Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 octobre 2009
N° CERTA-2009-ACT-042

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-42

Gestion du document

Référence	CERTA-2009-ACT-042
Titre	Bulletin d'actualité 2009-42
Date de la première version	16 octobre 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-042.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-042/

1 Courriels malveillants : le spectre des prétextes est large

Le CERTA constate une grande variété des motifs utilisés dans les courriels malveillants pour inciter les internautes à télécharger des programmes nocifs ou à divulguer leurs informations personnelles.

1.1 Fausses mises à jour Microsoft

Des courriels prétendant provenir de services de *Microsoft* incitent le destinataire à télécharger une mise à jour. Ces courriels, rédigés dans un français de bonne qualité, circulent depuis le 12 octobre, *patch Tuesday*. Le programme chargé est en fait un cheval de Troie.

La fraude utilise les ressorts classiques :

– le sentiment d'insécurité, si une mise à jour n'est pas appliquée ;
– un nom d'expéditeur apparent faux, comme `message@microsoft.fr` ;
– un logo *Microsoft Windows* ;
– un exécutable qui s'appelle *WindowsUpdate*, mot-clef vraisemblable pour le profane ;
– un lien masqué dans un message en HTML.

Les éditeurs de logiciels n'envoyent pas de notification de mises à jour à des destinataires qui ne se sont pas abonnés aux services de notication. *Microsoft* a réagi dans un communiqué :

http://www.microsoft.com/france/protect/yourself/phishing/windowsupdate.mspx

Le CERTA recommande :

- de lire les courriels en texte brut, ce qui permet de débusquer les liens masqués ;
- de vérifier l'origine du courriel par affichage de l'en-tête complet et analyse du chemin parcouru ;
- de ne pas cliquer sur un lien dans un courriel, mais de le composer soi-même dans la barre d'adresse du navigateur ;
- de ne télécharger de mises à jour, si elles ne sont pas automatiques, que depuis le site de l'éditeur ou des miroirs officiels.

1.2 Fausses mises à jour d'un serveur ou de la messagerie

Plusieurs campagnes concernent les mises à jour de serveurs (sans précision) ou de boîtes aux lettres électroniques. Le courriel prévient d'une mise à jour planifiée d'un serveur, d'une mise à jour de sécurité pour une boîte aux lettres dont l'adresse est dans le sujet du message ou d'une nouvelle configuration pour l'accès par *Outlook Web Access*. L'expéditeur prétendu est un service support de même domaine de messagerie que le destinataire. Cela vise à mettre ce dernier en confiance.

Ainsi le CERTA a reçu des courriels semblant émaner de `system-administrator@certa.ssi.gouv.fr`. Des liens malveillants contenus dans ces courriels conduisent à télécharger le programme malveillant `Zeus`.

Les ressorts sont les mêmes que précédement, avec une déclinaison légèrement différente :

- sentiment d'insécurité ou d'urgence ;
- domaine de l'expéditeur apparent connu (c'est celui du destinataire) ;
- lien caché dans un courriel en HTML.

Les recommandations sont donc toujours identiques.

Quelques articles sur le sujet :

- http://blogs.orange-business.com/securite/2009/10/attaque-de-phishing-visant-les-bals-dialoleanecom.html
- http://www.zdnet.fr/blogs/securite-cybercriminalite/mise-a-jour-attaque-ciblee-via-le-malware-zeus-39709361.htm

1.3 Faux remboursements

Aux campagnes qui ont concerné des prétendus remboursements de la part du Trésor public ou des caisses d'allocation familiales, s'ajoutent maintenant les campagnes qui laissent croire à des remboursements par les fournisseurs d'accès Internet. Le but est de capturer des données bancaires, comme lors des filoutages classiques. Pour attirer les victimes, ce n'est plus la simple mise à jour de données sur le site de la banque qui sert de prétexte, mais l'espoir de recevoir une somme d'argent.

Il est d'une prudence élémentaire d'aller vérifier sur le site officiel de l'organisme censé rembourser, en composant soi-même l'adresse (sans cliquer dans le courriel douteux), les modalités de remboursement ou de le contacter par téléphone ou par courriel.

