Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 décembre 2007
N° CERTA-2007-ACT-051

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-51

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-2007-ACT-051`

Gestion du document

Référence	CERTA-2007-ACT-051
Titre	Bulletin d'actualité 2007-51
Date de la première version	21 décembre 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-051.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-051/

1 Mise à jour de SquirrelMail

Nous avions évoqué, dans le précédent bulletin d'actualité, la compromission des versions en téléchargement de *SquirrelMail*. L'éditeur de ce *webmail* a rectifié son annonce en précisant que cette compromission a introduit une importante faille de sécurité (permettant l'inclusion de fichiers à distance) dans les sources du logiciel.

Afin d'éviter toute confusion, une nouvelle version, 1.4.13, a été publiée. Tous les utilisateurs des versions 1.4.11 et 1.4.12 sont invités à appliquer cette mise à jour. Le CERTA n'a cependant pas publié d'avis de sécurité, car ces versions ne corrigent pas de problèmes de sécurité concernant l'application.

Documentation :

– Site officiel du projet SquirrelMail :
http://www.squirrelmail.org/

2 Risques liés à l'utilisation d'outils de communication instantanée

Les outils de communication instantanée (on parle souvent de messagerie instantanée même si le terme « messagerie » n'est pas tout-à-fait approprié) tels que `MSN`, `ICQ`, `IRC` et autres, font l'objet des mêmes problèmes de sécurité que la messagerie (voir CERTA-2003-AVI-084) : propagation de vers et de canulars, *phishing* (hameçonnage), etc. La particularité de ces outils est leur aspect « instantané », c'est-à-dire que les utilisateurs ont tendance à réagir très rapidement aux messages reçus. Cette spontanéité fait de ces outils un très bon terreau pour la propagation de divers codes malveillants.

Nous avons par exemple pu voir récemment des vers se propageant sur `MSN`. La mécanique de propagation était simple, elle reposait sur le carnet d'adresses (les contacts) de la victime. Cet incident a montré que les bons réflexes pour la messagerie n'étaient pas toujours appliqués sur `MSN`.

Encore plus récemment, un message proposant des services pour `MSN` (en l'occurrence, vous informer des contacts qui vous ont bloqués ou supprimer de leur carnet d'adresses) a été largement diffusé par différents canaux (par `MSN` bien sûr, mais aussi par divers réseaux sociaux, *blogs*, etc.). Bon nombre de victimes étaient persuadées du bien-fondé de ce service... après avoir transmis à un site tiers leurs identifiants de connexion à `MSN` ! Dans ce cas précis, qui s'apparente à du *phishing*, de nombreuses d'adresses `MSN` ont pu être collectées, ainsi que les mots de passe associés à ces comptes. Les victimes doivent donc changer leur mot de passe ainsi que la question secrète, tout en gardant à l'esprit qu'un certain nombre de données personnelles éventuellement contenues dans les boîtes de messagerie associées ont déjà pu être capturées.

Avec l'approche des fêtes de fin d'année, on peut s'attendre à ce que de nouveaux codes malveillants se propagent par l'intermédiaire de ces outils de communication, par exemple sous la forme de cartes de vœux.

Recommandations :

La vigilance et la méfiance requises pour la messagerie doivent également être de mise pour les outils de communication instantanée. Les problèmes sont ou seront les mêmes, ce sont les habitudes et les populations d'utilisateurs qui pour le moment diffèrent le plus. Certains outils de communication proposent, par leur paramétrage, des mesures de sécurité qui peuvent être mises en place. Il est important de bien examiner la configuration de ces outils.

Documentation :

– Avis CERTA-2003-AVI-084 :
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-084/

3 Problème avec Internet Explorer suite à la mise à jour mensuelle Windows de décembre 2007

Cette semaine avant Noël, plusieurs personnes ont signalé des problèmes liés à l'installation de la mise à jour de sécurité KB942615 pour Internet Explorer relative au bulletin de sécurité MS07-069 du 11 décembre 2007. Cette mise à jour permet de protéger le système contre une vulnérabilité permettant l'exécution de code arbitraire à distance ou en local et un contournement de la politique de sécurité. Cette vulnérabilité a été détaillée dans l'avis CERTA-2007-AVI-540 du 12 décembre 2007.

