Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 avril 2008
N° CERTA-2008-ACT-015

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-15

Gestion du document

Référence	CERTA-2008-ACT-015
Titre	Bulletin d'actualité 2008-15
Date de la première version	11 avril 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-015.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-015/

1 Incidents de la semaine

Cette semaine, le CERTA est intervenu dans la gestion d'un traitement d'incident relatif à la compromission d'un serveur web. Lors de cette compromission, les attaquants ont réussi à exploiter une vulnérabilité d'un composant obsolète et vulnérable pour prendre le contrôle du serveur web. Cette vulnérabilité leur a permis d'obtenir sur la machine les droits du service web pour exécuter ensuite des commandes. Cependant la compromission ne s'arrête pas là : la gestion laxiste des permissions sur les répertoires du serveur leur a également permis de déposer divers contenus malveillants, notamment un site de filoutage (*phishing*).

Comme à son habitude, le CERTA recommande de maintenir à jour les applications et les composants de gestion de sites internet. Les composants inutiles ou vulnérables doivent être supprimés. De plus, sauf si le site le nécessite, l'utilisateur exécutant le service web doit uniquement avoir les droits de lecture sur les fichiers et dossiers du site web.

Documentation

– Note d'information CERTA-2002-INF-002, « Les bons réflexes en cas d'intrusion sur un système d'information » :

http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

– Portail de la Sécurité Informatique, « Mises à jour de sécurité » :
http://www.securite-informatique.gouv.fr/gp_article96.html

2 Les mises à jour Microsoft publiées cette semaine

2.1 Introduction

Microsoft a publié le 08 avril 2008 huit bulletins concernant des mises à jour de sécurité.
http://blogs.technet.com/msrc/archive/2008/04/08/april-2008-monthly-release.aspx

Le CERTA a émis différents avis de sécurité associés à ces publications. Les sections suivantes traitent de certains points qui n'ont pas nécessairement été mentionnés dans ces documents, mais qui présentent un intérêt en terme de sécurité.

Le lecteur comprendra à la lecture de ceux-ci qu'il est important de considérer l'application des mises à jour dans les plus brefs délais.

2.2 GDI

Microsoft a publié le bulletin de sécurité MS08-021, correspondant à CERTA-2008-AVI-192, afin de corriger plusieurs vulnérabilités affectant la bibliothèque GDI (*Graphics Device Interface*).

Elles sont exploitables par le biais de fichiers aux formats `EMF` (*Enhanced Meta-File*) et `WMF` (*Windows Meta-File*). Par exemple, l'opération pour calculer l'espace dans le tas (*heap*) estime par défaut que la variable *color depth* a une valeur fixe. En modifiant celle-ci, il est possible de provoquer un débordement dans l'allocation du tas. La variable *color depth* permet de définir le nombre de bits associés à chaque pixel de l'image. La vulnérabilité concerne plus précisément la fonction `CreateDIBPatternBrushPt`. Une autre vulnérabilité porte sur la manipulation des données du nom de fichier associé à une image. Elle peut provoquer sous certaines conditions un débordement au niveau de la pile.

Le CERTA attire l'intention de ses lecteurs sur le fait que des codes d'exploitation sont déjà disponibles sur l'Internet. Les précédentes vulnérabilités liées à GDI avaient également fait l'objet d'exploitations nombreuses et variées.

– Alerte CERTA-2004-ALE-011, « Diffusion de programmes exploitant la faille GDI+ », septembre 2004 :
http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-011/

Différents scénarios d'attaques sont possibles. Des personnes malveillantes peuvent insérer un fichier image sur un site web ou dans un courrier électronique au format HTML.

Les codes rencontrés à la date de rédaction de ce bulletin sont des images nommées `word.gif`, `top.jpg` ou `Ad02.jpg` insérées dans des pages web. Ils tentent d'établir des connexions vers des sites distants, en utilisant les ports TCP 53, 80 et 443 afin de récupérer d'autres charges utiles.

