Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 février 2010
N° CERTA-2010-ACT-005

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-05

Gestion du document

Référence	CERTA-2010-ACT-005
Titre	Bulletin d'actualité 2010-05
Date de la première version	05 février 2010
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-2010-ACT-005.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-2010-ACT-005/

1 Vulnérabilité dans Internet Explorer

1.1 Résumé

Cette semaine une vulnérabilité non corrigée affectant `Internet Explorer` a été dévoilée à la conférence *BlackHat DC*. Cette vulnérabilité n'a pas fait l'objet d'une alerte CERTA vu l'impact limité et l'absence d'exploitation connue.

1.2 Description

Si un utilisateur navigue sur un site spécialement malformé, il est alors possible pour l'attaquant de récupérer des fichiers présents sur le disque de la machine utilisateur.

Il y a cependant plusieurs facteurs atténuants :

– L'attaquant doit connaître le chemin complet des fichiers (pas de possibilité de lister les fichiers du disque). Les fichiers accessibles dépendent des droits de l'utilisateur et de leur état d'utilisation (impossibilité de copier un fichier ouvert par le système ou une application) ;

– `Microsoft` propose plusieurs contournements dans son bulletin de sécurité #980088, dont un paquet `FixIt` redistribuable utilisant le `Network Protocol Lockdown` permet de restreindre l'accès au protocole *file://* dans la zone Internet.
Le mode protégé d'`Internet Explorer` sous `Windows Vista` et `Windows 7` limite aussi l'accès aux fichiers du disque.

Le CERTA recommande l'utilisation du contournement `FixIt` proposé par l'éditeur si le navigateur n'utilise pas le mode protégé.

2 Documentation

– Bulletin de sécurité Microsoft #980088 du 03 février 2010 :
http://www.microsoft.com/technet/security/advisory/980088.mspx

3 Le ciblage comportemental sur Internet

3.1 Un profilage dissimulé

Si Internet est une source d'informations intarissable, il est aussi parfois montré du doigt pour son manque de respect de la vie privée. Les technologies utilisées par ce réseau sont variées et complexes. Il est donc souvent difficile pour un non-technicien de comprendre tous les flux d'information qu'il véhicule, d'autant que le sujet reste très vaste. On va s'intéresser ici plus particulièrement au profilage commercial des personnes sur le Web, appelé aussi « ciblage comportemental ».

Aujourd'hui, les habitués du Web ont globalement conscience que l'ère de la simple recherche d'information sur Internet est largement dépassée. Le présent est aux réseaux sociaux et aux contenus créés par les internautes : le Web social. Il faut savoir que les informations mises à disposition sur Internet peuvent être conservées pendant une période illimitée. Il ne sera pas question ici des réseaux professionnels, sociaux, et autres sites de rencontres, où le profilage commercial relève de l'évidence même.

L'objet de cet article porte sur des méthodes plus dissimulées de ciblage commercial. Par exemple, si vous envoyez un courriel à un ami, avec votre *Webmail* préféré, précisant votre envie de partir en vacances, il est tout à fait probable que lors de votre prochaine visite sur un site quelconque, des publicités pour des agences de voyage soient affichées.

3.2 Les cookies HTTP

Un *cookie*, ou fichier de session, est un fichier d'une taille inférieure à 4 Ko qui circule entre le navigateur et le serveur Web à chaque échange de données. Il est créé pour un nom de domaine unique, et ne peut être envoyé qu'à un serveur répondant à ce nom de domaine. Il est utilisé pour des objectifs variés : maintenir une session sur un site Web ou l'état d'un panier d'achats sur une application de commerce en ligne, observer le comportement des utilisateurs sur le site (recherches effectuées, ordre de navigation), etc.

