Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 octobre 2007
N° CERTA-2007-ACT-042

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-42

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-042

Gestion du document

Référence	CERTA-2007-ACT-042
Titre	Bulletin d'actualité 2007-42
Date de la première version	19 octobre 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-042.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-042/

1 Serveurs Web et fichiers de mots de passe

Lors du traitement d'un incident récent, le CERTA a découvert un fichier contenant des mots de passe disponibles depuis l'Internet. Les mots de passe de ce fichier n'étaient pas « en clair ». Toutefois, l'utilisation d'un outil dédié aux tests de robustesse des mots de passe a permis de trouver le texte clair de ces derniers.

La découverte de fichiers de mots de passe sur les serveurs Web est relativement aisée. Généralement, l'utilisation d'un moteur de recherche peut suffire. L'accès à de tels fichiers peut mener à la compromission des mots de passe, qui peuvent ensuite être utilisés pour accéder à des pages à lecture restreinte, ou encore pour se connecter à certains services de la même machine (parfois du même réseau). Dans certains cas, les mots de passe apparaissent en clair dans les fichiers.

Le CERTA recommande :

- de ne jamais stocker de mots de passe en clair dans des fichiers ;
- d'éprouver la robustesse de ces mots de passe à l'aide d'outils dédiés et hors-ligne ;
- de restreindre l'accès à certains fichiers qui, par nécessité, doivent se trouver sur des serveurs.
- Note d'information CERTA-2005-INF-001, « Les mots de passe » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/

2 Les listes noires de messagerie

Cette semaine, le CERTA a traité un incident relatif à la messagerie. Suite à une modification de son architecture de messagerie, une administration s'est vue rejeter tous ses courriers électroniques par certains destinataires. Suite à l'analyse des message de retour, les responsables de ce serveur de messagerie ont constaté qu'ils avaient été mis sur des listes noires (*blacklist*).

Il existe de plus en plus de listes noires sur l'Internet. Des sites permettent de vérifier la présence d'une adresse IP dans celles-ci. C'est le cas par exemple de `robtex` qui vérifie dans plus d'une centaine de listes noires :

http://www.robtex.com

La plupart de ces listes tentent d'expliquer de manière plus ou moins claire leurs critères de bannissement et certaines proposent une procédure de retrait d'une adresse IP. Les listes noires se basant sur les adresses IP émettrices, il est facile pour des virus et autres émetteurs de courriers non sollicités de les contourner en utilisant une nouvelle adresse IP ou en essayant d'infecter une nouvelle machine.

2.1 Une mauvaise configuration

Dans le cadre de cet incident, la présence de l'adresse IP dans certaines listes noires s'explique par une mauvaise configuration de la nouvelle architecture de messagerie. En effet, lors d'une connexion `SMTP`, le nouveau serveur de messagerie ne se présentait pas correctement :

- pendant une connexion SMTP, la manière correcte de se présenter est :

  ```
  EHLO <nom de domaine de messagerie ou adresse IP>
  ```

- la mauvaise manière (laissée dans une configuration par défaut) est :

  ```
  EHLO
  ```

Il est assez facile de contrôler la bonne présentation d'un serveur en regardant l'en-tête d'un courrier reçu par celui-ci :

```
Received: from <nom de domaine ou adresse IP présenté par le serveur>
(<nom résolu par le serveur recevant la connexion> [ADRESSE IP Réelle])
```

Exemple :

```
Received: from mail.certa.ssi.gouv.fr (mail.certa.ssi.gouv.fr [213.56.176.1])
```

2.2 Une réaction hâtive

Le second problème intervenu dans cet incident est qu'avant de corriger totalement leur problème de configuration, les administrateurs ont tenté de réaliser les procédures de retraits des listes noires, quand cela était possible. Mais, afin de limiter les abus, certaines listes noires n'autorisent qu'une ou deux tentatives de retrait par jour. Le CERTA a pu débloquer la situation après s'être assuré avec les administrateurs de la bonne configuration du serveur de messagerie.

Il faut noter que des codes malveillants vérifiant la présence d'une adresse IP dans les listes noires peuvent tenter d'épuiser le nombre de possibilités de retraits qu'ont les administrateurs. Il devient alors impossible de se « désinscrire » des listes.

