Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 avril 2009
N° CERTA-2009-ACT-014

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-14

Gestion du document

Référence	CERTA-2009-ACT-014
Titre	Bulletin d'actualité 2009-14
Date de la première version	03 avril 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-014.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-014/

1 La maîtrise des filtres utilisés

Cette semaine le CERTA a été sollicité par une administration suite au blocage d'un site Internet par l'un des filtres de passerelle utilisé. Le site en question avait été catégorisé dans son intégralité comme comportant un contenu malveillant. A la suite d'une compromission certaines pages Web peuvent, en effet, être étiquetées comme malveillantes car contenant :

- des balises « *iframe* » ajoutée ;
- du code *javascript* malveillant ;
- des liens visibles ou non renvoyant vers des sites malveillants ;
- ....

Dans le cas présent, après de nombreuses analyses des pages du site, le CERTA n'a pas été en mesure d'identifier le contenu malveillant. Le CERTA a donc contacté directement la société éditrice du filtre afin d'obtenir plus de précisions sur les raisons de ce bloquage. Il s'avère que cette société avait identifié par erreur ce site comme malveillant. Suite à l'intervention du CERTA, l'accès aux pages Web du site a, de nouveau, été possible.

Cet incident doit attirer l'attention du lecteur sur le choix et la pertinence de ces outils de filtrage, notamment en consultant la politique de blocage des sites sur les aspects suivants :

- la finesse d'information fournie lors du blocage des sites ;

– le blocage total ou partiel d'un site contenant une seule page corrompu ;
– la pertinence et le processus de filtrage d'un site ;
– la possibilité de demander la changement de catégorie d'un site ;
– l'accès aux journaux du filtre ;
– la fréquence de mise à jour des bases de données des sites malveillants ;
– la possibilité de mise en liste blanche des sites de confiance ;
– ....

2 Alerte sur Microsoft PowerPoint

Le CERTA a émis l'alerte CERTA-2009-ALE-005 le 03 avril 2009 concernant une vulnérabilité non corrigée dans Microsoft PowerPoint. L'ouverture d'un document spécialement conçu par une personne malveillante peut ainsi causer l'exécution de code arbitraire. Les versions suivantes de PowerPoint sont concernées :

– Microsoft Office PowerPoint 2000 SP3 ;
– Microsoft Office PowerPoint 2002 SP3 (Office XP) ;
– Microsoft Office PowerPoint 2003 SP3 ;
– Office PowerPoint 2004 sur Mac.

Selon Microsoft, Office 2007 n'est pas affecté par cette vulnérabilité. Son utilisation, ou celle de suites bureautique alternatives telle que OpenOffice.org permet donc de se protéger totalement de cette faille.

Il est important de noter que les fichiers au nouveau format XML `pptx` ne sont pas impactés par cette vulnérabilité. Ainsi, un contournement efficace est d'utiliser l'outil MOICE (*Microsoft Office Isolated Conversion Environment*) pour convertir les fichiers du format binaire vulnérable vers le format `Office Open XML`.

Un autre contournement, plus restrictif, est d'utiliser la fonctionnalité *FileOpenBlock* offerte par Microsoft Office. Ceci permet de bloquer l'ouverture de fichiers aux formats binaires utilisés avant Office 2007.

Ainsi, pour activer cette fonctionnalité sur Office 2003, il faut positionner à 1 la valeur `BinaryFiles` de la clé suivante:

```
HKCU\Software\Microsoft\Office\11.0\PowerPoint\Security\FileOpenBlock
```

Pour désactiver cette fonctionalité, il suffit de remettre la valeur à 0. Pour rappel, il est possible de spécifier à *FileOpenBlock* un « répertoire de confiance » depuis lequel les documents au format non autorisé peuvent être ouverts. Pour plus d'informations se reporter à l'article KB922848 (cf. section Documentation).

La vulnérabilité est actuellement exploitée et il est donc vivement recommandé d'appliquer des solutions de contournement. Il est fortement conseillé de ne pas ouvrir de documents provenant de sources non sûres, mais aussi d'être vigilant même lorsqu'un document provient d'une source qui semble sûre. Enfin, l'utilisation de l'application PowerPoint avec un compte aux droits limités pourrait limiter l'impact d'une éventuelle exploitation.

