



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 novembre 2007
N° CERTA-2007-ACT-048

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-48

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-2007-ACT-048>

Gestion du document

| | |
|-----------------------------|------------------------------|
| Référence | CERTA-2007-ACT-048 |
| Titre | Bulletin d'actualité 2007-48 |
| Date de la première version | 30 novembre 2007 |
| 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-2007-ACT-048.pdf>

Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-048/>

1 Des incidents traités cette semaine

1.1 Collecter le maximum d'informations

Cette semaine, le CERTA a traité un incident suite à la découverte dans des journaux de tentatives d'exploitations de *php include* par un site de l'administration. L'analyse du serveur a montré qu'il était lui-même vulnérable à ce type d'attaque. L'exploitation a résulté en l'exécution de bots IRC et l'utilisation du serveur comme plate-forme pour la recherche et la compromission d'autres machines.

Aucune porte dérobée n'a été installée sur le serveur et seuls des scripts d'automatisation de la recherche de sites vulnérables ont été téléchargés sur la machine. Les bots IRC s'exécutaient dès la réalisation du *php include* et n'étaient donc pas présents sur le disque.

Une copie de la mémoire vive, du *swap* et des résultats de commandes simples lancées par l'administrateur (*netstat*, *lsof*, ...) sur le serveur compromis ont été déterminants pour l'analyse de cet incident, car ils ont permis de rapidement préciser :

- la localisation immédiate de la page vulnérable au *php include* ;
- le type de bot IRC exécuté et son fonctionnement ;

- au moins une partie des commandes réalisées par l’attaquant ;
- les scripts qui ont été téléchargés.

Les copies de partitions classiques sont souvent les seuls éléments envoyés au CERTA pour analyse. Cet incident montre l’utilité d’autres éléments qui peuvent être déterminants, notamment l’exécution de commandes élémentaires sur la machine compromise, la copie de la mémoire vive, et la copie de la mémoire d’échange (*swap*). Il est cependant important de limiter les interactions avec la machine compromise pour ne pas effacer de traces ; il faut donc utiliser des commandes ou des outils peu intrusifs sur le système, qui sont également maîtrisés, et si possible après avoir effectué une copie physique des disques. Le CERTA reste à la disposition de ces correspondants en cas de difficulté pour effectuer ces opérations.

Une note d’information présente les bons réflexes à avoir en cas d’intrusion sur un système d’information : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/>

1.2 Les dangers de l’hébergement mutualisé

Cette semaine le CERTA a traité un incident impliquant un serveur mutualisant l’hébergement de sites Internet. L’adresse IP de ce serveur a été observée dans plusieurs tentatives d’attaques par injection de code arbitraire sur des sites web. Après avoir pris connaissance de ces attaques, le CERTA a contacté le responsable du serveur d’où proviennent les attaques en lui fournissant des traces issues des journaux des connexions de certains sites web ciblés.

Le serveur à l’origine de l’attaque mutualise plusieurs dizaines de sites web rendant difficile l’identification de l’origine de l’attaque :

- il peut y avoir un site hébergé compromis ;
- il peut y avoir l’exploitation d’une faille d’un service du serveur ;
- il peut y avoir un mot de passe faible donnant accès à l’un des sites hébergés ;
- ...

La solution de l’hébergement mutualisé doit être considérée avec précaution, comme abordée dans la note d’information CERTA-2005-INF-005. Pour éviter ce type de compromission, le CERTA rappelle que les connexions sortantes d’un serveur web peuvent être filtrées. Afin de ne pas compromettre la sécurité de l’ensemble des sites web mutualisés, il convient de maîtriser la sécurité de chaque site : par l’application et le suivi des correctifs de sécurité, l’analyse régulière des journaux des connexions, une politique de mot de passe adéquate, ...

Documentation

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

2 Alerte QuickTime et le protocole RTSP

2.1 Historique

Le CERTA a publié cette semaine une alerte concernant Apple QuickTime. Elle mentionne le protocole permettant d’établir et de contrôler des flux synchronisés de médias continus, RTSP (pour *Real Time Streaming Protocol*).