2.3 Ce qu'il faut en retenir

La mise en production d'une nouvelle application nécessite une vérification approfondie de son fonctionnement : tests de non-régression, maquettes, ...

Le CERTA constate que de plus en plus de listes « noires », « grises » ou « blanches » apparaissent sur l'Internet. Ces listes utilisent des critères parfois arbitraires et il est souvent très difficile de comprendre les raisons exactes de leur choix. D'autre listes se basent sur des listes tierces et sont incapables de supprimer une adresse listée. Ces listes doivent être utilisées avec beaucoup de précaution et il est impératif de garder la possibilité de contourner une mise en liste noire abusive.

Documentation associée

- Bulletin d'actualité CERTA-2007-ACT-001, « Utilisation des listes noires pour lutter contre les pourriels »: http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-001.pdf

- Bulletin d'actualité CERTA-2007-ACT-004, « La liste noire maintenue par Google » : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-004.pdf
- Bulletin d'actualité CERTA-2007-ACT-037, « Les listes blanches » : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-037.pdf
- Tester la présence d'une adresse IP dans une centaine de listes noires : http://www.robtex.com/rbl/

3 Les services de redirection gratuits par Internet

3.1 Incident traité cette semaine

Le CERTA a traité cette semaine le cas d'une défiguration de site. Il apparaît, après analyse, que le serveur hébergeant le site n'a pas été compromis. En revanche, la défiguration est due à un phénomène bien particulier : la page se visite par le biais d'une adresse réticulaire (URL), incluant un nom de domaine particulier, géré par une société tierce. Celle-ci doit en principe rediriger toute requête vers le site légitime. Dans le cas présent, le système de redirection de cette société tierce a été détourné vers un site malveillant.

Les détails de cette méthode, et les problématiques qu'elles comportent sont décrits ci-dessous.

3.2 Un service de redirection

Il existe sur Internet la possibilité d'acquérir gratuitement des noms de domaine. Ces noms peuvent être de la forme [monSite].[LESERVICE].[TLD] avec :

monSite qui est le nom désiré pour le site administré.

LESERVICE qui est tout ou partie du nom du service qui offre gracieusement la possibilité de créer son nom de domaine (presque) sur mesure ;

TLD qui correspond au `Top Level Domain`, par exemple `.fr`, `.org` ou `.com`.

Ces extensions permettent d'avoir une ou plusieurs adresses URL pointant sur un seul et même site A :

```
http://[monSite1].[LESERVICE].[TLD]/index.html => page index.html de site A
http://[monSite2].[LESERVICE].[TLD]/index.html => page index.html de site A
```

Seulement il ne s'agit pas d'entrées dans un serveur DNS. Il s'agit d'une redirection de pages. Les différentes interactions sont donc :

1. l'utilisateur navigue et cherche à se rendre sur [monSite1].[LESERVICE].[TLD]/index.html ;
2. une requête DNS lui indique que ce site se trouve sur une machine du service [LESERVICE].[TLD] ;
3. le navigateur cherche alors à récupérer la page d'accueil sur cette machine ;
4. cette dernière redirige par du code HTML l'utilisateur vers le vrai site où se trouve la page index.html attendue.

Le CERTA tient à attirer l'attention sur les risques que peuvent engendrer l'utilisation de tels services.

Dans le cas de l'incident traité, les machines physiques ne sont pas sous la maîtrise des responsables du service de redirection. Ils utilisent des machines virtuelles pour y mettre les pages de redirections, et ces machines sont installées sur un poste hôte maintenu par une autre société. Ces serveurs peuvent être compromis et toute modification de la page de redirection donnera l'impression que c'est le site original qui a été compromis.

De plus ces serveurs peuvent héberger plusieurs redirections de sites et donc poser des problèmes d'image lorsqu'une même adresse IP est associée à des sites peu recommandables. Les redirections se font de manière générale via une redirection de cadres (*frame*). Les autres cadres de la page permettent l'intégration de publicité, contre partie de la gratuité.

