Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 mars 2006
N° CERTA-2006-ACT-011

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-11

Gestion du document

Référence	CERTA-2006-ACT-011
Titre	Bulletin d'actualité 2006-11
Date de la première version	17 mars 2006
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.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-011.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-011/

1 Activité en cours

1.1 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 02 et le 09 mars 2006.

1.2 Vague d'infections par des codes malveillants

Le CERTA a été informé d'une vague d'infections de machines sous Windows par des codes malveillants de type `SDbot`. Ces infections ont eu pour principale caractéristique des tentatives de connexions depuis les machines infectées vers des serveurs `irc` en écoute sur le port 5599/tcp.

Le CERTA a pu reconstituer le scénario d'infection. Les utilisateurs de certains postes infectés ont reçu un message par le *service d'affichage des messages* (commandes NET SEND) les informant que leur machine contient des codes malveillants et les incitant à télécharger un outil pour nettoyer la machine. Le prétendu outil de désinfection est en fait un code malveillant aux multiples fonctions. Il tente de se connecter à des canaux `irc`. Le canal `irc` lui sert à recevoir des commandes en s'affranchissant de certaines protections apportées par les pare-feux par

exemple. Il tente également de se propager en exploitant des vulnérabilités bien connues (comme celle affectant le service `lsass`) ou des partages réseau. Les machines infectées engendrent des connexions à destination du port 5599/tcp de quelques serveurs à l'étranger, ainsi que de nombreux scans des ports 135/tcp, 139/tcp et 445/tcp.

Ce type de scénario d'infection a déjà été décrit dans le bulletin d'actualité du 10 juin 2005 (CERTA-2005-ACT-023) disponible à l'adresse :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-ACT-023.pdf

Il existe, outre la sensibilisation des utilisateurs, des moyens techniques pour se prémunir contre l'utilisation abusive du *service d'affichage des messages*. En effet, ce service peut être désactivé par les outils d'administration ou être bloqué par le réseau, en filtrant les ports 1026/udp et 1027/udp. Le CERTA constate que les rejets sur ces deux ports sont très nombreux, ce qui est visible sur la figure 1.

Pour empêcher une machine infectée de recevoir des instructions (via un canal `irc` par exemple), un filtrage en sortie peut être appliqué (interdire tous les ports sauf ceux explicitement nécessaires). Vous pouvez consulter la note d'information concernant le *filtrage et les pare-feux* (CERTA-2006-INF-001) disponible à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001/index.html

2 Liens utiles

- Mémento sur les virus ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information sur l'acquisition de correctifs ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
- Note d'information pour sur les systèmes obsolètes ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
- Note d'information sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien)
  http://www.auscert.org.au/render.html?it=1935

3 Rappel des avis et mises à jour émis

Durant la période du 10 mars au 16 mars 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-102 : Vulnérabilité dans l'installation Ubuntu
- CERTA-2006-AVI-103 : Vulnérabilité dans GnuPG
- CERTA-2006-AVI-104 : Vulnérabilité de Kpdf
- CERTA-2006-AVI-105 : Vulnérabilité de SSH.com SFTP
- CERTA-2006-AVI-106 : Vulnérabilité de Metamail
- CERTA-2006-AVI-107 : Vulnérabilité dans WordPress
- CERTA-2006-AVI-108 : Multiples vulnérabilités dans MacOS
- CERTA-2006-AVI-109 : Vulnérabilité dans Metamail
- CERTA-2006-AVI-110 : Vulnérabilité dans Flex
- CERTA-2006-AVI-111 : Vulnérabilité de nfsd sous FreeBSD
- CERTA-2006-AVI-112 : Multiples vulnérabilités dans Microsoft Office
- CERTA-2006-AVI-113 : Vulnérabilité de l'accès aux services dans Microsoft Windows
- CERTA-2006-AVI-114 : Vulnérabilités dans Flash Player
- CERTA-2006-AVI-115 : Plusieurs vulnérabilités dans l'outil zoo

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

- CERTA-2005-AVI-336-005 : Vulnérabilité du moteur d'expressions régulières PCRE
  (ajout de la référence au bulletin de sécurité Gentoo GLSA-200509-12, Gentoo GLSA-200509-19 et RedHat RHSA-2006:0197)

