



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 septembre 2007
N° CERTA-2007-ACT-036

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-36

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-036>

Gestion du document

Référence	CERTA-2007-ACT-036
Titre	Bulletin d'actualité 2007-36
Date de la première version	07 septembre 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-036.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-036/>

1 La tempête ?

1.1 Description

Un ver, connu sous les noms de Storm Worm, Zhelatin, Gang ou Nuwar se propage actuellement sur l'Internet. Ce dernier n'est pas récent et a fait l'objet, dès février, de plusieurs articles dans des publications du CERTA (cf. bulletins d'actualité CERTA-2007-ACT-007, CERTA-2007-ACT-028 et CERTA-2007-ACT-034). Il présente néanmoins quelques caractéristiques originales. Les rapports remontés par les antivirus de plusieurs correspondants motivent cet article.

Un ver se caractérise très souvent par trois caractéristiques :

- un vecteur d'attaque : comment entre-t-il sur un système ?
- un vecteur de contamination : que fait-il sur un système compromis ?
- un vecteur de propagation : comment va-t-il chercher de nouvelles victimes ?

Zhelatin n'utilise pas, dans ses versions actuelles, de vulnérabilités connues pour s'introduire dans un système. Sa propagation résulte en grande partie de techniques « d'ingénierie sociale », incitant l'utilisateur à se

rendre sur un site ou à cliquer dans un lien présent dans un courrier électronique, afin de télécharger et installer un fichier exécutable.

Le ver Zhelatin a plusieurs modes de propagation. Les machines compromises peuvent devenir des émetteurs de courriers électroniques. Le code s'appuie sur des listes pré-construites de corps de message, de sujets et de noms de domaines pour créer les expéditeurs. Les machines infectées envoient des courriels combinant ces informations à des adresses victimes, à un rythme soutenu.

Les sujets des méls peuvent être de tout ordre :

- liés à l'actualité (tempête de décembre 2006, fête nationale, Saint-Valentin, situation en Iran ou en Iraq, etc.) ;
- liés à des thèmes plus classiques : cartes postales électroniques, vidéo à télécharger, rencontres, argent facile, outils de sécurité ou de dissimulation de traces, etc.

Une autre forme de propagation observée consiste à ajouter des codes Javascript dissimulés dans des pages Web de serveur, ou sur des listes de diffusion / bloc-notes.

La contamination de l'ordinateur se traduit par un envoi de courriers non sollicités ou une participation à une attaque distribuée en déni-de-service. Il peut également y avoir une modification de la configuration DNS de la machine. Des outils de capture de frappe claviers ont également pu être observés sur certaines machines infectées, même si le lien direct avec Zhelatin n'est pas encore avéré. Les machines compromises (ou zombies) font partie d'un réseau, et l'objet de la compromission peut évoluer.

Il s'agit d'une architecture complexe, profitant de plusieurs caractéristiques : des réseaux pair-à-pair pour échanger des données et des instructions, et des enregistrements DNS éphémères (association entre une adresse IP et un nom de machine).

L'architecture n'est pas encore, à la date de rédaction de cet article, complètement connue.

Certains éléments permettent cependant d'identifier les compromissions et de limiter les risques. Ils sont détaillés dans la section suivante.

Les versions à jour de plusieurs anti-virus reconnaissent un grand nombre de variantes du ver.

Le CERTA invite ces correspondants à l'informer de toute découverte de traces à ce sujet.

1.2 Contournement provisoire

Plusieurs mesures standards peuvent être considérées pour éviter d'exposer ces systèmes à un tel ver, aussi bien par l'utilisateur, que par l'administrateur du réseau :

1° Pour les utilisateurs :

- ne pas faire confiance au champ FROM : des courriels ;
- ne pas cliquer de façon inconsidérée sur des liens insérés dans les messages ;
- désactiver le Javascript par défaut ;
- rester vigilant et méfiant. Par exemple, les mises à jour de sécurité sont rarement diffusées par mél, et les consignes de mises à jour sont annoncées par l'équipe de soutien informatique ou le responsable de sécurité.

