

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-47

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-047>

Gestion du document

Référence	CERTA-2007-ACT-047
Titre	Bulletin d'actualité 2007-47
Date de la première version	23 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-047.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-047/>

1 Les incidents traités cette semaine

1.1 Guppy et ses mises à jour

Le CERTA a récemment traité une compromission de serveur web suite à l'exploitation d'une vulnérabilité de *Guppy*. Cette attaque était similaire à celles décrites dans le bulletin d'actualité CERTA-2007-ACT-017 du 27 avril 2007. Cet incident était particulièrement intéressant parce que la version de *Guppy* installée était 4.5.18 alors que la vulnérabilité exploitée est censée être corrigée dans la version 4.5.17.

Se pose alors la question suivante : comment l'intrusion a-t-elle été possible ?

La réponse provient directement du site <http://www.freeguppy.org> (site officiel de *Guppy*) : la vulnérabilité n'a pas été correctement corrigée par la version 4.5.17. Il existe depuis le 10 novembre 2007 une version 4.5.19. Toutefois, les développeurs de *Guppy* recommandent de migrer en version 4.6, ce qui peut poser des problèmes de compatibilité de certains modules.

Il est important de préciser qu'il existe parfois deux types de correctifs (suivant les versions) sur le site de *Guppy* : les mises à jour totales et les correctifs non cumulatifs. L'installation d'un correctif non cumulatif de *Guppy* entraîne un changement de version (visible en bas de page) mais est susceptible de ne corriger qu'une partie des vulnérabilités. En particulier, le correctif 4.5.19 est non cumulatif, et il est essentiel d'installer la mise à jour 4.5.18 complète avant.

Documentation

- Avis CERTA-2007-AVI-507 (Vulnérabilité dans GuppY) :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-507/>
- Bulletin d'actualité CERTA-2007-ACT-017 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-017.pdf>

1.2 Les sites mourants

Cette semaine le CERTA a traité le cas d'un site officiel explicitement vulnérable. Les responsables ont été appelés et il s'est avéré qu'il s'agit d'un site plutôt ancien (développé il y a plus de cinq ans), dont la réalisation avait été externalisée et qui devrait bientôt être refait.

L'absence de connaissance interne ne permet pas une correction rapide. La maîtrise de l'existant peut être longue. Le site devant être refait, l'exploitant n'est pas enclin à investir dans ce maintien du site actuel.

Ce cas est le résultat d'une succession d'événements :

1. le développement initial du site n'a pas pris en compte plusieurs problématiques de sécurité ;
2. l'externalisation du site s'est déroulée sans prise de connaissance particulière des détails techniques de la mécanique du site ;
3. le site a continué de vivre pendant plusieurs années sans préoccupation majeure de la part des administrateurs.

Des solutions palliatives provisoires limitent les risques. Dans le cas présent, une première solution consiste à utiliser des règles de filtrage d'un relais mandataire (*reverse proxy*). En parallèle, une surveillance permanente permettrait au moins de détecter l'exploitation de la vulnérabilité identifiée. Il ne s'agit malheureusement que de solutions temporaires et qui peuvent aussi donner un faux sentiment de correction définitive.

1.3 Un faux sentiment de sécurité

Cette semaine le CERTA a traité deux incidents de sécurité liés à la compromission de site web. Le premier site web a été compromis à cause d'un défaut de mise à jours d'un CMS, le second par un manque de protection d'une variable passée en argument. L'analyse des serveurs a révélé la présence de codes malveillants, notamment des outils de prise de contrôle et d'attaque à distance (PHP Shell).

Les responsables des deux sites web ont été surpris d'apprendre et de constater la présence de codes malveillants car ils utilisaient régulièrement des antivirus et d'autres outils de détection de codes malveillants. Ces outils n'ont cependant pas détecté l'intégralité des codes malveillants, notamment les PHP Shell.

