Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 août 2007
N° CERTA-2007-ACT-033

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-33

Gestion du document

Référence	CERTA-2007-ACT-033
Titre	Bulletin d'actualité 2007-33
Date de la première version	17 août 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-033.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-033/

1 Retour de congés : période critique pour les postes

Comme à chaque retour d'une absence prolongée, le poste de travail que l'utilisateur rallume présente un retard dans la mise à jour des logiciels. Ces logiciels regroupent le système d'exploitation, les applications bureautiques ou spécialisées, les logiciels divers comme les antivirus, les utilitaires de transfert, d'archivage ou de sauvegarde…

Avant et pendant tout le processus de la mise à jour, les vulnérabilités des logiciels ne sont pas encore corrigées. Par contre, elles ont été publiées. Les agresseurs les ont analysées. Ils ont eu le temps de préparer des programmes qui exploitent les faiblesses et leur permettent de prendre le contrôle des postes.

L'organisation, la politique des droits, l'architecture et les outils présents sur le réseau de l'organisme permettent de répondre de manière très variée à ce problème. Une solution, peu réaliste hors des très petites structures, consiste à ce qu'un utilisateur présent allume les postes des absents lorsque son propre poste se met à jour et provoque (ou laisse se faire) la mise à jour des postes des absents. L'outillage, par exemple un gestionnaire de configuration, peut forcer la mise à jour du poste dès qu'il est allumé. Une autre stratégie utilise un sas virtuel. Tout poste non complètement à jour n'est autorisé à effectuer que des connexions restreintes. Lorsque le poste, rallumé, a fini sa mise à niveau, il recouvre entièrement ses droits à connexion.

Dans tous les cas, l'utilisateur doit être informé de la fragilité de son poste lorsqu'il rentre d'une absence prolongée. La navigation sur Internet doit être limitée ou retardée. La vigilance doit être renforcée lors de la

lecture des courriels qui se sont accumulés dans la boîte aux lettres. Il vaut ainsi mieux attendre la fin des mises à jour pour ouvrir les pièces jointes des courriels.

Lorsque les absences sont très longues (maternité, longue maladie) ou que le poste est resté sans utilisateur pendant plusieurs mois (ex. : poste pour un saisonnier), la fragilité du poste à son redémarrage est accrue d'autant. L'administrateur du parc doit veiller à ce que les mises à jour soient faites soit régulièrement, soit en bloc dans un contexte contrôlé.

2 Adobe Flash et balayage de ports

La technologie Adobe Flash est de plus en plus utilisée pour rendre les sites Internet plus interactifs, dynamiques ou pour créer des jeux en ligne.

L'animation au format Adobe Flash porte souvent l'extension `.swf` et peut être jouée par un lecteur qui est intégré au navigateur, et donc visualisée dans le contexte de pages Web ou jouée par une application séparée. Le format de fichiers Adobe Flash, pour permettre plus que des animations passives, repose sur le langage de programmation ActionScript qui est semblable au JavaScript. Il permet par exemple dans le cadre d'un jeu, de proposer des interactions à l'utilisateur mais aussi d'échanger des informations, telles que les scores, avec le serveur.

A l'aide d'ActionScript, il est possible d'essayer d'ouvrir des connexions avec une machine distante. L'interprétation des erreurs que cette dernière peut retourner permet d'obtenir des informations sur celle-ci, comme les ports ouverts et les services correspondants. Un animation Adobe Flash peut servir à rechercher illégalement des informations sur une machine tierce depuis le poste d'un utilisateur et à son insu.

L'exécution des animations reposant sur un lecteur et non pas directement sur le système d'exploitation, ce qui rend le détournement de fonctionnalité en est indépendant et donc réalisable sur un grand nombre de plates-formes. Ce détournement est similaire à celui qui avait été réalisé en Javascript et présenté dans le bulletin d'actualité du CERTA 2007-ACT-014 du 06 avril 2007. L'attaque par Adobe Flash semble plus efficace que celle avec javascript pour lancer des balayages de ports.

En d'autres termes, la simple visite d'une page Web contenant un code en Flash spécialement construit donne l'opportunité à une personne extérieure de balayer les ports de plusieurs machines dans le réseau interne.

