

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2008-12

---

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-012>

---

### Gestion du document

Référence	CERTA-2008-ACT-012
Titre	Bulletin d'actualité 2008-12
Date de la première version	21 mars 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-012.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-012/>

## 1 Incidents de la semaine

### 1.1 Le vol d'identifiants bancaires

Cette semaine, le CERTA a contribué à la fermeture d'un site malveillant. Suite à la compromission d'un site légitime, les attaquants ont déposé une page servant de support à une tentative de vol de numéros de cartes bancaires. En effet, la page frauduleuse utilisait le logo d'une banque française afin de mettre en confiance les victimes.

Les victimes, qui étaient invitées à saisir leur informations bancaires, étaient dirigées vers cette page frauduleuse par le biais d'une annonce d'une fausse agence de *casting*.

Le CERTA rappelle que les services de paiements sécurisés des banques doivent se trouver sur leur site. Il convient donc de s'assurer de la validité et de la sécurité du site avant de saisir des informations personnelles ou bancaires.

### Documentation

- Portail de la Sécurité Informatique, « Bien utiliser sa carte bancaire » :  
[http://www.securite-informatique.gouv.fr/gp\\_article244.html](http://www.securite-informatique.gouv.fr/gp_article244.html)

## 1.2 Pas de mise à jour : risque de compromission

Cette semaine le CERTA a traité un incident relatif à la compromission d'un site web. Ce site utilisait une version vulnérable du composant `Ext_Calendar`. Les attaquants ont profité de la vulnérabilité pour déposer un site bancaire frauduleux (*phishing* ou filoutage). Le CERTA recommande de suivre et d'appliquer les mises à jour conformément à la politique de sécurité du système d'information. Le CERTA rappelle également qu'il convient de désactiver les composants vulnérables ou inutilisés.

## 2 Logiciels libres et pilotes propriétaires

Un certain nombre de distributeurs fournissent maintenant des ordinateurs livrés en standard avec une distribution GNU/Linux préinstallée. Tout comme avec d'autres systèmes, il convient lorsque l'on fait l'acquisition de ce type de machines de s'intéresser à la sécurisation de ce type d'équipement. En effet, comme tout système d'exploitation, il doit en particulier être mis à jour.

Dans ce contexte, il est important de signaler que sur ce type de système le support du matériel sous-jacent peut se faire principalement de deux manières :

- soit le périphérique est nativement supporté par le noyau ( « *kernel* » ) ou bien encore le fabricant du périphérique a fourni un pilote dont la licence est compatible avec celle du noyau (GPL). Ceci est le cas idéal mais il conviendra de s'assurer que dans la deuxième hypothèse le pilote soit bien maintenu ;
- soit le pilote associé au périphérique n'est distribué qu'en code fermé et utilise des versions précises pour chaque distribution ou noyau. C'est le cas notamment pour certaines cartes graphiques ou certains contrôleurs RAID. Le problème dans ce cas est que la mise à jour du système deviendra éventuellement dépendante de la publication d'une nouvelle version de ce pilote.

Dans le deuxième cas, il peut arriver que l'éditeur, ne fournissant pas de version compatible avec le système de mise à jour, « casse » purement et simplement le système gérant les mises à jour. A cause d'un simple pilote, toutes les corrections de failles ne fonctionnent alors plus.

Le propos n'est pas ici de débattre sur le bien fondé de l'utilisation de tel ou tel type de licence ou de méthode de diffusion de pilotes. Il convient plutôt d'être vigilant sur les pilotes ou logiciels livrés en dehors du système intégré de gestion des logiciels. Ceux-ci peuvent parfois provoquer des effets de bord désastreux en terme de sécurité et de mises à jour.

## 3 Incompatibilités possibles entre deux services concurrents

Il est important de bien contrôler les services actifs sur une machine. Certains d'entre eux peuvent, à l'insu de l'utilisateur, être incompatibles et provoquer le non-respect de la politique de sécurité.

A valeur d'exemple, prenons SNTP : il s'agit de la version simplifiée du protocole de synchronisation NTP (pour *Network Time Protocol*). Ce dernier est normalement destiné à des réseaux dont la précision de synchronisation ne descend pas sous l'ordre de la seconde. Cette méthode « allégée » est en particulier adaptée pour des systèmes embarqués ou des éléments terminaux qui ne serviraient pas eux-même de référence à d'autres systèmes.

