Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 juillet 2004
N° CERTA-2004-ACT-009

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N9

Gestion du document

Référence	CERTA-2004-ACT-009
Titre	Bulletin d'actualité N9
Date de la première version	16 juillet 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 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.

2 Activité en cours

Durant la semaine du 1er au 8 juillet 2004, une machine compromise a pu être repérée suite à un rejet sur le port 22/tcp. Ce rejet correspondait à une tentative de connexion unique en SSH sur un serveur DNS. Ce type d'activité peut sembler anodin (un seul paquet rejeté), toutefois il est généralement caractéristique d'une machine compromise.

port	pourcentage
$135/tcp$	35,41
$445/tcp$	22,56
$137/udp$	10,58
$139/tcp$	8,13
$2745/tcp$	5,89
$80/tcp$	4,12
$1434/udp$	2,65
$1433/tcp$	2,13
$3127/tcp$	1,55
$5554/tcp$	1,32
$9898/tcp$	1,19
$4899/tcp$	1,18
$6129/tcp$	0,95
$443/tcp$	0,70
$21/tcp$	0,46
$1080/tcp$	0,33
$3128/tcp$	0,24
$111/tcp$	0,16
$3389/tcp$	0,16
$23/tcp$	0,12
$5000/tcp$	0,09
$22/tcp$	0,05

TAB. 2 – *Paquets rejetés*

3 Retour d'expérience sur incident

Le CERTA a récemment eu l'occasion d'analyser une machine qui avait été compromise quelques semaines auparavant. La compromission de cette machine avait été détectée par l'administrateur. Celui-ci avait trouvé un `rootkit` (ensemble d'outils ayant pour but de camoufler l'activité d'un intrus) sous la forme de binaires du système modifiés. Il avait placé ce `rootkit`, ainsi qu'un certain nombre d'outils installés lors de l'intrusion, dans une zone de quarantaine. La réaction de l'administrateur de la machine n'a pas été la meilleure possible. En effet, malgré les mesures prises par l'administrateur, l'intrus est parvenu à se maintenir sur le système compromis, depuis lequel il a pu se livrer à des activités délictueuses.

Il est important de rappeler qu'aucune confiance ne peut être accordée à un système compromis. Une réinstallation complète de la machine est recommandée, après avoir réalisé une copie physique du disque dur. La préservation des traces liées à la compromission est essentielle en cas de dépôt de plainte ou pour une analyse ultérieure. Il n'est généralement pas possible de savoir qu'elle a été l'activité de l'intrus sur la machine compromise, notamment si la machine a servi pour attaquer d'autres machines (attaques par rebond). Les réinstallations depuis des sauvegardes sont déconseillées, car il n'est pas garanti que le système était sain au moment de la sauvegarde. Il est aussi fortement recommandé de changer tous les mots de passe du système et du réseau. En effet, des `sniffers` (outils d'interception du trafic réseau) sont souvent installés par des intrus. Ces outils permettent de voler les mots de passe transitant dans le sous-réseau. Enfin, la compromission ne se limite pas forcément à un système du réseau. D'autres machines peuvent avoir été touchées (notamment celle ayant la même configuration, ou bien suite à un vol de mot de passe).

En cas d'intrusion, il est conseillé de lire la note d'information CERTA-2002-INF-002 (voir Documentation) avant d'entreprendre la moindre action.

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

La table 3 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. 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.

