Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 octobre 2007
N° CERTA-2007-ACT-040

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-40

Gestion du document

Référence	CERTA-2007-ACT-040
Titre	Bulletin d'actualité 2007-40
Date de la première version	05 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-040.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-040/

1 Quand l'attaquant referme la porte

Cette semaine le CERTA a traité une compromission d'un serveur web qui hébergeait un site bancaire frauduleux (*phishing*). Lors du premier contact avec le propriétaire du site web, cette personne a informé le CERTA que ce genre de désagrément s'était produit régulièrement malgré le retrait systématique du contenu frauduleux.

Le CERTA rappelle que lors d'un incident de sécurité, il faut éviter de supprimer des données qui pourraient être utiles à l'analyse ou à une éventuelle enquête judiciaire. Dans cet incident, l'analyse a mis en évidence que, dans un premier temps, l'attaquant a utilisé une faille dans le code PHP d'une page : une variable dont le contenu n'est pas suffisamment protégé. Une fois le contrôle de la machine obtenu et en y déposant des portes dérobées (*PHP Shell*), l'attaquant a lui même corrigé la page vulnérable. Sa correction n'était d'ailleurs pas dénuée d'humour car lors d'une tentative d'exploitation de la vulnérabilité la page affichait un message personnalisé de l'attaquant.

Le langage PHP offre beaucoup de facilités qu'il convient d'utiliser avec précaution. L'une d'entre elles est l'inclusion de pages passées en paramètre dans l'adresse réticulaire (*URL*) lors de l'appel de la page. Ces variables doivent être limitées aux seules pages du site ou faire l'objet de contrôles sémantiques et syntaxiques.

1.1 documentation

- Note d'information du CERTA sur le bon usage du langage PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/index.html
- Bulletin d'actualité du CERTA sur les inclusions PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-003.pdf

2 Question de point de vue

Cette semaine, le CERTA a été informé par l'un de ses homologues européens de la présence d'un outil malveillant (*malware*) sur le site Internet d'une administration. Suite au contact avec cette administration, ce qui aurait put être une compromission plutôt classique d'un serveur web pour y déposer un virus, se révèle être beaucoup plus important. En effet, la victime, qui ne s'était pas aperçue de la présence du virus sur son serveur, a pris contact avec son hébergeur. Celui-ci lui a indiqué un comportant anormal de la machine depuis plusieurs jours. Selon la société d'hébergement, le serveur compromis tentait d'initier un volume important de connexions vers des pays étrangers. L'état actuel de l'analyse de cet incident ne permet pas d'identifier l'origine ni le but de ces connexions.

Un serveur connecté à l'Internet est parfois accessible par plusieurs services. Inversement, il peut lui-même, si les règles de filtrage sortantes ne sont pas suffisamment rigoureuses, établir des connexions vers l'extérieur.

Le CERTA insiste donc sur le fait que l'analyse de journaux applicatifs est une très bonne chose, mais n'est pas suffisante. Il faut considérer, dans le cadre d'une bonne vigilance, plusieurs types de journaux concernant différents services, différentes couches protocolaires, et éventuellement compléter par ceux d'autres systèmes périmétriques (pare-feu, serveur DNS, etc.). Il faut surveiller depuis plusieurs points de vue le système.

2.1 documentation

- Note d'information du CERTA sur le filtrage et les pare-feux :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001/index.html
- Note d'information du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html

3 Les défigurations des pages Web difficilement visibles

3.1 Défigurations non visibles ?

Une définition de « défigurer » pourrait être « modifier l'aspect ». Il est courant d'utiliser ce terme pour une page Web, lorsque son apparence est modifiée. L'internaute visitant cette page ne voit pas ce qui est légitime.

Par extension, (ou abus de langage selon certains), la défiguration d'un site Web peut également concerner toute modification du code source de la page. En réalité, il se mélange deux concepts différents :

1° l'injection illégitime de code dans une page Web ;

2° les finalités de cette injection.

Si l'une de ces finalités consiste à modifier, d'une manière quelconque, l'aspect visuel de la page Web, alors il s'agit bien d'une défiguration. Dans les autres cas, il y a bien une perte d'intégrité du code source de la page, mais les raisons sont différentes.

