

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-29

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-029>

Gestion du document

Référence	CERTA-2007-ACT-029
Titre	Bulletin d'actualité 2007-29
Date de la première version	20 juillet 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-029.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-029/>

1 Une architecture de gestion des machines zombies

1.1 Introduction

Les personnes malveillantes sont souvent astucieuses, mais dans le cas général, elles cherchent assez naturellement à simplifier leurs modes opératoires, et à tirer un maximum de profits pour une opération donnée. Ces dernières années, il est donc fréquent d'entendre parler de réseaux de machines compromises, ou « machines zombies », dirigées par un contrôleur central (le C&C ou Command&Control). Ces machines, massivement compromises, sont soumises aux directives de ce serveur, soit directement, soit indirectement, par le biais d'une chaîne de contrôleurs intermédiaires, pour rendre l'accès au C&C plus opaque.

Les objectifs pour construire de tels réseaux de machines compromises sont variés :

- les utiliser comme relais de messagerie pour émettre des courriels indésirables (*spam*) ou utiles à une attaque par filoutage ;
- diffuser des codes malveillants, sous forme de pièces jointes à des courriels ;
- héberger des sites web frauduleux de filoutage ;
- stocker des données (vidéos, images, codes malveillants) ;
- attaquer en déni de service un serveur distant en synchronisation avec les autres machines zombies;

- louer à qui veut un parc de machines afin qu’il profite lui-même des possibilités mentionnées ci-dessus ;
- etc.

Le moyen de communication le plus fréquemment cité est l’IRC, qui peut se manifester par des trames échangées entre des machines internes au réseau et des machines distantes, vers leurs ports 6660-6670/TCP. Un très grand nombre de moyens de communication sont également possibles, afin d’utiliser des flux plus atypiques, comme ceux des données HTTP (pages, images), ou DNS, ou ICMP, etc. Il ne s’agit cependant pas ici de décrire certains types de canaux cachés, mais plutôt de montrer une évolution de cette architecture générale.

1.2 Architecture et astuces

Comme hypothèse, prenons un courrier de filoutage, contenant une adresse réticulaire `www.Mauvais_SiteXX.net`, redirigeant l’utilisateur vers une copie d’un site légitime.

Ce dernier, s’il découvre la supercherie, peut, soit mécaniquement par le biais d’un logiciel, soit manuellement, contacter le fournisseur d’accès pour signaler le comportement étrange de la machine `W.X.Y.Z` répondant au nom `www.Mauvais_SiteXX.net`.

Afin de rendre ces actions moins dangereuses pour leurs affaires, les personnes malveillantes utilisent parfois une architecture plus robuste. En voici les détails :

- 1° la personne malveillante dispose d’un nom de domaine complet (ou FQDN, pour *Fully Qualified Domain Name*) : `www.Mauvais_SiteXX.net` ;
- 2° elle dispose également d’un ensemble de machines compromises, ayant des adresses IPs distinctes : IP1, IP2, IP3, ... IPn.
- 3° les associations entre le nom de domaine et les adresses IPs précédentes changent très fréquemment, à partir par exemple d’un roulement régulier (*round-robin*) et d’une date d’expiration DNS (aussi appelée TTL ou *Time-To-Live*) très courte.

Pour la personne malveillante, cela permet de brouiller quelques pistes et de distribuer les charges de trafic vers les sites frauduleux.

Le scénario peut même impliquer deux groupes de machines compromises : celles contenant les sites de filoutage et celles servant de relais DNS.

Pour l’utilisateur, toutes les opérations se font à son insu. La figure 1 illustre une telle situation.

- il clique sur un lien contenu dans un courrier électronique, qui cherche à atteindre `www.Mauvais_SiteXX.net` ;
- pour contacter cette machine, une résolution de nom est nécessaire, et une requête est envoyée au serveur DNS (étape 1) ;
- en considérant qu’il n’y a pas la solution en cache et que les dates d’expiration sont très courtes, la hiérarchisation DNS conduit l’utilisateur vers le serveur de nom du domaine `Mauvais_SiteXX.net` (étape 2) ;
- ce serveur, pouvant également être un serveur compromis, ou une redirection vers un autre serveur DNS, retourne *in fine* une adresse IP, parmi celles disponibles et fonctionnelles du réseau de machines compromises (étape 3). Le choix de l’adresse peut varier toutes les minutes par exemple ;
- le navigateur de l’utilisateur peut charger la page malveillante, car il a contacté l’une des machines compromises, ici IP2 (étape 4).

