Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mai 2007
N° CERTA-2007-ACT-018

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-18

Gestion du document

Référence	CERTA-2007-ACT-018
Titre	Bulletin d'actualité 2007-18
Date de la première version	04 mai 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-018.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-018/

1 Les incidents traités cette semaine

1.1 L'injection de code indirecte, ou *Cross-Site Scripting*

La recherche de sites vulnérables permettant de réaliser des attaques par injection de code indirecte (*cross site scripting*, ou XSS) se systématise. Ainsi, une cinquantaine de sites publics n'ont pas la robustesse nécessaire face à ces attaques.

L'attaque permet d'injecter des données (généralement des scripts) via le site vulnérable et d'exécuter des commandes malveillantes sur le poste de l'internaute qui le visite. Sont potentiellement vulnérables tous les sites qui retournent à l'internaute une donnée que celui-ci a précédemment fournie. Deux exemples :

- un moteur de recherche qui affiche « n réponses pour la recherche : » suivi des mots clés entrés par l'internaute ;
- un site avec personnalisation affichant « Bienvenue » suivi de l'identité ou du pseudo de l'internaute.

Plus généralement, dès que l'internaute peut entrer une donnée dans un formulaire, la question du XSS se pose.

Comment l'attaque fonctionne-t-elle ? La donnée entrée dans le formulaire contient des caractères spéciaux, qui peuvent être interprétés en HTML (<, >, /,...). S'il s'agit d'une attaque XSS, l'entrée pourra contenir un fragment de la forme <SCRIPT>....</SCRIPT>.

Le processus d'acquisition et de validation des entrées ne fait pas de vérification lexicale et syntaxique :

- il ne rejette pas les entrées non conformes ;
- il n'élimine pas les caractères inattendus (si l'entrée doit être le nom d'un département, le caractère < n'a pas lieu d'apparaître par exemple) ;
- il ne transforme pas les caractères spéciaux en leurs équivalents affichés sans être interprétés comme code HTML (`<` , `>`, `/`...) ;
- la page retournée reprend telle quelle la chaîne de caractères entrée par l'internaute.

Le navigateur de l'internaute interprête le fragment `<SCRIPT>....</SCRIPT>` que l'internaute avait entré dans le formulaire. L'exécution du script se déroule sur le poste du visiteur. Ce script sera exécuté selon les autorisations que l'internaute a positionnées en fonction du site qu'il visite. Ces autorisations se matérialisent par l'utilisation des zones (internet, intranet, sites de confiance) dans *Internet Explorer* ou par des listes blanches dans des extensions de *Firefox* telles *Noscript*). Plus le site est censé être de confiance (institutions publiques, banques...), plus le contexte d'exécution du script sera permissif et plus le risque sera élevé.

Pourquoi un internaute entrerait-il dans un formulaire des caractères dont l'effet peut lui être néfaste ?

La question ne porte pas sur une action *volontaire*, mais sur une action mal maîtrisée, comme le clic sur un lien dans une autre page web ou dans un courriel rédigé en HTML : le lien apparent est inoffensif, mais masque le lien réel qui contient l'entrée malveillante (script injecté).

Les développeurs de ces sites doivent être particulièrement vigilants dans le filtrage des entrées fournies par l'internaute. Le CERTA recommande de réaliser systématiquement un contrôle lexical et syntaxique sur les données saisies dans les formulaires. Le contrôle sémantique permet d'affiner le filtrage syntaxique.

Documentation

- Vulnérabilité de type « Cross Site Scripting » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/
- Sécurité des applications Web et vulnérabilité de type « injection de données » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/

2 Le mois des vulnérabilités ActiveX MoAxB

Le CERTA renouvelle sa recommandation de désactiver les contrôles ActiveX dans Internet Explorer.

Après le mois des vulnérabilités des navigateurs, puis celui des vulnérabilités du langage PHP ou encore celui des vulnérabilités de MacOS, le mois de mai 2007 est déclaré mois de la recherche des failles ActiveX (MoAxB pour Month of ActiveX Bugs).

http://moaxb.blogspot.com/

Pour l'instant des applications non majeures sont touchées. Les quatre premiers avis publiés concernent en réalité des applications tierces comme des contrôles ActiveX de la société `officeocx`, qui permettent la visualisation de documents *Microsoft Office* dans le navigateur. Ces composants ne sont par largement répandus, mais il est probable que d'autres vulnérabilités feront prochainement leur apparition.

