Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 septembre 2007
N° CERTA-2007-ACT-039

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-39

Gestion du document

Référence	CERTA-2007-ACT-039
Titre	Bulletin d'actualité 2007-39
Date de la première version	28 septembre 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-039.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-039/

1 Intrusion : remise en cause de la protection globale

Quelle que soit son ampleur ou sa visibilité, une intrusion révèle un défaut dans les protections. Le retour à un niveau de sécurité convenable passe par une remise en cause des dispositions et des dispositifs utilisés.

1.1 Résumé des faits

Le site web d'un correspondant du CERTA a subi une modification illégitime qui pouvait paraître légère. Le premier symptôme était l'infection des ordinateurs des visiteurs. Le signalement par des internautes avait conduit l'exploitant à rechercher un virus sur le site, sans succès.

Le symptôme réel était l'insertion d'un javascript malveillant dans la page d'accueil. Le script construisait un cadre (`<IFRAME>`) invisible. Ce cadre conduisait l'internaute visitant le site public vers un site qui tentait de l'infecter. Un autre signalement avait permis la suppression du script malveillant.

Malgré cela, le phénomène a continué. La situation n'a pu évoluer qu'après analyse approfondie. Celle-ci a débouché sur la modification de la configuration des protections.

1.2 Recommandations

Une intrusion, même peu visible, révèle une insuffisance des protections. Le prélèvement des informations sur l'incident, y compris sur des éléments périphériques, est indispensable à l'analyse. Elle seule permet d'estimer l'ampleur de l'intrusion. En déterminant le mode opératoire des agresseurs et leurs actions, l'analyste proposera des actions correctives pour éviter une nouvelle intrusion et pour réparer des dommages aux données. La conséquence est une remise en cause des protections. Le processus est analogue à ce lui qui a précédé la mise en place de ces protections. Il est mentionné dans la note CERTA-2002-INF-002.

http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

Dans l'incident traité, les recommandations portent sur :

- le besoin d'en connaître ou de modifier :
  - inventaire des services utiles ;
  - contingentement des comptes utilisant ces services ;
  - exigence d'authentification ;
  - discrétion sur les briques logicielles utilisées ;
- la défense en profondeur :
  - filtrage réseau ;
  - robustesse et pérennité du système d'exploitation ;
  - filtrage applicatif ;
- la politique de traces, pour ne pas perdre d'information sur les évènements les plus anciens ;
- la configuration du système : versions utilisées, services indispensables, application des correctifs ;
- la gestion des comptes et des mots de passe.

2 Exportation des messages électroniques

2.1 Présentation

Les messages électroniques peuvent être lus par le biais d'interfaces web (`webmail`), ou directement sur un poste de travail, avec un client adapté. Parmi les clients les plus répandus, il peut s'agir de Outlook Express, de Microsoft Outlook, de Mozilla Thunderbird, d'Evolution, d'Eudora, d'IBM Lotus Notes (Domino), de Netscape Messenger, etc.

A un moment donné, l'utilisateur peut être amené à exporter la totalité, ou une partie, de ces courriers. Les raisons fréquentes conduisant à faire cela sont :

- un changement de machine, les courriers étant stockés localement sur le disque ;
- un changement de système d'exploitation ;
- un changement du client de messagerie ;
- une mise à jour du client de messagerie, ou du système d'exploitation, avec changement de version ;
- une volonté de sauvegarder et archiver les courriers sur un autre support/système ;
- un besoin d'analyser la messagerie sur un autre système de confiance ;
- etc.

Pour l'une ou l'autre de ces raisons, le choix du format d'exportation est primordial, pour éviter quelques soucis.

Voici deux courtes illustrations des difficultés pouvant être rencontrées :

- Sous Microsoft Outlook 2003, les courriers sont enregistrés avec une extension `.msg`, lorsqu'ils sont glissés/déposés de la boîte de messagerie vers un répertoire. Or ces fichiers ne peuvent pas être lus tels quels sous Outlook 2000 et Outlook 2002. Cette incompatibilité est due au fait que Outlook 2003 a enregistré le fichier `.msg` au format Unicode, qui n'est pas supporté par les anciennes versions du client. Pour désactiver cette propriété contraignante, il faut donc :
  - se rendre dans le menu "Outils" d'Outlook 2003 ;
  - choisir "Options" ;
  - aller dans l'onglet "Autre", et cliquer sur "options avancées" de la section "Général" ;
  - décocher la case "Utiliser le format de message Unicode pour enregistrer les messages.

