

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-13

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-013>

Gestion du document

Référence	CERTA-2009-ACT-013
Titre	Bulletin d'actualité 2009-13
Date de la première version	27 mars 2009
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-013.pdf>

Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-013/>

1 MS08-067, Conficker... une histoire sans fin ?

Le CERTA a informé ses correspondants à plusieurs reprises depuis octobre 2008 de la nécessité d'appliquer le correctif du bulletin MS08-067 puis de l'existence de codes d'exploitation utilisant pour se propager la vulnérabilité corrigée.

L'un d'eux, dénommé Conficker (ou Downadup ou Kido) a été largement médiatisé du fait du nombre de machines qu'il a réussi à compromettre. Le code évolue depuis janvier 2009, en réaction à certaines contremesures mises en place par les éditeurs et des équipes de sécurité.

La version la plus récente a été détectée la première semaine de mars. Les analyses en cours de cette souche indiquent que les méthodes de détection des versions précédentes ne sont plus, pour certaines, pertinentes. Bien que cette souche ait été installée sur des postes infectés depuis début mars, certains blocs fonctionnels ne seraient activés qu'ultérieurement, dans les premiers jours d'avril.

La nouvelle version rend plus complexe, du point de vue opérationnel, les moyens de surveillance des réseaux vis-à-vis du ver. En particulier :

- un contrôle du ver qui s'appuie sur des listes noires de noms de domaine s'avère très difficile à mettre en place. En effet, le code « pioche » chaque jour des noms parmi une liste de 50 000 aléatoires renouvelés quotidiennement ;

- un contrôle du ver qui s'appuie sur un blocage au niveau des passerelles de navigation est difficile à mettre en place. Les précédentes versions permettaient d'identifier des requêtes Web caractéristiques. La nouvelle souche génère une requête GET vide.

En revanche, la nouvelle version dispose de plusieurs méthodes pour communiquer. L'une d'elles consiste en une forme de protocole pair-à-pair. Elle implique l'ouverture de plusieurs ports non privilégiés en UDP et TCP visibles sur la machine dans les clés de registres comme :

```
SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\
StandardProfile\GloballyOpenPorts\List
```

Ce canal de communication ne fonctionne pas correctement si les pare-feux en périphérie appliquent une politique de filtrage des connexions sortantes rigoureuse et restrictive.

- P. Porras, H. Saidi, V. Yegneswaran, « Conficker C Analysis », SRI International Technical Report, 19 mars 2009 :
<http://mtc.sri.com/Conficker/addendumC/index.html>

Documentation

Liens du CERTA :

- Avis CERTA-2008-AVI-523 du 23 octobre 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-523/>
- Bulletin d'actualité CERTA-2008-ACT-43 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-043.pdf>
- Bulletin d'actualité CERTA-2008-ACT-45 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-045.pdf>
- Bulletin d'actualité CERTA-2008-ACT-48 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-048.pdf>
- Bulletin d'actualité CERTA-2009-ACT-002 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-002.pdf>
- Bulletin d'actualité CERTA-2009-ACT-004 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-004.pdf>
- Bulletin d'actualité CERTA-2009-ACT-005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-005.pdf>

Portail de la sécurité informatique :
www.securite-informatique.gouv.fr

Liens complémentaires :

- Bloc-Notes Microsoft MMPC, article du 22 janvier 2009 :
<http://blogs.technet.com/mmpc/archive/2009/01/22/centralized-information-about-the-conficker-worm.aspx>
- Article Microsoft KB 962007, « Alerte concernant le ver Win32/Conficker.B » :
<http://support.microsoft.com/kb/962007>
- Fiches d'analyse Microsoft de Conficker.C et Conficker.D :
<http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.C>
<http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm%3aWin32%2fConficker.D>
- Outil de suppression de logiciels malveillants Microsoft Windows :
<http://support.microsoft.com/?kbid=890830>
<http://www.microsoft.com/france/securite/malwareremove/default.aspx>
- Déploiement de l'outil de suppression de logiciels malveillants Microsoft Windows dans un environnement d'entreprise :
<http://support.microsoft.com/kb/891716>
- Bloc-notes de Mathieu Malaise :
<http://blogs.technet.com/mathieum/>

- Bloc-notes de F-Secure :
<http://www.f-secure.com/weblog/>
- Outil de nettoyage proposé par F-Secure :
<http://www.f-secure.com/weblog/archives/00001588.html>
<ftp://ftp.f-secure.com/anti-virus/tools/beta/f-downadup.zip>
- Forum et bloc-notes de Symantec :
<http://www.symantec.com/stn/blogs/index.jsp>
http://www.symantec.com/business/security_response/weblog/index.jsp
- Outil de nettoyage Symantec :
http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-011316-0247-99

2 Incidents de la semaine

2.1 Un problème d'étanchéité

2.1.1 Présentation

Cette semaine le CERTA a traité un incident de sécurité relatif à la compromission d'un serveur Web mutualisant une trentaine de sites Internet. La compromission d'un simple compte utilisateur (disposant d'un mot de passe trivial) a permis aux attaquants de déposer des archives de filoutage (*phishing*) sur tous les sites cohébergés parmi lesquels 2 administrations françaises.

