Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 février 2008
N° CERTA-2008-ACT-005

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-05

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-2008-ACT-005`

Gestion du document

Référence	CERTA-2008-ACT-005
Titre	Bulletin d'actualité 2008-05
Date de la première version	01 février 2008
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-2008-ACT-005.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-2008-ACT-005/

1 Machines zombie et encapsulation de données

Il est fréquent lors d'un traitement d'incident qu'une machine compromise héberge un logiciel de type « bot » permettant à un individu malveillant de prendre son contrôle à distance. Le principe de base de ce « robot » est d'établir une connexion sortante (entendre du réseau local vers l'Internet) vers un serveur de contrôle appelé « C&C » pour *Command and Control* utilisée par le pirate pour donner des ordres à ses « zombies ».

De façon très classique, les canaux de communication entre le « C&C » et ses clients peuvent être les protocoles `IRC`, `HTTP` ou bien encore ceux de réseaux Pair-à-Pair. Cependant, ces flux sont assez facilement détectables pour peu que l'on ait mis en place une politique de filtrage du trafic sortant sur le pare-feu/routeur d'accès à l'Internet.

Pour un attaquant, une méthode originale évitant le filtrage ou la détection peut consister en la mise en œuvre d'un tunnel à l'intérieur d'une connexion TCP via un port autorisé à destination du `C&C`. Celui-ci pourra, par exemple, passer des ordres à son zombie à travers ce tunnel. Ainsi, on peut rencontrer des codes malveillants établissant une connexion sortante de type `SOCKS v5` modifiée vers la machine de contrôle sur un port autorisé (HTTP, SMTP, SSH, ...). L'originalité de la chose est que le robot (« bot ») n'ira pas chercher d'ordres par l'intermédiaire de ce canal de contrôle mais va plutôt se comporter en serveur mandataire (`proxy`) pour la machine de contrôle. On a donc une connexion inverse qui s'établie du `C&C` vers le client à l'intérieur du tunnel. le contrôleur devient client du *bot*.

Autrement dit, la machine compromise va établir une connexion TCP permanente entre elle et un serveur malveillant sur un port autorisé. Cette connexion est, en fait, un tunnel par lequel le serveur malveillant pourra relayer ses actions comme de l'envoi de pourriel. Le robot ne se comporte plus comme une machine malveillante allant chercher des ordres sur un « C&C » mais bien comme un proxy ouvert à une ou plusieurs machines. On pourra parler de mandataire inverse : *Reverse Proxy* ou même de *Reverse Tunnel Proxy* puisque le flux illégitime est encapsulé.

Recommandation :

Il est assez difficile de détecter ce type de techniques car d'un point de vue extérieur, tout se passe par le biais de flux légitimes. Cependant, le serveur mandataire `SOCKS` emploie souvent une signature particulière dans ses paquets. Il est en théorie possible en connaissant cette signature de configurer un `NIDS` (détecteur d'intrusion réseau) pour qu'il identifie cette signature. Cependant, il conviendra comme toujours avec un `IDS` d'être très vigilant avec la pertinence des règles de détection car si la signature change la sonde devient aveugle. Il est aussi possible de surveiller la durée des sessions TCP auprès du pare-feu : une session excessivement longue (une journée entière ou plus) peut être un indicateur important. Ces mandataires inverses servent souvent de relais de pourriel, il est donc également envisageable de contrôler les requêtes `DNS` de type `MX` trop fréquentes pour des domaines sortant de l'ordinaire.

2 Fin des versions 4.5.x de *Mambo*

L'équipe de développement du gestionnaire de contenu Mambo a annoncé, sur le forum de son site Web, la fin des versions 4.5.x de leur produit. Les développeurs se consacrent désormais à la version 4.6, à la future version 4.7 (qui devrait prochainement être publiée) et envisagent l'implémentation d'une version 5.