1.3 Les moyens préventifs

1.3.1 Pour l’utilisateur

L’utilisateur, dans le scénario précédent, a voulu se rendre initialement sur le site `www.Mauvais_SiteXX.net`. Il est important de ne pas cliquer sur des liens inclus dans les corps des courriers électroniques, et de se rendre sur des sites de confiance, avec toutes les précautions nécessaires (interprétation de codes dynamiques désactivés).

Des mesures de filtrage par des listes dites « blanches » ou « noires » sont également possibles, par exemple à partir d’outils d’anti-filoutage. Cependant, ces solutions posent d’autres problèmes (origine de la liste, maintenance, faux-positifs, etc.) qui doivent également être pris en considération.

1.3.2 Détection au niveau des trames DNS

Il est souvent plus facile de filtrer les interactions des machines de son réseau avec le monde extérieur au niveau réseau (IP) et transport (TCP ou UDP par exemple). Dans le cas présent, il s’agit de filtrer à un niveau supérieur,

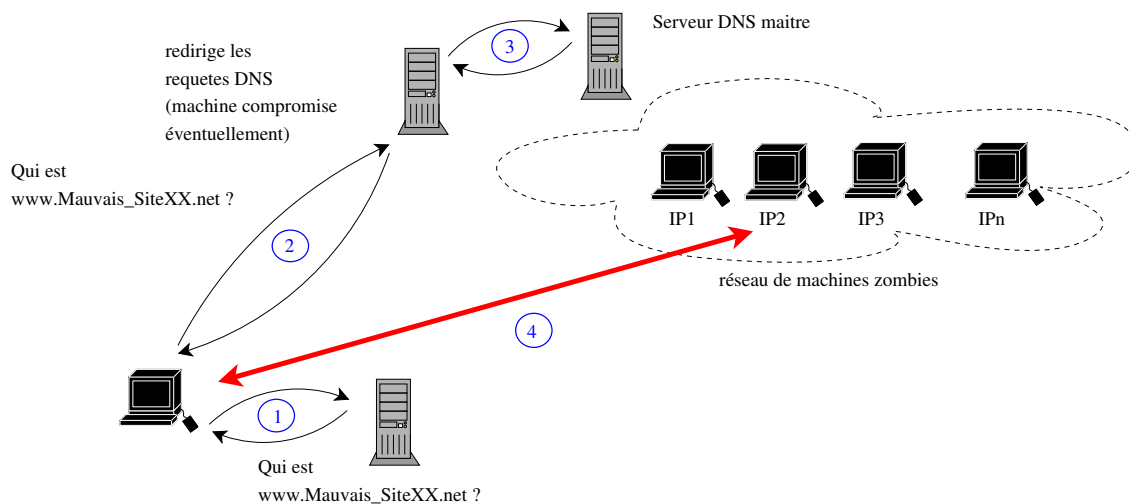


FIG. 1: Architecture possible de l'utilisation d'un réseau de machines zombies

afin d'empêcher des interactions avec certains noms de domaine. Des mesures peuvent être entreprises au niveau des serveurs de relais *proxy*, au moyen de règles et de listes blanches et noires.

L'administrateur peut également essayer d'analyser les trames DNS qui circulent. Les documents cités ci-dessous fournissent quelques pointeurs. Il s'agit de récupérer les réponses DNS (d'autorité si possible) (la requête se trouvant également incluse dans la trame réponse), et d'essayer d'en extraire les enregistrements les plus éphémères, ou le nombre d'enregistrements de type A ou NS retournés par requête. Les durées d'expiration de courte valeur sont également des critères d'observation.

Il faut cependant vérifier préalablement que cette collecte d'informations répond bien aux exigences de la politique de sécurité en vigueur.