Il existe aujourd'hui de nombreuses vulnérabilités non corrigées directement liées aux ActiveX et touchant en particulier Internet Explorer. La position du CERTA sur ces composants est rappelée à cette occasion. Ces composants sont intrinsèquement dangereux. Le CERTA recommande donc vivement de vérifier que les options ActiveX sont désactivées correctement dans le navigateur Internet Explorer. Elles ne doivent être utilisées que ponctuellement, au cours de la visite de pages web de confiance. D'une façon générale, les vulnérabilités propres à ces composants permettent de contourner la politique de sécurité (paramètres des zones de sécurité), d'exécuter des codes à distance ou encore de voler des informations.

Comme cela a déjà été souligné à l'occasion de nombreux articles (à titre d'exemple 3 alertes en 2005 : CERTA-2005-ALE-001, CERTA-2005-ALE-005, CERTA-2005-ALE-013), il peut être utile de prévoir l'utilisation d'un autre navigateur comme par exemple Firefox, Opera ou K-Meleon.

Pour désactiver ActiveX sous Internet Explorer :

- Ouvrir Internet Explorer
- Cliquer sur le menu "Outils"
- Choisir "Options Internet"
- Afficher l'onglet "Sécurité"

- Cliquer sur "Personnaliser le niveau"
- Sélectionner "Désactiver" pour les lignes suivantes :
  - Contrôles ActiveX reconnus sûrs pour l'écriture de scripts
  - Contrôles d'initialisation et de script ActiveX non marqués comme sécurisés
  - Exécuter les contrôles ActiveX et les plugins
  - Télécharger les contrôles ActiveX (signés et non signés)

3 Imperfections protocolaires sous IPv6

Le CERTA a publié l'année dernière une note d'information concernant IPv6, et en particulier certains aspects de sécurité à considérer. L'un d'eux correspond à une extension des en-têtes IPv6, le « *routage par la source* ». Celle-ci est prise en compte par les éléments intermédiaires et destinataires du paquet.

Cette fonctionnalité existe déjà sous IPv4, mais reste très peu utilisée. L'objectif est que l'émetteur du paquet, la `source`, puisse désigner des nœuds particuliers dans le réseau par lesquels le paquet doit circuler pour arriver à destination.

Sous IPv4, l'option `LSR` (pour *Loose Source Routing*) indique qu'une série d'adresses se trouve en complément dans l'en-tête. A chaque nœud intermédiaire (comme un routeur), l'adresse dans le champ destination est modifiée par une des adresses de la liste, dans l'ordre de cette dernière. Par ailleurs, sous IPv4, la longueur du champ option reste limitée (40 octets), ce qui empêche l'emploi abusif d'options.

Sous IPv6, le fonctionnement est identique, mais les documents de référence (dont le RFC 2460) fournissent moins de précisions. Une traduction du texte pourrait être : « L'en-tête de routage est utilisée par une source IPv6 pour lister un ou plusieurs nœuds intermédiaires qui devraient être *rencontrés* en cours d'acheminement vers le destinataire final. (...) L'en-tête de routage est identifiée par la valeur 43 dans le champ `En-tête Suivant`.»

Cette en-tête possède un format faisant intervenir quelques champs :

- le champ `En-tête Suivant`, ou `Next Header`, qui signale si une autre extension est utilisée après celle pour le routage par la source ;
- le champ `Header Length`, qui spécifie la longueur totale de cette extension, données comprises ;
- le champ `Routing Type`, qui caractérise le routage par la source. Nous nous intéressons ici à celui de valeur 0, le plus commun. La valeur 1 n'est pas utilisée, et la valeur 2 n'est exploitée que par les piles IPv6 mobiles `MIPv6`.
- le champ `Segments Left`, qui indique quels éléments de la liste de nœuds intermédiaires ont déjà été `rencontrés`, et ceux qu'il reste ;
- le champ de données, qui comprend donc la liste des nœuds intermédiaires.

Des imprécisions existent à ce sujet, et en particulier :

1. Quel élément doit interpréter ces en-têtes ? Il est bien précisé que cela concerne tout nœud intermédiaire, un nœud étant défini comme un système qui met en œuvre IPv6. Cela peut donc aussi bien être un routeur qu'une machine hôte.
2. Les mêmes nœuds doivent accepter et analyser toute extension dans l'en-tête IPv6, quel que soit l'ordre d'apparition des extensions dans l'en-tête, et leur occurrence.
3. la limite sur la taille de l'extension dans le paquet est bien trop laxiste (taille max du paquet IPv4, ou 2048 octets) ;
4. etc.

