Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 novembre 2007
N° CERTA-2007-ACT-044

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-44

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-044

Gestion du document

Référence	CERTA-2007-ACT-044
Titre	Bulletin d'actualité 2007-44
Date de la première version	02 novembre 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-044.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-044/

1 Rappel : vulnérabilités sur OpenSSL

Le CERTA rappelle que l'application `OpenSSL` a été récemment touchée par trois vulnérabilités importantes :

- la première faille concerne la fonction *BN_from_montgomery* qui n'implante pas correctement l'algorithme de multiplication de Montgomery dans les versions 0.9.8e et antérieures. Ceci permet à une personne malveillante de reconstruire la clé secrète utilisée ;
- la deuxième vulnérabilité est un débordement de mémoire dans la fonction *SSL_get_shared_ciphers* dans les versions d'`OpenSSL` antérieures à 0.9.8f. Un attaquant pourrait exploiter cette vulnérabilité en envoyant un paquet spécialement conçu et ainsi exécuter du code arbitraire à distance ;
- la dernière faille concerne l'implémentation de `DTLS` dans les versions d'`OpenSSL` antérieures à 0.9.8f et permettrait également l'exécution de code arbitraire à distance via des vecteurs inconnus.

Ces vulnérabilités ont été détaillées dans l'avis CERTA-2007-AVI-423. Le déploiement massif de cette application et le risque critique de ces trois vulnérabilités en font des cibles de choix pour des attaquants (potentiels). Le CERTA recommande donc la mise à jour sans tarder de l'application `OpenSSL`, la dernière version étant 0.9.8g (publiée le 19 octobre 2007).

Documentation

– Avis de sécurité CERTA-2007-AVI-423 du 04 octobre 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-423/index.html

2 La magie des nombres

2.1 Le cas Storm Worm

Le thème du réseau de machines zombie compromises par le code Storm Worm, aussi appelé Nuwar ou Zhelatin, est très débattu dans les média. Le CERTA a abordé les propriétés de celui-ci dans quelques bulletins d'actualité, dont CERTA-2007-ACT-007, CERTA-2007-ACT-028 et CERTA-2007-ACT-034.

Sa première caractéristique est l'utilisation des techniques pair-à-pair, et l'autre sa capacité au fil des mois à s'adapter et à évoluer. A valeur d'illustration, les versions les plus actuelles à la date de rédaction de ce bulletin profitent de la fête d'*Halloween* pour se propager par des pages Web et des courriers électroniques sur ce thème d'actualité.

L'objet de cet article n'est pas de revenir sur ces derniers traits de caractère, mais de regarder objectivement les informations disponibles sur l'Internet.

Depuis le mois de juillet 2007, les chiffres vont bon train dans les média. De quelques millions de machines compromises, certains articles parlent même de plus de 50 millions, et comparent même cette puissance de calcul potentielle à celle cumulée des 500 plus importants supercalculateurs existant à la date de rédaction de leur article. Cette information a été amplifiée dans de nombreux articles.

Or, en septembre 2007, Microsoft annonce sur un bloc-notes un nombre très différent : un peu plus de 200000 au mois d'août 2007. Il s'agit du nombre de remontées par l'outil facultatif MSRT (*Malicious Software Removal Tool*) de machines compromises.

Au mois d'octobre, un chercheur d'une université américaine a présenté les résultats de certains tests. Il a réalisé un *crawler*, ou générateur de trafic artificiel, afin de compter les machines compromises en fonction des réponses reçues. Il estime ainsi que quelques centaines de milliers de machines seraient victimes du code Storm Worm et actives.

Dans l'analyse publiée, il y a bien sûr quelques limitations (mentionnées). Celle-ci ne prend en compte que les nœuds actifs. Le nombre est donc sûrement sous-estimé. Par ailleurs, le code Storm Worm a subi au début du mois d'octobre quelques modifications, notamment dans sa méthode de chiffrement. Ces nouvelles variantes ne seraient également pas comptabilisées.

