Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juillet 2005
N° CERTA-2005-ACT-030

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-30

Gestion du document

Référence	CERTA-2005-ACT-030
Titre	Bulletin d'actualité n° 2005-30
Date de la première version	29 juillet 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 14 et le 21 juillet 2005.

1.2 Incidents traités

Le CERTA a traité trois cas de défiguration de site web. Pour ces cas, la faille suspectée d'avoir été exploitée est de type `php include`, dans l'application `PostNuke`. Ce type d'attaque est expliqué dans la note d'information CERTA-2004-INF-001 intitulée « Sécurité des applications Web et vulnérabilité de type injection de données » :
http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/index.html

1.3 Prolifération des `rootkits` sous Windows

Le CERTA a été informé récemment de la découverte de `rootkits` (ensemble d'outils dont le but est de camoufler l'activité d'un pirate) sur des machines compromises sous Windows. Les `rootkits`, très souvent utilisés lors des piratages de machines linux, compliquent considérablement la détection des machines compromises. Les machines sur lesquelles ces outils ont été trouvés étaient utilisées comme serveur `ftp warez` (échange de fichiers piratés).

1.3.1 Recommandation :

Il est conseillé d'utiliser des outils de métrologie pour surveiller l'activité du réseau. Ces outils permettent de détecter les machines qui sont à l'origine (ou destinataire) d'un trafic important, ce qui peut être symptomatique de la présence d'un serveur `ftp warez`.

1.4 Recrudescence de l'activité `MyTob`

Un des abonnés du CERTA a signalé une recrudescence de l'activité du ver `MyTob`. Ce ver se propage principalement par la messagerie.

1.4.1 Recommandation :

Il est conseillé de lire l'avis CERTA-2003-AVI-084 intitulé « Rappel sur les virus de messagerie » et disponible à l'adresse :
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-084/index.html

2 Rappel des avis et mises à jour émis

Durant la période du 18 juillet au 22 juillet 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-268 : Vulnérabilité de Shorewall
- CERTA-2005-AVI-269 : Vulnérabilité de Sybase EAServer
- CERTA-2005-AVI-270 : Multiples vulnérabilités de PowerDNS
- CERTA-2005-AVI-271 : Vulnérabilité dans Sun Management Center
- CERTA-2005-AVI-272 : Vulnérabilité de Kate / Kwrite
- CERTA-2005-AVI-273 : Vulnérabilité dans Novell Groupwise
- CERTA-2005-AVI-274 : Vulnérabilité dans SSH Tectia Server et Secure shell pour Windows
- CERTA-2005-AVI-275 : Vulnérabilité dans Airport d'Apple
- CERTA-2005-AVI-276 : Vulnérabilité sur la bibliothèque zlib
- CERTA-2005-AVI-277 : Vulnérabilité dans Avast Antivirus
- CERTA-2005-AVI-278 : Vulnérabilité dans Fetchmail

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

- CERTA-2005-AVI-239-002 : Multiples vulnérabilité dans heimdal telnetd server
  (ajout de la référence au bulletin de sécurité Debian DSA-758)
- CERTA-2005-AVI-242-008 : Vulnérabilités dans PHP PEAR
  (ajout de la référence au bulletin de sécurité Gentoo GLSA 200507-15)
- CERTA-2005-AVI-250-003 : Vulnérabilité de dhcpcd
  (ajout de la référence au bulletin de sécurité Gentoo 200507-16, correction du produit en dhcpcd)
- CERTA-2005-AVI-256-003 : Multiples vulnérabilité dans les produits Mozilla
  (ajout des références CVE et de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-257-003 : Vulnérabilité de MIT Kerberos 5
  (ajout de la référence au bulletin de sécurité Debian DSA-757)
- CERTA-2005-AVI-242-009 : Vulnérabilités dans PHP PEAR
  (ajout de la référence au bulletin de sécurité SGI 20050703-01-U)
- CERTA-2005-AVI-256-004 : Multiples vulnérabilité dans les produits Mozilla
  (ajout de Mozilla Thunderbird dans la liste des systèmes affectés ainsi que de la remarque dans la description)
- CERTA-2005-AVI-257-004 : Vulnérabilité de MIT Kerberos 5
  (ajout des références aux bulletins de sécurité RedHat RHSA-2005:562 et SGI 20050703-01-U)
- CERTA-2005-AVI-245-002 : Vulnérabilités dans OpenLDAP, nss_ldap et pam_ldap
  (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:121)
- CERTA-2005-AVI-251-001 : Vulnérabilité de cpio
  (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:116-1)