Beaucoup de pages Web vont chercher leurs contenus à des adresses différentes. Ainsi, il est tout à fait possible que l'adresse *http://site1.tld* aille chercher une partie de son contenu à l'adresse *http://site2.tld*. Il est donc possible d'échanger des *cookies* avec le domaine *site2.tld* alors que l'adresse apparaissant dans le navigateur est *http://site1.tld*.

Toujours à l'adresse *http://site1.tld*, si la connexion vers l'adresse *http://site2.tld* est effectuée par une référence à un code *JavaScript* situé à l'adresse *http://x3.y3.z3/script.js*, on échangera toujours des *cookies* avec le domaine *site2.tld* mais, sans même le voir apparaître dans le code source de la page téléchargée. On ne verra que la référence au code *JavaScript*. Ces *cookies*, au domaine ne correspondant pas à l'adresse qui apparaît dans le navigateur, sont communément appelés « *cookies* tierce partie ».

3.3 Les méthodes de profilage par cookies HTTP

La plupart des régies publicitaires présentes sur l'Internet utilisent les *cookies* tierce partie. Mais comment fonctionnent-ils ? En voici un exemple : un webmestre désire gagner un peu d'argent et veut donc placer de la publicité sur son site Web. Il contacte alors une régie publicitaire, par exemple *http://www.exemplefictifdepub.tld*, qui lui fournit une référence vers un code *JavaScript* à placer sur ses pages Web. Ce code *JavaScript* va charger des bannières publicitaires venant d'autres domaines, et fabriquer un *cookie* ayant pour domaine *exemplefictifdepub.tld*.

De plus, le code *JavaScript* va activer un robot qui va lire et qualifier le contenu de la page Web. Ainsi, à chaque fois qu'un utilisateur viendra sur cette page, il recevra un *cookie* sauvegardant, d'une manière ou d'une autre, le type de contenu de la page.

Imaginons maintenant que la société *http://www.exemplefictifdepub.tld* ait pignon sur rue, et que beaucoup de sites Web de la planète utilisent ses services. Chaque internaute a donc de bonnes chances d'avoir un *cookie* avec pour le domaine *exemplefictifdepub.tld* et répertoriant l'ensemble des types de contenu qu'il est allé visiter. À chaque fois que l'internaute va sur un site qui utilise ce code *JavaScript*, ce *cookie* est mis à jour en ajoutant un nouveau contenu. Et comme ce code *JavaScript* est aussi celui qui va chercher les publicités à afficher, il choisit les publicités qui correspondent aux types de contenu visités. Un profil commercial de l'utilisateur est donc établi de façon tout à fait transparente, alors que l'internaute n'a fait que quelques recherches sur l'Internet.

L'exemple des *Webmail* de l'introduction prend ici tout son sens. Certains *Webmails* référencent également ce type de code *JavaScript* qui se charge également de qualifier les courriels de l'internaute. A chaque fois que l'internaute ouvre un de ses messages, ce dernier est automatiquement lu et qualifié par un robot. Et ce pour pouvoir lui offrir de la publicité correspondant au contenu de ses courriels.

3.4 Eviter le profilage commercial par cookie HTTP

La grande majorité de ces techniques utilisent *JavaScript*, la désactivation du moteur *JavaScript* dans le navigateur les rend de fait inefficaces. Les navigateurs modernes proposent également une option réservée aux *cookies* tierce partie, qui propose de les rejeter systématiquement.

Enfin, l'association *NAI* (`http://www.networkadvertising.org`) regroupant 35 régies publicitaires, dont les 10 plus importantes des États-Unis, imposent des règles de bonne conduite à ses adhérents, notamment la possibilité de refuser ces *cookies* publicitaires en utilisant les *cookies OPT-OUT*. Ces derniers rejettent l'ajout d'informations de contenu pour un domaine. De nombreux modules de navigateur Web permettent aussi l'ajout et le maintien de ces *cookies* sur le système de l'utilisateur. Sans oublier la possibilité de créer ces *cookies OPT-OUT* à l'adresse `http://www.networkadvertising.org/managing/opt_out.asp`. Cette page permet aussi de savoir quels *cookies* tierce partie sont actuellement installés sur le système.

