

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-24

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-2008-ACT-024>

Gestion du document

Référence	CERTA-2008-ACT-024
Titre	Bulletin d'actualité 2008-24
Date de la première version	13 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-024.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-024/>

1 Les incidents de la semaine

1.1 Le phishing d'un site de vente en ligne

Cette semaine, le CERTA a traité un incident relatif au filoutage (ou *phishing*) d'un site de vente en ligne. Le site utilise un portail pour vendre les différents services qu'il propose. En analysant les statistiques de connexions, le responsable s'est rendu compte qu'un site qu'il ne connaissait pas le référençait (visible par le champ REFERER de l'en-tête HTTP fourni dans les journaux). En se rendant sur ce site, il a constaté qu'il reproduisait à l'identique son site légitime, utilisant le même nom de service, la même charte graphique, les mêmes images, les mêmes références clients, ... Les seuls changements portaient sur les tarifs pratiqués et les coordonnées de contacts.

Le CERTA rappelle que les escroqueries, comme le *phishing*, ne touchent pas que les banques ou les fournisseurs d'accès. Ils peuvent viser tout service en ligne sur Internet.

L'utilisateur doit donc rester vigilant et méfiant au cours de sa navigation, et ne pas fournir trop rapidement ses identifiants de connexion.

L'administrateur doit, comme il a été fait ici, surveiller avec attention ses journaux de connexion afin de déceler toute anomalie ou mettre en évidence des phénomènes étranges.

1.2 Compromissions en série

1.2.1 Présentation des faits

Cette semaine le CERTA a participé au traitement d'un incident relatif à la compromission de plusieurs sites Internet. Ces sites étaient tous co-hébergés sur le même serveur. Il a en fait suffi à l'attaquant de profiter de la vulnérabilité d'un des sites présents pour compromettre tous les autres et mettre en péril la sécurité du serveur. En effet, la même archive de kit de filoutage a pu être déployée sur tous les sites. Il est important de souligner qu'une telle compromission de masse n'a nécessité que l'exécution d'une seule commande sur le serveur.

Le CERTA rappelle qu'en matière d'hébergement mutualisé, il convient de respecter certaines bonnes pratiques, comme certaines décrites dans la note d'information du CERTA CERTA-2005-INF-005.

1.2.2 Documentation

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

2 A propos du contournement de MS08-033

L'avis CERTA-2008-AVI-307 qui concerne des vulnérabilités corrigées dans *Microsoft DirectX* est décrit par Microsoft dans son bulletin de sécurité MS08-033. Dans celui-ci, Microsoft propose un contournement provisoire qui consiste à modifier les ACL (*Access Control List*) du fichier `quartz.dll` ou de désactiver cette bibliothèque dans le registre. `quartz.dll` est une bibliothèque contenant des fonctions pour `DirectShow`, une partie de `DirectX`. Ce contournement a également été conseillé pour d'autres bulletins concernant *DirectX*, par exemple MS07-064 et MS06-005. Il peut être intéressant de l'appliquer pour des administrateurs qui ne peuvent effectuer les mises à jour immédiatement.

Pour restreindre les droits en modifiant les ACL, les commandes à taper sont les suivantes :

Sur Windows XP (avec un compte administrateur) :

```
Echo y| Cacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /E /P everyone:N
```

Sur Windows Vista (sous une invite de commandes ouverte en tant qu'administrateur) :

```
Takeown.exe /f %WINDIR%\SYSTEM32\QUARTZ.DLL  
Icacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /save %TEMP%\QUARTZ_ACL.TXT  
Icacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /deny everyone:(F)
```

Pour remettre les droits originaux :

Sur Windows XP :

```
Cacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /E /R everyone
```

Sur Windows Vista :

```
Icacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /grant everyone:(F)  
Icacls.exe %WINDIR%\SYSTEM32 /restore %TEMP%\QUARTZ_ACL.TXT
```

L'autre contournement consiste à désactiver `quartz.dll` :

```
Regsvr32.exe -u %WINDIR%\SYSTEM32\QUARTZ.DLL
```

Pour le réactiver :

```
Regsvr32.exe %WINDIR%\SYSTEM32\QUARTZ.DLL
```

`quartz.dll` étant un composant majeur de `DirectShow`, ces contournements ont des impacts qui peuvent être non négligeables. En effet, `DirectShow` est un *framework* (environnement de travail) multimédia utilisé par certaines applications sous Windows. Les effets de bord sont cependant différents selon le système d'exploitation. Ainsi, sur Windows XP, aucun fichier ne pourra être interprété dans une application utilisant `DirectShow`. Sur Windows Vista, seule la lecture des fichiers `.avi` et `.wav` avec des applications utilisant `DirectShow` serait concernée. Le lecteur Windows Media Player est notamment affecté par cet effet de bord.