Les bonnes pratiques pour contrôler un site web consistent à :

- suivre les évolutions et mettre à jour les applications utilisées ;
- limiter les composants de CMS au strict nécessaire ;
- contrôler régulièrement l'intégrité des données et des fichiers présents sur le serveur pour détecter une modification, un ajout, ... ;
- analyser régulièrement les journaux des connexions pour permettre de mettre en évidence une compromission effective ou une tentative.

2 Les applications clés-en-main

2.1 La problématique

Le CERTA, informé par ses homologues étrangers de certains incidents rencontrés, tient à rappeler les risques liés à l'utilisation d'offres applicatives « tout-en-un ». L'incident en question, une défiguration, s'est déroulé sur un serveur Microsoft Windows avec EasyPHP. Cette suite d'applications comporte un serveur Apache, PHP, MySQL, l'interface d'administration phpMyAdmin ainsi qu'une configuration par défaut. Le principe est d'offrir une solution simple pour que des utilisateurs non expérimentés puissent créer des serveurs web en quelques clics.

Ceci peut toutefois poser certains problèmes au niveau de la sécurité :

- une suite peut contenir des applications qui ne sont pas à jour et difficiles à mettre à jour ;
- il est possible que la suite d'applications soit peu maintenue par des développeurs moins actifs qu'au lancement du projet ;

- la configuration par défaut peut être insuffisante pour sécuriser le serveur et restera souvent en l'état car le public visé n'a pas toujours les compétences suffisantes en administration.

L'incident en question concernait une configuration par défaut laissée telle quelle par l'utilisateur, notamment les mots de passe. L'intrus qui a défiguré le site a ainsi pu s'y connecter en effectuant une attaque par recherche exhaustive (force brute).

D'autres applications ont déjà fait l'objet d'articles par le CERTA (cf. bulletin d'actualité CERTA-2007-ACT-035).

En plus des problèmes présentés ci-dessus qui dépendent surtout de la volonté ou des moyens de l'éditeur, on peut en citer deux autres liés intrinsèquement à l'utilisation de produits « tout-en-un » :

- certaines des applications installées ne sont peut-être pas nécessaires pour l'utilisateur et leur présence augmente les risques de vulnérabilités ainsi que la surface d'attaque ;
- un grand nombre de services sont lancés sur la même machine et non sur des machines séparées comme cela est généralement recommandé.

Ces deux derniers points sont également des problématiques concernant les *matériels* « tout-en-un, » qui peuvent tout faire mais présentent généralement des risques accrus pour un administrateur.

2.2 Recommandations

L'utilisation d'applications « tout-en-un » est généralement déconseillée pour des systèmes qui seront connectés à l'Internet. Dans le cas où celles-ci sont malgré tout utilisées, il est important de veiller aux mises à jour de chaque application, de désinstaller si possible les applications non-utilisées, de vérifier la configuration du système et de changer les mots de passe.

Références

- Les installations de systèmes clés-en-main, bulletin d'actualité CERTA-2007-ACT-035 : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-035.pdf>

3 Il n'y a rien d'intéressant sur la machine !

Lors du traitement des incidents, il est courant d'entendre : « De toute façon, il n'y a rien qui pourrait intéresser un pirate sur ma machine ! »

Dans l'esprit de l'utilisateur, cette remarque sonne comme un moyen de défense contre de potentielles critiques et remarques qu'il s'attend de recevoir. Il est important de décomposer ce qu'est un ordinateur et les différentes exploitations qu'il offre à une personne malintentionnée.

Un ordinateur est composé de ressources, parmi lesquelles :

- un accès à l'Internet qui permet à l'individu malveillant d'envoyer des pourriels ou de participer à une attaque en déni de service, ou encore l'anonymisation de requêtes grâce à l'installation d'un serveur proxy ;
- de la mémoire vive qui offre la possibilité de récolter des données sensibles comme les habitudes de navigations, les mots de passe, etc. ;
- de disques durs permettant le stockage d'information et de données : l'intrus peut héberger des données illicites.