Il est important d'appliquer les mises à jour fournies par Microsoft. Si cela n'est pas possible, le bulletin MS08-021 cite plusieurs contournements provisoires afin de limiter les risques, comme par exemple la désactivation de l'interprétation de *métafichiers* :

```
Ajouter la variable DisableMetaFiles DWORD
dans :
  HKEY_LOCAL_MACHINE\SOTFWARE\Microsoft\WindowsNT\CurrentVersion\GRE_Initialize
```

Dans tous les cas, les bonnes pratiques doivent être appliquées :

– naviguer depuis un compte aux droits limités ;
– naviguer sur des sites de confiance ;
– désactiver l'interprétation de code dynamique par défaut (JavaScript, ActiveX, etc.) ;
– lire ses courriers électroniques au format texte, et ne pas prévisualiser les pièces jointes ;
– avoir un antivirus à jour.

Documentation

– Documentation Microsoft, "MS-EMF : Enhanced Metafile Format Specification" :
http://msdn2.microsoft.com/en-us/library/cc204166.aspx
– Documentation Microsoft, "MS-WMF : Windows Metafile Format Specification" :
http://msdn2.microsoft.com/en-us/library/cc215212.aspx

2.3 Internet Explorer

Le CERTA a publié l'avis CERTA-2008-AVI-195 pour signaler la mise à jour cumulative d'Internet Explorer, détaillée dans le bulletin MS08-024.

Cette mise à jour change aussi une fonctionnalité du navigateur. L'`IE ACA` (comprendre ici *Internet Explorer Automatic Component Activation*) est disponible sur les navigateurs fraîchement mis à jour.

Certains contrôles ActiveX embarqués dans des sites web nécessitaient au préalable l'action de l'utilisateur via un message de la forme :

```
"Cliquer pour activer ce contrôle"
```

La fonctionnalité ajoutée supprime maintenant par défaut cette action. En réalité, l'action avait été imposée début 2006, suite à un différent entre Microsoft et la société Eolas. Il ne s'agit donc pas d'une mesure de sécurité particulière. Microsoft ne l'a d'ailleurs pas présentée comme tel.

Voici le tableau fourni par Microsoft sur le changement de comportement :

	Sans correctif MS08-024	Avec correctif
Contrôles ActiveX via JavaScript	Pas de clic	Pas de clic
Contrôles ActiveX chargés en HTML (<object>, <embed>, <applet>, ..	clic nécessaire	Pas de clic

Le CERTA profite de ce changement de fonctionnalité pour rappeler qu'il est vivement déconseillé d'interpréter par défaut sur son navigateur toute forme de contenu dynamique, et en particulier les contrôles ActiveX. Il est préférable de n'activer ces fonctionnalités que ponctuellement pour des sites de confiance, quand cela est strictement nécessaire.

Documentation

- Bloc-notes Microsoft, "IE Automatic Component Activation Now Available" : http://blogs.msdn.com/ie/archive/2008/04/08/ie-automatic-component-activation-now-available.aspx
- Bloc-notes Microsoft, "IE Automatic Component Activation (Changes to IE ActiveX Update)" : http://blogs.msdn.com/ie/archive/2007/11/08/ie-automatic-component-activation-changes-to-ie-activex-update.aspx
- Note de support technique Microsoft KB947864 : http://support.microsoft.com/kb/947864/fr
- MSDN, "Information for Developers about Internet Explorer", publié le 08 avril 2008 : http://msdn2.microsoft.com/en-us/bb969055.aspx
- Historique du différent entre Microsoft et Eolas : http://en.wikipedia.org/wiki/Eolas

2.4 DNS Client

Le bulletin de sécurité Microsoft MS08-020 mentionné dans CERTA-2008-AVI-191 précise une vulnérabilité associée au client DNS Windows en charge de la résolution de nom. La construction de l'identifiant de transaction DNS (TID) peut être prédictible sous certaines conditions. Une personne malveillante peut donc estimer la valeur de cet identifiant et forger une trame de réponse adaptée. Si celle-ci est interprétée sur le poste client avant la réponse légitime, alors elle permettra de détourner le trafic vers une machine tiers.

Cette attaque est classée comme « importante » mais non « critique » par Microsoft. Elle peut cependant être déployée dans un réseau local afin de compromettre des postes rapidement, comme cela peut se produire au niveau d'une couche protocolaire plus basse avec ARP.

Le CERTA insiste de nouveau sur l'importance de surveiller le trafic DNS de son réseau, comme cela a été rappelé dans un précédent bulletin en février 2008. Cela permet de déterminer rapidement de tels dysfonctionnements ou d'autres comportements DNS anormaux.

