Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 octobre 2007
N° CERTA-2007-ACT-043

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-43

Gestion du document

Référence	CERTA-2007-ACT-043
Titre	Bulletin d'actualité 2007-43
Date de la première version	26 octobre 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-043.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-043/

1 Exploitation d'une vulnérabilité d'Adobe Reader

Cette vulnérabilité mentionnée dans le bulletin CERTA-2007-ACT-042 fait l'objet d'une exploitation très large.

1.1 Historique

La vulnérabilité concernant les URI sous Windows XP avec Internet Explorer 7 n'est toujours pas corrigée par Microsoft. De son côté, l'éditeur Adobe a publié le 22 octobre 2007 une mise à jour corrigeant l'exploitation de cette faille sur ses applications Adobe Reader et Adobe Acrobat (voir CERTA-2007-AVI-455).

Le correctif concerne seulement les versions 8 de ces logiciels. Une mise à jour pour Adobe Reader 7.09 et Adobe Acrobat 7.0 9 est en préparation mais n'est toujours pas disponible à la date de rédaction de ce bulletin. Les personnes utilisant cette version et ne pouvant pas migrer vers la version 8.1.1 peuvent toutefois appliquer le contournement provisoire disponible sur le site de l'éditeur.

1.2 Exploitation

Des exploitations de cette vulnérabilité ont également été détectées sur l'Internet. Une campagne de *spam* est en cours. Elle se présente sous la forme d'une pièce jointe de courriel qui, à son ouverture, télécharge par FTP un fichier malveillant après avoir désactivé le pare-feu de Windows. La mise à jour d'Adobe Reader et/ou Adobe Acrobat arrive donc à point nommé. Son déploiement ne doit pas être retardé.

Les sujets qui ont été signalés pour le moment sont en langue anglaise. Parmi eux :

- Your Credit File
- Personal Balance Report
- Your credit points
- Personal Credit Points
- Personal Financial Statement
- Your balance report
- Your credit report

Le nom des pièces jointes associées connues :

- your_bill.pdf
- invoice.pdf
- report.pdf
- debt.2007.10.XX.XXX.pdf

Attention, car l'ouverture des pièces jointes PDF sur un système vulnérable provoque l'exécution d'un fichier exécutable téléchargé à distance à l'insu de l'utilisateur.

Documentation

- Avis CERTA-2007-AVI-455 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-455/index.html
- Bulletin de sécurité Adobe APSB07-18 du 22 octobre 2007 :
  http://www.adobe.com/support/security/bulletins/apsb07-18.html

2 Les incidents traités cette semaine

2.1 Le suivi des correctifs

Le CERTA a traité cette semaine une compromission de site web. Suite à la découverte d'un cas de filoutage (*phishing*), le CERTA a mis en évidence la présence d'un programme malveillant de type `PHP Shell` (*C99Shell*) hébergé sur le serveur web. Ce dernier permettait aux individus l'ayant déposé de se connecter et de prendre le contrôle du serveur, même une fois corrigée la vulnérabilité exploitée à l'origine. Le CERTA a alerté les responsables du site web afin de rapidement fermer l'accès à celui-ci : cette mesure permet d'éviter de nouvelles victimes du site de filoutage (site factice bancaire) (*phishing*) et d'empêcher les communications malveillantes en provenance ou à destination du serveur. Il s'avère que ce site web utilisait une version vulnérable du composant `Joomla ExtCalendar` que les attaquants ont exploitée.

L'analyse des journaux des connexions et de la copie physique du disque ont permis de mettre en évidence les actions réalisées par les individus et les vulnérabilités exploitées.