La branche de développement 4.5 se termine donc avec la version 4.5.6, appelée également *sunset* (crépuscule).

Tous les utilisateurs de Mambo 4.5.x sont encouragés à installer la version 4.5.6 et à réfléchir à une migration vers la branche 4.6 ou 4.7. Il est à noter que les versions 4.6.x existent en téléchargement depuis décembre 2006.

Documentation

- Annonce sur le site de Mambo :
  http://forum.mambo-foundation.org/showthread.php?t=9842

3 Les cadres numériques après Noël

La période de Noël a vu l'essor des cadres photos numériques. Cet appareil permet de se déplacer facilement avec des photos numériques (voire aussi d'autres contenus multimédia), en le connectant, par exemple, sur une machine d'un réseau domestique puis d'un réseau d'entreprise.

Le problème suivant se pose : les cadres numériques USB sont des périphériques USB comme les autres, souffrant des mêmes faiblesses. Le sujet a déjà été traité dans la note d'information CERTA-2006-INF-006 (*Risques associés aux clés USB*) et dans le bulletin d'actualité CERTA-2007-ACT-025 (*Les cadres pour photos numériques*).

http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/

L'actualité de la semaine rapportant le cas d'un programme malveillant présent dans des cadres numériques neufs, le CERTA rappelle qu'il faut faire attention à ces périphériques, comme à tous les médias amovibles. Même si l'appareil est « neuf », il est nécessaire de prendre des précautions. Pour cela, il est important d'appliquer la politique de sécurité en vigueur (qui peut inclure des mesures de décontamination de tout nouveau matériel à connecter).

Documentation

- Note d'information CERTA-2006-INF-006 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/
- Bulletin d'actualité CERTA-2007-ACT-025 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-025/

4 Bulletin MS08-001 et protocole *IGMPv3*

4.1 Retour sur le bulletin MS08-001

Le CERTA a publié le 09 janvier 2008 l'avis CERTA-2008-AVI-009 relatif au bulletin de sécurité MS08-001 de Microsoft.

Ce dernier concerne des vulnérabilités dans la mise en oeuvre de certains protocoles dans `tcpip.sys` sous Windows, et notamment ceux utilisés pour la diffusion de données en groupes, ou *multicast*.

Les protocoles mis en cause dans la vulnérabilité de référence CVE-2007-0069 sont `IGMPv3` (*Internet Group Management Protocol*) sous IPv4, et `MLDv2` (*Multicast Listener Discovery*) sous IPv6. Ces protocoles sont interprétés par défaut dans les systèmes d'exploitation Windows XP, Windows Vista, Windows Home Server et Small Business Server.

Windows Server 2003 n'utilise pas, par défaut et selon Microsoft, de services s'appuyant sur le *multicast*. Il n'est donc pas affecté par cette vulnérabilité, car les paquets IGMP reçus sont rejetés. Néanmoins, si d'autres applications ont été installées, ou des services comme `UPnP`, la vulnérabilité sera bien présente et exploitable.

Microsoft a publié un article fournissant davantage de détails : une machine fonctionnant sous Windows Server 2003 peut émettre des trames à destination du groupe *multicast* associé à l'adresse `224.0.0.1`, mais elle ignore les requêtes à destination de cette adresse. Pour vérifier si le serveur est associé ou non à d'autres groupes, il est possible de contrôler que seule la ligne suivante apparaît en tapant dans un terminal Windows la commande (un compte « invité » est suffisant) :

```
C:\>netsh int ip show joins

Adr d'interface    Groupe de multidiffusion
---------------    ------------------------
W.X.Y.Z            224.0.0.1
```

Comme nous venons de le signaler, Microsoft annonce donc qu'une installation Windows Server 2003 par défaut n'est pas vulnérable. Il faut cependant bien comprendre ici que cela ne signifie pas que l'interprétation de trames IGMP par le système ne s'effectue pas. Il y a donc une ambiguïté dans la formulation actuelle de l'article publié le 10 janvier 2008 sur le bloc-notes SVRD de Microsoft :

```
"Though the host (Windows Server 2003) would receive the
unicast IGMP packet, valid multicast address needs to be
contained in IGMP query payload so the packet would be ignored."
```