La vulnérabilité concerne l’interprétation des trames de réponse retournées par le serveur, au cours d’une tentative de connexion. Des codes d’exploitation sont largement diffusés sur l’Internet. Ils fonctionnent sur plusieurs systèmes d’exploitation, comme Windows XP SP2 ou MacOS Tiger et Leopard (versions PowerPC et Intel).

Les échanges se font en principe via les ports TCP et UDP 554, comme l’indique l’IANA dans la liste qu’elle maintient :

<http://www.iana.org/assignments/ports-numbers>

Cependant, cela ne signifie par que tout trafic passant par ces ports correspond au protocole RTSP, et réciproquement, que tout trafic RTSP circule par ces ports. Le serveur peut être configuré pour écouter sur un port quelconque. Le client, lui, se connecte au serveur de la manière suivante :

```
rtsp://Mon_Adresse_de_Serveur_Multimedia/MonFichier:Port_de_connexion
```

Le filtrage des connexions sortantes est donc une bonne mesure, mais n'est pas suffisante.

Si ce protocole n'est pas utilisé, il convient alors de configurer les applications pour ne pas l'interpréter par défaut, et surtout de ne pas l'associer à une version de QuickTime vulnérable. Le CERTA rappelle à cette occasion que l'alerte du 04 janvier 2007 CERTA-2007-ALE-001 impliquait ce même protocole ainsi que l'application Apple QuickTime. La vulnérabilité était différente et consistait en un manque de contrôle sur les liens, ou URLs de type `rtsp://...`

Les navigateurs Internet Explorer 7 et Firefox v. 2.0.0.10 ne gèrent plus par défaut ce protocole. En revanche, ce n'est pas le cas de tous les navigateurs (cf. Safari). Un utilisateur peut également cliquer suite à une sollicitation quelconque sur un fichier de type `.qt1` malveillant qui pourrait également chercher à communiquer avec le serveur distant.

Pour ces raisons, l'alerte CERTA-2007-ALE-017 cite plusieurs contournements provisoires, qui consistent surtout à désactiver la gestion du protocole : cela peut se faire au niveau de l'interface de configuration de QuickTime, ou des bases de registres pour le système Windows.

<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-017/>

2.2 Recommandations

De manière générale, il est important de configurer avec soin toute application avant son utilisation. Il faut être très méfiant vis-à-vis des installations par défaut. Elles tendent en principe à « faciliter » la vie de l'utilisateur, mais sont souvent très laxistes en terme de sécurité. A valeur d'illustration, plusieurs applications proposent à leur installation d'être systématiquement associées à plusieurs types d'extension (formats de fichiers). Si ces derniers ne sont pas utilisés, comme cela peut être le cas de certains formats multimédias, alors l'association entre l'extension et l'application ne doit pas être autorisée.

3 Compte administrateur et *sudo* sous MacOS

Plusieurs systèmes d'exploitation comme MacOS X ou Ubuntu utilisent une technique permettant de ne pas fixer un mot de passe pour le compte *root* ou compte « super-utilisateur ».

Une personne malintentionnée ne pourra ainsi pas attaquer ce mot de passe soit par un dictionnaire soit par force-brute.

Il est cependant indispensable de garder la possibilité pour un simple utilisateur d'effectuer des tâches administratives comme les mises-à-jour, la configuration d'un service réseau ou l'activation d'un composant matériel. Dans ce cas, des droits administrateur sont requis. Or sans mot de passe, il est impossible de se connecter en tant que super-utilisateur. C'est pourquoi les systèmes d'exploitation précédemment cités mettent en œuvre des techniques utilisant la commande *sudo*. C'est-à-dire qu'un utilisateur particulier de l'ordinateur (souvent l'utilisateur courant) aura le droit par le biais de cette commande d'effectuer des actions normalement réservées au seul compte *root*.

Ce qui pourrait paraître pour une bonne solution ici n'en est pas forcément une. En effet, cette commande *sudo* n'est souvent pas suffisamment bornée et permettra par exemple à l'utilisateur privilégié d'exécuter successivement de nouveaux « shell » ou invites de commande en tant que *root* sans entrer de nouveau le mot de passe. Cette élévation de privilèges reste ainsi valable pendant plusieurs minutes. L'utilisateur pourra alors exécuter toutes les commandes du système pendant ce temps imparti.