SNTP utilise le même port de communication que NTP (123/UDP) pour atteindre le serveur, mais, à la différence de NTP, peut utiliser des ports source arbitraires non nuls, comme le signale le standard RFC 4330. En pratique, le port 123/UDP est régulièrement utilisé à la fois comme source et destination.

Certains éléments de réseau comme des routeurs peuvent avoir un processus NTP actif, même si aucune commande explicite pour l'utiliser n'est installée. Ainsi, dans certains éléments Cisco, le service peut se lancer insidieusement par une commande de configuration `ntp logging`, et ne s'interrompt que lors d'un prochain chargement ou démarrage de l'appareil.

Les deux clients NTP et SNTP peuvent alors se retrouver en concurrence pour interpréter une trame de réponse émise par un serveur. Le client NTP a de fortes chances d'être le plus prompt à intercepter la réponse, et prive ainsi le client SNTP de cette dernière.

Il est préférable d'avoir une synchronisation précise, mais cette concurrence entre les deux services peut entraîner que la politique choisie ne soit pas respectée. Si le service NTP n'a pas été correctement configuré, car non prévu, c'est la synchronisation complète qui peut être remise en jeu.

Il est donc important de :

- vérifier avec soin la configuration voulue. Au niveau des routeurs, il est souvent possible de tester celle-ci : par exemple, sous Cisco, il existe les commandes `debug ntp packet` et `debug sntp packet`.

- vérifier la cohérence entre les traces réseau et les informations retournées par le système et la configuration mise en place.

## Documentation associée

- Standard RFC 4330, "Simple Network Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", janvier 2006 : <http://www.apps.ietf.org/rfc/rfc4330.html>

## 4 Sortie du Service Pack 1 pour Windows Vista

Le 18 mars 2008 est sorti le premier *Service Pack* pour Microsoft Windows Vista. Il est disponible en cinq langues (allemand, anglais, espagnol, français et japonais) pour les versions 32 bits et 64 bits du système d'exploitation. Le contenu de cette mise à jour a été détaillé dans le bulletin CERTA-2007-ACT-049, lors de la sortie de la version *release candidate*.

L'utilisateur a le choix de l'installer via l'application *Windows Update* ou de le télécharger sur le site internet de Microsoft. Dans le premier cas il faut choisir les mises à jour facultatives. La mise à jour automatique ne se fera en effet qu'à partir de mi-avril.

Enfin, il apparaît que certaines personnes n'ont pour le moment pas accès au *Service Pack* via *Windows Update* et doivent obligatoirement télécharger la version autonome manuellement. Il s'agit notamment de personnes dont les machines ont des pilotes de périphériques incompatibles avec le service pack 1, et qui doivent être mis à jour. Une liste de ces pilotes est disponible en documentation (KB948343 en anglais).

### 4.1 Documentation

- Téléchargement de Windows Vista Service Pack 1 autonome pour processeurs x86 : <http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=b0c7136d-5ebb-413b-89c9-cb3d06d12674>
- Téléchargement de Windows Vista Service Pack 1 autonome pour processeurs x64 : <http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=874a414b-32b2-41cc-bd8b-d71eda5ec07c>
- Microsoft Knowledgebase 948343 - liste des pilotes incompatibles <http://support.microsoft.com/kb/948343/en-us>

## 5 Attaques massives de type *SQL Injection*

### 5.1 Présentation des incidents cités dans la presse

Plusieurs articles ont récemment été publiés relatant qu'une grande quantité de sites Internet ont été victimes d'attaques de type *SQL injection*. Le schéma de ces attaques est le même que d'anciennes attaques de ce type et affecte le trio ASP, IIS, Microsoft SQL Server. Tout d'abord la personne malveillante cherche à déterminer si le site est vulnérable ou non. Pour cela elle envoie des requêtes d'injection classiques afin de tester les réactions du site. Il apparaît que la compromission se fait de différentes façons en fonction des réactions des serveurs. Selon les analyses publiées récemment, les premières requêtes envoyées se présentent de la forme suivante dans le journal des événements :

```
AAAA-MM-JJ hh:mm:ss /repertoire/page.asp
      id=z%20AND%20char(124)...
      HTTP/1.1 REFERER -- 200 0 17115 1171
AAAA-MM-JJ hh:mm:ss /repertoire/page.asp
      id=z%27%20AND%20char(124)...
      ... HTTP/1.1 REFERER -- 200 0 17115 562
```