2.1 Documentation

- Avis CERTA-2008-AVI-307, « Vulnérabilités dans Microsoft DirectX », 11 juin 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-307/>
- Entrée sur le bloc-notes Technet « Security Vulnerability Research and Defense » du 10 juin 2008 :
<http://blogs.technet.com/swi/archive/2008/06/10/ms08-033-so-what-breaks-when-you-acl-quartz-dll.aspx>
- Bulletin de sécurité Microsoft MS08-033 du 10 juin 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-033.mspx>

3 Les codes malveillants chiffnants

Une nouvelle variante d'un code malveillant a fait son apparition récemment. Cette dernière répond au nom de *gpcode.ak*. Elle est la dernière évolution d'un code aux manières un peu particulières : les victimes de ce programme constatent le chiffrement de l'ensemble des fichiers ayant une extension particulière (.doc, .txt, .pdf, .xls, .jpg, ...) selon les versions. Pour retrouver l'usage de ces fichiers, il est demandé de payer (\$100 ou \$200 ?) afin d'obtenir le programme de déchiffrement. Ce type de programme est connu sous le terme *ransomware*¹.

Si ce type de code malveillant n'est pas nouveau cette version pose toutefois des problèmes. Les anciennes versions avaient pu être déjouées grâce à un défaut dans l'implémentation de l'algorithme de chiffrement et ainsi permettre le déchiffrement des fichiers sans avoir à payer cette rançon. Cette nouvelle variante ne fait malheureusement pas la même erreur. La taille de la clé de chiffrement (1024 bits) ainsi que l'algorithme utilisé (RSA) ne permettent pas de trouver une méthode de décryptement.

Différentes initiatives, plus ou moins critiquables et critiquées, ont été lancées afin de trouver une solution à ce code malveillant. Par exemple, des projets de collaborations appelant toute personne volontaire à contribuer à la recherche d'un remède efficace ont été créés. A ce jour, aucun moyen n'est à disposition pour récupérer des données modifiées par ce code. Une signature de ce dernier est cependant disponible.

Le CERTA tient à rappeler l'ensemble des bonnes pratiques afin de limiter les risques d'infection et leurs impacts :

- faire des sauvegardes régulières ;
- ne pas stocker de données sensibles sur un poste exposé ;
- prendre les précautions d'usage pour prévenir les intrusions :
 - disposer d'un système d'information à jour (système d'exploitation, applicatifs, antivirus, ...) ;
 - ne pas ouvrir de pièce jointe dans un courriel ne provenant pas d'une source de confiance ;
 - ouvrir les courriels au format texte ;
 - ne pas cliquer sur des liens non sûrs ;
 - désactiver l'exécution des codes dynamiques du type JavaScript et flash de son navigateur.

4 Adobe 9 et autres nouveautés

Plusieurs sources sur l'Internet, dont Adobe, confirment l'arrivée prochaine de la version 9 de Adobe Reader. Cette nouvelle version sera, en outre, accompagnée d'une suite de logiciels enrichissant le catalogue des produits proposés par Adobe. Concernant Adobe Reader, il sera possible parmi les nouveautés avec la prochaine version d'inclure du contenu Flash (.swf) dans un fichier au format PDF (.pdf).

Le CERTA rappelle que la technologie Flash n'est pas sans risque (cf. CERTA-2008-ACT-016) et que, par conséquent, les risques liés à cette technologie pourront se retrouver également dans les fichiers PDF de dernière génération.

Pour mémoire il est possible, par exemple, avec la dernière version de Flash, d'utiliser des ressources réseau (*sockets*) dans le contexte de la lecture d'un fichier .swf. On comprend dès lors que le format Flash n'est plus un format statique sans interaction forte avec son environnement.

Quant à la suite logicielle qui sera proposée par Adobe, elle comprendra, à l'image d'un concurrent dans le domaine, un traitement de texte en ligne, un outil de travail collaboratif en ligne, un outil d'échange de fichiers et un convertisseur "universel" de fichiers en PDF. Tous ces outils, bien qu'installés en partie sur la machine, utiliseront des composantes distribuées en ligne. Dans ce contexte, il devient assez difficile de savoir quelle est la part de traitement qui est faite « en local » de la part réalisée en ligne. Cela complexifie la maîtrise des informations traitées localement de celles envoyées « pour traitement » sur un serveur distant. Ce type d'outil pose des problèmes évidents de confidentialité.