Afin d'éviter une nouvelle infection, le composant vulnérable a immédiatement été enlevé de la version hors-ligne du site hébergé sur un serveur de pré-production. Afin de repartir sur les meilleures bases, le site web de production va être entièrement supprimé (afin d'éliminer d'éventuels programmes malveillants non-identifiés) et réinstallé à partir de sources de confiance (système à jour installé, applications nettoyées et pages récupérées depuis le site web de pré-production).

documentation

- Note d'information du CERTA sur les réactions à avoir suite à un incident :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

2.2 La sécurité des réseaux déconnectés

Cette semaine, lors d'une analyse sur un réseau isolé, le CERTA a constaté qu'une application gérant des informations personnelles sensibles était vulnérable. Théoriquement, l'accès à cette application nécessite de s'authentifier, or il est possible de contourner cette authentification en accédant directement aux fiches de toute personne inscrite sur l'application.

Concernant les réseaux non-connectés, il est fréquent d'entendre : « *Je ne peux pas avoir de problème de sécurité, mon réseau n'est pas connecté à l'extérieur* ». Ce n'est pas tout à fait exact.

Ces réseaux doivent eux-aussi être pris en compte dans la Politique de Sécurité des Systèmes d'Information (PSSI) car ils peuvent être sensibles :

- au déni de service : un code malveillant introduit (par une clef USB par exemple) sur ce réseau pourrait réaliser un déni de service ;
- aux altérations : un code malveillant pourrait compromettre et modifier les documents disponibles par l'application ;
- à la fuite d'information vers l'extérieur : une machine compromise pourrait récupérer des informations et les déposer sur un support amovible ;
- à la divulgation d'informations personnelles à des personnes n'ayant pas le besoin d'en connaître : dans le cas présent, la vulnérabilité donne accès aux adresses, téléphones, informations bancaires, numéros de pièces d'identité à toute personne connectée dans ce réseau ;
- etc.

Le fait que cette application vulnérable reste dans un environnement isolé (réseau local) ne suffit pas à la sécuriser. Dès lors qu'elle manipule ou donne accès à des informations personnelles, confidentielles ou sensibles, toutes les mesures de sécurité doivent être prises.

3 Fuite d'informations et réseaux sociaux

3.1 Présentation

Les sites permettant de créer des réseaux sociaux sur l'Internet font légion. Il y a parmi eux LinkedIn, Facebook ou MySpace. Ce phénomène de mode n'est pas sans risque pour les utilisateurs et les entreprises. Le CERTA tient à faire le point sur ces nouveaux outils de référencement des personnes. Les sites Internet de réseaux sociaux sont nombreux et très connus. Ils affichent des dizaines de millions d'inscrits et permettent de se créer un réseau de « connaissances » et de contacts et cela dans plusieurs buts :

- trouver des clients potentiels, des fournisseurs de service, des experts ou des partenaires ;
- être trouvé pour des opportunités de contrat ;
- chercher un emploi ;
- découvrir de nouveaux contacts via les connexions avec les réseaux de connaissances ;
- etc.

Ces sites peuvent être détournés par des personnes malveillantes afin de trouver des informations sur les entreprises ou sur les personnes et faire de l'ingénierie sociale. Les utilisateurs restent le maillon faible dans ces services en ligne et ils n'ont pas nécessairement conscience des risques d'indiscrétion liés à l'utilisation de ce genre de site.

3.2 Les risques

Il est important pour les entreprises et les particuliers de prendre la mesure des menaces que font courir ces sites et de noter la dangerosité de certaines de leurs fonctionnalités. En effet la nature des informations présentes dans le profil de l'utilisateur et dans sa liste de contacts peut permettre différents méfaits. Les contacts permettent de regrouper quelques informations. Ils peuvent être de différents types :

- des amis ;
- des personnes côtoyant les mêmes cercles (sportifs, associatifs, ...) ;
- des collègues de travail ;
- des relations professionnelles.

La question est donc bien : Cette liste doit-elle être publique ?

