Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 avril 2005
N° CERTA-2005-ACT-015

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N2005-15

Gestion du document

Référence	CERTA-2005-ACT-015
Titre	Bulletin d'actualité N2005-15
Date de la première version	15 avril 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

1.1 Ports observés

Le tableau 3 montre les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 31 mars et le 07 avril 2005. Les rejets sont principalement composés de paquets à destination du port 445/tcp.

Nous avons ajouté le port 25/tcp à notre surveillance, suite à l'avis CERTA-2005-AVI-133 affectant Microsoft Exchange Server. Une vulnérabilité critique de ce serveur permet l'exécution de code arbitraire à distance. Nous n'avons pas connaissance d'exploitation de cette faille à ce jour, toutefois, si vous constatez une augmentation significative des rejets sur le port 25/tcp, il est important d'en informer le CERTA.

1.2 Incidents traités par le CERTA

Un cas de défiguration de site web a été traité par le CERTA. La faille exploitée affectait le forum phpBB.

D'autre part, un correspondant nous a fait part de la compromission possible d'une quinzaine de machines sous Windows (postes utilisateur). Quelques unes de ces machines ont été infectées par Blaster ou Sasser. Leur vulnérabilité était liée à leur réinstallation à partir d'une image logique faite depuis une machine qui n'avait pas été mise à jour. Une autre de ces machines avait un programme de type `adware` (logiciel affichant de la publicité de façon intempestive, et ayant parfois d'autres fonctionnalités). L'outil utilisé par l'administrateur (se présentant sous la forme d'un exécutable appelé `New_uninstall.exe`) pour désinstaller cet `adware` contenait un cheval de

Troie, aggravant ainsi l'incident. Il est conseillé de contacter le CERTA dès la détection des incidents de sécurité, quels qu'ils soient. Le CERTA, par son expertise, peut dans certains cas vous déconseiller l'utilisation de certains outils.

1.3 Infections par MyTob

Un correspondant nous a informés de l'infection virale de son réseau par MyTob. Au moment des faits, les signatures de l'antivirus ne permettaient pas de détecter le virus. Désormais, la plupart des antivirus reconnaissent le ver MyTob. Il est donc par conséquent important de mettre à jour la base des signatures des antivirus.

2 Utilisation des images logiques pour installer des machines

Un incident récemment traité par le CERTA a mis en évidence un problème posé par l'utilisation des images logiques pour installer des machines.

Les images logiques sont souvent utilisées par les administrateurs afin d'installer rapidement et massivement des machines. Ces images sont réalisées à partir d'une machine étalon. Il convient donc de mettre à jour cette machine étalon dès la sortie des correctifs, de vérifier qu'elle est exempte de failles de sécurité connues, et de s'assurer qu'elle n'est pas compromise avant de réaliser toute image. De surcroît, les images logiques ainsi réalisées doivent être refaites dès la sortie de nouveaux correctifs. Il est par ailleurs fortement conseillé d'utiliser une machine dédiée et isolée du réseau pour réaliser ces images.

3 Multiples vulnérabilités critiques dans Windows

Microsoft a publié le 12 avril 2005 de nombreux correctifs concernant des failles critiques d'Internet Explorer, de Microsoft Exchange Server, de MSN Messenger et de l'interpréteur de commandes Windows. Des outils d'exploitation de certaines de ces vullnérabilités (Internet Explorer et interpréteur de commandes Windows) ont été rendus publics. Il est donc extrêmement important d'appliquer sans délai ces correctifs.

4 Rappel des avis et mises à jour émis

Durant la période du 04 au 09 avril 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-127 : Vulnérabilités de SSH sous Cisco IOS
- CERTA-2005-AVI-128 : Vulnérabilité dans Sylpheed
- CERTA-2005-AVI-129 : Vulnérabilité du serveur d'application ColdFusion
- CERTA-2005-AVI-130 : Vulnérabilité dans Lotus Domino

Pendant cette même période, la mise à jour suivante a été publiée :

- CERTA-2005-AVI-122-002 : Multiples vulnérabilités dans ImageMagick
  (ajout des références aux bulletins de sécurité de Mandrake et Debian)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

6 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.

Liste des tableaux

Gestion détaillée du document

15 avril 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
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-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-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-05
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-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-05
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
3306	TCP	MySQL	–	–
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	–
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-02
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	–
15118	TCP	–	Netdepix	–

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

port	pourcentage
445/tcp	68,74
139/tcp	8,58
1433/tcp	6,97
1026/udp	3,66
137/udp	3,39
4899/tcp	2,24
1027/udp	1,74
15118/tcp	1,07
9898/tcp	0,51
1080/tcp	0,41
5554/tcp	0,38
1434/udp	0,31
23/tcp	0,23
22/tcp	0,22
80/tcp	0,22
42/tcp	0,20
3306/tcp	0,14
6129/tcp	0,14
1023/tcp	0,12
135/tcp	0,12
2745/tcp	0,11
443/tcp	0,09
3128/tcp	0,08
25/tcp	0,07
6101/tcp	0,07
21/tcp	0,05
11768/tcp	0,05
111/tcp	0,05
3127/tcp	0,04

TAB. 3 – *Paquets rejetés*