– Bulletin d'actualité CERTA-2008-ACT-008, « Surveiller le trafic DNS, une nécessité », 22 février 2008 : http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-008.pdf

2.5 Élévation de privilèges

L'avis CERTA-2008-AVI-196 mentionne l'existence d'une vulnérabilité dans le noyau Windows, qui permettrait à un code malveillant d'élever ses privilèges. Le bulletin Microsoft associé MS08-025 parle également d'une seule vulnérabilité, mais ce n'est pas le cas du bloc-notes de l'éditeur qui fournit des détails sur plusieurs vulnérabilités concernant `win32k.sys`.

Les tests de contrôle `ProbeForRead` et `ProbeForWrite` ne seraient pas suffisamment rigoureux au moment où l'utilisateur a besoin d'accéder à la mémoire. Ces tests doivent normalement s'assurer que la zone demandée se trouve dans l'espace mémoire dédié de l'utilisateur. Ils peuvent cependant être contournés à partir du moment où l'espace mémoire requis correspond à un intervalle nul.

Dans tous les cas, il est important :

– d'utiliser un compte utilisateur aux droits limités pour les usages courants (bureautique, navigation, lecture de courriels, etc.) ;
– de ne pas installer de logiciels qui ne soient pas de confiance, y compris via un compte aux droits restreints ;
– de mettre à jour le système d'exploitation.

Documentation

– Bloc-notes de Microsoft, "MS08-025: Win32k vulnerabilities" publié le 09 avril 2008 : http://blogs.technet.com/swi/archive/2008/04/09/ms08-025-win32k-vulnerabilities.aspx
– MSDN (Microsoft Developer Network), "Windows Driver Kit: Installable File System Driver - Buffer Handling" : http://msdn2.microsoft.com/en-us/library/ms790786.aspx
– MSDN (Microsoft Developer Network), "Device Drivers Technical Articles - Common Driver Reliability Issues" : http://www.microsoft.com/whdc/driver/security/drvqa.mspx http://msdn2.microsoft.com/en-us/library/ms809962.aspx

3 Filoutage contre les différents portails des fournisseurs d'accès à l'Internet (FAI)

Le CERTA rencontre, depuis quelques semaines, des cas de filoutages relatifs aux portails des fournisseurs d'accès à l'Internet. La stratégie d'attaque reste très classique et consiste en l'envoi d'un message semblant provenir du `FAI` demandant à l'internaute de se connecter sur l'interface d'administration fournie en lien dans le message. Cette interface n'est évidemment pas la bonne mais une ou plusieurs pages reconstruites servant à la collecte des données renseignées par les victimes.

Par ce biais, l'attaquant pourra obtenir les identifiants de connexion de la victime, lui donnant ainsi accès au vrai site d'administration chez le `FAI`.

L'intérêt de ce type de filoutage est multiple. En effet, par le biais de leur portail et de cette interface d'administration, nombre de grands FAI vont offrir à leurs clients des services en ligne comme l'achat et le téléchargement de musique, de video, etc. Un attaquant pourra donc réaliser des achats en ligne en utilisant le compte compromis. Plus simplement, il pourra aussi utiliser les services de messagerie pour diffuser des pourriels. Une autre motivation peut être la modification de la configuration de la *« box »* de la victime pour en détourner le fonctionnement normal. Ainsi l'attaquant pourra, par exemple, accéder aux paramètres de `ToIP` (`Téléphonie sur IP`) pour émettre des appels vers des numéros surtaxés qu'il contrôle ; ou bien encore modifier la configuration `DNS` de l'équipement pour intercepter le trafic réseau de la victime à son insu.

Recommandations :

Comme dans tous les cas de filoutage et de manière générale lorsque l'on a à utiliser des données sensibles (identifiants, informations personnelles) sur l'Internet, il conviendra de s'assurer de la provenance d'un message électronique et de la pertinence du site vers lequel ce message peut rediriger l'internaute.

4 Maîtriser ses logiciels : Firefox

L'une des recommandations les plus souvent faites par le CERTA est, «maîtrisez vos logiciels». Pour avancer dans cette direction, cet article aborde la configuration du navigateur Mozilla Firefox.