4.2 Le protocole IGMPv3

Le *multicast*, ou la diffusion multi-groupes, permet de communiquer simultanément avec un ensemble de machines, identifiées par une adresse de groupe spécifique. Cette technique est intéressante pour envoyer des flux vidéo (*streaming*), comme les diffusions de chaînes de télévision ou les visio-conférences. Elle peut aussi être employée pour effectuer des mises à jour ou des configurations collectives. D'autres protocoles s'appuient sur cette technique pour fonctionner, comme l'architecture `UPnP` récemment présentée dans le bulletin d'actualité CERTA-2008-ACT-003.

`IGMP` n'est pas un protocole des plus récents, et a fait l'objet de plusieurs standards RFC, dont RFC 1112 (1989) et RFC 2236 (1997). La version actuelle est la 3, définie dans le RFC 3376.

Ce protocole permet de gérer les déclarations d'appartenance à un (ou plusieurs) groupe auprès de routeurs *multicast*. L'annonce des appartenances se fait soit par la machine même, soit après une sollicitation, envoyée par exemple par un routeur à proximité.

`IGMP` est encapsulé dans un en-tête IP indiquant l'identifiant protocolaire `0x02`. L'en-tête `IP` doit également contenir une option *Router Alert*, afin que le paquet soit convenablement manipulé par le routeur. Le RFC 3376 mentionne également que le `TTL` (*Time-to-Live*) dans l'en-tête `IP` des trames `IGMP` doit avoir la valeur 1. Cette recommandation n'est pas nécessairement respectée par les routeurs `multicast`, selon leur configuration.

L'en-tête d'une trame `IGMPv3` n'est pas d'une grande complexité, et dépend du type. On distingue :

- `0x11` : les requêtes d'appartenance (*Membership Query*) ;
- `0x12` : les rapports d'appartenance pour IGMP version 1 (*Membership Report*) ;
- `0x16` : les rapports d'appartenance pour IGMP version 2 ;
- `0x22` : les rapports d'appartenance pour IGMP version 3 ;

– `0x17` : le signalement du départ du groupe (*Leave Group*).

Dans le cas des requêtes d'appartenance sous `IGMPv3`, les champs sont :

– `Max Resp Code` : il s'agit de la durée maximale attendue avant d'émettre un rapport ;
– `Checksum` : pour vérifier si des erreurs binaires existent dans l'en-tête ;
– `Group Address` : ce champ peut être vide, ou préciser l'adresse IP *multicast* d'appartenance interrogée ;
– `Resv` : réservé. Pas d'usage clair pour le moment ;
– `S Flag` : le noeud destinataire prend compte de cette valeur pour supprimer ou non sa mise à jour de minuteur ;
– `QRV et QQIC` : il s'agit des caractéristiques propres que l'émetteur de la requête veut transmettre ;
– `Sources Number` : cette valeur indique le nombre d'adresses sources présentes dans la requête (cf. champ suivant). Elle dépend donc de l'objectif de la requête, mais aussi, plus matériellement, de la taille maximale autorisée pour les trames dans le réseau (`MTU`) ;
– `Source Adresses` : un ensemble d'adresses IP *unicast*, dont le nombre doit théoriquement être celui indiqué par le champ précédent.

Les requêtes d'appartenance peuvent être adressées, toujours selon le RFC, aux adresses *multicast* d'intérêt, celle générique étant `224.0.0.1`. En revanche, il est aussi écrit que toute machine doit accepter et interpréter une requête IGMPv3 adressée à toute adresse assignée à l'interface réseau, en particulier *unicast* et *multicast* :

```
RFC 3376, Section 4.1.12 :

"*However*, a system MUST accept and process any Query whose
IP destination Address field contains *any* of the addresses
(unicast or multicast) assigned to the interface on which the
Query arrives".
```

Aucune recommandation ne concerne l'adresse IP source de la requête.

