Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 décembre 2007
N° CERTA-2007-ACT-049

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-49

Gestion du document

Référence	CERTA-2007-ACT-049
Titre	Bulletin d'actualité 2007-49
Date de la première version	09 décembre 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-049.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-049/

1 Des incidents traités cette semaine

1.1 L'affichage d'une page en fonction de la navigation de l'utilisateur

1.1.1 L'incident

Le CERTA a traité cette semaine la défiguration d'un site Web. Celle-ci était particulière, car la page modifiée apparaissait de manière intermittente aux utilisateurs se rendant sur le site : tantôt ils y trouvaient la page légitime, tantôt celle d'un *blog*, ou bloc-notes. La navigation sur cette dernière page provoquait alors plusieurs requêtes en cascade vers d'autres sites distants.

Il s'avère, après analyse, que le fichier `.htaccess` a été modifié. La nouvelle version effectuait pour chaque visite un filtre sur le champ `Referer`; en d'autres termes, elle se préoccupe du moyen utilisé pour parvenir à cette page. Si l'utilisateur se rend sur le site suite à un résultat obtenu par un moteur de recherche, il est automatiquement redirigé vers la mauvaise page. S'il tente d'accéder au site directement en tapant l'adresse dans son navigateur, la page apparaît normalement.

La nouvelle page `.htaccess` est donc de la forme :

```
RewriteEngine On
```

```
# Recherche des personnes venant après visite sur un moteur de recherche
RewriteCond %{HTTP_REFERER} .....*(google|msn|yahoo|....
RewriteCond %{HTTP_REFERER} .....(q|query|searchfor|...)\=

# Ces derniers sont dirigés vers une page différente
RewriteRule ^.*$ maPageMalveillante
```

La modification du fichier a été possible pour deux raisons :

- certaines variables dans des scripts PHP ne sont pas correctement contrôlées, et permettent d'insérer de nouveaux scripts PHP qui sont ensuite interprétés sur le serveur ;
- le fichier `.htaccess` d'origine a des droits trop laxistes qui permettent au code précédent de le modifier.

Le CERTA avait mentionné ce même problème dans un article relativement récent publié dans CERTA-2007-ACT-047.

- Bulletin d'actualité CERTA-2007-ACT-047, « L'intégrité du fichier `.htaccess` » : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-047.pdf

Cet incident montre que la simple visite régulière sur la page d'accueil du site ne permet pas de visualiser systématiquement une défiguration. Il est donc important que tout utilisateur signale un comportement anormal, car celui-ci n'est pas toujours directement visible par les responsables du site. Ces derniers, de leur côté, doivent régulièrement vérifier l'intégrité du site et consulter les journaux du serveur afin de mettre en évidence de telles activités.

1.1.2 Les motivations

Cette défiguration particulière a pour principal objectif d'exploiter la navigation des personnes se rendant sur le site depuis un moteur de recherche. Cette méthode peut paraître surprenante sous certains abords, mais est l'illustration de l'article du précédent bulletin d'actualité sur le détournement du service des moteurs de recherche :

- CERTA-2007-ACT-048, « Moteurs de recherche : la chance m'accompagne.... *I'm feeling (un)lucky* » : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-048.pdf

Le site de cette administration sert de moyen pour « amplifier » artificiellement la côte de fréquentation de certains sites associés à des mots-clés. Ces sites, affichés par cette méthode comme pertinents dans les moteurs de recherche (pour des mots-clés donnés), contiennent des codes malveillants : ceux-ci tentent d'exploiter plusieurs vulnérabilités lors de la navigation par l'utilisateur.

Le site défiguré peut également servir pour effectuer de nouvelles injections de codes vers d'autres sites, et rediriger directement l'utilisateur « exploité » vers d'autres pages dangereuses pour son poste.

1.2 Encombrement de tuyaux

Cette semaine, le CERTA a traité un incident relatif à la messagerie. Ces derniers jours, une augmentation du volume des courriers non désirés semble avoir pénalisé le traitement de courriers légitimes par certains serveurs de messagerie. Cette hausse concerne plus particulièrement des avis de non distribution ou `NDR` (*Non Delivery Report*). Ces courriers, qui ne semblent pas contenir de charge malveillante, sont envoyés à des adresses erronées en ayant pris soin au préalable d'usurper une adresse de retour. C'est alors que le principe des avis de non distribution s'applique, le courrier arrivant à une adresse erronée est renvoyé à l'adresse de retour pour signifier de la non-remise. Cette technique permet à des personnes malveillantes de surcharger les serveurs de messagerie.

