

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité du 10 mai 2004

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-2004-ACT-001>

Gestion du document

Référence	CERTA-2004-ACT-001
Titre	Bulletin d'actualité du 10 mai 2004
Date de la première version	10 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 de la semaine

Le tableau des paquets rejetés (cf. table 2) montre l'activité sur deux pare-feux configurés pour tout bloquer par défaut (à l'exception de quelques rares services comme le DNS, le SMTP et le HTTP qui sont autorisés pour des serveurs dédiés).

Le port 445/tcp, utilisé par les Windows (avec un noyau NT) pour divers services, est le port le plus recherché. Ceci s'explique en partie par l'activité de certains vers, comme *Sasser* (voir CERTA-2004-ALE-007).

port	pourcentage
445/tcp	57,13
135/tcp	13,66
80/tcp	7,62
2745/tcp	6,68
137/udp	6,04
139/tcp	2,95
3127/tcp	2,10
6129/tcp	1,38
1434/udp	0,60
1433/tcp	0,59
443/tcp	0,34
4899/tcp	0,31
21/tcp	0,21
3389/tcp	0,10
1080/tcp	0,09
3128/tcp	0,08
111/tcp	0,08
23/tcp	0,03
22/tcp	0,02

TAB. 2 – *Paquets rejetés*

Le port 135/tcp est associé aux services RPC sous Windows. Le tableau donne le sentiment qu'il y a 4 fois moins de rejets sur le port 135/tcp que sur le port 445/tcp, mais cela est dû essentiellement au fait que l'un des deux pare-feux a une adresse IP chez un fournisseur d'accès ADSL qui filtre le port 135/tcp en amont. Le trafic à destination du port 135/tcp n'est, en réalité, que deux fois moins important que celui à destination du port 445/tcp. Une vulnérabilité affectant l'un des services RPC de Windows a largement été exploitée par le ver Blaster (voir CERTA-2003-ALE-002).

Le port 80/tcp est encore très sondé. Il correspond au service HTTP, et est visé par de nombreux vers, tels que ceux de la famille `codered` (voir CERTA-2001-ALE-008) ou encore `nimda` (voir CERTA-2001-ALE-013).

Le port 2745/tcp correspond à la porte dérobée laissée par les différentes versions du ver Bagle. L'utilisation de cette porte dérobée fait partie des moyens de propagation de Phatbot (voir CERTA-2004-ALE-003). L'ouverture de ce port sur les machines sous Windows signifie probablement leur compromission.

Le port 137/udp est utilisé par le service de noms Netbios. Il s'agit là encore d'un port spécifique à Windows.

Le port 139/tcp est utilisé par Netbios et par Samba.

Le port 3127/tcp correspond à la porte dérobée ouverte après infection par les différentes versions du ver MyDoom. Cette porte dérobée est également exploitée par Phatbot. Les machines sous Windows avec ce port en écoute sont très probablement des machines compromises.

Le port 6129/tcp correspond à Dameware, un outil d'administration à distance des machines Windows. Une vulnérabilité -très exploitée- de Dameware Miniremote (voir CERTA-2003-AVI-214). Cette vulnérabilité est aussi utilisée par Phatbot pour se propager. L'outil Dameware est parfois installé par des intrus, suite à une compromission, afin de pouvoir facilement se reconnecter sur les machines compromises (par le biais d'une vulnérabilité quelconque, autre que celle affectant Dameware). Des versions vulnérables de Dameware ont ainsi été installées sur des machines compromises.

Les ports 1433/tcp et 1434/udp sont utilisés par MS/SQL. Ce service a fait l'objet de très nombreuses vulnérabilités exploitées notamment par deux vers nommés `spida` et `slammer`. Ces vulnérabilités sont assez anciennes (2 ans) mais sont toujours exploitées.

Le port 443/tcp est utilisé par HTTPS. La publication d'un outil permettant l'exploitation d'une faille dans le protocole PCT rendue récemment publique a provoqué une augmentation des recherches du port 443/tcp.

Le port 4899/tcp est utilisé par `radmin`, un outil d'administration à distance.

Le port 21/tcp correspond au service FTP. De nombreuses failles affectent différentes versions de serveur ftp. Le port 21/tcp est sondé pour exploiter ces failles, mais aussi pour trouver des serveurs ftp publics permettant le stockage de fichiers illicites.

Le port 3389/tcp est utilisé par le protocole RDP (Remote Desktop Protocol). Le but des sondages sur ce port

n'est pas très clair.

Le port 1080/tcp est utilisé par le serveur mandataire *Wingate*. Ce port était autrefois recherché pour être utilisé comme relais de navigation (permettant ainsi de commettre éventuellement des actes malveillants avec l'adresse IP du serveur *Wingate* plutôt que sa propre adresse IP). Il correspond aussi à une porte dérobée laissée par le ver *MyDoom.F* après infection, et c'est à ce titre qu'il est sondé par *Phatbot*.

Le port 3128/tcp est utilisé par le serveur mandataire *Squid*. Il correspond également à une porte dérobée laissée par certaines versions de *MyDoom*, et fait partie des ports recherchés par *Phatbot*.

Le port 111/tcp correspond au service *sunrpc-portmapper*. La recherche de ce port est typiquement une étape préparatoire à une compromission par l'exploitation d'une faille d'un service *rpc* (par exemple, *rpc.statd* dont une faille a été largement exploitée par le passé).