4.3 L'actualité

La vulnérabilité concerne la gestion de ces requêtes reçues par une machine, et le stockage temporaire de ces informations dans une table. Elle dépend donc aussi d'un contexte temporaire, car la table se vide régulièrement en fonction de la valeur `Max Resp Code` des requêtes.

Un code d'exploitation a été publié cette semaine dans un outil de sécurité. Il fonctionnerait, selon les auteurs, sur des versions Windows XP SP2, avec le pare-feu natif activé.

Le bon fonctionnement de ce code malveillant permet d'acquérir les droits du noyau (SYSTEM) à distance, et donc de prendre le contrôle total de la machine.

Microsoft détaillait dans un article du 08 janvier 2008 la difficulté d'exploitation de cette vulnérabilité. En effet, elle nécessite un envoi important de trames pour remplir la fameuse table, et des conditions propices (des valeurs aléatoires peuvent intervenir pour provoquer le nettoyage inopiné de la table). Le code de démonstration diffusé sur l'Internet montre lui que 180 paquets émis peuvent suffire pour faire aboutir l'attaque.

4.4 Exploitation de la vulnérabilité

Il existe une vulnérabilité mentionnée dans MS08-001. A la date de rédaction de cet article, du code d'exploitation a été rendu public. Il semble fonctionner sur des systèmes Windows XP SP2 (anglais installé par défaut) avec le pare-feu activé. La vulnérabilité concerne aussi les autres systèmes d'exploitation Microsoft. Windows Server 2003 ne semble pas moins vulnérable. Vista a une pile protocolaire qui a été réécrite par les développeurs de Microsoft. Elle souffre cependant de la même vulnérabilité, et des codes d'exploitation visant ce système sont envisageables dans les prochains mois.

La vulnérabilité existe également pour le protocole `MLDv2` sous IPv6 qui met en oeuvre les mêmes fonctionnalités que `IGMPv3`.

Une propagation massive d'un code exploitant cette vulnérabilité semble peu probable, étant données les restrictions et les contraintes du fonctionnement *multicast*. Cependant, des configurations trop laxistes au niveau des routeurs et des pare-feux périphériques peuvent favoriser l'exploitation de cette vulnérabilité dans des réseaux locaux.

4.5 Recommandations

Compte tenu des paragraphes précédents, le CERTA invite ses correspondants à :

- mettre à jour leur système d'exploitation ;
- surveiller le trafic réseau, et notamment le volume de trafic `IGMP` ;
- désactiver si cela n'est pas nécessaire ces protocoles dans les clés de registre de Windows. Le bulletin MS08-001 donne les indications pour effectuer cette opération sous XP et Vista ;
- vérifier que la politique de filtrage est correcte, en particulier vis-à-vis des protocoles *multicast*. Les pare-feux périphériques devraient bloquer par défaut tous les flux entrants et sortants qui ne sont pas nécessaires. Certains pare-feux permettent également de limiter le volume de trames d'un protocole donné dans une fenêtre de temps.