Dans tous les cas, l'origine du problème reste l'injection de code, qui met en évidence un défaut de garantie de l'intégrité de la page, qu'il faut comprendre.

Plusieurs cas ont été médiatisés cette semaine, et le CERTA a traité ces derniers mois de nombreux incidents liés à des injections de code ne modifiant pas l'aspect visuel, mais le code source. Le responsable d'un serveur Web doit connaître ces risques.

3.2 Les objectifs

Injecter du code dans une page Web peut avoir plusieurs finalités, comme nous venons de le voir. En voici quelques-unes à valeur d'illustration :

- la défiguration, pour communiquer et s'exprimer sur un thème donné ; Qu'il s'agisse d'une réaction à un événement politique, économique, ou social, la défiguration est alors un moyen pour exprimer des idées. Elle met en avant des éléments (textes, vidéos, images) parfois violents, calomnieux et/ou répréhensibles ;

– l'augmentation de notoriété d'un site Internet. Les moteurs de recherche ont par exemple des mécanismes prédéfinis pour organiser l'affichage des résultats. Injecter dans de nombreux sites le lien vers une page peut largement augmenter sa notoriété. L'exploitation de cette notoriété est un autre sujet qui n'est pas abordé ici ;
– l'injection de code dynamique pour différents motifs, afin de faire effectuer une action sur le navigateur de l'utilisateur naviguant sur la page, comme une redirection vers un autre site. Il peut s'agir d'un site de filoutage. Il peut également s'agir de traçabilité, afin d'identifier les adresses des personnes accédant au site d'origine ;
– l'injection de code dynamique pour tester et exploiter plusieurs vulnérabilités touchant les navigateurs. Les conséquences peuvent alors être la compromission complète du système vulnérable de l'internaute naviguant sur le site.

3.3 Différentes manières

Les injections de code seront différentes en fonction des finalités, et elles peuvent évoluer. Celle que l'on rencontre souvent actuellement fait l'objet de nombreux articles dans les précédents bulletins d'actualité et concerne la balise HTML IFRAME.

```
<_iframe src="http://wwww.monSiteTresMalveillant/... style="display:none">
</_iframe>
```

Mais il est fait mention dans CERTA-2007-ACT-033 de la balise définissant les sections DIV :

```
<_DIV id=".." style="display:none">
      <_a href="http://wwww.monSiteTresMalveillant/... </a>
</DIV>
```

Il est aussi possible d'ajouter directement un code Javascript :

```
      <_SCRIPT language=javascript>
              function MauvaiseIntension() {
                      alert("Mauvaises intensions en cours...");
      </_SCRIPT>
```

Comme le bulletin CERTA-2007-ACT-035 l'évoque, il reste possible d'exploiter des fonctionnalités associées aux données de style (CSS), soit au niveau de la page HTML, soit dans l'un des fichiers de style associé.

D'autres *scénarii* sont imaginables pour mettre en œuvre les objectifs cités dans le paragraphe précédent.

3.4 Les recommandations du CERTA

3.5 De manière générale

Plusieurs démarches peuvent être entreprises pour limiter les risques. En particulier :

– ne pas naviguer, ni même se connecter sur l'Internet depuis une machine contenant des données sensibles ;
– au cours de la navigation, il faut se limiter à des sites de confiance. Cette politique peut être renforcée par l'application de listes blanches. Les limites de ces listes ont cependant été abordées dans le bulletin CERTA-2007-ACT-037 ;
– il faut configurer les navigateurs avec une politique très rigoureuse ;
– les passerelles Web doivent être adaptées à ce genre de menace ;
– il reste possible d'utiliser des navigateurs « légers » en cas de doute. Certains permettent de visualiser un contenu très épuré, comme par exemple `w3m` ou `lynx`.

3.6 Le filtrage au niveau d'une passerelle

Les passerelles Web permettent normalement de faire un filtrage du contenu. Les *proxys* locaux comme `privoxy` offrent également une telle possibilité. Le filtrage est souvent effectué sous la forme d'expressions régulières, qui caractérisent des chaînes de caractères données. Dans l'hypothèse où les chaînes sont normalisées, l'application de ces expressions permet de générer des actions intéressantes.

