Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juin 2008
N° CERTA-2008-ACT-026

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-26

Gestion du document

Référence	CERTA-2008-ACT-026
Titre	Bulletin d'actualité 2008-26
Date de la première version	27 juin 2008
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

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

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-026.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-026/

1 Incident de la semaine

Résilience DNS et déni de service

Le CERTA a traité cette semaine, un incident qui pouvait laisser croire à un déni de service sur plusieurs serveurs web simultanément. Mais après une rapide vérification, il n'en était rien. En effet, une première analyse a permis de constater que les serveurs prétendument indisponibles étaient hébergés par une seule et même entité.

Rapidement, on pouvait constater que le serveur DNS principal de cet hébergeur était injoignable tandis que leur "secondaire" fonctionnait très bien. L'indisponibilité constatée venait donc du fait que la résolution de nom ne fonctionnait plus pour les domaines concernés.

Cependant, l'hébergeur mettant à disposition un serveur secondaire pour la zone, la résolution aurait du fonctionner tout de même. D'ailleurs en interrogeant ce serveur DNS secondaire, on obtenait bien une résolution de nom satisfaisante.

Une investigation plus approfondie fut donc nécessaire et permis de mettre en évidence le fait qu'en utilisant différents serveurs DNS chez différents FAIs, la résolution fonctionnait ou pas. Ainsi, en utilisant les DNS d'un FAI X, les sites étaient résolus alors qu'avec le FAI Y, la résolution ne fonctionnait pas.

Il semble donc que certains serveurs DNS mettant en cache les enregistrements des zones pour lesquelles ils ne sont pas autorités, ne le fassent qu'en se basant sur un seul des serveurs DNS autorités de ces zones.

Ainsi, si ce DNS autorité particulier vient à tomber, les caches ne consulteront pas le second pour obtenir des enregistrements valides. À expiration du délais de conservation en cache, le domaine sera considéré comme inexistant par ce serveur cache DNS.

C'est exactement, ce que le CERTA a constaté dans le cadre de cet incident. En fonction du serveur DNS public utilisé pour résoudre les noms de domaines des machines 'en déni de service', les serveurs web étaient joignables ou pas.

Ceci montre bien que la constatation d'un déni de service sur des machines distantes est hautement subjective. Il peut très bien arriver que ce soit un équipement de l'observateur lui-même ou dans la chaîne de routage de l'information qui soit à l'origine du prétendu déni de service. Auquel cas, il n'y a en aucun cas un déni de service pour le reste de l'Internet. Seul, le recoupement entre plusieurs points de mesures pertinents permet de déterminer de façon fiable si il y a ou pas un réel déni de service.

2 Des protocoles anodins ?

2.1 Introduction

Il existe une multitude de protocoles déployés de nos jours, quel que soit leur positionnement dans les couches du modèle de référence OSI (*Open System Interconnection*). Ils apparaissent pour répondre à la nécessité de nouvelles technologies et de besoins opérationnels. Il n'est pas toujours évident pour un administrateur réseau de s'y retrouver et d'avoir une compréhension complète des activités qui semblent circuler dans son système.

À cette multitude de protocoles, il ne faut pas négliger certaines vicissitudes des plus anciens d'entre eux. Le CERTA revient dans ce bulletin en particulier sur l'un d'eux : ICMP (*Internet Control Message Protocol*).

Ce protocole ne se limite pas qu'à la seule fonction de « ping » (ECHO Request et Reply, de type 8 et 0), mais il permet aussi, comme le précise les standards RFC 792 et 1122 (pour ICMPv4) :

– le signalement d'erreurs bénignes (*soft errors*) ;
– le signalement d'erreurs graves (*hard errors*).

Parmi les signalements possibles, il peut s'agir :

– de l'impossibilité d'atteindre le destinataire (type 3) ;
– de la gestion des flux et des congestions réseau (type 4, code 0) ;
– de la découverte du MTU (*Maximum Transfer Unit*) d'un chemin réseau (RFC 1191, type 3 et code 4) ;
– etc.

