Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 janvier 2008
N° CERTA-2008-ACT-004

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-04

Conditions d'utilisation de ce document : http://www.certa.ssi.gouv.fr/certa/apropos.html
Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-004

Gestion du document

Référence	CERTA-2008-ACT-004
Titre	Bulletin d'actualité 2008-04
Date de la première version	25 janvier 2008
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-2008-ACT-004.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-2008-ACT-004/

1 Sur la confiance accordée aux outils utilisant des bases de signature

Cette semaine, le CERTA a traité un incident concernant la compromission d'un serveur web. Ce serveur d'hébergement mutualisé de sites internet dissimulait un site de filoutage (*phishing*).

Le CERTA a pris contact avec l'hébergeur. L'hébergeur a indiqué que le serveur subissait des compromissions successives depuis plus de six mois à la suite d'une première défiguration. Pourtant le serveur était régulièrement analysé par un outil de découverte de *rootkit*, qui n'a rien signalé de particulier.

Cet outil a donné un faux sentiment de sécurité à l'hébergeur qui ne comprenait pas comment les attaquants pouvaient revenir si fréquemment.

Il semble finalement, après une première analyse du CERTA, que le serveur n'était pas à jour en terme de correctifs de sécurité des applications et qu'il contenait un code malveillant de type *PHP Shell* permettant aux attaquants de revenir très simplement sur le serveur. L'outil de découverte de *rootkit* n'a jamais vu ce fichier.

Le CERTA rappelle que les outils utilisant des bases de signature ne peuvent reconnaître que les codes malveillants bien identifiés. Ces outils, bien qu'utiles, ne doivent pas constituer le premier moyen de surveillance d'une machine. Leur efficacité a des limites. Le problème ne concerne pas uniquement leur mise et jour et la qualité de leurs signatures. Ils modifient également des informations sur le système quand ils sont lancés (dates) et peuvent compliquer la tâche des spécialistes dans leur analyse.

Un audit régulier du code des applications utilisées, le suivi des correctifs, une politique rigoureuse des droits des utilisateurs et un cloisonnement des réseaux restent les premières et les meilleures pratiques de défense.

2 Les outils d'assistance réseau en ligne

Plusieurs sites Internet publics proposent à l'utilisateur des outils d'assistance réseau mis en ligne. Ces outils peuvent servir à :

- convertir sous différents formats des données de configuration réseau (décimal, hexadécimal, binaire par exemple) ;
- fournir des outils de calcul et d'aide-mémoire : plage d'adresses disponibles suivant un masque CIDR, adresse de diffusion, etc.
- effectuer des requêtes DNS ou des résolutions de noms inverses ;
- interroger des bases de nommage Whois ;
- lancer des tests de type `traceroute` pour évaluer le cheminement des paquets. Des outils récents, combinés à des cartes du monde (API Google) montrent le résultat de manière visuelle.
- récupérer les en-têtes de requêtes ou réponses HTTP, en particulier les informations concernant le `User-Agent`, la version HTTP annoncée, les méthodes pour encoder, etc.
- obtenir sa propre adresse IP publique.

Pour chacune de ces utilisations, plusieurs questions peuvent être légitimement posées. Certaines concernent directement les fonctionnalités et les mécanismes du service fourni :

- Dans le cas d'une résolution de nom, il est important de connaître certaines informations comme notamment les serveurs DNS interrogés pour interpréter correctement le résultat retourné.
- Les calculatrices en ligne sont pratiques, mais des données peuvent être récupérées côté serveur quand l'administrateur les utilise : elles peuvent concerner des plans d'adressage internes. Ces données ne doivent pas être publiques.
- L'outil `traceroute` mentionné précédemment a une présentation visuelle attrayante, mais le site mettant en ligne l'outil explique que le paquet doit nécessairement transiter par un de leur système avant d'atteindre sa destination. Est-ce la fonctionnalité attendue d'un `traceroute` ?
- Il y a rarement d'information fournie sur les bases interrogées pour les requêtes Whois. Quelles bases sont utilisées ? Est-ce une copie de base publique stockée localement ? Quelle version est alors utilisée ?

Les motivations qui poussent à mettre en ligne de tels services sont parfois peu claires.

Ces services en ligne restent attrayants car gratuits et simples d'usage, mais leur maintenance peut être motivée par des raisons moins sympathiques : collecte d'information, usage publicitaire, etc.