La chaîne suivante est un exemple permettant de filtrer les balises IFRAME. L'action peut alors être de supprimer, ou de modifier le cadre d'origine. Ici, elle est transformée pour pointer systématiquement sur une fenêtre

du CERTA. Elle signifie que dans une chaîne de la forme "<iframe>...</iframe>", tous les caractères commençant à "src=" et finissant avant le "<" de "</iframe>" sont remplacés par la chaîne spécifiée.

```
  FILTER: Remove all iframes from webpages
s|(<iframe.*)src=.*(</iframe)|$1src=http://www.certa.ssi.gouv.fr frameborder=1
                                  width="200" height="180" scrolling="no"$2|igU
```

L'expression régulière peut ensuite être adaptée, ou plus précise. Elle peut, par exemple se préoccuper des champs "display:none", etc. Il faut cependant faire attention, car cette opération risque de modifier l'affichage de données utiles.

Les expressions régulières permettent une grande souplesse de filtrage.

L'objectif de cet article n'est pas de détailler les expressions régulières, mais d'insister sur le fait qu'elles existent, et sont souvent mises à disposition par les différentes passerelles. Elles peuvent ainsi permettre de filtrer des contenus potentiellement dangereux, avant qu'ils soient directement interprétés par le navigateur de l'utilisateur.

4 Les applications contenues sur une clé

Le CERTA a publié en 2006 la note d'information CERTA-2006-INF-006. Elle aborde les risques associés aux supports de données amovibles USB (Universal Serial Bus).

L'un des points-clés de cette publication est de montrer deux choses :

1° un périphérique USB peut faire courir un risque au système sur lequel il est branché ;

2° les données d'un périphérique USB peuvent courir un risque lorsque celui-ci est branché sur un système.

L'idée n'est pas ici d'écrire à nouveau cette note d'information, mais de montrer que les scénarios 1 et 2 existent bien, par deux exemples concrets d'actualité.

– Note d'information du CERTA sur les risques associés aux clés USB :
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/

4.1 Un incident traité cette semaine

Le CERTA a traité cette semaine un incident concernant une machine non connectée à l'Internet. Celle-ci a été compromise par un code malveillant qui a déposé deux *keyloggers*. Si ceux-ci ne pouvaient pas se connecter sur des sites distants pour envoyer des informations capturées, cet exemple montre néanmoins que les machines déconnectées de l'Internet ne sont pas pour autant protégées. Le vecteur de propagation de ce code malveillant semblait ainsi être un périphérique amovible et/ou un partage réseau. L'une de ses variantes se copie notamment sur des clés USB avec un fichier `autorun.inf` pour son exécution automatique sur un système Windows avec la fonctionnalité `autorun` activée. L'antivirus installé sur la machine n'a pas détecté les `keyloggers` présents, toutefois d'autres les détectent avec succès.

Le type d'informations qui sont capturées puis envoyées peut différer selon le code :

– captures liées à des connexions sur des sites prédéfinis (identifiants bancaires ou commerciaux par exemple);

– captures liées à l'utilisation d'Internet ;

– captures liées à toute frappe clavier dans une fenêtre (documents, etc.).

Les codes de ce type ne sont pas toujours faciles à détecter. L'analyse régulière des fichiers journaux de connexions sortantes est souvent le meilleur moyen car ce type de programme va tenter d'envoyer les données collectées. De plus, ils peuvent parfois provoquer des comportements suspects sur la machine : par exemple, le code analysé cette semaine provoquait des doublons lors de frappes de certaines touches particulières du clavier.

4.2 Rappel concernant les supports de données amovibles USB (Universal Serial Bus)

Sur différents sites, forum de discussions et listes de diffusion françaises, des personnes mentionnent parfois la possibilité d'installer et d'utiliser des applications préconstruites pour les périphériques de stockage de données USB (par exemple : une clé ou un disque dur amovible).

La page d'un projet offrant de telles applications affiche plus de 200 applications à son catalogue, directement utilisables, une fois copiées sur un périphérique (elles sont compilées de manière statique). Cela inclut :

– des outils de bureautique (calculatrice, bloc-notes, lecteur PDF, etc.) ;

– des outils de gravure CD ou DVD ;

– des outils de gestion de fichiers (sauvegarde, archivage, compression, etc.) ;

– des outils pour exploiter une connexion Internet (client de messagerie, navigateur, aspirateur de site, logiciel d'échange pair-à-pair, etc.)
– des outils multimédia (lecteurs d'images ou de vidéos, etc.) ;
– des outils d'administration (accès à la base de registres, gestionnaire de processus, générateur d'informations, sécurité, etc.).