– Il a tout d'abord été rapporté des difficultés lors du chargement de la page du site Microsoft contenant ce bulletin de sécurité. Ces problèmes sont dûs à la taille du fichier contenant les informations associées aux bulletins de sécurité d'Internet Explorer. Les informations ont été déplacées dans l'article de la base de connaissances Microsoft relatif à ce bulletin afin d'alléger la taille de page et accélérer son chargement.
– Des problèmes liés à l'installation touchant plus particulièrement les machines ayant `Windows XP SP2` et `Internet Explorer 6` ont également été signalés. En effet, après installation du correctif, Internet Explorer se révèle instable et peut afficher un message d'erreur informant d'une éventuelle perte de données en cours de traitement par le navigateur et invite à l'envoi d'un rapport d'erreurs. Ce rapport est relatif au dysfonctionnement de la bibliothèque *urlmon.dll*. Microsoft a publié une nouvelle mise à jour de sécurité KB946627 afin de corriger les problèmes liés à la première.
Cette nouvelle mise à jour est disponible via les mises à jour automatiques ou directement en se rendant sur le site de *Windows Update*.

3.0.1 Documentations

- Avis de sécurité CERTA-2007-AVI-540 du 12 décembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-540/
- Bulletin de sécurité Microsoft MS07-069 du 11 décembre 2007 :
  http://www.microsoft.com/technet/security/Bulletin/MS07-069.mspx
- Mise à jour de sécurité Microsoft KB942615 du 11 décembre 2007 :
  http://support.microsoft.com/kb/942615
- Mise à jour de sécurité Microsoft KB946627 du 20 décembre 2007 :
  http://support.microsoft.com/kb/946627

4 Problème de mise à jour du logiciel de messagerie Thunderbird

Le logiciel de messagerie libre Thunderbird existe à travers deux branches de développement : la branche 2.0.0.x, recommandée, et la branche plus ancienne 1.5.0.x . Une erreur dans le traitement des URI `mailto:` a été corrigée le 17 juillet 2007 par la fondation Mozilla, mais le mode de déploiement du correctif dans la branche 1.5.0 était insatisfaisant :

- l'installation complète de la version 1.5.0.13 offrait la protection ;
- la mise à jour automatique depuis une version 1.5.0.x (x<13) n'offrait pas cette protection.

Il est donc recommandé :

- de préférer la branche de développement 2 ;
- pour ceux qui ne peuvent réaliser cette migration, installer la version 1.5.0.14.

Il faut enfin noter que la branche 1.5 de Mozilla Firefox n'est, elle, plus maintenue depuis la fin du mois d'avril 2007, comme il a été rappelé dans le bulletin CERTA-2007-ACT-016.

Documentation :

- Bulletin Mozilla MFSA 2007-40 du 19 décembre 2007 :
  http://www.mozilla.org/security/announce/2007/mfsa2007-40.html
- Bulletin d'actualité CERTA-2007-ACT-016 du 20 avril 2007, « Fin de vie de la branche 1.5 de Firefox » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-016.pdf

5 Ordinateurs préinstallés

Il est fréquent lorsque l'on fait l'acquisition d'un ordinateur dans le commerce ou bien lors d'un renouvellement de parc informatique de recevoir une machine disposant déjà d'un système d'exploitation évitant ainsi la fastidieuse étape de l'installation puis de la configuration du système et des logiciels appropriés. Or, cette étape est pourtant cruciale si l'on veut avoir un niveau de sécurité suffisant sur sa machine. En effet, ces ordinateurs pré-installés sont souvent configurés pour satisfaire les besoins du plus grand nombre. On trouve donc sur ce type de machines des applications parfois totalement inutiles, voire pas à jour et donc vulnérables. Il y a également des logiciels en version d'évaluation et très souvent des adaptations faites avec le système d'exploitation. Par exemple, dans l'avis CERTA-2007-AVI-556 rédigé le 19 décembre 2007, il est détaillé une vulnérabilité liée à une application spécifique à certains modèles de portables : elle concerne d'un contrôle ActiveX installé par défaut.

Il est donc indispensable lors de l'achat tant d'ordinateurs de bureau que de portables de bien vérifier :

- la pertinence des applications déjà installées ;
- le niveau de mise à jour du système d'exploitation et des logiciels ;
- la présence de logiciels comportant des vulnérabilités non-corrigées.