4.1 Recommandations

Dans un cas comme dans l'autre, le CERTA recommande la plus grande prudence vis-à-vis de ces technologies qui, certes, apportent de nouvelles fonctionnalités mais entraînent surtout d'inquiétants problèmes de confidentialité et plus généralement de sécurité.

¹cf. terminologie du CERTA, CERTA-2006-INF-002

5 SNMP : une gestion dangereuse ?

5.1 La gestion de réseau

La gestion des réseaux n'est pas une tâche évidente. Elle impose souvent de connaître l'état des équipements, comprendre leurs demandes, voire aussi modifier certains paramètres de configuration. Pour cela, des architectures de communication sont mises en place. Elles recourent souvent à un protocole : SNMP (pour *Simple Network Management Protocol*), standardisé au début des années 90. Les données utiles pour gérer des équipements (dotés d'« agents » SNMP) se présentent sous forme de variables qui peuvent être interrogées et modifiées (l'information complète étant une collection d'objets appelée MIB ou *Management Information Base* dont le langage respecte la SMI ou *Structure of Management Information*). Plusieurs versions de ce protocole existent. Le standard RFC 2570, publié en avril 1999, décrit la version la plus récente : SNMPv3.

En terme de sécurité, SNMPv3 comble quelques lacunes des versions précédentes en offrant des solutions d'authentification et de chiffrement précisées dans le standard RFC 2574. La méthode s'appuie sur le principe d'utilisateurs définis par un nom, des droits d'accès et un mot de passe.

- chiffrement : les données peuvent être chiffrées par chaînes de blocs avec DES (*Data Encryption Standard*). Le secret est partagé entre les deux acteurs de la communication ;
- le contrôle d'accès : le contrôle se fait sur le principe de « vues » ; les informations peuvent être lues ou modifiées selon les utilisateurs ;
- protection contre le rejeu : un compteur est inclus dans chaque message. Il représente la durée depuis le dernier redémarrage du service de gestion d'administration ainsi que le nombre total de redémarrages depuis son installation. À la réception, le service vérifie que ce compteur reste dans une marge d'erreur raisonnable pour estimer s'il s'agit d'un rejeu. Cette mesure n'est donc pas parfaite ;
- authentification : un principe de condensat appliqué au secret partagé est utilisé pour s'authentifier : il s'agit de HMAC (*keyed-Hashing for Message Authentication*) précisé dans le standard RFC 2104. Il s'agit en réalité de concaténer les données avec le secret partagé, puis d'en calculer un condensat avec une fonction donnée, comme MD5 (HMAC-MD5) ou SHA-1 (HMAC-SHA1).

Même si cette version est celle qui est préconisée depuis son lancement, elle est loin d'être déployée dans la majorité des architectures de gestion.

5.2 Le problème actuel : CVE-2008-0960

HMAC (*keyed-Hashing for Message Authentication Code*) peut ainsi être utilisé pour authentifier les utilisateurs. Cependant, plusieurs applications ne vérifient pas que les valeurs fournies sont de taille raisonnable, permettant à quiconque d'envoyer des condensats de 1 octet. Cela se résume à 256 valeurs de condensats différentes. En d'autres termes, l'envoi d'une trame usurpée a donc 1 chance sur 256 de passer la phase d'authentification avec succès. Cette vulnérabilité reste valable pour les variantes HMAC-SHA-96 et HMAC-MD5-96 s'appuyant respectivement sur les algorithmes *Secure Hashing Algorithm-1* (SHA-1) et *Message-Digest Algorithm 5* (MD5).

Du code d'exploitation est déjà disponible.

Cette vulnérabilité a été initialement détectée sur les mises en œuvre de SNMP suivantes :

- Net-SNMP
<http://net-snmp.sourceforge.net/>
- UCD-SNMP (repris depuis quelques années par le projet Net-SNMP)
- eCos
<http://ecos.sourceware.org/>
- etc.

L'avis CERTA-2008-AVI-302 rappelle ainsi que les versions vulnérables de NET-SNMP sont toutes celles antérieures à 5.4.1.1, 5.3.2.1 et 5.2.4.1.