2 Retour sur les avis de la semaine

2.1 Avis Microsoft

Cette semaine a vu la publication de 13 bulletins de sécurité par `Microsoft`. Ces bulletins apportent de nombreux correctifs. Parmi les vulnérabilités corrigées, deux fournissent une solution à des problèmes ayant levé une alerte CERTA :

vulnérabilité SMBv2 : l'alerte CERTA-2009-ALE-016 est corrigée par le bulletin MS09-050 (avis CERTA numéro CERTA-2009-AVI-443) ;

vulnérabilité du serveur FTP de Microsoft IIS : l'alerte CERTA-2009-ALE-015 est corrigée par le bulletin MS09-053 (avis CERTA numéro CERTA-2009-AVI-433).

De plus, une modification de la `CryptoAPI` de `Microsoft Windows` permet de corriger le problème dû à l'utilisation d'un caractère nul dans les certificats SSL (vulnérabilité décrite dans le bulletin d'actualité du CERTA numéro CERTA-2009-ACT-041).

Le CERTA recommande d'appliquer au plus vite ces correctifs.

2.2 Avis Adobe Reader et Adobe Acrobat

Le 09 octobre 2009, le CERTA a publié une alerte concernant une vulnérabilité découverte dans les logiciels Adobe Reader et Adobe Acrobat.

Cette vulnérabilité vient d'être corrigée par Adobe, via leur bulletin de sécurité numéro apsb09-15 du 13 octobre 2009 (cf. avis de sécurité du CERTA numéro CERTA-2009-AVI-445).

Le CERTA recommande d'appliquer au plus vite ce correctif.

3 La politique de sécurité du contenu contre l'injection de code indirecte

Cette semaine la fondation *Mozilla* a mis en ligne un site de démonstration de sa nouvelle « protection » CSP (*Content Security Policy*) permettant de lutter, entre autres, contre les attaques en XSS (*Cross Site Scripting*) ou injection de code indirecte.

3.1 Rappel sur les XSS

Une injection de code indirecte simple consiste à exécuter du code dans le navigateur d'un internaute, et cela dans le contexte d'un site tiers. Par exemple, une personne malveillante peut utiliser une variable affichée et non validée d'un site pour introduire un script qui sera exécuté dans le navigateur de la victime et cela dans le contexte du site hebergeant la variable.

3.2 Principes du CSP de la fondation *Mozilla*

L'idée principale est de contrôler l'origine et la forme des scripts exécutés, et plus généralement des contenus de la page. Pour cela le développeur du site doit définir une *politique de sécurité du contenu* qui est passée dans l'entête HTTP (X-Content-Security-Policy). Il peut, entre autres, y préciser les origines autorisées et les formes de code acceptées. Par exemple, la politique par défaut n'autorise pas l'appel à eval() mais cela peut être changé à l'aide de l'option eval-script. S'il ne veut autoriser que les contenus en provenance de son domaine, l'entête contiendra X-Content-Security-Policy: allow self. Il doit donc modifier les entêtes retournés et s'assurer que le code respecte la politique qu'il a définie.

Dans le même temps, le navigateur utilisé doit être compatible pour interpréter ces informations et contrôler que la page respecte bien la politique définie. À ce jour, seule une version spécialisée de firefox proposée par la fondation *Mozilla* est disponible. Si un des deux protagonistes n'est pas compatible, la navigation continue classiquement.

Pour lutter contre les attaques du type XSS, le CERTA recommande aux développeurs d'appliquer les bonnes pratiques de sécurité et aux internautes de n'activer l'interprétation des scripts qu'au besoin, même sur les sites fréquement visités.

3.3 Documentation

- Présentation du CSP :
  https://wiki.mozilla.org/Security/CSP
- Spécifications du CSP :
  https://wiki.mozilla.org/Security/CSP/Spec
- Page de démonstration :
  http://people.mozilla.org/~bsterne/content-security-policy/demo.cgi

