Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 juin 2007
N° CERTA-2007-ACT-022

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-22

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-022

Gestion du document

Référence	CERTA-2007-ACT-022
Titre	Bulletin d'actualité 2007-22
Date de la première version	01 juin 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-022.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-022/

1 Les incidents traités cette semaine

1.1 Vulnérabilités dans *Dokeos*

Des vulnérabilités affectant les versions 1.6.5 et 1.8.0 de `Dokeos` ont récemment été rendues publiques. L'une de ces vulnérabilités est activement exploitée, comme nous l'avons mentionné dans le bulletin d'actualité CERTA-2007-ACT-021.

Les éditeurs de `Dokeos` n'envisagent pas de publier un correctif pour la version 1.6.5. En effet, la branche 1.6.x devrait, faute de moyens, ne plus être maintenue (hormis sur demande contractuelle). En revanche, une version 1.8.1, corrigeant la faille exploitée, est prévue pour la mi-juin 2007. Toutefois, les éditeurs de `Dokeos` ont mis à disposition du CERTA un correctif temporaire pour la version 1.8.0 permettant d'empêcher les récentes attaques. Ce correctif peut être obtenu sur demande auprès du CERTA. Il s'agit d'un correctif temporaire car toutes les vulnérabilités n'ont pas encore été identifiées.

Recommandations :

Nous recommandons aux utilisateurs de `Dokeos` 1.6.x de migrer vers la branche 1.8.x (cette dernière nécessite l'utilisation de PHP 5), d'entrer en contact avec leur responsable de sécurité pour l'obtention du correctif

temporaire et de suivre la sortie d'un correctif définitif.

1.2 Validation des paramètres d'une fonction, précaution indispensable

Les bonnes pratiques du génie logiciel comprennent, entre autres, la vérification des valeurs des paramètres d'entrées dans une fonction ou dans une procédure. Cette règle est trop souvent oubliée. L'absence de la vérification et de la validation crée des faiblesses dans les programmes, exploitées par les agresseurs des systèmes d'information. Le CERTA traite des incidents qui résultent de cette exploitation délictueuse. A valeur d'illustration, les derniers bulletins d'actualité traitent :

- de failles de type *PHP include* ;
- de possibilités d'injection de code (*cross site scripting*).

Cette liste n'est hélas pas close. L'utilisation d'une redirection par un `servlet` doit respecter les bonnes pratiques de développement. C'est particulièrement vrai lorsque la page vers laquelle l'internaute sera redirigée ou lorsque le cadre (*frame*) qui sera chargé figure en argument dans l'URL. Sur le navigateur de l'internaute, la barre d'adresse contient :
`http://www.site-imparfait.fr/chemin/redirect.jsp?page=la-page-a-charger.html`
Si le contenu de la variable `page` n'est pas vérifié, alors cette variable peut être détournée. Des actions de filoutage (*phishing*) peuvent utiliser le site pour diriger l'internaute victime vers un site frauduleux. Comme pour les vulnérabilitées déjà mentionnées dans son bulletin d'actualité, le CERTA recommande plusieurs niveaux de filtrage et de vérification des valeurs entrées :

- gestion de la longueur de l'entrée, prévention des débordements ;
- prise en compte des différents codages admis dans les URL, plus généralement dans les entrées ;
- jeu de caractères utilisé (aseptisation si les caractères spéciaux n'ont pas lieu d'être présents) ;
- syntaxe ;
- sémantique, appartenance à un ensemble de valeurs permises ;
- restriction au strict nécessaire des flux sortants (exemple : HTTP) provenant d'un serveur.

Cette liste de précaution n'est pas exhaustive. Elle s'applique aussi bien au niveau du serveur, qu'à celui des éventuelles passerelles (*proxy*).

Documentation

- Note d'information, « Du bon usage de PHP », publiée le 20 mars 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/
- Note d'information, « Vulnérabilité de type Cross Site Scripting », publiée le 22 mars 2002 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/
- Note d'information, « Sécurité des applications Web et vulnérabilité de type "injection de données" », publiée le 03 janvier 2005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/

2 Virus embarqués dans des fichiers *RTF*

Les nombreuses vulnérabilités touchant Microsoft Office incitent les personnes à utiliser des formats plus sûrs tels que `RTF` (*Rich Text Format*). Toutefois ce format, lisible par de nombreux éditeurs de texte, est utilisé depuis peu comme conteneur de certains virus. Ces virus utilisent une propriété permettant à chacun d'insérer des objets dans les documents `RTF` ; dans ce cas précis, l'objet est un fichier exécutable.