– Microsoft permet d'exporter l'ensemble des données d'un utilisateur de Outlook (journal, tâche, courriers électroniques, etc.) en `.pst`. Cependant, suivant les versions de Outlook, le fichier résultant peut être par défaut en format ANSI (Outlook 2002 ainsi que les versions antérieures), ou Unicode. Une fois le fichier exporté, peu de clients de messagerie peuvent actuellement interpréter le fichier `.pst` ; c'est aussi le cas de Outlook Express.

Plusieurs formats sont disponibles pour exporter un courrier, ou l'ensemble de la messagerie. Outre `.pst`, ou `.msg`, il y a le format `maildir` de D.J. Bernstein ou le plus ancien `mbox`. Ce dernier a l'avantage d'être lisible par la grande majorité des clients. Il fonctionne de la manière suivante :

– un fichier est créé pour chaque dossier ;
– le contenu du fichier est facilement lisible, car codé en ASCII (7 bits).

Des variantes sont également proposées par des clients, comme `mboxrd`, `mboxo`, `mboxcl` ou `mboxcl2`. Ces variantes ne sont pas toutes compatibles et compréhensibles par n'importe quel client de messagerie. `maildir` est un format similaire en ASCII, mais un fichier d'export est créé par message, avec un nommage particulier. Certains clients le supportent également.

2.2 Recommandations du CERTA

Les courriers exportés sont souvent exportés dans l'objectif de les importer sur un autre système, ou d'y accéder après une période de temps plus ou moins longue. C'est typiquement le cas dans le cadre d'une analyse d'incident.

Il est donc important de considérer ces deux points pour la mise en œuvre et le déploiement de l'archivage et de l'exportation. Il faut prendre garde à ne pas choisir les options par défaut, et être attentif au format, sous peine d'avoir quelques surprises le jour où les archives doivent être utilisées.

Par défaut, il faut donc privilégier un format lisible et suffisamment répandu, et anticiper les conversions futures.

2.3 Documentation associée

– Publication Microsoft, « Le format et la taille limite de dossier du fichier .PST sont différents dans Outlook 2007 et Outlook 2003 » :
http://support.microsoft.com/kb/830336
– Documentation sur mbox :
http://www.qmail.org/man/man5/mbox.html
– Documentation sur le format maildir par D.J. Bernstein :
http://cr.yp.to/proto/maildir.html

3 Vulnérabilité dans Adobe Reader

Le chercheur qui avait publié les codes de démonstration concernant des vulnérabilités ou problèmes dans les lecteurs multimédia `Quicktime` et `Windows Media Player` (cf. Bulletin d'actualité CERTA-2007-ACT-038 du 21 septembre 2007) affirme avoir également trouvé une vulnérabilité critique touchant `Adobe Reader 8.1`. Une personne malveillante pourrait ainsi, par le biais d'un fichier `pdf` spécifiquement construit, exécuter du code arbitraire sur la machine d'un utilisateur ouvrant le fichier manuellement ou via son navigateur.

Aucun code de démonstration n'a été publié, ni d'explication supplémentaire quant à la nature de la vulnérabilité. Une personne de Adobe a déclaré travailler en ce moment avec le chercheur pour la publication d'un correctif, ce qui semble confirmer l'existence de la faille. Celle-ci pourrait toucher d'autres logiciels que `Adobe Reader`.

Le format `pdf` est souvent perçu à tort comme plus sûr que d'autres formats de documents. Comme pour les fichiers multimédias qui avaient fait l'objet d'un article dans le dernier bulletin d'actualité, ce format contient de plus en plus de fonctionnalités au fur et à mesure de son évolution; sa documentation fait aujourd'hui 1310 pages pour le format 1.7. On peut y voir, par exemple, qu'un fichier `pdf` peut contenir du `Javascript`, des vidéos, du contenu provenant de l'Internet, etc.. Certaines de ces fonctionnalités sont désactivables ou simplement non prises en compte suivant les logiciels utilisés, et présentent davantage de risques pour l'utilisateur.