Pour se protéger de cette vulnérabilité, il est conseillé de désactiver par défaut la lecture des animations Flash. Si cela s'avère nécessaire, il ne faut autoriser la lecture des animations que provenant de sites de confiance.

Enfin, le CERTA insiste de nouveau sur le fait que tout code dynamique (Flash, Java, Javascript ou ActiveX...) doit rester désactivé par défaut.

3 Gadgets et Widgets

Microsoft a publié cette semaine une mise à jour corrigeant des failles dans des « gadgets » de `Windows Vista`, détaillées dans l'avis CERTA-2007-AVI-359.

Les gadgets ou *widgets* sont de deux types : de petites applications de bureau pouvant fournir des informations visuelles sur le bureau de l'utilisateur (*desktop widgets*) ou des modules de sites Internet (*web widgets*) développés en HTML, Javascript, Flash, etc. offrant le même type d'informations et affichés sur des sites les supportant (par exemple, iGoogle, Microsoft Live, MySpace ou des blogs construits avec `Wordpress` ou `TypePad`). La météo, les cours de bourse, une calculatrice, un affichage de flux RSS, etc. sont des exemples d'informations affichées pour l'utilisateur. Comme les *web widgets* interprétés par un site Internet, les *desktop widgets* sont interprétés par un moteur, les plus connus étant `Google Desktop`, `gDesklets`, `Windows Vista Sidebar` et `Apple OSX Dashboard`. Des moteurs de gadgets existent également pour les téléphones mobiles.

Dans le cas des gadgets de bureau, il s'agit d'applications téléchargées, qui peuvent donc contenir du code malveillant. Même écrits sans esprit malveillant, les gadgets peuvent présenter des vulnérabilités, leurs développeurs se préoccupant souvent peu des problèmes de sécurité.

Plusieurs possibilités d'exploitation de vulnérabilités ont récemment été présentées pour les gadgets de bureau et sur internet, permettant l'interception de connexions, la récupération d'identifiants, l'exploitation de failles du navigateur, etc. La problématique est globalement la même que celle évoquée pour les `ActiveX`, ou les extensions de `Firefox`, car il s'agit du téléchargement, de l'installation ou de l'interprétation non contrôlée de codes sur le système.

Concernant `Windows Vista`, ce sont les gadgets Météo, Contacts et Titres qui présentaient des failles de sécurité, chacune permettant l'exécution de code arbitraire à distance dans `Windows Vista Sidebar`. Pour le gadget Météo, cela pouvait se produire en cliquant sur un lien malicieux, pour le gadgets Contacts en ajoutant un fichier de contact spécifiquement construit et pour le gadget Titres en s'abonnant à un flux RSS malicieux.

Ces failles sont d'autant plus dangereuses que le rendu HTML est effectué par `Internet Explorer 7`, mais n'utilise pas le « mode protégé » du navigateur disponible sur `Windows Vista`.

Les recommandations concernant les gadgets en général sont peu surprenantes et similaires aux extensions de navigateurs :

- par défaut, il faut désactiver et éviter d'utiliser ces fonctionnalités ;
- si nécessaire, n'installer et n'autoriser que ceux correctement signés et connus ;
- utiliser les gadgets respectant les modèles de développement les concernant (le standard W3C `Widgets 1.0`).

Liens utiles :

Avis du CERTA CERTA-2007-AVI-359 du 14 août 2007 :

http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-359/index.html

4 SSL, fichiers de session et prudence

4.1 Présentation

Au cours d'une conférence en sécurité survenues début août 2007, deux chercheurs ont présenté une technique d'attaque appelée `SideJacking`. Elle est présentée dans le contexte d'un réseau sans-fil Wi-Fi et cible les utilisateurs visitant certains sites populaires.

Plusieurs sites offrent des services complexes aux utilisateurs, comme de la messagerie, des espaces personnels sous forme de bloc-notes, de la publicité adaptée intégrée aux pages Web ou la consolidation de réseaux sociaux, etc. Parmi ceux-ci, on peut évoquer Google Mail, Yahoo Mail!, BlogSpot, MySpace, LinkedIn, FaceBook, Google Adsense, etc.