Des fonctions similaires sont apportées par la version ICMPv6 dans ses RFC respectifs.

2.2 Détails concernant la gestion des erreurs

Le standard initial ne précise malheureusement pas le comportement à adopter lors de la réception de messages de signalement d'erreurs ICMP. Il précise uniquement que des actions doivent être prises.

Pour faciliter la compréhension de l'erreur, une partie de la trame initiale ayant provoqué la dite erreur est reprise dans le paquet ICMP (l'en-tête IP et les 64 premiers bits du reste en général). Il peut s'agir du début d'en-tête TCP, ce qui permet finalement de récupérer l'ensemble (IP source, port source, IP destination, port destination) qui caractérise la session posant problème.

Le port source diffère souvent à chaque nouvelle session mais peut rester relativement prévisible. Il faut également noter que le numéro de séquence TCP peut être également inclus dans les données ICMP (64 premiers bits de l'en-tête TCP).

2.3 Exemple de risques

Certaines mises en oeuvre de TCP / IP réagissent de manière dangereuse à la réception de telles trames. Elles peuvent ne pas vérifier, par exemple, la cohérence de la réception ICMP par rapport au contenu de la trame ou le suivi du numéro de séquence.

On peut donc imaginer le scénario suivant.

Forger un paquet IP avec les caractéristiques suivantes :

```
IP source : une adresse quelconque, qui sera considérée comme un noeud intermédiaire
IP destination : l'adresse d'une machine A
```

```
Type ICMP : Type 3, Code 2 (Protocol Unreachable)
Valeurs TCP/IP reprises dans la trame ICMP :
adresse IP source : celle de la machine A d'où proviendrait l'erreur
adresse IP destination : l'adresse d'une machine B (par exemple un serveur web)
port source : XXX
port destination : port cible, par exemple 80/tcp
```

Ce scénario peut provoquer sous certaines conditions la rupture de communication TCP entre la machine A et le serveur web B. L'une des raisons est que le routeur réceptionnant le paquet ne va pas nécessairement vérifier la cohérence du contenu dans la trame ICMP. La seule difficulté réside à prévoir le port source utilisé dans la communication initiale. Ce n'est pas une tâche impossible.

Un scénario identique peut être appliqué avec la classe ICMP (type 4, code 0, *ICMP Source Quench*) pour modifier le comportement dans le réseau et tricher sur les bandes passante disponibles. D'autres sont envisageables.

Le lecteur comprendra ici que plusieurs malversations sont envisageables. Des outils sont disponibles sur Internet et en mettent certaines à disposition par simple "clicks".

2.4 Recommandations

2.4.1 Filtrage ICMP

Les trames ICMP ne peuvent pas être considérées *a priori* comme de confiance. Leur filtrage doit être fait de la manière la plus rigoureuse possible en fonction des besoins.

Ce filtrage doit prendre en compte non seulement le protocole, mais toutes les spécificités de son en-tête pour restreindre les trames autorisées à circuler.

L'opération de filtrage s'effectue au niveau des postes utilisateurs ou dans les équipements réseaux.

2.4.2 Mises à jour

Des mises à jour sont parfois fournies par les constructeurs. Il faut donc vérifier régulièrement les nouvelles disponibilités et appliquer avec toutes les précautions d'usage ces mises à jour sur les systèmes, y compris les boitiers routeurs ou pare-feux. Certains correctifs vérifient maintenant, par exemple, la pertinence du numéro de séquence TCP retourné dans la trame ICMP. Elle doit correspondre plus ou moins à celle attendue des données envoyées mais dont la réception n'a pas été confirmée (ACK). Une personne malveillante devra alors déterminer à la fois le port source de la communication et une valeur de séquence adéquate. Cette vérification est effectuée par des systèmes d'exploitation depuis quelques années (BSD). Elle n'est cependant pas suffisante dans le cas où les trames peuvent être interceptées (réseau Wi-Fi ouvert, hub, etc.).