L'ensemble de ces services est en réalité accessible par tout utilisateur, au moyen de commandes tapées sur son système d'exploitation (`whois`, `nslookup`, `dig`, `traceroute`, etc.). Ces dernières gardent l'avantage de permettre à l'utilisateur de maîtriser les options de configuration, et les actions entreprises. Elles évitent de recourir à une interface tierce méconnue.

3 Vulnérabilité dans Mozilla Firefox

En début de semaine, une nouvelle vulnérabilité dans Mozilla Firefox a été publiée par un chercheur. Cette faille concerne les URIs de la forme `chrome:` qui n'annulent pas certains caractères dans le cas d'extensions non contenues dans un fichier de type `.jar`. Ceci permet à une personne malintentionnée d'effectuer une traversée de répertoire, et donc potentiellement d'obtenir des informations sur l'ordinateur de la victime. Le type de fichier accessible est toutefois très limité (scripts, images, feuilles de style), ce qui rend cette faille .

Désactiver JavaScript par défaut est la première mesure préventive. L'extension *NoScript* permet également de se protéger de cette vulnérabilité que le site visité soit reconnu comme fiable ou non. En effet, cette extension empêche, dans sa version la plus récente, par défaut, l'appel de modules (*packages*) `chrome` depuis un contenu Web.

L'éditeur `Mozilla` a reconnu la vulnérabilité le 22 janvier 2008 en publiant une entrée sur son bloc-notes (*blog*). Un correctif devrait donc être disponible dans l'une des prochaines versions du navigateur.

- Entrée dans le bloc-notes (*blog*) de Mozilla :
  http://blog.mozilla.com/2008/01/22/chrome-protocol-directory-traversal/
- Rapport de bogue Bugzilla numéro 413250, "chrome directory traversal (local access via flat addons)" :
  https://bugzilla.mozilla.org/show_bug.cgi?id=413250

4 Mise à niveau d'Internet Explorer

Microsoft a publié le bulletin KB946202 relatif à la sortie de la mise à niveau d'Internet Explorer le 12 février dans le catalogue des serveurs *Windows Server Update Services* (*WSUS*). Cette mise à disposition implique que le changement d'Internet Explorer 6 vers Internet Explorer 7 se fera de manière automatique si le serveur *WSUS* est configuré avec l'approbation automatique des ensembles de correctifs. Ce choix de configuration n'est cependant pas celui par défaut.

Certaines applications développées en interne peuvent ne pas fonctionner correctement sous Internet Explorer 7. Cette mise à niveau forcée pourrait donc causer dans certains cas des dysfonctionnements. Dans ces conditions, il est préférable que cette mise à niveau ne se fasse pas automatiquement, mais après avoir vérifié que l'intégration du nouveau navigateur ne pose pas de problème. Si c'est le cas, il est préférable de suivre la procédure suivante :

- désactiver l'approbation automatique ;
- synchroniser le serveur WSUS avec les serveurs de Microsoft ;
- le 12 février la mise Internet Explorer va apparaitre dans la liste des mises à jour non approuvées ;
- il sera alors possible de repasser le serveur WSUS en approbation automatique.

Pour rappel, les utilisateurs d'Internet Explorer 6 ont pu rencontrer des problèmes dans les mises à jour de Microsoft de décembre 2007. Ceci a été évoqué dans le bulletin d'actualité CERTA-2007-ACT-051 et par le bulletin Microsoft KB946627.

documentation

- Bulletin Microsoft KB946202 :
  http://support.microsoft.com/kb/946202
- Bulletin d'actualité CERTA-2007-ACT-051 du 21 décembre 2007, section 3, « Problème avec Internet Explorer suite à la mise à jour mensuelle Windows de Décembre 2007 » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-051.pdf

5 DNS et hôte local : un point, c'est tout

Il est très fréquent, sur l'Internet, que le serveur de noms de domaines BIND soit utilisé. L'avis CERTA-2008-AVI-037 portant sur une vulnérabilité liée à ce serveur a été publié le 24 janvier 2008. Cet article n'aborde pas cette vulnérabilité, mais il est important de noter que ce type de serveurs nécessite une attention toute particulière. En effet, une erreur souvent constatée est d'oublier le point terminal à la fin d'un enregistrement de type « A » disposant déjà d'un nom complètement qualifié (FQDN). En particulier, si cet oubli concerne la zone *localhost* et l'enregistrement « A localhost », un serveur autorité pour la zone MonDomaine.tld répondra 127.0.0.1 si on le solicite sur l'enregistrement :

localhost.MonDomaine.tld

127.0.0.1 est l'adresse IP utilisée pour communiquer (en IP) avec sa propre machine : *localhost*, ou hôte local.