L'infection sous Microsoft Word se fait de la manière suivante :

- les victimes reçoivent un courriel avec le fichier `RTF` en pièce jointe, qui semble inoffensif ;
- l'ouverture de ce document provoque un faux message d'erreur dans l'éditeur de texte : l'utilisateur est invité à double-cliquer sur l'icône apparue dans Word pour rouvrir le fichier (cette icône représente en fait l'exécutable contenu dans le document) ;
- le lancement de l'exécutable provoque l'infection de l'ordinateur.

Cette technique n'utilise aucune faille de Microsoft Word mais seulement un peu d'ingénierie sociale. Il est à noter que le fait de double-cliquer sur l'objet contenu dans le document `RTF` ouvert provoque un avertissement sous Microsoft Windows qui demande une confirmation.

A la date de rédaction de ce bulletin, trois variantes de ce virus ont été clairement identifiées. L'utilisation de fichiers au format `RTF` n'est évidemment pas à proscrire, toutefois le CERTA rappelle à chacun la nécessité d'être très vigilant vis-à-vis de tout type de fichier qui n'est pas d'une provenance sûre, quelque soit son format.

3 Les événements Windows

Microsoft Windows identifie dans les journaux les événements par leurs identifiants. Parmi ceux intéressants et nouveaux, il y a l'identifiant `4907`. Il notifie tout changement de `SACL` d'un objet, par l'administrateur ou un programme. L'objet peut aussi bien être une clé de registre, qu'un fichier ou un répertoire. Le `SACL` (pour *System Access Control List*) sert à Windows pour définir quels utilisateurs ou groupes d'utilisateurs peuvent surveiller (« auditer») l'objet.

En prenant un exemple, voici à quoi ressemble un tel événement :

```
Sujet:
      ID de sécurité:               SYSTEM
      Nom du compte:                TEST$
      Domaine du compte:            WORKGROUP
      ID d'ouverture de session:    0x3e7
Objet:
      Serveur de l'objet:   Security
      Type d'objet:         File
      Nom de l'objet:       C:\Program Files\Windows Defender\MpSoftEx.dll
      ID du handle:         0x1d4
Informations sur le processus:
      ID du processus:      0x6e0
      Nom du processus:     C:\Windows\servicing\TrustedInstaller.exe
Paramètres d'audit:
      Descripteur de sécurité d'origine:
      Nouveau descripteur de sécurité: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
```

Cela indique notamment :

1. qui a changé le `SACL` (SYSTEM TEST)
2. quel programme a été utilisé pour changer le `SACL` (TrustedInstaller.exe)
3. le nom et le type d'objet qui a eu ses attributs modifiés (*file*)

Le dernier champ, correspondant au *Descripteur de sécurité* est une chaîne de caractères particulière, dont l'interprétation est expliquée à l'adresse :

http://www.washington.edu/computing/support/windows/UWdomains/SDDL.html On peut constater dans l'exemple que cette chaîne a été créée, et ne contenait aucune valeur à l'origine.

Suivre ces événements permet donc de vérifier rapidement si les caractéristiques de surveillance des objets ont été modifiées, ainsi que de déterminer quels changements ont été effectués.

4 Les risques des jeux en ligne

Certains jeux en ligne populaires, comme actuellement `World of Warcraft` font l'objet de convoitise de la part de codes malveillants. En effet, plusieurs vers et chevaux de Troie ont été observés de part le monde, et notamment en France, avec pour principal objectif de dérober les identifiants de connexion de ces jeux.

Il est alors légitime de se demander pourquoi un tel « attrait » envers ceux-ci plutôt que d'autres. En voici quelques raisons :

- ces jeux en ligne sont payants. Il existe un trafic permettant d'acheter des comptes ayant obtenu des niveaux avancés dans le jeu, et ainsi progresser plus vite de manière frauduleuse ;
- certains joueurs peuvent être victimes de chantage. Etant à un stage avancé du jeu, leurs identifiants, récupérés et modifiés par la personne malintentionnée, peuvent leur être restitués en échange de crédits, d'aides, ou d'argent.
- une fois les identifiants entrés dans le jeu, cela donne accès aux données personnelles de l'utilisateur, incluant son adresse, et parfois ses coordonnées bancaires. Ces informations sont intéressantes pour plusieurs raisons, que ce soit pour mieux cibler des attaques de type filoutage, ou d'escroqueries financières par exemple.
- une fâcheuse habitude est de conserver les mêmes identifiants pour plusieurs accès à des sites ou services différents. La personne malveillante peut donc les tester, et les ajouter à un dictionnaire pour faire des attaques en force brute sur les mots de passe.