Cet incident regroupe plusieurs problèmes :

- la sécurité des hébergements mutualisés : les restrictions d'accès des comptes utilisateurs doivent interdire toute modification en dehors du périmètre autorisé ;
- la compromission à partir d'un accès distant : dans la mesure du possible, les accès distants doivent être filtrés ou restreints aux seules personnes autorisées ;
- le mot de passe faible : les ordinateurs connectés à l'Internet sont régulièrement victimes de tentatives d'attaques sur les comptes et mots de passe standards ou prévisibles. Il convient donc de choisir des mots de passe dits « forts » pour réduire le succès de ces attaques.

Il s'avère, de plus, que ce serveur était loin d'être à jour en termes de correctifs de sécurité, l'hébergeur justifiant cette situation par la prochaine migration de ses clients sur une nouvelle architecture.

Le choix d'une solution de mutualisation ou de cohébergement doit faire l'objet d'une attention toute particulière quant à la sécurité mise en œuvre car dans ce contexte le niveau de sécurité effectif du serveur sera celui du site Internet cohébergé le moins sécurisé ou n'appliquant pas les correctifs de sécurité.

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/>
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>

2.2 Utilisation d'un script par un cheval de Troie

Le CERTA a été informé cette semaine d'un incident peu courant. Le site Web d'une administration hébergeait un script (légitime) qui permettait d'envoyer des messages électroniques. Ce script n'ayant pas de protection particulière, il était accessible à tout internaute et permettait, entre autres, de relayer des courriels non désirés.

Dans le cadre de cet incident, ce script a été utilisé à une tout autre fin. En effet, un cheval de Troie destiné à obtenir frauduleusement des données de connexions saisies au clavier (par le biais d'un *keylogger*) utilisait ce site Web pour l'envoi des informations ainsi obtenues.

Les journaux d'accès au serveur Web ainsi que ceux de la messagerie étaient chargés par les accès des machines infectées. En cas de propagation importante de ce cheval de Troie, cela peut se traduire par un déni de service. La lecture de ces journaux permet néanmoins de détecter les machines ainsi infectées.

3 Deux nouvelles alertes

Cette semaine le CERTA a publié deux nouvelles alertes, la première relative à une vulnérabilité dans `Apple Mac OS X` et la seconde à une vulnérabilité dans `Mozilla Firefox`.

3.1 Vulnérabilité dans Mac OS X

Une vulnérabilité non corrigée dans `Mac OS X` permet à une personne malintentionnée d'élever ses privilèges sur la machine cible. Cette vulnérabilité affecte un appel système lié au format de système de fichiers `HFS+`. Des codes d'exploitation sont déjà disponibles sur l'Internet.

Le CERTA recommande donc de rester prudent dans l'exécution de fichiers provenant d'une source non sûre afin de limiter les possibilités d'installation d'un code malveillant.

A titre d'exemple, cette semaine un éditeur d'antivirus a détecté la nouvelle variante `OSX/RSPlug-F` d'un cheval de Troie. Ce code malveillant repose sur les mêmes méthodes que `DNSChanger`. La propagation de ce code se fait sous la forme d'un faux programme `HDTV/DTV` nommé `MacCinema`.

3.2 Vulnérabilité dans Mozilla Firefox

L'alerte CERTA-2009-ALE-004 publiée aujourd'hui fait état d'une vulnérabilité non corrigée dans le navigateur `Mozilla Firefox`. Une personne malveillante peut exécuter du code arbitraire à distance via une erreur dans l'interprétation des fichiers au format `XSL`. Des preuves de faisabilité sont disponibles sur l'Internet et un correctif est en cours d'élaboration. Ce dernier doit être fourni dans la prochaine version 3.0.8 du navigateur le 01 avril 2009.

Dans l'attente de correctif, le CERTA recommande d'utiliser un navigateur alternatif et d'appliquer les bonnes pratiques suivantes pour limiter les risques :

- désactiver l'interprétation du `JavaScript` ;
- naviguer avec un compte utilisateur aux droits limités.

3.3 Documentation

- Alerte CERTA-2009-ALE-003 du 24 mars 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-003/>
- Alerte CERTA-2009-ALE-004 du 27 mars 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-004/>

4 Noyau Linux 2.6.29 et nouvelles fonctionnalités

4.1 Détails

La dernière version du noyau `Linux` a été publiée cette semaine apportant son lot de nouveautés et de corrections de bogues. Pour ce deuxième aspect, le CERTA reviendra dans un article ultérieur sur la politique à adopter en la matière. En ce qui concerne les nouvelles fonctionnalités apportées par cette version, on pourra s'attarder sur deux d'entre elles en particulier :

- 1° le `kernel modesetting` ;
- 2° un nouveau format de système de fichiers, le `btrfs`.