2.1 Documentation

– Alerte CERTA-2009-ALE-005 du 03 avril 2009 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-004/
– Blog Technet, « New 0-day Exploits Using PowerPoint Files » :
http://blogs.technet.com/mmpc/archive/2009/04/02/new-0-day-exploits-using-powerpoint-files.aspx
– Bulletin de sécurité #969136 du 02 avril 2009 :
http://www.microsoft.com/technet/security/advisory/969136.mspx
– Article KB922848 sur FileOpenBlock :
http://support.microsoft.com/kb/922848

3 Windows XP et phase d'extension de support

3.1 Présentation

Le CERTA tenait à rappeler que selon `Microsoft`, le système d'exploitation `Windows XP` entrera dans la phase d'extension de support à compter du 14 avril 2009. Ceci signifie concrètement que dès cette date, `Microsoft` :

– rendra payant le support d'incident pour ce système ;

– ne supportera plus les correctifs logiciels non-liés à la sécurité ;
– ne prendra plus en compte les déclarations de dommage relatif à ce système ;
– ne prendra plus en compte les demandes de changements de conception ou l'ajout de nouvelles fonctionnalités.

Ceci est valable pour toutes les versions de `Windows XP` : Service Pack 2 et 3, versions 32bit ou x86_64, etc. Le système `Windows XP` étant largement déployé, il conviendra de bien prendre en compte cet état de fait.

Il est tout de même à noter que la phase d'extension de support durera, quant à elle, jusqu'au 08 avril 2014. Ainsi jusqu'à cette date au moins, `Microsoft` fournira le support des mises à jour de sécurité, le support via la base de connaissance `Microsoft`, le support via les FAQ `Microsoft` ainsi qu'un support payant pour les mises à jour non-relatives à la sécurité.

Il ne faudra pas attendre avril 2014 pour envisager une migration de parc. Cette opération est toujours un projet à part entière qui nécessite beaucoup de tests.

3.2 Références

– Information sur les différents types de support `Microsoft` :
http://support.microsoft.com/gp/lifepolicy
– Echéancier du support de `Windows XP` :
http://support.microsoft.com/lifecycle/?p1=3223

4 MS08-067 - De la prévention à la détection

4.1 Présentation générale

Appliquer le correctif MS08-067 à temps était une mesure préventive simple. Ne pas avoir appliquer cette mesure dès le mois d'octobre a pu avoir des conséquences dommageables. L'absence de mesures préventives a permis à plusieurs codes malveillants, dont Conficker/Downadup/Kido, de se propager et d'infecter un nombre important de machines.

La détection permet, quant à elle, de s'apercevoir si la politique de sécurité n'a pas été respectée. Dans le cas particulier de Conficker, plusieurs méthodes de détection de machines compromises par les variantes connues de ce code ont été rendues publiques. Voici ci-dessous le principe de certaines d'entre elles, qui peuvent éventuellement être adaptées dans le cadre d'autres scénarios. Celles présentées permettent de s'abstenir d'intervenir directement sur tous les postes d'un réseau.

4.2 Bloquer des interrogations de noms de domaine

4.2.1 Méthode

Le code malveillant modifie en mémoire les appels aux bibliothèques `dnsapi.dll` ou `dnsrslvr.dll` (selon les versions de Windows), afin d'empêcher les machines infectées de résoudre certains noms de domaine. Elles ne peuvent ainsi plus, *a priori*, communiquer avec les sites de ces domaines pour télécharger des outils de sécurité ou des mises à jour. Ce blocage ne bloque pas complètement les résolutions de noms. Une requête en ligne de commande par `nslookup` fonctionne normalement. Chaque nouvelle version de Conficker, jusqu'à maintenant, ajoute de nouveaux noms à la liste initiale.

Certaines astuces permettent de contourner ce blocage, comme par exemple arrêter la mise en cache DNS sous Windows :

```
net stop dnscache
```

Certains sites proposent eux une manière assez simple de détecter ce blocage en visualisant sur une page HTML un ensemble d'images provenant des sites Web associés aux noms de domaine bloqués. En fonction des images affichées, il est possible de vérifier qu'aucun blocage est en cours, ou bien que celui-ci est partiel (signe éventuel d'une compromission par l'une des versions de Conficker en fonction des images absentes).

Cette méthode est intéressante mais :

– elle ne permet pas de trouver les machines uniquement infectées par la première variante du ver car le blocage de résolution de noms n'est pas utilisé ;
– elle fonctionne si la machine Windows utilise bien les bibliothèques pour afficher la page, ce qui n'est pas toujours le cas dans des environnements où une passerelle Web est utilisée (cache).