4 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/

5 Rappel des avis émis

Dans la période du 09 au 16 octobre 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-430 : Vulnérabilité des systèmes IBM AIX et VIOS
– CERTA-2009-AVI-431 : Vulnérabilités dans CA Anti-Virus
– CERTA-2009-AVI-432 : Vulnérabilité dans Microsoft Windows Media Player
– CERTA-2009-AVI-433 : Vulnérabilités du serveur FTP de Microsoft IIS
– CERTA-2009-AVI-434 : Multiples vulnérabilités de Microsoft Internet Explorer
– CERTA-2009-AVI-435 : Vulnérabilité des composants ActiveX utilisant la bibliothèque ATL
– CERTA-2009-AVI-436 : Vulnérabilités dans Windows CryptoAPI
– CERTA-2009-AVI-437 : Vulnérabilité dans le service d'indexation de Windows
– CERTA-2009-AVI-438 : Vulnérabilité dans Microsoft Windows
– CERTA-2009-AVI-439 : Vulnérabilité dans Local Security Authority Subsystem Service
– CERTA-2009-AVI-440 : Multiples vulnérabilités dans Microsoft Active Template Library ActiveX controls pour Microsoft Office
– CERTA-2009-AVI-441 : Multiples vulnérabilités dans Microsoft NET Common Language Runtime
– CERTA-2009-AVI-442 : Multiples vulnérabilités des produits Microsoft utilisant GDI+
– CERTA-2009-AVI-443 : Multiples vulnérabilités de SMBv2 dans Microsoft Windows
– CERTA-2009-AVI-444 : Multiples vulnérabilités dans Microsoft Windows Media Runtime
– CERTA-2009-AVI-445 : Multiples vulnérabilités dans Adobe Reader et Acrobat

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

– CERTA-2009-AVI-363-001 : Vulnérabilité de wget (ajout des références aux bulletins de sécurité Debian et Ubuntu, et de la référence CVE)
– CERTA-2009-AVI-380-001 : Multiples vulnérabilités dans PostgreSQL (ajout des références aux bulletins de sécurité Debian, et RedHat et des références CVE)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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/

7 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.

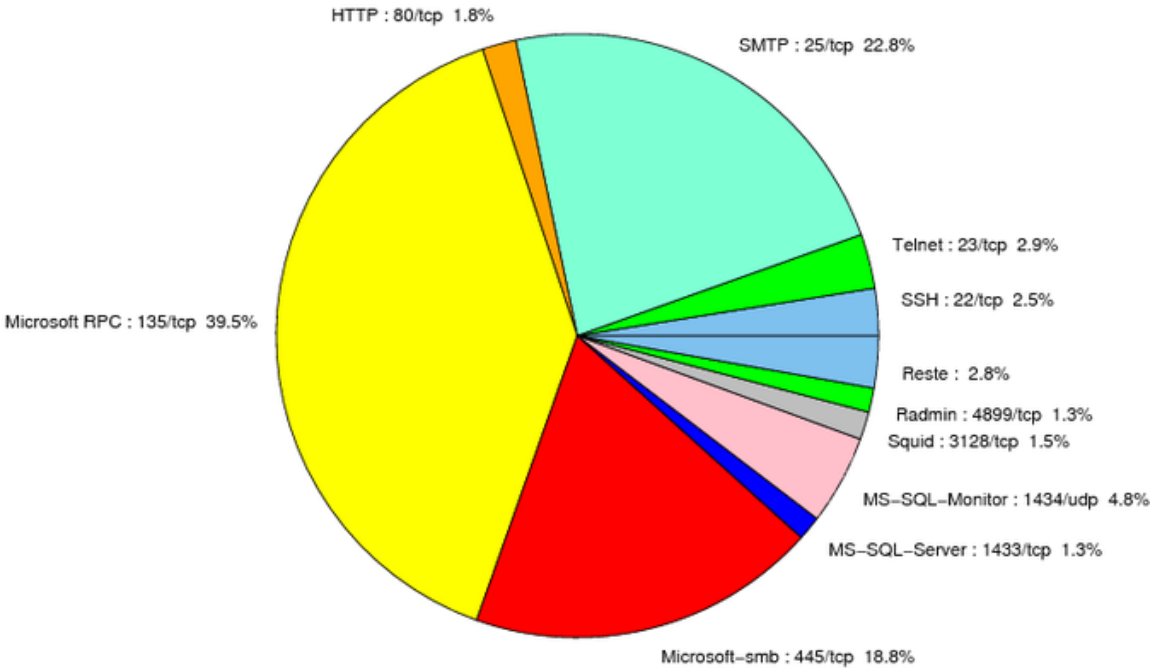

FIG. 1: Répartition relative des ports pour la semaine du 08 au 15 octobre 2009

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	39.48
25/tcp	22.84
445/tcp	18.77
1434/udp	4.78
23/tcp	2.97
22/tcp	2.52
80/tcp	1.94
3128/tcp	1.48
4899/tcp	1.29
21/tcp	0.77
2967/tcp	0.64
3389/tcp	0.58
1080/tcp	0.51
143/tcp	0.19
2100/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

16 octobre 2009 version initiale.