Il ne s'agit pas ici de critiquer la méthode présentée, mais bien de comprendre que les chiffres mentionnés dans le document ont une origine correctement détaillée. Ils peuvent être vrais, ils peuvent être faux, mais ils sont justifiés d'une certaine manière. Ceci est également valable avec le chiffre de Microsoft.

D'un autre côté, les millions de machines compromises citées en juillet n'ont pas une telle justification. Elles sont issues de déclarations reprises sans plus plus de vérification dans de multiples articles sur la toile.

2.2 Rationalité face aux *magic numbers*

Les chiffres sont souvent très manipulés et manipulables sur l'Internet. Il est cependant important de faire la part des choses. Il est, de manière générale, toujours préférable de favoriser les chiffres justifiés par une méthode documentée. Il est également important de ne pas interpréter ces derniers aussi rapidement que certains articles tendent à le faire.

La plus grande prudence doit être appliquée à l'annonce de telles informations, et seul l'esprit critique du lecteur peut l'aider à faire la part des choses.

Documentation associée

– Bloc-notes de Microsoft : « Storm Drain »:
http://blogs.technet.com/antimalware/archive/2007/09/20/storm-drain.aspx
– Présentation de B. Enright à la conférence Toorcon 2007 :
http://noh.ucsd.edu/ bmenrigh/exposing_storm.ppt

3 Les modifications de configuration DNS

Un cheval de Troie fait, à la date de rédaction de ce document, parler de lui car il vise les systèmes Mac OS. Comme tout cheval de Troie, il faut à un moment donné que l'utilisateur installe le code malveillant : ce dernier se présentant comme un *codec* au format `.DMG`, qui est proposé au téléchargement à l'ouverture d'une vidéo par QuickTime Player.

Ses actions sur le poste infecté consistent en particulier à modifier la configuration DNS, afin de diriger l'utilisateur vers des sites particuliers (sites de filoutage, sites malveillants ou sites publicitaires...).

L'interface de configuration visuelle (menu *Réseau* dans *Préférences Systèmes*) ne montre pas nécessairement cette modification DNS simplement (sous Mac OS 10.4 par exemple).

La simple visualisation par cette interface n'est donc pas suffisante.

Il est donc recommandé de :

- filtrer les connexions sortantes du réseau et de n'autoriser que les flux légitimes (ports 53 TCP et UDP associés au DNS notamment) ;
- surveiller le trafic DNS, afin de déterminer des machines potentiellement compromises ;
- vérifier sur le poste la bonne configuration, si possible au niveau des fichiers de configuration, comme `resolv.conf` et `hosts` ;
- signaler tout comportement anormal du navigateur (ouverture de pages de publicité, etc.) ;
- ne pas installer de code venant de sources n'étant pas de confiance. Il est aussi vivement recommandé de naviguer sur un compte aux droits limités.

Documentation

- Alerte d'Intego, "OSX.RSPlug.A Trojan Horse Changes Local DNS Settings to Redirect to Malicious DNS Servers :
  http://www.intego.com/news/ism0705.asp

4 *Phishing* : du neuf avec du vieux

Les différentes techniques de *phishing* (ou filoutage) sont connues et ont été détaillées dans plusieurs bulletins d'actualité ces derniers mois : un courriel est envoyé à un échantillon de personnes, prétendant provenir d'un organisme de confiance et qui, par une tournure plus ou moins élégante, incite le client à se rendre sur une page Web ressemblant à une légitime (page bancaire, page d'une boutique ou d'un service en ligne, etc.) et à rentrer ses informations personnelles. La personne malintentionnée à l'origine de cette escroquerie récupère ainsi des identifiants et des mots de passe valides, dont il peut faire usage par la suite.

Une autre approche peut être utilisée pour récupérer les identifiants des utilisateurs. Au lieu d'inciter le lecteur du courriel à cliquer sur un lien spécifiquement construit, le courrier électronique indique de prendre contact avec son service client (ou son support) en téléphonant à un numéro joint dans le corps du message. Ce numéro de téléphone est bien sûr faux, redirigeant la victime vers un serveur vocal ou un responsable client fictif. Les identifiants sont alors demandés via ce nouveau canal de communication, et la fuite d'information échappe donc au contrôle informatique pur (outils anti-filoutage). Ces techniques d'escroqueries téléphoniques ne sont pas nouvelles, loin de là, mais permettent de contourner plusieurs outils supposés réduire les risques de filoutage.

