



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 juin 2004
N° CERTA-2004-ACT-005

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N5

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-005>

Gestion du document

Référence	CERTA-2004-ACT-005
Titre	Bulletin d'actualité N5
Date de la première version	15 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 03 juin 2004 au 10 juin 2004 sont composés essentiellement par le trafic port 445/tcp. Ces rejets sont deux fois plus importants que ceux sur le port 135/tcp, et quatre fois plus importants que ceux sur le port 137/udp. Ces trois ports correspondent à des services fonctionnant sous Windows, et qui ne sont généralement pas des serveurs ouverts à l'Internet.

Les rejets sur le port 22/tcp (*ssh*) sont faibles en proportion. Toutefois, ils sont généralement caractéristiques de machines compromises. L'un des rejets constatés provenait d'une machine dans une direction départementale

port	pourcentage
445/tcp	41,44
135/tcp	20,39
137/udp	11,42
80/tcp	5,58
2745/tcp	4,47
139/tcp	4,12
1434/udp	2,40
3127/tcp	1,93
1433/tcp	1,82
6129/tcp	1,34
4899/tcp	0,97
5000/tcp	0,96
5554/tcp	0,85
21/tcp	0,68
9898/tcp	0,57
1080/tcp	0,55
443/tcp	0,20
3389/tcp	0,09
3128/tcp	0,08
23/tcp	0,07
10080/tcp	0,02
6112/tcp	0,02
22/tcp	0,01
111/tcp	0,01

TAB. 2 – *Paquets rejetés*

d'un ministère. Cette machine est considérée comme compromise. Elle présentait par ailleurs des dysfonctionnements dans certains de ces services. Tout dysfonctionnement d'un service est généralement caractéristique d'une compromission de la machine. En effet, lors des intrusions informatiques, certains binaires sont souvent remplacés par d'autres fichiers ayant des fonctionnalités différentes, ce qui a des conséquences sur le bon fonctionnement du système.

3 Retour d'expérience sur les incidents

3.1 Enregistreur de clavier

Le CERTA a récemment communiqué au sujet du ver *Korgo*. Une analyse de ce ver a été faite par un CERT partenaire du CERTA. Ce ver peut être associé à un logiciel malveillant qui enregistre toutes les frappes au clavier avant de les transmettre à un site WEB accessible à tous ceux qui en connaissent l'URL. Les analystes de ce logiciel enregistreur de clavier pensent qu'il est destiné essentiellement à recueillir des données bancaires comme un numéro de carte par exemple.

Grâce à la collaboration entre CERT, le CERTA a pu identifier quelques adresses IP au travers desquelles des machines infectées sont connues du site de recueil des données capturées. Ces adresses peuvent être différentes de l'adresse IP de la machine réellement infectée en raison de l'architecture du réseau (routeur, serveur mandataire, pare-feu avec de la NAT, ...).

Avec l'aide de la chaîne fonctionnelle de sécurité des ministères, il a été possible d'identifier avec certitude des machines contaminées. L'analyse de ces machines montre quelques similitudes qui seront décrites ultérieurement.

Quelques enseignements sur l'architecture de sécurité peuvent cependant être tirés de cet incident :

Dans le cas d'une machine compromise avec l'enregistreur de clavier, les données capturées ont traversé avec l'aide du protocole HTTP deux serveurs mandataires, un pare-feu et un filtre d'URL avant d'être enregistrées et rendues accessibles sur un site WEB public. N'importe qui, connaissant l'URL où sont stockées les données peut lire toutes les saisies au clavier. Dans notre cas particulier la machine compromise servait à saisir des informations nominatives dans une base de données. Cette base de données était accessible au travers d'une interface WEB sur l'Internet protégée par un nom et un mot de passe. Quelque soit la qualité du mot de passe, dans la mesure où il peut être lu par n'importe qui, la protection des informations de la base de données devient inefficace.

Les données bancaires sont protégées habituellement par le protocole HTTPS. Quelque soit la qualité de ce protocole pour la protection des flux de données, il est important de constater qu'il est rendu inutile lorsque tout ce qui est saisi au clavier est envoyé sur un site distant tiers.

Nous vous invitons à garder à l'esprit cet incident lorsque vous concevez de nouvelles applications en ligne. La sécurité d'un système d'information dépend de l'élément le plus faible : ici le poste de travail qui, malgré de nombreux dispositifs de filtrage, laisse fuir des informations. N'oubliez pas que dans le cas des informations nominatives vous avez l'obligation légale d'assurer la sécurité relative à la confidentialité de ces données.

3.2 Bonnes vacances

L'été approche. C'est l'occasion de prendre quelques vacances bien méritées après un début d'année chargé en activités liées à la sécurité des systèmes d'information et aux virus informatiques en particulier.

Chaque année l'été fournit une situation favorable à la prolifération des vers et autres virus. On a pu le constater par exemple avec CodeRed au début du mois d'août 2001 ou avec Blaster en été 2003. Par ailleurs des vulnérabilités majeures peuvent être publiées pendant l'été, comme par exemple Cisco en juillet 2003, qui a publié un avis touchant tous ses produits.

Le problème posé par les virus de l'été vient plus de la capacité de réaction amoindrie par la concomitance des congés de ceux qui habituellement administrent les mises à jour et la sécurité du parc informatique et réseau, que des caractéristiques techniques des virus qui sortent à cette période.

C'est pourquoi le CERTA vous rappelle de bien préparer l'été en :

- appliquant les correctifs de sécurité ;
- désignant une équipe capable de prendre les premières mesures en cas de problèmes.

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.

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

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-001 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-120
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-120
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-150
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-120
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-001
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-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
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–

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

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.

Liste des tableaux

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

Gestion détaillée du document

15 juin 2004 version initiale.