Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 juin 2007
N° CERTA-2007-ACT-025

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-25

Gestion du document

Référence	CERTA-2007-ACT-025
Titre	Bulletin d'actualité 2007-25
Date de la première version	22 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-025.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-025/

1 Mots de passe et incidents

Le CERTA traite régulièrement des incidents liés à l'utilisation frauduleuse d'identifiants de connexion. Nous distinguons trois catégories principales d'incidents :

- les mots de passe faibles ;
- les mots de passe mal protégés ;
- la capture des mots de passe.

1.1 Les mots de passe faibles

La fragilité des mots de passe est un problème fréquemment rencontré. De nombreux utilisateurs conçoivent leur mot de passe en se basant entre autres sur des mots du dictionnaire, des dates ou des noms propres. Il arrive parfois que le mot de passe soit tout bonnement le nom du compte. Ce phénomène survient souvent avec les comptes de test ou encore au moment de la création des profils utilisateur. Cette faiblesse expose les machines à des accès frauduleux, notamment suite à des attaques dites « par dictionnaire ». Ces attaques sont assez courantes, les services SSH et FTP ayant été particulièrement ciblés ces dernières années.

Quelques mesures peuvent être mises en place pour prévenir ce risque. L'une d'entre elles consiste à forcer le changement de mot de passe lors de la première connexion de l'utilisateur et à appliquer des règles de construction particulières (utilisation obligatoire de plusieurs groupes différents parmi les majuscules, minuscules, chiffres et caractères spéciaux, longueur minimum, etc.). L'administrateur peut également tester régulièrement la robustesse des mots de passe à l'aide de certains outils.

1.2 Les mots de passe mal protégés

Les mots de passe sont parfois stockés « en clair » dans certains fichiers qui sont accessibles par tous. Le CERTA a traité quelques cas d'incidents d'accès frauduleux rendus possible car le mot de passe était en clair dans un fichier accessible depuis l'Internet. Il est extrêmement important d'éviter de stocker les mots de passe dans des fichiers. Si ce n'est pas possible, alors il convient de mettre des droits très restrictifs sur ces fichiers.

Il est important de garder à l'esprit que les mots de passe sont parfois stockés « accidentellement » dans des fichiers. C'est le cas avec les historiques d'interpréteur de commandes lorsque les identifiants sont passés en paramètres d'une ligne de commande et avec les journaux de connexion lorsque l'utilisateur saisit par erreur son mot de passe au lieu du nom de compte.

1.3 La capture des mots de passe

Un grand nombre d'applications ont un mécanisme d'authentification faible car il repose sur l'envoi du mot de passe « en clair ». C'est le cas, entre autres, pour TELNET ou FTP. Le mot de passe peut être intercepté par des utilisateurs sur le même réseau local (notion beaucoup plus large dans le cas d'un réseau sans-fil) qui feraient usage d'un renifleur réseau (`sniffer`).

Il est suggéré, quand c'est possible, de chiffrer l'authentification. Par exemple, pour les serveurs Web, il est possible d'utiliser le protocole HTTPS. Les attaques par capture seront beaucoup plus complexes à réaliser. De même, le remplacement de TELNET par SSH, et de FTP par SCP, SFTP ou FTPS est une bonne chose.

Enfin, la capture est possible directement sur le poste de l'utilisateur si un enregistreur de frappes clavier ou de mouvement de la souris est installé, que la phase d'authentification soit chiffrée ou non. Il n'y a pas de réelle parade à ce type d'attaques, une fois l'enregistreur installé. L'hygiène informatique et comportementale doit prévenir l'installation d'un tel code malveillant.

Documentation

Note d'information CERTA-2005-INF-001 « Les mots de passe » :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/

2 Les cadres pour photos numériques WiFi et autres « *gadgets* » autonomes

Après les lapins communicants Nabaztag discutés dans le bulletin d'actualité CERTA-2006-ACT-052, de nouveaux périphériques multimédia réseaux autonomes voient le jour. Parmi ceux-ci, il y a les cadres photo numériques. Ces nouveaux appareils se présentent sous la forme d'un cadre contenant un écran LCD et permettant de faire défiler des photos ou des films. Alors que les versions les plus répandues nécessitent que les médias à afficher soient chargés dans la mémoire de l'appareil via soit une connexion directe à un ordinateur, soit un support amovible (clef USB ...), les derniers modèles sont dits « communicants » et peuvent automatiquement récupérer les fichiers sur un ordinateur en se connectant au réseau local, voir même sur Internet. Les "e-lapins" ne s'installaient qu'au domicile d'une catégorie d'utilisateurs restreints, mais ce type d'objets décoratifs pourrait séduire un plus large public.