Des méta-données peuvent également être ajoutées à un fichier `pdf`. Adobe décrit avec détail sur son site `XMP`, pour *Extensible Metadata Platform*. Cela permet d'ajouter de nouvelles propriétés à des objets comme des images, voir au document `pdf` en entier.

http://www.adobe.com/devnet/xmp/

Il est recommandé d'utiliser un lecteur minimaliste par défaut, c'est à dire supportant les fonctionnalités basiques du `pdf`, tout en se gardant la possibilité d'utiliser un logiciel plus avancé si besoin est, pour des fichiers provenant de sources sûres. Il faut toutefois faire attention à choisir une application maintenue à jour.

4 Les attaques en déni de service

Le CERTA traite parfois des demandes d'administrateurs persuadés que leurs systèmes ont été victimes d'attaques en déni de service.

Dans l'expression attaque en déni de service on retrouve deux notions. Celle de l'attaque qui implique une action malveillante volontaire, et le déni de service qui, selon la terminologie du CERTA, se définit ainsi : action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.

Donc, pour qu'il y ait un déni de service, il doit y avoir un dysfonctionnement d'un service, et pas seulement l'observation d'une forte activité. Par exemple, une aspiration de site génère un très fort trafic identifiable dans les journaux, mais n'est pas nécessairement un déni de service.

A l'inverse, s'il y a effectivement un dysfonctionnement, il ne s'agit pas forcement d'une attaque ; il peut s'agir tout simplement d'un dysfonctionnement technique lié à une panne, d'un problème de configuration ou d'une mauvaise utilisation. Pour reprendre l'exemple précédent, si l'aspiration provoque une surcharge entraînant un dysfonctionnement, il ne s'agit pas pour autant d'une attaque, mais plutôt d'une utilisation peu respectueuse de l'Internet (la courtoisie étant ici de signaler à l'administrateur l'aspiration du site, et d'éviter les heures où les visites sont les plus nombreuses).

Les attaques en déni de service existent et représentent un risque à prendre en compte, mais il faut bien faire attention à ne pas conclure trop vite. La qualification d'une activité comme attaque en déni de service exige *a priori* une analyse approfondie et technique de journaux et des traces.

4.1 Documentation

- Note d'information CERTA-2006-INF-002, « Terminologie d'usage au CERTA » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
- Note d'information CERTA-2000-INF-001, « Le déni de service distribué » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-001/
- Note d'information CERTA-2000-INF-003, « Évolution des outils de déni de service distribué » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-003/

5 Boîtiers opaques

Avec un accès ADSL, il est fréquent de disposer d'un routeur en lieu et place d'un traditionnel modem. Ce routeur offre généralement de nombreuses fonctionnalités comme le `Wi-Fi`, une interface `Bluetooth` ou `USB-Maître` pour brancher d'autres périphériques.

Bref, cet élément s'approche parfois d'un mini-ordinateur complet administrable généralement via une interface web. Le CERTA attire l'attention sur le fait que ces routeurs sont souvent livrés avec toutes ces fonctionnalités activées et dans une configuration par défaut ne répondant pas forcement aux exigences de sécurité de l'infrastructure. Il convient donc de choisir un routeur n'ayant que les fonctions qui sont indispensables et de les configurer correctement.

Par ailleurs, ces routeurs offrant des fonctionnalités évoluées et complexes, il n'est pas rare qu'ils soient vulnérables à des failles que l'on retrouve dans des produits plus classiques : les piles protocolaires (IP par exemple), l'interface web d'administration ou le pare-feu intégré. Il est donc important d'envisager ces routeurs comme des machines à part entière de l'infrastructure nécessitant des mises-à-jour, une configuration précise et une attention particulière compte tenu de leur rôle au sein du système d'information. Enfin, pour des raisons pratiques, les mots de passe sont souvent fixés à une valeur par défaut qu'il conviendra de changer dès que possible.

6 Vulnérabilités applicatives dans des produits et services Google

Cette semaine plusieurs vulnérabilités concernant des produits `Google` ont été annoncées. Elles sont détaillées dans les paragraphes suivants.

6.1 Google Mail

La première vulnérabilité concerne les utilisateurs de `Google Mail`. Un site malveillant pourrait, sous certaines conditions, modifier la configuration du compte `gmail` afin de donner accès aux courriers à un individu malintentionné. L'action effectuée consisterait à modifier les règles de filtrage de la messagerie.

