Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 juin 2009
N° CERTA-2009-ACT-025

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-25

Gestion du document

Référence	CERTA-2009-ACT-025
Titre	Bulletin d'actualité 2009-25
Date de la première version	19 juin 2009
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.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-025.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-025/

1 Procédures de départ d'un employé

Lorsqu'un employé quitte sa fonction, il doit généralement suivre un certain nombre de procédures comme la remise du matériel informatique utilisé, la résiliation des badges d'accès, etc. Toutefois, d'un point de vue informatique, ces procédures sont souvent incomplètes, ce qui peut avoir des conséquences en termes de sécurité. Nous passons ici en revue quelques étapes qui ne sont pas toujours correctement traitées.

1.1 Nettoyer les comptes de messagerie

Les comptes de messagerie constituent un enjeu important. En effet, il est fréquent qu'après le départ d'un employé, celui-ci continue de recevoir des messages professionnels. Si le compte n'a pas été invalidé, son correspondant peut croire que le message est correctement parvenu à son destinataire, et attendre une réponse qui ne viendra jamais. Par ailleurs, la boîte aux lettres d'un compte qui n'a pas été désactivé peut continuer à grossir, jusqu'à atteindre les limites de quota (si elles existent), ce qui encombre inutilement le disque dur (et dans les pires cas, cela peut engendrer une saturation du disque).

Il est important également de bien se désinscrire de toute liste de diffusion, afin d'éviter des envois inutiles de messages.

1.2 Changer les mots de passe

Le changement des mots de passe est une étape souvent oubliée ou ignorée après un départ de personnel. En effet, il est possible que l'employé ait partagé un compte commun de connexion avec des collègues, éventuellement sur un service disponible via l'Internet. Dans ce cas, cet employé, bien que ne travaillant plus pour sa société, est susceptible d'avoir des accès à ce compte. La presse a récemment relaté des cas de personnes licenciées qui ont exploité des accès ainsi oubliés pour se venger.

1.3 Supprimer les éventuels accès distants

Par nécessité de service, certaines entreprises mettent en place des accès distants pour leurs employés (par exemple dans le cas du télétravail depuis un domicile). Il est évidemment important de penser à fermer de tels accès, ainsi que de passer en revue les règles de filtrage (par exemple, retirer les autorisations de mettre à jour un site Web).

2 Serveurs Web et capacité de délivrer un service

2.1 Actualité

Un outil a récemment fait l'objet de plusieurs discussions sur l'Internet. Il s'agit d'un code qui perturbe le service Web rendu par un serveur.

Il existe bien entendu plusieurs façons de tirer profit des ressources limitées d'un serveur. Ce dernier présente un ensemble de paramètres d'ajustement mais qui s'avèrent être dans certains cas peu ou pas satisfaisants dans le cadre d'attaques en déni de service.

A valeur d'exemple, Il existe plusieurs manières envisageables de perturber le serveur, comme :

- Envoyer une information `content-length` dans l'en-tête dont la valeur indiquée est plus importante que les données effectivement envoyées ;
- demander de conserver la connexion en ajoutant régulièrement un `keep-alive` dans l'en-tête ;
- etc.

Des outils de tests de performance et de charge Apache (branche 1.x) peuvent également être utilisés de bonne ou mauvaise manière. Ils fonctionnent de la même façon.

Plus simplement, plusieurs centaines d'ouvertures de sessions TCP adressées au serveur peuvent également affecter son fonctionnement. Elles ne seront pas nécessairement visibles dans les journaux de l'application, si aucune requête HTTP n'est émise.

Le lecteur comprendra ici que les manières de submerger un serveur Web sont multiples. Nous décrivons dans la section suivante la méthode proposée qui fait l'objet de l'outil en question. Mais les bonnes pratiques et la gestion du risque restent plus généraux que pour cette seule méthode.

2.2 Principe

L'attaque tire profit d'une fonctionnalité protocolaire concernant des requêtes HTTP incomplètes. Elle consiste simplement à laisser un client envoyer toutes les informations de sa requête (GET/POST/etc.) en plusieurs trames.

Selon les configurations des serveurs Web, ceux-ci peuvent entreprendre de réserver des ressources substancielles dès la réception de la première trame de requête incomplète en perspective de sa réponse, tout en attendant les données manquantes.