4.2.2 Références

- Conficker Detection, T. Holz, 02 avril 2009 :
  http://www.honeyblog.org/junkyard/conficker/
- The H-Security, Heise Online, "Simple Conficker test for end users", 03 avril 2009 :
  http://www.h-online.com/security/Simple-Conficker-test-for-end-users–/news/112995
- Support Microsoft, « Comment faire pour désactiver la mise en cache DNS côté client dans Windows XP et Windows Server 2003, 12 octobre 2007 » :
  http://support.microsoft.com/kb/318803

4.3 Corriger de manière non officielle une vulnérabilité

4.3.1 Méthode

Le code, dans ses versions connues, applique en mémoire un pseudo-correctif de la vulnérabilité mentionnée dans le bulletin MS08-067 afin de prévenir les surinfections par d'autres codes. Le code va ainsi "*patcher*" la fonction vulnérable `NetpwPathCanonicalize()` et prendre en charge la manipulation d'arguments, dont le chemin. Un traitement particulier est effectué pour un chemin ayant une chaîne de caractères de la forme `\..\`. Le pseudo-correctif actuel retourne sous certaines conditions et pour un chemin valide un code d'erreur, ce qu'une machine saine ne fera pas.

Des outils de balayage (*scan*) ont été publiés cette semaine. Ils cherchent à vérifier si de tels comportements se produisent.

Cette méthode peut être intéressante dans certains environnements car elle permet de s'abstenir d'intervenir directement sur les postes pour chercher de possibles infections, mais :

- il s'agit d'une méthode active. Comme tout balayage et interrogation de ports, il est difficile de prévoir tous les comportements des systèmes ciblés. Certains peuvent être perturbés par de telles activités ;
- le balayage peut provoquer des remontées d'alertes par les équipements de surveillance réseaux de type IDS. Il n'est pas toujours simple de distinguer un « bon scan » d'un « scan à des fins malveillantes » ;
- le balayage ne fonctionne que dans certaines conditions et quand les machines peuvent être contactées sur leur port 445/TCP. Le balayage ne doit pas être une raison pour modifier ou s'abstenir des bonnes pratiques de filtrage et de configuration des communications entre postes Windows.

4.3.2 Références

- Article "Know Your Enemy: Containing Conficker", F. Leder, T. Werner, 30 mars 2009 :
  http://honeynet.org/papers/conficker
- D. Kaminsky, "Taming Conficker, THe Easy Way", 30 mars 2009 :
  http://www.doxpara.com/?p=1285

4.4 Communiquer sur des ports prévisibles mais non courants

4.4.1 Méthode

La dernière variante de Conficker met en place un mécanisme de pair-à-pair original pour que les machines infectées communiquent et puissent par exemple distribuer des charges utiles. Les échanges s'effectuent en s'appuyant sur deux ports TCP et deux ports UDP ouverts par le code malveillant. Pour que les machines puissent déterminer, pour une adresse IP donnée, vers quel port s'adresser, un mécanisme est utilisé. Il s'appuie sur l'adresse IP et sur le nombre de semaines écoulées entre la date actuelle et le 1er janvier 1970 (EPOCH sous Unix).

En d'autres termes, pour une adresse IP et une date données, les ports utilisés pour la communication pair-à-pair de Conficker sont prédictibles. Mais :

- ce mécanisme de choix des ports n'est valable que pour une seule variante du code ;
- tester l'ouverture des ports par des techniques de balayage présente les mêmes inconvénients que la méthode précédente.

Il faut noter que la communication pair-à-pair de la dernière variante de Conficker génère un volume important de trafic en UDP. Une inversion du ratio TCP/UDP en faveur d'UDP n'est pas un élément très probant mais doit éveiller la curiosité de l'administrateur du réseau.

4.4.2 Références

– Bloc-notes du CERT LEXSI, « Conficker.C : de peer en peer ! », F. Perigaud, 31 mars 2009 :
https://cert.lexsi.com/weblog/index.php/2009/03/31/291-confickerc-peer-en-peer

4.5 Dans tous les cas

Le lecteur aura compris à travers ces différentes astuces qu'il existe des méthodes de détection envisageables, chacune avec leurs limitations (pertinence et effets de bord). Il y a fort à parier que les futures évolutions des codes malveillants tiendront compte de ces méthodes pour se rendre plus discrets. Il n'est tout simplement pas possible et raisonnable d'appuyer toute sa sécurité sur le seul principe de détection ni sur la seule pertinence des remontées antivirales.

Par ailleurs, plusieurs personnes profitent actuellement des effets médiatiques de certains codes comme Conficker pour promouvoir de faux outils de sécurité et de désinfection afin *in fine* d'infecter également les postes. Il s'agit d'une forme de cheval de Troie.