Le port 23/tcp correspond au service *telnet*. Ce service permet la connexion à distance sur des machines après authentification. Toutefois, l'utilisation de ce service facilite le vol des noms de compte utilisateur et des mots de passe lors de l'authentification, car celle-ci n'est pas chiffrée.

Le port 22/tcp correspond au service *ssh*. Ce service permet, tout comme *telnet*, de se connecter à distance sur des machines, mais la connexion est chiffrée, ce qui garantit une meilleure sécurité. Une vulnérabilité affectant le service de détection des attaques a largement été exploitée par le passé. Cette vulnérabilité semble toujours être recherchée.

Le tableau montre que les vulnérabilités assez anciennes sont toujours recherchées, et probablement dans certains cas avec succès.

3 Activité particulière

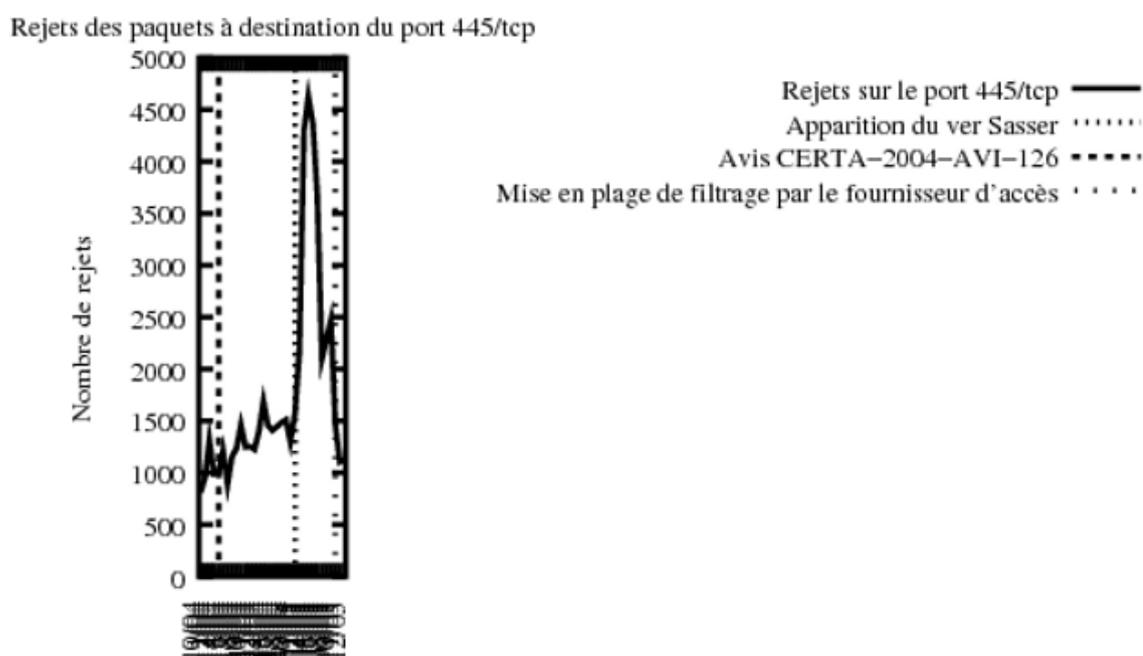


FIG. 1 – Historique des rejets de paquets sur le port exploité par le ver *SASSER*

L'actualité a été marquée par la propagation du ver *Sasser*. Ce ver se propage en exploitant une vulnérabilité connue du service *lsass* (port 445/tcp) sous *Windows*. Il n'existe qu'un seul moyen efficace de bloquer cette propagation : mettre à jour les machines. Les contournements provisoires, tels que la mise en place de règles de filtrage sur le port 445/tcp au niveau des pare-feux, sont efficaces, à l'unique condition que ces règles de filtrage ne soient pas elles-mêmes contournées. Or, il est fréquent de voir des postes nomades (portables) être protégés uniquement par des pare-feux réseau. Les postes nomades sont généralement voués à être déplacés, et éventuellement connectés à des réseaux qui ne sont pas forcément protégés par des pare-feux bien configurés. L'activation du pare-feu livré avec *Windows XP* est suffisante pour endiguer ce ver. Néanmoins, il est tout de même recommandé d'appliquer le correctif de *Microsoft*, qui corrige de nombreuses autres vulnérabilités.

L'activité de ce ver se traduit par un triplement du volume des rejets sur le port 445/tcp.

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-002 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-006
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-157
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	–	–
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-001
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
10080	TCP	Amanda	MyDoom	–

TAB. 3 – Correctifs correspondants aux ports destination des paquets rejetés

4 Documentation

Alerte CERTA-2001-ALE-008 «Propagation du ver Code Red» :

<http://www.certa.ssi.gouv.fr/site/CERTA-2001-ALE-008>

Alerte CERTA-2001-ALE-013 «Propagation du ver/virus NIMDA (Concept Virus)» :

<http://www.certa.ssi.gouv.fr/site/CERTA-2001-ALE-013>

Alerte CERTA-2003-ALE-002 «Exploitation d'une faille de Windows RPC» :

<http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-002>

Alerte CERTA-2004-ALE-003 «Propagation du ver Phatbot» :

<http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-003>

Alerte CERTA-2004-ALE-007 «Exploitation de la vulnérabilité LSASS sous Windows : apparition du ver Sasser» :

<http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-007>

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	2
3	Correctifs correspondants aux ports destination des paquets rejetés	4

Gestion détaillée du document

10 mai 2004 version initiale.