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 octobre 2009
N° CERTA-2009-ACT-041

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2009-41**

| | |
|---|---|
| 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-2009-ACT-041` |

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2009-ACT-041 |
| Titre | Bulletin d'actualité 2009-41 |
| Date de la première version | 09 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-041.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-041/

## 1 Vulnérabilité dans Adobe Reader et Adobe Acrobat

Des codes malveillants exploitant la vulnérabilité annoncée par `Adobe` hier sont disponibles sur internet. Pour rappel, cette vulnérabilité concerne les dernières versions d'`Adobe Reader` et `Adobe Acrobat` (9.1.3, 8.1.6 et 7.1.3) et les versions antérieures, pour toutes les plateformes. Elle ne nécessite pas que l'interprétation du `JavaScript` soit activée bien que cela en facilite l'exploitation. Les personnes l'ayant désactivé auparavant ne sont donc pas protégées.

L'éditeur a annoncé qu'un correctif serait disponible le 13 octobre 2009.

En attendant, le CERTA recommande :

- d'utiliser des logiciels alternatifs ;
- de laisser inactif l'interprétation des *JavaScript* ;
- d'activer le DEP (Data Execution Protection) sur Windows Vista pour tous les exécutables du système (l'activation de cette fonctionnalité peut avoir des effets indésirables sur certaines applications) ;
- de convertir les fichiers suspects au format *PostScript* puis de nouveau au format PDF sur une machine sas ;
- de n'ouvrir que des fichiers provenant de sources qualifiées de sûres.

### Documentation

- Bulletin de sécurité Adobe APSB09-15 du 08 octobre 2009 :
  http://www.adobe.com/support/security/bulletins/apsb09-15.html
- Alerte CERTA du 9 octobre 2009, CERTA-2009-ALE-018 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-018
- Référence CVE CVE-2009-3459 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3459

## 2 Incidents de la semaine

Cette semaine, le CERTA a traité, parmi de très nombreux autres cas de filoutage, deux cas sortant de l'ordinaire. En effet, ils touchaient non pas des banques ou des systèmes de paiement en ligne mais deux institutions françaises n'ayant normalement pas trait à du commerce directement. Pourtant sur chacune des fausses pages utilisées pour l'hameçonnage, on trouvait des formulaires demandant les coordonnées bancaires des victimes. C'est d'ailleurs ce qui a interpelé certains destinataires des messages frauduleux car le niveau de réalisme à la fois des messages mais aussi des sites était assez élevé (reproduction de la charte graphique, pas de faute d'orthographe). Ces sites étaient évidemment hébergés à l'étranger.

### Recommandations :

Comme cela a été rappelé sur les sites légitimes des institutions concernées mais aussi dans le passé par de nombreuses institutions bancaires, il est impossible que soit demandé par courriel, le changement en ligne des informations de connexion. Tout message électronique ou site invitant à cette démarche doit être considéré comme hautement suspect. Enfin, il est tout à fait possible d'utiliser les outils proposés dans les navigateurs pour contrôler la légitimité d'un site.

## 3 Vulnérabilité dans la bibliothèque Microsoft CryptoAPI : Certificat SSL Wildcard

Afin de sécuriser l'échange de données sensibles sur le Web, le protocole HTTPS est utilisé. Il est en fait le protocole HTTP couplé avec SSL (Secure Socket Layer). Le principe est le suivant :

- le navigateur Web récupère le certificat *X509* du domaine auquel il se connecte. Une clé publique de chiffrement fait partie des informations présentes dans ce certificat ;
- le navigateur Web s'assure que le certificat est de confiance, c'est-à-dire qu'il est signé par une autorité tiers elle-même de confiance ;
- le navigateur Web utilise la clé publique contenue dans le certificat pour chiffrer la clé secrète qui sera utilisée pour sécuriser la communication avec le domaine visité.

La sécurité du protocole SSL repose sur la confiance que l'on accorde aux certificats, ces derniers servent à se protéger contre des attaques du type « homme au milieu ».

Cependant, un certificat SSL valide et signé a été publié pour usurper n'importe quel site HTTPS légitime dès lors que la victime utilise un navigateur vulnérable à l'insertion du caractère NULL au sein du champ *Common Name* d'un certificat *X509*.

L'exploitation se base sur le fait que les caractères à droite du caractère NULL sont ignorés par la bibliothèque *CryptoAPI* de `Microsoft`. Par conséquent, tous les navigateurs utilisant la *CryptoAPI* sont vulnérables à cette attaque. Ces navigateurs sont Internet Explorer, Google Chrome, et Apple Safari, dans leur version pour Windows.