Outre le fait que ces appareils peuvent présenter les mêmes risques que tout support de données amovibles en USB, comme décrits dans la note d'information CERTA-2006-INF-006, ces cadres sont également des machines , avec un système d'exploitation et une interface réseau (WiFi). Bien que succinctes, ces machines possèdent donc les même caractéristiques qu'un vrai ordinateur (des services, de l'espace de stockage..). Seulement, pour celles-ci, il est difficile de contrôler l'état des mises à jour des correctifs de sécurité, et ses activités.

Certains cadres pour photos numériques WiFi offrent deux modes pour récupérer les photos :

– ils se connectent à un serveur Internet dédié, et récupèrent les photos que l'utilisateur aura laissées sur son espace personnel sur ce même site ;

– ils se connectent à l'ordinateur, sur lequel une application dédiée a été installée et permet le partage derépertoires.

Dans les deux configurations, il est difficile actuellement de comprendre les interactions exactes qui ont lieu.

Associer un cadre à une machine d'un réseau revient donc à donner à une machine inconnue et non maîtrisée un accès aux réseaux interne et externe. Par ailleurs, pour plus de simplicité et de convivialité, l'utilisateur est encouragé à partager des images présentes sur son ordinateur avec le cadre, et donc ouvrir un accès privilégié à un utilisateur virtuel inconnu.

Ce type de périphériques WiFi au contenu inconnu a tendance à « *gadgétiser* » l'utilisation du réseau et à faire baisser de façon drastique le niveau de sécurité et la prise de conscience du degré de risque.

Le CERTA est revenu à plusieurs reprises dans ces dernières publications sur les risques liés aux pilotes des interfaces sans-fil. Il s'agit d'une problématique importante, et difficile à gérer. Il est donc normal d'apporter le plus grand doute sur ces appareils WiFi qui ne font aucune mise à jour, et qui présentent par ailleurs les même caractéristiques qu'une machine.

Le CERTA déconseille fortement de les relier à un réseau professionnel. Il invite également ses correspondants à auditer régulièrement les bâtiments à la recherche de « *gadgets* » communiquants, qu'ils soient sous forme de cadre ou de lapin, et à sensibiliser les utilisateurs aux risques de leur utilisation.

3 Fausses mises à jour Microsoft

De nombreux codes malveillants exploitent des techniques d'ingénierie sociale de façon à tromper l'utilisateur afin qu'il réalise lui-même une action qui le mènera à compromettre son ordinateur.

Parmi ces techniques, ils existent les fausses mises à jour pour Microsoft Windows. En général, ces codes malveillants se propagent par messagerie électronique en usurpant une adresse électronique provenant de Microsoft. Tout en prétextant une mise à jour critique, ils incitent l'utilisateur à "double cliquer" sur la pièce jointe ou à suivre un lien. En fait de mise à jour, l'internaute naïf installe un code malveillant.

L'une des dernières variantes de ces codes malveillants utilise l'interface que Microsoft présente à l'utilisateur. Elle peut apparaître en visitant un site (fenêtre surgissante). Ainsi, cette boîte de dialogue ressemble à s'y méprendre à la véritable boîte de dialogue de mise à jour de Microsoft Windows.

L'application ou/et l'annonce de mise à jour pour Microsoft Windows ne se fait jamais par messagerie électronique et ce pour au moins deux raisons :

– les risques liés à l'utilisation de la messagerie électronique dont l'usurpation d'identité ;
– l'existence du mécanisme de mise à jour automatique dans Microsoft Windows.

C'est pourquoi dès la réception d'un message électronique annonçant la publication de mise à jour de sécurité pour Microsoft Windows, il est recommandé de :

– ne pas suivre le lien proposé ;
– ne pas ouvrir une pièce jointe au message ;
– réaliser l'opération "Windows Update" manuellement.