La configuration du serveur DNS serait alors de la forme :

```
localhost        IN   A  127.0.0.1
```

En réalité, la configuration correcte aurait dû être :

```
localhost.        IN   A  127.0.0.1
```

Il est ainsi possible de contourner la politique de sécurité ou de conduire des attaques de type « injection de code indirecte » (*cross-site scripting*).

Par exemple, sur une machine multi-utilisateurs de type UNIX, il est possible pour un utilisateur de lancer un serveur web sur un port non-privilégié (>1024) et d'inviter un autre utilisateur à visiter un serveur du type http://localhost.MonDomaine.tld:9999. La requête contiendra alors les en-têtes du *cookie* de session décrit dans le standard RFC2109. Ce cookie est utilisé pour éviter l'usurpation de session. Or, dans ce cas précis, si un attaquant intercepte ces informations, il lui sera possible d'obtenir des informations d'identification de la victime.

Recommandation

Le point final (.) à la fin d'un enregistrement FQDN ou relatif au bouclage local (localhost est indispensable et évite ce genre de désagréments. Si vous êtes amenés à mettre en œuvre un serveur DNS BIND, il est important de bien vérifier que les enregistrements FQDN et *localhost* sont bien terminés par ces point finaux.

6 Les vers applicatifs à injection de code indirecte (*XSS Worms*)

L'actualité de la semaine de rédaction de ce bulletin a concerné la fin d'un concours, dont le sujet était l'écriture d'un ver `XSS` de taille minimale, et la mise à disposition d'un module générique d'écriture de vers `XSS`. Ces événements sont l'occasion de faire un point sur le sujet.

6.1 Définition

Un ver informatique est par définition un programme qui se propage par réplication entre machines. Une injection de code indirecte (XSS, ou *cross site scripting*) consiste à faire exécuter du code dynamique interprétable dans une page web. Ce code dynamique, potentiellement malveillant, s'exécutera à travers le navigateur des personnes consultant le site web, à leur insu. Ce code peut être introduit via des paramètres de l'adresse (URL) ou de façon permanente par le biais de champs de données réécrites dans une page. Un ver `XSS` est donc, par extension, un code, potentiellement malveillant, qui base sa réplication sur son auto-injection dans des pages vulnérables au *cross site scripting*. C'est un ver dont le mode de propagation s'appuie sur la couche applicative (et plus particulièrement le niveau 7 de la couche OSI).

6.2 L'origine

Le premier ver célèbre se comportant de la sorte a été nommé *Samy*. Il s'est propagé au sein du site de réseau social *MySpace* en octobre 2004, en se dupliquant sur les pages de profil des utilisateurs. L'auteur du ver, cherchant un moyen de contourner les protections de ce site, a commencé par trouver un biais dans les mécanismes de sécurité offrant la possibilité d'injecter toute sorte de contenu, et en particulier du code Javascript, dans quelques champs de données.

Lorsqu'une personne inscrite sur *MySpace* visualisait la page d'un profil infectée, le script était alors interprété par le navigateur du lecteur. Comme ce lecteur disposait d'un profil sur *Myspace*, le ver profitait des droits de sa victime pour s'injecter dans ce nouveau profil en exploitant les mêmes failles qu'initialement. La page *MySpace* de l'internaute ayant navigué devenait à son tour infectée, donc contagieuse, pouvant alors contaminer les pages de nouveaux visiteurs, et ainsi de suite... Ce ver aurait compromis *in fine* plus d'un million de pages (correspondant à un million de profils de personnes distinctes) en moins d'une journée, ce qui démontre la rapidité de propagation de ce type de ver.

Par la suite, d'autres vers exploitant ce type de vulnérabilité dans leur processus de propagation ont vu le jour. On peut citer parmi eux le ver *Yammaner*, exploitant une faille dans l'interprétation du JavaScript du webmail de Yahoo afin de s'injecter dans un courrier envoyé à tous les contacts de la victime. On peut aussi citer le ver *Quickspace* se propageant sur le site *MySpace* à travers l'exploitation d'une exécution de code indirecte dans une vidéo au format *Quicktime*.

6.3 Conclusion

Même si *Samy* n'a été développé que pour accroître la popularité de son auteur (popularité selon la définition du site *MySpace*), on peut craindre une utilisation plus agressive ou dévastatrice de ce type de vers. Ces codes malveillants deviennent de plus en plus des outils aux fonctionnalités très élargies et à la discrétion accrue. Le module générique fourni à la suite du concours est public et propose, par exemple, des fonctionnalités d'injection SQL, de polymorphisme, d'interface de contrôle etc.