Cette vulnérabilité critique fut révélée lors de la conférence Black Hat fin Juin 2009, un correctif est toujours en attente de la part de `Microsoft`. Quant à `Mozilla`, Firefox a été corrigé quelques jours après la découverte de la vulnérabilité.

Au vu de l'importance de cette vulnérabilité, le CERTA recommande fortement l'utilisation d'un navigateur non vulnérable sous Windows dans l'attente du correctif.

### Documentation

- Avis CERTA CERTA-2009-AVI-306 : Vulnérabilités dans Firefox
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-306/

# 4 Des codes malveillants de plus en plus intelligents

## 4.1 Introduction

Dans le domaine de la sécurité informatique, comme dans beaucoup d'autres domaines, on assiste à une course entre les agresseurs et ceux chargés de les contrer. La sphère des codes malveillants n'échappe pas à cette règle : les attaquants sont sans arrêt à la recherche de nouvelles techniques permettant de retarder et décourager les personnes chargées d'analyser les codes.

## 4.2 L'exemple des Bankers

Les *Bankers* forment à eux seuls une famille de code malveillant chargés de piéger un utilisateur accédant à son compte en banque en ligne. Initialement, ces codes se chargeaient uniquement de récupérer les identifiants de connexion et de les transmettre à un serveur contrôlé par l'attaquant. Ainsi, ce dernier pouvait à loisir accéder au compte en ligne de la victime et transférer illégalement de l'argent vers son propre compte ou vers le compte d'une mule. Cependant, les nouveaux modes de sécurisation des sites de banque en ligne (ajout d'aléa, mot de passe à rentrer en cliquant avec la souris, jeton, etc.) ont rendu quasiment inefficace ce mode de fonctionnement.

Les codes ont donc dû évoluer. Au lieu de voler les identifiants de connexion, ils ont été programmés pour s'injecter dans l'espace mémoire du navigateur afin d'utiliser une connexion ouverte de manière légitime pour passer des commandes bancaires (un virement de compte à compte, par exemple). Tout était automatique et préconfiguré suivant un fichier, embarqué lors de l'infection ou récupéré après coup auprès d'un serveur de contrôle. En revanche, comme aucun contrôle n'était effectué sur les sommes versées, il se pouvait que, le compte ne disposant pas de la somme, le versement soit bloqué et la supercherie découverte rapidement par la banque.

La dernière génération de code malveillant bancaire est beaucoup plus sophistiquée. Au lieu de procéder à un virement hasardeux, le code injecté dans le navigateur vérifie l'état du compte de la victime et ne verse qu'une sous-partie de la somme vers des comptes tirés aléatoirement parmi toutes les mules disponible. Ainsi, les virements frauduleux ne provoquent aucune erreur et le versement est validé. Les enquêteurs et les banques devront donc trouver de nouvelles parades pour arriver à différencier un virement anormal d'un virement légitime.

## 4.3 Contournement des environnements de test

Le perfectionnement des codes malveillants ne s'arrête pas à l'amélioration de la finalité. En effet, pour qu'un code soit efficace, il faut qu'il ne soit pas découvert, ou plutôt qu'il soit découvert après le plus de temps possible.

Un attaquant jugera donc indispensable de retarder l'analyse de son code. Pour cela, plusieurs techniques sont mises en œuvre : chiffrement, détection de machines virtuelles, détection de débogueurs, protection contre les anti-virus, obscurcissement de code, etc. Toutes ces techniques mises bout à bout peuvent mettre en défaut une large majorité d'outils de protection et retardent de manière significative l'analyse par un expert.

## 4.4 Rappel des bonnes pratiques

Pour se prévenir des codes malveillants, il est indispensable de suivre certaines bonnes pratiques :

**comportement utilisateur** Le comportement de l'utilisateur constitue certainement la pierre angulaire de la lutte contre les codes malveillants, à plusieurs titres. En prévention, l'utilisateur peut limiter les risques d'infection en prenant garde aux éléments extérieurs reçus (clefs USB, mails, etc.) et en n'utilisant que ce qui lui est strictement nécessaire et adressé. En réaction, pour limiter la fuite d'information, il ne faut traiter des données sensibles (données bancaires, données métier, etc.) qu'à partir d'un environnement dont on est strictement certain de la sécurité.

