Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 juillet 2005
N° CERTA-2005-ACT-026

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-26

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-026`

Gestion du document

Référence	CERTA-2005-ACT-026
Titre	Bulletin d'actualité n° 2005-26
Date de la première version	01 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 16 et le 23 juin 2005.

Nous avons ajouté le port 10000/tcp à notre surveillance, suite à la publication d'un outil exploitant automatiquement une des vulnérabilités de `Veritas Backup Exec` décrites dans l'avis CERTA-2005-AVI-229. Il est urgent de mettre à jour cet applicatif.

1.2 Activité port 139/tcp et 80/tcp

Le CERTA constate encore une forte activité sur le port 139/tcp, accompagnée d'un trafic un peu plus faible sur le port 80/tcp. Un ver, nommé `Tdiserv` par un éditeur d'antivirus, a récemment été découvert. Ce ver aurait la particularité de se propager par les partages réseau. Il installerait un `rootkit` (ensemble d'outils dont le but est de camoufler un piratage), ce qui rendrait sa détection difficile. En revanche, les machines infectées ont un comportement caractéristique : elles tentent de nombreuses connexions vers différentes destinations sur leurs ports 139/tcp et 80/tcp.

Recommandation

Il est conseillé de vérifier qu'aucune machine de votre réseau ne se comporte tel que décrit ci-dessus. Si vous constatiez un tel trafic, contactez le CERTA.

2 Publication de nombreux outils d'attaque

De nombreux outils d'attaque concernant des vulnérabilités ont récemment été mis à disposition sur l'Internet. Ceux-ci concernent les failles suivantes :

- `phpBB` versions 2.0.15 et antérieures (voir CERTA-2005-AVI-237). La faille est très proche celle qui avait été décrite dans l'alerte CERTA-2004-ALE-014. Cet outil est déjà utilisé.
- Prise en compte de NNTP par Microsoft Outlook Express (voir CERTA-2005-AVI-210). L'exploitation repose sur l'envoi d'un message contenant un lien cliquable avec le protocole `news://`.
- Application `Message Queuing` (voir CERTA-2005-AVI-137).

Recommandation

Il est urgent d'appliquer les correctifs indiqués dans les avis cités ci-dessus.

3 Exploitation de la faille `autologin` de `phpBB`

Une des failles régulièrement exploitées de `phpBB` est celle affectant `autologin` dans le fichier `sessions.php` (voir avis CERTA-2005-AVI-096). La particularité de cette faille est que son exploitation ne laisse pas des traces flagrantes dans les journaux.

Voici un exemple de trace laissée par une tentative d'exploitation de cette faille :

```
adresse_IP_attaquant - - [30/June/2005:15:32:17 +0200] "GET /forum/admin/admin_board.php
HTTP/1.1" 200 16796 - "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Le succès de la compromission se traduira par une ligne du type :

```
adresse_IP_attaquant - - [30/June/2005:15:32:26 +0200] "POST /forum/admin/admin_board.php
HTTP/1.1" 200 1700 - "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Recommandation

Il est conseillé d'examiner régulièrement les journaux, et de signaler les tentatives d'exploitation de cette faille (réussies ou non) au CERTA.

4 Rappel des avis et mises à jour émis

Durant la période du 20 au 24 juin 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-226 : Vulnérabilité dans l'utilitaire sudo
- CERTA-2005-AVI-227 : Multiples vulnérabilités de Cacti
- CERTA-2005-AVI-228 : Vulnérabilité des produits webmail de SUN
- CERTA-2005-AVI-229 : Multiples vulnérabilités de Veritas Backup Exec
- CERTA-2005-AVI-230 : Multiples vulnérabilités des lecteurs RealPlayer

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

- CERTA-2005-AVI-202-003 : Multiples vulnérabilités de Gaim
  (ajout des références aux bulletins de sécurité FreeBSD)
- CERTA-2005-AVI-209-001 : Vulnérabilités des versions Sun de Java 2 Standard Edition
  (ajout des références aux bulletins de sécurité de Blackdown Java-Linux et Gentoo)
- CERTA-2005-AVI-220-001 : Vulnérabilité dans des produits Adobe
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-224-001 : Vulnérabilité de SquirrelMail
  (ajout de la référence au bulletin de sécurité FreeBSD)

