Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 décembre 2008
N° CERTA-2008-ACT-051

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-51

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-2008-ACT-051`

Gestion du document

Référence	CERTA-2008-ACT-051
Titre	Bulletin d'actualité 2008-51
Date de la première version	19 décembre 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-051.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-051/

1 Vulnérabilité Internet Explorer

Pour la seconde fois de l'année, `Microsoft` a publié un correctif hors cycle afin de combler la vulnérabilité de `Microsoft Internet Explorer` qui avait fait l'objet de l'alerte CERTA-2008-ALE-016.

1.1 Rappel des faits

Pour mémoire, cette vulnérabilité affectait plus précisement le parseur *XML* du navigateur. En imbriquant deux balises *SPAN* et en faisant appel à une source d'image contenant des caractères spécifiques, il était alors possible d'effectuer une exécution de code arbitraire à distance via une page Internet spécialement conçue. Le savoir-faire permettant l'exploitation de cette vulnérabilité avait rapidement été mis en ligne sur l'Internet.

1.2 Les risques

Différents sites Internet profitent de la visite sur certaines pages pour faire exécuter du code malveillant à l'utilisateur imprudent. Dans un premier temps, les codes se contentaient de voler des identifiants et mots de passe de jeux en ligne massivement multijoueurs.

Une seconde technique d'exploitation a vu le jour récemment. Il s'agit d'un document au format *Word* embarquant un contrôle *ActiveX* émettant à l'ouverture du document une requête vers un site Internet mettant en œuvre le code d'exploitation. Il est alors possible d'exploiter cette vulnérabilité par le biais d'un courriel ou par un autre système d'ingénierie sociale.

1.3 Les solutions

Depuis le 17 décembre 2008, le correctif est disponible sur le site de `Microsoft` ou via le téléchargement automatique des mises à jour (*Windows Update*). Le CERTA rappelle qu'il est impératif d'appliquer ce correctif.

De plus, afin de limiter les risques de compromission au travers d'un document *Word* malveillant, il est recommandé de désactiver l'exécution automatique des contrôles *ActiveX*.

1.4 Documentation

- Bulletin d'actualité CERTA-2008-ACT-050 du 12 décembre 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-050.pdf
- Alerte CERTA-2008-ALE-016 du 17 décembre 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-016
- Avis CERTA-2008-AVI-604 du 17 décembre 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-604
- Bulletin de sécurité Microsoft MS08-078 du 17 décembre 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-078.mspx

2 Les indiscrétions d'un moteur de recherche

2.1 Présentation

Les moteurs de recherche sur l'Internet ont pour vocation de délivrer à l'internaute le résultat de la recherche faite. Les recherches demandées font l'objet de statistiques. Ainsi, des moteurs de recherche sont capables de fournir par exemple des palmarès des mots-clefs les plus souvent recherchés par pays, par ville, ...

Il est moins évident d'imaginer que le choix de l'internaute dans le resultat proposé soit lui aussi conservé par le moteur de recherche. En effet la page de résultats fournie semble contenir des liens « classiques » et a priori seul le site Internet finale connaîtra, via le *Referer* du navigateur, le choix de l'internaute dans la liste des résultats.

Le moteur de recherche de *Google* ajoute une balise `onmousedown` sur chaque lien des résultats proposés. Ainsi, cela lui permet de connaître les intérêts de l'internaute mais aussi les résultats choisis lors de ses recherches. Pour des raisons inconnues, le fait de suivre ainsi les choix des internautes ne semble s'appliquer que pour les navigateurs les plus utilisés et dans leurs configurations standards. Dans sa configuration standard, un navigateur indique, par le biais de son *UserAgent*, aux sites Internet visités des informations relatives à l'ordinateur utilisé. Ces informations sont censées être utilisées pour fournir un contenu adapté à la configuration utilisée par l'internaute.

La présence du nom du navigateur (écrit de manière standard) et le *UserAgent*, déclenchent ainsi dans les pages de résultats l'apparition de la balise `onmousedown`. Une simple modification du paramètre du navigateur supprimera l'apparition de cette balise et donc le suivi du choix de l'internaute dans la page de recherche.