On a donc juste déplacé le problème car celui qui connaît le mot de passe de l'utilisateur est virtuellement déjà super-utilisateur. On pourrait avancer que l'utilisateur doit retaper son mot de passe lors de l'utilisation de la commande mais là encore, le choix qui a été fait par défaut concernant ce comportement n'est pas parfait. Il est fréquent qu'un délai soit autorisé entre deux commandes *sudo* pendant lequel aucun mot de passe n'est nécessaire. Ainsi on tape son mot de passe une seule fois au départ puis pendant une minute par exemple il n'est plus nécessaire pour utiliser *sudo*. On peut imaginer dès lors une attaque en deux temps où un utilisateur malintentionné invite, par le biais d'un tutoriel par exemple, à une commande anodine en tant que super-utilisateur puis à exécuter un script « magique » qui vous apporte la dernière fonctionnalité à la mode... En guise de nouvelles fonctions il a alors tous les privilèges pour installer ce qu'il veut, y compris une porte dérobée sur l'ordinateur...

Il est à noter, par ailleurs, que le problème se pose sur les systèmes précédemment cités mais qu'il est transposable aux systèmes d'exploitation de type Windows qui, par défaut, donnent des droits administrateur au compte courant.

3.1 Recommandations :

Il existe des solutions pour parer à ce type de problème mais la démarche reste toujours identique :

- utiliser des mots de passe robustes ;
- créer un compte standard ne pouvant pas utiliser `sudo` pour toutes les tâches quotidiennes (surf, messagerie, bureautique...) ;
- n'utiliser le compte privilégié que lorsqu'il est nécessaire d'effectuer des tâches administratives indispensables.

4 Actualité Microsoft

Microsoft a fait l'objet de nombreux articles dans l'actualité cette semaine. Le CERTA revient tout particulièrement sur les éléments suivants :

4.1 Vulnérabilité Macrovision

Le CERTA tient à mettre en garde les utilisateurs de l'application Macrovision SafeDisc 4.x de l'exploitation en cours d'une vulnérabilité permettant à un utilisateur local malintentionné d'élever ces privilèges. Un correctif est disponible chez l'éditeur et a fait l'objet de la publication de l'avis CERTA-2007-AVI-480. Il est donc important d'appliquer le correctif ou de prendre les mesures nécessaires afin d'empêcher l'utilisation de cette vulnérabilité par toute personne malveillante.

4.2 Le protocole WPAD

Le protocole WPAD ((Web Proxy Automatic Discovery)) permet à un poste client d'obtenir automatiquement les informations de connexion au serveur mandataire. Une vulnérabilité datant de mars 2007, pour laquelle le CERTA avait émis l'avis CERTA-2007-AVI-276 fait l'objet, à la date de rédaction de ce bulletin, de plusieurs articles dans la presse spécialisée. Cette vulnérabilité a été corrigée par Microsoft et mentionnée dans son bulletin KB934864 du 23 mars 2007. Le problème évoqué dans les médias est que le service WPAD peut être activé par défaut dans certaines versions de Microsoft Windows. Il est fortement recommandé que le navigateur soit configuré afin de ne pas rechercher automatiquement les informations relatives au serveur mandataire. L'option « Détection automatiquement les paramètres réseaux » ne doit pas être active. Celle-ci est accessible via les « paramètres réseaux » de l'onglet « connexions » de la fenêtre « options Internet » disponible dans le « panneau de configuration » de Microsoft Windows. Le CERTA rappelle qu'il est important de maintenir tous les applicatifs installés et le système d'exploitation à jour.

4.3 Microsoft FTP Client

Le logiciel (Microsoft FTP Client) a fait l'objet de nombreuses discussions relatives à une vulnérabilité permettant un dépassement de mémoire tampon. Le service ne gère pas correctement les informations fournies avec les commandes de type `mget`, `dir` ou `ls`. Cette vulnérabilité permet une exécution de code arbitraire avec les privilèges de l'utilisateur connecté. L'exploitation de cette vulnérabilité ne serait exploitable que lorsque l'utilisateur lance de son propre chef un script ou tape une commande particulière caractérisée par sa longueur excessive. L'impact reste donc limité mais le CERTA rappelle qu'il est important de ne pas exécuter un script inconnu et de vérifier préalablement les actions entreprises par celui-ci avant de le lancer.

