

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°2005-21

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-2005-ACT-021>

Gestion du document

Référence	CERTA-2005-ACT-021
Titre	Bulletin d'actualité N°2005-21
Date de la première version	27 mai 2005
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 Activité en cours

1.1 Ports observés

Le tableau 3 montre les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 12 et le 19 mai 2005.

1.2 Activité sur le port 22/tcp

Nous constatons depuis quelques semaines une activité soutenue sur le port 22/tcp. Ce trafic correspond à une tentative d'exploitation de mots de passe triviaux pour se connecter sur des comptes connus, tels que root, guest, test, mais aussi sur des comptes correspondant à des prénoms (Patrick, Alan, etc). Cette activité avait fait l'objet d'un article dans le bulletin d'actualité CERTA-2005-ACT-014.

Il est extrêmement important d'utiliser des mots de passe forts, et de restreindre les accès SSH à certains comptes, et certaines adresses IP si possible. Nous vous rappelons que le CERTA a récemment publié la note d'information CERTA-2005-INF-001 sur les mots de passe, disponible à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html>

1.3 Incident traité

Un de nos correspondants nous a informés de la compromission de 35 machines sur ses réseaux. Les machines étaient infectées par le ver MyToB. Ce ver a la particularité d'installer un cheval de Troie qui effectue des

connexions sur un serveur irc. Dès la connexion établie, le cheval de Troie se signale dans un canal de discussion, et ensuite se met en attente d'instructions telles que lancer un déni de service par exemple. Une analyse approfondie de ce cheval de Troie est actuellement menée par le CERTA.

Recommandation :

Pour déterminer si des machines de votre réseau sont infectés par MyTob, il faut vérifier au niveau du pare-feu s'il y a des connexions vers la machine `irc.blackcarder.net` (sur le port 6667/tcp notamment). C'est d'ailleurs de cette façon que les 35 machines infectées ont été découvertes.

1.4 Analyse d'un flux inconnu

Un de nos correspondants nous a contactés après avoir vu une connexion établie entre son pare-feu et une machine située à l'étranger sur le port 6000/tcp.

Le CERTA a analysé ce trafic inconnu avec l'administrateur du pare-feu. Ce travail en commun a permis de découvrir qu'il s'agissait d'une mise à jour effectuée par le pare-feu (Astaro Secure Linux). A la suite d'un contact avec le revendeur, nous avons ainsi appris que ce pare-feu se mettait régulièrement à jour en se connectant aux adresses IP 65.118.228.2, 212.126.210.198, 195.127.173.135, et 195.127.173.136 sur le port 6000/tcp.

Nous vous rappelons que le CERTA peut vous assister dans l'analyse de vos journaux. N'hésitez donc pas à nous contacter en cas de difficulté à interpréter des journaux.

2 Rappel des avis et mises à jour émis

Durant la période du 16 au 20 mai 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-164 : Multiples vulnérabilités dans tcpdump
- CERTA-2005-AVI-165 : Vulnérabilité dans Squid
- CERTA-2005-AVI-166 : Multiples vulnérabilités dans PostgreSQL
- CERTA-2005-AVI-167 : Multiples vulnérabilités dans CVS

Pendant cette même période, les mises à jour suivantes ont été publiées :

- CERTA-2005-AVI-141-001 : Vulnérabilité dans kdelibs
(ajout des références aux bulletins de sécurité Gentoo, Debian, Mandriva et Fedora)
- CERTA-2005-AVI-148-001 : Multiples vulnérabilités des produits Mozilla
(ajout des références CVE et des bulletins de sécurité Mandriva, RedHat et SuSE)

3 Actions suggérées

3.1 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. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

3.2 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.

3.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

3.4 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 certaines 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 correct d'un pare-feu.

3.5 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.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

3.6 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 inexplicables 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.

4 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.

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	4
3	Paquets rejetés	5

Gestion détaillée du document

27 mai 2005 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2004-AVI-066 CERTA-2004-AVI-064 CERTA-2003-AVI-132
22	TCP	SSH	–	CERTA-2003-AVI-152
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	–	CERTA-2005-AVI-133
42	TCP	WINS	–	CERTA-2004-AVI-384
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
139/tcp	20,15
1026/udp	16,93
1433/tcp	16,50
137/udp	9,07
1027/udp	7,36
445/tcp	6,91
4899/tcp	4,08
80/tcp	3,23
15118/tcp	3,06
1434/udp	2,58
5000/tcp	1,50
2745/tcp	1,08
6129/tcp	1,05
9898/tcp	0,93
5554/tcp	0,92
42/tcp	0,87
23/tcp	0,67
22/tcp	0,60
1080/tcp	0,47
25/tcp	0,42
3306/tcp	0,30
443/tcp	0,22
11768/tcp	0,18
1023/tcp	0,15
2100/tcp	0,15
111/tcp	0,15
3127/tcp	0,13
21/tcp	0,13
3128/tcp	0,08
6101/tcp	0,07
3389/tcp	0,05
135/tcp	0,02

TAB. 3: Paquets rejetés