

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N° 10

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-2004-ACT-010>

Gestion du document

Référence	CERTA-2004-ACT-010
Titre	Bulletin d'actualité N° 10
Date de la première version	15 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

Outre le bruit permanent engendré par les rejets sur les quatre ports correspondant à des services caractéristiques de Windows, à savoir les ports 135/tcp, 445/tcp, 139/tcp et 137/udp, on distingue dans le tableau un nombre de rejet important sur le port 5554/tcp. Ces rejets correspondent à la recherche de machines infectées par le ver Sasser qui installe un serveur ftp servant à la propagation du ver.

port	pourcentage
135/tcp	26,84
445/tcp	25,72
139/tcp	12,67
137/udp	10,83
5554/tcp	5,71
80/tcp	3,40
2745/tcp	3,13
1433/tcp	1,94
1434/udp	1,87
9898/tcp	1,56
3127/tcp	1,55
4899/tcp	1,11
1023/tcp	1,08
6129/tcp	0,86
21/tcp	0,67
443/tcp	0,28
1080/tcp	0,19
3128/tcp	0,13
111/tcp	0,13
5000/tcp	0,12
22/tcp	0,06
23/tcp	0,05
3389/tcp	0,04
6112/tcp	0,04
10080/tcp	0,01

TAB. 2 – Paquets rejetés

3 Retour d'expérience sur les incidents

Les récentes expertises effectuées sur quelques machines compromises ont montré une augmentation de l'installation de BHOs (Browser Helper Object).

3.1 Qu'est ce qu'un BHO ?

Comme son nom l'indique, un BHO est un objet chargé d'apporter des fonctionnalités supplémentaires au navigateur (exemple d'ajout de fonctionnalités : amélioration de la barre de contrôle). Cette possibilité introduit par Microsoft est disponible sur les navigateurs basés sur Internet Explorer. Dans la plupart des cas, un BHO est installé sous forme de bibliothèque partagée exécutée au démarrage d'Internet Explorer.

3.2 Pourquoi craindre une fonctionnalité ?

Dans certains cas, le BHO est installé par un ActiveX présent sur un site Internet ou dans un email. Ce type d'installation est par défaut transparente pour l'utilisateur. Le fait de ne pas contrôler l'installation d'une fonctionnalité est un premier problème de sécurité. De plus, un retour sur expérience montre qu'un grand nombre de BHO que l'on retrouve sur les machines des utilisateurs sont souvent des programmes utilisées à des fins malveillantes. En effet, ces BHOs font partie de deux grandes familles d'outils malveillants :

- les BHOs publicitaires chargeant automatiquement certaines pages non sollicitées contenant de la publicité.
- les BHOs espionciels (spywares) chargés d'enregistrer les actions effectuées par l'utilisateur pour ensuite les transmettre dans une base centralisée (exemple : outil chargé d'enregistrer tout les informations fournies dans les pages HTTPS dans un navigateur, utilisé pour le vol d'identifiant et mot de passe sur un site bancaire).

3.3 Comment détecter et supprimer les BHOs sur ma machine?

Le moyen le plus efficace pour connaître les BHOs associés à son navigateur est d'afficher le contenu de la clef de registre