2° Pour les administrateurs et responsables informatiques :

- au niveau réseau :
 - vérifier les politiques de filtrage réseau au niveau des pare-feux, et notamment les règles associées aux connexions sortantes. Le trafic pair-à-pair doit être surveillé ou bloqué. Les machines compromises se caractérisent par un trafic souvent plus important en UDP, vers des ports Overnet/eDonkey (valeurs des ports variables).
 - vérifier au niveau des journaux si des connexions ont pu être établies vers des machines associées à certains domaines suspects ;
 - vérifier l'intégrité du contenu des sites Web, et contrôler avec vigilance les données entrées par les utilisateurs sur des forums ou des listes de diffusion ;
 - filtrer au niveau des passerelles de navigation et de messagerie les téléchargements et les pièces jointes (les versions actuelles du ver se limitent pour le moment aux extensions .EXE et .GIF) ;
 - consulter les journaux des serveurs DNS et des serveurs de messagerie pour vérifier aucun comportement anormal : hausse importante du nombre de requêtes de type MX, augmentation du nombre de courriers retournés invalides, volume accru d'envois, etc.

- modérer les forums et les listes de diffusion sur lesquelles des personnes extérieures peuvent contribuer.
- au niveau des postes des utilisateurs :
 - vérifier que la politique de sécurité est bien respectée : par exemple, la navigation, ou la lecture d'une messagerie doit se faire d'un compte aux droits limités
 - mettre à jour les systèmes et les logiciels ;
 - sensibiliser les utilisateurs (en s'appuyant par exemple sur les documents disponibles sur le site du CERTA).

1.3 Documentation

- Bulletin d'actualité CERTA-2007-ACT-007 du 16 février 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-007.pdf>
- Bulletin d'actualité CERTA-2007-ACT-028 du 13 juillet 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-028.pdf>
- Bulletin d'actualité CERTA-2007-ACT-034 du 24 août 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-034.pdf>
- Note d'information CERTA-2005-INF-004 : « Limiter l'impact du SPAM » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004>
- Les mémentos du CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002.pdf>

2 Traitement des URI par Mozilla Firefox

L'alerte CERTA-2007-ALE-013 du 27 juillet 2007 détaillait une vulnérabilité de Mozilla Firefox permettant à une personne d'exécuter des commandes arbitraires à distance en incitant un utilisateur à suivre un lien spécialement conçu. Mozilla avait rapidement réagi en sortant les versions 2.0.0.6 de Firefox et Thunderbird ; toutefois ces mises à jour n'ont corrigé la vulnérabilité que partiellement.

L'éditeur lui-même avait en effet expliqué dans son bulletin de sécurité MFSA2007-27 que le correctif empêche l'exécution des preuves de faisabilité publiées, mais ne corrige pas le problème sous-jacent. Ainsi, le traitement des URI est encore vulnérable, dans le sens où il reste possible de contourner l'action par défaut liée au protocole et de passer au contraire par le gestionnaire de type de fichier, qui lancera un programme en fonction de l'extension du fichier appelé dans l'URI.

Récemment, les chercheurs qui avaient publié la vulnérabilité ainsi qu'une première preuve de faisabilité ont annoncé avoir trouvé au moins un moyen de contourner le dernier correctif de Mozilla. Aucune preuve de faisabilité n'a cependant été publiée. Le CERTA rappelle un contournement non-intrusif consistant à mettre les options `network.protocol-handler.warn-external.XX` à "true" dans la fenêtre `about:config` pour forcer l'affichage d'avertissements par Mozilla Firefox.

Documentation associée

- Bloc-notes de Billy Rios :
<http://xs-sniper.com/blog/2007/09/01/firefox-file-handling-woes>
- Bulletin de sécurité Mozilla MFSA 2007-27 du 30 juillet 2007 :
<http://www.mozilla.org/security/announce/2007/mfsa2007-27.html>

3 Mises à jour de Microsoft pour le mois de septembre

Microsoft a annoncé, par le biais d'un article dans son bloc-notes, les différentes mises à jour qui seront publiées mardi 11 septembre 2007. Cinq bulletins de sécurité sont prévus, dont :

- un concernant Microsoft Windows, et estimé par la société comme « critique » ;
- un concernant Microsoft Visual Studio, et estimé par la société comme « important » ;
- un concernant Microsoft Windows Services pour Unix, et estimé par la société comme « important » ;
- un concernant Microsoft MSN Messenger, et estimé par la société comme « important » ;

- un concernant Microsoft Windows et Microsoft SharePoint Server, et estimé par la société comme « important ».

En marge de ces bulletins, Microsoft annonce aussi une mise à jour prioritaire de Microsoft Update, mais qui ne serait pas, selon le document de la société, lié à un problème de sécurité.