Au final, les données utilisateurs stockées volontairement sur la machine ne sont pas les seules cibles des intrus. La puissance de calcul et l'accès Internet sont aussi attractives pour les personnes malveillantes, comme les données qui ne font qu'y transiter (mots de passe, coordonnées bancaires, etc.). C'est le principe des outils de capture de frappes clavier (*keylogger*) par exemple.

Le CERTA rappelle donc qu'il est important de n'utiliser que des postes de confiance pour être connecté sur l'Internet.

4 Nouvelle alerte au ver via Microsoft Live Messenger

Un nouveau cheval de Troie a fait son apparition début novembre. Il se propage via le logiciel de messagerie instantanée Microsoft Live Messenger. Comme dans de précédentes versions, une personne de la liste de contacts propose de télécharger un fichier. Ce fichier tente de passer pour une photo grâce à un nom proche de ceux générés par des appareils photos, par exemple *DSC00123.jpg.exe* ou *IMG1234.jpg.pif*. Une fois installé, ce code

malveillant rebondit via la liste de contacts de Live Messenger et recherche des machines offrant la possibilité de se connecter à distance via le logiciel VNC. La multiplication des vecteurs de propagation permet à ce code malveillant de construire rapidement un réseau d'ordinateurs zombies. Il a également la particularité d'essayer de récupérer les fichiers contenant des mots de passe pour les envoyer ensuite vers un site central. Le CERTA préconise de vérifier auprès des contacts que l'envoi des fichiers provient effectivement d'eux avant de les télécharger. Il est de plus possible d'effectuer une vérification antivirale des fichiers téléchargés en activant l'option se situant dans Windows Live Messenger. Cette option permet de contrôler la présence de certains virus dans les fichiers téléchargés via Windows Live One Care ou un antivirus tiers.

Le CERTA rappelle enfin que Microsoft Live Messenger, comme plusieurs logiciels équivalents, souffrent de vulnérabilités fréquemment rendues publiques. L'article du bulletin CERTA-2007-ACT-038

5 L'intégrité du fichier *.htaccess*

Le CERTA a signalé à de nombreuses reprises qu'il est important de vérifier régulièrement l'intégrité des pages Web. Celles-ci peuvent ne pas subir de changement visible, mais avoir des modifications dans leur code source, afin d'injecter des données malveillantes : fraude au clic, cadre IFRAME pointant vers des pages dangereuses, etc.

Une autre technique a été observée lors de l'analyse d'un serveur Web compromis. Il s'agit de la modification du fichier *.htaccess*. Ce dernier, combiné au module Apache *mod_rewrite*, peut être utilisé pour écrire différemment les URLs demandées à la volée, à partir d'expressions régulières.

Il est donc possible d'y ajouter les lignes suivantes :

```
RewriteEngine On
(...)
RewriteRule ^pageXXXX/(.+)$/evil/maPageMalveillante
```

Toute personne cherchant à contacter par exemple http://Mon_site/pageXXXX/script.php?id=4 sera directement redirigée vers http://Mon_site/evil/maPageMalveillante.

L'intérêt pour la personne malveillante est de centraliser toutes les tentatives de navigation sur le site victime, quelle que soit la page demandée, vers celles qu'il vient d'insérer.

Cette attaque nécessite un accès préalable au fichier *.htaccess*.

Le CERTA insiste donc sur l'importance de vérifier l'intégrité non seulement les pages du site Web, mais également des fichiers système.

- Apache Tutorial: *.htaccess* files :
<http://httpd.apache.org/docs/2.2/howto/htaccess.html>
- Apache Module *mod_rewrite* :
http://httpd.apache.org/docs/2.2/mod/mod_rewrite.html

6 Un besoin d'anonymat ?

6.1 Les solutions à la mode

La presse spécialisée se fait le relais de nombreuses solutions pour préserver l'anonymat sur l'Internet. On y trouve des extensions de navigateurs, comme par exemple le bouton Tor (Torbutton), les proxies garantissant « l'anonymat gratuitement » comme Proxify, ou des navigateurs dédiés, comme Torpark (XeroBank Browser). Les solutions disponibles sur l'Internet sont nombreuses, et l'utilisateur n'a que l'embarras du choix.