En cas de problème, une première solution consistera à désinstaller les applications inutiles et mettre à jour celles qui seront conservées. Une deuxième solution plus « propre » sera plutôt de réinstaller totalement la machine en sélectionnant les composants et les logiciels à installer, afin d'avoir un système bien mieux maîtrisé.

6 Les canaux cachés DNS

DNS est un protocole largement utilisé pour déterminer la correspondance entre le nom d'une machine et son adresse IP associée.

Un tunnel DNS se caractérise par des échanges illustrés dans la figure 1 ; à première vue, ce sont des échanges sous forme de requêtes et de réponses. La requête correspond à la demande du poste, comme par exemple pour accéder à la page d'accueil du CERTA www.certa.ssi.gouv.fr.

Dans le cas présent, le poste se trouve derrière un pare-feu, et ne peut normalement pas communiquer vers l'extérieur. Le pare-feu n'est cependant pas très regardant pour des protocoles standards comme DNS, NTP ou ICMP et laisse sortir ces flux de manière très laxiste. Ce cas de figure peut se rencontrer dans la mise en œuvre d'un portail captif Wi-Fi. Un autre cas de figure consiste à simplement bloquer les ports HTTP/HTTPS courants (80,443,8080, ...) et à ne pas donner l'accès du relais mandataire web aux utilisateurs qui ne doivent pas naviguer.

La machine interne peut donc néanmoins émettre des requêtes DNS, qui sont soit directement envoyées vers un serveur DNS externe, soit transférées par un serveur DNS interne.

La requête est généralement codée en Base32 (encodage équivalent à Base64, mais chaque caractère est codé sur 5 bits au lieu de 6, et il n'y a plus de distinction entre majuscule et minuscule). Elle concerne un sous-domaine bien particulier, géré par une personne qui en garde le contrôle (sous forme de « délégation » DNS du domaine par exemple).

Le serveur est interrogé pour répondre à cette requête. Il va donc interpréter les données encodées, et les traiter. Il peut s'agir en réalité de données SSH, ou d'URL.

Ce serveur a la possibilité de requérir les services d'un relais mandataire pour répondre, ou effectuer lui-même cette tâche. Sa réponse est ensuite envoyée sous forme d'un enregistrement de type `TXT`. Cet enregistrement est transmis de bout en bout, et doit en principe parvenir à la machine dans le réseau interne.

L'administrateur de ce même réseau n'a que les trames DNS pour découvrir le contournement de la politique de sécurité mise en place au niveau du pare-feu. Le schéma est volontairement simplifié sur la figure 1 :

- les données échangées via les requêtes et les réponses DNS ne sont pas toujours lisibles et peuvent être encapsulées par exemple dans un tunnel SSH. Le serveur DNS malveillant peut alors jouer le rôle de relais SSH.
- tous les moyens pour mettre en œuvre cette architecture, y compris le tunnel SSH mentionné précédemment, sont très accessibles et largement documentés sur l'Internet. D'autres enregistrements comme `KEY` avec DNSSEC sont également utilisés...

Cet usage est très souvent un contournement de la politique de sécurité et reste mal connu des administrateurs. Pour toutes ces raisons, le CERTA émet quelques recommandations :

- cet échange se fait suivant certaines contraintes. Les requêtes DNS ont une taille limite de 253 caractères, dont 63 par « sous-domaine » (entre les "."), mais ces longueurs extrêmes sont très rarement utilisées. De même, les réponses du serveur doivent tenir compte des contraintes de longueur et de fragmentation possible. Ces spécificités peuvent être visibles si l'on procède à une analyse régulière des journaux :
  - surveillance du nombre de requêtes ;
  - surveillance de la variation de l'intervalle de temps entre chaque requête par rapport à une valeur moyenne (écar t-type) ;
  - surveillance du volume des données échangées....
- une analyse du trafic au niveau du réseau peut apporter une vue supplémentaire : surveillance régulière du trafic, à partir de méthodes statistiques simples pour déterminer par exemple les échanges et les volumes de données émis et reçus (asymétrie ?), la taille moyenne des paquets DNS, les domaines interrogés, etc.
- dans le cas d'un DNS interne, seul le relais mandataire applicatif doit être en mesure d'interroger des DNS externes ;
- certains serveurs DNS interprètent les enregistrements et les traduisent à la volée. Cette méthode permet également de filtrer des enregistrements jugés suspects (comme `TXT`).