Il en va de même si une fenêtre apparait étrangement à l'écran.

Il est possible de vérifier la véracité de tels messages de mise à jour en se rendant sur le site de l'éditeur :
http://www.microsoft.com/technet/security/current.aspx

4 Les cadres incorporés, ou *IFRAME*

4.1 Présentation générale

Un `IFRAME` est un élément proposé par HTML 4.0, qui permet d'afficher dans une page Web, un cadre, contenant du code HTML local ou distant. Parmi les attributs offerts avec l'élément, il y a :

– `src` : la source du contenu à insérer dans le cadre ;
– `name` : le nom du cadre, permettant de construire des liens vers celui-ci ;
– `frameborder` : variable servant à activer ou désactiver la bordure ;
– `longdesc` : description du contenu du cadre ;
– `scrolling` : variable donnant la possibilité ou non d'utiliser la roulette de la souris ;
– ainsi que toutes les options pour gérer le cadre, comme sa visibilité, sa largeur, sa longueur, sa position dans la page, les marges, etc.

Cet élément est très semblable fonctionnellement à un autre élément, nommé `OBJECT`. Cependant, ce dernier est inclus, lui, dans le type de documment « HTML Strict » (la déclaration se fait normalement dans les premières lignes du document HTML). Le contenu de l'élément `IFRAME` ne devrait être affiché, en revanche, que par les navigateurs qui ne reconnaissent pas le cadre ou qui sont configurés pour ne pas les afficher, comme en illustre l'exemple suivant :

```
<_IFRAME src="http://www.certa.ssi.gouv.fr" width="400" height="500"
        scrolling="auto" frameborder="1">
Si vous lisez ce message, cela signifie que votre navigateur
ne reconnait pas les cadres,
ou que votre configuration en empeche l'affichage.
Vous pouvez néanmoins visualiser la page en vous rendant sur :
<_A href="http://www.certa.ssi.gouv.fr"> la page CERTA </_A>
</_IFRAME>
```

Les fonctionnalités sont multiples, et il est également possible d'imbriquer des jeux d'encadrement (cf. l'élément `FRAMESET`).

4.2 Des défigurations de sites

Plusieurs incidents ont été récemment signalés. Le mode opératoire est le suivant :

1° plusieurs sites sont défigurés en très peu de temps. Cette phase de défiguration massive est généralement dûe à une vulnérabilité nouvellement trouvée sur une application Web ou sur une administration laxiste (cf. Section 1);

2° la défiguration du site, loin d'être évidente, consiste au simple ajout d'un élément `IFRAME` dans la page. Celui-ci passe donc assez inaperçu.

3° les utilisateurs qui naviguent sur une des pages défigurées se voient redirigés par le champ "src" de l'`IFRAME` (directement ou après quelques redirections) vers une page malveillante. Celle-ci contient un ensemble de vulnérabilités choisies en fonction du poste de l'internaute. Lorsque le navigateur de l'utilisateur interprète à son insu cette page, ces vulnérabilités compromettent le système s'il n'est pas à jour ou s'il est configuré de manière trop laxiste ;

4° cette contamination permet d'obtenir un ensemble de machines compromises zombis (*botnet*), utilisées pour lancer des attaques en déni de service. Mais, elle permet aussi de dérober différents types de données et d'informations depuis les machines compromises.

4.3 Les recommandations du CERTA

4.3.1 à l'administrateur

Pour l'administrateur du site, il faut garder à l'esprit que l'utilisation de ce genre de cadres peut être dangereuse par nature. En effet, il s'agit d'intégrer dans une page légitime un contenu extérieur non maîtrisé. Défigurer la page vers laquelle l'`IFRAME` pointe permet de défigurer tous les sites ayant l'élément `IFRAME`.

L'intégrité, sur les sites relativement statiques, doit être rigoureusement surveillée, par exemple avec des techniques d'empreintes (MD5, SHA1, etc.), ces dernières n'étant pas stockées sur le même serveur. Une simple surveillance de l'aspect visuel des pages n'est clairement pas suffisant, pour plusieurs raisons :

- cette tâche peut difficilement être faite sur l'ensemble des pages d'un site conséquent ;
- cette tâche est purement humaine et visuelle : l'administrateur risque ainsi de ne pas apercevoir de minimes défigurations, comme un changement de commentaire d'une figure, ou une phrase de texte.
- tout changement dans le code de la page, et non visible, ne sera pas détecté. Le cas des `IFRAME` en est un excellent exemple.

