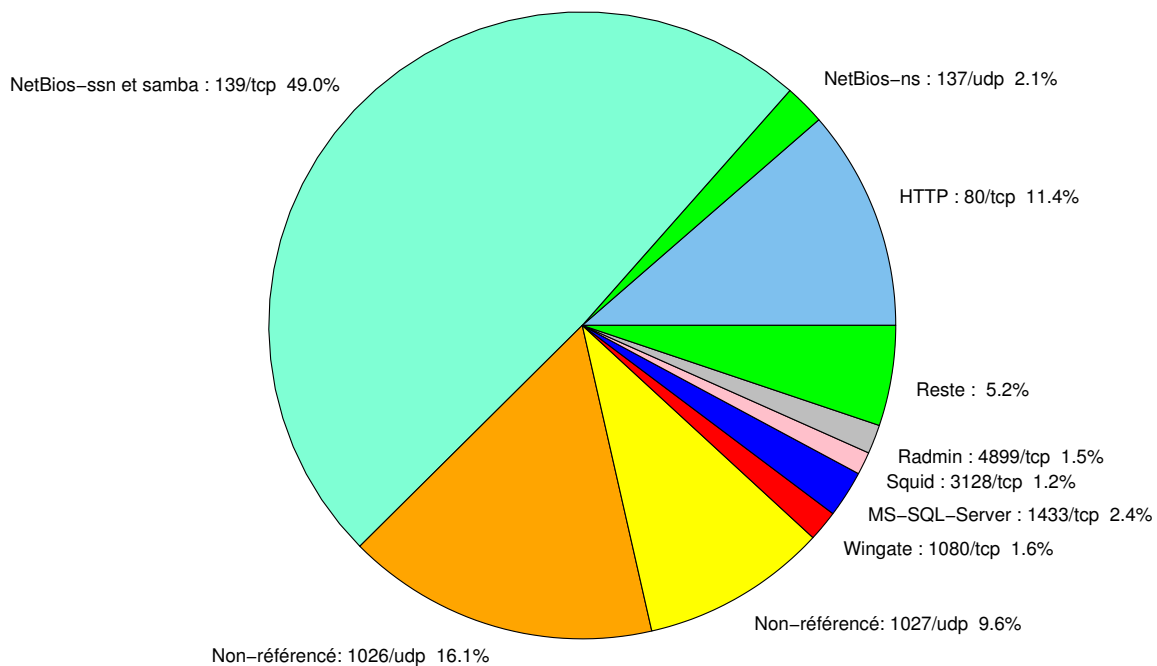


FIG. 1: Répartition relative des ports pour la semaine du 08.12.2005 au 15.12.2005

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	6
3	Paquets rejetés	8

Gestion détaillée du document

16 décembre 2005 version initiale.

port	pourcentage
139/tcp	48.96
1026/udp	16.11
80/tcp	11.38
1027/udp	9.59
1433/tcp	2.41
137/udp	2.08
1080/tcp	1.58
4899/tcp	1.49
3128/tcp	1.17
10000/tcp	0.83
1434/udp	0.81
5000/tcp	0.42
443/tcp	0.41
23/tcp	0.4
22/tcp	0.39
15118/tcp	0.33
3127/tcp	0.31
10080/tcp	0.2
5554/tcp	0.14
6129/tcp	0.13
3306/tcp	0.12
9898/tcp	0.09
111/tcp	0.05
3389/tcp	0.04
11768/tcp	0.03
2745/tcp	0.02

TAB. 3: Paquets rejetés