

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-49

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-049>

Gestion du document

Référence	CERTA-2009-ACT-049
Titre	Bulletin d'actualité 2009-49
Date de la première version	04 décembre 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-049.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-049/>

1 Incident de la semaine

Cette semaine, le CERTA a traité, parmi de très nombreuses autres affaires de filoutage (*phishing*), un cas particulièrement intéressant. L'analyse de cet incident montre que les fichiers servant au filoutage ont été déposés suite à l'exploitation d'une vulnérabilité dans `phpMyAdmin` (référence CERTA : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-117/CERTA-2009-AVI-117.html>).

La particularité de cette attaque réside dans la date de l'exploitation, qui a eu lieu plusieurs semaines avant la création des fichiers servant au filoutage. Plusieurs intrusions ont été par la suite constatées entre l'exploitation de cette vulnérabilité de `phpMyAdmin` et la mise en place des pages Web frauduleuses.

Cette exploitation place une porte dérobée sur le serveur en modifiant le fichier `config.inc.php`. Des programmes malveillants parcourent l'Internet à la recherche de fichiers `config.inc.php` incluant cette porte dérobée. C'est ainsi que ce serveur a été victime d'une intrusion, suivie d'une élévation de privilèges et installation d'un *rootkit* plusieurs jours avant la création du filoutage.

Le CERTA recommande donc de mettre à jour `phpMyAdmin` car cette faille est actuellement exploitée. Il est également conseillé de vérifier le contenu de vos fichiers `config.inc.php`.

2 L'UAC

L'UAC ou *User Account Control* est une fonctionnalité introduite avec Windows Vista, également présente dans les versions ultérieures de Windows (Windows 7, Windows 2008). Cet article a pour principal objectif de rappeler son principe de fonctionnement et de présenter un changement apparu avec Windows 7.

2.1 Rappels sur le fonctionnement de l'UAC

L'UAC est intimement lié à des objets associés à chaque processus appelés *access tokens* ou jetons d'accès.

En effet, lorsqu'un utilisateur s'authentifie sur le système, un jeton est créé pour cet utilisateur qui sera associé avec tous ses processus. Ce *token* contient plusieurs informations, telles que le SID (*Security Identifier*) du compte, les SID des groupes, et les privilèges. Lorsqu'un objet tente d'être accédé par un processus, le système d'exploitation compare les éléments de son descripteur de sécurité (notamment, les entrées de sa liste de contrôle d'accès discrétionnaire ou DACL) avec les informations contenues dans le jeton du processus. A partir de Windows Vista, il existe trois types de jetons sur lesquels se base l'UAC :

- le jeton de type `TokenElevationTypeDefault` qu'on appellera jeton standard ;
- le jeton de type `TokenElevationTypeLimited` qu'on appellera jeton filtré ;
- le jeton de type `TokenElevationTypeFull` qu'on appellera jeton élevé.

Les types de jetons ne régissent pas les droits des processus, mais plutôt la manière dont l'élévation de privilèges doit s'effectuer.

En règle générale et dans la configuration par défaut, le premier jeton est utilisé pour les utilisateurs standards et les deux autres jetons pour les membres d'un groupe administratif (tel que le groupe Administrateurs). Ces derniers ont en effet deux jetons, liés entre eux, car s'ils ont bien des droits élevés, ceux-ci sont toutefois plus restreints par défaut. Le premier jeton de l'administrateur est appelé jeton filtré car il n'octroie pas tous les privilèges administrateur. Les processus exécutés par l'utilisateur hériteront alors de ce *token* par défaut. Le deuxième jeton est uniquement utilisé pour exécuter des processus requérant des droits plus élevés. Pour accéder à ce jeton, l'administrateur doit, dans la configuration par défaut, confirmer l'action via une boîte de dialogue. C'est le « mode d'approbation d'administrateur » ou AAM, configurable dans les options de sécurité des stratégies locales.