Documentations

- Avis CERTA-2007-AVI-480 du 07 novembre 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-480/>
- Avis CERTA-2007-ACT-013 du 30 mars 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-013.pdf>

5 Découverte de trafic pair-à-pair

La politique de sécurité appliquée pour certains réseaux spécifie que le trafic pair-à-pair est à éviter, notamment s'il n'est pas utilisé dans le cadre du travail. L'objectif de ce court paragraphe n'est pas de justifier ou non cette politique. Ce débat est largement médiatisé.

Il est en revanche important de se poser les bonnes questions, si jamais un tel trafic est bien en désaccord avec la politique de sécurité, et est détecté. Une première réaction de l'administrateur consiste bien souvent à couper les connexions impliquées, comme les ports. Les adresses IP de source ou destination peuvent faire l'objet de nouvelles règles de filtrage particulières.

Il faut également s'assurer que :

- le logiciel client sur le poste de l'utilisateur est proprement désinstallé, et ne laisse pas des portes ouvertes rémanentes ;
- l'utilisateur est sensibilisé à cette action ;
- il faut comprendre quelles informations ont pu être échangées. Cela implique de vérifier la configuration du logiciel client sur le poste de l'utilisateur avant sa désinstallation.

Ce dernier point est important. Une mauvaise configuration (par défaut ou intentionnelle) peut mettre en partage sur le réseau pair-à-pair des données plus sensibles que celles initialement voulues par l'utilisateur. Elles sont devenues publiques.

Il est donc important de traiter ce type de violation de la politique de sécurité comme tout autre incident : le traitement doit être complet.

6 Moteurs de recherche : la chance m'accompagne... (*I'm feeling (un)lucky*)

Quoi de plus inoffensif qu'un moteur de recherche, pense-t-on souvent. L'utilisateur tape les mots-clés de sa recherche, puis le résultat du moteur s'affiche avec les réponses que le moteur estime pertinentes. Les sites affichés sont « référencés » par le moteur de recherche, qui utilise avant d'afficher son choix une moulinette complexe basée sur la visite régulière de sites, et l'indexation de l'information trouvées sur les pages.

Il est possible de voir, à la fin du mois de novembre, plusieurs techniques d'exploitation des moteurs de recherche à des fins malveillantes. Ces techniques consistent à forcer le référencement de sites contenant du code malveillant, afin que ces sites soient dans les premières réponses d'une requête courante. Cela peut se faire en trompant les robots des moteurs de recherche qui visitent les pages sur l'Internet. Par exemple, cette semaine, le fait de chercher sur le site www.google.com les mots "*christmas*" "*gift*" et "*sold*" renvoyait à l'utilisateur plusieurs sites malveillants parmi les dix premières réponses.

Ces sites malveillants peuvent avoir plusieurs comportements :

- téléchargement d'un fichier malveillant (virus, cheval de troie, etc.) ;
- exploitation d'une faille du navigateur ;
- utilisation détournée de la consultation du site (pour augmenter un compteur de visite) ;
- etc.

Google a enlevé ces sites dangereux « trop » référencés. Le problème est bien entendu indépendant du moteur de recherche, et le scénario reste valable pour les autres. Il faut cependant bien comprendre ici que les sites de moteurs de recherche n'apportent pas de garantie sur les résultats affichés. Ces derniers sont le fruit d'une décision arbitraire du moteur qui peut faire l'objet d'un biais exploité par des personnes malveillantes.

Ces techniques ne sont pas nouvelles, mais peuvent devenir problématiques dès lors que les principes de sécurité de base ne sont pas respectés. Ainsi, il est vivement recommandé de prendre l'habitude de naviguer sur Internet en ayant désactivé par défaut toute interprétation de code dynamique (Javascript, Java, ActiveX, ...). Une fois que le site visité est considéré comme sûr, ce code dynamique peut être réactivé si nécessaire. Certains moteurs de recherche présentent également au préalable un extrait du contenu du site, qui reste intéressant à regarder. Par ailleurs, il est toujours envisageable d'utiliser des moteurs de recherche alternatifs, afin de croiser les informations retournées.