4.6 Documentation associée

- RFC 1112, "Host Extensions for IP Multicasting", août 1989 :
  http://tools.ietf.org/rfc/rfc1112.txt
- RFC 2236, "Internet Group Management Protocol, Version 2", novembre 1997 :
  http://tools.ietf.org/rfc/rfc2236.txt
- RFC 3228, "IANA Considerations for IPv4 Internet Group Management Protocol (IGMP), février 2002 :
  http://tools.ietf.org/rfc/rfc3228.txt
- RFC 3376, "Internet Group Management Protocol, Version 3", octobre 2002 :
  http://tools.ietf.org/rfc/rfc3376.txt
- RFC 4607, "Source-Specific Multicast for IP", août 2006 :
  http://tools.ietf.org/rfc/rfc4607.txt
- Article du blog SVRD de Microsoft, "MS08-001 - The case of the Moderate, Important, and Critical network vulnerabilities", publié le 08 janvier 2008 :
  http://blogs.technet.com/swi/archive/2008/01/08/ms08-001-the-case-of-the-moderate-important-and-critical-network-vulnerabilities.aspx
- Article du blog SVRD de Microsoft, " MS08-001(part 3) - The case of the IGMP network critical", publié le 08 janvier 2008 :
  http://blogs.technet.com/swi/archive/2008/01/08/ms08-001-part-3-the-case-of-the-igmp-network-critical.aspx
- Article du blog SVRD de Microsoft, "MS08-001 - The case of the missing Windows Server 2003 attack vector", publié le 10 janvier 2008 :
  http://blogs.technet.com/swi/archive/2008/01/MS08_2D00_001-_2D00_-The-case-of-the-missing-Windows-Server-2003-attack-vector.aspx
- Document Cisco, "Source Specific Multicast with IGMPv3, IGMP v3lite, and URD" :
  http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dtssm5t.pdf

5 Les codes malveillants sous Apple Mac OS X

5.1 L'actualité de la semaine

Les utilisateurs du système d'exploitation Microsoft Windows sont généralement conscients des dangers des codes malveillants, qu'ils se nomment virus, vers ou enregistreurs de frappes clavier. Ces types de codes peuvent cependant exister sur tout système d'exploitation : Apple Mac OS X n'échappe pas à la règle. Les utilisateurs du système d'exploitation de la marque à la pomme ne doivent pas oublier ces codes malveillants, ou se croire naturellement immunisés. Il est important d'appliquer les mêmes principes de configuration et de sécurité quel que soit le système d'exploitation. Il est préférable de ne pas pratiquer une « monoculture » dans un réseau mais encore faut-il le faire de façon réfléchie.

Des articles ont fait état cette semaine d'un code malveillant capable d'enregistrer les frappes clavier. Ce logiciel a été créé pour fonctionner sur Apple Mac OS X et se présente sous la forme d'un paquet instalable (`pkg`) qui nécessite des droits d'administration. Il ne peut donc, en théorie, pas compromettre une machine à l'insu de l'utilisateur. Ce dernier est le principal acteur de la compromission : il doit, à un moment donné, décider d'installer un tel logiciel.

5.2 Les recommandations

Le CERTA tient donc à rappeler les règles d'usage en la matière :

- Ne pas naviguer sur l'Internet ou exécuter des applications avec des droits d'administration, à moins que ceux-ci ne soient nécessaires pendant une durée déterminée. Un article du bulletin d'actualité CERTA-2007-ACT-048 sur la gestion des comptes administrateur d'Apple Mac OS X rappelle les règles de bonne utilisation de ce type de compte ;
- activer et configurer le pare-feu afin de filtrer les connexions entrantes et sortantes ;
- désactiver les services inutiles. Les services comme `bonjour` ou `mDNS` sont-ils indispensables au bon fonctionnement de la machine ?
- désactiver les interfaces inutiles (bluetooth, infrarouge, WiFi, ethernet, etc.) et configurer avec soin celles qui le sont ;
- ne pas installer de logiciels et applications qui ne sont pas de confiance, sans être sûr de leur intégrité et de l'absence de volonté malveillante.

Documentation

- Bulletin d'actualité CERTA-2007-ACT-048 du 30 novembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-048.pdf

6 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 24 et le 31 janvier 2008.