Ceci relève surtout d'une fonctionnalité du « Web 2.0 », i.e. la propriété offerte par plusieurs sites de pointer librement vers les autres. Cette vulnérabilité n'est pas un lapin sorti du chapeau : elle correspond aux mêmes caractéristiques que celle décrite dans un précédent bulletin d'actualité; un lien inséré dans une page quelconque (sous forme d'IFRAME par exemple) peut forcer l'utilisateur à se déconnecter de son compte de messagerie Gmail. C'est également envisageable par le biais de flux RSS. Dans le cas présent, le lien peut modifier les filtres du compte de messagerie.

Dans ces conditions, la personne malveillante peut être amenée à créer deux filtres :

- l'un filtrant les messages du champ "FROM" avec l'adresse de l'utilisateur, et les redirigeant vers l'adresse de la personne malveillante ;
- l'autre filtrant les messages du champ "TO" avec l'adresse de l'utilisateur, et les redirigeant vers l'adresse de la personne malveillante.

Dans un cas, ce sont les messages envoyés par l'utilisateur qui sont lus incidieusement. Dans l'autre cas, ce sont les messages reçus. Le filtre peut aussi, plus simplement, jeter les messages filtrer.

6.1.1 Les recommandations du CERTA aux utilisateurs

Les recommandations traditionnelles s'appliquent ici encore. Il est préférable de :

- vérifier les filtres appliqués à sa messagerie Google Mail si l'on est utilisateur de ce service ;
- ne pas ouvrir de services Google avec d'autres navigations en cours vers des sites différents ;
- avoir une politique très rigoureuse sur la configuration du navigateur, et en particulier :
  - sur la gestion des fichiers de session ;
  - sur l'interprétation des codes dynamiques comme le Javascript ;
  - sur l'utilisation de sessions sécurisées en HTTPS.
- ne pas utiliser sa messagerie personnelle pour échanger ou transférer des courriers professionnels ;
- naviguer sur des sites de confiance uniquement, et ne pas cliquer trop rapidement sur des liens.

6.2 Google Urchin

`Google Urchin` est une version installée du portail `Google Analytics`. Une vulnérabilité de type injection de code indirecte (XSS) de `Google Urchin` pourrait permettre à une personne malintentionnée de tromper un utilisateur ou de lui voler ses identifiants de connexion.

Cette vulnérabilité utilise des adresses réticulaires construites de façon particulière qui pourraient être transmises par courrier électronique ou présentes sur une page web. Le CERTA rappelle une nouvelle fois qu'il est préférable de recopier une adresse réticulaire à la main dans le navigateur plutot que de cliquer sur un lien présent dans un courrier électronique ou une page web.

6.3 La gestion des images par Google Picasa

L'installation de Google Picasa souffre apparemment de problèmes similaires à ceux signalés dans les bulletins d'actualité CERTA-2007-ACT-020, CERTA-2007-ACT-022 ou CERTA-2007-ACT-029 : elle enregistre à l'occasion sur le système un nouveau format de protocole `picasa://`.

Une page malveillante peut donc contenir un lien commençant par `picasa://` afin d'accéder aux données de l'utilisateur, et en particulier ses photos. Ces dernières seront récupérées et stockées sur un serveur distant non légitime.

Il est possible de supprimer l'interprétation de `picasa://` du système, mais cela peut géner les utilisateurs du service. En revanche, si l'utilisation n'est pas nécessaire ou justifiée dans le réseau, il peut être intéressant de filtrer le contenu au niveau d'une passerelle web, à la recherche de liens réticulaires construits de cette manière.

6.4 Vulnérabilité dans Google Search Appliance

Une vulnérabilité de type injection de code indirecte (XSS) a été identifiée dans le matériel Google Code Search Appliance. La personne qui a publié cette vulnérabilité a également fourni une méthode assez simple pour identifier les sites utilisant une telle technologie, par le biais d'une requête dans le moteur de recherche web Google (Google Hack).

Ces technologies doivent être gérées avec la même rigueur que les sites Web associés. Elles font partie intégrante du parc informatique, et sont vues de l'extérieur comme élément du site. Les règles de filtrage doivent ainsi être respectées, ainsi que la gestion des flux et l'application de mises à jour.

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 20 et le 27 septembre 2007.