Le premier cas (le `kernel modesetting`) concerne une fonctionnalité fort intéressante qui consiste à mettre en œuvre le changement de mode de la carte graphique dans le noyau et non plus à la fois en espace noyau et en espace utilisateur comme c'est le cas actuellement. Le mode d'une carte graphique définit ce qu'elle est capable d'afficher en matière de résolution : largeur, hauteur, nombre de couleurs possibles, ...

Ainsi, lorsque l'on « passe » du serveur `X` à une console par l'appui simultané de `Ctrl+Alt+F1` par exemple, on change le mode de la carte graphique. Or, cette opération est complexe : on passe d'un pilote de serveur `X` en espace utilisateur à un pilote de type « `framebuffer` » géré par le noyau. Chaque passage de l'un à l'autre nécessite une réinitialisation de la carte graphique. Ceci n'est pas sans conséquence sur la stabilité et la robustesse du système, en particulier lorsque le pilote du serveur `X` pour des raisons de performance est couplé à un pilote noyau mettant en œuvre du `DRI` (`Direct Rendering Interface`).

Un apport majeur de cette délégation au noyau est donc d'éviter cette réinitialisation. En termes de sécurité, cela apporte également la possibilité de faire fonctionner un serveur X sans les privilèges de l'administrateur autrefois nécessaires à certains pilotes (*drivers*) qui devaient disposer d'un accès direct à la mémoire de la carte vidéo. Dorénavant, tout est géré en espace noyau.

Cette fonctionnalité, bien qu'intéressante, manque encore de son « pendant » en mode utilisateur car il faudra adapter certains pilotes et certaines applications du serveur X pour s'interfacer correctement avec ce nouveau mode de fonctionnement.

Le deuxième cas est le système de fichiers *btrfs* dont la vocation est de « concurrencer » les systèmes de fichiers comme ZFS de Sun ou Hammer de DragonFlyBSD. Il apporterait donc le même type de fonctionnalités attendues pour des systèmes de fichiers modernes utilisés sur des serveurs. Cependant, selon l'avis même des développeurs, ce système de fichiers n'est qu'en phase d'évaluation et reste expérimental.

4.2 Recommandations

Dans les deux cas présentés précédemment, les nouvelles fonctionnalités de cette version du noyau Linux apportent un gain en robustesse ou en sécurité. Cependant, il faut bien garder à l'esprit que, comme toute nouvelle fonctionnalité, elle n'a pas encore été éprouvée et peut même encore être considérée comme expérimentale. Il conviendra donc de rester prudent et de ne pas céder à l'attrait de la nouveauté, en particulier dans un environnement de production.

5 Mises à jour Adobe

Le CERTA a précisé dans son précédent bulletin d'actualité l'existence de correctifs fournis par Adobe pour la vulnérabilité concernant les objets encodés en JBIG2 (alerte CERTA-2009-ALE-001). Adobe a également fourni des correctifs pour les versions de ses applications Adobe Reader et Acrobat sous Mac OS, Linux et Solaris. La mise à jour du bulletin de l'éditeur APSB09-04 précise que l'exploitation de cette vulnérabilité peut également conduire sous ces systèmes d'exploitation à l'exécution de commandes arbitraires. La mise à jour Adobe corrige les vulnérabilités référencées suivantes : CVE-2008-2549, CVE-2009-4813, CVE-2009-4814, CVE-2009-0193, CVE-2009-0658, CVE-2009-0927, CVE-2009-0928, CVE-2009-1061, CVE-2009-1062.

Plusieurs codes d'exploitation circulent actuellement sur l'Internet. Le CERTA en profite donc une nouvelle fois pour rappeler l'impérative nécessité de mettre à jour ses applications Adobe.

Documentation

- Bulletin d'actualité CERTA-2009-ACT-012, « Vulnérabilités PDF et exploitations », 20 mars 2009 : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-012.pdf>
- Bulletin Adobe APSB09-04 mis à jour le 24 mars 2009 : <http://www.adobe.com/support/security/bulletins/apsb09-04.html>

6 Mise à jour de la note d'information CERTA-2000-INF-002

La note d'information CERTA-2000-INF-002 traite des mesures de prévention relatives à la messagerie. La mise à jour de cette note actualise, par exemple, les captures d'écran pour la configuration des clients de messagerie dans leurs dernières versions et permet de lire et envoyer ses messages électroniques au format texte ou d'extraire les en-têtes des messages reçus.