2.4.3 Configurations par défaut

Il est de bon usage de modifier les configurations par défaut, et en particulier les ports d'écoute comme pour les proxy web.

2.5 Documentation

- RFC 1122 : "Requirements for Internet Hosts - Communication Layers" :
  http://www.faqs.org/rfcs/rfc1122.html
- RFC 1191 : "Path MTU Discovery" :
  http://www.faqs.org/rfcs/rfc1191.html
- RFC 4301 : "Security architecture for the Internet Protocol" :
  http://www.faqs.org/rfcs/rfc4301.html
- OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection, H. Zimmermann, avril 1980 :
  http://www.comsoc.org/livepubs/50_journals/pdf/RightsManagement_eid=136833.pdf
- F. Gont, "Attacks against TCP", mai 2005 :
  http://www.gont.com.ar/drafts
  http://www.gont.com.ar/advisories

3 NetBios sous Mac OS X Leopard

Dans un but d'interopérabilité maximale, Apple a activé par défaut le support du protocole NetBios sur la dernière version de son système d'exploitation Mac OS X Leopard (Mac OS version 10.5). Ce protocole développé à l'origine par IBM et Sytec servant essentiellement au partage de ressources sur un réseau est utilisé majoritairement par Microsoft pour son système d'exploitation Windows. NetBios comprend, en particulier, un service de nommage permettant d'identifier de façon unique sur un réseau différentes machines ainsi que leurs services associés (partage de fichiers, d'imprimantes, ...).

Or ce service de nommage fonctionne sur un principe d'inondation réseau (*broadcast*) pour découvrir d'autres machines disponibles. Ceci occasionne du trafic sur le réseau car les machines s'annoncent et s'enquièrent régulièrement.

Le service de nommage de Netbios peut servir à une personne malintentionnée pour collecter des informations sur les machines présentes sur le réseau via quelques requêtes judicieusement choisies.

Jusqu'à la version 10.4 ou Tiger de Mac OS X, il est assez aisé de désactiver la mise en œuvre du protocole Netbios en ajustant les services démarrés dans Applications/Utilitaires/Format de répertoire. Il suffit dans ce menu de décocher la case SMB/CIFS. Il n'en va pas de même pour la version 10.5 (Leopard). L'utilitaire Format de répertoire n'est plus présent dans les Applications. Il convient donc de manipuler les fichiers de configuration du serveur samba intégré à Mac OS X. Pour ce faire, on éditera le fichier */etc/smb.conf* et on rajoutera dans la section [Global] les deux lignes suivantes :

```
disable netbios = yes
smb ports = 445
```

On pourra également désactiver, si cela n'est pas déjà fait, le service de nommage nmbd en tapant la ligne suivante :

```
sudo launchctl unload -w /System/Library/LaunchDaemons/nmbd.plist
```

Les modifications ne seront prises en compte qu'au prochain redémarrage.

Dans une optique de défense en profondeur, il est rappelé que le pare-feu dans Mac OS X Leopard n'est pas activé par défaut et que l'on peut remédier à cela en cochant la case : *Définir l'accès de certains services et applications* dans le menu : Préférences Système/Sécurité/Coupe-feu.

4 Vulnérabilité non corrigée de Mac OS X

Une vulnérabilité non corrigée dans le système d'exploitation Apple a été découverte la semaine dernière. Cette faille permet d'effectuer une élévation de privilège en local sur les machines installées avec Mac OS X dans sa version 10.5.