Dans un navigateur, la requête prend la forme :

```
http://www.Le_Site.tld.../page.asp?id=z%20AND%20char(124)...
```

Cette requête est encodée deux fois. Le premier encodage est pris en charge par *IIS*. Ce sont les jeux de caractères commençant par "%" comme %20 qui correspond au caractère « espace ». La seconde phase d'encodage se situe au niveau de *SQL Server*. On remarque que la requête utilise d'ailleurs des fonctions SQL. Après avoir retiré l'encodage, on obtient :

```
id=z AND |user|=0
id=z AND |user|=0 and ''=''
```

Grâce à une nouvelle requête, le message d'erreur reçu en retour permet d'obtenir de précieuses informations comme l'utilisateur de l'application web. La requête en question est de cette forme :

```
AAAA-MM-JJ hh:mm:ss /repertoire/page.asp
id=z%27%20AND%20char(124)%2Buser%2Bchar(124)=0...
...|Syntax_error_converting_the_nvarchar
_value_'|IUSR_Server'|_to_a_column_of_data_type_int.
... HTTP/1.1 REFERER - - 500 0 292 390
```

Après avoir décodé, on obtient cette requête :

```
id=z AND |user|=0 and '%']=''
```

Il est parfois nécessaire d'envoyer une nouvelle requête afin d'avoir l'assurance que l'utilisateur possède les droits *sysadmin*. Enfin, une requête permettant la déclaration d'une variable est ensuite envoyée. Cette requête convertit une chaîne de caractères hexadécimale en une chaîne de type *NVARCHAR* puis tente d'exécuter cette dernière.

```
AAAA-MM-JJ hh:mm:ss /repertoire/page.asp
id=z;DECLARE%20@S%20NVARCHAR(4000);SET%20
@S=CAST(0x440045004300...VARCHAR(4000));EXEC(@S);...
HTTP/1.0 REFERER - - 200 0
```

Après décodage, on obtient cette requête :

```
DECLARE @S NVARCHAR(4000);
SET @S=CAST(0x440045004300... AS NVARCHAR(4000));
EXEC(@S);...
```

Le script inséré dans la base consiste en la déclaration de quelques variables, avant de parcourir l'ensemble des tables *sysobjects syscolumns*, qui contiennent l'ensemble des tables et colonnes de la base de données, à la recherche de type de champs pouvant contenir des données de type *strings*. Cela a pour conséquence l'ajout dans ces champs de liens vers un code *JavaScript* pointant vers un site malveillant.

## 5.2 Les recommandations du CERTA

- Pour les développeurs :
  - mettre en place des contrôles permettant la vérification des variables dans les pages *ASP* ;
  - vérifier l'intégrité de la base de données ;
  - contrôler les flux entrant et sortant ;
  - surveiller les traces journaux à la recherche de requêtes particulières (mots-clés *varchar*, *exec*, etc.);
  - éviter de lancer les applications web avec un utilisateur ayant les droits *sysadmin*.
- Pour les utilisateurs :
  - désactiver dans le navigateur l'exécution de code *JavaScript*, y compris sur des sites de confiance, lorsque cela n'est pas nécessaire ;
  - prévenir son correspondant en sécurité informatique, RSSI, en cas de comportements bizarres suite à une navigation ;
  - avoir impérativement son système à jour avant toute navigation ;
  - naviguer avec un compte utilisateur aux droits limités.

## Documentation

- Bloc-notes de Microsoft sur les incidents du 15 mars 2008 :  
<http://blogs.technet.com/neilcar/archive/2008/03/15/anatomy-of-sql-injection-incident-part-2-meat.aspx>
- Bloc-notes de Microsoft sur les incidents du 14 mars 2008 :  
<http://blogs.technet.com/neilcar/archive/2008/03/14/anatomy-of-sql-injection-incident.aspx>

## 6 CUPS - Common UNIX Printing System

Le CERTA a publié cette semaine un avis sur une vulnérabilité de CUPS (CERTA-AVI-2008-156).

CUPS, pour *Common Unix Printing Systems*, est un serveur d'impression, permettant à différents éléments ou machines de traiter et d'envoyer des tâches d'impression à l'imprimante associée.