Plusieurs solutions peuvent permettre de réduire l'impact de ces attaques, que ce soit pour limiter celui d'une réception massive de NDR, ou pour éviter de participer involontairement à celles-ci :

- identifier et bloquer un réseau de machines compromises à l'origine des envois. Cette tâche peut cependant s'avérer très difficile dans le cas d'un réseau distribué sur l'Internet ;
- filtrer en amont les avis de non distribution ou `NDR` ;
- limiter le nombre d'envois d'avis de non distribution par jour et par domaine ;
- prendre la décision de ne plus envoyer les avis de non distribution. Cette solution ne respecte pas les standards, et notamment le RFC 2821 (cf. Section 3.7) du protocole *Simple Mail Transfer Protocol* (SMTP). Elle a été néanmoins appliquée chez certains fournisseurs de messagerie, et est mentionnée dans des documents Microsoft de configuration Exchange.

Les trois solutions précédentes peuvent perturber l'utilisateur légitime, qui n'aura pas de retour sur l'envoi de son courrier. Ces solutions doivent donc être considérées en toute connaissance de causes.

Dans tous les cas, il est important de journaliser ces événements afin de pouvoir en faire une analyse approfondie *a posteriori*.

Documentation

- Bulletin d'actualité du CERTA CERTA-2007-ACT-010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-010.pdf
- Microsoft, KB 886208, "Exchange queues fill with many non-delivery reports from the postmaster account in Small Business Server 2003" :
  http://support.microsoft.com/kb/886208/
- Microsoft, KB 294757, "How to control non-delivery reports when you use Exchange 2000 or Exchange 2003" :
  http://support.microsoft.com/?kbid=294757
- Microsoft, KB 842851, "SMTP tar pit feature for Microsoft Windows Server 2003" :
  http://support.microsoft.com/kb/842851

2 Windows Vista Service Pack 1 RC

Le premier *Service Pack* pour Windows Vista sera disponible publiquement en version *release candidate* la semaine prochaine, et il est d'ores-et-déjà proposé aux abonnés des services *Technet* et *MSDN*. Ceci est la dernière phase avant la sortie de la version *release-to-manufacturing*. Cet article a pour but de détailler les changements les plus importants apportés par ce *service pack*.

Cette mise à jour, dont la version définitive sortirait début 2008, contiendra notamment toutes les mises à jour disponibles précédemment via *Windows Update*. De nouvelles améliorations dites de « qualité » y seraient également présentes : améliorations de performance (mise en veille prolongée, transferts de fichiers, Internet Explorer 7, durée de charge des batteries, etc.), de fiabilité (compatibilité, pilotes) mais aussi de sécurité (amélioration de *RemoteApp*, *Remote Desktop Protocol*, et ajout d'un nouveau générateur pseudo-aléatoire).

Deux améliorations de *Bitlocker* seront également apportées. Il sera maintenant possible de chiffrer tous les volumes et non plus le volume du système seul, et un nouveau mode d'authentification sera proposé, basé sur le TPM (*Trusted Platform Module*) combiné à une clé USB et un code PIN. Le défragmenteur de disque sera aussi mis à jour et il sera enfin possible de choisir les partitions à défragmenter.

Un autre changement important est la suppression de l'outil GPMC (*Group Policy Management Console*) du système d'exploitation ; il sera maintenant nécessaire (comme sur les autres systèmes) de le télécharger.

Enfin, le *Service Pack 1* ajoute les fonctionnalités suivantes :

- support du nouveau système de fichiers exFAT (*extended File Allocation Table*) ;
- support du démarrage réseau pour les versions 64 bits utilisant l'EFI (*Extensible Firmware Interface*) ;
- installation de DirectX 10.1 ;
- support du *Secure Digital Advanced Direct Memory Access* ;
- ajout du protocole SSTP (*Secure Socket Tunneling Protocol*) utilisé pour les VPN.

Si ce premier *service pack* n'est pas aussi révolutionnaire que l'a été par exemple le deuxième *service pack* de Windows XP, il apporte toutefois quelques améliorations intéressantes.