Qu'entend-on par anonymat ? Il s'agit en principe de l'état d'une chose ou d'une personne, dont on ignore l'identité. En d'autre terme, pour une personne connectée à l'Internet, l'anonymat n'a de sens qu'en précisant qui constate l'état.

Si l'on considère les solutions maintenues par des tiers, comme les proxies Web, il n'y a pas de garantie d'anonymat. Ce service tiers fait une promesse, offre beaucoup de garanties dans sa section de questions fréquentes (FAQ), mais dans tous les cas, les informations personnelles arrivent jusqu'à lui. L'anonymat n'est donc évidemment pas préservé, puisque des données permettant une identification sont fournies sur un système qui n'est pas de confiance.

Si l'on considère les solutions de « tunnel », ou d'encapsulation comme Tor, il est important de comprendre qu'elles ne garantissent pas « l'anonymat », mais assurent en théorie qu'il est difficile de faire le lien entre une connexion entrant dans le tunnel et une sortante. Pas plus, pas moins.

Si l'on considère les proxies locaux, a-t-on une garantie ? Prenons l'exemple simple d'un courrier électronique. Il se compose de plusieurs éléments. On trouve notamment dans l'en-tête l'adresse de l'émetteur, la machine

émettrice ainsi que diverses adresses IP. D'autres éléments peuvent s'y ajouter. Rendre le courrier anonyme revient-il à supprimer ou dissimuler les noms et adresses IP des machines ? Faut-il aussi ôter l'adresse électronique de l'émetteur ? D'autres éléments ?

Dans ces hypothèses, des informations sur l'identité peuvent encore être visibles dans le corps du message, comme la signature, voire aussi les pièces jointes (documents personnels, CVs, etc.). Garantir l'anonymat est donc une tâche extrêmement complexe, et bien souvent utopique.

Comme toute technique, il est important de comprendre ce qu'on utilise. Le risque peut être, dans le cas contraire, accru par une méconnaissance des solutions employées.

6.2 Revue de quelques caractéristiques

La presse a signalé ces dernières semaines la récupération de nombreux identifiants et mots de passe par une personne. Celle-ci a opéré de la manière suivante : elle a capturé toutes les trames au niveau de nœuds de sortie du réseau Tor. Or Tor ne chiffre pas le trafic entre le nœud de sortie de Tor et la machine destinataire. Les personnes se connectant sans chiffrement particulier à leurs serveurs de messagerie via Tor ont pu voir leurs identifiants dérobés de cette manière.

Dans l'autre sens, des utilisateurs du bouton Tor n'ont pas la garantie que tout leur trafic passe bien le réseau Tor. En effet, ce dernier est une extension du navigateur, qui joue le rôle d'un proxy. Rien n'impose, par exemple, aux autres extensions, d'utiliser la configuration du proxy indiquée. Des développeurs ont proposé récemment, au cours d'une conférence de sécurité, d'éviter ce problème, en désactivant toutes les extensions à partir du moment où le bouton est activé. Cela comprend donc les extensions utilisées pour filtrer les codes dynamiques, vérifier les sites possibles de filoutage, etc.

La question n'est pas de donner raison ici à l'une ou l'autre de ces initiatives, mais bien de réaliser que de telles solutions ont des limitations. Celles-ci peuvent d'ailleurs évoluer au cours du temps.

Il peut être parfois plus dangereux d'utiliser de telles solutions en méconnaissant leurs limitations. Dans le cas des nœuds de sortie mentionnés ci-dessus, les utilisateurs n'auraient peut-être pas été aussi « ciblés » s'ils avaient eu le comportement normal d'autres utilisateurs n'ayant pas la conscience des risques.