Pour modifier le nom du navigateur dans son *UserAgent* :

- pour *FireFox* et *Iceweasel*, ouvrir la page de configuration (about:config) et modifier le contenu du paramètre : *general.useragent.extra.firefox* ;
- pour *Internet Explorer*, modifier (ou créer) la clef de registre *Version* :

  ```
  [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Ver
  ```

- pour *Safari*, modifier le fichier com.apple.Safari.plist à l'aide du *Property List Editor* ou lancer la commande :

  ```
  defaults write com.apple.Safari CustomUserAgent "\"chaine souhaitée\""
  ```

Cette modification peut être effectuée au niveau d'une passerelle HTTP (*proxy*). Cela peut néanmoins perturber la navigation sur certains sites.

2.2 Documentation

– Note Wikipedia sur les User-Agents des navigateurs :
http://fr.wikipedia.org/wiki/User-Agent

3 Nouvelles notes d'information du CERTA

3.1 Présentation

Cette semaine, le CERTA a publié deux notes d'information :

– CERTA-2008-INF-003 : cette note aborde la problématique des injections de requêtes illégitimes par rebond (*Cross Site Request Forgery*). Il y est présenté le principe, les risques ainsi que différentes méthodes de protection ;
– CERTA-2008-INF-004 : ce document fait un retour sur l'*e-mail backscatting* ou la pollution de serveur de messagerie par des rapports de non-livraison des courriers électroniques. Il y est fait le point sur la méthode ainsi que les différents moyens de limitation de cette nuisance.

Le CERTA espère que ces documents aideront ses lecteurs à mieux appréhender ces deux problématiques.

3.2 Documentation

– Note d'information CERTA-2008-INF-003 du 17 décembre 2008 :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-003
– Note d'information CERTA-2008-INF-003 du 19 décembre 2008 :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-004

4 Sortie de SPIP 2.0

4.1 Présentation

La version 2.0 du gestionnaire de contenu `SPIP` est sortie cette semaine. D'après les auteurs du projet, ce changement majeur de version est synonyme d'une évolution importante dans l'architecture et dans les fonctionnalités offertes. Ainsi, `SPIP` dispose désormais, à l'image de ses concurrents :

– d'un système de gestions d'extensions (*plugins*) ;
– d'un support accru pour différentes bases de données ;
– de la mise en œuvre de fonctionnalités `AJAX` pour enrichir certains contenus.

Cette version venant juste d'être livrée, le CERTA manque, pour le moment, de recul sur sa fiabilité. La prudence reste donc de mise. Par ailleurs, les technologies mise en jeu au sein du projet s'approchant de celles des concurrents du même type, on pourra rester vigilant sur certains aspects dont on connaît déjà les risques associés :

– mise à jour des extensions ;
– fonctionnalités en `Javascript` pouvant poser des problèmes de sécurité ;
– variables *PHP* non-protégées laissant le champ à des attaques de type injection de code ;

4.2 Recommandation

Une des solutions évoquées précédemment par le CERTA pour rendre un système à base de `SPIP` plus sûr reste toujours d'actualité : « statifier » le contenu dynamique et ne mettre en ligne que cette version statique. Ceci est décrit dans le bulletin d'actualité CERTA-2008-ACT-044. Cette « statification » ne s'applique pas si les forums ou d'autres fonctions d'interaction avec les internautes sont utilisées.

5 Vulnérabilité critique dans Moodle

5.1 Présentation

Cette semaine, un code d'exploitation d'une vulnérabilité critique de `Moodle` a été corrigée. Pour fonctionner, il nécessite que la variable *registers_globals* soit activée (positionnée à `on`).

L'éditeur a corrigé la faille dans la dernière version, mais précise qu'il y en a d'autres, et que pour éviter leur exploitation, un mécanisme a été rajouté à l'installeur. Ce dernier vérifie que la variable *registers_global* est désactivée et bloque l'installation dans le cas contraire. Il est cependant possible de la désactiver pour l'installation et de la réactiver ensuite. Dans ce cas, il y aura un message d'alerte dans l'interface d'administration, mais le système fonctionnera normalement. Bien que la variable *registers_global* soit "dangereuse", elle est encore trop souvent activée, et la limitation imposée lors de l'installation de `Moodle` étant facilement contournable, il est à craindre d'autres compromissions.

Le CERTA recommande aux administrateurs de désactiver cette variable, et aux développeurs de faire attention à la provenance, à l'initialisation et au contenu des variables dans les scripts PHP.