L'attaque consiste ainsi à créer plusieurs sessions HTTP en parallèle et envoyer pour chacune d'elles une requête incomplète. Puis, dans un délai de l'ordre de quelques minutes, ces requêtes sont maintenues par des données additionnelles mais sans jamais compléter totalement l'en-tête de la requête.

Tout service Web qui gère les sessions incomplètes de la manière précédente sont potentiellement vulnérables, sans autre contrôle adapté. C'est le cas des serveurs Apache (versions 1.x et 2.x) et de la passerelle Squid. Microsoft IIS 6.0 et 7.0 ne sont pas affectés.

L'attaque ne permet cependant pas d'usurper simplement des adresses IP émettrices arbitraires, car les sessions TCP sont établies.

2.3 Recommandations

2.3.1 Filtrage HTTP

Certains articles signalent que l'outil a une « signature » particulière. En effet, son en-tête HTTP est de la forme :

```
GET / HTTP/1.1
Host: leServeurCible
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0;
            .NET CLR 1.1.4322; .NET CLR 2.0.503l3; .NET CLR 3.0.4506.2152;
            .NET CLR 3.5.30729; MSOffice 12)
Content-Length: 42
X-a: b
```

L'information `" X-a: b"` est celle envoyée à intervalles de temps réguliers pour prévenir le serveur que l'en-tête continue d'être émis. Elle ne veut rien dire de particulier. Il n'y a pas de ligne vide précisant la fin de l'en-tête (code retour de fin ligne - CRLF - seul).

Il est donc possible de chercher et couper toute connexion de machine ayant cette caractéristique. Néanmoins cette méthode ne reste adaptée qu'à cette variante de l'outil et il est très simple de la modifier (simple édition d'un script). Il en va de même pour la valeur du `User-Agent`.

2.3.2 Filtrage réseau

Autre caractéristique de l'outil : il cherche à ouvrir plusieurs sessions HTTP (*sockets*) en parallèle. Cela se caractérise donc dans un intervalle de temps très court par de multiples demandes de connexion TCP adressées au serveur. Un pare-feu en amont peut, de manière préventive, limiter le nombre de sessions TCP ouvertes par adresse IP distincte. Cette approche peut avoir des effets de bord sur du trafic légitime (translation d'adresse et partage d'une même adresse IP publique par plusieurs machines, ou utilisation d'une passerelle inverse (*reverse proxy*) qui serait la seule adresse IP vue par le serveur).

2.3.3 Configuration du serveur Web

Pour Apache, il est, par exemple, possible dans la configuration d'ajuster les valeurs suivantes :

- MaxClients : il s'agit du nombre maximal de connexions (sessions) gérées simultanément ;
- MaxRequestsPerChild : il s'agit du nombre maximal de requêtes qu'un processus peut traiter (*child server process*) ;
- ThreadsPerChild : il s'agit du nombre de *threads* par processus ;
- MaxSpareThreads : il s'agit du nombre maximal de *threads* inactifs ;
- LimitRequestFields : il s'agit du nombre maximal de champs acceptés dans l'en-tête envoyé par un client.
- etc.

Les paramètres *MaxClients* et *MaxRequestsPerChild* ne changent pas grand chose à la réussite de l'attaque. *LimitRequestFields* peut lui réduire la durée d'une tentative mais l'attaquant a toujours la possibilité de recommencer l'opération depuis le départ.

Plusieurs suggestions ont été faites et sont effectivement envisageables, comme la notion d'un minuteur dynamique (*dynamic timer*) pour la durée des sessions dont la valeur est choisie en fonction de la charge réelle du serveur.

Des modules tiers à ajouter au serveur peuvent aider à se défendre dans le cadre de cette attaque. Il faut cependant être très vigilant avec ces codes qui sont pas nécessairement audités proprement, qui peuvent prendre des initiatives (activations de règles de pare-feu) et qui peuvent être eux même directement ciblés. Leur usage n'est donc pas conseillé.

2.3.4 Architecture

La meilleure prévention contre cette catégorie d'attaques consiste à renforcer l'architecture Web. Il est possible de considérer l'utilisation :

- d'un pare-feu applicatif qui transfère uniquement les requêtes complètes au serveur ;

– d'un serveur frontal permettant d'équilibrer les charges (*load balancers*) ;
– de serveurs de cache frontaux.