Cependant l'utilisation de ces applications présente des risques : l'utilisation de logiciels comme des navigateurs Internet ou des clients de messagerie implique le stockage de données personnelles sur le support. Une personne malveillante peut, lors de la connexion du périphérique sur une machine compromise, « aspirer » les données, parfois confidentielles comme :

– la liste des contacts ;
– l'historique de navigation ;
– les mots de passe stockés ;
– les courriers électroniques ;
– les documents bureautiques créés et modifiés ;
– etc.

Ces périphériques, de taille toujours plus réduites, peuvent aussi être facilement perdus ou dérobés.

Enfin, les logiciels offerts impliquent également un grande confiance vis-à-vis du projet, car les codes source ne sont pas toujours disponibles, et les fichiers exécutables sont rarement analysés.

Dans de nombreux incidents, la compromission du système est due à l'absence de mises à jour ou patchs correctifs. L'utilisation de ces support de stockage USB contenant des applications prêtes à l'emploi rend plus compliquée et incertaine la mise à jour de ces applications. La mise à jour dépend du projet tiers. Ainsi, dans celui mentionné, il apparaît que de nombreuses applications ne sont pas fournies dans leur version la plus récente. Ces applications obsolètes incluent un navigateur, une suite bureautique et des lecteurs multimédia.

Le CERTA recommande donc de bien étudier toutes ces problématiques avant d'utiliser de telles solutions pour des périphériques de stockage USB.

5 Quelques anomalies DNS

Le CERTA a reçu plusieurs courriels signalant le cas d'un site qui tenterait de se faire passer pour celui d'un éditeur et qui pourrait ainsi proposer des logiciels malveillants en lieu et place de ceux légitimes. Après analyse, il s'agirait plutôt d'une utilisation abusive d'une fonctionnalité DNS. L'objectif de cet article est d'expliquer cet abus.

Le but du protocole DNS est d'établir un lien entre le nom d'une machine et son adresse réseau (IP). Par exemple l'adresse "www.certa.ssi.gouv.fr" correspond, à la date de rédaction de ce document, à l'adresse "213.56.176.2". Ces associations ne pouvant être maintenues dans une unique base de données partagée, le système a été organisé selon une architecture arborescente. Les noms représentent des feuilles ou des nœuds de l'arbre, et la structure des noms représente un chemin dans l'arbre.

Chaque nœud de l'arbre (domaine) a un nom et contient une liste de noms de machines (hôtes) ou des sous-nœuds (sous-domaines). Un ensemble de domaines et de sous-domaines gérés au même endroit est appelé une zone. Les sous-domaines peuvent faire partis de la même zone que leur ascendant ou être noeud d'une nouvelle zone.

A chaque zone correspond une base ou les noms sont associés à une adresse physique, mais pas uniquement. En effet d'autres précisions peuvent y être associées, par exemple des informations pour le routage des courriels ou les alias. Un alias (CNAME) peut pointer sur le nom d'un hôte, dans la même zone ou une autre.

Dans le cas des remontées faites au CERTA, le problème est donc le suivant : un utilisateur a enregistré son nom de domaine MonSiteMauvais en le définissant comme alias (ou CNAME) de www.MonEntreprise.

L'utilisateur qui clique sur un lien d'une page vers MonSiteMauvais a la surprise de visualiser une page légitime du site www.MonEntreprise.

Il ne s'agit pas d'un cas de filoutage, mais plutôt d'une tentative de nuire à l'image de la société, en faisant pointer plusieurs noms de machines (humoristiques ou agressifs) vers le site officiel www.MonEntreprise.

On peut cependant imaginer que cette configuration DNS change, et dirige cette fois le nom MonSiteMauvais vers une page malveillante à une adresse donnée (champ A remplaçant champ CNAME dans la configuration DNS).