Comme toute mise à jour importante, il est toutefois recommandé d'attendre la sortie de la version définitive de ce *service pack* pour l'installer.

Documentation

- Windows Vista Service Pack 1 Beta Overview :
  http://www.microsoft.com/downloads/details.aspx?familyid=090deaf6-2eaa-4aaa-8b3b-2e199db4a97d

3 Retour sur la fin du MoBiC

Le CERTA avait abordé le sujet du MoBiC (*Month Of Bug In Captchas*) dans ses bulletins d'actualité CERTA-2007-ACT-044 et CERTA-2007-ACT-046. Le MoBiC a pris fin le week-end dernier et l'auteur propose un bilan. 32 systèmes de Captcha ont été testés, 75 vulnérabilités ont été trouvées, et à la date du 1er décembre, seulement 5 ont été corrigées.

3.1 Présentation

Les *Captchas* (*Completely Automated Public Turing test to tell Computers and Human Apart*) sont des systèmes maintenant bien connus qui permettent de vérifier la présence d'un humain lors d'une action en ligne. Souvent sous la forme d'une image contenant du texte déformé à recopier, ils sont par exemple utilisés pour l'ouverture de nouveaux comptes de messagerie. Il ne s'agit pas d'éléments de sécurité mais de contrôle permettant de lutter contre l'utilisation automatique et illicite d'un site ; par exemple pour éviter la création automatique de comptes de messagerie permettant l'envoi de SPAM.

3.2 La problématique

Plusieurs failles avaient été abordées dans le bulletin d'actualité CERTA-2007-ACT-046. La plupart permettent de contourner le principe de contrôle qu'est censé fournir un *Captcha*. Par exemple, si le nombre d'images pouvant être créées n'est pas assez grand, il est possible de réaliser une table associant les images et les valeurs attendues et à l'aide de cette table de contourner le *Captcha* en question sur l'ensemble des sites où il sera utilisé. Mais le MoBiC a aussi mis en avant que plusieurs modules de *Captchas* sont vulnérables à des attaques de type XSS (*Cross Site Scripting*) ou à des injections SQL. Bien qu'il s'agit de petits modules qu'il est facile d'oublier de mettre à jour et qui ne sont pas toujours considérés comme un logiciel à part entière, ces outils de contrôle sont des briques logicielles pouvant contenir des vulnérabilités importantes qui se répercutent sur les sites où elles sont utilisées.

3.3 Conclusions

Le CERTA recommande qu'avant la mise en place d'un tel système, et comme pour tout logiciel tiers, il soit évalué ainsi que son impact et son intérêt. Il faut éviter d'utiliser des modules « gadgets » au maintien douteux et sans correctif régulier, et privilégier des éditeurs sérieux. Et il faut bien sûr ensuite le maintenir à jour.

3.4 Documentation

- Site du projet MoBiC :
  http://websecurity.com.ua/category/mobic
- Bulletins d'actualité du CERTA traitant du projet :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-044.pdf
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-046.pdf

4 Gestion du temps et synchronisation sous Windows

Lorsque le CERTA est amené à analyser une machine compromise, un des points d'entrée est souvent les journaux du système. Pour qu'ils soient pertinents, l'horodatage de ces journaux doit être cohérent avec celui des autres élements du réseau : passerelle de messagerie, pare-feu ou serveur web... Pour obtenir cette cohérence, il est indispensable d'utiliser une base de temps fiable sur laquelle les machines du SI (Système d'Information) vont se synchroniser. Il est fréquent d'employer le protocole `NTP` (`Network Time Protocol`) sur le port *123/udp* (RFC-1305, RFC-4330). On trouve d'ailleurs sur l'Internet une hiérarchie de serveurs publics repartis en strates fournissant une source de temps fiable. Certains de ces serveurs utilisent une horloge atomique comme source primaire. Il est aussi possible d'utiliser un signal radio émis par `Radio France` pour effectuer cette opération via une antenne particulière.

