Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 juin 2007
N° CERTA-2007-ACT-023

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-23

Gestion du document

Référence	CERTA-2007-ACT-023
Titre	Bulletin d'actualité 2007-23
Date de la première version	08 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-023.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-023/

1 Les incidents traités cette semaine

1.1 Les versions des applications sur un serveur Web

Dans un incident traité cette semaine au CERTA, la personne malintentionnée a déterminé l'application vulnérable en faisant une simple recherche sur *Google*. Ces attaques, qui sont très souvent opportunistes, reposent sur le fait que chaque application utilisée pour mettre en œuvre un site Web peut révéler publiquement son numéro de version. Une personne malveillante ayant accès au code d'exploitation d'une vulnérabilité affectant une version donnée d'une application effectue simplement une requête sur un moteur de recherche avec comme mots-clés l'application en question et son numéro de version. Cette technique est très fréquemment rencontrée par le CERTA.

Par exemple, pour une faille touchant *phpBB 2.0.10*, le pirate effectuera une recherche *'Powered by phpBB 2.0.10'*, signature de cette application. Il obtiendra immédiatement une liste de sites vulnérables. Dans le cas de serveurs Web, ce sont les requêtes provoquant des erreurs (erreur `404` par exemple) qui permettent souvent de connaître les produits utilisés et leurs versions.

Il existe des techniques beaucoup plus sophistiquées (*fingerprinting* ou prise d'empreinte) pour déterminer les applications et leurs versions utilisées et ainsi choisir le bon code d'exploitation. Dans le cas présent, il est recommandé, pour éviter d'être une cible qui apparaît dans les moteurs de recherche, d'anonymiser au maximum les

applications utilisées sur Internet. Ces moteurs de recherche indexent le texte affiché sur le site et les adresses correspondantes, il est donc important qu'aucun texte permettant d'identifier précisément la version de l'application, voire aussi son nom, ne soit contenu dans le site. Ceci inclut les codes source (les numéros de version sont souvent en commentaire dans les codes HTML) et les pages d'erreur. Par exemple, la plupart des serveurs Web ont une page d'erreur par défaut, qu'il faut modifier.

Cependant, si de telles mesures sont nécessaires, car elles protègent de recherches de sites vulnérables à un type de faille donnée, elles ne protègent pas contre ces vulnérabilités et ne protègent pas contre les attaques lancées « en aveugle ». Il est donc toujours important de mettre à jour régulièrement ses applications et d'appliquer les autres mesures de protection habituelles.

1.2 Des outils de filoutage à disposition

Cette semaine le CERTA a rencontré des sites mettant à disposition plusieurs dizaines d'outils permettant d'installer des sites de filoutage (*phishing*) reproduisant frauduleusement les sites de plusieurs sociétés dont certaines françaises (ou filiales françaises de sociétés internationales) : `Free`, `Hotmail`, `eBay` et `Paypal`. N'importe quel autre site aurait pu également se trouver « copié ».

Le CERTA rappelle que l'utilisation comme la détention de tels outils est réprimée par la loi.

Le CERTA recommande aussi d'être particulièrement vigilant lors de la saisie de données personnelles et/ou confidentielles sur un site Internet. Le CERTA rappelle également d'éviter de cliquer dans un lien se trouvant dans un courrier électronique. Il est préférable de saisir le lien souhaité sois-même à la main dans son navigateur. Cet incident montre une nouvelle fois que les clients de toute société peuvent être visés par ces actions malveillantes, pas uniquement ceux des banques.

1.3 Évolution d'un site Web hébergeant des pages de filoutage : le retour

Dans son bulletin d'actualité numéro CERTA-2007-ACT-020, le CERTA indiquait l'évolution d'une compromission d'un serveur Web entraînant la mise en place de multiples sites de filoutage (*phishing*). Cette semaine, c'est au tour d'une banque australienne d'être victime d'un site frauduleux hébergeux sur ce même serveur. Cette évolution peut s'expliquer de plusieurs façon :

- la faille exploitée n'a pas été corrigée : en effet bien que l'accès à un module vulnérable (ExtCalendar) ait été supprim é, les fichiers vulnérables étaient toujours présents sur le serveur ;
- les individus malveillants ont pu revenir en utilisant un outils d éposé lors des précédentes compromissions ;
- ce site étant mutualisé avec d'autre site web, les attaquants peuvent compromettre ce site en utilisant une faille présente sur un autre site. De la même façon, tous les autres sites mutualisés sur ce serveur sont susceptibles d'être compromis.