- CERTA-2005-AVI-428-003 : Multiples vulnérabilités dans PHP
  (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2006:035)
- CERTA-2005-AVI-499-003 : Vulnérabilité dans la bibliothèque libavcodec
  (ajout de la référence aux bulletin de sécurité Debian DSA-992)
- CERTA-2006-AVI-092-003 : Vulnérabilité de GNU tar
  (ajout des références aux bulletins de sécurité SUSE et Gentoo)
- CERTA-2006-AVI-095-003 : Multiples vulnérabilités dans Squirrelmail
  (ajout des références aux bulletins de sécurité SUSE et Gentoo)
- CERTA-2006-AVI-103-001 : Vulnérabilité dans GnuPG
  (ajout des références aux bulletins de sécurité Gentoo et Mandriva, corrections références Debian et FreeBSD)
- CERTA-2006-AVI-103-002 : Vulnérabilité dans GnuPG
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2006-AVI-114-001 : Vulnérabilités dans Flash Player
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-497-002 : Mise à jour des noyaux des distributions Linux
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2006:0144)

4 Actions suggérées

4.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

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. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

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 immédiate. 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.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

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.

4.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

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.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER

135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CER
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
15118	TCP	–	Netdepix	–

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

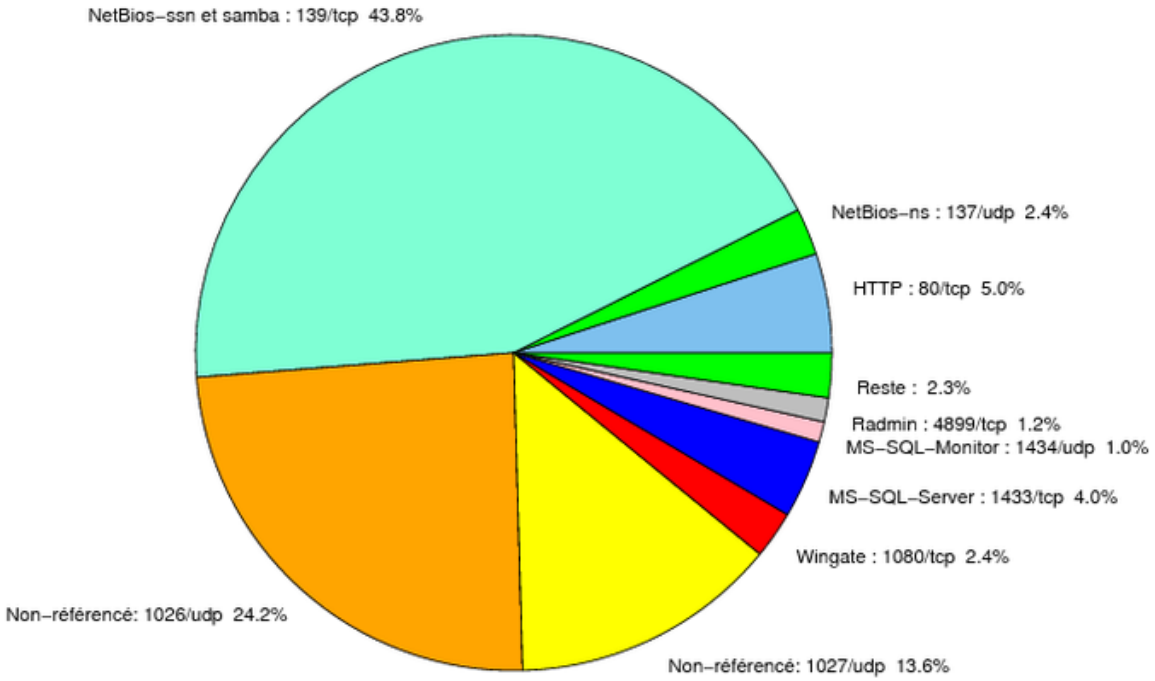

FIG. 1: Répartition relative des ports pour la semaine du 09.03.2006 au 16.03.2006

Liste des tableaux

Gestion détaillée du document

17 mars 2006 version initiale.

port	pourcentage
139/tcp	43,81
1026/udp	24,21
1027/udp	13,63
80/tcp	5,04
1433/tcp	3,97
1080/tcp	2,4
137/udp	2,37
4899/tcp	1,22
1434/udp	1,04
22/tcp	0,39
3306/tcp	0,25
3128/tcp	0,24
10000/tcp	0,19
9898/tcp	0,16
5554/tcp	0,13
443/tcp	0,11
106/tcp	0,1
15118/tcp	0,09
143/tcp	0,06
25/tcp	0,05
6129/tcp	0,04
2745/tcp	0,03
11768/tcp	0,02
6112/tcp	0,01

TAB. 3: Paquets rejetés