- CERTA-2005-AVI-225-001 : Vulnérabilité dans SpamAssassin
  (modification de la référence CVE et ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-069-003 : Vulnérabilité de cpio
  (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2005-AVI-225-002 : Vulnérabilité dans SpamAssassin
  (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2005-AVI-223-001 : Vulnérabilité de Opera
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-224-002 : Vulnérabilité de SquirrelMail
  (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2005-AVI-085-003 : Vulnérabilité de unace
  (ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2005-AVI-209-002 : Vulnérabilités des versions Sun de Java 2 Standard Edition
  (ajout de la référence au bulletin de sécurité de SUSE et ajout de la référence CVE CAN-2005-1974)
- CERTA-2005-AVI-223-002 : Vulnérabilité de Opera
  (ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2005-AVI-225-003 : Vulnérabilité dans SpamAssassin
  (ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2005-AVI-226-001 : Vulnérabilité dans l'utilitaire sudo
  (ajout référence CVE. Ajout bulletin de sécurité Mandriva. Ajout références mise-à-jour Fedora)
- CERTA-2005-AVI-226-002 : Vulnérabilité dans l'utilitaire sudo
  (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2004-AVI-319-005 : Multiples vulnérabilités dans gdk-pixbuf
  (ajout référence au bulletin de sécurité #101776 de Sun)
- CERTA-2005-AVI-170-003 : Vulnérabilité dans FreeRADIUS
  (ajout du bulletin Red Hat RHSA-2005:524)
- CERTA-2005-AVI-225-004 : Vulnérabilité dans SpamAssassin
  (ajout de la référence au bulletin de sécurité RHSA-2005-498 de Red Hat)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

6 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

01 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*

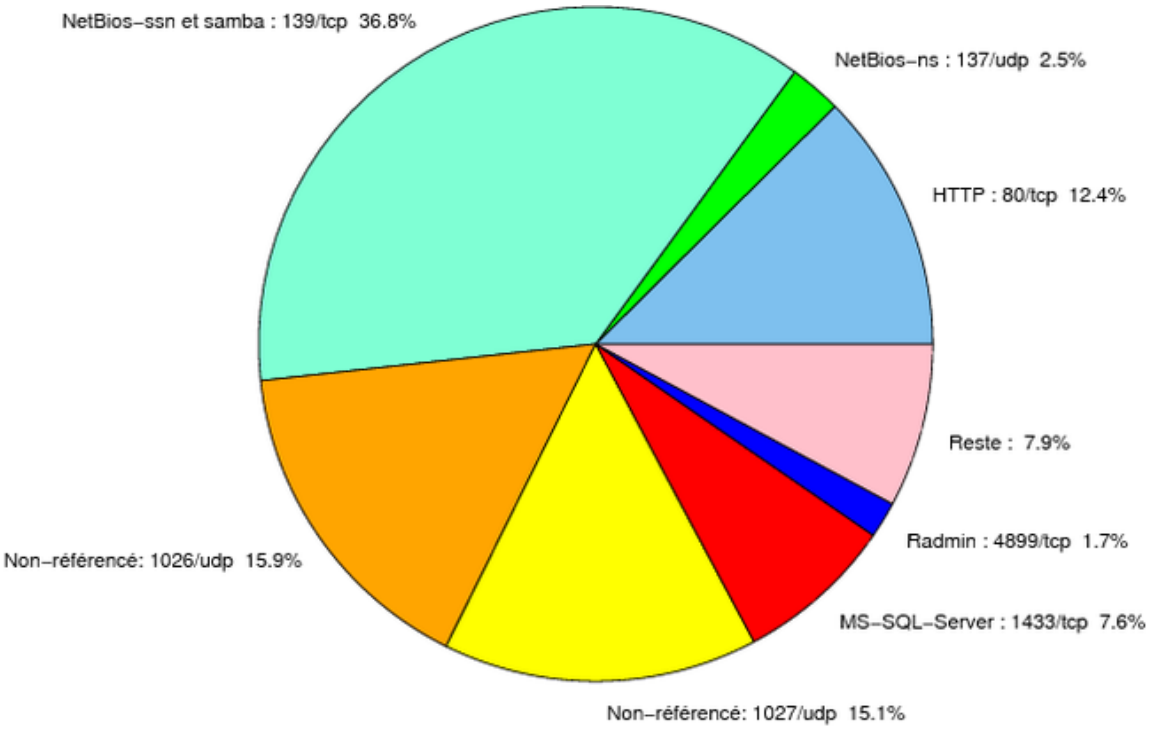

FIG. 1 – *Répartition relative des ports pour la semaine du 16.06.2005 au 23.06.2005*

port	pourcentage
139/tcp	35,16
1026/udp	19,14
1027/udp	15,26
80/tcp	11,27
1433/tcp	9,10
137/udp	3,15
4899/tcp	1,72
445/tcp	1,13
15118/tcp	0,78
1080/tcp	0,55
9898/tcp	0,55
1434/udp	0,55
5554/tcp	0,45
22/tcp	0,25
3306/tcp	0,25
23/tcp	0,18
111/tcp	0,13
143/tcp	0,10
25/tcp	0,08
2745/tcp	0,08
1023/tcp	0,03
6129/tcp	0,03
21/tcp	0,03
42/tcp	0,03

TAB. 3 – *Paquets rejetés*