Adapté sur plusieurs distributions Linux, CUPS est également utilisé comme le système d'impression par défaut sur Mac OS X d'Apple, qui en est également le propriétaire depuis 2007.

Ce logiciel est vulnérable à un dépassement de mémoire qui, sous certaines conditions, permet l'exécution de code arbitraire à distance. Il est installé par défaut, entre autres, sur Mac OS X, et l'interface de configuration est accessible à l'adresse <http://localhost:631>. Une des conditions nécessaires à l'exécution de code est qu'une imprimante partagée soit installée. Il semble cependant possible de contourner cette restriction en configurant CUPS, au détriment de l'utilisateur, et cela via une page web spécifiquement créée. Pour savoir si CUPS tourne sur la machine locale, il suffit de tester l'accès à un élément déterminant tel qu'une image, et cela via l'adresse de configuration.

Pour cela, un simple code JavaScript inséré dans une page permet d'effectuer un test. Il suffit par exemple de vérifier l'existence d'une image via l'interface CUPS. Si le test est positif, cela déclenche l'exécution d'une action JavaScript (*onload*). La page malveillante peut alors manipuler la configuration de CUPS à l'aide du code JavaScript.

Le CERTA recommande de mettre à jour les applications, et, comme il est souvent répété, de n'activer le JavaScript que ponctuellement, quand celui-ci est indispensable, et sur un site de confiance.

Par ailleurs, les services doivent être correctement configurés, et la navigation doit se faire par le biais d'un compte aux droits limités.

## Documentation

- Site officiel de CUPS :  
<http://www.cups.org>
- Documentation détaillée de CUPS :  
<http://www.cups.org/documentation.php>

## 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 13 et le 20 mars 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 14 au 20 mars 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-130 : Vulnérabilité dans Sun Java Server Faces
- CERTA-2008-AVI-131 : Vulnérabilité dans IBM WebSphere MQ pour HP NonStop
- CERTA-2008-AVI-132 : Multiples vulnérabilités dans IBM WebSphere Application Server
- CERTA-2008-AVI-133 : Multiples vulnérabilités dans Cisco User-Changeable Password
- CERTA-2008-AVI-134 : Vulnérabilités dans Adobe ColdFusion
- CERTA-2008-AVI-135 : Multiples vulnérabilités dans IBM AIX
- CERTA-2008-AVI-136 : Vulnérabilité dans Nagios
- CERTA-2008-AVI-137 : Vulnérabilité dans Sun Java Desktop System
- CERTA-2008-AVI-138 : Vulnérabilité dans CiscoWorks Internetwork Performance Monitor
- CERTA-2008-AVI-139 : Vulnérabilité dans Novell Groupwise
- CERTA-2008-AVI-140 : Multiples vulnérabilités dans CISCO ACS UCP
- CERTA-2008-AVI-141 : Vulnérabilités dans les produits VMware
- CERTA-2008-AVI-142 : Vulnérabilité dans Avaya Call Management System
- CERTA-2008-AVI-143 : Vulnérabilité des produits F-Secure
- CERTA-2008-AVI-144 : Vulnérabilité de la bibliothèque Perl Net::DNS
- CERTA-2008-AVI-145 : Multiples vulnérabilités dans Safari
- CERTA-2008-AVI-146 : Vulnérabilité dans MDaemon
- CERTA-2008-AVI-147 : Vulnérabilité de Symantec Altiris Deployment Server
- CERTA-2008-AVI-148 : Multiples vulnérabilités dans Apple Mac OS X
- CERTA-2008-AVI-149 : Vulnérabilité dans Checkpoint VPN-1
- CERTA-2008-AVI-150 : Multiples vulnérabilités dans Asterisk
- CERTA-2008-AVI-151 : Vulnérabilité dans HP-UX StorageWorks
- CERTA-2008-AVI-152 : Multiples vulnérabilités dans WinRAR
- CERTA-2008-AVI-153 : Vulnérabilité dans bzip2
- CERTA-2008-AVI-154 : Multiples vulnérabilités dans Kerberos
- CERTA-2008-AVI-155 : Multiples vulnérabilités dans IBM Informix Dynamic Server
- CERTA-2008-AVI-156 : Vulnérabilité dans CUPS

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

- CERTA-2007-AVI-502-002 : Vulnérabilités dans Samba  
(ajout de la référence au bulletin de sécurité HP-UX)