La plus grande difficulté est ici de sensibiliser les utilisateurs aux motivations précédemment citées. Ceux-ci doivent prendre les précautions adaptées pour se connecter depuis une machine et un réseau de confiance (pas une borne publique ou partagée par exemple). Ils doivent également se limiter à fournir l'information explicitement et strictement nécessaire à l'inscription. Les administrateurs doivent, eux, vérifier que la politique de sécurité est bien adaptée, et que l'usage de tels divertissements n'en soit pas un contournement.

5 Des problèmes avec Mozilla Firefox

5.1 La récupération d'informations

Le CERTA a publié dans le précédent bulletin d'actualité CERTA-2007-ACT-021 les détails d'une vulnérabilité concernant l'accès illégitime à des fichiers par le biais de code Javascript et du protocole `resource://`. Cette dernière devait être corrigée dans la version 2.0.0.4 du navigateur. Cependant, les modifications publiées le 30 mai pour cette version ne font pas état de telles corrections. Les tests effectués semblent également indiqués que la vulnérabilité existe toujours. Dans ces conditions, le CERTA rappelle qu'il est vivement recommandé de désactiver Javascript par défaut, et de ne l'employer que sur certains sites de confiance, quand cela s'avère nécessaire.

Si des passerelles filtrant le contenu sont utilisées, il faut également vérifier que des adresses de type `resource://` soient correctement filtrées.

Documentation

- Bulletin d'actualité CERTA-2007-ACT-020 du 18 mai 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-020/
- Les changements de versions de Firefox :
  http://en-us.www.mozilla.com/en-US/firefox/2.0.0.4/releasenotes/
- Les avis de sécurité de Mozilla :
  http://www.mozilla.org/security/announce/
- Avis CERTA-2007-AVI-245 du 01 juin 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-245/

5.2 La gestion des mises à jour d'extensions

5.2.1 Présentation du problème

Une vulnérabilité existe actuellement sous Firefox : elle concerne la mise à jour des extensions qui ne sont pas hébergées sur le site `https://addons.mozilla.org`.

Ces extensions incluent la liste suivante :

- Google Toolbar
- Yahoo Tolbar
- AOL Toolbar
- PhishTank SiteChecker
- etc.

La liste est bien entendu non exhaustive.

La mise à jour de ces extensions se fait sans authentification du serveur. Il est donc possible, par une attaque de type « empoisonnement de DNS » ou « homme-au-milieu » de pretexter une mise à jour pour charger un code malveillant et d'exécuter du code arbitraire sur la machine à l'ouverture du navigateur.

Le problème vient donc à la fois :

- des développeurs d'extensions, qui n'utilisent pas SSL (HTTPS) pour les mises à jour automatiques,
- de la configuration par défaut de Firefox.

A l'installation d'une extension, Firefox ne prévient pas des risques que les mises à jour peuvent faire courir. De plus, le comportement standard est d'ajouter, lors de cette installation, le site de mise à jour d'une extension à la liste des sites autorisé à faire des mises à jour sans prévenir. Cette liste est accessible :

1. en se rendant dans l'onglet « Sécurité » de la configuration Firefox
2. en cliquant sur "exceptions" à côté de la ligne "prévenir lorsque les sites essaient d'installer des modules complémentaires"

Les sites utilisant SSL ne sont pas différenciés de ceux ne l'employant pas.

Dans l'attente de correctifs, de la part de Firefox et des développeurs de ses extensions, le CERTA recommande de :

- désinstaller autant que possible de telles extensions ;
- vérifier qu'elles n'ont pas été ajoutées au cours de l'installation d'un logiciel tiers ;
- vérifier que la liste des 'sites autorisés' ne contient que ceux utilisant SSL. Cette liste peut très bien se limiter à 'addons.mozilla.org' par exemple, voire être vide.

5.2.2 Les aspects plus techniques

Plus techniquement, voici les détails de cette vulnérabilité : le fichier `Manifest` associé à l'extension définit les sites pour les mises à jour. Le gestionnaire de mise à jour de Firefox inspecte alors régulièrement ce fichier pour déterminer si de nouvelles versions sont disponibles. Le lien des mises à jour, qui peut aussi être joint à un fichier `update.rdf` se caractérise par le mot-clé `updateURL`.