Ces informations sont visibles sur le bloc-notes de Microsoft :

<http://blogs.technet.com/msrc/archive/2007/09/06/september-2007-bulletin-release-advance-notification.aspx>

4 Connaître la boîte, pour mieux déterminer ses vulnérabilités

4.1 Problématique générale

Plusieurs solutions commerciales vendues actuellement, sous une forme logicielle ou matérielle, s'appuient en partie sur des codes ou projets existants, mis à disposition dans le cadre de partenariats ou de logiciels libres. Ceci n'est pas surprenant. Etant donnée la complexité des systèmes actuels, il est quasiment impossible pour une entreprise de développer des solutions dans leur intégralité. La remarque de cet article n'est pas de ce propos, mais concerne plutôt les conséquences que cette intégration implique sur la notion de mise à jour.

Il est important de connaître ces intégrations dans les solutions commerciales. La raison principale est que les vulnérabilités découvertes sur les logiciels intégrés sont très fréquemment rendues publiques, et qu'il est donc possible d'estimer rapidement les vulnérabilités pouvant affecter la solution commerciale. Si les fabricants n'ont pas une veille attentive sur ces produits, ou se préoccupent peu de celle-ci, il y a alors des risques d'avoir des vulnérabilités permanentes dans la solution commercialisée. Cela doit être pris en compte dans la politique de sécurité globale.

Le CERTA insiste donc bien auprès de sa communauté à considérer ces aspects d'intégration et de transparence par les fabricants dans leur choix de mise en œuvre.

4.2 Une illustration

Les exemples liés à la remarque précédente sont très nombreux, et couvrent des technologies très diverses. Considérons les outils d'analyse réseau. Qu'ils soient sous forme d'IDS (*Intrusion Detection Systems*), de renifleurs (*sniffers*), d'outils d'identification de protocoles ou simplement de statistique du trafic (*netflow* par exemple), ces outils ont souvent des caractéristiques communes. Ils s'appuient sur des projets libres comme :

- libpcap et sa variante pour Windows winpcap
- tcpdump
- wireshark (anciennement ethereal)

Cette utilisation est soit clairement annoncée, soit dissimulée.

Plusieurs vulnérabilités ont affectées ces logiciels. Pour 2007 :

- CERTA-2007-AVI-067 : des vulnérabilités de Wireshark dans des modules d'analyse TCP, HTTP, 802.11 ou LLT de Wireshark seraient exploitables par l'envoi de paquets spécialement construits ;
- CERTA-2007-AVI-278 : des vulnérabilités de Wireshark concernant l'interprétation de paquets HTTP, DCP ETSI, SSL, MMS ou DHCP pourraient, si elles sont exploitées, provoquer la perturbation du service Wire-shark ;
- CERTA-2007-AVI-323 : une vulnérabilité de tcpdump concernant la manipulation de paquets associés au protocole de routage BGP pourrait permettre à une personne distante d'exécuter du code arbitraire sur le système vulnérable, par le biais d'un paquet spécialement construit ;
- CERTA-2007-AVI-289 : une vulnérabilité dans la gestion du pilote NPF.SYS de winpcap permet à un utilisateur local d'élever ses privilèges à ceux du système pour exécuter des commandes arbitraires.

Certaines des vulnérabilités publiées ne font pas l'objet d'avis du CERTA, car elles concernent des anciennes versions de ces logiciels.

Ainsi, la première semaine de septembre 2007, un code d'exploitation a été diffusé sur l'Internet, et cible le module d'analyse du protocole DNP3. Le *Distributed Network Protocol* regroupe en réalité plusieurs protocoles de communication et se retrouve dans des systèmes de type SCADA. Une personne distante, par le biais d'un paquet spécialement conçu, peut exploiter la vulnérabilité en question afin de provoquer un déni de service.

Cette vulnérabilité pose des problèmes car, très souvent, la surveillance d'un réseau repose sur des outils tels que ceux mentionnés. Si ceux-ci sont indisponibles, la surveillance est largement réduite.

Quid des mises à jour des solutions commerciales ? Plusieurs boîtiers s'appuient sur les modules d'analyse de Wireshark. L'administrateur doit donc se poser les questions suivantes :

- Mes systèmes emploient-ils de tels modules ?

- Sont-ils vulnérables à une telle exploitation ?
 - Dans l'affirmative, ont-ils été mis à jour ?
- Ce questionnement implique de connaître certains détails techniques que les boîtiers enveloppent.

Documentation associée

- Référence CVE CVE-2007-4721 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4721>
- Annonce de sécurité IBM Internet Security Systems du 30 août 2007 :
<http://xforce.iss.net/xforce/xfdb/36392>
- Mises à jour proposées par le projet Wireshark :
<http://www.wireshark.org>

5 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 30 août et le 06 septembre 2007.