Comment limiter la propagation de tels codes ?

- pour les développeurs et les administrateurs :
  une bonne hygiène d'administration des serveurs est un des seuls moyens efficaces pour éviter la propagation de tels codes. En amont, il est nécessaire de contrôler toutes les entrées sur les pages de son site, afin de s'assurer que l'on n'autorise que ce qui est légitime et nécessaire. Par exemple, dans un formulaire visant à renseigner un nom et un prénom, il n'est pas utile d'autoriser des chiffres et des caractères spéciaux. Enfin, en phase de production, il est indispensable de vérifier régulièrement l'intégrité du site (le système de fichiers et les bases de données). Enfin, il est préférable de développer des sites Web qui n'obligent pas les visiteurs à activer le JavaScript ou toute autre forme de contenu actif.
- pour les utilisateurs :
  l'utilisateur visitant les pages infectées devient malgré lui le vecteur de propagation du code. La pratique qui consiste à désactiver par défaut l'interprétation du JavaScript par son navigateur, et à ne l'activer que temporairement pour une fonction qui le rend nécessaire sur un site de confiance, reste valable. Malheureusement,

les utilisateurs exploités sont les clients des services de sites ciblés par les vers, et n'ont pas respecté cette règle pour pouvoir y accéder.

7 Des codes malveillants sur Symbian

Un code malveillant affectant les systèmes d'exploitation Symbian a été détecté par des éditeurs d'antivirus. Ce code malveillant requiert une action de la part de l'utilisateur afin qu'il compromette lui-même son système. Selon les rapports d'analyse, ce code aurait gagné en efficacité sans pour autant chercher à se dissimuler. De plus il n'exploite aucune vulnérabilité sur le système d'exploitation, il se propage simplement par voie de messagerie.

Dans la version analysée à la date de rédaction de ce bulletin, les versions antérieures au système d'exploitation Symbian 9.1/S60 3rd Edition seraient impactées. Elles peuvent concerner des appareils mobiles comme les Nokia 6600, 6630, 7610, N70 ou N72. Les victimes sont amenées à installer un fichier d'installation (`SIS`, ou *Symbian OS Installer*). Ils apparaissent à l'écran, pour le code en question, sous le nom `Beauty.jpg`, `Love.rm` ou `Sex.mp3`.

Le code se propage ensuite en prenant la liste de contacts, et en émettant un message multimédia (`MMS`) à chacun, avec bien entendu une réplique du code en document joint.

Le CERTA signale que certains équipements de type mobile et communiquant ne prennent pas en compte la notion d'utilisateur privilégié ou limité. Ainsi, l'utilisateur possède constamment les droits administrateur sur son système mobile. C'est pourquoi il est recommandé d'être très vigilant lors de la réception de contenu actif (application, installation, etc.).

Certains équipementiers mettent en place un système de signature de contenu pour tenter de limiter l'impact de contenu non sûr. En réalité, seule la partie dite « métadonnée » du fichier d'installation .SIS est réellement signée. Celle-ci contient un *hash* des données du fichier. Ces données sont donc vérifiées avant de lancer l'opération d'installation. Elles sont indépendantes des tests d'intégrité, par ailleurs optionnels. Cependant, pour l'utilisateur, il n'y a pas de garantie que ces informations soient correctement vérifiées par le système mobile quand il va lancer l'installation. De manière pratique, il apparaît que la signature de nombreuses applications téléchargeables, y compris certaines fournies par des opérateurs, ne soient pas aisément vérifiables. L'utilisateur du mobile tend donc dans la majorité des cas à transgresser ce contrôle en annulant la vérification de la signature dans les options de son téléphone. Cette mesure de signature est donc insuffisante car difficilement vérifiable.

- Note de communication par F-Secure publiée le 22 janvier 2008 :
  http://www.f-secure.com/weblog/
- Note de communication par Trend Micro publiée le 24 janvier 2008 :
  http://blog.trendmicro.com/symbian-malware-gives-loves-and-beauty-and-sex-a-bad-name/
- Note de communication par Fortinet du 21 janvier 2008 :
  http://www.fortiguardcenter.com/advisory/FGA-2008-03.html
- "Symbian OS v9.X - SIS File Format Specification" :
  http://developer.symbian.com/main/downloads/papers/SymbianOSv91/softwareinstallsis.pdf

8 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 17 et le 24 janvier 2008.