Voici un exemple fourni sur le site de Mozilla :

```
<_em:updateURL>http://www.XXX/update.cgi?id=%ID%&amp;version=%VER%</em:updateURL>
<_em:updateURL>http://www.XXX/extension/windows.rdf</em:updateURL>
```

Il faut cependant noter que la branche 1.5.0.X, en fin de maintenance, n'offre aucun accès simple à la gestion des mises à jour, exceptée le choix pour « les modules installés et les thèmes », sans distinction.

Mozilla a annoncé dans un article récent daté du 30 mai 2007 avoir l'intention, dans la version 3 du navigateur Firefox, d'empêcher les développeurs de modules d'utiliser des canaux non sécurisés et d'améliorer l'écriture de ces derniers. Ceci est encore en phase de discussion.

- Les intententions des développeurs Mozilla, publiées le 30 mai 2007 :
  http://developer.mozilla.org/devnews/index.php/2007/05/30/add-on-updates/
- Discussion des développeurs Mozilla sur *updateURL* :
  http://developer.mozilla.org/en/docs/Install_Manifests#updateURL

6 Les mises à jour de Microsoft Office sous Vista

Dans son dernier système d'exploitation `Windows Vista`, `Microsoft` propose une interface locale à la machine pour procéder aux mises à jour des différents produits Microsoft installés. Ainsi, si `Microsoft Office 2007` est présent sur la machine, cette interface proposera les mises à jour pour le système d'exploitation mais également pour la suite Office. Cependant, ceci ne fonctionne qu'avec la dernière version `Office 2007`. Il n'en va pas de même pour `Office XP` par exemple. Avec cette version, `Windows Update` ne prendra pas en charge par défaut les mises à jour. De plus en se rendant sur le site `http://update.microsoft.com`, l'utilisateur sera redirigé vers l'interface locale l'empêchant de consulter ce site. Il convient dans ce cas de figure :

- de se rendre sur `http://office.microsoft.com/` et de télécharger et appliquer les mises à jour « à la main » ;
- de se rendre sur `http://udpdate.microsoft.com/microsoftupdate` et, si vous acceptez les conditions d'utilisation, d'installer le contrôle `ActiveX` de `Microsoft Update`. Une fois cet `ActiveX` installé, l'interface de `Windows Update` de `Vista` proposera les mises à jour adéquates pour la suite `Office`.

7 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 24 et le 31 mai 2007.

8 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html

– Note d'information sur les systèmes obsolètes :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
– Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
– Note d'information sur les mots de passe :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
– Note d'information sur la terminologie d'usage au CERTA :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
– Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html
– 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 CERTA-2006-INF-006, Risques associés aux clés USB :
http://www.certa.ssi.gouv.f r/site/CERTA-2000-INF-006/
– Note d'information du CERTA CERTA-2006-INF-009 sur les outils d'indexation et de recherche :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
– Note d'information du CERTA CERTA-2007-INF-001 sur la gestion des noms de domaine :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
– Note d'information sur le bon usage de PHP :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002

9 Rappel des avis émis

Durant la période du 25 au 31 mai 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-228 : Vulnérabilité d'un produit Citrix
– CERTA-2007-AVI-229 : Vulnérabilité dans Tomcat
– CERTA-2007-AVI-230 : Vulnérabilités dans NOD32
– CERTA-2007-AVI-231 : Vulnérabilité dans Symantec Enterprise Security Manager
– CERTA-2007-AVI-232 : Multiples vulnérabilités d'Antivir
– CERTA-2007-AVI-233 : Vulnérabilités dans Apple QuickTime
– CERTA-2007-AVI-234 : Multiples vulnérabilités dans Apple Mac OS X
– CERTA-2007-AVI-235 : Vulnérabilités dans Avast! Antivirus
– CERTA-2007-AVI-236 : Vulnérabilités sur Sun Java System Web Proxy Server
– CERTA-2007-AVI-237 : Vulnérabilité de Sun Solaris
– CERTA-2007-AVI-238 : Vulnérabilité dans Sun Java Web Start
– CERTA-2007-AVI-239 : Multiples vulnérabilités dans HP System Management Homepage