Si un courriel de ce type arrive dans la boîte aux lettres, le CERTA recommande de:

- vérifier le numéro de téléphone fourni en contactant le service à son numéro habituel (disponible sur le contrat au moment de la souscription) ;
- ne jamais dévoiler de données personnelles, privées ou sensibles par téléphone, quel que soit le contexte;
- prévenir les responsables du service légitime de la tentative d'escroquerie afin qu'ils prennent les mesures nécessaires à la résolution de cet incident.

5 Vulnérabilité dans Nagios et le module SNMP

Le CERTA a publié le 02 novembre 2007 l'avis CERTA-2007-AVI-473 relatif à deux vulnérabilités dans les extensions du logiciel de supervision `Nagios`. L'une d'entre elles concerne une faille dans l'extension *check_snmp* et permet l'exécution de code arbitraire à distance. Ce module donne la possibilité à `Nagios` d'intéroger des éléments du réseau via le protocole `SNMP` (`Simple Network Management Protocol`). Généralement, les équipements de réseau comme les routeurs ou les commutateurs mettent en œuvre ce protocole afin de fournir des

éléments de supervision à une console de centralisation comme Nagios ou Big Brother. Outre le fait que la vulnérabilité de Nagios soit relativement importante et doive être corrigée dans les plus brefs délais, le CERTA attire l'attention sur l'absence de prise en compte de la sécurité dans la première version du protocole SNMP ou SNMPv1. En effet, la version 1 de SNMP (RFC-1157, port 161/udp et 161/tcp) n'offre aucun mécanisme d'authentification hormis un système de communautés (*communities*) souvent au nombre de 2 et nommées simplement publique et privée. Il conviendra donc de mettre en œuvre une politique de sécurité visant à limiter l'accès aux services SNMP sur les machines par le biais, par exemple, d'un réseau d'administration dédié ou par l'emploi de réseaux virtuels (VLAN ou VPN) si cela est possible.

6 Les images nommées Captchas

6.1 Introduction

Un Captcha (pour *Completely Automated Turing Test To Tell Computers and Humans Apart*) est une forme de test permettant de distinguer un utilisateur d'une machine. Il se présente souvent sous la forme d'une image dont le contenu est difficilement interprétable par des moyens logiciels. Il peut également s'agir de fichiers audios ou videos.

Le choix d'images pour effectuer ces tests ne favorise pas les personnes malvoyantes ou ayant des troubles affectant l'identification de mots écrits (formes de dyslexie), comme le souligne un rapport du W3C. Des alternatives existent donc au format des images. Nous allons cependant traiter ce cas dans les paragraphes suivants, car il s'agit à la date de rédaction de cet article, du test le plus répandu.

6.2 *MoBIC* : Le mois des vulnérabilités concernant les Captchas

Les mois précédents ont vu l'apparition de défis, sous la forme : « le mois des vulnérabilités sur ... ». Le CERTA a mentionné dans plusieurs bulletins ces défis. Ce mois de novembre 2007 est dédié, par certains, aux Captchas : MoBIC (*Month of Bugs in Captchas*).

Le CERTA reviendra éventuellement dans de prochains articles sur des publications intéressantes liées à cet événement. La sécurité des Captchas se limite parfois dans les esprits à la difficulté que les outils automatiques peuvent rencontrer pour interpréter le contenu visuel de l'image. En effet, le fondement même du développement et du déploiement des Captchas repose sur ce point sensible. Des sites présentent d'ailleurs certaines faiblesses des images Captchas, en fonction de leur méthode de construction (cf. section Documentation). Il est en revanche plus rare de considérer les vulnérabilités plus contextuelles ou architecturales liées à la mise en œuvre d'une solution basée sur les Captchas.