- il est possible d'intégrer le carnet d'adresses d'un client de messagerie dans les contacts et donc de faire sortir des données confidentielles de l'entreprise en quelques clics ;
- toute personne inscrite sur le site peut explorer les contacts des autres personnes. C'est le comportement par défaut s'il n'a pas été modifié. Il est possible de récupérer des informations sur les activités de l'entreprise grâce aux relations commerciales et aux partenaires qui y sont enregistrés. Ces données peuvent être intéressantes pour un concurrent à la recherche de nouveaux clients ou de compétences extérieures (intelligence économique) ;
- il est possible d'exporter l'ensemble des contacts dans un fichier de type CSV (*Comma-separated values*) et il est donc facile pour une personne malintentionnée de se créer une base de données d'informations personnelles issues de son réseau social pour une éventuelle campagne de filoutage ou de courriers électroniques indésirables.

Les informations du profil de l'utilisateur peuvent être également exploitées. Toutes les informations mises en ligne par l'utilisateur et en libre consultation sur Internet et peuvent rendre bien des services aux personnes malintentionnées en recherche d'informations pour une future attaque. Voici un extrait des risques potentiels :

- ces données peuvent éclairer sur l'organisation l'entreprise, découvrir des outils technologiques employés grâce à la consultation des curriculum vitae des employés (label, certification, etc.) ;
- un individu malveillant peut, grâce à la récolte de données personnelles ou relatives à une entreprise, orchestrer une attaque spécifique difficilement détectable et beaucoup plus pertinente.

3.3 Les contre-mesures

Tous ces risques peuvent être maîtrisés ou limités assez facilement.
Ce qui peut être fait par les employeurs :

- sensibiliser le personnel aux risques possibles ;
- élaborer une gestion précise des descriptions des contacts et modifier leurs politiques de sécurité afin d'intégrer ces risques et d'éduquer leurs employés sur une bonne utilisation des réseaux sociaux en ligne en leur faisant prendre conscience des inconvénients ;
- vérifier les informations rendues publiques sur ces sites et leur nuisance potentielle.

Ce que doivent faire les utilisateurs de tels services :

- éviter si cela n'est pas indispensable leur utilisation ;
- assurer la confidentialité du réseau de contacts afin de n'en faire profiter que les personnes concernées ;
- s'assurer de l'identité de la personne avant de l'intégrer à la liste de ces contacts ;
- ne pas diffuser d'information sensible.

Il est important que tous les acteurs mis en jeu dans ces réseaux sociaux soient conscients que les informations sont en libre accès comme si elles avaient été publiées dans la presse.

4 Les imprimantes sans-fil

Certains constructeurs d'imprimantes ou de combinés « scanner - imprimante » proposent des solutions sans-fil pour relier leurs périphériques à un ordinateur. Dans certains cas, ces interfaces Wi-Fi ou Bluetooth peuvent d'ailleurs être activées par défaut. Par ailleurs, ces périphériques embarquent souvent de nombreux services comme un serveur HTTP, des fonctionnalités de gestions de partages réseau pour les impressions de fichiers distants, ...

Il conviendra donc de prendre un certain nombre de précautions lors de l'intégration de ce type d'équipements dans un système d'information. En effet, il n'est pas forcement utile d'investir dans une solution offrant du « Wi-Fi » si celui-ci n'est pas utilisé *in fine*. Dans tous les cas, il faudra s'assurer que cette interface n'est pas activée par défaut ou configurée avec un niveau de sécurité insuffisant. Il faudra également vérifier que le contrôle d'accès ne permet aucune connexion extérieure vers le périphérique. Enfin, comme pour tout appareil, un intérêt tout particulier devra être porté sur les mises à jour à lui appliquer.

5 Mise à jour des serveurs racines DNS

Le protocole actuellement utilisé pour organiser la correspondance entre des noms de domaine et des adresses IP est le `DNS` (*Domain Name System*). Il fonctionne sous forme d'une base de données distribuée. Sa structure

ressemble à celle des systèmes de fichiers Unix : un arbre, avec un nœud racine représenté par le point (« . »). Chaque hôte d'un réseau a ainsi un nom, et le nom de longueur nulle est réservé à cette racine; ainsi, le nom complet du serveur web du CERTA est `www.certa.ssi.gouv.fr.`. Il s'agit du FQDN, ou *Fully Qualified Name*.