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

– CERTA-2007-AVI-122-001 : Vulnérabilité dans MPlayer et Xine-lib
(ajout des références aux bulletins de sécurité Gentoo, Mandrivo, SuSE)
– CERTA-2007-AVI-138-003 : Vulnérabilité dans file
(ajout de la référence CVE et des références aux bulletins de sécurité Gentoo, RedHat)
– CERTA-2007-AVI-151-001 : Vulnérabilité mod_perl pour Apache
(ajout de la référence au bulletin de sécurité SuSE)
– CERTA-2007-AVI-158-001 : Multiples vulnérabilités de Kerberos
(ajout des références aux bulletins de sécurité HP, Gentoo, Debian, Mandriva, Red Hat, Ubuntu, SuSE)
– CERTA-2007-AVI-201-001 : Multiples vulnérabilités dans PHP
(ajout des réffences aux bulletins de sécurité Gentoo, SuSE, Mandriva, Red Hat)
– CERTA-2007-AVI-225-001 : Vulnérabilité dans Vim
(ajout de la référence au bulletin de sécurité SuSE)
– CERTA-2007-AVI-226-001 : Vulnérabilité dans FreeType
(ajout des références aux bulletins de sécurité Gentoo, Ubuntu)

10 Actions suggérées

10.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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.

10.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

10.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

10.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

10.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

10.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements 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.

10.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

11 Les bulletins d'actualité

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

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

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

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

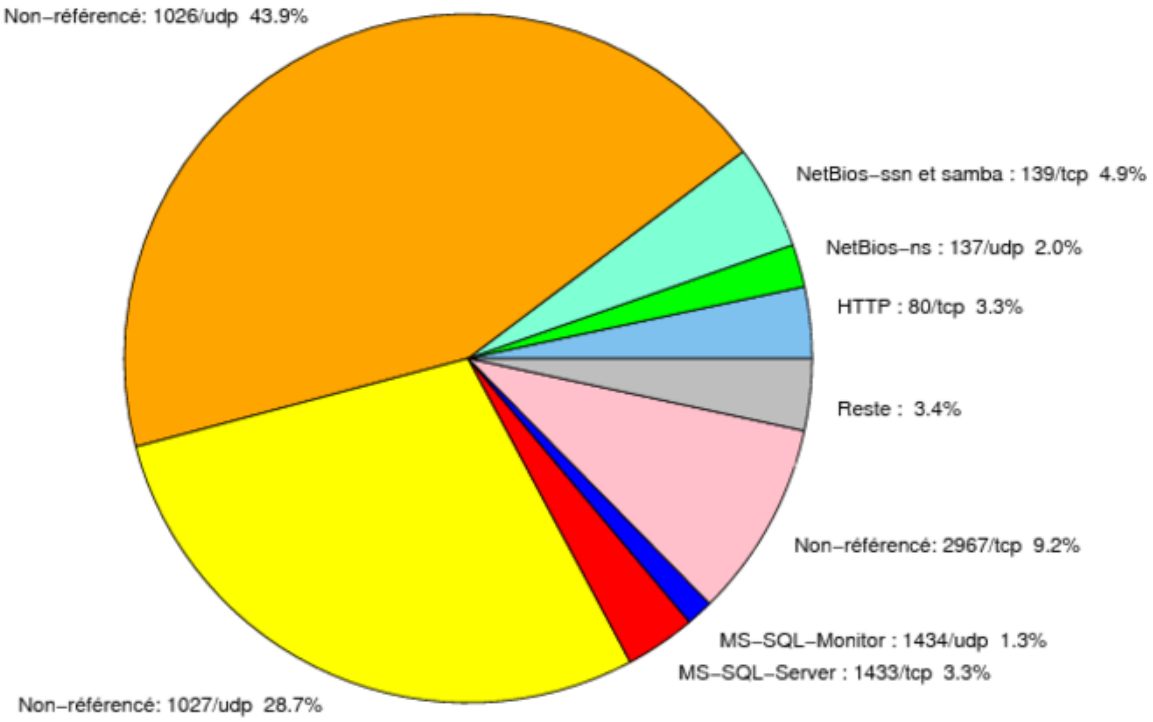

FIG. 1: Répartition relative des ports pour la semaine du 24.05.2007 au 31.05.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE

2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

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

port	pourcentage
1026/udp	43.87
1027/udp	28.68
2967/tcp	9.23
139/tcp	4.9
80/tcp	3.34
1433/tcp	3.3
137/udp	2
1434/udp	1.26
22/tcp	0.77
4899/tcp	0.61
1080/tcp	0.42
3128/tcp	0.3
3306/tcp	0.29
21/tcp	0.28
443/tcp	0.16
25/tcp	0.14
23/tcp	0.1
143/tcp	0.09
15118/tcp	0.06
5554/tcp	0.04
9898/tcp	0.03
3389/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

01 juin 2007 version initiale.