L'effet « boule de neige » issu de la réutilisation de mêmes codes par plusieurs applications implique de nombreux autres produits. Parmi ceux-ci :

- Cisco (Cisco IOS, Cisco IOS-XR, Cisco CatOS, Cisco NX-OS, Cisco ACE)
- Juniper Networks (Session and Resource Control SRC pour les versions 1.0.0, 1.0.1 ou 2.0.0) ;
- Sun Microsystems
- Red Hat (Red Hat Enterprise Linux 2.1, 3, 4 et 5 utilisant les paquets ucd-snmp ou net-snmp) ;
- Network Appliance (Data ONTAP version 7.3RC1, 7.3RC2) ;

- SNMP Research (produits ayant SNMPv3 pour les versions 16.1 et antérieures).

Une liste est maintenue à l'adresse suivante :

<http://www.kb.cert.org/vuls/id/878044>

Cette vulnérabilité est relativement importante. Il ne faut pas oublier non plus que de tels services ne doivent pas être accessibles depuis l'Internet. En effet, il est possible de cartographier l'ensemble des équipements ayant de telles vulnérabilités par des balayages de ports à large échelle. Des personnes ont déjà lancé de telles opérations et le résultat a été rendu public. Toute interface connectée à l'Internet ne peut pas cacher simplement les services en écoute sur des ports.

Il suffit d'un équipement embarqué mal configuré comme un routeur pour mettre en danger l'ensemble des communications sortantes d'un réseau.

5.3 Recommandations

Plusieurs mesures peuvent être entreprises pour limiter les risques.

La première consiste à vérifier si SNMP est effectivement déployé ou activé sur les équipements ; l'usage de ce protocole n'est parfois pas clairement mentionné par les outils d'administration à distance. Cela peut se faire par le biais de balayages contrôlés dans le réseau local, par une écoute passive des trames ou en interrogeant directement la configuration des équipements.

Par exemple, les équipements Cisco (IOS, CatOS ou IOS-XR) peuvent être interrogés par la commande `show snmp group`. L'information est visible dans le champ `security model`, qui signale par `usm` ou `v3 auth` que SNMPv3 est configuré.

Si SNMP est effectivement utilisé, il faut alors s'assurer qu'il est correctement configuré avec l'application des différentes mesures de sécurité. De manière générale, des utilisateurs distincts sont utilisés pour la lecture et l'écriture de données. De même, le chiffrement peut s'activer ou se désactiver. Dans la configuration Net-SNMP, cela se fait avec le champ `priv`.

```
# écriture et lecture
rwuser certa1 priv
# lecture seulement
rouser certa2 priv
```

Il est souvent possible de journaliser les erreurs d'authentification et d'émettre un signal (`trap`) à la console d'administration quand cela se produit. Pour Net-SNMP, il suffit également d'ajouter dans le fichier de configuration `snmpd.conf` la ligne :

```
authtrapenable 1
# définir aussi la destination des "trap"
```

Parmi les autres mesures envisageables :

- vérifier les cloisonnements des services. Les échanges de données pour administrer les équipements doivent être physiquement (ou logiquement si cela n'est pas possible) décorrélés du réseau et les interfaces doivent être inaccessibles pour toute autre application que celle de console d'administration sur un poste dédié ;
- surveiller le trafic SNMP. Par défaut, il utilise les ports de destination 161/udp et 162/udp ;
- mettre à jour les équipements.

5.4 Documentation

- Avis de sécurité CERTA-2008-AVI-302, « Vulnérabilité dans Net-SNMP » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-302/>
- Avis de sécurité CERTA-2008-AVI-310, « Vulnérabilité dans des produits CISCO » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-310/>
- Documentation Cisco pour SNMPv3 :
http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html
- Avis de sécurité oCERT ocert-2008-006 du 09 juin 2008 :
<http://www.ocert.org/advisories/ocert-2008-006.html>
- Recommandations et note de mise à jour du projet Net-SNMP du 09 juin 2008 :
http://sourceforge.net/forum/forum.php?forum_id=833770
- RFC 2104, "HMAC: Keyed-Hashing for Message Authentication", février 1997 :
<http://www.ietf.org/rfc/rfc2104.txt>

- RFC 2570, "Introduction to Version 3 of the Internet-Standard Network Management Framework", avril 1999 :
<http://www.ietf.org/rfc/rfc2570.txt>
- RFC 2574, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", avril 1999 :
<http://www.ietf.org/rfc/rfc2574.txt>
- RFC 2575, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", avril 1999 :
<http://www.ietf.org/rfc/rfc2575.txt>