En ce qui concerne l'utilisateur standard, il n'a qu'un seul jeton. Pour exécuter un processus nécessitant des privilèges élevés, il doit, comme sur Windows XP, l'exécuter en tant qu'administrateur de la machine et donc entrer le mot de passe d'un compte d'administration. Le processus utilise alors un autre jeton standard mais qui sera associé au compte administrateur, et donc avec davantage de privilèges.

Lorsque l'UAC est désactivé, un administrateur qui s'authentifie sur le système n'a qu'un seul jeton standard de type `TokenElevationTypeDefault`. Tous les processus sont alors exécutés avec ce jeton et ses privilèges élevés.

2.2 Les manifestes

Certains programmes tels que `regedit.exe` et `mmc.exe` sont toujours exécutés en tant qu'administrateur. Cela se fait au moyen d'options que les développeurs inscrivent dans le fichier « manifeste » de l'application.

Il en existe trois :

- `asInvoker` : l'application sera lancée avec les droits de l'utilisateur ;
- `requireAdministrator` : l'application sera exécutée en tant qu'administrateur ;
- `highestAvailable` : l'application sera exécutée en tant qu'administrateur seulement si l'utilisateur est administrateur.

2.3 UAC et l'intégrité

Les niveaux d'intégrité ont également été introduits avec Windows Vista et fonctionnent en complément de l'UAC. Leur intérêt est principalement, comme leur nom l'indique, de protéger l'intégrité du système d'exploitation. Il existe, par défaut, cinq niveaux d'intégrité : *untrusted*, faible, moyen, élevé, et système.

Le jeton d'un utilisateur standard a un niveau d'intégrité moyen, de même que le jeton « filtré » d'un administrateur. Tous les processus exécutés auront donc par défaut un niveau d'intégrité moyen. En revanche, le deuxième jeton d'un administrateur a un niveau d'intégrité élevé, de même que son jeton standard.

Les fichiers et répertoires ont également des niveaux d'intégrité. En général, la règle *no write up* est définie pour les répertoires et spécifie qu'un processus de niveau strictement plus bas ne peut y écrire. D'autres règles peuvent être appliquées, qui sont *no read up* et *no execute up*. Le « mode protégé » d'Internet Explorer 7 et 8

depuis Windows Vista repose sur ce principe, car il est exécuté avec un niveau faible et ne peut donc écrire par défaut que dans certains répertoires bien spécifiques.

Ces vérifications d'intégrité ne remettent pas en cause le mécanisme de contrôle d'accès discrétionnaire d'un objet qui est vérifié après l'intégrité.

2.4 UIPI

L'UIPI (*User Interface Privilege Isolation*) est un principe utilisant les niveaux d'intégrité qui empêche des processus d'envoyer certains messages (*window messages*) vers d'autres processus de niveau plus élevé. Cela permet d'empêcher certaines attaques de type *shatter attack* qui profitaient de l'envoi de messages entre processus pour exécuter du code avec des privilèges plus élevés. Certaines fonctions sont également limitées pour empêcher notamment les injections de code.

2.5 L'UAC dans Windows 7

Du point de vue d'un utilisateur, l'UAC est une fonctionnalité qui engendre de nombreuses boîtes de dialogue sur lesquelles, de toute manière, on clique toujours sur « oui ». Cela est notamment dû à la mauvaise habitude qu'ont pris les développeurs avec Windows XP de créer des applications qui ne fonctionneront qu'avec des droits administrateur. En créant ce système de jetons liés, Microsoft veut forcer les développeurs à écrire des applications plus propres qui ne nécessitent pas de droits administrateur, sauf pour leur installation.

Cela n'a toutefois pas suffi et, pour satisfaire ses utilisateurs, Microsoft a, dans Windows 7, baissé le niveau par défaut de l'UAC pour ne pas avertir les utilisateurs lorsqu'ils « modifient eux-mêmes les paramètres de Windows. » Par exemple, lorsque l'utilisateur active ou désactive le pare-feu, aucun consentement n'est demandé.

