



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 octobre 2004
N° CERTA-2004-ACT-020

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°20

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-020>

Gestion du document

Référence	CERTA-2004-ACT-020
Titre	Bulletin d'actualité N°20
Date de la première version	01 octobre 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 16 septembre au 23 septembre 2004, l'activité a été marquée par le trafic à destination du port 445/tcp. Un ministère nous a fait part de ses observations pour ce port : à partir du 21 septembre 2004, les rejets des paquets à destination du port 445/tcp sont environ 6 fois plus importants que ceux constatés pour la semaine qui précédait. Nous constatons également sur nos propres équipements une augmentation de ce type d'activité à partir du 21 septembre, mais l'augmentation n'est pas aussi forte.

Un ministère a signalé de très nombreuses tentatives d'intrusion sur un de ses serveurs http, provenant d'une seule adresse IP. Ce type de tentatives ne se remarque pas sur les pare-feux, mais dans les journaux des serveurs ou sur d'éventuelles sondes (il semble que ces tentatives soient un acte isolé). Il est toutefois important de les signaler, car il peut s'agir d'une attaque généralisée sur tous les ministères.

Enfin, un de nos correspondants a signalé l'infection d'un poste par un cheval de Troie. Celui-ci nous a été transmis, et est à l'étude.

La suite du bulletin d'actualité fait le point sur un aspect souvent méconnu : l'utilisation des flux de données additionnels pour cacher des données. Cette technique a pu être mise en évidence lors d'un incident récemment traité par le CERTA.

port	pourcentage
445/tcp	28,26
137/udp	20,11
135/tcp	16,63
139/tcp	3,98
80/tcp	3,66
2745/tcp	3,23
1026/udp	2,88
1433/tcp	2,70
5554/tcp	2,69
9898/tcp	2,67
1080/tcp	2,43
1023/tcp	2,42
1434/udp	1,70
1027/udp	1,52
6129/tcp	1,10
3127/tcp	0,84
21/tcp	0,74
4899/tcp	0,67
3128/tcp	0,43
22/tcp	0,38
23/tcp	0,26
111/tcp	0,21
443/tcp	0,19
5000/tcp	0,15
3389/tcp	0,10
6112/tcp	0,04
10080/tcp	0,02
389/tcp	0,01

TAB. 2 – Paquets rejetés

3 Les flux de données additionnels

3.1 Historique

Le système de fichiers NTFS (NT FileSystem) a été développé par Microsoft à la fin des années 90 pour équiper le système d'exploitation Windows NT destiné au marché des serveurs. Il est utilisé depuis, par défaut, avec Windows NT, 2000, XP et 2003. Fort de l'expérience acquise dans le développement d'OS/2 et de son système de fichiers HPFS (High Performance File System) avec IBM, Microsoft a conçu un système de fichiers en phase avec l'état de l'art, ce qui était loin d'être le cas des vieillissants systèmes FAT. Parmi les apports, on peut relever la journalisation, le support du contrôle d'accès, la capacité à trier des fichiers d'après un attribut à l'aide d'index en arbres B (un répertoire est seulement un index qui trie les noms de fichier qu'il contient),...

3.2 Organisation

Chaque fichier présent est complètement décrit à l'aide d'un enregistrement (*file record*) de taille fixe (parfois plusieurs, surtout en cas de fragmentation du fichier). L'ensemble des enregistrements constitue un méta-fichier système appelé \$MFT (Master File Table) présent à la racine (visible jusqu'à NT4 avec la commande `dir /ah C:\$MFT` dans une console). A titre d'exemple, le premier enregistrement décrit le fichier \$MFT lui-même. Un enregistrement est une collection d'attributs (*attributes*). L'enregistrement inclut les attributs de petite taille (attributs résidents) ou liste les clusters du disque occupés par l'attribut (attribut non résident). Un attribut possède un type appartenant à une liste prédéfinie et éventuellement un nom codé en Unicode Microsoft (UTF16LE). Quelques types courants :

- information standard (*standard information*): contient en particulier les dates de création, écriture et accès au fichier et de modification de l'enregistrement dans le fichier \$MFT ;
- nom (*file name*): nom du fichier dans un espace de nommage donné (nom Win32, nom compatible DOS - format 8+3 -,...). Un fichier peut avoir plusieurs attributs de ce type, par exemple lorsque les noms DOS et Win32 sont différents ou lorsque des liens « durs » sont créés ;
- descripteur de sécurité (*security descriptor*): -systématiquement présent jusqu'à NT4- contient le propriétaire et le groupe sous forme de SID (*security identifier*) et les éventuelles listes de contrôle d'accès (SACL) et d'audit (DACL) ;
- l'attribut le plus facile à appréhender est celui du flux de données (*data stream*), dans sa version anonyme il correspond au contenu au sens usuel d'un fichier régulier ;
- les répertoires de fichier nécessitent 1 (pour les plus petits) ou 3 attributs ayant de types encore différents et tous nommés \$I30.

3.3 Les flux de données additionnels (Alternate Data Streams)

Un fichier peut ainsi avoir plusieurs flux de données (plusieurs contenus): le principal qui n'a pas de nom et d'autres éventuels pour peu qu'ils possèdent chacun un nom. On parle alors de flux de données additionnels (*alternate data streams*) ou flux nommés. Cependant la taille affichée par les applications courantes correspond toujours à celle du flux anonyme. A titre d'exemple, taper les commandes suivantes dans une console :

- `echo test >exemple:flux1`
- `dir exemple`
- `more <exemple:flux1`

Les commandes précédentes ont permis de créer dans le fichier « exemple » un flux nommé « flux1 », la commande `dir` annonce un fichier de taille nulle donc a priori vide et pourtant le contenu du flux additionnel peut être récupéré (plus déconcertant encore : créer un flux nommé dans un répertoire en faisant précéder les commandes ci-dessus de `mkdir exemple`).