L'administrateur du réseau doit aussi prévenir ce genre de compromission, en limitant par exemple l'usage des `IFRAME` à certains sites, ou en appliquant quelques règle simples. Une source "src" écrite avec une adresse IP n'est pas courante par exemple, sauf dans le cas des attaques précédemment décrites. Dans l'exemple ci-dessous, le format du champ "src" est peu commun, ainsi que le style, et l'`IFRAME` n'a aucun contenu pour les navigateurs ne reconnaissant pas le cadre :

```
<_IFRAME src="XX.XX.XX.XX/index.php (...) style="display:none">
</_IFRAME>
```

L'option de style aurait tout aussi bien pu être "visible:hidden", voir ne rien chercher à dissimuler.

4.3.2 à l'utilisateur

Il est toujours possible de refuser l'affichage des cadres `IFRAME`, même si cette solution peut perturber la navigation de plusieurs sites. Sous Firefox, cela se fait par le biais de l'adresse « about:config » dans la barre d'adressage, en modifiant la variable `browser.frames.enabled` à *false*. Sous Internet Explorer, il est possible, dans l'onglet « Sécurité » qui spécifie les niveaux de sécurité de la zone Internet, de personnaliser l'option « Lancement des programmes et des fichiers dans un iFrame ».

De manière générale, les incidents cités ci-dessus ont surtout posé problème aux utilisateurs qui n'avaient pas les dernières mises à jour appliquées sur leur système d'exploitation. La méthode décrite ne fait qu'attirer les utilisateurs de manière artificielle vers des codes exploitant des vulnérabilités connues. C'est pourquoi le CERTA insiste encore et à nouveau sur l'importance d'avoir un système à jour, surtout quand celui-ci est connecté à l'Internet.

5 *MOSEB : Month of search engine bugs*

Dans la lignée des *month of browser bugs*, *month of PHP bugs* et autres initiatives divulguant des failles sur des applications spécifiques en un mois, juin 2007 est consacré à des vulnérabilités trouvées sur des moteurs de recherche : le *MOSEB*, ou *month of search engine bugs*. A la date de rédaction de cet article, 20 moteurs de recherche différents ont fait l'objet de publication de vulnérabilités, soit un par jour avec parfois plusieurs failles les concernant.

Parmi ces moteurs de recherche, on rencontre les plus connus tels que google.com, yahoo.com, lycos.com et msn.com.

Les failles sont toutes des injections indirectes de code ou *cross-site scripting* (XSS), et détaillées avec des exemples d'exploitation qui montrent les risques de ce type de vulnérabilité : injection de code html, redirection, exécution de code sur le poste de l'internaute, etc.

Des exemples intéressants de vulnérabilités concernent les moteurs de recherche locaux, comme `Google Custom Search Engine` et le moteur local d'Altavista. Les risques sont les mêmes que pour les autres moteurs, mais l'étendue est plus grande. Les attaques en *cross-site scripting* sont en effet alors possibles sur tous les sites implémentant ces moteurs locaux sans protection supplémentaire.

Certaines failles ont d'ores et déjà été corrigées. Ce *month of search engine bugs* nous montre cependant qu'un site offrant un moteur de recherche n'est pas nécessairement de confiance pour deux raisons principales :

- il retourne du contenu (les pages ou les adresses de pages indexées, les images, etc.) qui ne dépend pas de lui. Ce contenu peut être malveillant.
- il prend comme données d'entrée les requêtes de l'utilisateur, ce qui peut favoriser les attaques de type injection de code indirecte (XSS).

Tout lien associé à une page proposant un moteur de recherche est donc à suivre avec précaution, la première étant la désactivation du Javascript.

