



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 novembre 2005
N° CERTA-2005-ACT-044

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-44

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-044>

Gestion du document

Référence	CERTA-2005-ACT-044
Titre	Bulletin d'actualité n° 2005-44
Date de la première version	04 novembre 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 27 octobre et le 03 novembre 2005.

1.2 Incidents traités

1.2.1 Défiguration d'un site web

Un cas de défiguration de site web a été traité par le CERTA. Les auteurs de cette défiguration ont profité d'un problème de configuration sur la machine (droits en écriture) pour ajouter une page web.

1.2.2 Compromission d'un serveur web

Un cas de compromission d'un serveur web est en cours de traitement. La faille exploitée affecte le forum phpBB. Les intrus ont ensuite installé une page imitant un site de commerce en ligne (« phishing »).

Il est à noter que ces forums vulnérables sont faciles à trouver en utilisant des techniques de « Google Hacking ».

Recommandation :

Il est conseillé pour les administrateurs d'utiliser ces techniques de « Google Hacking » pour rechercher d'éventuelles vulnérabilités sur les serveurs web de leur réseau.

1.2.3 Infection virale

Un de nos correspondants nous a signalé l'infection virale d'une de ses machines pourtant équipée d'un antivirus à jour. L'infection a été détectée suite au comportement anormal de la machine : perte des icônes et de la barre des tâches et ressources système complètement saturées. Les administrateurs de la machine ont découvert l'origine de l'infection, et ont testé le fichier infecté avec 6 antivirus. Seuls deux d'entre eux ont détecté un virus. Le fichier a ensuite été transmis à un éditeur d'antivirus qu'il soit intégré à la base de signatures.

Recommandation :

Cet incident est l'illustration que la lutte antivirale ne peut pas reposer uniquement sur l'antivirus. Une bonne remontée des informations de la part des utilisateurs vers les administrateurs est essentielle pour le traitement de ce type d'incidents.

1.2.4 Compromission d'un blog

Le CERTA a été informé de la compromission d'un « blog » (journal en ligne) par l'exploitation d'une vulnérabilité de `sphpblog-0.4.0`. Celle-ci permet de récupérer le mot de passe (sous forme chiffrée) d'administration du blog. Ce mot de passe était trivial, et a probablement été « cassé » à l'aide d'outils spécifiques. L'utilisation de ce mot de passe d'administration du blog a permis d'ajouter de nouvelles pages, notamment une page de « phishing ».

2 Rappel des avis et mises à jour émis

Durant la période du 24 au 28 octobre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-422 : Vulnérabilité dans phpMyAdmin
- CERTA-2005-AVI-423 : Vulnérabilités Skype
- CERTA-2005-AVI-424 : Vulnérabilité dans Oracle pour HP Openview

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

- CERTA-2005-AVI-394-001 : Vulnérabilité dans Microsoft DirectX (ajout de références aux bulletins de sécurité Microsoft)
- CERTA-2005-AVI-403-001 : Multiples vulnérabilités dans Microsoft Windows (ajout du bulletin de sécurité #909444 Microsoft)

3 Actions suggérées

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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>

4 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.

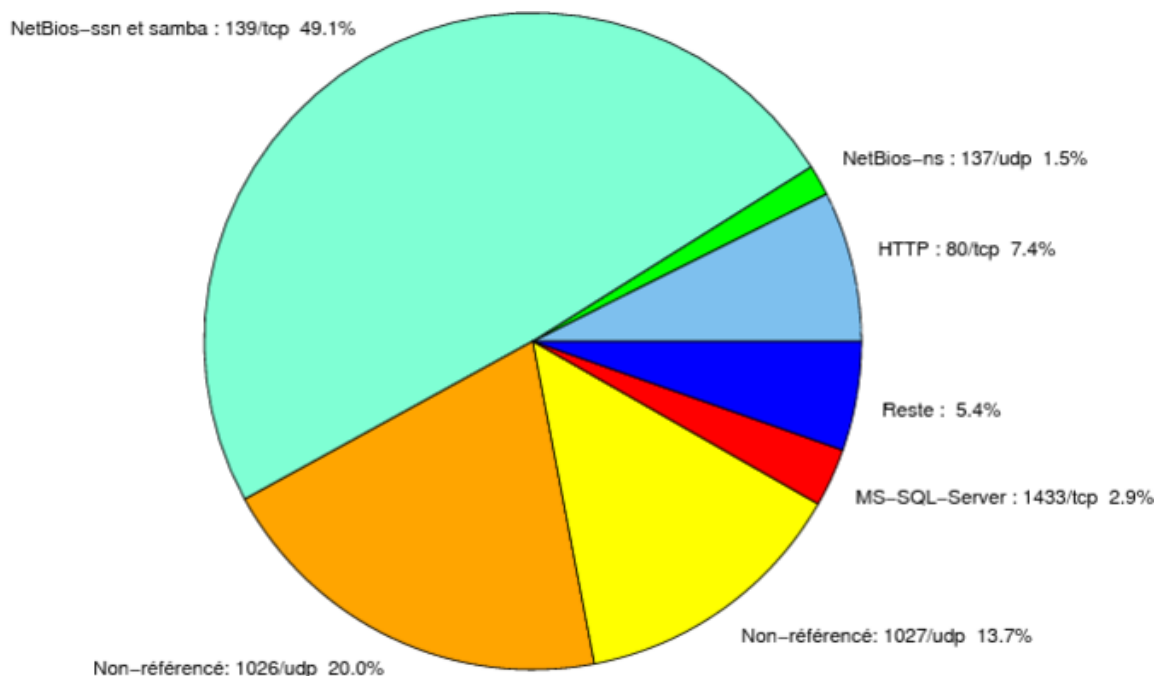


FIG. 1: Répartition relative des ports pour la semaine du 27.10.2005 au 03.11.2005

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-01 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-02 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-03
22	TCP	SSH	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-04
23	TCP	Telnet	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-05 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-06
25	TCP	SMTP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-07
42	TCP	WINS	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-08
80	TCP	HTTP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-09 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-10
111	TCP	Sunrpc-portmapper	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-11
119	TCP	NNTP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-12
135	TCP	Microsoft RPC	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-13 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-14 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-15
137	UDP	NetBios-ns	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-16
139	TCP	NetBios-ssn et samba	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-17 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-18 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-19 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-20 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-21 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-22
143	TCP	IMAP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-23
389	TCP	LDAP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-24 http://www.certa.ssi.gouv.fr/site/CERTA-2005-011-25

				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 re-jetés

port	pourcentage
139/tcp	49,08
1026/udp	20,01
1027/udp	13,74
80/tcp	7,39
1433/tcp	2,86
137/udp	1,51
1434/udp	0,94
1080/tcp	0,73
4899/tcp	0,71
10000/tcp	0,65
3128/tcp	0,6
23/tcp	0,3
15118/tcp	0,23
22/tcp	0,17
9898/tcp	0,15
6129/tcp	0,11
5554/tcp	0,07
2100/tcp	0,06
42/tcp	0,05
11768/tcp	0,02
6112/tcp	0,01

TAB. 3: Paquets rejetés

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

04 novembre 2005 version initiale.