Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mai 2004
N° CERTA-2004-ACT-002

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N2

Gestion du document

Référence	CERTA-2004-ACT-002
Titre	Bulletin d'actualité N2
Date de la première version	26 mai 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

Le tableau des paquets rejetés (cf. table 2) montre l'activité entrante refusée sur deux pare-feux configurés pour tout bloquer par défaut et n'autoriser que quelques services sur quelques serveurs. Les ports présents dans ce tableau ont été choisis pour leur fréquence d'apparition ou pour leur caractère dangereux constaté dans des incidents traités par le CERTA.

Il s'agit de déterminer à quoi correspondent ces paquets rejetés et quels sont les enseignements pragmatiques en termes d'administration quotidienne de la sécurité que l'on peut retirer de l'observation de ces rejets de paquets.

Durant la période du 13 mai 2004 au 20 mai 2004, l'activité a été à peu près équivalente sur les ports 135/tcp et 445/tcp. Malgré des mesures de filtrage spécifiques mises en place par des fournisseurs d'accès, ces deux ports sont toujours les plus recherchés. Les rejets sur les ports 135/tcp et 445/tcp représentent, à eux deux, plus de la moitié des rejets constatés.

L'activité des vers `Bobax` et `Kibuv` se traduit par la brusque augmentation des rejets sur le port 5000/tcp (voir Actualité particulière). Un paquet sur vingt rejetés semble lié à ces deux vers.

Le ver `Dabber` qui exploite le serveur ftp déposé par le ver `Sasser`, et en écoute sur le port 5554/tcp, ne semble pas s'être propagé aussi rapidement que `Bobax` et `Kibuv`. Le port 5554/tcp est parfois recherché en même temps que le port 9898/tcp qui correspond à la porte dérobée laissée par `Dabber`.

port	pourcentage
445/tcp	29,78
135/tcp	29,37
80/tcp	10,80
137/udp	6,91
2745/tcp	6,38
5000/tcp	5,19
3127/tcp	2,77
139/tcp	2,45
6129/tcp	1,63
1433/tcp	1,11
1434/udp	1,07
5554/tcp	0,48
443/tcp	0,44
4899/tcp	0,41
21/tcp	0,34
9898/tcp	0,25
1080/tcp	0,22
23/tcp	0,11
111/tcp	0,10
3128/tcp	0,08
3389/tcp	0,06
6112/tcp	0,03
22/tcp	0,03

TAB. 2 – *Paquets rejetés*

3 Actualité particulière

3.1 Le ver Sasser

Durant la semaine du 13 mai 2004 au 20 mai 2004, le nombre de rejets sur le port 445/tcp a diminué, pour revenir au niveau du début du mois d'avril 2004, c'est-à-dire avant que ne soit rendue publique la faille affectant le service `lsass` de Windows. Plusieurs raisons peuvent expliquer ce phénomène :

- les correctifs de Microsoft ont été appliqués, limitant ainsi la propagation du ver Sasser ;
- des mesures de filtrage ont été mises en place par certains fournisseurs d'accès ;
- des mesures de filtrage ont été mises en place par les entreprises et les administrations.

3.2 Les vers Bobax et Kibuv

Les vers `Bobax` et `Kibuv` ont fait leur apparition à la mi-mai 2004. Ces vers se distinguent car ils recherchent le port 5000/tcp. Ce port correspond généralement au service `UPnP` de Microsoft qui permet de détecter les périphériques sur le réseau. Ce service est installé et lancé par défaut sur les machines sous Windows XP. Le scan sur le port 5000/tcp est la signature de ces vers probablement dans le but d'identifier les machines sous Windows XP afin de les compromettre en exploitant diverses failles (dont `lsass`). Ces vers ne se propagent pas en exploitant