Cet exemple montre qu'en l'absence d'un traitement complet de l'incident, on ne peut pas comprendre la vulnérabilité à l'origine de l'attaque, ainsi que la portée de cette dernière. On s'expose donc à de multiples récidives.

Documentation

- Bulletin d'actualité CERTA-2007-ACT-020 du 18 mai 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-20
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005

2 Retour sur les récentes vulnérabilités des navigateurs Mozilla Firefox et Microsoft Internet Explorer

2.1 Vulnérabilité *IFRAME* dans Firefox

Cette semaine, le CERTA a publié l'alerte CERTA-2007-ALE-012 relative aux vulnérabilités non-corrigées dans `Mozilla Firefox`. Deux d'entre elles ont déjà été abordées dans les bulletins d'actualité CERTA-2007-ACT-020 et CERTA-2007-ACT-022. Plusieurs autres vulnérabilités ont été rendues publiques cette semaine. En particulier, l'une d'entre elles concerne une mauvaise gestion des `IFRAME` (*Inline HTML frames*). Celles-ci sont très souvent utilisées conjointement avec la requête `XMLHttpRequest` afin de produire des effets dynamiques dans des pages web comme des « glisser/déposer » ou le rafraîchissement d'une partie de la page...

Dans Firefox, il est possible à une page tierce de modifier une IFRAME par l'intermédiaire de la méthode document.write(). Malgré un contrôle plus strict dans les dernières versions de Firefox, il est encore possible d'utiliser cettte méthode de façon malveillante lors du chargement de l'IFRAME que l'on veut modifier.

Dans les faits, cette vulnérabilité permet à une page malveillante de remplacer une IFRAME d'une autre page web en cours de chargement par une IFRAME disposant de fonctionnalités arbitraires comme de la capture de frappes clavier par exemple. Il est à noter qu'il existe déjà des preuves de faisabilité (*proof of concept*) disponibles sur l'Internet.

2.2 L'interprétation des extensions de fichiers sous Firefox

Une autre vulnérabilité importante est due au fait que Firefox ne filtre pas correctement les extensions des fichiers qui lui sont fournies via une adresse réticulaire (URL). Il est ainsi possible de modifier le comportement de Firefox vis-à-vis d'un fichier par le biais d'une extension construite de façon particulière. Cette faille permet donc à un utilisateur malveillant d'exécuter du code arbitraire à distance. Une attaque en deux temps pourrait consister en la consultation par la victime d'une page d'extension .html puis une seconde fois mais avec une URL légèrement modifiée. La deuxième consultation provoque alors l'exécution de code et non plus l'affichage d'une page web.

2.3 Vulnérabilités dans Microsoft Internet Explorer

Deux vulnérabilités affectant l'explorateur de Microsoft ont été rendues publiques cette semaine et sont actuellement sans correctif.

La première affecte les dernières versions, même à jour. Il est possible d'exécuter des scripts arbitraires provenant d'une page sur une autre page. Cela permettrait par exemple de récupérer des informations de l'utilisateur lié à cette page (fichiers de sessions, ou *cookies*) ou de modifier la destination des informations soumises à un formulaire, et ainsi dérober des données personnelles.

La seconde concerne uniquement la version 6 d'Internet Explorer. Il est possible pour une personne malveillante d'afficher un contenu arbitraire en remplacement de la barre d'adresse qui affiche normalement celle du site légitime. L'utilisateur pense alors naviguer sur des pages de confiance. Cette méthode pourrait être utilisée dans une attaque en filoutage : le fait de vérifier visuellement l'adresse affichée ne permettrait pas de détecter la supercherie.

Dans les deux cas, la désactivation du JavaScript rend les vulnérabilités inexploitables. Pour qu'un site reste de confiance, il ne faut pas s'y rendre depuis une source non sûre, i.e. en cliquant sur un lien dans un courrier électronique, ou sur un site tiers, etc.