8 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/

9 Rappel des avis émis

Dans la période du 21 au 27 septembre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-409 : Multiples vulnérabilités dans les produits VMware
- CERTA-2007-AVI-410 : Vulnérabilité de KDE
- CERTA-2007-AVI-411 : Multiples vulnérabilités de Tivoli
- CERTA-2007-AVI-412 : Vulnérabilité dans HP-UX
- CERTA-2007-AVI-413 : Vulnérabilités dans libvorbis
- CERTA-2007-AVI-414 : Multiples vulnérabilités dans ImageMagick
- CERTA-2007-AVI-415 : Multiples vulnérabilités dans les produits CA ARCserve
- CERTA-2007-AVI-416 : Vulnérabilité du noyau Linux

– CERTA-2007-AVI-417 : Vulnérabilité de Webmin
– CERTA-2007-AVI-418 : Multiples vulnérabilités dans BrightStor Hierarchical Storage Manager
– CERTA-2007-AVI-419 : Vulnérabilité dans Tcl/Tk

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.

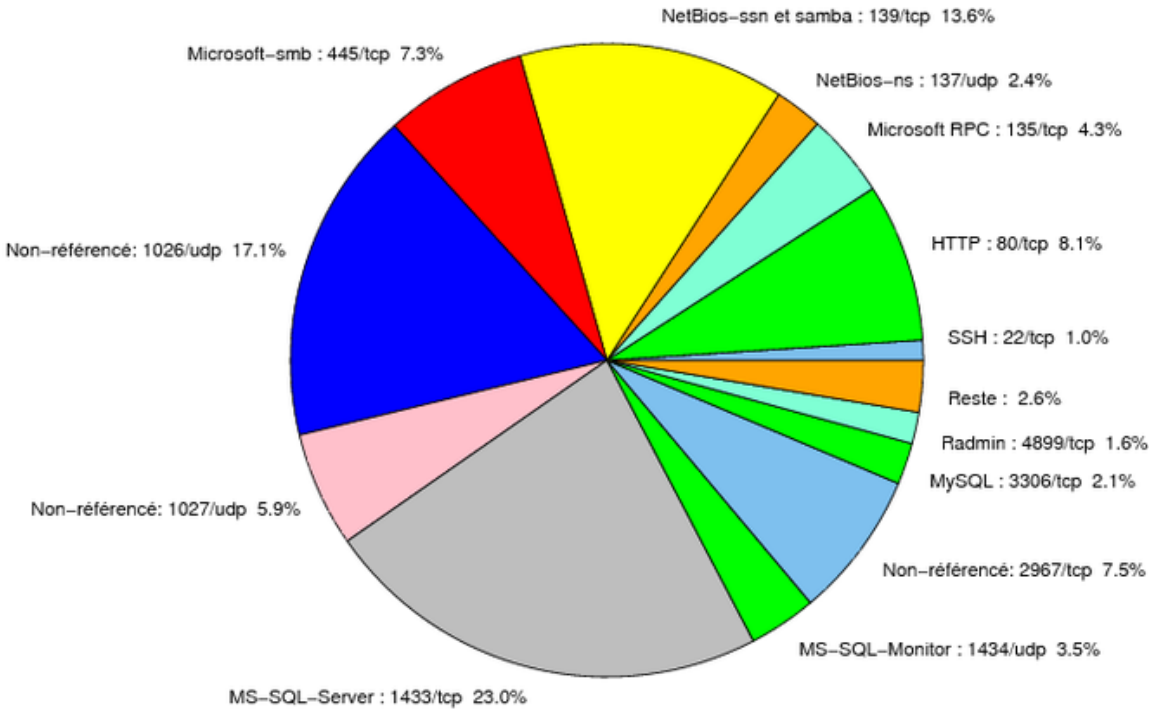

FIG. 1: Répartition relative des ports pour la semaine du 20.09.2007 au 27.09.2007

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
1433/tcp	22.99
1026/udp	17.06
139/tcp	13.57
80/tcp	8.1
2967/tcp	7.51
445/tcp	7.29
1027/udp	5.87
135/tcp	4.29
1434/udp	3.46
137/udp	2.44
3306/tcp	2.11
4899/tcp	1.6
22/tcp	1.01
25/tcp	0.61
1080/tcp	0.59
3128/tcp	0.56
21/tcp	0.37
23/tcp	0.13
143/tcp	0.1
3389/tcp	0.08
9898/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

28 septembre 2007 version initiale.