2.4 Conclusion

Cette attaque est intéressante mais s'ajoute aux autres méthodes existantes et relativement semblables pour perturber un service Web en ligne.

Il n'existe pas de mesure « universelle » permettant de se protéger des attaques en déni de service. En revanche, il est important d'estimer le risque et de préparer préventivement un certain nombre de mesures dans le cas où certaines tentatives seraient tentées contre un site.

2.5 Documentation

– Documentation W3C, "Hypertext Transfer Protocol Version 1.x" :
http://www.w3.org/Protocols/HTTP/
– Documentation W3C, RFC 2616, "Hypertext Transfer Protocol – HTTP/1.1" :
http://www.w3.org/Protocols/rfc2616/rfc2616-sec4.html

3 WebCam et systèmes embarqués

3.1 Présentation

Les *webcams* sont devenues une option courante sur les ordinateurs personnels récents, en particulier sur les ordinateurs portables où ils sont, le plus souvent, intégrés dans l'entourage de l'écran. Le CERTA a déjà pu aborder les risques associés à ce type de technologie en particulier dans un contexte de messagerie instantanée (CERTA-2008-ACT-46, CERTA-2007-ACT-38).

Sont apparues plus récemment, des *webcams* non plus asservies à un ordinateur mais pourvues d'un système embarqué complet les rendant totalement autonomes. Il existe ainsi des modèles disposant d'une pile `IP` complète leur permettant de communiquer via un réseau filaire ou bien en `Wi-Fi`. Sur certaines autres, on peut également trouver des fonctions d'enregistrement local.

Ces nombreuses fonctionnalités ne peuvent être mises en œuvre que par l'intermédiaire d'un système d'exploitation embarqué capable, par exemple, d'enregistrer sur un support numérique type `SD-CARD` ou bien encore d'envoyer des flux vidéo et audio sur `IP` vers une centrale d'enregistrement. Or, comme tout système, il peut être vulnérable et constituer un point d'entrée privilégié pour certains attaquants car facilement identifiable et rarement mis à jour.

3.2 Recommandations

Avec ce type d'équipement, il est donc indispensable d'appliquer une politique de sécurité rigoureuse, comme tout ordinateur ou autre système du réseau :

– Adapter la politique de filtrage ;
– appliquer de façon systématique les mises à jour éventuelles ;
– disposer si cela est possible d'une politique de journalisation prenant en compte ce type d'équipement.

4 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 11 et le 18 juin 2009.

5 Liens utiles

– Mémento sur les virus :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
– Note d'information du CERTA sur l'acquisition de correctifs :
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/

– Note d'information du CERTA sur les systèmes obsolètes :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
– Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
– Note d'information du CERTA sur les mots de passe :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
– Note d'information sur la terminologie d'usage au CERTA :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
– Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/
– Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
http://www.auscert.org.au/render.html?it=1935
– Note d'information du CERTA sur les risques associés aux clés USB :
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/
– Note d'information du CERTA sur les outils d'indexation et de recherche :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
– Note d'information du CERTA sur la gestion des noms de domaine :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
– Note d'information du CERTA sur le bon usage de PHP :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

6 Rappel des avis émis

Dans la période du 12 au 19 juin 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-231 : Multiples vulnérabilités dans Google Chrome
– CERTA-2009-AVI-232 : Vulnérabilité dans Ruby
– CERTA-2009-AVI-233 : Mulitples vulnérabilités dans Mozilla Firefox
– CERTA-2009-AVI-234 : Vulnérabilité dans IBM WebSphere MQ
– CERTA-2009-AVI-235 : Vulnérabilité dans IBM OS/400
– CERTA-2009-AVI-236 : Multiples vulnérabilités de l'antivirus Norman
– CERTA-2009-AVI-237 : Multiples vulnérabilités dans CA ARCserve Backup
– CERTA-2009-AVI-238 : Vulnérabilité dans CA Service Desk
– CERTA-2009-AVI-239 : Vulnérabilité Java de Mac OS X
– CERTA-2009-AVI-240 : Vulnérabilité dans F-Secure Messaging Security Gateway

Durant la même période, les trois avis suivants ont été mis à jour :

– CERTA-2008-AVI-556-002 : Vulnérabilité dans GnuTLS
(ajout des références aux bulletins de sécurité Fedora et Sun)
– CERTA-2009-AVI-073-002 : Vulnérabilité dans libpng
(ajout des références aux bulletins de sécurité VMware et)
– CERTA-2009-AVI-120-002 : Multiples vulnérabilités dans OpenSSL
(ajout des références aux bulletins de sécurité Mandriva, HP et Suse)

7 Actions suggérées

7.1 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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme 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.