3 Les documents composites

Les applications bureautiques permettent très souvent à l'utilisateur d'insérer, au sein d'un document, un autre document, qui peut être dans un format très différent. Ainsi, un fichier au format .doc de Word peut contenir des fichiers .xls produits à partir du tableur Excel, ou des transparents .ppt d'un fichier Powerpoint, etc. Sous Microsoft Office, cela peut se faire de la manière suivante :

1° créer un nouveau document certa.doc

2° choisir dans « Insertion » l'option « Objet »

3° insérer l'objet voulu, en cochant éventuellement « Afficher sous forme d'icône »

Cette succession de fichiers insérés les uns dans les autres, à la manière des fameuses *matriochkas* ou poupées russes gigognes, peut être de n'importe quelle profondeur.

Le problème est alors assez simple : le fichier original peut être d'apparence « sain », mais contenir d'autres fichiers qui, eux, contiennent du code malveillant. Une pratique courante consiste à convertir les fichiers avant de les ouvrir. Cette approche est intéressante, et a, par exemple, fait l'objet de l'apparition d'une récente application chez Microsoft : MOICE (pour *Microsoft Office Isolated Conversion Environment*), qui a été présenté dans CERTA-2007-ACT-021. Il peut aussi s'agir d'une conversion dans des formats comme .pdf. L'idée sous-jacente et attendue consiste à estimer qu'un fichier construit spécifiquement pour exploiter une vulnérabilité dans un format donné deviendra inoffensif sous un autre format.

Que deviennent les documents insérés au cours de cette conversion ? Sont-ils conservés ? Modifiés ? Supprimés ? En d'autres termes, il est important de déterminer si la phase de conversion élimine ou non les risques pouvant être introduits par les documents insérés.

En effet, une personne malveillante peut profiter de cette technique pour contourner les politiques de filtrage d'extensions (pièce jointe à un courrier électronique par exemple), ou les antivirus. L'utilisateur, en revanche, a toutes les chances, s'il ouvre le premier document, d'ouvrir également ceux qui y sont insérés.

Le CERTA recommande donc les actions suivantes :

- sensibiliser les utilisateurs à ne pas utiliser ces techniques d'insertion. Des liens relatifs peuvent remplacer l'insertion d'un document. Il faut alors échanger l'ensemble des documents.
- vérifier que les solutions de conversion, si elles sont utilisées à des fins de sécurité, prennent en compte ce problème. En particulier, la solution `MOICE` actuelle ne permet pas de le faire, tandis qu'`Acrobat Distiller` semble ignorer ces fichiers insérés.
- s'assurer que les filtrages mis en place, par exemple aux niveaux des messageries pour vérifier les extensions, ne sont pas vulnérables à ces insertions chaînées. Pour cela, des tests simples avec des pièces jointes peuvent être lancés.

4 Une commande Unix vulnérable

La commande Unix `file` permet, via une ligne de commande, d'afficher les propriétés d'un fichier, obtenues par certains tests :

```
test@labo:~/Desktop$ file MonFichier.pdf
MonFichier.pdf: PDF document, version 1.6
test@labo:~/Desktop$ file MonDeuxiemeFichier.odt
MonDeuxiemeFichier.odt: Zip archive data, at least v2.0 to extract
test@labo:~/Desktop$ file MonAutreFichier.txt
MonAutreFichier.text: MS-DOS executable (EXE)
```

Cet exemple illustre que l'extension peut parfois être trompeuse. Un exécutable peut très bien se cacher derrière une extension `.txt`.

Le CERTA a publié cette semaine une mise à jour de l'avis CERTA-2007-AVI-138. Ce dernier évoque une vulnérabilité dan s la commande `file` utilisée par plusieurs systèmes d'exploitation.

La vulnérabilité, de type « débordement d'entier », peut être exploitée sous la forme d'un fichier spécialement construit qui, manipulé par `file`, exécutera du code arbitraire à l'insu de l'utilisateur.