Ainsi, dès le premier jour de ce MoBIC, des vulnérabilités ont été signalées :

1° la première vulnérabilité vise la construction de l'image à partir d'un texte. Certains sites produisent le texte (via un Javascript) sur le poste client, puis le communiquent au serveur par une méthode HTTP GET au site distant afin de générer l'image à afficher. Il suffit donc à une personne malveillante d'intercepter cette requête sortante, pour avoir la réponse directe au Captcha, avant même que celui-ci ne s'affiche ;

2° certains sites laisseraient la possibilité à une personne malveillante de ré-utiliser le même code d'un Captcha à de multiples reprises. La vulnérabilité s'appuie sur une mise en œuvre ASP.NET, et le contournement de la protection CSRF (*Cross-Site Request Forgery*). Elle consiste à réutiliser certaines valeurs de variables.

Dans ces deux cas, il ne s'agit donc pas de la qualité même de la construction de Captchas, mais de son utilisation dans un environnement de production.

6.3 L'interprétation des Captchas par des tierces personnes

Certains sites proposent ainsi de tels tests pour empêcher à des « robots » l'accès de certaines pages. Si une personne malveillante n'a pas le temps d'interpréter chaque image qui lui est présentée, mais si elle souhaite néanmoins automatiser diverses actions, elle peut passer par la manipulation de tierces personnes. Cela peut se faire suivant deux grandes méthodes :

- par l'embauche, ou la participation de personnes dévouées à cette tâche, et pouvant être rémunérées ;
- par la manipulation de toute personne allant visiter un site. Ce dernier doit avoir, de préférence, un taux de fréquentation élevé, afin d'assurer une certaine « efficacité » à interpréter un grand nombre de Captchas

différents ; il s'agit bien souvent de sites au contenu pornographique, ou de téléchargement. Le scénario est le suivant :

1° la personne malveillante a un outil qui récupère les Captchas sur les sites susceptibles de l'intéresser ;

2° elle les affiche sur un site à forte fréquentation, en proposant par exemple l'affichage ou le téléchargement à tout utilisateur après interprétation du Captcha ;

3° l'utilisateur intéressé renseigne le site malveillant ;

4° ce dernier retourne le résultat sur le site d'origine, et peut accéder au contenu initialement d'accès limité.

L'utilisateur doit donc comprendre qu'il peut être manipulé et servir d'intermédiaire à de telles activités malveillantes. Il est important de ne pas naviguer sur des sites dangereux ou d'apparence plus que douteuse. L'administrateur du site peut, lui, surveiller les temps de réaction entre la création d'un Captcha et la réception de la réponse de l'utilisateur, et ajouter éventuellement un compte-à-rebours. La solution par nature du Captcha est de distinguer la machine d'une personne, mais pas de garantir que la personne qui lui réponde est habilitée à le faire. D'autres mécanismes doivent être mis en place pour assurer ce dernier point.

6.4 Documentation

- Le site sur les Captchas, maintenu par l'université de Carnegie-Mellon :
  http://www.captcha.net
- Des alternatives aux Captchas visuels, proposées par le W3C Working Group :
  http://www.w3.org/TR/turingtest/
- Les faiblesses techniques de certaines mises en œuvre de Captchas :
  http://sam.zoy.org/pwntcha

7 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 25 octobre et le 01 novembre 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 26 octobre au 01 novembre 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-456 : Vulnérabilité de l'antivirus Trend Micro
– CERTA-2007-AVI-457 : Multiples vulnérabilités dans RealPlayer
– CERTA-2007-AVI-458 : Multiples vulnérabilités de HP OpenView
– CERTA-2007-AVI-459 : Multiples Vulnérabilités dans IBM Lotus Notes
– CERTA-2007-AVI-460 : Vulnérabilités dans OpenLDAP
– CERTA-2007-AVI-461 : Multiples vulnérabilités dans IBM Lotus Domino
– CERTA-2007-AVI-462 : Vulnérabilité de McAfee e-Business Server
– CERTA-2007-AVI-463 : Vulnérabilités dans Symantec Mail Security for SMTP
– CERTA-2007-AVI-464 : Multiples vulnérabilités dans IBM AIX
– CERTA-2007-AVI-465 : Vulnérabilité dans NuFW
– CERTA-2007-AVI-466 : Vulnérabilité dans les serveurs Sun Fire X2100/X2200 M2