1.4 Documentation associée

- B. Zdrnja, N. Brownlee, D. Wessels, « Passive Monitoring of DNS Anomalies » : http://www.caida.org/publications/papers/2007/dns_anomalies/
- « Know Your Enemy: Fast-Flux Service Networks » : <http://www.honeynet.org/papers/ff/fast-flux.html>

2 Révélation de mots de passe par certains logiciels

Cette semaine, IBM a confirmé une vulnérabilité¹ découverte dans le client de messagerie Lotus Notes. En effet, le fait d'ajouter deux lignes dans le fichier de configuration du logiciel a pour conséquence de créer des informations de débogage dans un fichier, parmi lesquelles figure le mot de passe en clair de l'utilisateur. Voici ces deux lignes :

```
KFM_ShowEntropy=1
Debug_Outfile=c:\testvowe.txt
```

Ce mot de passe étant la pierre angulaire de la sécurisation de Lotus Notes, l'ajout de ces lignes dans le fichier de configuration est à proscrire.

Ce comportement n'est malheureusement pas isolé, et un grand nombre de logiciels sauvegardent des mots de passe dans des fichiers texte en clair. C'est notamment le cas de nombreux CMS (*Content management System*, ou Système de Gestion de Contenu).

Il est donc important de rester vigilant lors de l'installation de tout logiciel, et de vérifier le contenu des fichiers créés afin que ceux-ci ne mettent pas en défaut la sécurité de son système.

¹Le CERTA n'a pas publié d'avis concernant cette vulnérabilité car celle-ci n'est pas présente sur une installation classique du logiciel.

3 URL spoofing dans les navigateurs Internet

Dernièrement, plusieurs vulnérabilités ont été publiées concernant les navigateurs Firefox, Internet Explorer, Opera et Konqueror.

En ce qui concerne Firefox, des pages web malveillantes peuvent accéder au cache du navigateur via des URI de type `wyciwyg://` (*What You Click is What You Get*). Celles-ci sont normalement inaccessibles pour des utilisateurs, toutefois trois moyens différents contournant le contrôle d'accès ont été révélés par un chercheur. L'accès à l'URI `wyciwyg` permet notamment à un attaquant d'accéder à des informations confidentielles, d'injecter des données dans les documents, ou encore d'usurper la barre d'adresse URL. Cette vulnérabilité est corrigée dans la mise à jour 2.0.0.5 de Firefox, dont le contenu entier est détaillé dans l'avis CERTA-2007-AVI-318 du 18 juillet 2007.

La vulnérabilité dans Internet Explorer, qui utilise Javascript, consiste à empêcher une personne de quitter une page créée par l'attaquant tout en affichant correctement l'URL spécifiée par l'utilisateur. Le principe est d'appeler continuellement une fonction pour qu'elle soit invoquée avant la transition vers la page appelée. La particularité de cette faille est qu'elle fonctionne si l'utilisateur tape directement une URL dans la barre d'adresse. La vulnérabilité n'est pas corrigée et concerne au moins le navigateur Internet Explorer 7.

Enfin, la vulnérabilité concernant les navigateurs Opera et Konqueror est due à un mauvais affichage des URL `data:` qui contiennent des données. En effet, seule la fin d'une adresse URL est affichée dans une page web construite de cette manière. Il est donc possible de cacher la véritable URL en utilisant des caractères espace. Cette vulnérabilité est corrigée dans la version 9.22 d'Opera, dont le détail se trouve dans l'avis CERTA-2007-AVI-324 du 20 juillet 2007.

Ces trois vulnérabilités permettent donc de cacher les véritables URL des sites visités par un utilisateur. Elles seraient particulièrement efficaces dans des attaques par filoutage, par exemple. S'il est recommandé de taper des URL manuellement, la faille concernant Internet Explorer contourne cela. Cependant, celle-ci utilise du code Javascript, qui devrait être désactivé par défaut.

3.1 Références

- Avis du CERTA CERTA-2007-AVI-318 du 18 juillet 2007 : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-318/>
- Avis du CERTA CERTA-2007-AVI-324 du 20 juillet 2007 : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-324/>

4 Cycle de vie de php4

Le projet php développeur du langage du même nom, a annoncé sur son site (<http://www.php.net>) que la branche 4.x de php ne serait plus maintenue à compter du 31 décembre 2007. Cela veut dire qu'à partir de cette date, il ne sera plus fourni de mise à jour ou de correctif de sécurité pour cette version. Le CERTA recommande vivement d'envisager dès à présent une migration vers la version 5.