Ces imprécisions peuvent être utilisées à des fins malveillantes. Une présentation récente a ainsi montré que des systèmes d'exploitation interprétaient par défaut cette extension (respectueux de la RFC 2640, comme FreeBSD, NetBSD ou OpenBSD), tandis que d'autres ont choisi de jeter tout paquet l'utilisant, estimant que cette extension n'est pas justifiée (Microsoft Windows XP SP2 et Vista par exemple). S'appuyant sur cette particularité, il est possible :

- de lancer des requêtes `traceroute` par des routes bien précises, afin de tester la capacité des nœuds à gérer cette extension ;
- de contourner certaines propriétés de la technologie `anycast` (utilisée par plusieurs serveurs DNS) afin d'identifier et de perturber les différentes machines impliquées (les différents miroirs d'un serveur DNS par exemple) ;
- de véhiculer pendant une longue période (plusieurs dizaines de secondes), un paquet IPv6 entre deux nœuds intermédiaires, afin d'occuper la bande passante, ou de stocker provisoirement des données dans les réseaux ;

– etc.

Il est en revanche très difficile de filtrer proprement cette extension, car chaque matériel a sa propre méthode. Cisco propose par exemple pour IOS la commande `no ipv6 source-route`.

3.1 Recommandations du CERTA

Que conclure ? Tout d'abord, cette extension propre à IPv6 est dangereuse, car elle présente pour l'instant des risques, tandis que son utilisation légitime reste très limitée. Il faut donc prendre quelques précautions, tant au niveau du réseau qu'au niveau des postes terminaux :

– vérifier que les outils de filtrage permettent de rejeter tout paquet contenant une telle extension ;
– mettre à jour les systèmes d'exploitation. FreeBSD a ainsi fourni une mise à jour pour limiter les impacts (cf. section Documentation) ;
– consulter le document CERTA-2006-INF-004 pour obtenir de plus amples détails sur la désactivation des piles IPv6 (quand leur activation n'est pas justifiée) ;
– journaliser et consulter les traces liées au trafic IPv6, ces dernières pouvant souvent être ignorées ou oubliées.

3.2 Documentation associée

– RFC 2460, "Internet Protocol, Version 6 (IPv6)" :
http://www.ietf.org/rfc/rfc2460.txt
– Note d'information CERTA-2006-INF-004, « Migration IPv6 : enjeux de sécurité » :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-I NF-004/
– Référence CVE CVE-2007-2242 :
http://cve.mitre.org/cgi-bin/cvename.cgi ?name=CVE-2007-2242
– Correctif facultatif proposé sous OpenBSD :
http://openbsd.org/errata40.html#012_route6
– Correctif facultatif proposé sous OpenBSD :
http://openbsd.org/errata39.html#022_route6
– Avis de sécurité FreeBSD :
http://security.freebsd.org/advisor ies/FreeBSD-SA-07:03.ipv6.asc

4 Vol d'identifiants, et conséquences

Récemment, un certain nombre de cas de filoutage touchant le site de réseau social `MySpace` a été observé. Le vol d'identifiants d'applications non critiques telles que ceux de ce site `MySpace`, ou bien même `MSN`, etc. semble inoffensif mais peut avoir des conséquences importantes.

Le site `MySpace` offre à disposition de ses membres enregistrés un espace Web personnalisé. Mais il aurait pu s'agir en réalité de tout autre service en ligne nécessitant un accès contrôlé par identifiant et mot de passe. Ces derniers ne manipulant pas *a priori* de données trop sensibles (bancaires ou personnelles, même si...), les utilisateurs sont plus enclins à choisir des mots de passe faciles à retenir, et souvent très "faibles". Cela peut avoir plusieurs conséquences, pas toujours envisagées au moment du choix des identifiants.

En effet, l'identifiant volé peut ensuite servir de plusieurs manières malveillantes :

– réutilisation de ce même identifiant dans d'autres programmes plus sensibles : cela part du postulat que l'utilisateur a gardé le même mot de passe (ou très proche) pour d'autres services en ligne ;
– ingénierie sociale : la personne malveillante se fait passer pour l'utilisateur pour avoir des informations complémentaires le concernant ;
– envoi de spam via la liste de contacts disponible dans l'espace personnel ;
– etc.

Il est donc important de choisir des mots de passe forts pour tout type d'application, qu'elle soit critique ou qu'elle semble plus « *banale* ». La note d'information du CERTA CERTA-2005-INF-001 accessible à l'adresse

http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html rappelle les bonnes pratiques en ce qui concerne la construction d'un mot de passe fort.