4.1 Configuration

Il est possible de modifier un nombre limité d'options en utilisant le sous menu «préférences», mais une configuration plus avancée nécessite de passer par la page *about:config*, dans laquelle on retrouve aussi les informations accessibles par l'interface graphique. Par exemple la taille maximale du cache se retrouve dans la clé *browser.cache.disk.capacity* et dans l'onglet «avancé». Toutes les modifications nécessitent un redémarrage, mais pas de sauvegarde.

4.2 Quelques exemples de paramètres utiles

- Depuis la version 2.0 le navigateur précharge les liens présents sur une page pour accélérer la navigation. Pour éviter ce comportement par défaut il faut mettre à «faux» (*false*) la clé *network.prefetch-next*.
- Il est possible de limiter la mémoire qu'utilise le navigateur en initialisant la clé *browser.cache.memory.capacity*. Elle n'est pas dans la liste et doit être créée. L'utilisation actuelle est accessible à l'adresse *about:cache?device=memory*
- *network.security.ports.banned* permet de bloquer un certain nombre de ports
- Lorsqu'une adresse réticulaire (URL) contient un login et un mot de passe (ex: *ftp://login:mdp@uri*), la variable *browser.fixup.hide_user_pass* permet de contrôler la sauvergarde dans l'historique du mot de passe.

4.3 Conclusion

Toutes ces clés sont détaillées sur le site de Mozilla (cf. section Documentation). Une fois le navigateur paramétré en fonction des besoins il est important de sauvegarder la configuration. Pour cela, il faut manuellement sauvegarder le fichier du «profil» correspondant. En fonctions des systèmes il n'est pas situé au même endroit mais la liste les différents chemins d'accés est disponible sur une page du support Mozilla (cf. section Documentation).

Il existe d'autres pages du même type. Par exemple, `about:` permet de verifier la version du logiciel et `about:plugins` donne les associations entre les types de média et les programmes tiers les ouvrant, ce qui est utile lorsque certains d'eux sont vulnérables.

4.4 Documentation

- Lister la configuration du navigateur :
  about:config
- Liste les associations des programmes tiers :
  about:plugins
- Détails des clés :
  http://kb.mozillazine.org/Firefox_:_FAQs_:_About:config_Entries
- Sauvegarde de la configuration :
  http://support.mozilla.com/fr/kb/Backing+up+your+information

5 Kraken : faire du neuf avec du vieux ?

Depuis quelques semaines, Kraken, un ver (ou plutôt un calmar[1]), fait parler de lui dans les médias. Est-il nouveau ? Pas tout a fait pour certains. En effet, certains rapports publiés semblent montrer des similitudes avec un vieux code malveillant (*trojan*) datant de 2004 : Bobax. Qu'en est-il réellement ?

[1] Kraken est le nom d'un calmar géant issu des légendes scandinaves

5.1 Rappel : comportement de Bobax

Bobax a été défini comme un code malveillant à diffusion semi-automatique, le but de ce code malveillant étant d'offrir la possibilité à qui le contrôlait d'envoyer un grand nombre de spams "à la demande". Le code était novateur dans le sens où il embarquait des schémas (*templates*) de mails préconçus. Pour pouvoir recevoir des commandes, Bobax ouvre un serveur HTTP en écoute sur un port choisi au hasard sur la plage allant de 2000/TCP à 62000/TCP, afin de communiquer avec le serveur de contrôle.

Outre cette fonctionnalité d'envoi de spams, il intégre un moteur de reproduction à travers le réseau : une fois installée, Bobax scanne plusieurs réseaux (dont celui local) à la recherche de machines vulnérables à la faille décrite et corrigée dans le bulletin de Microsoft numéro MS04-011.

– Bulletin d'actualité CERTA-2004-ACT-002, « Les vers Bobax et Kibuv » :
http://www.certa.ssi.gouv.fr/site/CERTA-2004-ACT-002.pdf

5.2 Fonctionnement de Kraken

Kraken semble être diffusé sur l'Internet depuis fin 2007. Il est considéré comme un ver à diffusion de pourriels (*spam*), dont les mails sont construits suivant des schémas (*templates*) embarqués dans le code.

