

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-01

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-2007-ACT-001>

Gestion du document

Référence	CERTA-2007-ACT-001
Titre	Bulletin d'actualité 2007-01
Date de la première version	05 janvier 2007
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-2007-ACT-001.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-2007-ACT-001/>

1 Activité en cours

1.1 Cartes de voeux

Le CERTA a eu plusieurs remontées d'informations concernant des infections suite à l'ouverture de fichiers joints dans des prétendues cartes de voeux. Ces infections sont attribuées à un ver appelé Luder, Nuwar, Dref ou Mixor (selon les éditeurs d'antivirus). Ce code malveillant n'était pas correctement détecté par les antivirus au moment de sa possible apparition (le 29 décembre 2006). Désormais, il est reconnu par presque tous les antivirus. Le comportement constaté, après infection, est un trafic HTTP à destination de machines situées dans la classe d'adresse 81.177.3.0/24 dans le but de télécharger et d'exécuter d'autres fichiers.

Il est possible que d'autres variantes de ce ver apparaissent au cours du mois de janvier.

Les recommandations du CERTA à ce sujet sont toujours d'actualité :

<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-001/>

2 Utilisation des listes noires pour lutter contre les pourriels

Un incident récent incite le CERTA à prôner la plus grande prudence dans l'utilisation des listes noires.

La lutte contre les pourriels repose sur plusieurs techniques dont certaines sont décrites dans la note d'information CERTA-2005-INF-004. L'une des techniques consiste à interroger un serveur de liste noire à l'arrivée de chaque message. Les listes noires contiennent des adresses et des noms de machine ou de domaine réputés pour diffuser des pourriels. L'utilisation classique est de rejeter tous les courriels provenant de machines ou de domaines qualifiés de « spammeurs » au vu des listes noires.

La gestion de ces listes noires n'offre pas la transparence nécessaire pour juger de leur fiabilité. Une machine peut être mise en liste noire sans contrôle objectif et vérifiable. Dans certains cas, une simple dénonciation auprès d'un gestionnaire de listes noires permet à un utilisateur malveillant de provoquer un déni de service.

3 « Month of Apple Bugs »

Depuis le 2 janvier, un projet appelé « Month of Apple Bugs » consiste en la diffusion journalière de vulnérabilités concernant les produits Apple. Pour cette semaine, ont été publiées 4 vulnérabilités :

- une dans la mise en œuvre du protocole RTSP par Apple Quicktime (MOAB-01-01-2007). Elle a fait l'objet d'une alerte (CERTA-2007-ALE-001) par le CERTA ;
- une autre dans la version pour MacOS X du lecteur multimedia VLC (MOAB-02-01-2007). Elle a fait l'objet d'un avis (CERTA-2007-AVI-002) du CERTA ;
- la troisième permettrait la réalisation d'attaques de type cross-site scripting par l'intermédiaire de Apple QuickTime ;
- enfin, la dernière concerne une faille dans le logiciel iPhoto et son composant de consultation d'album photographique en ligne ou photocast.

Ces publications vont normalement durer tout le mois de janvier. Le CERTA vous recommande donc d'effectuer une veille accrue sur d'éventuelles nouvelles publications concernant les produits Apple.

4 Vulnérabilité non-corrigée dans QuickTime

Cette Vulnérabilité a fait l'objet d'une alerte du CERTA : CERTA-2007-ALE-001. En effet, Un manque de contrôle sur les liens ou URI de type `rtsp://` permet à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire dans le contexte de l'utilisateur de l'application QuickTime vulnérable. L'exploitation de la vulnérabilité peut se faire par le biais d'un lien `rtsp://` directement ou bien par le biais d'un fichier `.qt1` construit de façon particulière. Il est à noter qu'il existe déjà, disponible sur l'Internet, du code malveillant exploitant cette vulnérabilité pour les versions Windows et MacOS X de QuickTime.

5 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 28 décembre 2006 et le 04 janvier 2007.