5.2 Documentation

- Site de `Moodle` :
  http://www.moodle.org
- Avis de sécurité Moodle CERTA-2008-AVI-608 du 19 décembre 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-608/index.html

6 Windows Vista et le Wi-Fi

6.1 Présentation

Windows Vista offre nativement plus de possibilités d'accès à la pile IEEE 802.11 que son prédécesseur Windows XP. Microsoft a en effet développé une interface relativement complète, la NDIS 6 (*Network Driver Interface Specification*). Cette dernière offre des caractéristiques intéressantes pour les développeurs de produits aussi bien que pour les développeurs de codes malveillants. Les codes peuvent interagir avec les APIs du pilote *Native WiFi - NWF - Miniport Driver*.

Plusieurs commandes via l'utilitaire `netsh` permettent d'accéder rapidement à plusieurs informations Wi-Fi.

Parmi les plus utiles :

```
C:\netsh wlan show interfaces
```

Cette commande fournit les informations sur la carte, en particulier son état (connecté ou non) et les informations disponibles si elle est associée à un point d'accès.

```
C:\netsh wlan show drivers
```

Cette commande permet de récupérer la liste des pilotes installés ainsi que leurs capacités. Comme l'un des plus grands risques de compromission en sans-fil provient de la vulnérabilité des pilotes, il est important de cataloguer les versions utilisées dans son parc informatique et de vérifier régulièrement sur les sites des constructeurs si des mises à jour sont disponibles.

```
C:\netsh wlan show settings
```

```
C:\netsh wlan show profiles
C:\netsh wlan export profile name="xxxxx"
C:\netsh wlan connect profile name="xxxxx"
```

Cette commande retourne l'historique des profils de connexion créés. Ils correspondent aux réseaux auxquels la machine a été précédemment connectée. Quelques astuces existent cependant pour se connecter sans créer pour autant un profil mais elles ne sont pas abordées ici. Chacun des profils peut être exporté au format XML. La clé WPA PSK fait partie des informations ainsi récupérées.

Ces informations sont également visibles dans certaines clés de registres, comme par exemple :

`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Wireless`

Une machine compromise peut également avoir de nouveaux profils qui y ont été ajoutés, comme la connexion à un réseau ouvert ou un réseau *ad hoc*. Cette connexion peut être activée ponctuellement ou en fonction du contexte d'installation de la machine (bureau/domicile). Cette connexion, sous certaines conditions, permet alors d'accéder à l'interface filaire de la machine. La personne malveillante peut interagir avec le réseau interne via la machine compromise.

Vista a également la possibilité de découvrir et lister les réseaux naturellement, sans passer nécessairement par une application tiers comme Netstumbler.

```
C:\netsh wlan show networks mode=bssid
```

Cette commande reprend les dernières informations récupérées par NDIS 6.
NDIS 6 permet enfin d'utiliser le mode moniteur de la carte assez simplement.

6.2 Conclusion

Le lecteur aura compris que beaucoup d'actions liées au Wi-Fi sont envisageables sans pour autant passer par une fenêtre graphique (GUI). Il peut s'agir de quelques lignes de commandes, tout comme cela peut aussi se faire avec d'autres systèmes d'exploitation. Ces dernières, une fois lancées, peuvent exposer tout réseau auquel sera branché l'équipement sans-fil.

Le CERTA rappelle donc l'impérative nécessité de :

- supprimer physiquement toute interface sans-fil qui n'est pas nécessaire, dans la mesure du possible ;
- supprimer tout code associé au sans-fil (pilotes) au moment de l'installation d'un système, quand ce service n'est pas utilisé ;
- considérer dans la politique de sécurité que tout poste nomade équipé d'une interface est une porte d'entrée potentielle dans les réseaux auxquels il sera branché ;
- sensibiliser les utilisateurs à désactiver leurs interfaces quand elles ne sont pas utilisées.

6.3 Documentation associée

- Documentations Microsoft, Section "Windows Vista Resources" :
  http://technet.microsoft.com/en-us/network/bb530679.aspx
- Documentation Microsoft, "Extending Windows Vista Native Wi-Fi Capabilities", 2006 :
  http://downloads.microsoft.com/
- J. Wright, InGuardians, "Vista Wireless Power Tools", décembre 2008 :
  http://www.inguardians.com/pubs/Vista_Wireless_Power_Tools-Wright.pdf

7 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 11 et le 18 décembre 2008.