Outre cette fonctionnalité, Kraken ouvre les ports 447/TCP et 447/UDP en écoute afin de communiquer via un canal chiffré (ou du moins brouillé) avec son canal de contrôle.

5.3 Comparaison entre les deux vers

Des comparaisons ont été rapidement faites entre Kraken et Bobax, et le moins que l'on puisse dire, c'est que les deux codes comportent quelques ressemblances :

– *serveurs DNS utilisés* : les deux codes utilisent quelques serveurs DNS dynamiques identiques, à savoir les suffixes *dynserv.com*, *mooo.com*, *yi.org*. Cette liste peut cependant évoluée.
– *génération des noms de domaines* : l'algorithme de génération des noms de domaines semble être le même.
– *génération de spam* : la génération des spams est effectuée à l'aide de *templates*.
– *finalité* : la finalité est pour l'instant identique, à savoir l'envoi de spams.

En revanche, une différence entre les deux réseaux de machines zombies (*botnet*) réside dans la méthode de communication utilisée pour le canal de contrôle : là où Bobax utilisait un canal HTTP sans chiffrement, Kraken utilise un canal de communication construit sur un algorithme méconnu et chiffré.

5.4 De manière plus pragmatique

Ces deux vers sont-ils de la même famille ? Ont-il été conçus par les mêmes personnes ? L'un est-il l'ancêtre de l'autre ?

L'objectif de cet article n'est pas de répondre à ce débat.

Ce qui est établi concernant Kraken est que le nombre de machines compromises est relativement important. Pourtant sa méthode d'infection reste simple, voire simpliste : le code est envoyé en pièce jointe, prenant la forme d'un faux fichier image, ou installé grâce à un autre logiciel malveillant.

Les méthodes de brouillage du code sont complexes et peu d'antivirus proposent une signature fiable.

Il est cependant relativement facile de déterminer si une machine est infectée ou pas. Pour cela, il suffit de vérifier les choses suivantes :

– tentatives de connexions à destination de serveurs DNS comme *dyndns.org*, *dynserv.com*, *mooo.com*, *yi.org*… ;
– présence des ports 447/TCP ou 447/UDP en écoute sur une machine ;
– tentatives de connexions à destination du port 25/TCP (associé au protocole SMTP) vers des adresses IP inconnues, ou ne correspondant pas au serveur de messagerie légitime.

L'importance des journaux d'événements du pare-feu prend alors une nouvelle fois tout son sens, et accentue la nécessité de journaliser les connexions sortantes (qu'elles soient réussies ou rejetées).

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 03 et le 10 avril 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 04 au 10 avril 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-177 : Vulnérabilité dans lighttpd
- CERTA-2008-AVI-178 : Vulnérabilité dans Apache-SSL
- CERTA-2008-AVI-179 : Multiples vulnérabilités du logiciel multimédia Quicktime d'Apple
- CERTA-2008-AVI-180 : Vulnérabilité de certains produits Cisco
- CERTA-2008-AVI-181 : Multiples vulnérabilités dans le navigateur Opera
- CERTA-2008-AVI-182 : Vulnérabilités dans des produits Symantec
- CERTA-2008-AVI-183 : Vulnérabilités dans CUPS
- CERTA-2008-AVI-184 : Multiples vulnérabilités de CA Alert Notification Server
- CERTA-2008-AVI-185 : Vulnérabilités dans CA ARCserve Backup
- CERTA-2008-AVI-186 : Vulnérabilité dans UnZip
- CERTA-2008-AVI-187 : Vulnérabilité dans HP Integrity Server
- CERTA-2008-AVI-188 : Vulnérabilité du serveur applicatif IBM Websphere
- CERTA-2008-AVI-189 : Vulnérabilité dans Microsoft Project
- CERTA-2008-AVI-190 : Vulnérabilités dans Microsoft Office Viso
- CERTA-2008-AVI-191 : Vulnérabilité du client DNS de Microsoft Windows
- CERTA-2008-AVI-192 : Vulnérabilités dans Graphics Device Interface (GDI) de Windows
- CERTA-2008-AVI-193 : Vulnérabilités des moteurs de script VBScript et JScript de Windows
- CERTA-2008-AVI-194 : Vulnérabilité dans un contrôle ActiveX de Microsoft Windows
- CERTA-2008-AVI-195 : Vulnérabilités dans Microsoft Internet Explorer
- CERTA-2008-AVI-196 : Vulnérabilité dans le noyau Windows
- CERTA-2008-AVI-197 : Vulnérabilités dans Adobe Flash Player
- CERTA-2008-AVI-198 : Vulnérabilités dans Symantec Mail Security