7 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/

8 Rappel des avis émis

Dans la période du 25 janvier au 01 février 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-036 : Vulnérabilité dans HP-UX ARPA
- CERTA-2008-AVI-037 : Vulnérabilités dans des produits Cisco
- CERTA-2008-AVI-038 : Multiples vulnérabilités dans IBM AIX
- CERTA-2008-AVI-039 : Vulnérabilité dans ISC BIND
- CERTA-2008-AVI-040 : Multiples vulnérabilités dans IBM Informix

Pendant la même période, l'avis suivant a été mis à jour :

- CERTA-2008-AVI-029-001 : Mutiples vulnérabilités des produits Oracle
  (Modification de l'URL d'Oracle et des systèmes affectés)

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'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.

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 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.

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.

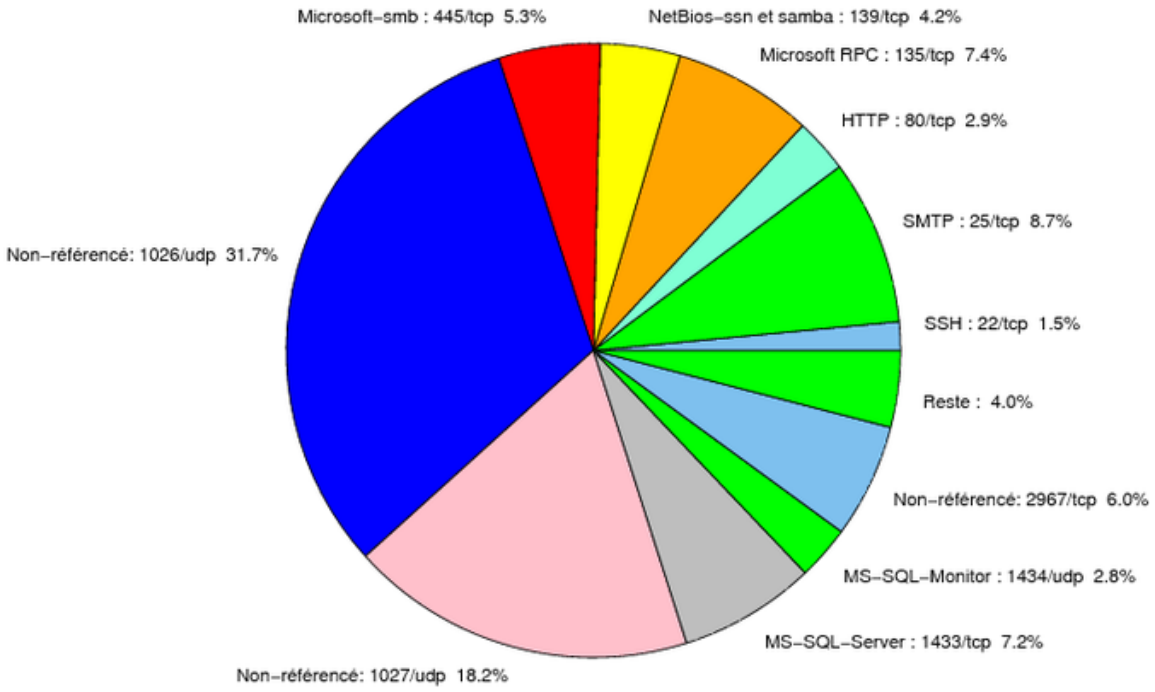

FIG. 1: Répartition relative des ports pour la semaine du 24.01.2008 au 31.01.2008

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/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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	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
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	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
445	TCP	Microsoft-smb	–	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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	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
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
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/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
80/tcp	228.57
1026/udp	31.7
1027/udp	18.22
25/tcp	8.7
135/tcp	7.39
1433/tcp	7.2
2967/tcp	6.01
445/tcp	5.34
139/tcp	4.19
1434/udp	2.83
22/tcp	1.5
137/udp	0.97
4899/tcp	0.71
3128/tcp	0.66
3306/tcp	0.45
1080/tcp	0.42
21/tcp	0.31
23/tcp	0.14
143/tcp	0.11
2100/tcp	0.09
42/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

01 février 2008 version initiale.