Cette vulnérabilité exploite une faiblesse de l'agent *ARD* (Apple Remote Desktop), utilitaire permettant une prise de contrôle à distance de la machine. Afin de déterminer si une machine est vulnérable il suffit de lancer la commande suivante :

```
osascript -e 'tell application "ARDAgent" to do shell script "whoami"'
```

Si cette commande retourne *root*, cela signifie que l'élévation de privilège est possible. De nombreux codes malveillants exploitant cette vulnérabilité circulent sur l'Internet. Des personnes malveillantes ont profité de cette faille de sécurité pour développer des chevaux de Troie et autres codes malveillants l'exploitant. L'installation de ces codes nécessite néanmoins une action de l'utilisateur afin de lancer leur exécution.

Il existe un moyen de se protéger de cette vulnérabilité. Il suffit de lancer la commande suivante :

```
sudo chmod u-s
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent
```

Cette commande permet de retirer le bit définissant l'utilisateur (ici *root*) lançant l'application. Après cette opération, si la première commande est relancée, elle doit retourner le nom de l'utilisateur connecté à la machine.

Le CERTA tient donc à alerter ces lecteurs et recommande les actions suivantes :

- appliquer le correctif détaillé ci-dessus ;
- ne pas cliquer sur un lien ou un fichier non sûr ;
- ne pas utiliser de compte avec des droits d'administration lorsque cela n'est pas nécessaire.

5 Un "mode protégé" pour *Mozilla Firefox*

Windows Vista a apporté une nouveauté qui est le « mode protégé » d'Internet Explorer 7. Ceci correspond à l'exécution du processus `iexplore.exe` en mode d'intégrité faible. Dans ce mode, à cause de la règle par défaut *NoWriteUp* (`NW` dans `icacls`) qui est utilisée, Internet Explorer ne peut que écrire dans des objets ayant un niveau également faible. Ces objets sont d'autres processus ou des fichiers, par exemple. Les répertoires usuels (favoris, historique, fichiers temporaires, etc.) ont justement un niveau faible pour permettre cela. Deux processus supplémentaires (appelés *broker processes*) sont également utilisés : `IEInstal.exe` et `IEUser.exe`. Le premier s'exécute en mode d'intégrité élevée et sert notamment pour installer des contrôles `ActiveX`, le second s'exécute en mode d'intégrité moyen et permet notamment à un utilisateur de sauvegarder des fichiers en dehors de « zones faibles » .

Une couche de compatibilité (virtualisation propre à Internet Explorer) redirige également les tentatives d'écriture par des modules additionnels, par exemple. Ainsi des tentatives d'écriture vers des répertoires de niveau moyen ou vers la ruche HKCU sont redirigées vers un répertoire et une clé spécifiques :

```
"Documents and Settings\%USERPROFILE%\AppData\Local\Microsoft\WindowsTemporary
Internet Files\Virtualized"

"HKCU\Software\Microsoft\Internet Explorer\InternetRegistry"
```

Enfin, Internet Explorer étant « virtualisé » (pas la version 64 bits), ce schéma existe aussi pour les actions de l'utilisateur (sauvegardés dans le *VirtualStore*) :

```
"%USERPROFILE%\Appdata\Local\VirtualStore".
```

En ce qui concerne *Mozilla Firefox*, il était annoncé qu'il ait également un « mode protégé » avec la version 3 mais cela ne semble finalement pas être le cas. Il est toutefois possible de s'en rapprocher en forçant le programme à se lancer en niveau faible et en changeant les niveaux d'intégrité des répertoires utilisés. L'exemple ci-dessous concerne *Mozilla Firefox* 2.0.0.14 :

Pour toujours exécuter *Firefox* en mode d'intégrité faible (nb : toutes les commandes sont à exécuter dans une invite de commandes en tant qu'administrateur) :

```
icacls "%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe" /setintegritylevel low
```

Remarque : attention, les mises à jour de *Firefox* peuvent remettre l'exécutable en niveau moyen par défaut.