Si l'évolution de l'API win32 permet maintenant de programmer aisément avec les flux nommés, le support au niveau des applications (même au sein des systèmes d'exploitation Windows) est quasi inexistant.

Il y a quelques années (en 2000 !), le CERTA avait relayé une information du SANS Institute qui faisait état d'un virus utilisant les flux nommés et s'inquiétait de l'absence de support dans les antivirus majeurs. Le problème n'est donc pas récent, mais semble avoir été marginalement exploité. Cependant, il apparaît que cette technique est un peu plus couramment employée de nos jours. Il est alors possible pour un virus de dissimuler l'essentiel de son code dans un ou des flux nommés en ne laissant apparaître dans le flux anonyme que peu de code. Si ce code résiduel n'est pas très caractéristique, il pourrait mettre en échec certains antivirus, tant que les moteurs d'analyse n'auront pas évolué, la grande majorité utilisant des signatures.

Lors d'un incident récemment traité par le CERTA, un virus utilisant les flux de données additionnels pour se dissimuler a été trouvé.

3.4 Sources

- Inside NTFS - Mark Russinovitch (en anglais) :
<http://www.winntmag.com/Articles/Index.cfm?IssueID=27&ArticleID=3455>
- Inside Win2K NTFS, Part 1 - Mark Russinovitch (en anglais) :
<http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15719>
- Inside Win2K NTFS, Part 2 - Mark Russinovitch (en anglais) :
<http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15900>

- NTFS Documentation - Richard Russon (d'après un travail initial de Remy Card) (en anglais) : <http://linux-ntfs.sourceforge.net/ntfs/index.html>
- Mauvaise compatibilité des scanners de virus avec NTFS : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-ALE-012/>

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

À 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 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 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

Pendant la période du 20 au 25 septembre 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-322 : Vulnérabilité du filtre d'impression foomatic-rip
- CERTA-2004-AVI-323 : Vulnérabilités sous FreeRadius
- CERTA-2004-AVI-324 : Vulnérabilité dans Sudo

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 CERTA-2004-AVI-313 CERTA-2004-AVI-315
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 CERTA-2004-AVI-247 CERTA-2004-AVI-301 CERTA-2004-AVI-313
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2003-AVI-038 CERTA-2004-AVI-126
1023	TCP	–	Serveur ftp de Sasser.E	–
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 CERTA-2004-AVI-316
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

- CERTA-2004-AVI-325 : Vulnérabilités de XFree86 et de libXpm
- CERTA-2004-AVI-326 : Multiples vulnérabilités dans les pare-feux Symantec

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

- CERTA-2004-AVI-319-002 : Multiples vulnérabilités dans gdk-pixbuf (ajout référence au bulletin de sécurité de SuSE. Ajout référence au bulletin de sécurité RHSA-2004:466 de Red Hat et DSA-549 de Debian)
- CERTA-2004-AVI-296-001 : Vulnérabilités de WinZip (ajout lien pour la mise-à-jour WinZip 9.0 SR-1 version française)
- CERTA-2004-AVI-278-004 : Vulnérabilité de la bibliothèque NSS (ajout de la référence au bulletin de sécurité de SUN du 16 septembre 2004)
- CERTA-2004-AVI-292-005 : Vulnérabilités de imlib et imlib2 (ajout de la référence au bulletin de sécurité de SUN)
- CERTA-2004-AVI-317-001 : Vulnérabilité de CUPS (ajout référence au bulletin de sécurité de Gentoo)
- CERTA-2004-AVI-272-003 : Vulnérabilités du serveur tnftpd (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2004-AVI-295-003 : Vulnérabilité dans ImageMagick (ajout de la référence au bulletin de sécurité Sun)
- CERTA-2004-AVI-319-003 : Multiples vulnérabilités dans gdk-pixbuf (ajout référence au bulletin de sécurité de Gentoo)
- CERTA-2004-AVI-292-006 : Vulnérabilités de imlib et imlib2 (ajout de la référence au bulletin de sécurité de Debian (DSA-552) pour imlib2)
- CERTA-2004-AVI-295-004 : Vulnérabilité dans ImageMagick (ajout de la référence au bulletin de sécurité Mandrake)
- CERTA-2004-AVI-304-003 : Vulnérabilité de mpg123 (ajout de la référence au bulletin de sécurité Mandrake)
- CERTA-2004-AVI-306-004 : Vulnérabilité de Usermin (ajout de la référence au bulletin de sécurité de Mandrake)
- CERTA-2004-AVI-311-001 : Multiples vulnérabilités de Samba (ajout de la référence au bulletin de sécurité de Red Hat)
- CERTA-2004-AVI-312-001 : Vulnérabilité de GDI+ de Microsoft (précision concernant les applicatifs tiers affectés par la vulnérabilité)

Par ailleurs, le CERTA a publié une alerte le 23 septembre :

- CERTA-2004-ALE-011 : Diffusion de programmes exploitant la faille GDI+

6 Documentation

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	2
3	Correctifs correspondant aux ports destination des paquets rejetés	5

Gestion détaillée du document

01 octobre 2004 version initiale.