Cela fonctionne au moyen d'une auto-élévation de la part de Windows de certains exécutables. Ceux-ci doivent être signés par l'éditeur de Windows, et se trouver dans certains répertoires spécifiques. Les exécutables doivent également avoir la propriété `autoElevate` dans leur manifeste. Des listes en dur existent aussi pour certains autres exécutables de Windows et les *snap-in* de MMC.

Si cette propriété peut sembler intéressante d'un point de vue ergonomique, il a été démontré qu'elle n'est pas infaillible et qu'il existe des moyens pour des codes malveillants de profiter de l'auto-élévation pour s'exécuter avec des droits élevés. Il est donc fortement recommandé de revenir au niveau par défaut tel qu'il était sur Windows Vista, soit de toujours demander un consentement lors d'une élévation de privilèges.

Pour cela, il faut aller dans :

Panneau de configuration - Comptes d'utilisateurs - Modifier les paramètres de contrôle de compte d'utilisateur. et mettre le niveau à « toujours m'avertir. » Cela correspond au quatrième niveau qui est le plus élevé.

2.6 Conclusion

L'UAC est une fonctionnalité qui, comme toutes les nouveautés, a été critiquée de nombreuses fois. Il a toutefois un intérêt qui réside dans le fait que, depuis Windows Vista, un compte d'administrateur est privé de ses privilèges par défaut et fonctionne de manière semblable à un compte d'utilisateur standard. L'utilisation d'un poste bureautique ne nécessite normalement en aucun cas des droits d'administrateur, si les applications sont développées convenablement.

L'UAC ne doit toutefois pas se substituer à l'utilisation d'un compte standard, lorsque cela est possible. Comme lors de l'utilisation d'un compte standard, il n'empêche pas non plus l'exécution et l'installation de tous les codes malveillants. Dans tous les cas, il est fortement recommandé de le laisser activé et, sous Windows 7, au niveau maximum de demande de consentement.

3 Attaques par dictionnaire

Le SANS relate la découverte d'un script permettant de lancer des attaques par dictionnaire à l'encontre du compte d'administration de *WordPress*. La particularité de ce script est qu'il permet la répartition des attaques depuis plusieurs machines. Le SANS préconise notamment de changer le nom du compte administrateur, d'utiliser des mots de passe forts et de restreindre les accès à l'interface d'administration.

Les attaques par dictionnaire ne sont pas une nouveauté. Par contre, ce qui est original avec ce script, c'est la répartition de la charge de travail entre plusieurs attaquants, et la possibilité d'interrompre l'opération et de la reprendre ultérieurement. La détection de l'attaque dans les journaux devient ainsi plus difficile.

Après SSH et FTP, c'est donc au tour d'un CMS (gestionnaire de contenu) de subir des attaques par dictionnaire. Il ne serait pas surprenant que dans un futur proche, tous les services permettant une authentification par identifiants soient concernés par des tentatives automatisées de ce type. Par conséquent, le CERTA recommande :

- de n'utiliser que des mots de passe forts ;
- de supprimer les comptes inutiles ;
- de restreindre, quand cela est possible, les interfaces de connexion aux adresses IP attendues.

Documentation :

- Article du SANS du 30 novembre 2009 :
<http://isc.sans.org/diary.html?date=2009-11-30>

4 Réponses DNS substituées : L'ICANN met en garde !

Depuis quelques années, certains opérateurs réseaux, dans le but d'offrir un « meilleur service » à leurs clients, et accessoirement de créer de nouveaux revenus via de nouveaux supports de publicité, se sont intéressés de près au DNS (*Domain Name System*, serveur de résolution de nom sur l'Internet). Parmi les pratiques parfois rencontrées, la substitution de « NX Domain » (pour *Non-Existent Domain*, domaine non existant, message normalement renvoyé par un serveur DNS quand l'enregistrement demandé n'existe pas) est ainsi apparue chez certains fournisseurs d'accès. L'idée est ainsi de re-router les connexions d'un utilisateur vers une adresse IP hébergeant par exemple un moteur de recherche.