Les serveurs de nom de la racine savent où se trouvent les serveurs de noms des zones de niveau supérieurs, et font même souvent autorité sur les domaines génériques supérieurs (les gTLDs, ou *generic Top Level Domain*).

Les documents de référence décrivant ce protocole sont les RFC 1034 et 1035.

L'ICANN (*Internet Corporation for Assigned Names and Numbers* est l'organisme international en charge de la gestion globale du DNS. Ils ont récemment annoncé que le serveur racine L changera d'adresse le 01 novembre 2007.

Son ancienne adresse était : 198.32.64.12. Elle devient :

```
199.7.83.42
```

Il est bon de vérifier régulièrement, par exemple à chaque trimestre, la cohérence du fichier racine. Plusieurs solutions sont possibles pour faire cela :

- en modifiant à la main le fichier où ces adresses sont spécifiées (comme `db.cache` sous Bind) ;
- en récupérant une liste actualisée par FTP à l'une des adresses suivantes :
  - ftp://rs.internic.net/domain/db.cache
  - ftp://rs.internic.net/domain/named.cache
  - ftp://rs.internic.net/domain/named.root
  - ftp://ftp.internic.net/domain/db.cache
  - ftp://ftp.internic.net/domain/named.cache
  - ftp://ftp.internic.net/domain/named.root

Plusieurs clients de serveurs de noms, ou `resolvers` sont également interrogés localement par des applications. Ces `resolvers` gèrent l'interrogation des serveurs de noms, interprètent les réponses et retournent l'information au programme demandeur. Ils peuvent stocker localement les informations liées aux serveurs racines (fichiers *hints*). Ces derniers doivent donc être mis à jour si possible.

6 Communication massive par courriels

6.1 Faire parvenir l'information à l'utilisateur

Plusieurs courriels reçus dans sa boîte de messagerie ne sont malheureusement pas sollicités. Ils parviennent cependant à destination, du fait de la diversité des techniques utilisées pour contourner des filtres.

Ces courriels peuvent être les vecteurs de propagation de codes malveillants (cf. l'article concernant les formats PDF et DOC dans le bulletin d'actualité CERTA-2007-ACT-042).

Il peut aussi s'agir de courriels incitant l'utilisateur à se rendre sur un site malveillant, afin de télécharger un document malveillant, d'exploiter la vulnérabilité du navigateur ou de tromper l'utilisateur par de fausses pages Web (filoutage ou *phishing*).

Enfin, dans d'autres cas, l'objectif principal est de véhiculer de l'information très largement :

- pour désinformer rapidement et massivement. La propagation par courriels présente en effet un avantage certain, notamment si l'utilisateur transfère le message à d'autres personnes ;
- pour perturber, ou du moins influencer à une certaine échelle les valeurs boursières. Il s'agit d'un cas particulier de la situation précédente, où de fausses informations permettent de gonfler artificiellement les cours. Cette technique porte le nom de *pump & dump* ;
- pour inciter l'utilisateur à participer à des fraudes financières ou à donner gracieusement de l'argent, comme le « scam 419 » ou « arnaque nigériane ». Certains de ces dangers ont été évoqués dans le bulletin d'actualité CERTA-2007-ACT-007.

Dans tous les cas précédents, l'objectif premier des auteurs des courriels consiste à faire parvenir de l'information à un très grand nombre de personnes. Cela implique *a fortiori* d'éviter les politiques de filtrage mises en place. Le paragraphe suivant décrit deux méthodes qui sont actuellement utilisées pour arriver à cette fin.

6.2 Les images GIFs animées et les sons audio MP3

Pour mener à bien l'objectif précédemment décrit, deux méthodes parmi plusieurs autres, mais peu communes, sont, à la date de rédaction de cet article, utilisées.

