Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 juin 2004
N° CERTA-2004-ACT-006

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N6

Gestion du document

Référence	CERTA-2004-ACT-006
Titre	Bulletin d'actualité N6
Date de la première version	23 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

Les rejets constatés pendant la période du 10 juin 2004 au 17 juin 2004 sont composés pour moitié par le trafic sur le port 445/tcp. Il est à noter que près de 90% de ces rejets proviennent du bloc 213.0.0.0/8, dans lequel se trouve un de nos dispositifs de filtrage.

port	pourcentage
445/tcp	48,14
135/tcp	16,60
137/udp	10,66
80/tcp	4,85
139/tcp	4,83
2745/tcp	3,87
1433/tcp	1,71
1434/udp	1,69
3127/tcp	1,63
6129/tcp	1,32
5554/tcp	0,96
4899/tcp	0,90
9898/tcp	0,82
21/tcp	0,57
1080/tcp	0,46
443/tcp	0,26
5000/tcp	0,23
111/tcp	0,17
3128/tcp	0,14
3389/tcp	0,10
23/tcp	0,05
10080/tcp	0,02
22/tcp	0,01

TAB. 2 – *Paquets rejetés*

3 Retour d'expérience sur les incidents

3.1 Déni de service provoqué par le spam

Nous avons été récemment confrontés à de nombreux incidents concernant les courriers électroniques non sollicités (*spam*).

Si toutes les organisations sont victimes de ce désagrément, il arrive ponctuellement que la charge dûe à courriers provoque une véritable saturation des serveurs de messagerie.

Les auteurs de ces envois utilisent notamment deux techniques pour inonder les boîtes aux lettres d'une organisation :

- soit un robot envoie directement les courriers électroniques à destination de l'organisation ;
- soit les courriers sont envoyés à une adresse non valide, avec pour champ expéditeur l'adresse mail à atteindre. C'est alors le message d'erreur qui transmettra le courrier non sollicité.

Dans les deux cas, et comme souvent lorsqu'il s'agit d'attaque de type déni de service, il est difficile de mettre en place une solution efficace. Les adresses émettrices varient en général d'un message à l'autre, et bloquer des domaines entiers peut provoquer le rejet de certains messages légitimes.

Une première étape peut consister à ne plus envoyer de messages d'erreurs lorsqu'un courrier électronique parvient au serveur avec un destinataire inconnu. Cela allègera la charge du trafic sur le réseau et ne donnera pas d'information sur les comptes de messagerie de l'organisation.

La suppression du message d'erreur abaissera néanmoins la qualité de service de votre messagerie : en effet un correspondant légitime ne sera plus prévenu en cas d'erreur dans l'orthographe du nom du destinataire.

Pour alléger la charge du serveur de messagerie, il est également possible de mettre en cascade un deuxième serveur SMTP chargé d'effectuer un premier filtre. A l'aide d'une expression régulière, il est possible de vérifier qu'une adresse est bien formée (par exemple *prenom.nom@nomdedomaine*).

Enfin, pour déterminer l'origine de ces messages et en retracer le cheminement à travers différents serveurs de courrier, il est nécessaire de conserver l'intégralité des en-têtes des messages.

3.2 Un spam particulier venu d'Allemagne

Certains membres de notre communauté ont eu la désagréable surprise de recevoir ces derniers temps des courriers électroniques en allemand à caractère raciste, et ce, malgré un filtrage de leur courrier par un logiciel anti-spam.

Outre le fonctionnement parfois imparfait de ces outils, les filtres fonctionnent surtout sur des mots ou expressions anglaises, souvent à caractère pornographique ou commercial.
Dans ce cas, les chaînes de texte en allemand n'ont pas été identifiées comme génântes.

Ces messages sont en fait un des effets de bord d'une des versions du virus *Sober* qui s'est récemment propagée.

Voici une liste des titres des messages qu'il est possible de filtrer (une liste complémentaire peut être trouvée sur le site de NAI - cf. section Documentation) :

- Bin ich zu weltfremd? Ich glaube wohl kaum
- Libanesen in Berlin <Id:1892>
- Auslaendergewalt: Herr Rau, wo waren Sie? #Key:4683#
- TUERKEN-TERROR AM HIMMELFAHRTSTAG
- Geschrieben von Margrit am 07. April 2004
- Bankrott des Gesundheitswesens durch Auslaender!
- Die Deform der sozialen Ordnung (Key:8677)
- Diplomatische Zensur
- Skandalurteil in Darmstadt
- So sieht die Wahrheit aus!
- Auslaendergewalt: Herr Rau, wo waren Sie?
- Richter unterstuetzt kriminelle Auslaenderin [Id:8890]

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 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.

4.3 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.

4.4 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 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.

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*

4.5 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.

4.6 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.

5 Documentation

Article de l'ADAE sur la lutte contre le spam :
http://www.adae.gouv.fr/article.php?id_article=475
Description du virus *Sober* sur le site de NAI :
http://vil.nai.com/vil/content/v_126243.htm

Liste des tableaux

Gestion détaillée du document

23 juin 2004 version initiale.