– CERTA-2008-AVI-199 : Multiples vulnérabilités d'IBM Lotus Notes
– CERTA-2008-AVI-200 : Vulnérabilité du logiciel Adobe ColdFusion
– CERTA-2008-AVI-201 : Vulnérabilités dans Drupal
– CERTA-2008-AVI-202 : Vulnérabilité dans HP Storage Essentials

9 Actions suggérées

9.1 Respecter la politique de sécurité

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

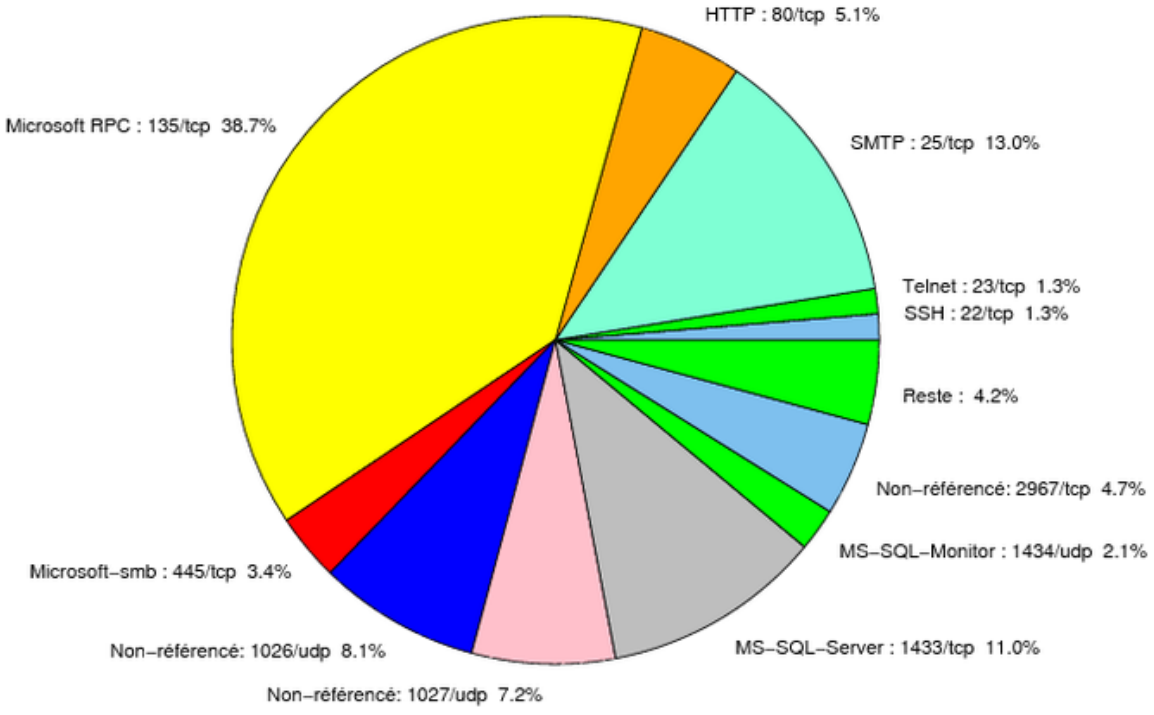

FIG. 1: Répartition relative des ports pour la semaine du 03.04.2008 au 10.04.2008

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
135/tcp	38.71
25/tcp	13.01
1433/tcp	10.98
1026/udp	8.07
1027/udp	7.15
80/tcp	5.19
2967/tcp	4.68
445/tcp	3.35
1434/udp	2.13
23/tcp	1.36
22/tcp	1.29
143/tcp	0.95
139/tcp	0.84
4899/tcp	0.66
137/udp	0.51
3306/tcp	0.47
3389/tcp	0.14
2100/tcp	0.11
1080/tcp	0.07
9898/tcp	0.03

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

11 avril 2008 version initiale.