8 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/

9 Rappel des avis émis

Dans la période du 12 au 19 décembre 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-592 : Vulnérabilité dans phpMyAdmin
– CERTA-2008-AVI-593 : Vulnérabilité dans PHP
– CERTA-2008-AVI-594 : Multiples vulnérabilités dans IBM AIX
– CERTA-2008-AVI-595 : Vulnérabilité dans HP OpenView
– CERTA-2008-AVI-596 : Multiples vulnérabilités dans Drupal
– CERTA-2008-AVI-597 : Vulnérabilité dans Sun Java System Portal Server
– CERTA-2008-AVI-598 : Vulnérabilité dans ARCserve Backup
– CERTA-2008-AVI-599 : Vulnérabilité dans Asterisk
– CERTA-2008-AVI-600 : Vulnérabilité dans OpenSSL de Sun Solaris
– CERTA-2008-AVI-601 : Vulnérabilité dans IBM Tivoli Provisioning Manager
– CERTA-2008-AVI-602 : Multiples vulnérabilités dans IBM WebSphere Portal
– CERTA-2008-AVI-603 : Vulnérabilités dans Mac OS X
– CERTA-2008-AVI-604 : Vulnérabilité dans Microsoft Internet Explorer

Durant la même période, l'avis suivant a été mis à jour :

– CERTA-2008-AVI-574-002 : Vulnérabilité dans ClamAV
(ajout de la référence Mandriva et du CVE)

10 Actions suggérées

10.1 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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/

11 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.

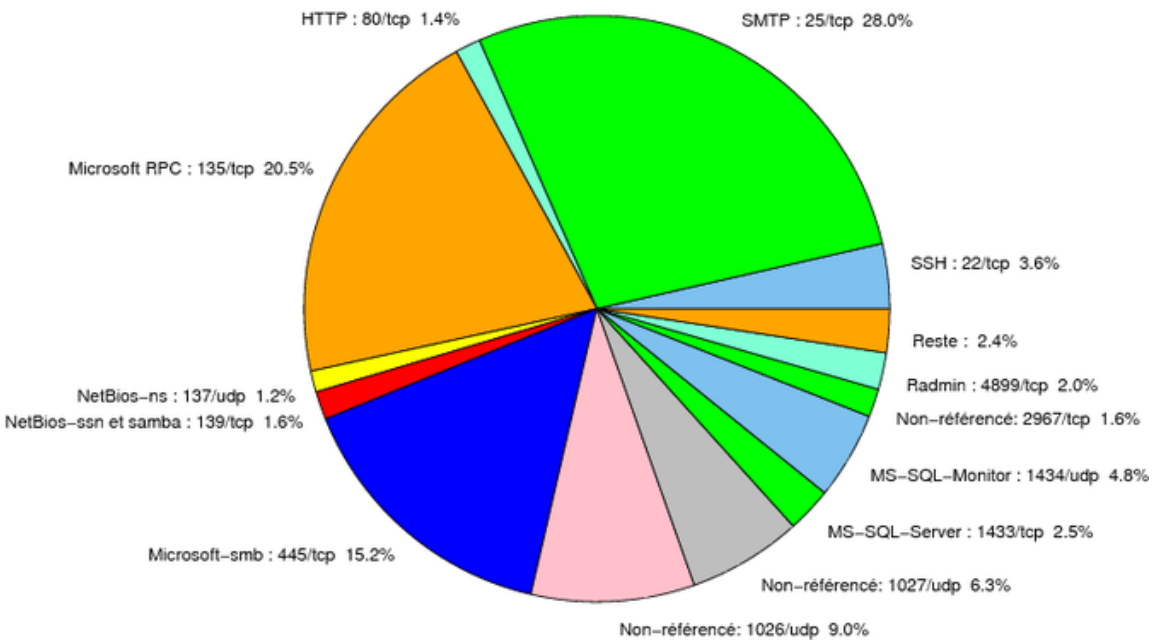

FIG. 1: Répartition relative des ports pour la semaine du 11.12.2008 au 18.12.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CERT
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CERT
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERT
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERT
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERT
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT

				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	27.99
135/tcp	20.45
445/tcp	15.24
1026/udp	9.02
1027/udp	6.29
1434/udp	4.82
22/tcp	3.57
1433/tcp	2.48
4899/tcp	2.02
2967/tcp	1.55
80/tcp	1.39
137/udp	1.16
21/tcp	0.93
23/tcp	0.38
3389/tcp	0.31
3128/tcp	0.15
9898/tcp	0.07

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

19 décembre 2008 version initiale.