6 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/>

7 Rappel des avis émis

Dans la période du 31 août au 06 septembre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-383 : Vulnérabilité dans Subversion (svn)
- CERTA-2007-AVI-384 : Multiples vulnérabilités dans Konqueror
- CERTA-2007-AVI-385 : Multiples vulnérabilités de BEA Weblogic
- CERTA-2007-AVI-386 : Vulnérabilités dans Claroline

- CERTA-2007-AVI-387 : Vulnérabilité de Policyd pour Postfix
- CERTA-2007-AVI-388 : Multiples vulnérabilités dans PHP
- CERTA-2007-AVI-389 : Vulnérabilité de Apple AirPort Extreme Base Station
- CERTA-2007-AVI-390 : Vulnérabilités dans Kerberos
- CERTA-2007-AVI-391 : Vulnérabilité dans GNU Tar
- CERTA-2007-AVI-392 : Vulnérabilités dans IBM AIX

8 Actions suggérées

8.1 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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme 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 réglementaire, 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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 inexplicables 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.

8.7 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>

9 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.

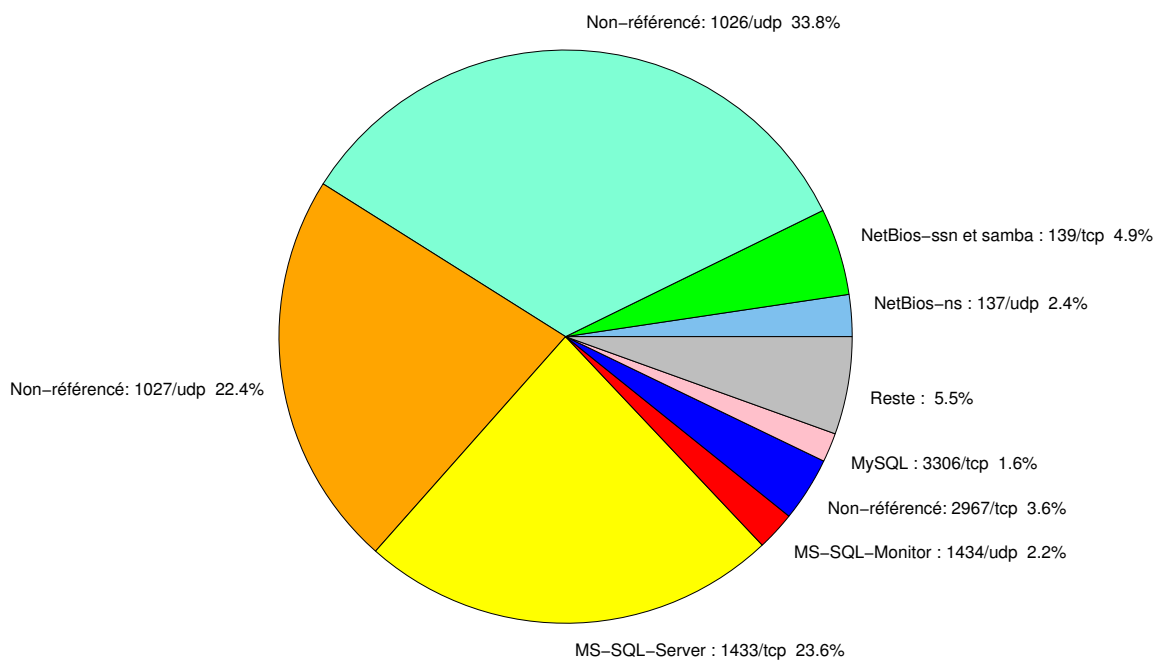


FIG. 1: Répartition relative des ports pour la semaine du 30.08.2007 au 06.09.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002

2381	TCP	–	HP System Management	CERTA-2006-AVI-248
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310

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

port	pourcentage
1026/udp	33.79
1433/tcp	23.57
1027/udp	22.41
139/tcp	4.89
2967/tcp	3.62
137/udp	2.35
1434/udp	2.19
3306/tcp	1.63
80/tcp	0.99
4899/tcp	0.97
22/tcp	0.9
25/tcp	0.82
3128/tcp	0.57
1080/tcp	0.53
3389/tcp	0.12
443/tcp	0.11
15118/tcp	0.07
9898/tcp	0.05
143/tcp	0.03
1023/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	9
3	Paquets rejetés	10

Gestion détaillée du document

07 septembre 2007 version initiale.