La redirection par cadre peut prendre la forme suivante :

```
<_html>
 <_head>
  <_title>Titre de la page</title>
 <_/head>
  <_frameset rows="20,*" frameborder="NO" border="0" framespacing="0">
  <_frame name="pub" src="/publicite.html" noresize scrolling="no">
  <_frame name="principale" src="http://adresse_du_site_A/index.html">
```

```
 <_/frameset>
<_/html>
```

Il faut également avoir conscience que toute visite d'un internaute vers le site A passe au préalable par une requête vers le site de [LESERVICE].[TLD] (étape 3). Cette requête est journalisée.

La société tierce peut donc savoir :

- quels internautes se rendent sur le site A ;
- à quelle heure ils s'y rendent ;
- depuis quelle adresse IP ils s'y rendent ;
- le navigateur utilisé par l'internaute ;
- depuis quel site il se rend sur le site A ;
- etc.

Ce sont donc des données collectées à l'insu de l'utilisateur, et ce dernier n'a pas moyen de savoir qu'elles seront les exploitations faites de ces dernières.

Toutes ces raisons amènent le CERTA à vivement déconseiller de tels services. Ils peuvent provoquer la méfiance des internautes, et ils apportent dans tous les cas une surface supplémentaire d'attaques pour défigurer des sites.

4 Mise à jour de la liste des logiciels obsolètes

La liste des logiciels obsolètes maintenue dans la note d'information CERTA-2005-INF-003 a été mise à jour pour ajouter les deux sections suivantes :

- les versions de php supportées : la version 4 sera obsolète à la fin de l'année.
- les versions de Microsoft Office encore supportées : 2000, XP, 2003 et 2007.

Le document est disponible à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/

5 Deux formats d'actualité

5.1 Les documents au format PDF

Le CERTA a publié le 10 octobre une alerte concernant la vulnérabilité dans le traitement des URI sous Windows. La présence d'Internet Explorer 7 est un pré-requis pour l'exploitation de cette vulnérabilité, qui peut alors être provoquée par plusieurs applications tierces.

L'une d'elles est l'interprétation de fichiers `PDF` (*Portable Document Format*) par des lecteurs comme Adobe Acrobat Reader. Des preuves de faisabilité ont été assez largement publiées sur l'Internet, et leur modification n'est pas très complexe. Des commandes peuvent ainsi être exécutées à l'insu de l'utilisateur, au moment de l'ouverture d'un document spécialement construit.

Dans l'attente d'un correctif par Microsoft, le CERTA recommande la plus grande méfiance vis-à-vis de ces documents. Ils peuvent se caractériser par l'existence de la chaîne de caractères `mailto:%` dans le code source. Adobe a également publié dans son avis de sécurité du 05 octobre 2007 quelques mesures préventives :
http://www.adobe.com/support/security/advisories/apsa07-04.html

- Alerte CERTA-2007-ALE-015, « Vulnérabilité dans le traitement des URI sous Windows » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-015/

5.2 Les documents au format DOC

Le CERTA a publié le 10 octobre 2007 l'avis de sécurité CERTA-2007-AVI-430. Celui-ci concerne le logiciel bureautique Microsoft Word, et présente le correctif de Microsoft décrit dans son bulletin MS07-060.

Le CERTA a, depuis, été informé de l'existence de documents Word tentant d'exploiter la vulnérabilité décrite (CVE-2007-3899). *Symantec* a par ailleurs signalé le 14 octobre 2007 l'existence d'un Cheval de Troie similaire, utilisant cette vulnérabilité, et prénommé `Trojan.Mdropper.Z`. Il se présente actuellement sous la forme d'un document `.doc` intitulé `hope see again.doc`. Il tente alors d'exécuter du code sur la machine ayant une version vulnérable, et cherche ensuite à correspondre en TCP via le port 80 vers un site distant.

Il est donc important de vérifier que les versions d'Office sont à jour, et le CERTA recommande également la plus grande méfiance à l'ouverture de tels documents. Il est important de ne pas ouvrir de fichiers dont la source n'est pas de confiance, notamment en pièce jointe d'un courriel.

6 Evénements sous Windows

Les événements sous Microsoft Windows sont souvent délaissés par les administrateurs car la documentation les concernant peut être difficile à trouver ; de plus, à chaque nouvelle version de Windows des changements sont apportés par Microsoft. Puisqu'il est impossible d'être exhaustif et de détailler chaque événement selon le système utilisé, cet article a pour but de fournir au lecteur quelques pointeurs pour obtenir des documentations officielles concernant les événements.