Le niveau d'intégrité du répertoire contenant le profile de l'utilisateur dans lequel *Firefox* a besoin de pouvoir écrire doit également être changé :

```
icacls "%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<profile>"
/setintegritylevel (ui)(ci)low
```

Puisqu'il est maintenant impossible de sauvegarder des fichiers dans des « zones moyennes », il est préférable de créer un répertoire de sauvegarde par défaut (modifiable dans Outils - options - Général) de niveau faible :

```
mkdir "%USERPROFILE%\Desktop\Save-low"

icacls "%USERPROFILE%\Desktop\Save-low\  /setintegritylevel (ui)(ci)low
```

Mozilla Firefox utilisant le répertoire "%USERPROFILE%\Appdata\Local\Temp" comme répertoire temporaire, il faudrait également changer son niveau d'intégrité. Puisqu'il est utilisé par d'autres programmes, il serait en fait plus propre de forcer Firefox à utiliser le répertoire "%USERPROFILE%\Appdata\Local\Temp\Low" qui a déjà un niveau d'intégrité faible. Cela ne semble toutefois pas possible pour le moment. On peut donc soit décider de modifier le niveau du répertoire utilisé actuellement, soit accepter le fait que certaines fonctionnalités (mises à jour de modules additionnels, téléchargements par le navigateur) ne fonctionneront pas (sauf avec une exécution explicite en mode administrateur). Il faut d'ailleurs noter que la mise à jour du navigateur ne fonctionne plus et qu'il faut la faire manuellement.

Enfin, l'exécution de *Mozilla Firefox* en mode d'intégrité faible donne un message d'avertissement à chaque fois. Il est possible de s'en débarrasser en créant le raccourci suivant :

```
cmd.exe /c "%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe"
```

Comme on peut le voir, créer une sorte de « mode protégé » pour *Mozilla Firefox* est possible mais nécessite quelques concessions. Selon Mozilla, un véritable « mode protégé » devrait apparaître avec *Firefox* 3.1 ou 4.0.

5.1 Documentation

– Wiki Mozilla - A quand le mode protégé dans Firefox?
http://wiki.mozilla.org/Mozilla_2/Protected_Mode

6 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 19 et le 26 juin 2008.

7 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/

8 Rappel des avis émis

Dans la période du 20 au 26 juin 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-326 : Vulnérabilité dans Adobe Flex 3
– CERTA-2008-AVI-327 : Vulnérabilité dans Perl
– CERTA-2008-AVI-328 : Vulnérabilité dans Sun Java System Calendar Server
– CERTA-2008-AVI-329 : Vulnérabilité de l'implémentation TCP sous FreeBSD
– CERTA-2008-AVI-330 : Vulnérabilité de Novell eDirectory
– CERTA-2008-AVI-331 : Vulnérabilité du navigateur Safari
– CERTA-2008-AVI-332 : Multiples vulnérabilités dans HP Storage Management Appliance
– CERTA-2008-AVI-333 : Vulnérabilité dans Sun Solaris
– CERTA-2008-AVI-334 : Vulnérabilité dans phpMyAdmin
– CERTA-2008-AVI-335 : Vulnérabilité dans Novell GroupWise
– CERTA-2008-AVI-336 : Vulnérabilité dans les produits Adobe
– CERTA-2008-AVI-337 : Multiples vulnérabilités du serveur CIFS de HP-UX

- CERTA-2008-AVI-338 : Vulnérabilité dans Cisco Wide Area Application Services
- CERTA-2008-AVI-339 : Vulnérabilités dans Cisco Unified Communications Manager
- CERTA-2008-AVI-340 : Vulnérabilité dans Cisco VPN Client

- CERTA-2008-AVI-225-001 : Multiples vulnérabilités dans PHP (ajout des références aux CVE et au bulletin de sécurité Fedora)
- CERTA-2008-AVI-252-001 : Multiples vulnérabilités du noyau Linux (ajout de la référence au bulletin de sécurité OpenSUSE)
- CERTA-2008-AVI-300-002 : Vulnérabilité dans OpenOfficeorg (ajout de la référence au bulletin de sécurité Red Hat.)
- CERTA-2008-AVI-314-001 : Multiples vulnérabilités dans FreeType (ajout de la référence au bulletin de sécurité Sun)
- CERTA-2008-AVI-317-001 : Multiples vulnérabilités dans XOrg (ajout des référence aux bulletins de sécurité Suse et Sun.)
- CERTA-2008-AVI-320-001 : Vulnérabilités dans le navigateur Opera (ajout des références aux CVE et au bulletin de sécurité OpenSUSE)

9 Actions suggérées

9.1 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 règlementaire, 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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 inexpliqués 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.