Le scénario peut être le suivant : un utilisateur fait une faute de frappe en saisissant une adresse dans son navigateur Web. En fonctionnement normal, le serveur DNS qui reçoit la requête devrait renvoyer une réponse « NX Domain » indiquant que le site n'existe pas, ce qui entraîne l'apparition d'une page d'erreur sur le navigateur Web. Si le fournisseur de service (opérant le DNS de l'abonné) a mis en place une substitution de « NX Domain », il peut alors renvoyer en réponse à la requête une adresse IP valide, pointant par exemple sur le portail dudit opérateur (et pourquoi pas, sur un moteur de recherche « maison » copieusement rempli de publicités). Le problème est encore plus grave lors de l'envoi d'un message électronique, car si l'utilisateur rentre par mégarde un nom de domaine inexistant, un opérateur utilisant la substitution de « NX Domain » est alors en mesure d'aspirer ces éléments.

En septembre 2003, Verisign, un des opérateurs de l'infrastructure DNS mondiale avait tenté de mettre en place de telles pratiques, mais le mécontentement global engendré avait forcé cette société à rapidement faire demi-tour (histoire disponible sur <http://www.icann.org/en/topics/wildcard-history.html>).

Fin novembre 2009, l'ICANN est revenue une nouvelle fois sur le sujet des « NX Domain », et maintient un discours strict sur le danger de leur substitution. Avec la création prochaine de nouveaux GTLDs (*Generic top-level domain*), il est important de comprendre que les substitutions de « NX Domain » pourraient entraîner de nombreux problèmes, et ne doivent pas être mises en place. On notera que si l'ICANN se prononce ici spécifiquement à destination des opérateurs de GTLDs, le message est cependant identique pour tous les opérateurs de DNS, quel que soit le niveau. Parmi les problèmes signalés, citons :

- dégradation de l'expérience utilisateur ;
- violation de la confidentialité des données utilisateur, avec potentiel accès à des données qui n'auraient pas dû être envoyées à l'opérateur du service ;
- abus de position de la part de l'opérateur dans la mise en place de cette pratique ;
- risque sur la résilience globale du service DNS.

Le CERTA recommande la plus grande prudence face à ces pratiques, qu'il déconseille fortement.

Documentation

- NXDomain est défini dans les RFC 1034 et RFC 4592 relatives aux noms de domaine :
<http://www.ietf.org/rfc/rfc1034.txt>
<http://www.ietf.org/rfc/rfc4592.txt>
- Recommandation de l'ICANN :
<http://www.icann.org/en/announcements/announcement-2-24nov09-en.htm>

5 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=1937>
- 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/>

6 Rappel des avis émis

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

- CERTA-2009-AVI-514 : Vulnérabilité dans Symantec Altiris
- CERTA-2009-AVI-516 : Multiples vulnérabilités dans les produits Adobe
- CERTA-2009-AVI-517 : Vulnérabilités dans la bibliothèque libvorbis
- CERTA-2009-AVI-518 : Vulnérabilité dans la bibliothèque libtool
- CERTA-2009-AVI-519 : Multiples vulnérabilités dans Cacti
- CERTA-2009-AVI-520 : Vulnérabilité dans kdelibs
- CERTA-2009-AVI-521 : Vulnérabilité dans le service sshd de Sun Solaris
- CERTA-2009-AVI-522 : Vulnérabilités dans MySQL
- CERTA-2009-AVI-523 : Vulnérabilité dans HP Operation Manager
- CERTA-2009-AVI-524 : Vulnérabilités dans IBM WebSphere
- CERTA-2009-AVI-525 : Multiples vulnérabilités dans ActivePerl
- CERTA-2009-AVI-526 : Vulnérabilité dans Ruby on Rails
- CERTA-2009-AVI-527 : Vulnérabilité dans Asterisk
- CERTA-2009-AVI-528 : Multiples vulnérabilités des systèmes FreeBSD