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 22 et le 29 novembre 2007.

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 23 au 30 novembre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-509 : Vulnérabilités dans Mozilla Firefox
- CERTA-2007-AVI-510 : Multiples vulnérabilités dans Wireshark
- CERTA-2007-AVI-511 : Vulnérabilités dans Symantec Backup Exec for Windows Server

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 œuvre (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.

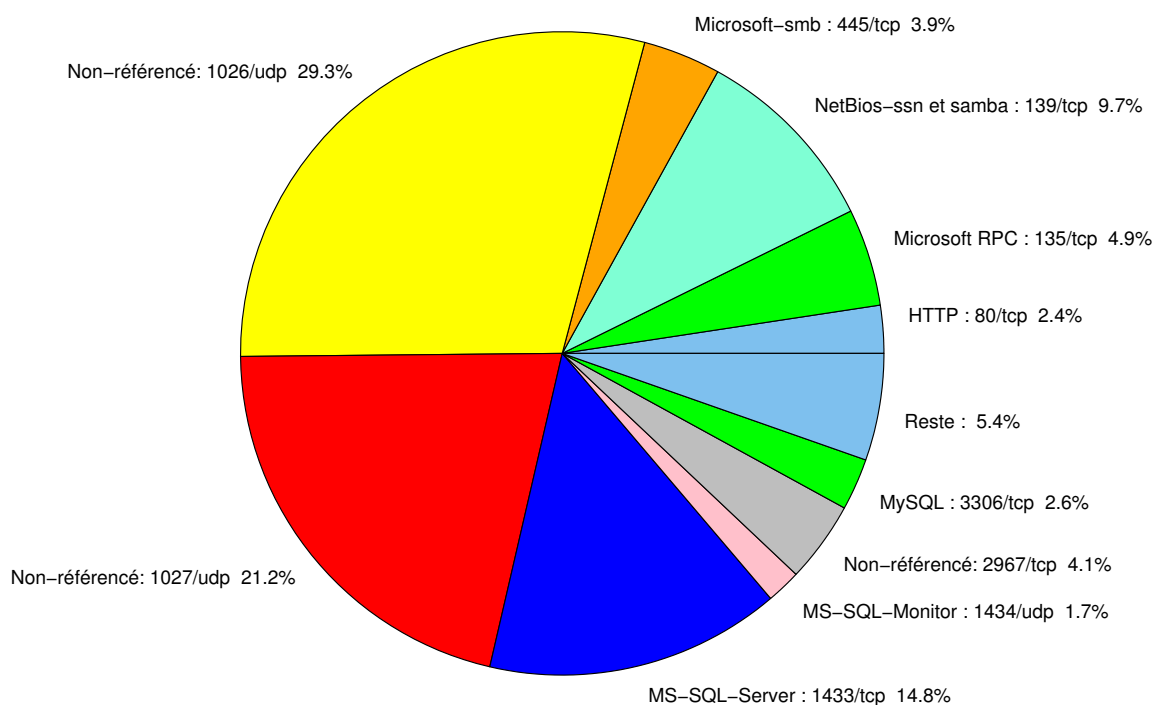


FIG. 1: Répartition relative des ports pour la semaine du 22.11.2007 au 29.11.2007

| 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 |
|----------|-------------|
| 443/tcp | 85.92 |
| 80/tcp | 3.25 |
| 1026/udp | 1.96 |
| 1433/tcp | 1.82 |
| 1027/udp | 1.61 |
| 25/tcp | 1.03 |
| 135/tcp | 0.93 |
| 139/tcp | 0.68 |
| 3306/tcp | 0.62 |
| 2967/tcp | 0.35 |
| 445/tcp | 0.31 |
| 22/tcp | 0.29 |
| 1080/tcp | 0.24 |
| 137/udp | 0.22 |
| 23/tcp | 0.2 |
| 1434/udp | 0.18 |
| 2100/tcp | 0.08 |
| 4899/tcp | 0.06 |
| 143/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

30 novembre 2007 version initiale.