Documentation

- Note d'information CERTA-2000-INF-002 du 27 mars 2009 : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/>

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 19 et le 26 mars 2009.

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 20 au 27 mars 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-109 : Multiples vulnérabilités dans Mozilla Thunderbird
- CERTA-2009-AVI-110 : Vulnérabilité dans IBM Lotus Notes
- CERTA-2009-AVI-111 : Vulnérabilités dans Sun Java System Identity Manager
- CERTA-2009-AVI-112 : Vulnérabilité de Sun Management Center
- CERTA-2009-AVI-113 : Vulnérabilité dans les commutateurs 3Com 4500G
- CERTA-2009-AVI-114 : Vulnérabilité dans HP-UX
- CERTA-2009-AVI-115 : Vulnérabilité du noyau FreeBSD
- CERTA-2009-AVI-116 : Multiples vulnérabilités dans HP OpenView Network Node Manager
- CERTA-2009-AVI-117 : Vulnérabilités dans phpMyAdmin
- CERTA-2009-AVI-118 : Multiples vulnérabilités dans Cisco IOS
- CERTA-2009-AVI-119 : Multiples vulnérabilités dans Java
- CERTA-2009-AVI-120 : Multiples vulnérabilités dans OpenSSL

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

- CERTA-2009-AVI-094-001 : Vulnérabilité dans l'interprétation JBIG2 des produits Adobe (ajout des références au bulletin de sécurité APSB09-04 concernant les versions 7x et 8.x.)

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 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 :

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.

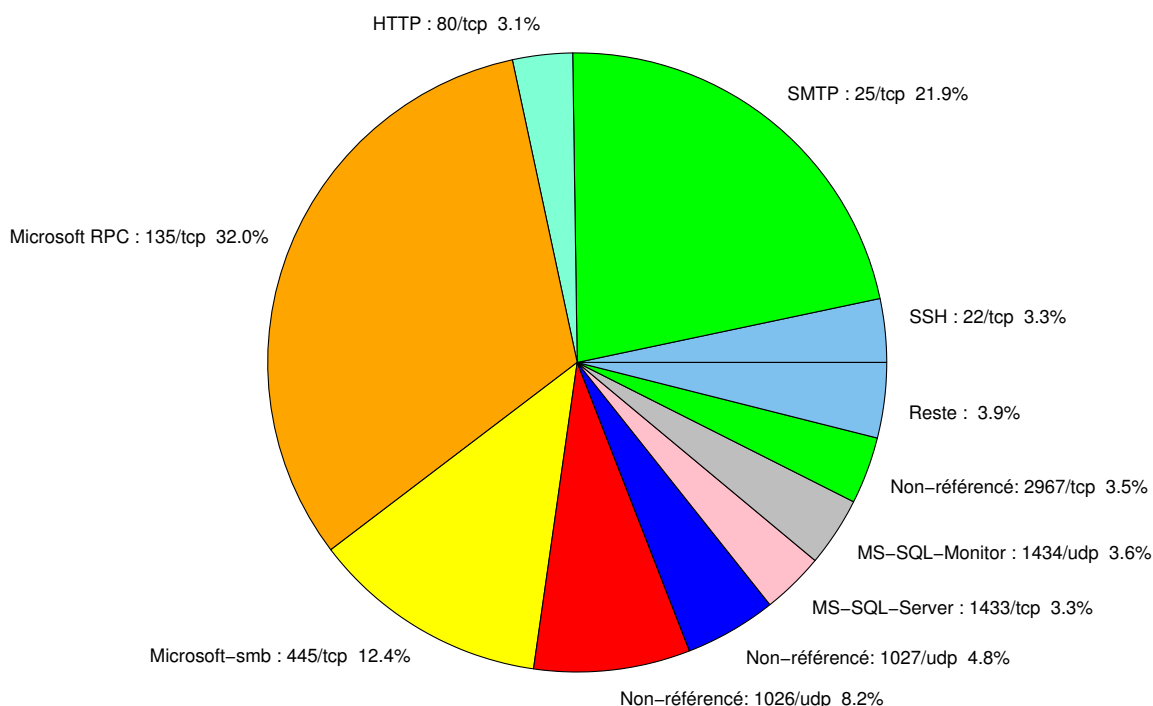


FIG. 1: Répartition relative des ports pour la semaine du 19 au 26 mars 2009

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	– CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283

				CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

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

port	pourcentage
135/tcp	31.98
25/tcp	21.91
445/tcp	12.4
1026/udp	8.16
1027/udp	4.78
1434/udp	3.62
2967/tcp	3.49
22/tcp	3.31
1433/tcp	3.25
137/udp	0.85
4899/tcp	0.61
3128/tcp	0.55
21/tcp	0.49
1080/tcp	0.18
3306/tcp	0.12
9898/tcp	0.06

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

27 mars 2009 version initiale.