**mises à jour** Quelques virus se reproduisent en utilisant des failles logicielles plutôt que la naïveté de certains utilisateurs. Dans une très grande majorité, les vulnérabilités utilisées sont corrigées par les éditeurs. L'application des correctifs constituent donc un premier rempart efficace.

**outils de sécurité** Un antivirus, comme n'importe quel autre équipement ou logiciel de sécurité, représente un appui important pour se prémunir du tout venant. En revanche, il convient de garder à l'esprit que ces outils ne constituent pas, loin s'en faut, une protection efficace à 100%. Des techniques mettant en défaut les antivirus existent et sont utilisées.

En cas de doute, il convient de se retourner vers les personnes adéquates (RSSI, CERT, etc.) afin de limiter l'infection et/ou la perte ou l'utilisation de données sensibles.

# 5 PluginCheck

Dans le bulletin d'actualité CERTA-2009-ACT-037 du 11 septembre 2009 a été évoquée l'initiative de `Mozilla`, après mise à jour du navigateur, de présenter une page indiquant la nécessité de mettre à jour le *plugin Flash* si celui-ci était vulnérable.

Depuis peu, la fondation propose un nouveau service permettant de vérifier l'état de mise à jour d'un nombre importants de *plugins* installés sur le navigateur. Ceci se fait sur une page web dédiée nécessitant l'activation de *JavaScript*. Parmi les modules complémentaires supportés, on peut citer notamment *Flash*, *Acrobat*, *Java*, *Windows Media Player*, *QuickTime*, etc. Pour chacun, le site est censé indiquer les cas suivants :

- module inconnu ;
- module à jour ;
- module potentiellement vulnérable (version inconnue) ;
- module vulnérable ;
- module vulnérable à une faille non corrigée.

Dans les premiers cas, un lien vers le site de l'éditeur est affiché pour mettre à jour le module. Lorsqu'il n'y a pas de correctif, un bouton pour désactiver le module est présent.

Le projet étant nouveau, il se peut que la détection ne fonctionne pas dans tous les cas de figure. On ne peut toutefois que saluer cette bonne initiative de `Mozilla`. Les modules complémentaires sont en effet un vecteur d'infection de plus en plus utilisé par des attaquants car moins souvent mis à jour par rapport aux systèmes d'exploitation ou applications.

## 5.1 Documentation

- PluginCheck :
  http://www-trunk-stage.mozilla.com/en-US/plugincheck/
- Article du bloc-notes de Mozilla :
  http://blog.mozilla.com/webdev/2009/10/02/upyourplug-needs-your-help/
- Bulletin d'actualité CERTA-2009-ACT-037 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-037.pdf

# 6 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/

# 7 Rappel des avis émis

Dans la période du 02 au 08 octobre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-418 : Vulnérabilité dans IBM Tivoli Composite Application Manager pour WebSphere
- CERTA-2009-AVI-419 : Multiples vulnérabilités du logiciel VMware Fusion
- CERTA-2009-AVI-420 : Multiples vulnérabilités dans Samba
- CERTA-2009-AVI-421 : Vulnérabilité dans OSIsoft PI server
- CERTA-2009-AVI-422 : Vulnérabilité dans Mc Afee Email and Web Security Appliance
- CERTA-2009-AVI-423 : Multiples vulnérabilités dans Wireshark
- CERTA-2009-AVI-424 : Multiples vulnérabilités dans Apache
- CERTA-2009-AVI-425 : Multiples Vulnérabilités de FreeBSD
- CERTA-2009-AVI-426 : Vulnérabilité dans Xen
- CERTA-2009-AVI-427 : Vulnérabilité dans HP Remote Graphics software
- CERTA-2009-AVI-428 : Multiples vulnérabilités dans Kerberos sous HP-UX
- CERTA-2009-AVI-429 : Vulnérabilité dans Sun Solaris clsetup