Enfin, les réponses aux « questions secrètes », souvent utilisées pour récupérer un mot de passe oublié, sont un des maillons faibles. En effet, elles sont trop souvent un mot du dictionnaire, alors qu'elles sont aussi importantes que le mot de passe. Il est donc vivement recommandé de ne pas utiliser ce moyen ou de renseigner une réponse construite sur les mêmes règles que les mots de passe forts.

5 Vocabulaire informatique

Le vocabulaire informatique français vient de s'enrichir. En effet, la commission générale de terminologie et de néologie a publié une liste de termes informatiques nouveaux et de traductions. Cette liste peut être consultée à l'adresse :

http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=CTNX0710138K

Le CERTA pourrait prochainement utiliser ces nouveaux termes dans ses productions, comme, par exemple, le verbe « implémenter ».

6 Liens publicitaires sous Google

Le moteur de recherche Google affiche, en réponse à une requête, quelques liens publicitaires. Ces liens sont construits de la manière suivante : les sociétés achètent leur apparition dans Google pour certains mots-clés. Seulement Google a également une autre caractéristique lorsqu'il retourne une réponse : le passage de la souris sur un lien standard affiche dans la barre d'état l'adresse réticulaire qui va être ouverte, tandis que cette option n'existe pas pour les liens commerciaux.

Voici donc un scénario possible :

une société malveillante achète son affichage dans Google pour le mot clé VWXYZ. Toute personne voulant accéder au site www.VWXYZ.tld peut le faire en tapant naturellement VWXYZ dans son moteur de recherche. Le lien commercial peut présenter sous Google un bref résumé qui laisse à penser qu'il s'agit bien du site officiel www.VWXYZ.tld. On suppose donc ici que VWXYZ n'apparaît pas, car n'a pas acheté de liens commerciaux correspondant à son nom comme mot-clé dans Google. L'utilisateur qui approchera sa souris du lien commercial proposé ne verra pas apparaître la véritable `URL` dans sa barre d'état, ce qui ne l'aidera pas à avoir quelques soupçons. En revanche, lorsqu'il cliquera dessus, on peut imaginer qu'il soit redirigé vers :

- un site de filoutage (*phishing*) ressemblant fortement à www.VWXYZ.tld
- un site concurrent à VWXYZ, qui adaptera alors son offre
- un site contenant du code malveillant
- etc.

Tout cela, sans oublier également que la société malveillante touchera à chaque clic sur le lien commercial de l'argent, grâce à l'exploitation de la popularité de VWXYZ.

Ce scénario peut sembler invraisemblable, mais il a déjà été signalé dans quelques cas pour des sites étrangers.

Le CERTA recommande donc de vérifier occasionnellement les résultats retournés par les moteurs de recherche, afin de détecter tout abus similaire au cas précédemment exposé.

7 Nouveauté côté OpenBSD

Le projet OpenBSD a publié cette semaine la nouvelle version de son système d'exploitation : OpenBSD 4.1. Seules les deux dernières versions sont maintenues par les développeurs. OpenBSD 3.9 est donc maintenant osbolète. Il conviendra de procéder à une migration dans les plus brefs délais si vous disposez encore de ce système en production. Outre les habituelles corrections de bugs et de nouveau type de composants pris en compte comme les processeurs UltraSparc III, on notera des améliorations fonctionnelles dans le pare-feu PacketFilter :

- règles '*stateful*' par défaut (i.e. à état, dans le sens du protocole TCP) ;
- filtrage sur les drapeaux 'TCP' par défaut.

Ces modifications rendent ainsi l'écriture et la lisibilité des règles de filtrage plus facile.

Vous pouvez consulter la liste complète des changements apportés à la version 4.1 de OpenBSD à :
http://www.openbsd.org/41.html

8 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 26 avril et le 03 mai 2007.