En ce qui concerne Windows 2000, un article en deux parties de la base de connaissances KB299475 de Microsoft liste et détaille les événements de sécurité du système d'exploitation.

Une documentation concernant les événements de sécurité dans Windows Server 2003 est également disponible en ligne sur le site de Microsoft, dans le chapitre 4 du guide de sécurité (*Windows Server 2003 Security Guide*). Les événements sont ici groupés par catégorie (connexions au système, gestion des utilisateurs, utilisation de privilèges...) ce qui peut aider pour le choix de la politique d'audit, mais sont peu détaillés.

Le site *Technet Events & Errors Message Center* permet d'obtenir plus de détails concernant les événements particuliers que l'on spécifie via un moteur de recherche. Seuls les systèmes Windows 2000 et 2003 semblent supportés.

Enfin, concernant Windows Vista et le futur Windows Server 2008, aucune documentation officielle de la part de l'éditeur n'a été publiée pour le moment, mais un article devrait paraître dans la base de connaissances.

Toutefois, l'utilitaire en ligne de commande `wevtutil` (*Windows Events Command Line Utility*), qui sert à gérer les événements sur ces systèmes, peut donner beaucoup d'informations sur ceux-ci. Ainsi, la commande `wevtutil gp Microsoft-Windows-Security-Auditing /ge /gm:true /f:xml` listera au format XML tous les événements disponibles pour la catégorie `Microsoft-Windows-Security-Auditing`. Toutes les catégories sont visibles avec la commande `wevtutil el`. Il est ainsi possible d'obtenir un descriptif de tous les événements du système.

6.1 Documentation

- Base de connaissances Microsoft KB 299475 - événements de sécurité sous Windows 2000
  http://support.microsoft.com/kb/299475
- *Windows Server 2003 Security Guide* - Chapitre 4
  http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/s3sgch04.mspx#EKH
- *Technet Events & Errors Message Center* - Centre technet des messages d'erreur et événements
  http://www.microsoft.com/technet/support/ee/ee_advanced.aspx
- Bloc-notes *Windows Security Logging and Other Esoterica*
  http://blogs.msdn.com/ericfitz/default.mspx
- Bulletin d'actualité CERTA-2007-ACT-017, « Les événements sous Microsoft Vista » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-017.pdf
- Bulletin d'actualité CERTA-2007-ACT-022, « Les événements Windows » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-022.pdf

7 Les canaux de communication et les réseaux de machines zombies

7.1 Des exemples de canaux de communication

Des machines compromises peuvent être gardées sous contrôle, afin de créer un réseau de zombies. Ce dernier peut alors être utilisé à différentes fins, comme l'envoi de courriers non sollicités ou le lancement d'attaques distribuées en déni de service. Il y a *a fortiori* un canal de communication, qui permet aux personnes malveillantes, directement ou pas, de commander ce réseau, afin de lui signaler les actions à entreprendre.

Le plus populaire des canaux de communication pour ces réseaux est IRC. Ce dernier est assez facilement identifiable par une analyse réseau. Sa mise en œuvre se fait fréquemment avec l'utilisation du port TCP 6667, même si tout autre port est en théorie possible. Le client peut utiliser un *proxy*, et le serveur peut être configuré pour écouter sur le port de son choix. Une première surveillance au niveau du pare-feu périmétrique de toute tentative de connexion utilisant ces ports en particulier est donc un signe d'utilisation d'IRC. L'analyse de la machine infirme ou confirme ensuite que ce canal de communication est utilisé à des fins malveillantes.

Le CERTA a mentionné dans différents bulletins d'actualité cette année, notamment CERTA-2007-ACT-034, l'existence du ver Storm Worm. Celui-ci, aussi nommé par certains Zhelatin, a la particularité d'utiliser le réseau

pair-à-pair Overnet pour communiquer, et prendre connaissance des commandes à exécuter. Les échanges se font de la même manière qu'un utilisateur normal, avec les différents types de requêtes :

- `Publicize` pour annoncer aux voisins son existence, et identifier les ressources disponible (UDP) ;
- `Connect` pour commencer des transferts de données (TCP) ;
- `Search` pour chercher des ressources particulières parmi les nœuds voisins.