Le CERTA profite de cette occasion pour signaler que le fait de ne pas utiliser régulièrement dans un terminal ce genre de commandes ne signifie pas pour autant qu'une infection de la machine de cette manière est impossible. En effet, les commandes offertes par le système d'exploitation, comme ici `file` peuvent très bien être utilisées par d'autres applications. C'est le cas du logiciel libre antiviral `AMaViS` (branche maintenue : `amarisd-new`) qui utilise `file` pour caractériser les fichiers extraits des courriers électroniques. Ce dernier a donc publié un avis de sécurité le 05 juin 2007. Des développements internes d'applications peuvent présenter les mêmes vulnérabilités.

Documentation associée

- Avis de sécurité AMaViS du 05 juin 2007 :
  http://www.amavis.org/security/asa-2007-3.txt
- Vulnérabilité dans 'file' de référence CVE CVE-2007-1536 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1536
- Vulnérabilité dans 'file' de référence CVE CVE-2007-2026 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2026
- Vulnérabilité dans 'file' de référence CVE CVE-2007-2799 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2799

5 Les documents Microsoft Office, et la diffusion d'information

Le problème n'est pas récent, mais il semblerait qu'il reste méconnu auprès des utilisateurs de la suite bureautique *Microsoft Office*.

Lorsqu'un document est enregistré pour la première fois, par exemple `certa.doc`, il contient des données affichées à l'écran par *Word*. Supposons que le mot « CERTA » est ajouté dans le document.

Lorsque le document est modifié, c'est-à-dire que des données sont ajoutées, mais aussi effacées et changées, et que l'enregistrement se limite à appuyer sur `Ctrl + S` ou « `Enregistrer` », toutes les données peuvent être sauvegardées dans le corps du fichier. Dans l'exemple précédent, remplaçons « CERTA » par « CSIRT français ».

L'utilisateur pense que celles-ci n'existent plus, car elle n'apparaissent plus à l'ouverture de Word. Or il faut bien comprendre que Word interprète le fameux fichier, pour en afficher ce qu'il estime nécessaire. Visualiser le même fichier avec `bloc-notes` par exemple peut révéler que les informations pourtant effacées dans l'interface de saisie sont toujours présentes dans le document. Dans notre exemple, On y retrouve alors la chaîne de caractères `CERTA` qui avait pourtant été effacée.

Cette propriété est due à une option bien précise de *Microsoft Office*, qui s'appelle « les enregistrements rapides ». Lorsque celle-ci est activée, elle peut porter préjudice quand le document se diffuse, car il peut contenir des modifications, mais aussi des commentaires et d'autres informations que l'utilisateur n'a pas forcément envie de communiquer.

Pour toutes ses raisons, il est important de penser à :

- vérifier que l'option est bien désactivée. Elle l'est par défaut sous Office 2002 et Office 2007. En revanche, ce n'est pas le cas par exemple avec Office 98 et Office 2000. Pour cela :
  - cliquer en haut de la fenêtre sur « Outils »
  - sélectionner « Options »
  - se rendre dans l'onglet « enregistrement »
  - décocher la case : « Autoriser les enregistrements rapides »
- créer un nouveau document régulièrement, et de ne pas travailler en permanence sur les mêmes souches de fichiers ;
- convertir les documents avant de les communiquer à d'autres personnes sous un autre format ;

6 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 31 mai et le 07 juin 2007.

7 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

8 Rappel des avis émis

Durant la période du 01 au 07 juin 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-240 : Vulnérabilité dans GIMP
- CERTA-2007-AVI-241 : Multiples vulnérabilités dans IBM AIX
- CERTA-2007-AVI-242 : Vulnérabilité dans libpng
- CERTA-2007-AVI-243 : Vulnérabilité des produits Nortel
- CERTA-2007-AVI-244 : Multiples vulnérabilités des produits F-Secure
- CERTA-2007-AVI-245 : Multiples vulnérabilités dans les produits Mozilla
- CERTA-2007-AVI-246 : Vulnérabilité dans Novell Groupwise
- CERTA-2007-AVI-247 : Vulnérabilité dans inetd sur Sun Solaris
- CERTA-2007-AVI-248 : Vulnérabilités dans Symantec Veritas Storage
- CERTA-2007-AVI-249 : Vulnérabilité dans IBM Lotus Domino
- CERTA-2007-AVI-250 : Vulnérabilités dans Symantec Reporting Server
- CERTA-2007-AVI-251 : Vulnérabilité dans Sun Solaris Management Console
- CERTA-2007-AVI-252 : Multiples vulnérabilités de produits Computer Associates
- CERTA-2007-AVI-253 : Multiples vulnérabilités du serveur CIFS de HP-UX
- CERTA-2007-AVI-254 : Vulnérabilités de Symantec Ghost
- CERTA-2007-AVI-255 : Multiples vulnérabilités dans la machine virtuelle Java de Sun