Appliquer préventivement le correctif dès sa publication évite finalement bien des soucis…

5 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 26 mars et le 02 avril 2009.

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=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/

7 Rappel des avis émis

Dans la période du 27 mars au 03 avril 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-117 : Vulnérabilités dans phpMyAdmin

– CERTA-2009-AVI-118 : Multiples vulnérabilités dans Cisco IOS
– CERTA-2009-AVI-119 : Multiples vulnérabilités dans Java
– CERTA-2009-AVI-120 : Multiples vulnérabilités dans OpenSSL
– CERTA-2009-AVI-121 : Multiples vulnérabilités dans Mozilla Firefox
– CERTA-2009-AVI-122 : Vulnérabilité dans Bugzilla
– CERTA-2009-AVI-123 : Vulnérabilité dans les commutateurs 3Com 5500 / 5500G
– CERTA-2009-AVI-124 : Vulnérabilité dans Sun Solaris
– CERTA-2009-AVI-125 : Multiples vulnérabilités de Tivoli Storage Manager
– CERTA-2009-AVI-126 : Vulnérabilités de IBM WebSphere
– CERTA-2009-AVI-127 : Vulnérabilité de nss-ldap

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, la DCSSI dispose d'un centre de formation :

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

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.

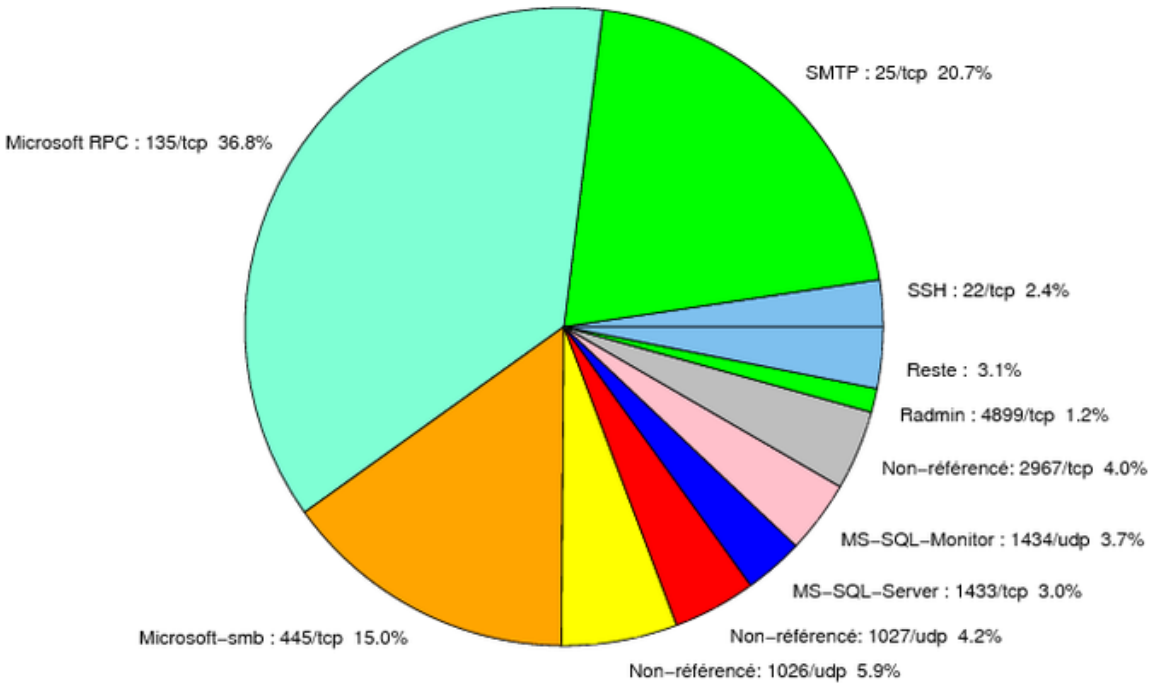

FIG. 1: Répartition relative des ports pour la semaine du 26 mars au 02 avril 2009

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	36.82
25/tcp	20.69
445/tcp	14.98
1026/udp	5.87
1027/udp	4.2
2967/tcp	4.03
1434/udp	3.68
1433/tcp	2.99
22/tcp	2.36
4899/tcp	1.21
80/tcp	0.46
3389/tcp	0.4
137/udp	0.34
3306/tcp	0.28
143/tcp	0.11

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

03 avril 2009 version initiale.