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\BrowserHelperObject
```

. Un autre moyen est d'utiliser un programme permettant de lister et désactiver ces BHOs, comme par exemple l'outil BHODemon (cf. section 3.5).

Remarques :

- Dans le service pack 2 de Windows XP une gestion des BHOs sera incluse en natif ;
- une autre possibilité pour ne pas avoir de BHO sur sa machine est d'utiliser un autre navigateur qu'Internet Explorer.

3.4 Rappel concernant la navigation sur Internet

De manière générale, la navigation sur l'Internet nécessite quelques précautions :

- ne pas exécuter systématiquement les scripts (ActiveX, Java, Javascript, ...);
- ne pas accepter systématiquement les *cookies* ;
- appliquer les correctifs de sécurité dès leur sortie pour le système, le navigateur et tous ses composants (JVM, plug-ins, ...);
- éviter une diffusion excessive d'informations personnelles.

3.5 Documentation

- Site pour le téléchargement de BHODemon :
<http://www.definitivesolutions.com/bhodemon.htm>
- BHO « The Browser the way you want it » par Microsoft :
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp>
- Article 179230 de Microsoft : IEHelper-Attaching to Internet Explorer 4.0 by using a Browser Helper Object
<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q179/2/30.asp&NoWebC>

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.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2004-AVI-066 CERTA-2004-AVI-064 CERTA-2003-AVI-132
22	TCP	SSH	–	CERTA-2003-AVI-152
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-179 CERTA-2003-AVI-131
80	TCP	HTTP	–	CERTA-2004-AVI-050 CERTA-2004-AVI-195 CERTA-2004-AVI-210 CERTA-2004-AVI-239
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn	–	CERTA-2003-AVI-168 CERTA-2003-AVI-144 CERTA-2004-AVI-126
389	TCP	LDAP	–	CERTA-2004-AVI-045 CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-095 CERTA-2004-AVI-126 CERTA-2004-AVI-178
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2003-AVI-038 CERTA-2004-AVI-126
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	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

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 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.

5 Rappel des avis et des mises à jour émis

Du 11 juillet 2004 au 17 juillet 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-235 : Vulnérabilité d'Adobe Acrobat et d'Adobe Reader
- CERTA-2004-AVI-236 : Vulnérabilité dans Microsoft Outlook Express
- CERTA-2004-AVI-237 : Vulnérabilité dans Utility Manager sous Windows
- CERTA-2004-AVI-238 : Vulnérabilité du composant POSIX de Microsoft
- CERTA-2004-AVI-239 : Vulnérabilité dans Microsoft Internet Information Server (IIS) 4.0
- CERTA-2004-AVI-240 : Vulnérabilité dans Microsoft Windows Task Scheduler
- CERTA-2004-AVI-241 : Vulnérabilités dans les fichiers d'aide HTML de Microsoft
- CERTA-2004-AVI-242 : Vulnérabilité dans l'interpréteur de commandes Windows
- CERTA-2004-AVI-243 : Vulnérabilité de la bibliothèque wv
- CERTA-2004-AVI-244 : Vulnérabilité de PHP
- CERTA-2004-AVI-245 : Vulnérabilité dans FreeS/Wan, Openswan, StrongSwan et Super FreeS/Wan
- CERTA-2004-AVI-246 : Vulnérabilité dans Novell BorderManager
- CERTA-2004-AVI-247 : Vulnérabilité du module Apache mod_ssl

Les mises à jour suivantes ont été publiées :

- CERTA-2004-AVI-166-004 : Multiples vulnérabilités dans Ethereal (ajout du site Internet d'Ethereal et de la référence au bulletin de sécurité FreeBSD).
- CERTA-2004-AVI-228-002 : Vulnérabilités dans Ethereal (ajout des références aux bulletins de sécurité Gentoo, Mandrake et FreeBSD et ajout des références CVE).
- CERTA-2004-AVI-153-005 : Vulnérabilité dans Rsync (ajout de la référence au bulletin de sécurité Gentoo).
- CERTA-2004-AVI-136-003 : Vulnérabilité de KAME Racocon (ajout de la référence au bulletin de sécurité Mandrake).
- CERTA-2004-AVI-224-001 : Vulnérabilité de netfilter dans les noyaux Linux 2.6 (ajout de la référence au bulletin de sécurité Gentoo).

- CERTA-2004-AVI-240-001 : Vulnérabilité dans Microsoft Windows Task Scheduler (correction des systèmes affectés et ajout du risque).
- CERTA-2004-AVI-244-001 : Vulnérabilité de PHP (ajout de la référence au bulletin de sécurité Gentoo).
- CERTA-2004-AVI-244-002 : Vulnérabilité de PHP (ajout de la référence au bulletin de sécurité SUSE).
- CERTA-2004-AVI-074-003 : Vulnérabilités de du serveur wu-ftpd (modification des références aux bulletins de sécurité Debian et HP. Modification de la référence CVE CAN-2004-0148. Ajout de la référence au bulletin de sécurité HP-UX).

6 Documentation

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	2
3	Correctifs correspondant aux ports destination des paquets rejetés	4

Gestion détaillée du document

15 juillet 2004 version initiale.