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-226-001 : Vulnérabilité dans FreeType
  (ajout des références aux bulletins de sécurité Gentoo, Ubuntu)

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'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.

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 œuvre (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 COSSI/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.

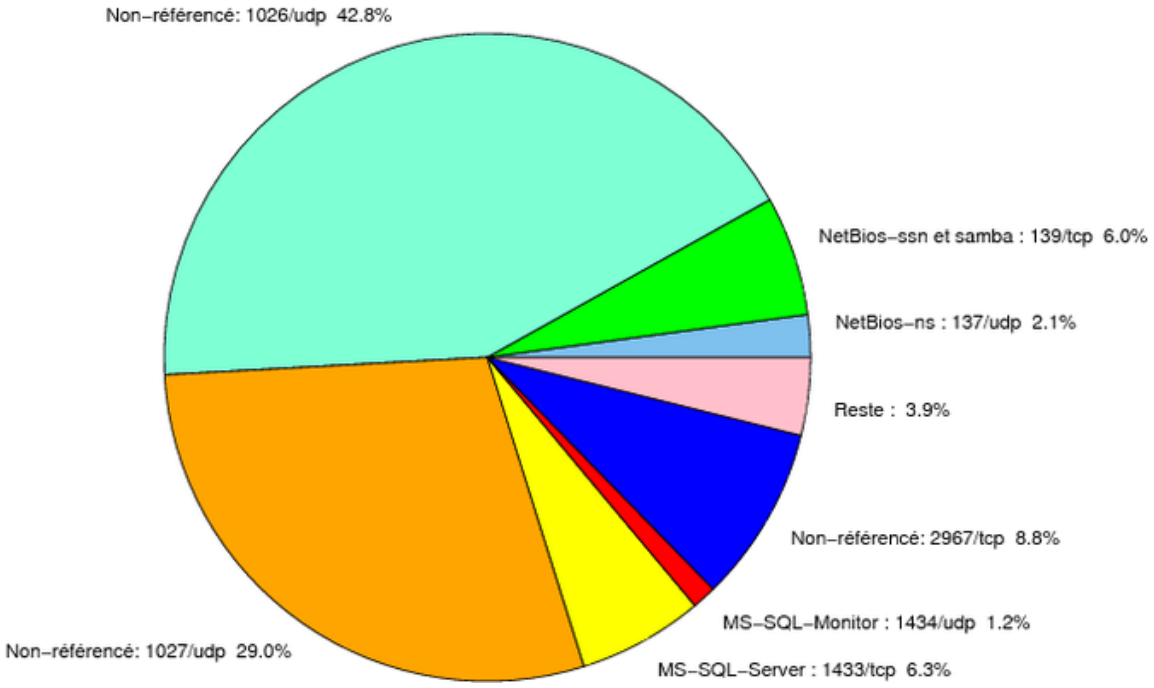

FIG. 1: Répartition relative des ports pour la semaine du 31.05.2007 au 07.06.2007

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	42.77
1027/udp	28.97
2967/tcp	8.8
1433/tcp	6.26
139/tcp	5.97
137/udp	2.11
1434/udp	1.21
22/tcp	0.64
80/tcp	0.58
4899/tcp	0.55
3128/tcp	0.39
1080/tcp	0.34
3306/tcp	0.25
3389/tcp	0.16
15118/tcp	0.09
143/tcp	0.06
2100/tcp	0.05
443/tcp	0.04
2745/tcp	0.03
5000/tcp	0.02
9898/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

08 juin 2007 version initiale.