Le cas le plus fréquent est de disposer dans son réseau d'une source de temps sous la forme d'un serveur `NTP` synchronisé sur un référentiel extérieur comme un serveur publique de l'Internet. Il conviendra dans ce cas de ne pas se limiter à une seule source extérieure mais plutôt à un « pool » de serveurs publics. Ainsi, la source locale de temps ne sera pas mise en défaut si son référentiel extérieur venait à disparaître. En outre, une synchronisation unique et initiale n'est pas suffisante pour les éléments du SI. En effet, il est possible de rencontrer des machines sujettes à des dérives de temps relativement importantes pouvant aller jusqu'à 1 heure par semaine (cas déjà observé). Ceci est souvent dû à des horloges internes défaillantes ou mal utilisées par le système d'exploitation. Il sera donc indispensable de procéder à des synchronisations régulières dont la fréquence sera à adapter en fonction des éventuelles dérives constatées. Le système d'exploitation `Windows` de `Microsoft` n'échappe pas à la règle et doit être paramétré dans un environnement de production. Le lien `http://support.microsoft.com/kb/314054` détaille la façon dont peut être configuré le client `NTP` sur ce système d'exploitation.

L'intervalle de temps entre les ajustements est par exemple défini par la clé suivante :

`HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config\UpdateInterval`

La valeur par défaut donnée par Microsoft est de 100 secondes pour les contrôleurs de domaine, et 360000 secondes pour les postes clients et serveurs standards. Il est donc fortement recommandé de réduire cette valeur.

Documentation associée

- RFC 1305, "Network Time Protocol" (version 3), Specification, Implementation and Analysis : http://tools.ietf.org/html/rfc1305
- RFC 4330, "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI" : http://tools.ietf.org/html/rfc4330
- Microsoft KB 314054, "How to configure an authoritative time server in Windows XP" : http://support.microsoft.com/kb/314054

5 USB Mass Storage : quand la base de registre vous rend service

Avec l'arrivée des clefs USB U3 et la généralisation de l'utilisation de support de stockage de masse USB comme média d'échange de fichiers, il devient nécessaire de prendre en compte cette évolution dans l'élaboration de la sécurité d'un système d'information. Le CERTA a déjà publié de nombreux articles et notes sur le danger des clefs USB, le danger des clefs U3 (cf. CERTA-2006-INF-006), ou encore sur les problèmes de conditionnement (cf. CERTA-2007-ACT-040).

De manière radicale, un des moyens les plus simples est de désactiver totalement les pilotes permettant le chargement de clefs USB. Pour cela, la base de registre peut être d'un grand secours. En effet, la clef suivante:

`HKLM\SYSTEM\CurrentControlSet\Services`

permet un contrôle total sur l'ensemble des pilotes matériels, des pilotes systèmes, ainsi que des pilotes de services *WIN32*. Chaque pilote est décrit par une clef de registre contenant plusieurs valeurs (cf. http://support.microsoft.com/kb/103000 pour plus de précisions sur ces valeurs). Une de ces valeurs est particulièrement intéressante : `Start`. Cette valeur permet de définir la manière dont le pilote est chargé :

0x00 le pilote est chargé au moment du démarrage (par le *boot loader*);

0x01 le pilote est chargé au moment de l'initialisation du noyau ;

0x02 le pilote est chargé automatiquement au démarrage du système d'exploitation ;

0x03 le pilote est chargé par le système d'exploitation à la demande, faisant suite à une action de l'utilisateur (l'insertion d'une clef USB, par exemple) ;

0x04 le pilote ne sera jamais chargé.

Il est alors facile de désactiver le chargement des pilotes USB en attribuant le *DWORD 0x04* à la valeur `Start` des clef suivantes, par exemple :

`HKLM\SYSTEM\CurrentControlSet\Services\USBSTOR` : pour désactiver le support du stockage de masse USB ;

`HKLM\SYSTEM\CurrentControlSet\Services\usbhub` : pour désactiver totalement le pont USB ;

`HKLM\SYSTEM\CurrentControlSet\Services\usbuhci` : pour désactiver le support du protocole USB1;

`etc.` : plein d'autre drivers existent, qu'il faut découvrir en fonction du matériel.

Il faut enfin faire attention à la désactivation totale du support de l'USB, car cela perturbe aussi la connectique de la souris et du clavier en USB...