Documentation

- RFC 1035, "Domain Names - Implementation and Specification", novembre 1987 : http://tools.ietf.org/html/rfc1035
- RFC 1101, "DNS Encoding of Network Names and Other Types", avril 1989 : http://tools.ietf.org/html/rfc1101
- RFC 2181, "Clarifications to the DNS Specification", juillet 1997 : http://tools.ietf.org/html/rfc2181

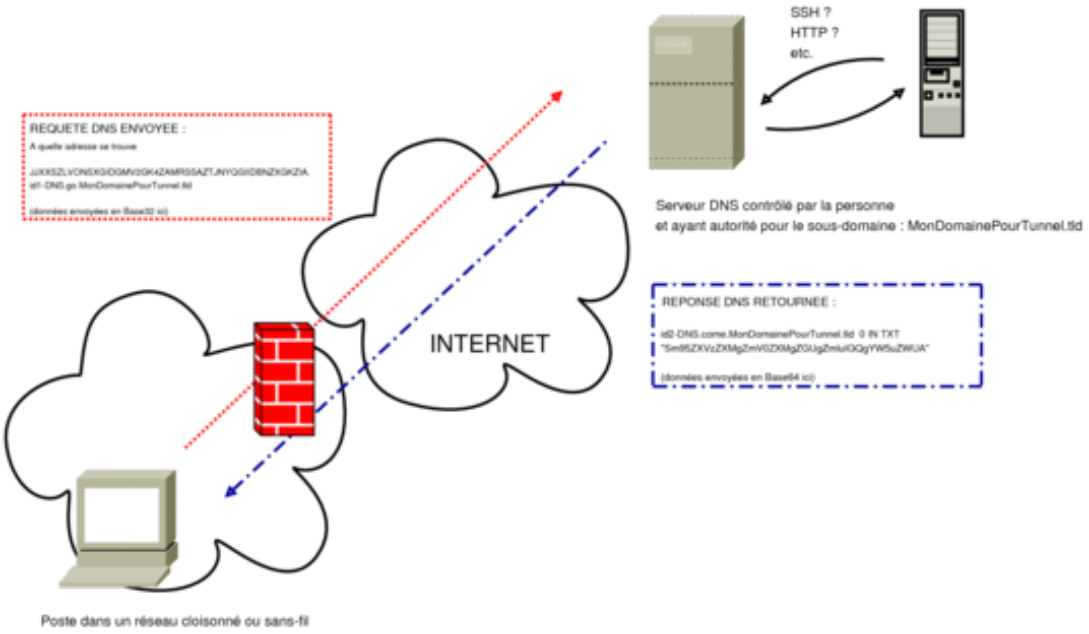

FIG. 1: Schéma d'un tunnel DNS possible

- RFC 4343, "Domain Name System (DNS) Case Insensitivity Clarification", janvier 2006 : http://tools.ietf.org/html/rfc4343
- Note d'information CERTA-2001-INF-003, « Tunnels et pare-feux : une cohabitation difficile » : http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003/

7 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 13 et le 20 décembre 2007.

8 Liens utiles

- Mémento sur les virus : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information du CERTA sur l'acquisition de correctifs : http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
- Note d'information du CERTA sur les systèmes obsolètes : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
- Note d'information du CERTA sur les mots de passe : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
- Note d'information sur la terminologie d'usage au CERTA : http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 : http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) : http://www.auscert.org.au/render.html?it=1935
- Note d'information du CERTA sur les risques associés aux clés USB : http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/

– Note d'information du CERTA sur les outils d'indexation et de recherche :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
– Note d'information du CERTA sur la gestion des noms de domaine :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
– Note d'information du CERTA sur le bon usage de PHP :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