Les techniques présentées dans la section précédente sont très répandues sur le Web. Elles ne posent pas de problèmes de sécurité immédiats, mais peuvent s'avérer gênantes pour certaines personnes et organisations. Il est donc déconseillé à une organisation qui a des besoins de sécurité et de confidentialité importants d'utiliser des sites ou *Webmails* forçant ce genre de pratique.

3.5 Les journaux

Le *cookie* n'est pas le seul mécanisme de profilage. L'immense majorité des sites ont des journaux de serveurs Web pouvant tracer un utilisateur de manière très fine, parfois plus qu'avec l'aide de *cookies*. À la différence des *cookies* tierce partie, ces journaux n'informent que le gestionnaire du site sur lequel l'internaute se connecte.

4 Mise en œuvre de DNSSEC

Depuis cette semaine le serveur `DNS` racine `L.root-servers.net` (`199.7.83.42`) met en œuvre la signature d'un certain nombre d'informations dans ses réponses par le biais de `DNSSEC`. Comme le prévoit ce protocole, le serveur géré par l'`ICANN` inclut donc dans ses réponses des éléments de signatures des enregistrements fournis. Ce déploiement progressif devrait se poursuivre jusqu'en juillet.

Ainsi, il est désormais possible pour les administrateurs de `DNS` de tester leur future configuration `DNSSEC` mais également de vérifier la compatibilité de leurs équipements de filtrage avec la `RFC 2671` qui précise qu'il est désormais possible pour des serveurs `DNS` d'émettre des paquets `UDP` de taille supérieure à `512 octets`. En effet, historiquement, si une réponse dépassait cette limite, le serveur utilisait `TCP`.

Désormais, ce n'est plus le cas et l'utilisation de `DNSSEC` engendrera quasi systématiquement des paquets de taille supérieure à `512 octets`.

4.1 Recommandation

Si l'on envisage un déploiement de `DNSSEC`, il est indispensable de vérifier que les équipements de filtrage et routage en amont du serveur `DNS` sont capables de supporter et « router » des paquets `UDP` supérieurs à 512 octets. Le serveur `L.root-servers.net` est un bon moyen de tester cet état de fait.

4.2 Documentation

- Note d'information « Du bon usage du DNS » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002/
- RFC 2671 :
  http://www.ietf.org/rfc/rfc2671.txt

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=1937
- 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 29 janvier au 04 février 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-033 : Vulnérabilités dans Sun Java System Web Server
- CERTA-2010-AVI-034 : Multiples vulnérabilités dans Cisco Unified MeetingPlace
- CERTA-2010-AVI-035 : Multiples vulnérabilités dans Wireshark
- CERTA-2010-AVI-036 : Vulnérabilité dans HP OpenView Storage Data Protector
- CERTA-2010-AVI-037 : Vulnérabilité des produits Hitachi
- CERTA-2010-AVI-038 : Vulnérabilité dans Samba
- CERTA-2010-AVI-039 : Vulnérabilité dans IBM DataPower
- CERTA-2010-AVI-040 : Vulnérabilité dans Symantec Altiris Notification Server
- CERTA-2010-AVI-042 : Vulnérabilité dans Cisco Secure Desktop
- CERTA-2010-AVI-043 : Multiples vulnérabilités dans les produits VMware
- CERTA-2010-AVI-044 : Vulnérabilité dans BIND avec DNSSEC
- CERTA-2010-AVI-045 : Vulnérabilités dans Squid
- CERTA-2010-AVI-046 : Multiples vulnérabilités dans Apple iPhone OS
- CERTA-2010-AVI-047 : Vulnérabilité dans Adobe ColdFusion
- CERTA-2010-AVI-048 : Vulnérabilité dans Citrix XenServer