Il ne s'agit pas ici de décrire le fonctionnement de Storm, mais de signaler que certains comportements dans un réseau local de taille modeste peuvent mettre en évidence son existence. Outre les différents échanges mentionnés précédemment, une simple augmentation du trafic UDP peut déjà éveiller les premiers soupçons, ainsi que l'apparition de certains éléments dans les en-têtes TCP ou UDP (identifiant de protocoles, ports de destination, etc.).

7.2 BlackEnergy

Récemment, une étude est apparue et a décrit en détail un autre type de réseau de machines zombies. Ce réseau se nomme `BlackEnergy` et a pour principale motivation les attaques en déni de service, du moins à la date de l'analyse effectuée.

- J. Nazario, Arbor Networks, "BlackEnergy DDoS Bot Analysis", octobre 2007 :
  http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf
  http://asert.arbornetworks.com/2007/10/blackenergy-ddoas-bot-analysis-available/

Ce réseau en lui-même consiste selon l'auteur en peu de machines. Son activité est pour le moment restreinte à des machines localisées en Asie et en Europe de l'Est. Ce qui est intéressant dans `BlackEnergy`, en revanche, c'est son mode de communication qui s'appuie sur des requêtes HTTP valides. Des serveurs Web sont compromis et l'utilisation de PHP et MySQL de ceux-ci est détournée. Les machines compromises cherchent alors leurs instructions sur ces serveurs par des requêtes HTTP en mode POST. Dans l'exemple décrit par l'article, il s'agit d'une requête de la forme :

```
POST /dot/stat.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
.NET CLR 1.1.4322)
Host: **********
Content-Length: 31
Cache-Control: no-cache
id=xxxxxxxxxxxxxxx&build_id=yyyyy
```

Il inclut dans l'en-tête son identifiant.

Le serveur lui répond en retour :

```
HTTP/1.1 200 OK
Date: Tue, XX Sep 2007 08:30:13 GMT
Server: Apache/2.0.59 (Unix) FrontPage/5.0.2.2635 PHP/5.2.3
mod_ssl/2.0.59 OpenSSL/0.9.7e-p1
X-Powered-By: PHP/5.2.3
Content-Length: 80
Connection: close
Content-Type: text/html
MTA7MjAwMDsxMDswOzA7MzA7MTAwOzM7MjA7MTAwMDsyMDAwI3dhaXQjMTAjeENSMl8yN
(...)
```

La dernière ligne de données transmises correspond à la commande attendue. Elle peut préciser les paramètres d'une attaque par inondation de trames, ou d'un fichier à télécharger et à exécuter.

La question est donc : que peut-on détecter ?

Des initiatives envisageables sont :

- l'identification des requêtes vers le serveur distant, si celui-ci est connu comme étant compromis ;
- des recherches de contenus sur des chaînes de caractères particulières, mais pouvant provoquer beaucoup de fausses alertes, ou faux positifs.

Le lecteur comprendra ici que les moyens d'identifier ce canal de communication ne sont pas simples à mettre en œuvre.

7.3 Le fond du problème

Les exemples précédents montrent la complexité à identifier les canaux de communication de manière précise. Si ceux-ci sont bien connus, des heuristiques peuvent aider à les trouver (IRC), mais les méthodes déployées par les codes malveillants sont toujours plus furtives (recours à Overnet, HTTP, POP3, etc.). Dissimuler un canal de communication est faisable par le biais de multiples méthodes. Le détecter est beaucoup plus complexe.

Suite à la médiatisation du ver Storm Worm, des signatures sont apparues pour aider des administrateurs de réseaux à identifier des machines compromises qui communiquent. Ces signatures doivent venir enrichir la base de connaissance d'une sonde détection d'intrusions.

Le CERTA tient cependant à attirer l'attention sur le fait que ces signatures sont bien sûr intéressantes, mais ne représentent pas l'approche la plus pertinente pour combattre ces activités.