L'identification initiale pour se connecter à ce genre de service peut utiliser une connexion protégée HTTPS (SSL *Secure Socket Layer*). Cependant, pour des raisons techniques, le choix consiste parfois à ne pas poursuivre la session établie en HTTPS et à utiliser une connexion en clair (HTTP).

Une fois que l'utilisateur est authentifié, les serveurs produisent un `identifiant de session` qui est récupéré par le navigateur, sous forme de fichier de session (*cookie*) ou contenu dans l'adresse réticulaire (URL). Des efforts sont généralement faits pour rendre cet identifiant peu prévisible. Malheureusement, cette information circule en clair dans le réseau, et peut être récupérée par une personne malveillante.

Récupérer cet identifiant, et l'utiliser pour se connecter au site Web s'appelle le `SideJacking`. Les auteurs proposent ainsi de renifler simplement le trafic sans-fil à la recherche de ces fameux identifiants. Une fois trouvés, il suffit de les importer dans un navigateur, et de se connecter au site. Cela donne accès directement à l'espace de l'utilisateur, tant que celui-ci ne se déconnecte pas explicitement. La fraude permet d'accéder à la plupart des manipulations et des données à la disposition de l'utilisateur. La possibilité de changer le mot de passe de l'utilisateur reste difficile, car elle nécessite souvent d'entrer le mot de passe en cours.

Cette technique leur a permis de faire quelques démonstrations spectaculaires, et notamment d'accéder aux messageries de certaines personnes de l'assistance.

4.2 Les choses à retenir

Prenant l'exemple de Google Mail, deux options sont possibles à la date de rédaction de ce document :

- l'adresse `https://www.gmail.com` utilise HTTPS pour la phase d'identification, et continue la session en clair ;
- l'adresse `https://mail.google.com` utilise HTTPS pour toute la durée de la session.

En théorie, la deuxième option empêche donc l'attaque précédemment citée d'avoir lieu. Cela est vrai quand seule la messagerie est ouverte. Si l'utilisateur, depuis sa session existante, ouvre un autre service (Reader, Photos, Calendar, etc.), l'identifiant de session est cette fois envoyé en clair au site Google. Donc l'intérêt de la protection est définitivement perdu. La session peut être « *sidejackée* ».

Il s'agit d'une illustration des risques. D'autres sites sont susceptibles d'avoir le même comportement.

Cette attaque n'est pas en soi récente, ni révolutionnaire. Tout trafic récupéré en clair, est une source d'information importante qui peut être récupérée par des mains et un clavier malveillants. Dans le cas présent, ce sont les courriers électroniques ou les listes de contacts qui sont accessibles. L'opération est aussi facilitée dans le contexte du monde sans-fil, car les fameuses trames circulent dans les airs, et sont donc aisément récupérables. Si la connexion est complètement ouverte (aucun chiffrement, comme cela peut se voir pour certains points d'accès publics) ou utilise un chiffrement mauvais (WEP), un logiciel qui automatise la procédure rend l'attaque triviale.

L'attaque exige de pouvoir lire les trames. Elle sera plus complexe que lancer un simple exécutable pour des chiffrements Wi-Fi plus solides (WPA, WPA2), car il faut d'abord déchiffrer les trames.

Le CERTA recommande enfin la plus grande prudence lors de la navigation sur des réseaux qui ne sont pas de confiance, les réseaux sans-fil, les points d'accès en libre service, les cyber-cafés, etc.

5 Les affichages dissimulés à l'intérieur de page Web

Dans son bulletin d'actualité CERTA-2007-ACT-025 du 25 juin 2007 le CERTA présentait des compromissions mises en œuvre ou utilisant un `IFRAME` dont l'affichage pouvait être dissimulé :

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

Une autre balise, `DIV`, plus banale qu'un `IFRAME`, peut également être utilisée à des fins malveillantes :

```
<_DIV id=".." style="display:none">
<A href="http://XX.XX.XX.XX/(..)"> (..) </A>
</_DIV>
```

Cette balise sert normalement à structurer un document HTML en plusieurs sections.