1° les images GIFs animés ;

2° les fichiers de sons MP3.

6.2.1 Les images GIFs animés

Cette forme n'est pas toute récente, puisque certains sites en faisaient mention dès septembre 2006. Elle permet de contourner des techniques de filtrage d'images courantes. Les antivirus s'appuient par exemple sur la signature des informations en texte qui se trouvent dans le code de l'image. Le format GIF permet d'associer plusieurs images, et de les compresser ensemble. Chaque fichier GIF contient donc un ou plusieurs blocs correspondant à des images différentes. L'astuce actuellement utilisée consiste à afficher une lettre par image. L'utilisateur visualisant le GIF en animation verra le texte complet, par exemple "C", puis "E", puis "R", puis "T" et "A".

Le CERTA avait mentionné dans le bulletin d'actualité CERTA-2007-ACT-027 ce problème, avec les courriers non sollicités au format `PDF`. Il s'agit de la problématique duale des `captchas` (*Completely Automated Test To Tell Computers and Humans Apart*). Ces images ont pour objectif de ne pouvoir être interprétables que par un œil humain. Ces mêmes techniques peuvent tout aussi bien être appliquées pour tromper les mécanismes de filtrage des antivirus (non humains...).

- Documentation W3C sur *Graphics Interchange Format*, version 89a :
  http://www.w3c.org/Graphics/GIF/spec-gif89a.txt
- Bulletin d'actualité CERTA-2007-ACT-027, « Courriers non sollicités et documents PDF » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-027.pdf

6.2.2 Les fichiers de son MP3

L'autre forme, moins commune, est l'envoi en pièce jointe de fichiers MP3. Le CERTA a récupéré cette semaine quelques échantillons de ces courriels. Les fichiers MP3 vus se caractérisent par :

- une très mauvaise qualité audio ; la taille n'excède pas la centaine de kilo-octets, et un débit de 16kb/s ;
- les durées des messages sont courtes, inférieures à une minute ;
- les fichiers audio ne contiennent pas de méta-données, comme celles pouvant être fournies au format ouvert `ID3 Tag` : informations sur le titre, l'interprète, l'album, etc.

6.3 Les recommandations du CERTA

L'imagination est aux commandes dans ce domaine, et il est possible d'imaginer tout type de format. Cette année, le CERTA a donc cité entre autres des fichiers Excel, des images en PDF, des animations GIF, des fichiers MP3, mais la liste ne s'arrête pas là.

Les antivirus ont régulièrement besoin d'un temps d'adaptation entre la diffusion de ces nouvelles stratégies et la mise en œuvre de leurs filtrages. Par ailleurs, comme il a été précédemment mentionné, ce filtrage n'est pas évident à réaliser, donc pas toujours efficace et pertinent.

L'utilisateur, lui qui est destinataire de ces messages, n'a pas de moyen `a priori` de déterminer si la pièce jointe est de l'information diffusée en masse, ou une forme pernicieuse de code malveillant.

La meilleure des protections consiste donc à ne pas ouvrir les pièces jointes, surtout si elles ne proviennent pas de sources de confiance. S'il y a le moindre doute, il est vivement recommandé de demander conseil à son responsable de sécurité ou au CERTA avant toute ouverture.

7 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 18 et le 25 octobre 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 19 au 25 octobre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-444 : Vulnérabilité dans IrfanView
- CERTA-2007-AVI-445 : Multiples vulnérabilités dans Opera
- CERTA-2007-AVI-446 : Multiples vulnérabilités dans des produits Mozilla
- CERTA-2007-AVI-447 : Multiples vulnérabilités dans des produits Cisco
- CERTA-2007-AVI-448 : Multiples vulnérabilités dans des produits Nortel
- CERTA-2007-AVI-449 : Vulnérabilité EAP dans les produits Cisco
- CERTA-2007-AVI-450 : Vulnérabilité dans RealPlayer
- CERTA-2007-AVI-451 : Vulnérabilité dans Nagios
- CERTA-2007-AVI-452 : Vulnérabilité de CA HIPS
- CERTA-2007-AVI-453 : Vulnérabilités de Netscape Navigator
- CERTA-2007-AVI-454 : Vulnérabilité dans la machine virtuelle Java
- CERTA-2007-AVI-455 : Vulnérabilité d'Acrobat et Adobe Reader

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.

