Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 décembre 2004
N° CERTA-2004-ACT-028

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N28

Gestion du document

Référence	CERTA-2004-ACT-028
Titre	Bulletin d'actualité N28
Date de la première version	10 décembre 2004
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

Le tableau 3 montre les rejets sur deux dispositifs de filtrage entre le 25 novembre 2004 et le 02 décembre 2004. On ne constate aucune évolution majeure du trafic des paquets rejetés. Les failles actuellement exploitées reposent essentiellement sur des vulnérabilités dans des applicatifs, ce qui laisse peu de traces réseau.

2 Le filtrage en sortie

Le CERTA est intervenu récemment sur un incident relatif à la compromission d'un serveur WEB.

Une analyse des journaux du pare-feu placé en bordure de la DMZ a permis de mettre en évidence un trafic non sollicité tentant de sortir sur l'Internet, bloqué par le dispositif de filtrage, en provenance d'un serveur Web localisé dans la DMZ.

Ce filtrage en sortie de DMZ (vers l'Internet) a mis en évidence que le serveur était compromis et que les "visiteurs" s'employaient à récupérer sur des sites WEB de l'Internet des outils permettant le maintien frauduleux dans le système compromis.

Faute de pouvoir effectuer le téléchargement, les pirates ont vite délaissé leur proie...

Cet événement illustre que la mise en œuvre d'un filtrage en sortie au niveau du pare-feu, précaution trop souvent négligée, peut s'avérer utile dans certains cas :

– mise en évidence de la compromission d'un serveur (à condition de lire les journaux des pare-feux) ;

– limitation des effets de la compromission d'un serveur (maintien dans le système plus complexe, empêche les attaques par rebond...).

Toutefois, ce n'est pas une protection suffisante face à un intrus expérimenté (utilisation d'un flux autorisé en sortie).

Dans le cadre de sa mission de réponse aux incidents de sécurité informatique, le CERTA peut vous assister dans l'analyse des journaux et leur interprétation.

3 Rappel des avis et des mises à jour émis

Durant la période du 29 novembre au 03 décembre 2004, le CERTA a émis les avis suivants :

– CERTA-2004-AVI-381 : Vulnérabilité dans WS_FTP Server
– CERTA-2004-AVI-382 : Vulnérabilité de Solaris
– CERTA-2004-AVI-383 : Vulnérabilité dans Internet Explorer 6
– CERTA-2004-AVI-384 : Vulnérabilité du service WINS de Microsoft
– CERTA-2004-AVI-385 : Vulnérabilité dans OpenSSL
– CERTA-2004-AVI-386 : Multiples vulnérabilités dans Mac OS X

Pendant cette même période, le CERTA a publié les mises à jour suivantes :

– CERTA-2004-AVI-373-001 : Vulnérabilité de unarj
(ajout de la référence au bulletin de sécurité FreeBSD)
– CERTA-2004-AVI-360-003 : Vulnérabilité de la bibliothèque gd
(ajout de la référence au bulletin de sécurité de Debian)
– CERTA-2004-AVI-360-004 : Vulnérabilité de la bibliothèque gd
(ajout de la référence au bulletin de sécurité de Debian DSA-602)
– CERTA-2004-AVI-377-003 : Vulnérabilité dans la machine virtuelle Java de SUN
(ajout de la référence au bulletin de sécurité Gentoo)

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.

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. Unpare-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.

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 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.

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.

Liste des tableaux

Gestion détaillée du document

26 novembre 2004 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-20 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-17 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-19 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-21 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-23 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-05
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-00 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-11 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-03
139	TCP	NetBios-ssn	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-16 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-14 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-00 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-09 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-17 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-24 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-30 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-03 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
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-ALE-00
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-15
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-18 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-21
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-16
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-00
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-21
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–

TAB. 2 – *Correctifs correspondant aux ports destination des paquets rejetés*

port	pourcentage
135/tcp	28,85
445/tcp	28,68
139/tcp	8,09
137/udp	5,22
80/tcp	2,78
1433/tcp	2,72
1026/udp	2,57
9898/tcp	2,45
5554/tcp	2,43
1023/tcp	2,33
2745/tcp	2,26
1434/udp	1,96
1027/udp	1,91
4899/tcp	1,32
3127/tcp	1,32
22/tcp	1,01
6129/tcp	0,92
1080/tcp	0,89
21/tcp	0,79
443/tcp	0,48
111/tcp	0,36
23/tcp	0,24
3389/tcp	0,17
3128/tcp	0,09
5000/tcp	0,08
6112/tcp	0,03
389/tcp	0,02
119/tcp	0,02

TAB. 3 – *Paquets rejetés*