Dans ce cas, le lien dissimulé ne sera pas affiché mais pourra par exemple augmenter la popularité du site auquel il fait référence en profitant d'un manque de contrôle des robots de certains moteurs de recherche.

Cette construction peut être utilisée par des individus malveillants lors de la compromission d'un site Internet ou insérée de manière discrète dans des pages légitimes modifiées mais pas défigurées.

Il est également possible de rencontrer des instructions de ce genre dissimulées à l'intérieur du code de certains thèmes pour site Web à télécharger sur l'Internet. Parfois très populaires, ces thèmes peuvent être téléchargés et installés sur des millions de sites, les codes sources de ces thèmes étant disponibles sur plusieurs sites parfois malveillants ou compromis.

Le CERTA recommande, tout comme pour les fichiers d'installation, de n'utiliser que des sources de confiance pour installer un produit, une application ou un thème pour site Internet. Le site de l'éditeur ou celui du créateur sont à privilégier.

La recherche systématique dans le code source des mots clef `IFRAME` ou `DIV` peut s'avérer infructueuse. En effet, dans le bulletin d'actualité CERTA-2007-ACT-032, le CERTA abordait une compromission dans laquelle le code malveillant était dissimulé à l'aide de `javascript`. C'est pourquoi lors de la compromission d'une machine, et si possible périodiquement dans une option préventive, il faut contrôler l'intégrité de l'ensembles des fichiers et données présents sur cette machine.

5.1 Documentation

- Bulletin d'actualité CERTA-2007-ACT-025 du 25 juin 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-025.pdf
- Bulletin d'actualité CERTA-2007-ACT-032 du 10 août 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-032.pdf

6 Des façons originales de diffuser de la publicité

Un nouveau concept de communication a fait son apparition, il s'agit de faire passer un message incluant un certain niveau d'interactivité avec le destinataire. Cela peut se présenter comme un panneau publicitaire auquel est ajouté une borne possédant une interface Bluetooth. L'utilisateur est invité à activer la connexion Bluetooth de son périphérique (téléphone portable ou assistant personnel) et de configurer celui-ci en mode "découverte".

De telles bornes interactives sont visibles dans Paris par exemple.

Cette interaction implique de diminuer fortement le degré de protection de son périphérique : activer le mode "découverte", autoriser un périphérique inconnu à accéder aux ressources de son appareil. Ce moyen de communication peut être détourné par des utilisateurs malintentionnés, au moyen d'ingénierie sociale, afin d'accéder au ressources d'un appareil non sécurisé. Par analogie, cela revient à laisser une porte ouverte à tous sur son portable. Or ce genre d'appareils est difficilement maîtrisable, contôlé, mis à jour, etc. Le CERTA a également expliqué dans de précédentes publications que la notion de courte portée en Bluetooth est trompeuse, car les interactions peuvent avoir lieu avec des éléments distants de quelques centaines de mètres.

Le CERTA a publié une note d'information portant spécifiquement sur les réseaux sans fil Bluetooth en y ajoutant les recommandations liées à l'utilisation d'un appareil disposant d'une interface Bluetooth.

6.1 Documentation

– Note d'information du CERTA sur la sécurité des réseaux sans fil Bluetooth, du 01 août 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003/

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 09 et le 16 août 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 10 au 16 août 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-350 : Multiples vulnérabilités dans Cisco IOS
– CERTA-2007-AVI-351 : Multiples vulnérabilités dans HP OpenView
– CERTA-2007-AVI-352 : Multiples vulnérabilités dans IBM AIX
– CERTA-2007-AVI-353 : Vulnérabilité dans Microsoft XML Core services
– CERTA-2007-AVI-354 : Vulnérabilité dans Microsoft Excel
– CERTA-2007-AVI-355 : Vulnérabilité de Microsoft OLE
– CERTA-2007-AVI-356 : Multiples vulnérabilités dans Internet Explorer
– CERTA-2007-AVI-357 : Vulnérabilité dans le moteur de rendu graphique Microsoft (GDI)
– CERTA-2007-AVI-358 : Vulnérabilités dans Windows Media Player
– CERTA-2007-AVI-359 : Vulnérabilités dans les Gadgets de Microsoft Windows Vista
– CERTA-2007-AVI-360 : Vulnérabilité de Microsoft Virtual PC et Virtual Server
– CERTA-2007-AVI-361 : Vulnérabilité dans le gestionnaire VML de Windows