9 Rappel des avis émis

Dans la période du 14 au 20 décembre 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-543 : vulnérabilité dans TYPO3
– CERTA-2007-AVI-544 : Multiples vulnérabilités d'Apple QuickTime
– CERTA-2007-AVI-545 : Vulnérabilité de Sun Solaris
– CERTA-2007-AVI-546 : Multiples vulnérabilités dans Apple Mac OS X
– CERTA-2007-AVI-547 : Vulnérabilité dans les produits Juniper
– CERTA-2007-AVI-548 : Vulnérabilité de JBoss
– CERTA-2007-AVI-549 : Vulnérabilité dans BEA WebLogic Mobility Server
– CERTA-2007-AVI-550 : Vulnérabilité dans CUPS
– CERTA-2007-AVI-551 : Multiples vulnérabilités dans Apple Mac OS X
– CERTA-2007-AVI-552 : Vulnérabilité dans ClamAV
– CERTA-2007-AVI-553 : Multiples vulnérabilités d'Adobe Flash Player
– CERTA-2007-AVI-554 : Vulnérabilité dans Citrix Web Interface
– CERTA-2007-AVI-555 : Multiples vulnérabilités dans Opera
– CERTA-2007-AVI-556 : Multiples vulnérabilités dans HP Quick Launch Button (QLB)
– CERTA-2007-AVI-557 : Vulnérabilité d'un module CISCO
– CERTA-2007-AVI-558 : Vulnérabilité dans les produits Computer Associates
– CERTA-2007-AVI-559 : Multiples vulnérabilités dans Wireshark

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.

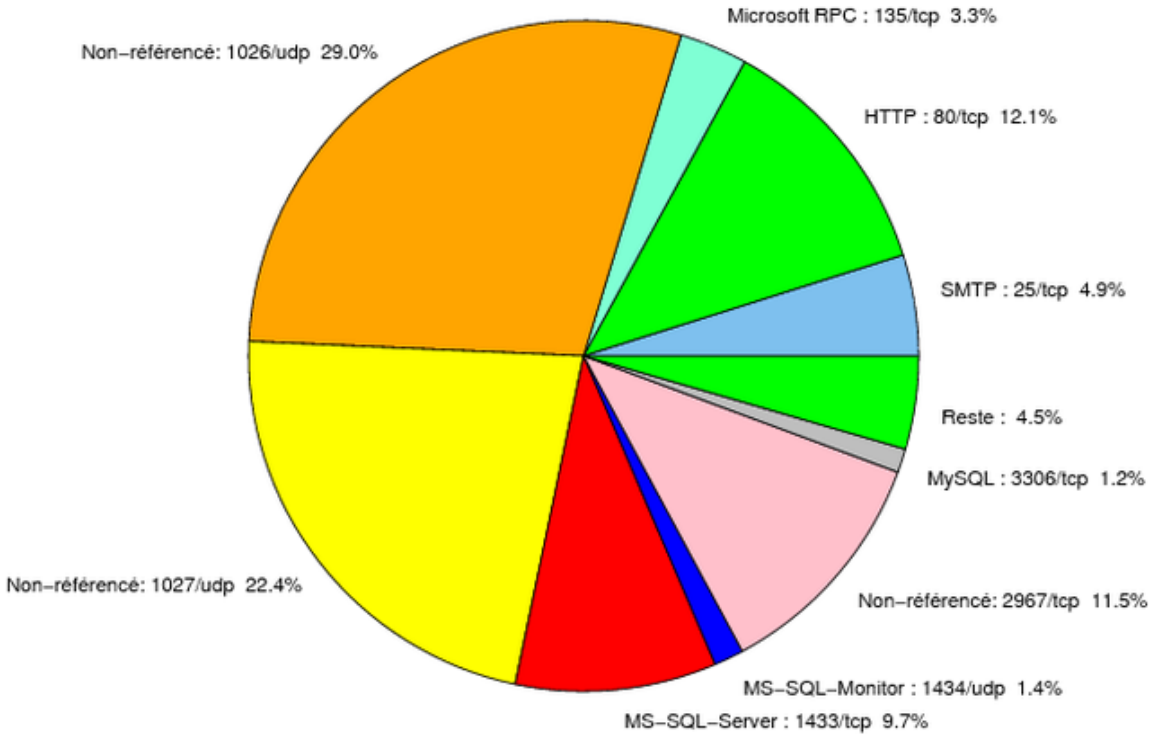

FIG. 2: Répartition relative des ports pour la semaine du 13.12.2007 au 20.12.2007

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/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 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
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	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 http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	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 http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	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 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 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
1026/udp	29.01
1027/udp	22.41
80/tcp	12.14
2967/tcp	11.5
1433/tcp	9.7
25/tcp	4.86
135/tcp	3.27
1434/udp	1.42
3306/tcp	1.15
4899/tcp	0.9
139/tcp	0.86
137/udp	0.3
15118/tcp	0.13
21/tcp	0.1
23/tcp	0.08
143/tcp	0.05
3389/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

21 décembre 2007 version initiale.