La détection des canaux de communication est une opération complexe, qui peut s'avérer impossible, et le premier effort consiste à prévenir le danger.

Dans tous les cas présentés auparavant, les machines ont d'abord été compromises.

Storm Worm se propage par plusieurs vecteurs, dont l'un est une simple technique d'ingénierie sociale (clic et installation de fichiers exécutables), et un autre une exploitation de vulnérabilités dans des navigateurs qui ne sont pas à jour et qui ont une configuration trop laxiste.

BlackEnergy contamine des serveurs Web, en ajoutant des tables MySQL particulières et des pages PHP.

Quelques mesures simples sont donc suffisantes, en principe, pour se prémunir de telles activités :

- les systèmes et les applications installées doivent être à jour ;
- l'utilisation standard d'un poste de travail doit se faire avec des privilèges limités ;
- la navigation doit se faire depuis un navigateur correctement configuré, n'interprétant pas les codes dynamiques par défaut. Il est préférable de se limiter également à une navigation sur des sites de confiance.
- l'intégrité des pages et des services d'un serveur doit être régulièrement vérifiée.

L'effort doit être mis en priorité dans l'application de ces mesures. L'investissement s'applique ainsi contre plusieurs codes malveillants. La détection par signatures, quant à elle, ne vient qu'en complément, car elle tend à être, par définition, propre à quelques variantes de codes : la signature ne caractérise au mieux qu'un trait particulier d'un canal de communication, et parfois de manière inexacte.

8 Nouvelles fonctionnalités Vista

Dans son nouveau système d'exploitation, Vista et dans la future version serveur de celui-ci (Windows 2008 Server), *Microsoft* a inclus certaines fonctionnalités d'administration à distance. Il y a en particulier le service `WinRM` (`Windows Remote Management`). Ce dernier permet à un administrateur d'accéder à certaines fonctionnalités d'inventaire ou de diagnostics d'une machine sous Windows Vista à distance. Cette commande avec des paramètres bien choisis donne aussi la possibilité d'obtenir des informations très utiles en vue de conduire une attaque.

Par ailleurs, il existe une autre commande nommée `WinRS` (`Windows Remote Service`) dont la finalité est de permettre à un administrateur d'exécuter des commandes sur une machine distante. Grâce à ce service, il serait donc possible de lancer une installation d'un logiciel ou d'exécuter une commande système.

Ces deux fonctionnalités ne sont pas activées par défaut dans Windows Vista.

Recommandations :

Dans ce contexte, il est impératif de définir précisément un périmètre d'utilisation de ce genre de services. En effet, ces commandes peuvent tout à fait être inclues dans des scripts `VB` pour en automatiser l'utilisation. Le CERTA recommande donc de bien vérifier que ces services sont désactivés par défaut s'ils ne sont pas utilisés.

Dans l'hypothèse où ces services sont nécessaires, il conviendrait d'accompagner cette activation par des mesures visant à limiter leurs accès de manière rigoureuse et à journaliser leur utilisation.

9 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 11 et le 18 octobre 2007.

10 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/

11 Rappel des avis émis

Dans la période du 12 au 18 octobre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-436 : Vulnérabilité dans EMC RepliStor
- CERTA-2007-AVI-437 : Multiples vulnérabilités dans BrightStor ARCserve Backup
- CERTA-2007-AVI-438 : Vulnérabilité dans Cisco IOS Line Printer Daemon
- CERTA-2007-AVI-439 : Vulnérabilités de FLAC et Winamp
- CERTA-2007-AVI-440 : Multiples vulnérabilités dans la machine virtuelle JAVA (JRE) de SUN
- CERTA-2007-AVI-441 : Vulnérabilité dans Cisco Wireless Control System (WCS)
- CERTA-2007-AVI-442 : Vulnérabilité dans IBM WebSphere
- CERTA-2007-AVI-443 : Multiples vulnérabilités dans des produits Oracle
- CERTA-2007-AVI-444 : Vulnérabilité dans IrfanView
- CERTA-2007-AVI-445 : Multiples vulnérabilités dans Opera

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

- CERTA-2007-AVI-423-001 : Vulnérabilités d'OpenSSL
  (ajout de la référence CVE-2007-4995 et des références aux bulletins de sécurité OpenBSD, Gentoo, Red Hat, SuSE et Mandriva)
- CERTA-2006-AVI-329-002 : Multiples vulnérabilités dans la bibliothèque libTIFF
  (ajout de la référence au bulletin de sécurité Sun 103099)
- CERTA-2006-AVI-227-002 : Multiples vulnérabilités dans les produits Mozilla
  (ajout des références au bulletin de sécurité Sun 102943)
- CERTA-2005-AVI-188-006 : Multiples vulnérabilités dans bzip2
  (ajout de la référence au bulletin de sécurité Sun 103118)

12 Actions suggérées

12.1 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.