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 Rappel des avis et des mises à jour émis

Pendant la semaine du 05 au 09 juillet 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-220 : Vulnérabilité dans la gestion d'appels système sous FreeBSD
- CERTA-2004-AVI-221 : Vulnérabilité de GNATS
- CERTA-2004-AVI-222 : Vulnérabilité dans le JUNOS de Juniper
- CERTA-2004-AVI-223 : Vulnérabilité de MySQL
- CERTA-2004-AVI-224 : Vulnérabilité de netfilter dans les noyaux Linux 2.6
- CERTA-2004-AVI-225 : Multiples vulnérabilités du noyau Linux
- CERTA-2004-AVI-226 : Vulnérabilité de WinGate
- CERTA-2004-AVI-227 : Vulnérabilité dans les pare-feux NetScreen 5GT
- CERTA-2004-AVI-228 : Vulnérabilités dans Ethereal
- CERTA-2004-AVI-229 : Vulnérabilité de nCipher netHSM
- CERTA-2004-AVI-230 : Vulnérabilité dans le module de sécurité BSM sur Solaris
- CERTA-2004-AVI-231 : Vulnérabilité de plusieurs navigateurs
- CERTA-2004-AVI-232 : Vulnérabilité de la suite Mozilla sous Windows XP
- CERTA-2004-AVI-233 : Vulnérabilité dans Shorewall
- CERTA-2004-AVI-234 : Faille dans le serveur SSLtelnet

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-066 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-064 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-132
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-152
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-209 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-179 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-131
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-050 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-195 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-210 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-239
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-052
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-111 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-031
139	TCP	NetBios-ssn	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-168 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-144 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-045 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-102 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-068 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-041 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-004 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-156 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-095 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-178
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-053 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-105 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-038 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
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-157
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-062 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-186
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-165
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-214
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–

TAB. 3 – *Correctifs correspondant aux ports destination des paquets rejetés*

Les mises à jour suivantes ont été publiées :

- CERTA-2004-AVI-189-001 : Vulnérabilité de Mailman (ajout de la référence au bulletin de sécurité OpenBSD)
- CERTA-2004-AVI-202-001 : Vulnérabilité de Webmin et Usermin (ajout des références à Usermin. Ajout des bulletins de sécurité SNS, Debian et des références CVE)
- CERTA-2004-AVI-205-001 : Vulnérabilité de Pure-FTPd (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2004-AVI-210-002 : Vulnérabilité du serveur HTTP Apache (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2004-AVI-216-002 : Vulnérabilité de pavuk (ajout des références aux bulletins de sécurité Debian et FreeBSD)
- CERTA-2004-AVI-217-001 : Vulnérabilités dans MPlayer (ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2004-AVI-211-001 : Vulnérabilité dans XFree86 (ajout de la référence au bulletin de sécurité Gentoo, de la référence CVE et du site Internet de XFree86)
- CERTA-2004-AVI-178-005 : Vulnérabilité du module Apache mod_ssl (ajout d'une seconde référence au bulletin de sécurité RedHat)
- CERTA-2004-AVI-195-004 : Vulnérabilité du module mod_proxy du serveur HTTP Apache (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2004-AVI-210-003 : Vulnérabilité du serveur HTTP Apache (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2004-AVI-182-004 : Vulnérabilité de Tripwire (ajout de la référence au second bulletin de sécurité de Mandrake)
- CERTA-2004-AVI-212-001 : Vulnérabilité dans la bibliothèque libpng (ajout de la référence au bulletin de sécurité OpenBSD)
- CERTA-2004-AVI-131-002 : Vulnérabilité du noyau linux (ajout références au bulletin de sécurité Gentoo GLSA-200407-02)
- CERTA-2004-AVI-225-001 : Multiples vulnérabilités du noyau Linux (première révision : prise en compte des vulnérabilités CVE CAN-2004-0565 et CVE CAN-2004-0587 et ajout référence au bulletin de sécurité Mandrake MDKSA-2004:066)
- CERTA-2004-AVI-228-001 : Vulnérabilités dans Ethereal (ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2004-AVI-212-002 : Vulnérabilité dans la bibliothèque libpng (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2004-ALE-009-002 : Vulnérabilités d'Internet Explorer (deuxième révision : modification des versions affectées et prise en compte de l'exploitation des vulnérabilités)

6 Documentation

- Note d'information CERTA-2002-INF-002 : Les bons réflexes en cas d'intrusion sur un système d'information
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002

Liste des tableaux

Gestion détaillée du document

16 juillet 2004 version initiale.