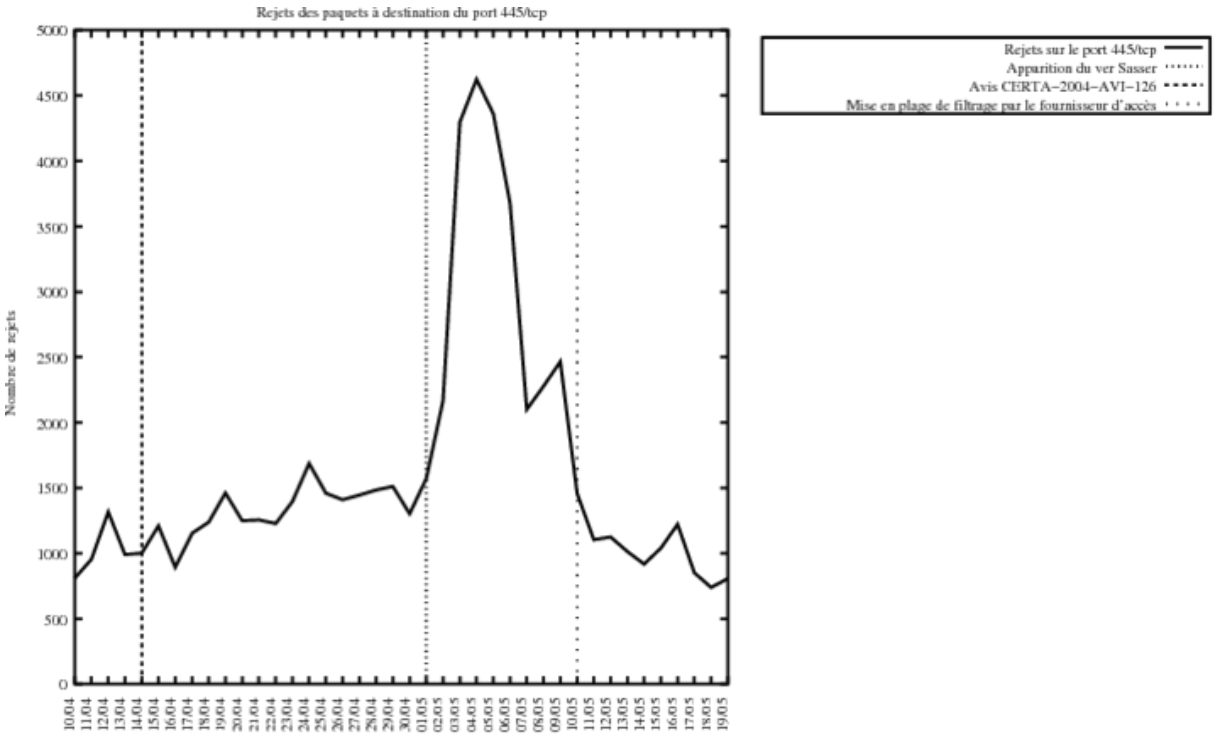

FIG. 1 – *Historique des rejets de paquets sur le port exploité par le ver Sasser*

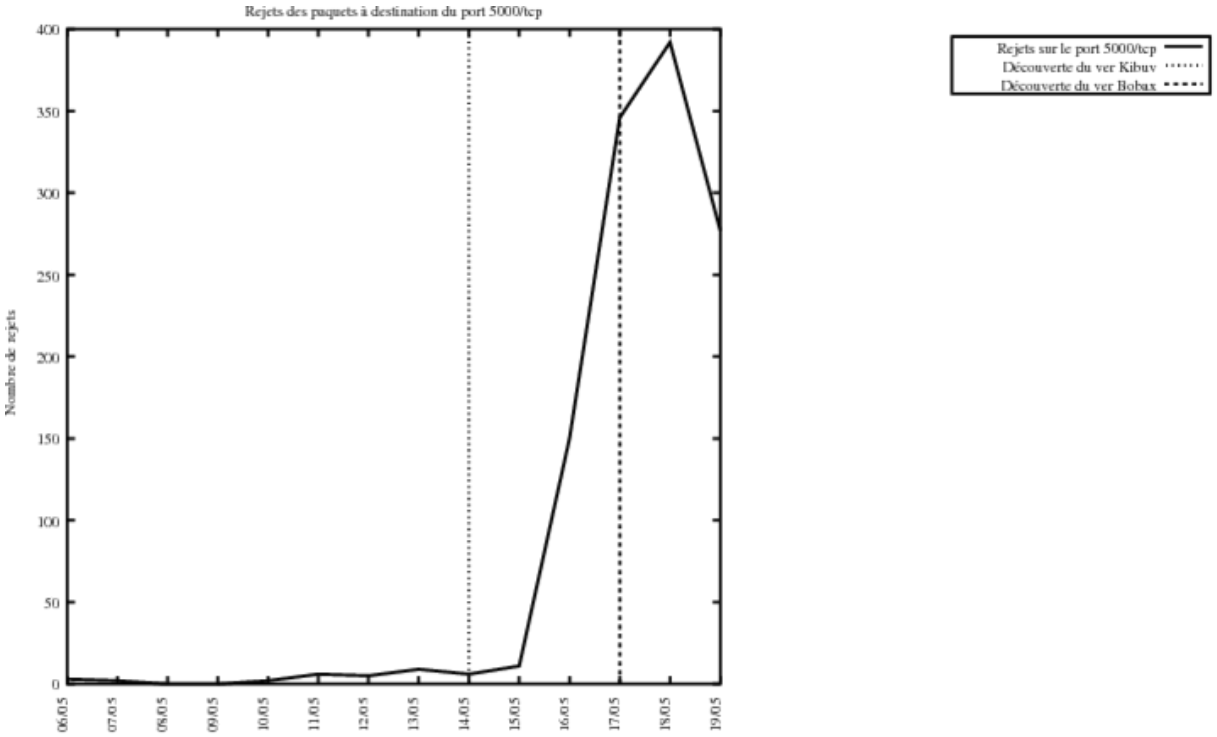

FIG. 2 – *Historique des rejets de paquets sur le port recherché par les vers Bobax et Kibuv*

la faille de UPnP découverte en 2001. L'application des correctifs de Microsoft est la meilleure parade à ces vers. Des règles de filtrage sur le port 5000/tcp sont également adéquates (même si elles ne suffisent pas) puisque le trafic sur le port 5000/tcp ne devrait pas circuler sur l'Internet.

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 Appliquer les correctifs de sécurité

La table 3 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

4.3 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 les 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 d'un pare-feu.

4.4 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 de sorte à découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

4.5 Réagir aux incidents de sécurité

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

Liste des tableaux

Gestion détaillée du document

26 mai 2004 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-066 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-064 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-132
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-152
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-209 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-179 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-131
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-050
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-052
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-111 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-031
139	TCP	NetBios-ssn	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-168 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-144 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-045 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-102 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-068 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-041 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-004 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-156
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-095 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-053 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-105 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-038 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
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-157
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-062
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-165
5554	TCP	–	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-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*