5 Installation de pilotes sous GNU/Linux

Le constructeur Samsung propose des pilotes pour ses imprimantes et ses scanners sous GNU/Linux. Cependant, il semblerait que le programme d'installation exécute des opérations affaiblissant le niveau de sécurité du système. En effet si l'on examine le code du script shell d'installation on peut y trouver la section suivante :

```
wrap_setuid_third_party_application xsane
wrap_setuid_third_party_application xscanimage

wrap_setuid_ooo_application soffice
wrap_setuid_ooo_application swriter
wrap_setuid_ooo_application simpres
wrap_setuid_ooo_application scalc
```

On peut ensuite examiner le code correspondant aux fonctions appelées ici :

```
wrap_setuid_third_party_application() {
    if echo "$1" | grep -q "/" ; then
```

```

        APP_NAME=$1
    else
        APP_NAME=`which $1 2> /dev/null`
    fi
    NEW_NAME=${APP_NAME}.bin

    if test -n "$APP_NAME" ; then
        if ! test -f "$NEW_NAME" && ! test -d "$NEW_NAME"; then
            mv "$APP_NAME" "$NEW_NAME"
            cp -af /opt/${VENDOR}/mfp/bin/suwrap "$APP_NAME"
            chown root:root "$APP_NAME"
            chmod 4755 "$APP_NAME"
        fi
    fi
}

wrap_setuid_ooo_application() {
    WRAPPING_BIN=`ls /usr/lib*/*/program/$1.bin /opt/*/program/$1.bin 2> /dev/null`
    if test -n "$WRAPPING_BIN" ; then
        ${2}wrap_setuid_third_party_application $WRAPPING_BIN
    fi
}

```

Dans les faits, cette partie de code, rend root propriétaire des exécutables soffice, swriter, etc. et positionne le bit SUID sur ces fichiers. Ceci revient à demander au système d'exécuter les exécutables de la suite OpenOffice.org en tant qu'administrateur en permanence quelque soit l'utilisateur lançant ces commandes. Le CERTA recommande donc de modifier soit le script d'installation en remplaçant `chmod 4755` par un `chmod 0755` ou bien d'effectuer cette opération *a posteriori*: `chmod 0755 soffice swriter simpresc scalc` dans le répertoire où ils se trouvent.

6 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 12 et le 19 juillet 2007.

7 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html>
- Note d'information sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html>
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html>
- Note d'information sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html>
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html>
- 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 CERTA-2006-INF-006, Risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/>

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

8 Rappel des avis émis

Dans la période du 13 au 19 juillet 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-303 : Vulnérabilité dans Symantec Backup Exec
- CERTA-2007-AVI-304 : Vulnérabilité dans Cisco Unified Communications Manager
- CERTA-2007-AVI-305 : Vulnérabilité dans AIX d’IBM
- CERTA-2007-AVI-306 : Vulnérabilité de ClamAV
- CERTA-2007-AVI-307 : Multiples vulnérabilités de AVG Antivirus
- CERTA-2007-AVI-308 : Multiples vulnérabilités dans Apple QuickTime
- CERTA-2007-AVI-309 : Multiples vulnérabilités des produits Symantec
- CERTA-2007-AVI-310 : Vulnérabilité dans la commande rcp sous Sun Solaris
- CERTA-2007-AVI-311 : Multiples vulnérabilités dans les produits Oracle
- CERTA-2007-AVI-312 : Vulnérabilité dans IPSwitch WS_FTP Logging Server
- CERTA-2007-AVI-313 : Vulnérabilité de FreeBSD
- CERTA-2007-AVI-314 : Multiples vulnérabilités dans des produits Hitachi
- CERTA-2007-AVI-315 : Multiples vulnérabilités dans les produits CA
- CERTA-2007-AVI-316 : Vulnérabilité dans Kaspersky Anti-Virus pour Check Point Firewall-1
- CERTA-2007-AVI-317 : Vulnérabilité des produits RSA
- CERTA-2007-AVI-318 : Multiples vulnérabilités dans Mozilla Firefox
- CERTA-2007-AVI-319 : Vulnérabilité dans HP ServiceGuard
- CERTA-2007-AVI-320 : Vulnérabilité d’IBM Tivoli Provisioning Manager
- CERTA-2007-AVI-321 : Vulnérabilité dans Cisco Wide Area Application Services (WAAS)
- CERTA-2007-AVI-322 : Plusieurs vulnérabilités dans Ipswitch IMail Server
- CERTA-2007-AVI-323 : Vulnérabilité dans tcpdump