– CERTA-2007-AVI-362 : Multiples vulnérabilités de Tomcat
– CERTA-2007-AVI-363 : Vulnérabilité dans Opera
– CERTA-2007-AVI-364 : Vulnérabilités dans CISCO VPN Client
– CERTA-2007-AVI-365 : Multiples vulnérabilités dans IBM DB2
– CERTA-2007-AVI-366 : Vulnérabilité de Sun Java Runtime Environment (JRE)

Pendant la même période, l'avis suivant a été mis à jour :

– CERTA-2007-AVI-341-001 : Vulnérabilité dans gpdf
(ajout des références aux bulletins de sécurité Mandriva, Debian, SuSE, Red Hat)

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.

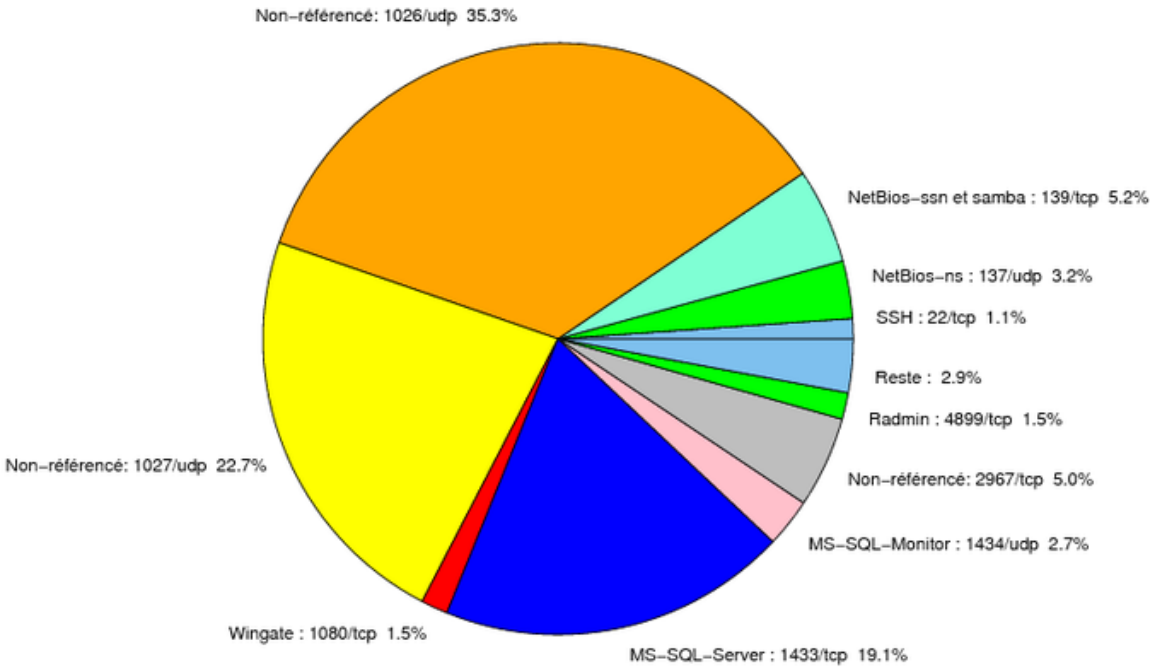

FIG. 1: Répartition relative des ports pour la semaine du 09.08.2007 au 16.08.2007

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	35.27
1027/udp	22.65
1433/tcp	19.12
139/tcp	5.2
2967/tcp	4.98
137/udp	3.15
1434/udp	2.65
1080/tcp	1.47
4899/tcp	1.45
22/tcp	1.09
3128/tcp	0.6
25/tcp	0.52
80/tcp	0.41
443/tcp	0.28
3306/tcp	0.26
3389/tcp	0.22
143/tcp	0.16
23/tcp	0.09
9898/tcp	0.03
5554/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

17 août 2007 version initiale.