Pendant la même période, les avis suivants ont été mis à jour :

- CERTA-2009-AVI-448-001 : Vulnérabilités dans Xpdf et dérivés (ajout des références CVE et des bulletins de sécurité Red Hat, SuSE, Ubuntu et Debian)
- CERTA-2009-AVI-482-001 : Vulnérabilité du protocole SSL/TLS (ajout du bulletin de sécurité Sun)
- CERTA-2009-AVI-510-001 : Multiples vulnérabilités dans PHP (ajout des références CVE et des bulletins de sécurité Debian et SuSE)
- CERTA-2009-AVI-515-001 : Vulnérabilité dans BIND avec DNSSEC (ajout du bulletin de sécurité Sun)

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique63.html

8 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.

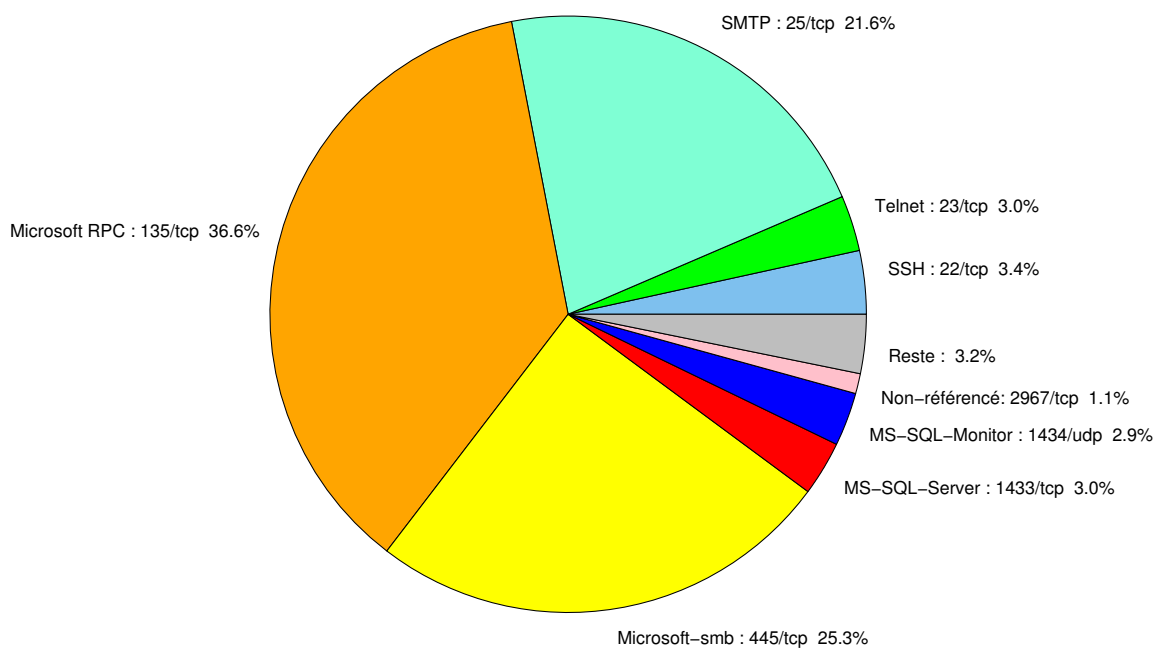


FIG. 1: Répartition relative des ports pour la semaine du 27 novembre au 03 décembre 2009

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	36.55
445/tcp	25.33
25/tcp	21.59
22/tcp	3.43
23/tcp	3.01
1433/tcp	2.95
1434/udp	2.89
80/tcp	1.99
2967/tcp	1.08
4899/tcp	0.6
21/tcp	0.54
3128/tcp	0.48
3389/tcp	0.18

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	9
3	Paquets rejetés	10

Gestion détaillée du document

04 décembre 2009 version initiale.