Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 juin 2004
N° CERTA-2004-ACT-004

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N4

Gestion du document

Référence	CERTA-2004-ACT-004
Titre	Bulletin d'actualité N4
Date de la première version	09 juin 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.

port	pourcentage
445/tcp	32,07
135/tcp	31,26
80/tcp	8,02
137/udp	7,76
139/tcp	4,49
2745/tcp	4,47
3127/tcp	2,30
1433/tcp	1,81
6129/tcp	1,63
1434/udp	1,26
5000/tcp	0,93
4899/tcp	0,83
21/tcp	0,62
1080/tcp	0,58
5554/tcp	0,54
9898/tcp	0,44
443/tcp	0,29
111/tcp	0,21
3128/tcp	0,19
23/tcp	0,09
22/tcp	0,09
3389/tcp	0,08
6112/tcp	0,03
10080/tcp	0,01

TAB. 2 – *Paquets rejetés*

Le tableau des rejets montre l'activité durant la période du 27 mai 2004 au 03 juin 2004. Les rejets sur les ports 135/tcp et 445/tcp représentent près des deux tiers de l'activité. Une grosse partie des paquets rejetés peut correspondre aux tentatives de propagation de différents vers. Ces vers, qui s'attaquent tous à des machines Windows, sont responsables d'une grosse partie des paquets rejetés. L'application de règles de filtrage en sortie et le cloisonnement des réseaux internes limiteraient ce type de trafic.

3 Un regard sur l'actualité

Le mercredi 26 mai 2004 est paru un article dans le quotidien *Libération* sur les mouchards contenus dans certains courriers électroniques (cf. section Documentation).

L'article mentionnait le service du site *didtheyreadit.com*, qui permet à un utilisateur de vérifier que son courrier électronique a bien été lu par son destinataire, et même d'en préciser l'heure de lecture.

Le principe utilisé est l'insertion dans le courrier électronique d'une image invisible (d'une taille d'un pixel par exemple, également appelée *webbug*). Voici le lien inséré dans le code source du message au format HTML :

```
<img src="http://www.didtheyreadit.com/index.php?worker.code=3102383a7c63eb7640b... "
width="1" height="1" />
```

L'image est récupérée sur le serveur à la lecture du courrier électronique. En analysant les journaux d'événements de ce serveur, il est donc possible d'en déterminer la date et l'heure, l'adresse IP du lecteur ou de son serveur mandataire (proxy), l'adresse du Webmail dans certains cas, ...

Contrairement à ce qui est mentionné dans l'article, un pare-feu ou autre équipement de filtrage réseau a peu de chance d'empêcher ce mécanisme. En effet, il faudrait pour cela bloquer le port 80/tcp (correspondant au protocole HTTP) sur le trafic sortant.

Pour laisser aux utilisateurs un accès aux sites Internet, cela est rarement fait.

Ceci peut néanmoins être fait sur des postes dédiés au courrier, sur lesquels on n'autorise que les protocoles SMTP (25/tcp), POP3 (110/tcp) et IMAP (143/tcp).

En revanche, il existe une parade efficace : ne consulter les courriers électronique qu'au format texte. Dans ce cas, le code HTML contenant l'appel vers l'image ne sera pas exécuté. De plus, cela vous protègera également contre l'exécution de code malicieux contenu dans le code source du message.

Certains clients de messagerie n'interprètent pas le HTML, d'autres peuvent être configurés pour ne pas prendre en compte le format HTML.

Vous pouvez vous référer à la note d'information du CERTA CERTA-2000-INF-002 concernant les mesures de prévention relatives à la messagerie (cf. section Documentation).

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.

5 Documentation

- Article du quotidien *Libération* du 26 mai 2004 :
  http://www.liberation.fr/page.php?Article=209082
- Site *Didtheyreadit.com* :
  http://www.didtheyreadit.com
- Note d'information du CERTA CERTA-2000-INF-002 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html

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	SGI ESP HTTP	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*

Liste des tableaux

Gestion détaillée du document

09 juin 2004 version initiale.