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 septembre 2005
N° CERTA-2005-ACT-036

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-36

Gestion du document

Référence	CERTA-2005-ACT-036
Titre	Bulletin d'actualité n° 2005-36
Date de la première version	09 septembre 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 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 01 et le 08 septembre 2005.

1.2 Incidents traités

Le CERTA traite actuellement un cas de compromissions massives. Au moins 80 machines sous linux sont compromises, toutes par l'exploitation d'un mot de passe trivial pour un compte ne disposant pas de privilèges élevés. L'outil utilisé par le pirate pour découvrir ces mots de passe repose sur un fichier contenant plus de 70000 noms de compte et plus de 80000 mots de passe différents.

Le pirate se connecte donc sur les machines avec un compte non privilégié découvert avec l'outil décrit ci-dessus, puis élève ses droits sur le système, probablement en exploitant une faille du noyau. Il installe ensuite un `rootkit` (ensemble d'outils dont le but est de camoufler le piratage), un `sniffer` réseau (outil permettant de récupérer les informations transitant « en clair » sur le réseau local, ce qui inclut notamment les identifiants de compte et les mots de passe), et des outils permettant de compromettre des serveurs web via une faille de `AWstats.pl` (voir avis CERTA-2005-AVI-035). Enfin, un robot qui se connecte automatiquement sur un serveur `irc` a été retrouvé.

Recommandation :

Cet incident montre que les failles permettant l'élévation de privilèges ne sont pas à négliger : elles sont parfois exploitées, en combinaison d'une autre vulnérabilité, afin d'obtenir les droits de l'administrateur sur une machine. La première étape repose encore une fois sur l'exploitation d'un mot de passe faible.

Il est recommandé aux administrateurs d'appliquer tous les correctifs affectant leurs systèmes d'exploitation, et d'utiliser de temps en temps des outils pour vérifier la robustesse des mots de passe.

2 Rappel des avis et mises à jour émis

Durant la période du 29 août au 02 septembre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-322 : Vulnérabilité dans les produits Adobe Acrobat
- CERTA-2005-AVI-323 : Vulnérabilité dans Cisco Intrusion Prevention System
- CERTA-2005-AVI-324 : Vulnérabilité sur Novell Netware
- CERTA-2005-AVI-325 : Vulnérabilité des clients DHCP sous Solaris 10
- CERTA-2005-AVI-326 : Vulnérabilité de DameWare Mini Remote Control
- CERTA-2005-AVI-327 : Vulnérabilité de l'interface utilisateur du Firewall de Microsoft Windows

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

- CERTA-2004-AVI-308-003 : Vulnérabilité dans OpenSSH
  (ajout référence au bulletin de sécurité ASA-2005-167 de Avaya)
- CERTA-2004-AVI-385-002 : Vulnérabilité dans OpenSSL
  (ajout de la référence au bulletin de sécurité Avaya)
- CERTA-2005-AVI-183-006 : Vulnérabiltés dans gzip
  ajout de la référence au bulletin de sécurité Avaya ASA-2005-172)
- CERTA-2005-AVI-317-001 : Vulnérabilité dans Cisco Clean Access
  (ajout de la référence au bulletin de sécurité Cisco #66147)
- CERTA-2005-AVI-284-002 : Multiples vulnérabilités dans le logiciel Ethereal
  (ajout des références aux bulletins de sécurité SuSE, Red Hat, Mandriva et Avaya)
- CERTA-2005-AVI-292-002 : Vulnérabilité de l'éditeur Vim
  (ajout des références aux bulletins de sécurité RedHat, Mandriva et Avaya)
- CERTA-2005-AVI-307-002 : Vulnérabilité de AWStats
  (ajout du bulletin de sécurité Gentoo et SuSE)
- CERTA-2005-AVI-311-002 : Multiples vulnérabilités dans Gaim
  (ajout des bulletins de sécurité Mandriva, Gentoo et SuSE)
- CERTA-2005-AVI-322-001 : Vulnérabilité dans les produits Adobe Acrobat
  (version ajout de la référence au bulletin de sécurité du CERTA)

3 Actions suggérées

3.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

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 immédiate. 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 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.

3.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

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.

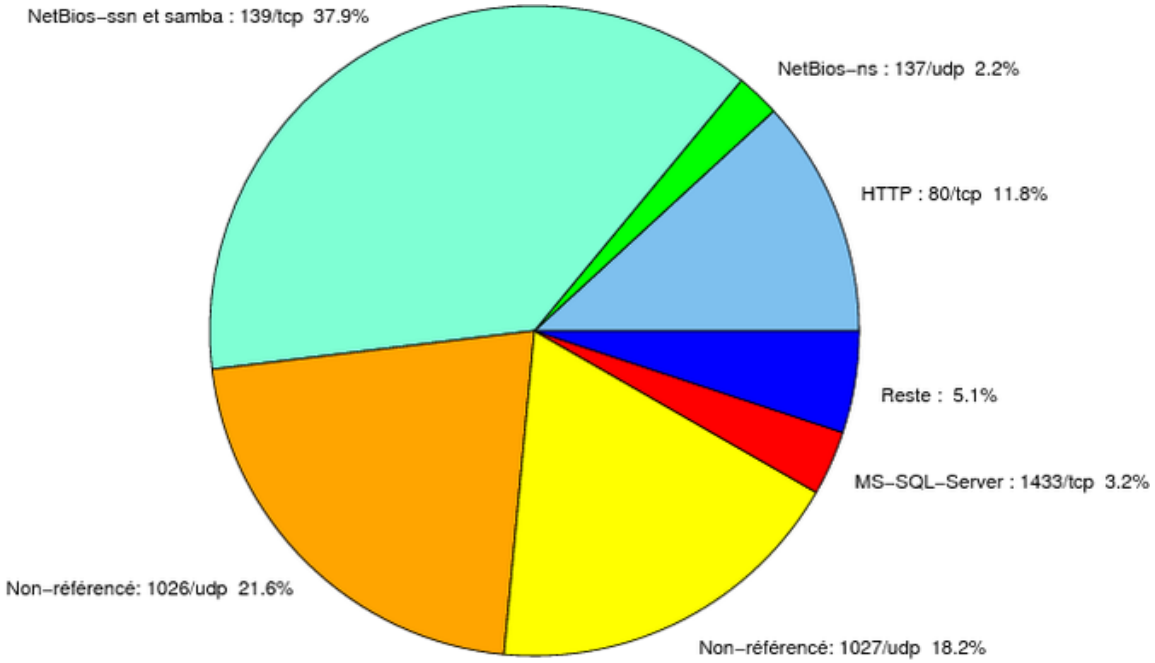

FIG. 1: Répartition relative des ports pour la semaine du 01.09.2005 au 08.09.2005

Liste des tableaux

Gestion détaillée du document

09 septembre 2005 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CER
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070 6101	TCP TCP	BrightStor ARCserve/Enterprise Backup Veritas Backup Exec	– –	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–

port	pourcentage
139/tcp	37,9
1026/udp	21,61
1027/udp	18,21
80/tcp	11,81
1433/tcp	3,21
137/udp	2,18
1434/udp	0,81
143/tcp	0,73
6101/tcp	0,57
4899/tcp	0,52
1080/tcp	0,4
15118/tcp	0,33
22/tcp	0,2
6129/tcp	0,15
9898/tcp	0,12
5554/tcp	0,1
3306/tcp	0,09
443/tcp	0,08
3127/tcp	0,07
2745/tcp	0,06
10000/tcp	0,05
21/tcp	0,04
5000/tcp	0,03
11768/tcp	0,02

TAB. 3: Paquets rejetés