10 Actions suggérées

10.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

10.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

10.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

10.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

10.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

10.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexpliqués et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

10.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

11 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

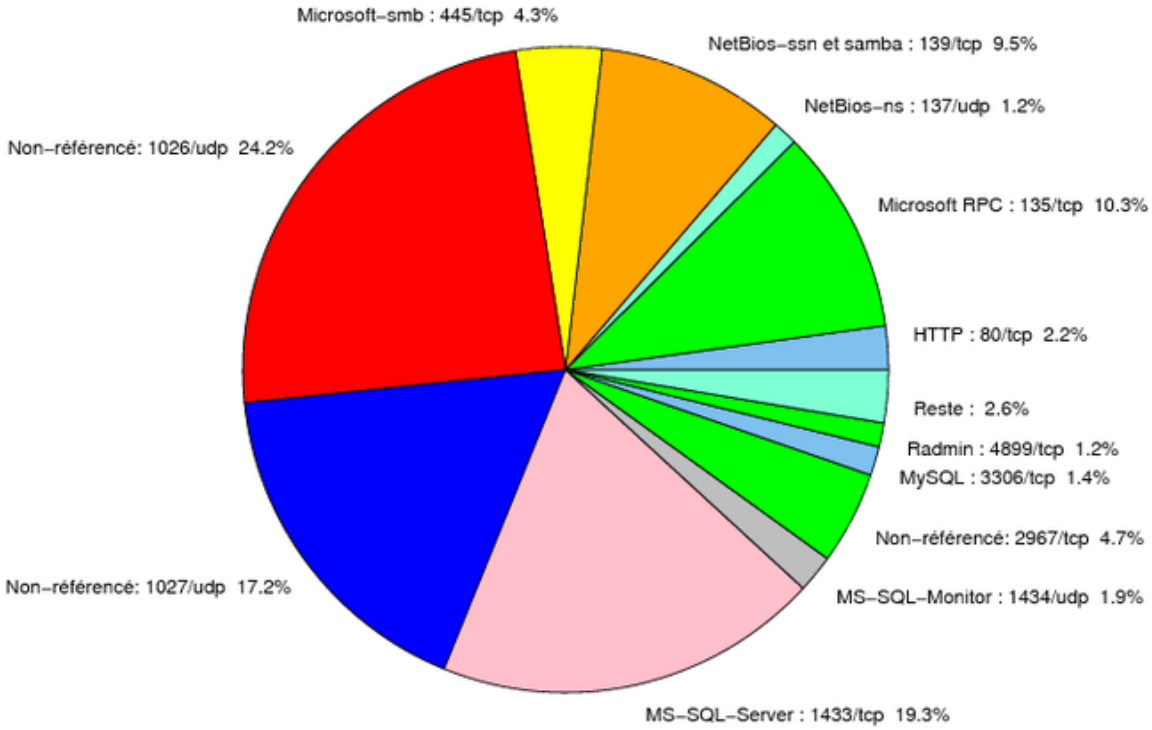

FIG. 1: Répartition relative des ports pour la semaine du 25.10.2007 au 01.11.2007

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	24.15
1433/tcp	19.3
1027/udp	17.22
135/tcp	10.28
139/tcp	9.47
2967/tcp	4.65
445/tcp	4.3
80/tcp	2.18
1434/udp	1.89
3306/tcp	1.44
137/udp	1.23
4899/tcp	1.19
22/tcp	0.79
1080/tcp	0.54
3128/tcp	0.42
21/tcp	0.27
23/tcp	0.23
143/tcp	0.11
2100/tcp	0.07
3389/tcp	0.05
15118/tcp	0.03

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

02 novembre 2007 version initiale.