6.3 Les recommandations du CERTA

La difficulté principale pour utiliser ces outils n'est pas leur mise en place, mais la compréhension complète du fonctionnement. Une solution dédiée à la sécurité n'a de valeur que si elle est totalement maîtrisée et ses limites comprises.

Cette attitude est valable quel que soit l'outil. Ces commentaires restent donc valables pour les déploiements de solutions antivirales ou de détection d'intrusion (IDS) par exemple.

6.4 Documentation associée

- Wiki du projet Onion Router, "Can exit nodes eavesdrop on communications? Isn't that bad?" : <http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#ExitEavesdroppers>
- Wiki du projet Onion Router, "So I'm totally anonymous if I use Tor?" : <http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#TotallyAnonymous>
- "Securing the Tor Network", M. Perry : <http://www.blackhat.com/presentations/bh-usa-07/Perry/Whitepaper/bh-usa-07-perry-WP.pdf>
- "A tor, et à travers...", Sid, 19 novembre 2007 : <http://sid.rstack.org/blog/index.php/233-tor-et-travers>

7 Routeurs et interface d'administration

Le bulletin d'actualité CERTA-2007-ACT-043 détaillait les risques associés aux accès sans fil sur des éléments d'un système d'information comme des imprimantes ou des routeurs. On s'attardera cette semaine sur ces derniers et plus particulièrement sur leur interface d'administration souvent constituée d'un serveur web léger et de pages en HTML enrichies parfois de javascript. Comme expliqué dans ce précédent article, il est délicat de mettre à jour cette interface bien qu'elle soit vulnérable.

En effet, le CERTA a pu rencontrer des cas où des routeurs comportaient une interface d'administration vulnérable à des attaques de type XSS (Cross-Site Scripting) pour lesquelles la mise à jour tardait à être

publiée par l'éditeur, tout du moins pour la version traduite en français. La mise à jour se faisant par une écrasement du micrologiciel (*firmware*), remplacer une version française par une version anglaise peut poser des problèmes comme la perte de fonctionnalités, ou rendre des commandes inopérentes. . . . On pourrait arguer qu'il n'est pas essentiel de mettre à jour ce composant dans la mesure où l'accès à l'interface d'administration vulnérable ne peut se faire qu'en interne à partir du réseau local. Cependant, le CERTA a eu connaissance de différentes méthodes permettant à un attaquant de contourner cet écueil. Par exemple, en utilisant des techniques de type *DNS Spoofing*, il sera possible à un attaquant via le navigateur d'une personne du réseau local de conduire une attaque de type injection de code indirecte (*Cross-Site Scripting*). La technique du `dns pinning` a été présentée dans le bulletin CERTA-2007-ACT-028 du 13 juillet 2007.

Qui plus est, si les identifiants d'accès à l'interface d'administration n'ont pas été changés après l'installation, l'attaquant pourra avoir la totale maîtrise du routeur en ajoutant des règles d'accès ou en configurant l'équipement dans un mode laxiste.

Concernant ces routeurs, il est donc indispensable d'appliquer les correctifs dès qu'ils sont disponibles et de bien veiller à les configurer correctement : mot de passe robuste, filtrage le plus précis et le plus restrictif possible. Enfin, ces équipements sont souvent capables de journaliser leur fonctionnement. Il est donc recommandé d'analyser régulièrement les journaux.

8 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 15 et le 22 novembre 2007.

9 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/>

10 Rappel des avis émis

Dans la période du 16 au 22 novembre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-500 : Multiples vulnérabilités du Firewall Mac OS X 'Tiger'

- CERTA-2007-AVI-501 : Multiples vulnérabilités d'IBM DB2
- CERTA-2007-AVI-502 : Vulnérabilités dans Samba
- CERTA-2007-AVI-503 : Vulnérabilité dans Citrix Presentation Server
- CERTA-2007-AVI-504 : Vulnérabilité dans Cacti
- CERTA-2007-AVI-505 : Vulnérabilités dans Mozilla Thunderbird
- CERTA-2007-AVI-506 : Vulnérabilité dans Alcatel OmniPCX Enterprise Communication Server
- CERTA-2007-AVI-507 : Vulnérabilité dans GuppY
- CERTA-2007-AVI-508 : Vulnérabilité de phpMyAdmin