12.2 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.

12.3 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.

12.4 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.

12.5 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.

12.6 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.

12.7 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

13 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.

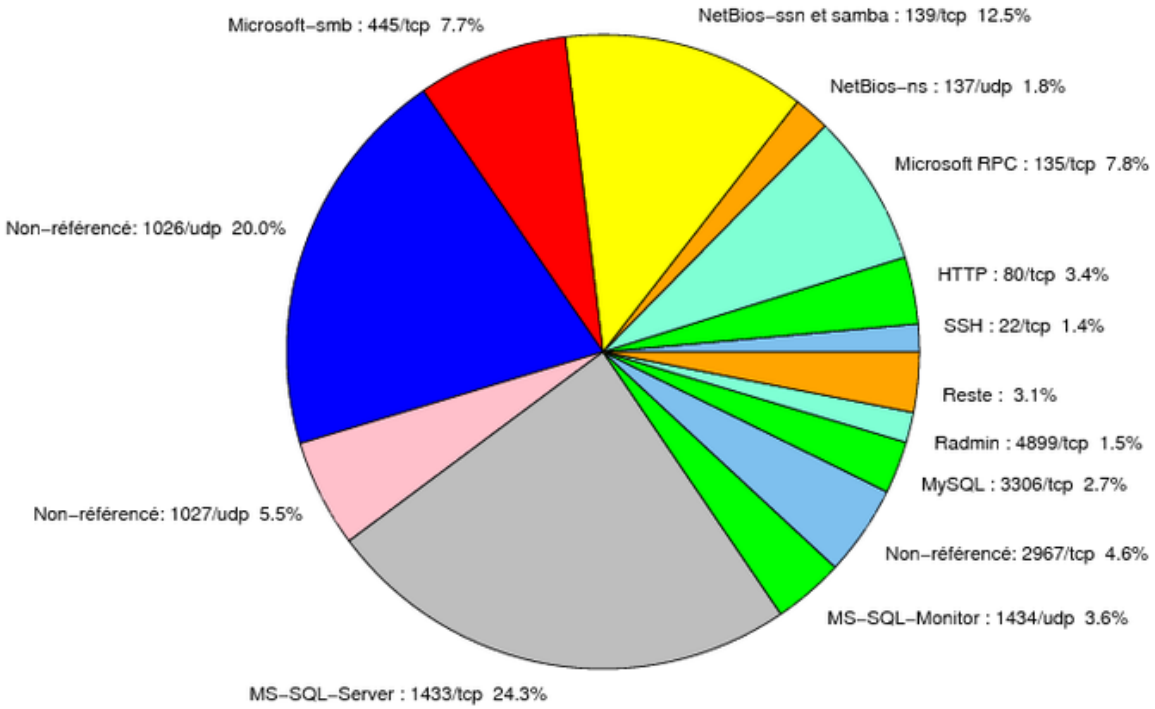

FIG. 1: Répartition relative des ports pour la semaine du 11.10.2007 au 18.10.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/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
1433/tcp	24.33
1026/udp	20.04
139/tcp	12.45
135/tcp	7.78
445/tcp	7.7
1027/udp	5.5
2967/tcp	4.61
1434/udp	3.6
80/tcp	3.41
3306/tcp	2.65
137/udp	1.84
4899/tcp	1.54
22/tcp	1.41
3128/tcp	0.67
1080/tcp	0.59
25/tcp	0.43
21/tcp	0.37
23/tcp	0.24
143/tcp	0.21
3389/tcp	0.1
15118/tcp	0.05
9898/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

19 octobre 2007 version initiale.