La possibilité de se définir comme alias d'un autre nom hors de sa zone dépend des limitations imposées par les noms de domaines les plus hauts (Top Level Domain, « com », « fr », « org », . . .). Des commandes comme «

nslookup » ou « dig » permettent de voir qu'il ne s'agit que d'un alias. On voit que le nom canonique (le nom « réel ») est associé à celui malveillant.

```
        $dig MonSiteMauvais
(..)
;; ANSWER SECTION:
MonSiteMauvais       TTL1  IN  CNAME www.MonEntreprise
www.MonEntreprise    TTL2  IN  A     W.X.Y.Z
(...)
```

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 27 septembre et le 04 octobre 2007.

7 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/

8 Rappel des avis émis

Dans la période du 28 septembre et 04 octobre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-420 : Vulnérabilité de l'antivirus F-Secure
- CERTA-2007-AVI-421 : Multiples vulnérabilités de Websphere
- CERTA-2007-AVI-422 : Multiples vulnérabilités dans Sun Solaris
- CERTA-2007-AVI-423 : Vulnérabilités d'OpenSSL
- CERTA-2007-AVI-424 : Multiples vulnérabilités dans XOrg

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.

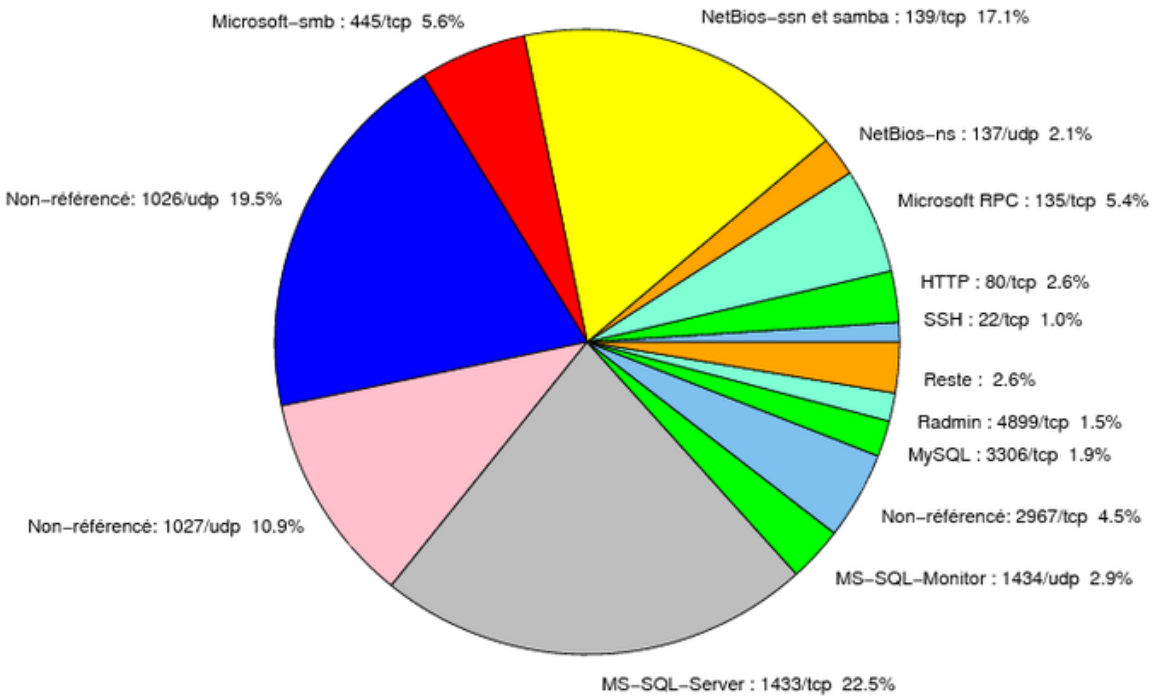

FIG. 1: Répartition relative des ports pour la semaine du 27.09.2007 au 04.10.2007

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

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

port	pourcentage
1433/tcp	22.46
1026/udp	19.47
139/tcp	17.09
1027/udp	10.93
445/tcp	5.56
135/tcp	5.44
2967/tcp	4.52
1434/udp	2.85
80/tcp	2.64
137/udp	2.05
3306/tcp	1.86
4899/tcp	1.46
22/tcp	1.01
3128/tcp	0.56
25/tcp	0.47
21/tcp	0.44
15118/tcp	0.21
2100/tcp	0.09
143/tcp	0.07
443/tcp	0.04
5554/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

05 octobre 2007 version initiale.