7.2 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 oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

7.3 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.

7.4 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.

7.5 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 CERTA peut vous aider dans ce travail d'analyse.

7.6 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.

7.7 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.ssi.gouv.fr/fr/formation/

8 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.

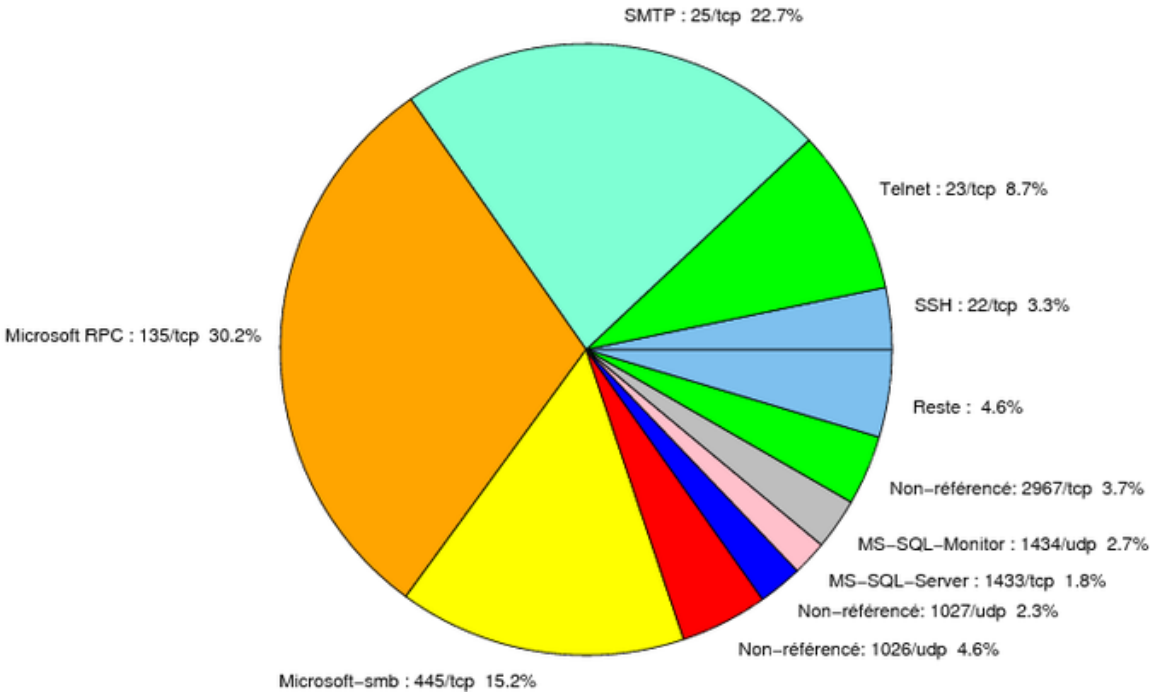

FIG. 1: Répartition relative des ports pour la semaine du 11 au 18 juin 2009

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 http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER 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 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	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 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
106	TCP	MailSite Email Server	–	– 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 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 http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	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 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 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	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
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
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
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
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	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
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	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	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
135/tcp	30.23
25/tcp	22.72
445/tcp	15.2
23/tcp	8.8
1026/udp	4.61
2967/tcp	3.69
22/tcp	3.26
1434/udp	2.7
1027/udp	2.33
1433/tcp	1.84
80/tcp	0.98
4899/tcp	0.67
3128/tcp	0.61
3306/tcp	0.49
21/tcp	0.36
3389/tcp	0.3
137/udp	0.24
143/tcp	0.12
111/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

19 juin 2009 version initiale.