9.7 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

10 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

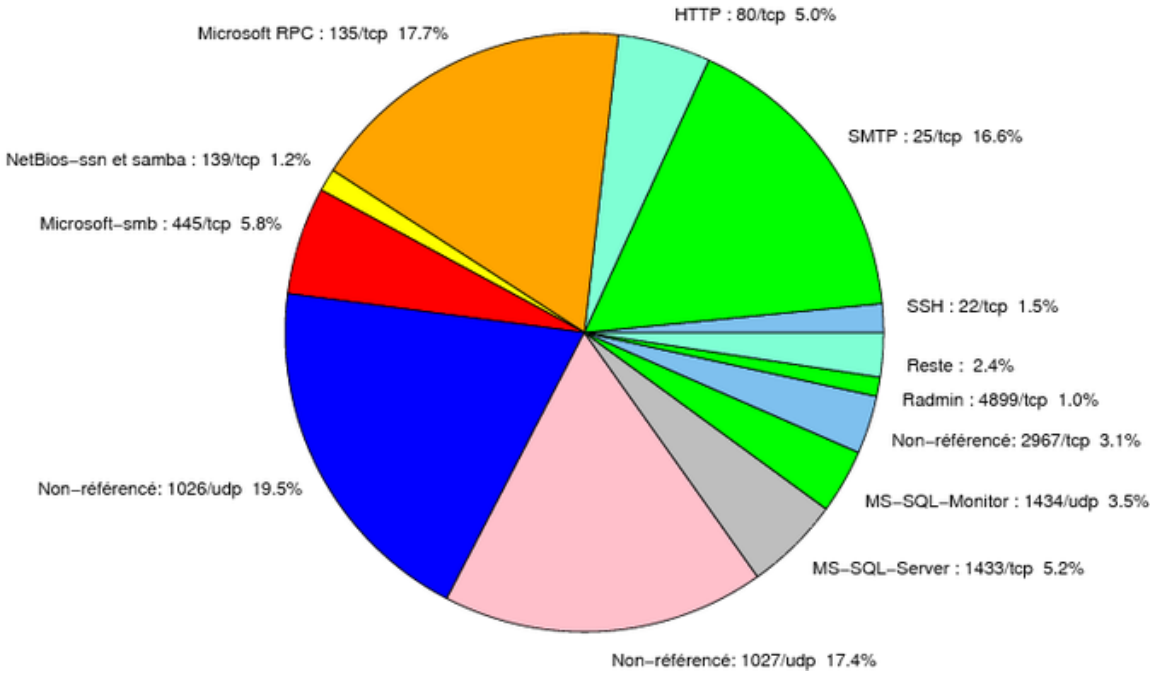

FIG. 1: Répartition relative des ports pour la semaine du 19.06.2008 au 26.06.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CERT
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CERT
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CERT
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CERT
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CERT
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT

6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CERT
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CERT
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CERT
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CERT
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CERT
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CERT

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

port	pourcentage
1026/udp	19.48
135/tcp	17.7
1027/udp	17.42
25/tcp	16.62
445/tcp	5.8
80/tcp	5.24
1433/tcp	5.15
1434/udp	3.46
2967/tcp	3.13
22/tcp	1.54
139/tcp	1.21
4899/tcp	1.03
3306/tcp	0.56
137/udp	0.42
143/tcp	0.23
3128/tcp	0.14
3389/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

27 juin 2008 version initiale.