## **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 réglementaire, 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 COSSI/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 inexplicables 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.formation.ssi.gouv.fr>

## 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.

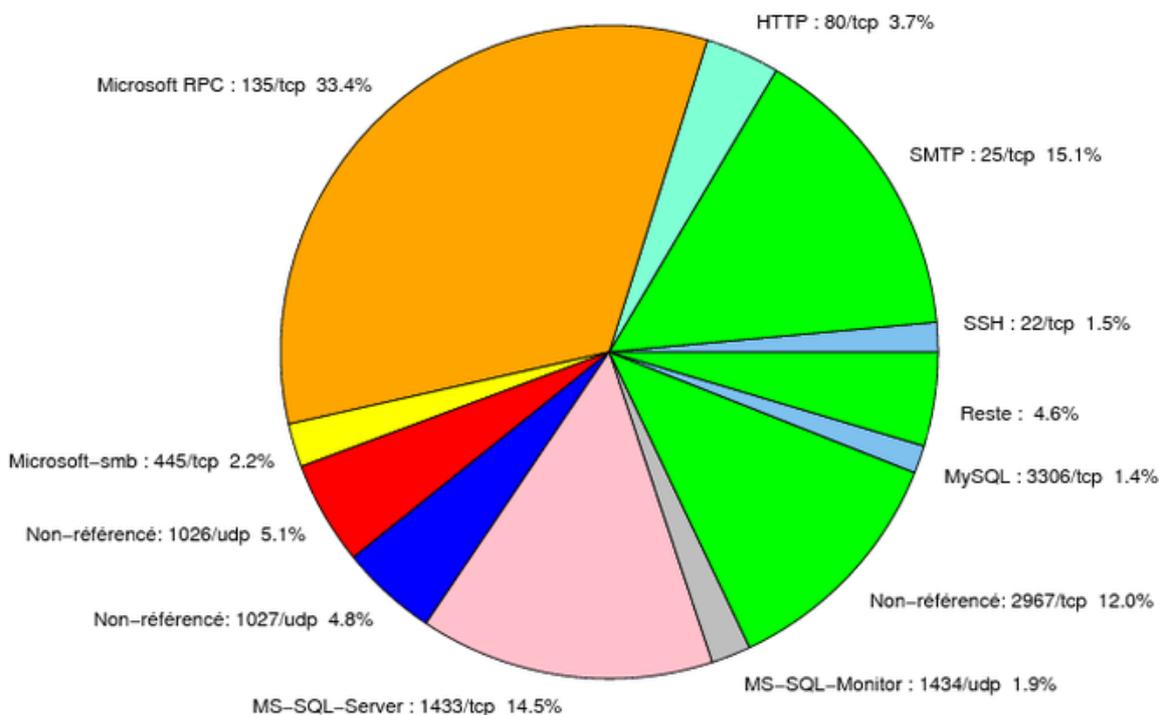


FIG. 1: Répartition relative des ports pour la semaine du 13.03.2008 au 20.03.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
22	TCP	SSH	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
23	TCP	Telnet	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> CERTA-2007-ALE-005-001
25	TCP	SMTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
42	TCP	WINS	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
69	UDP	IBM Tivoli Provisioning Manager	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
80	TCP	HTTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
106	TCP	MailSite Email Server	-	- <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
111	TCP	Sunrpc-portmapper	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
119	TCP	NNTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
135	TCP	Microsoft RPC	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
137	UDP	NetBios-ns	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
139	TCP	NetBios-ssn et samba	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
143	TCP	IMAP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
389	TCP	LDAP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
427	TCP	Novell Client	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
443	TCP	HTTPS	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
445	TCP	Microsoft-smb	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>

				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	33.41
25/tcp	15.05
1433/tcp	14.49
2967/tcp	12
1026/udp	5.11
1027/udp	4.77
80/tcp	3.74
445/tcp	2.15
1434/udp	1.93
22/tcp	1.46
3306/tcp	1.37
23/tcp	0.94
4899/tcp	0.77
1080/tcp	0.73
139/tcp	0.64
137/udp	0.43
3128/tcp	0.38
21/tcp	0.21
143/tcp	0.17
2100/tcp	0.12
42/tcp	0.04

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	10
3	Paquets rejetés . . . . .	11

## Gestion détaillée du document

21 mars 2008 version initiale.