– CERTA-2010-AVI-049 : Vulnérabilité dans OpenVMS RMS
– CERTA-2010-AVI-050 : Vulnérabilité dans Fetchmail
– CERTA-2010-AVI-051 : Vulnérabilité dans Asterisk
– CERTA-2010-AVI-052 : Vulnérabilité dans Trend Micro OfficeScan
– CERTA-2010-AVI-053 : Vulnérabilité dans Novell NetStorage
– CERTA-2010-AVI-054 : Vulnérabilité dans Apache HTTP Server
– CERTA-2010-AVI-055 : Vulnérabilité dans lighttpd

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

– CERTA-2010-AVI-041-001 : Multiples vulnérabilités dans Apache Tomcat (précision de la section Solution du document)

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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique67.html

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.

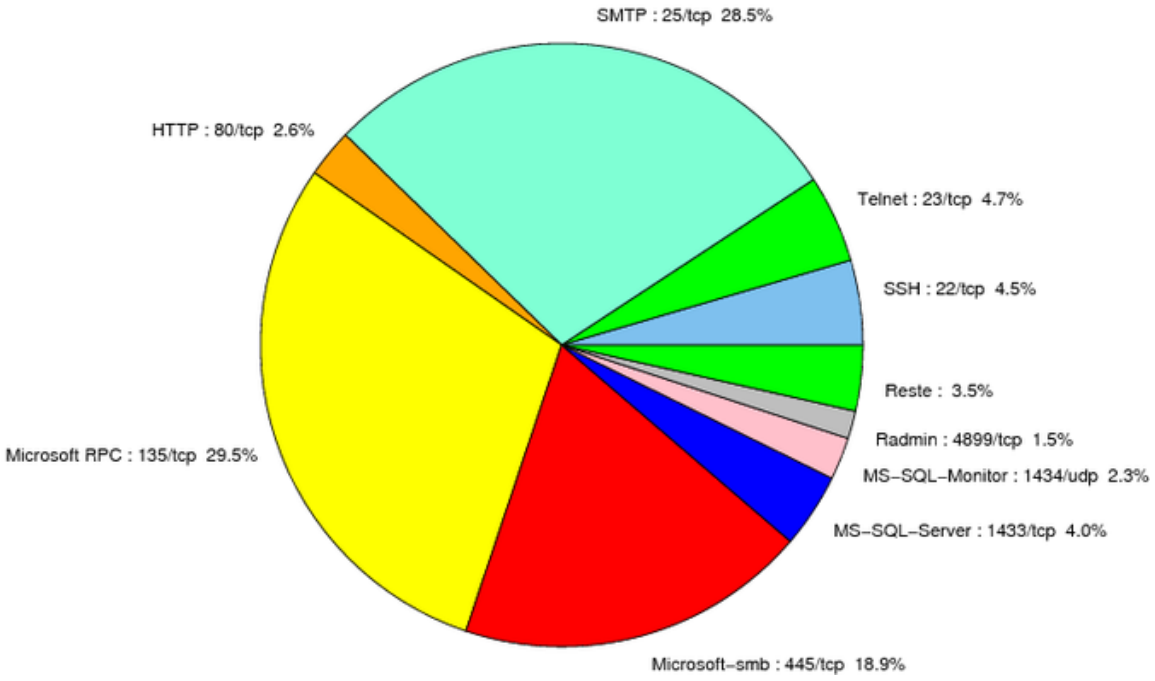

FIG. 1: Répartition relative des ports pour la semaine du 29 janvier au 04 février 2010

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	29.52
25/tcp	28.5
445/tcp	18.87
23/tcp	4.77
22/tcp	4.54
1433/tcp	3.99
80/tcp	3.28
1434/udp	2.27
4899/tcp	1.48
3389/tcp	0.86
2967/tcp	0.7
1080/tcp	0.62
21/tcp	0.54
3128/tcp	0.46
3306/tcp	0.39

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

05 février 2010 version initiale.