Pendant la même période, les avis suivants ont été mis à jour :

- CERTA-2007-AVI-298-001 : Vulnérabilité dans 3Com TippingPoint IPS (ajout de la référence CVE associée)
- CERTA-2007-AVI-311-001 : Multiples vulnérabilités dans les produits Oracle (ajout des nombreuses références CVE)

9 Actions suggérées

9.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d’Information (PSSI) est l’ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d’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.

9.2 Concevoir une architecture robuste

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

9.3 Appliquer les correctifs de sécurité

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

9.4 Utiliser un pare-feu

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

9.5 Analyser le réseau

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

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

9.6 Réagir aux incidents de sécurité

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

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

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements 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.

9.7 Former et sensibiliser les utilisateurs

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

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

10 Les bulletins d'actualité

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

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

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

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

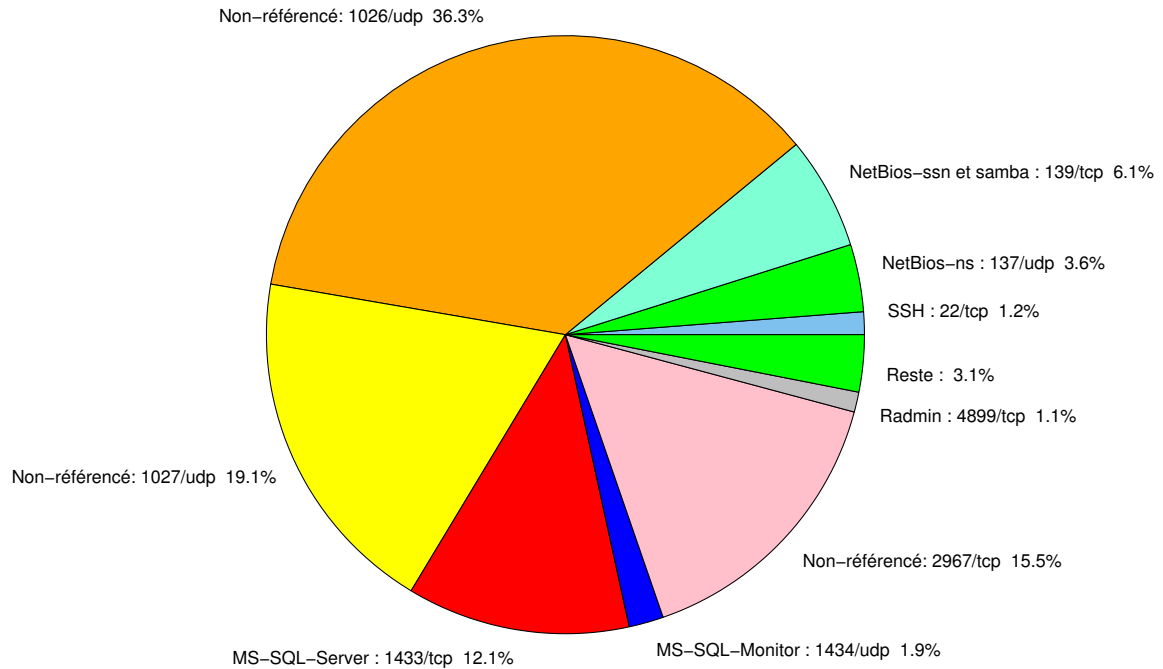


FIG. 2: Répartition relative des ports pour la semaine du 12.07.2007 au 19.07.2007

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	36.31
1027/udp	19.07
2967/tcp	15.53
1433/tcp	12.05
139/tcp	6.1
137/udp	3.64
1434/udp	1.87
22/tcp	1.22
4899/tcp	1.08
3128/tcp	0.66
1080/tcp	0.58
25/tcp	0.41
80/tcp	0.39
3306/tcp	0.37
15118/tcp	0.08
9898/tcp	0.04
2100/tcp	0.02

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

20 juillet 2007 version initiale.