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 14 et le 21 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 15 au 21 juin 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-264 : Vulnérabilité dans OpenOffice
– CERTA-2007-AVI-265 : Vulnérabilités dans Safari
– CERTA-2007-AVI-266 : Vulnérabilité dans Novell NetWare
– CERTA-2007-AVI-267 : Vulnérabilité de Tomcat
– CERTA-2007-AVI-268 : Vulnérabilité dans Apache SpamAssassin
– CERTA-2007-AVI-269 : Vulnérabilités dans Astaro Security Gateway
– CERTA-2007-AVI-270 : Vulnérabilité dans HP System Management Homepage
– CERTA-2007-AVI-271 : Vulnérabilités dans IBM WebSphere Application Server
– CERTA-2007-AVI-272 : Vulnérabilité dans les produits F-Secure
– CERTA-2007-AVI-273 : Vulnérabilités dans VLC Media Player
– CERTA-2007-AVI-274 : Vulnérabilité dans PHPMailer

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

– CERTA-2007-AVI-025-003 : Multiples vulnérabilités de Xorg
(ajout de la référence au bulletin HP.)

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.

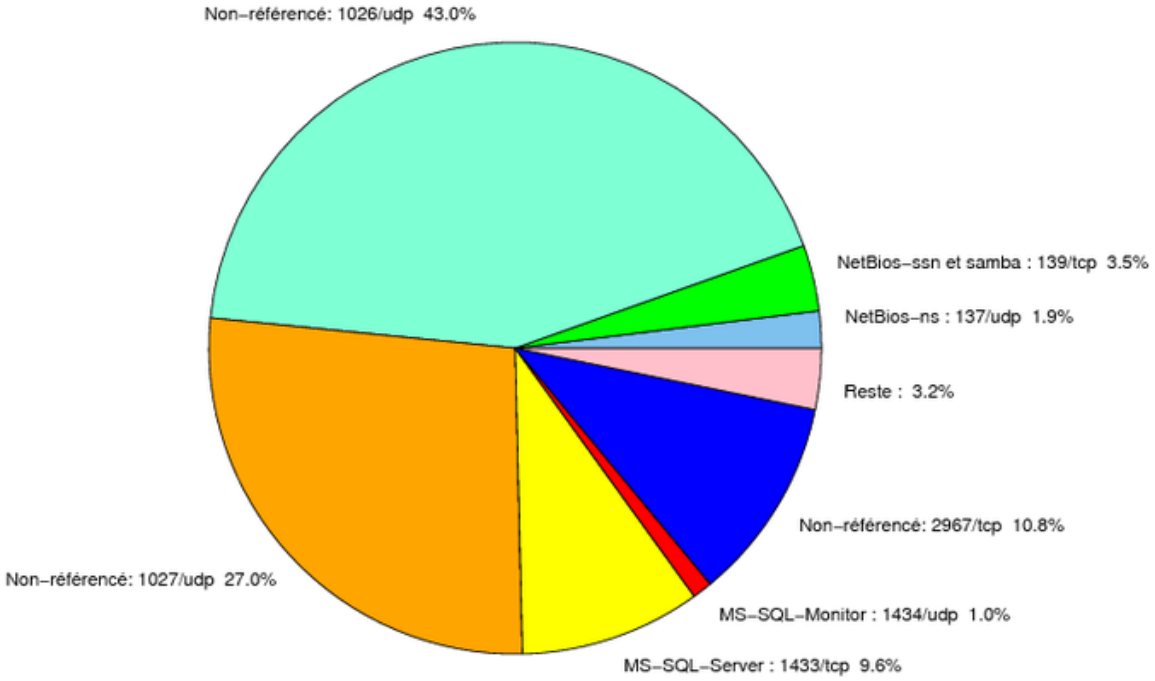

FIG. 1: Répartition relative des ports pour la semaine du 14.06.2007 au 21.06.2007

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	42.98
1027/udp	26.95
2967/tcp	10.77
1433/tcp	9.56
139/tcp	3.49
137/udp	1.94
1434/udp	1.04
4899/tcp	0.66
22/tcp	0.53
80/tcp	0.38
25/tcp	0.28
443/tcp	0.23
1080/tcp	0.21
3389/tcp	0.19
3128/tcp	0.12
3306/tcp	0.11
15118/tcp	0.09
143/tcp	0.02
9898/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

22 juin 2007 version initiale.