# 8 Actions suggérées

## 8.1 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.

## 8.2 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.

## 8.3 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.

## 8.4 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.

## 8.5 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.

## 8.6 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.

## 8.7 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_rubrique63.html

# 9 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.

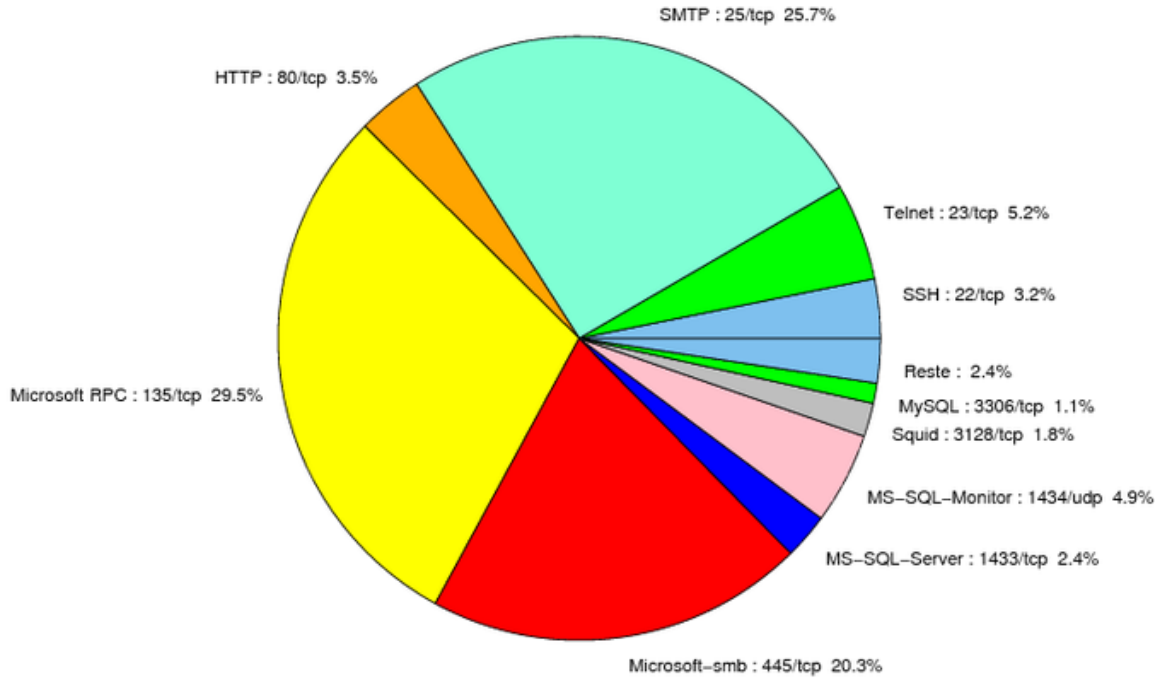


FIG. 1: Répartition relative des ports pour la semaine du 01 au 08 octobre 2009

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|---|---|---|---|---|
| 21 | TCP | FTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 23 | TCP | Telnet | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>CERTA-2007-ALE-005-001 |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 106 | TCP | MailSite Email Server | – | –<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |

| | | | | |
|---|---|---|---|---|
| | | | | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 445 | TCP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>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/CERT |
| 6101 | TCP | Veritas Backup Exec | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 6106 | TCP | Symantec Backup Exec | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 6129 | TCP | Dameware Miniremote | – | http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT |
| 6502 | TCP | CA BrightStor ARCserve Backup | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 6503 | TCP | CA BrightStor ARCserve Backup | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 6504 | TCP | CA BrightStor ARCserve Backup | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 8080 | TCP | IBM Tivoli Provisioning Manager | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 8866 | TCP | – | Porte dérobée Bagle.B | – |
| 9898 | TCP | – | Porte dérobée Dabber | – |
| 10000 | TCP | Webmin, Veritas Backup Exec | – | http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT |
| 10080 | TCP | Amanda | MyDoom | – |
| 10110 | TCP | IBM Tivoli Monitoring | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 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/CERT |
| 13701 | TCP | Veritas NetBackup | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 18264 | TCP | CheckPoint interface | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 54345 | TCP | HP Mercury | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 65535 | UDP | LANDesk Management Suite | – | http://www.certa.ssi.gouv.fr/site/CERT |

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

| port | pourcentage |
|---|---|
| 135/tcp | 29.46 |
| 25/tcp | 25.72 |
| 445/tcp | 20.38 |
| 23/tcp | 5.47 |
| 1434/udp | 4.89 |
| 80/tcp | 4.32 |
| 22/tcp | 3.17 |
| 1433/tcp | 2.44 |
| 3128/tcp | 1.8 |
| 3306/tcp | 1.08 |
| 4899/tcp | 0.72 |
| 1080/tcp | 0.57 |
| 2967/tcp | 0.5 |
| 3389/tcp | 0.07 |

TAB. 3: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**09 octobre 2009** version initiale.