6 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 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>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html>
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/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>
- Note d'information du CERTA CERTA-2006-INF-006, Risques associés aux clés USB : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/>
- Note d'information du CERTA CERTA-2006-INF-008 sur les outils d'indexation et de recherche : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-008/>

7 Rappel des avis émis

Durant la période du 29 décembre 2006 au 04 janvier 2007, le CERTA a émis l'alerte et les avis suivants :

- CERTA-2007-ALE-001 : Vulnérabilité dans Apple Quicktime
- CERTA-2007-AVI-001 : Vulnérabilités dans Cacti
- CERTA-2007-AVI-002 : Vulnérabilité dans VLC media player
- CERTA-2007-AVI-003 : Multiples vulnérabilités du greffon Adobe Acrobat Reader
- CERTA-2007-AVI-004 : Vulnérabilités dans Cisco Clean Access

8 Actions suggérées

8.1 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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme 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 réglementaire, 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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>

9 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.

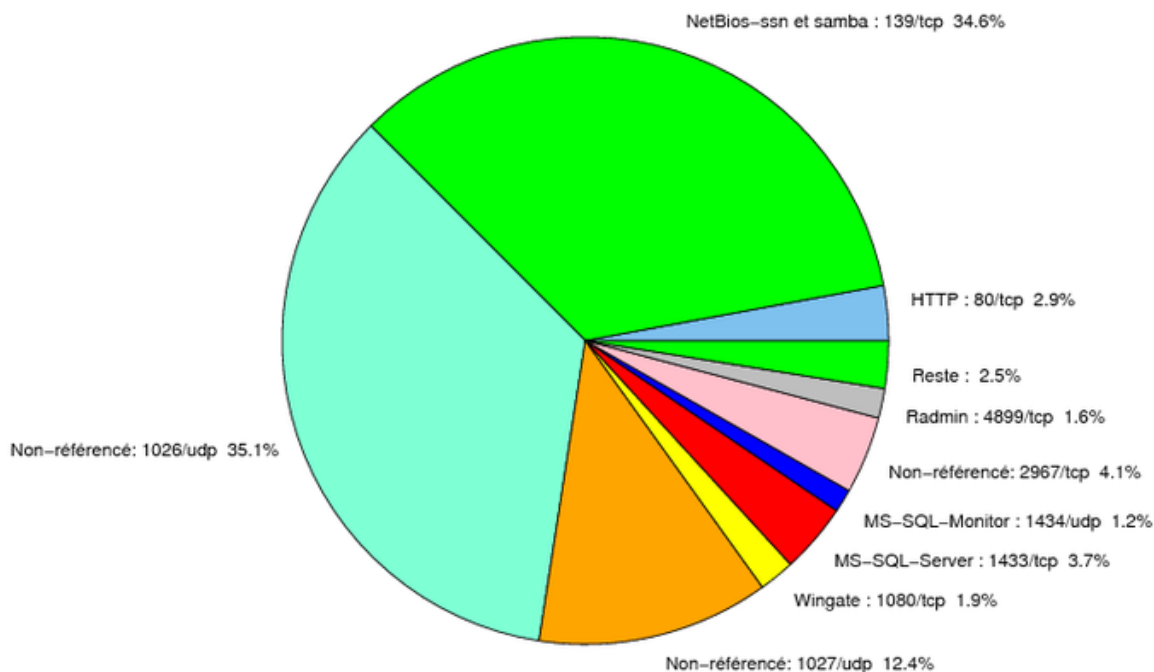


FIG. 1: Répartition relative des ports pour la semaine du 28.12.2006 au 04.01.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CEI
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CEI
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CEI
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CEI
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI

				http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE
2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

TAB. 2: Correctifs correspondant aux ports destination des paquets re-jetés

port	pourcentage
1026/udp	35.05
139/tcp	34.59
1027/udp	12.36
2967/tcp	4.12
1433/tcp	3.71
80/tcp	2.9
1080/tcp	1.89
4899/tcp	1.57
1434/udp	1.23
137/udp	0.54
22/tcp	0.48
25/tcp	0.46
3128/tcp	0.42
443/tcp	0.22
15118/tcp	0.2
143/tcp	0.08
3306/tcp	0.04
42/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	6
3	Paquets rejetés	7

Gestion détaillée du document

05 janvier 2007 version initiale.