- CERTA-2005-AVI-227-001 : Multiples vulnérabilités de Cacti
  (ajout de la référence au bulletin de sécurité Debian DSA-764)
- CERTA-2005-AVI-243-003 : Multiples vulnérabilités de Cacti
  (ajout de la référence au bulletin de sécurité Debian DSA-764)
- CERTA-2005-AVI-268-001 : Vulnérabilité de Shorewall
  (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:123 et ajout de la référence CVE CAN-2005-2317)
- CERTA-2005-AVI-272-001 : Vulnérabilité de Kate / Kwrite
  (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:122)
- CERTA-2005-AVI-183-005 : Vulnérabilités dans gzip
  (ajout de la référence au bulletin de sécurité Sun #101816)
- CERTA-2005-AVI-251-002 : Vulnérabilité de cpio
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:378)
- CERTA-2005-AVI-268-002 : Vulnérabilité de Shorewall
  (ajout de la référence au bulletin de sécurité Gentoo GLSA 200507-20)
- CERTA-2005-AVI-270-001 : Multiples vulnérabilités de PowerDNS
  (ajout de la référence au bulletin de sécurité FreeBSD, de la référence CVE CAN-2005-2302)
- CERTA-2005-AVI-256-005 : Multiples vulnérabilité dans les produits Mozilla
  (ajout des références aux bulletins de sécurité RedHat RHSA-2005:586, RHSA-2005:587 et RHSA-2005:601)
- CERTA-2005-AVI-124-005 : Multiples vulnérabilités dans le client Telnet
  (ajout de la référence au bulletin de sécurité Debian DSA-765)

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'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.

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 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.

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 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.

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 chose s, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participen t à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utili sateurs, 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.

Liste des tableaux

Gestion détaillée du document

29 juillet 2005 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2005-A http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
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-A
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-A
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-A
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-A
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-A
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

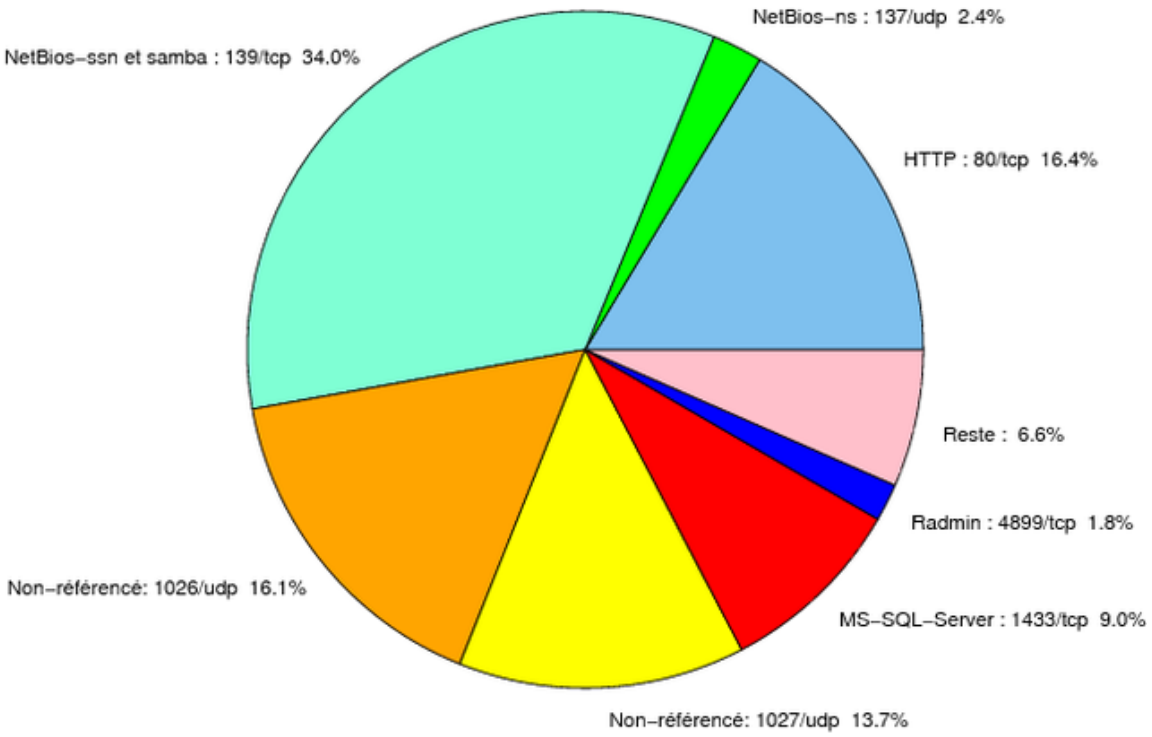

FIG. 1: Répartition relative des ports pour la semaine du 14.07.2005 au 21.07.2005

port	pourcentage
139/tcp	41,15
1433/tcp	13,41
1026/udp	12,21
1027/udp	10,56
80/tcp	7,19
137/udp	3,37
445/tcp	3,25
4899/tcp	2,85
2745/tcp	0,97
1434/udp	0,86
15118/tcp	0,80
1080/tcp	0,68
6129/tcp	0,63
3127/tcp	0,46
10000/tcp	0,40
22/tcp	0,40
9898/tcp	0,23
5554/tcp	0,17
42/tcp	0,17
6101/tcp	0,17
3306/tcp	0,06

TAB. 3: Paquets rejetés