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

- CERTA-2007-AVI-348-002 : Multiples vulnérabilités dans la machine Java d'IBM (ajout de la référence au bulletin de sécurité HP OpenView)
- CERTA-2007-AVI-409-001 : Multiples vulnérabilités dans les produits VMware (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2007-AVI-440-001 : Multiples vulnérabilités dans la machine virtuelle JAVA (JRE) de SUN (ajout de la référence au bulletin de sécurité HP-UX)
- CERTA-2007-AVI-469-001 : Vulnérabilité dans IBM Lotus Domino (mise à jour du risque, de la description et des références)

11 Actions suggérées

11.1 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.

11.2 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.

11.3 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.

11.4 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.

11.5 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.

11.6 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.

11.7 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>

12 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.

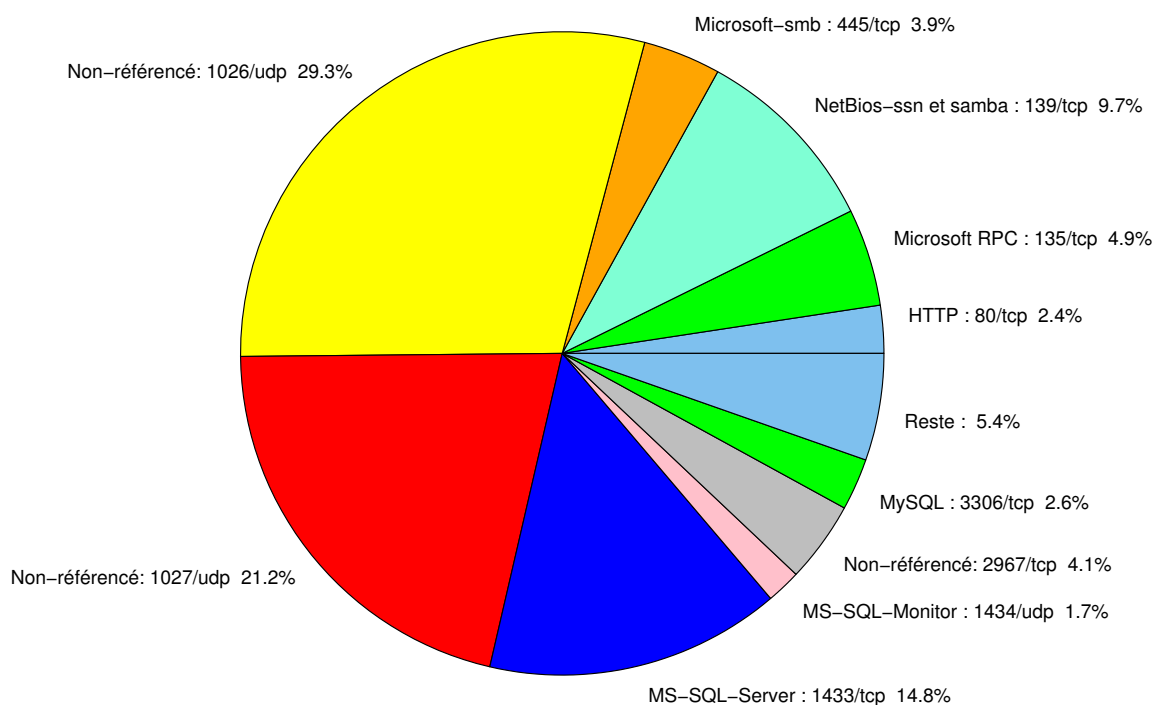


FIG. 1: Répartition relative des ports pour la semaine du 15.11.2007 au 22.11.2007

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	11
3	Paquets rejetés	12

Gestion détaillée du document

23 novembre 2007 version initiale.