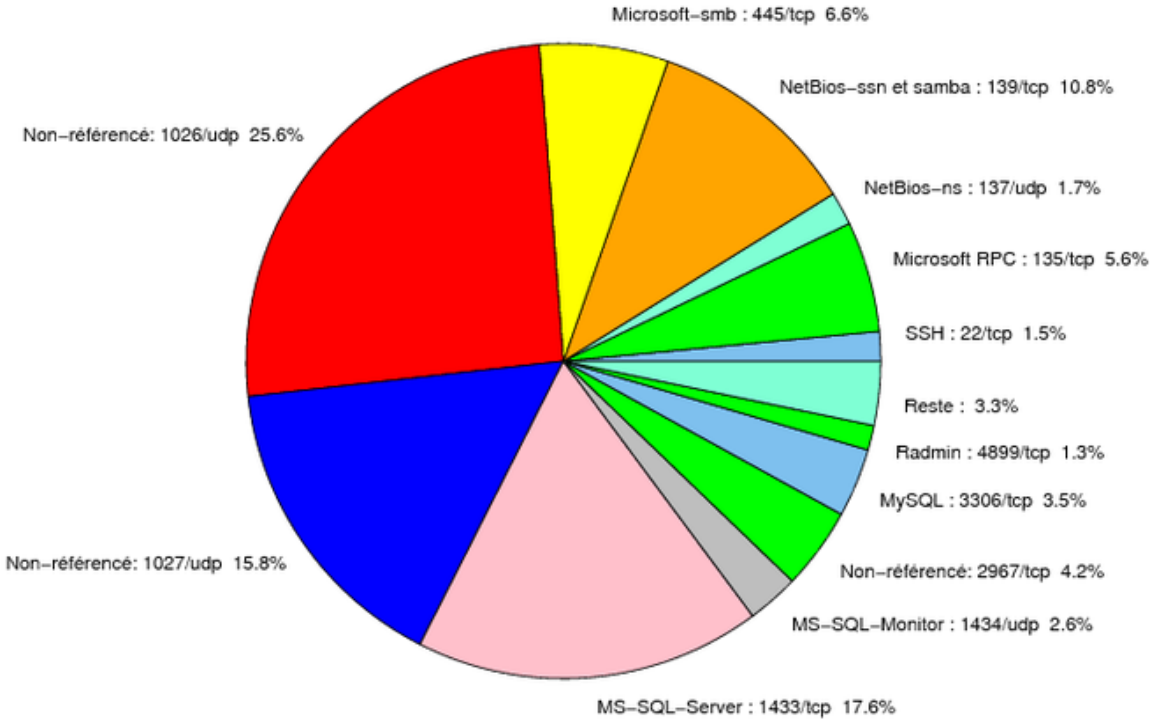

FIG. 1: Répartition relative des ports pour la semaine du 18.10.2007 au 25.10.2007

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

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
1026/udp	25.56
1433/tcp	17.64
1027/udp	15.75
139/tcp	10.82
445/tcp	6.55
135/tcp	5.64
2967/tcp	4.16
3306/tcp	3.49
1434/udp	2.64
137/udp	1.69
22/tcp	1.49
4899/tcp	1.25
80/tcp	0.93
1080/tcp	0.78
21/tcp	0.39
3128/tcp	0.34
25/tcp	0.23
143/tcp	0.17
443/tcp	0.1
2100/tcp	0.08
9898/tcp	0.04
15118/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 11
3 Paquets rejetés 12

Gestion détaillée du document

26 octobre 2007 version initiale.