9 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.f r/site/CERTA-2000-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

10 Rappel des avis émis

Durant la période du 20 au 27 avril 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-194 : Vulnérabilité dans QuickTime
- CERTA-2007-AVI-195 : Vulnérabilité des produits Symantec
- CERTA-2007-AVI-196 : Vulnérabilité de VMware workstation
- CERTA-2007-AVI-197 : Multiples vulnérabilités du logiciel Qemu
- CERTA-2007-AVI-198 : Multiples vulnérabilités dans Cisco ASA et PIX
- CERTA-2007-AVI-199 : Vulnérabilité de BIND

Pendant la même période, l'alerte et l'avis suivants ont été mis à jour :

- CERTA-2007-ALE-009-001 : Vulnérabilité dans BrightStor ARCServe Backup
  (ajout de la section Solution, des références au bulletin de sécurité Computer Associates et des entrées CVE.
- CERTA-2007-AVI-185-001 : Multiples vulnérabilités dans Apple MacOS X
  (ajout de la mise à jour du bulletin d'avril 2007, ainsi que la référence au CVE CVE-2007-0745)

11 Actions suggérées

11.1 Respecter la politique de sécurité

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

menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

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

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

11.2 Concevoir une architecture robuste

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

11.3 Appliquer les correctifs de sécurité

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

11.4 Utiliser un pare-feu

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

11.5 Analyser le réseau

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

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

11.6 Réagir aux incidents de sécurité

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

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

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

11.7 Former et sensibiliser les utilisateurs

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

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

12 Les bulletins d'actualité

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

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

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

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

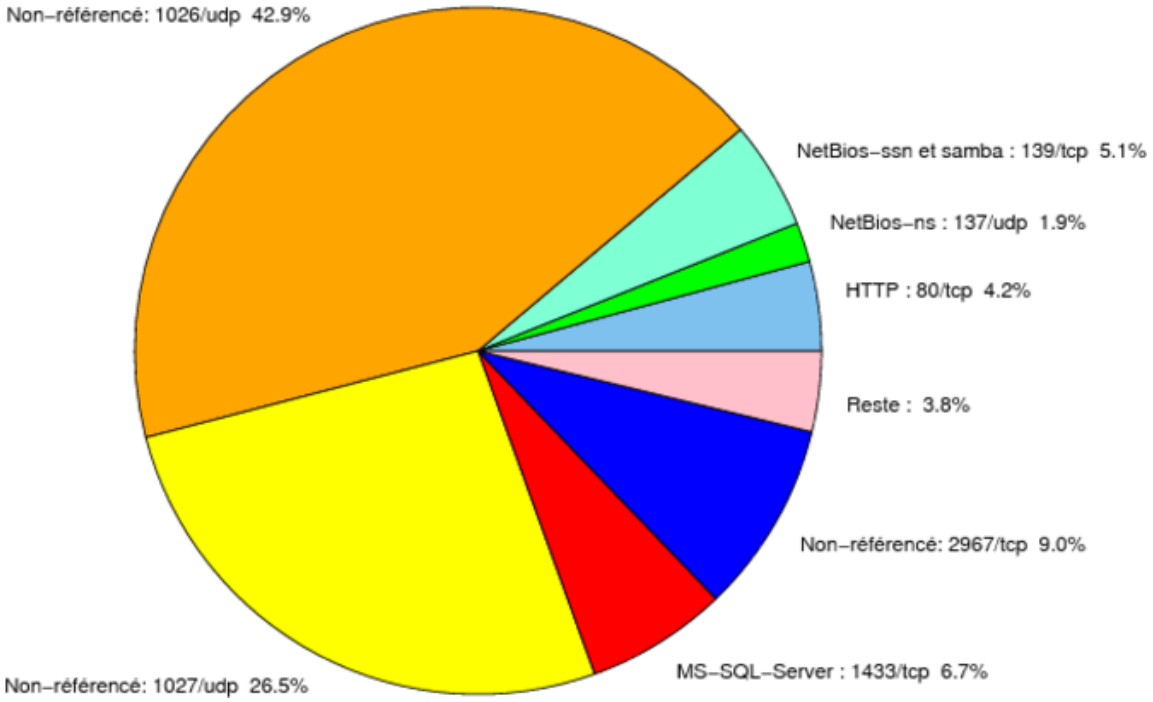

FIG. 1: Répartition relative des ports pour la semaine du 26.04.2007 au 03.05.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE

2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

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

port	pourcentage
1026/udp	42.91
1027/udp	26.46
2967/tcp	9.03
1433/tcp	6.65
139/tcp	5.08
80/tcp	4.19
137/udp	1.86
1434/udp	0.87
4899/tcp	0.76
1080/tcp	0.63
22/tcp	0.43
21/tcp	0.29
25/tcp	0.22
3128/tcp	0.21
443/tcp	0.08
15118/tcp	0.04
2100/tcp	0.03
9898/tcp	0.02
143/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

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

Gestion détaillée du document

04 mai 2007 version initiale.