Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 janvier 2005
N° CERTA-2005-ACT-002

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N2005-02

Gestion du document

Référence	CERTA-2005-ACT-002
Titre	Bulletin d'actualité N2005-02
Date de la première version	14 janvier 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

Le tableau 3 montre les rejets sur deux dispositifs de filtrage entre le 30 décembre 2004 et le 06 janvier 2005. Le CERTA a traité le cas d'une machine infectée par le cheval de Troie nommé `Netdepix` ou encore `Oddbob` (selon les éditeurs d'antivirus). Une des particularités de ce cheval de Troie est de provoquer un gros trafic réseau à destination de certaines classes d'adresses IP sur le port 11768/tcp. Nous avons donc ajouté le port 11768/tcp à notre liste de ports sous surveillance. Puisque toutes les classes d'adresses IP ne sont pas sondées par ce cheval de Troie, il est possible de n'avoir aucun rejet sur le port 11768/tcp en entrée. En revanche, il est possible d'en avoir en sortie si une machine a été infectée. Si vous constatez du trafic sortant ou entrant sur le port 11768/tcp, contactez le CERTA.

2 Windows NT 4 n'est plus maintenu

Depuis le 31 décembre 2004, Windows NT 4 Server n'est plus maintenu par Microsoft. Windows NT 4 Workstation ne sera plus maintenu à partir du 30 juin 2005.

Cela signifie donc qu'il n'y aura plus de correctif pour ce système d'exploitation, et probablement que dans les futurs avis émis par Microsoft, il ne sera pas précisé si Windows NT 4 est affecté ou non.

Les recommandations de base du CERTA sont d'appliquer les correctifs dès qu'ils sont disponibles, avec les réserves indiquées dans la note d'information CERTA-2001-INF-001. Pour ceux qui auraient encore des machines avec le système d'exploitation Windows NT 4, il est urgent de migrer vers d'autres systèmes d'exploitation maintenus.

3 Rappel des avis et des mises à jour émis

Durant la période du 03 au 07 janvier 2005, le CERTA a émis l'avis suivant :

- CERTA-2005-AVI-001 : Vulnérabilité sur CUPS
- CERTA-2005-AVI-002 : Vulnérabilité de l'utilitaire SAM sous HP-UX
- CERTA-2005-AVI-003 : Multiples vulnérabilités de libtiff
- CERTA-2005-AVI-004 : Vulnérabilité dans Xine
- CERTA-2005-AVI-005 : Vulnérabilité du noyau NetBSD
- CERTA-2005-AVI-006 : Vulnérabilité de KDE
- CERTA-2005-AVI-007 : Vulnérabilité du navigateur Mozilla
- CERTA-2005-AVI-008 : Vulnérabilité dans SHOUTcast
- CERTA-2005-AVI-009 : Vulnérabilité de Netscape Directory Server sous HP-UX

4 Actions suggérées

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

- CERTA-2004-AVI-388-003 : Vulnérabilité dans imlib
  (Ajout référence au bulletin de sécurité de Debian)
- CERTA-2004-AVI-402-005 : Vulnérabilité de Samba
  (ajout référence au bulletin de sécurité Mandrake MDKSA-2004:158)
- CERTA-2004-AVI-414-002 : Vulnérabilités dans MPlayer
  (ajout référence au bulletin de sécurité Gentoo)
- CERTA-2004-AVI-418-001 : Vulnérabilité de Xpdf
  (première révision : ajout des applications associées et ajout des avis Debian et Mandrake)
- CERTA-2004-AVI-289-001 : Vulnérabilité de gnome-vfs
  (ajout référence au bulletin de sécurité OpenBSD)
- CERTA-2004-AVI-398-004 : Vulnérabilité de Adobe Acrobat Reader sous Unix
  (ajout référence au bulletin de sécurité de Red Hat)
- CERTA-2004-AVI-370-002 : Vulnérabilités du serveur HTTP Apache
  (ajout de la référence au bulletin de sécurité HPSBTU01106 pour Apache sur Tru64 UNIX)
- CERTA-2004-AVI-412-001 : Vulnérabilité dans le service FTP sous HP-UX
  (ajout référence au bulletin de sécurité de HP)
- CERTA-2004-AVI-143-004 : Vulnérabilité dans le protocole TCP
  (ajout référence au bulletin de sécurité HP HPSBTU01077 pour Tru64 UNIX)
- CERTA-2004-AVI-409-003 : Nombreuses failles du noyau Linux
  (ajout référence au bulletin de sécurité RedHat RHSA-2004:689. Ajout référence CVE CAN-2004-1234)
- CERTA-2004-AVI-417-001 : Vulnérabilité dans mpg123
  (Ajout référence au bulletin de sécurité de FreeBSD. Correction erreur typo. dans le titre)
- CERTA-2004-AVI-391-002 : Vulnérabilité de zip
  (ajout référence au bulletin de sécurité de Debian)
- CERTA-2004-AVI-402-006 : Vulnérabilité de Samba
  (ajout référence au bulletin de sécurité Red Hat RHSA-2005-020)
- CERTA-2004-AVI-411-002 : Vulnérabilité de MIT Kerberos 5
  (ajout référence au bulletin de sécurité Gentoo GLSA 200501-05)
- CERTA-2005-AVI-003-001 : Multiples vulnérabilités de libtiff
  (ajout référence au bulletin de sécurité Gentoo GLSA 200501-06. Ajout référence CVE)
- CERTA-2004-AVI-388-004 : Vulnérabilité dans imlib
  (Ajout référence au bulletin de sécurité Debian DSA-628 pour imlib2)
- CERTA-2005-AVI-003-002 : Multiples vulnérabilités de libtiff
  (jout références aux bulletins de sécurité Mandrake MDKSA-2005:001, Debian DSA-626 et bulletins FreeBSD. Ajout référence CVE 1183)

– CERTA-2005-AVI-004-001 : Vulnérabilité dans Xine
(ajout référence au bulletin de sécurité Gentoo GLSA-200501-07)
– CERTA-2005-AVI-007-001 : Vulnérabilité du navigateur Mozilla
(ajout référence au bulletin de sécurité de Gentoo)
– CERTA-2005-AVI-008-001 : Vulnérabilité dans SHOUTcast
(ajout réference au bulletin de sécurité de Gentoo)

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. 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 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.

6 Documentation

– Note d'information CERTA-2001-INF-004 « Acquisition des correctifs » :
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004

Liste des tableaux

Gestion détaillée du document

14 janvier 2005 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-13
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-38
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-19 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-23
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 et samba	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-36 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-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-12 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-24 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	–
11768	TCP	–	Netdepix	–

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

port	pourcentage
445/tcp	31,91
135/tcp	26,25
139/tcp	11,20
1026/udp	4,06
1027/udp	3,24
137/udp	3,18
1433/tcp	2,53
4899/tcp	2,37
1434/udp	1,98
80/tcp	1,84
5554/tcp	1,56
9898/tcp	1,49
1023/tcp	1,37
42/tcp	1,05
6129/tcp	1,04
2745/tcp	1,03
22/tcp	0,76
21/tcp	0,69
443/tcp	0,66
1080/tcp	0,61
3127/tcp	0,49
23/tcp	0,20
3389/tcp	0,19
111/tcp	0,09
5000/tcp	0,09
3128/tcp	0,06
6112/tcp	0,06
10080/tcp	0,01

TAB. 3 – *Paquets rejetés*