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 05 et le 12 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 06 au 12 juin 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-295 : Multiples vulnérabilités dans VLC
- CERTA-2008-AVI-296 : Multiples vulnérabilités dans Novell GroupWise Messenger
- CERTA-2008-AVI-297 : Vulnérabilité du noyau Linux
- CERTA-2008-AVI-298 : Vulnérabilité dans HP StorageWorks Storage Monitoring
- CERTA-2008-AVI-299 : Plusieurs vulnérabilités dans IBM DB2
- CERTA-2008-AVI-300 : Vulnérabilité dans OpenOffice.org
- CERTA-2008-AVI-301 : Multiples vulnérabilités dans Apple QuickTime

- CERTA-2008-AVI-302 : Vulnérabilité dans Net-SNMP
- CERTA-2008-AVI-303 : Vulnérabilité de la pile Bluetooth Windows
- CERTA-2008-AVI-304 : Vulnérabilités dans Microsoft Internet Explorer
- CERTA-2008-AVI-305 : Vulnérabilité du service Microsoft WINS
- CERTA-2008-AVI-306 : Vulnérabilités protocolaires dans Windows (PGM)
- CERTA-2008-AVI-307 : Vulnérabilités dans Microsoft DirectX
- CERTA-2008-AVI-308 : Vulnérabilité liée au service de reconnaissance vocale Windows
- CERTA-2008-AVI-309 : Vulnérabilité dans Active Directory
- CERTA-2008-AVI-310 : Vulnérabilité dans les produits CISCO

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 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.

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 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.

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.

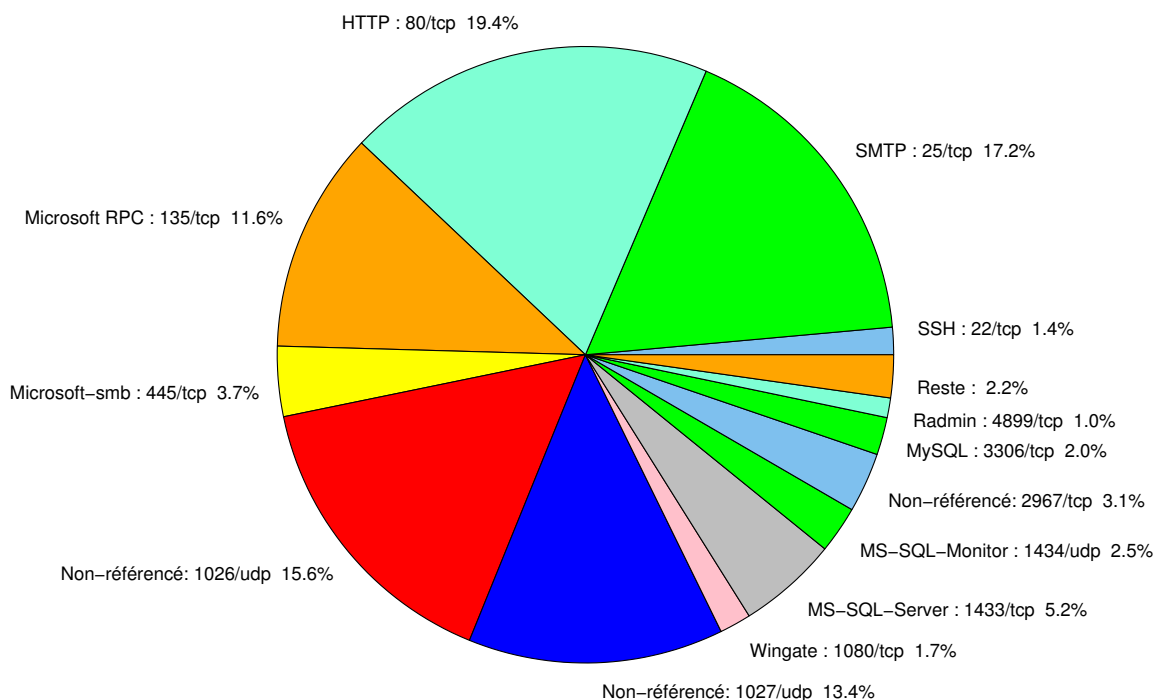


FIG. 1: Répartition relative des ports pour la semaine du 05.06.2008 au 12.06.2008

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
80/tcp	19.35
25/tcp	17.15
1026/udp	15.63
1027/udp	13.39
135/tcp	11.64
1433/tcp	5.24
445/tcp	3.71
2967/tcp	3.13
1434/udp	2.46
3306/tcp	1.97
1080/tcp	1.65
22/tcp	1.43
4899/tcp	1.07
3128/tcp	0.8
137/udp	0.62
139/tcp	0.31
143/tcp	0.17
23/tcp	0.13

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

13 juin 2008 version initiale.