9 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/

10 Rappel des avis émis

Dans la période du 18 au 25 janvier 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-027 : Vulnérabilité de produits Citrix
– CERTA-2008-AVI-028 : Vulnérabilité dans Cisco Unified Communication Manager
– CERTA-2008-AVI-029 : Mutiples vulnérabilités des produits Oracle
– CERTA-2008-AVI-030 : Multiples vulnérabilités dans XOrg
– CERTA-2008-AVI-031 : Vulnérabilités dans WordPress
– CERTA-2008-AVI-032 : Vulnérabilité de Horde3
– CERTA-2008-AVI-033 : Vulnérabilité dans cPanel
– CERTA-2008-AVI-034 : Vulnérabilité dans Dreamweaver et Contribute
– CERTA-2008-AVI-035 : Multiples vulnérabilités des produits IBM
– CERTA-2008-AVI-036 : Vulnérabilité dans HP-UX ARPA
– CERTA-2008-AVI-037 : Vulnérabilités dans des produits Cisco

11 Actions suggérées

11.1 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.

11.2 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.

11.3 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.

11.4 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.

11.5 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.

11.6 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.

11.7 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

12 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.

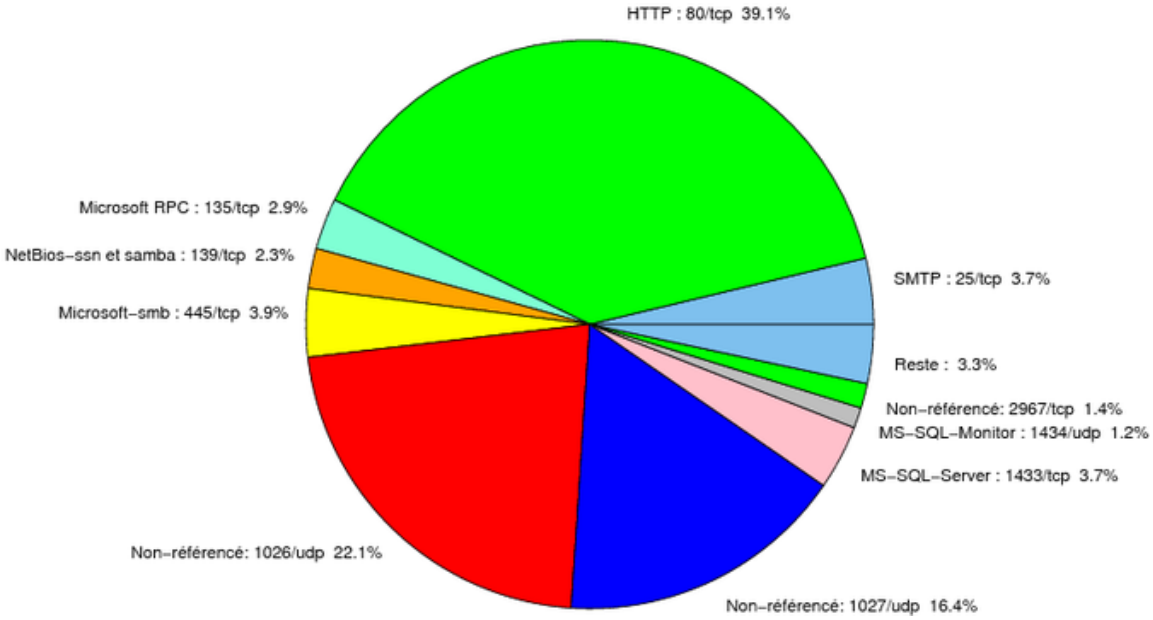

FIG. 1: Répartition relative des ports pour la semaine du 17.01.2008 au 24.01.2008

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

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER

6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
80/tcp	39.05
1026/udp	22.09
1027/udp	16.44
445/tcp	3.87
25/tcp	3.74
1433/tcp	3.67
135/tcp	2.9
139/tcp	2.28
2967/tcp	1.41
1434/udp	1.16
22/tcp	0.72
1080/tcp	0.61
4899/tcp	0.41
137/udp	0.38
3128/tcp	0.37
3306/tcp	0.15
21/tcp	0.12
3127/tcp	0.1
143/tcp	0.02
2100/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 10
3 Paquets rejetés 11

Gestion détaillée du document

25 janvier 2008 version initiale.