Documentation

- Note d'information CERTA-2006-INF-006, « Risques associés aux clés USB » : http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/
- Bulletin d'actualité CERTA-2007-ACT-040, « Les applications contenues sur une clé » : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-040.pdf
- Microsoft KB 103000, "CurrentControlSet\Services Subkey Entries" : http://support.microsoft.com/kb/103000

6 Les claviers sans fil Microsoft

6.1 L'actualité

Différents articles ont rapporté l'information suivante pendant la semaine : la méthode de chiffrement employée dans certains claviers sans fil de Microsoft aurait été "cassée". Cette découverte permet à un individu malveillant d'intercepter les communications entre les périphériques et la base. Ces communications se font par ondes radio avec la bande de fréquence de 27 MHz. Elles transportent entre autres les frappes clavier effectuées. Cette interception n'est possible qu'à courte distance (environ dix mètres) et ce à l'aide d'une simple radio. Il n'est pas exclu que des récepteurs plus sensibles puissent effectuer cette capture à des distances plus élevées. Il est également possible d'intercepter les communications de plusieurs périphériques avec le même appareil. Le mécanisme de chiffrement repose selon les auteurs sur un opération "ou exclusif" (*xor*) avec un seul octet de donnée aléatoire. Il n'existe donc que 256 clés différentes possibles.

6.2 Les recommandations

Le CERTA tient donc à attirer l'attention sur les risques liés au déploiement de ces matériels. L'utilisation des périphériques sans fil pose les problèmes suivants :

- l'impossibilité de mettre à jour le matériel ;
- les protocoles utilisés sont propriétaires, il est donc plus difficile d'éprouver leur robustesse ;
- les réseaux sans fil ne procurent pas de cloisonnement physique permettant une limitation des risques.

Le CERTA recommande de bien prendre en compte l'ensemble de ces problèmes avant le déploiement des ces matériels.

7 Retour sur WPAD

Microsoft a publié cette semaine un nouveau bulletin sur la vulnérabilité affectant WPAD. Ce bulletin KB945713 n'est qu'un rappel des éléments déjà rapportés dans les bulletins d'actualité CERTA-2007-ACT-013 et CERTA-2007-ACT-048.

7.0.1 Documentation

- Bulletin d'actualité CERTA-2007-ACT-013 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-013.pdf
- Bulletin d'actualité CERTA-2007-ACT-048 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-048.pdf

8 Les organisations des sites malveillants

8.1 Présentation

Le CERTA a mentionné dans un précédent article du bulletin CERTA-2007-ACT-029 une architecture possible de gestion des machines zombies. Il s'agissait notamment pour une personne malveillante en possession d'un nom de domaine, de pointer selon certains critères (choix aléatoire, roulement régulier *round-robin*, géolocalisation de l'adresse IP de la machine victime, etc.) vers l'une des machines compromises sous son contrôle. Cette résolution dynamique implique qu'un nom unique peut correspondre, au cours d'une période relativement courte à plusieurs machines physiques distinctes.

http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-029.pdf

Cette organisation est différente de celles plus anciennes, consistant à associer plusieurs noms de domaines vers une unique adresse IP.

Quelques publications sur l'Internet distinguent ainsi ces architectures :

- celles nommées `single-flux`, où un seul domaine est en jeu : plusieurs machines compromises servent alors de relais vers l'un des sites malveillants mis en place. Le domaine géré permet d'orienter les requêtes vers ces machines relais uniquement. Cette technique se caractérise par une « durée de vie » de la résolution de noms DNS relativement courte, souvent de quelques minutes. Un scénario est caractérisé par la figure

1 : une personne est dirigée, par le biais d'un clic dans un courriel, ou un cadre non visible inséré dans une page légitime ou un fichier `.htaccess` modifié sur un site de confiance par exemple, vers le site www.SiteMalveillant.

– celles nommées `double-flux`, où un seul serveur de nom peut avoir plusieurs adresses IP. Il y a un « double » flux, car dans un premier temps, la requête DNS effectuée vers www.SiteMalveillant sera redirigée vers l'une des machines d'adresse IP1 à IPn. Celles-ci, en fonction des instructions retournées par un coordinateur (aussi appelé *Command and Control* ou C&C), redirige dans un second temps les requêtes HTTP vers l'une des machines d'adresses IP1 à IPn. Les machines compromises servent donc, comme l'illustre la figure 2 à la fois de relais DNS et HTTP. La victime n'interagit jamais directement avec le C&C. Ce dernier peut également se dissimuler dans la masse de machines compromises (adresse IPk sur le dessin).

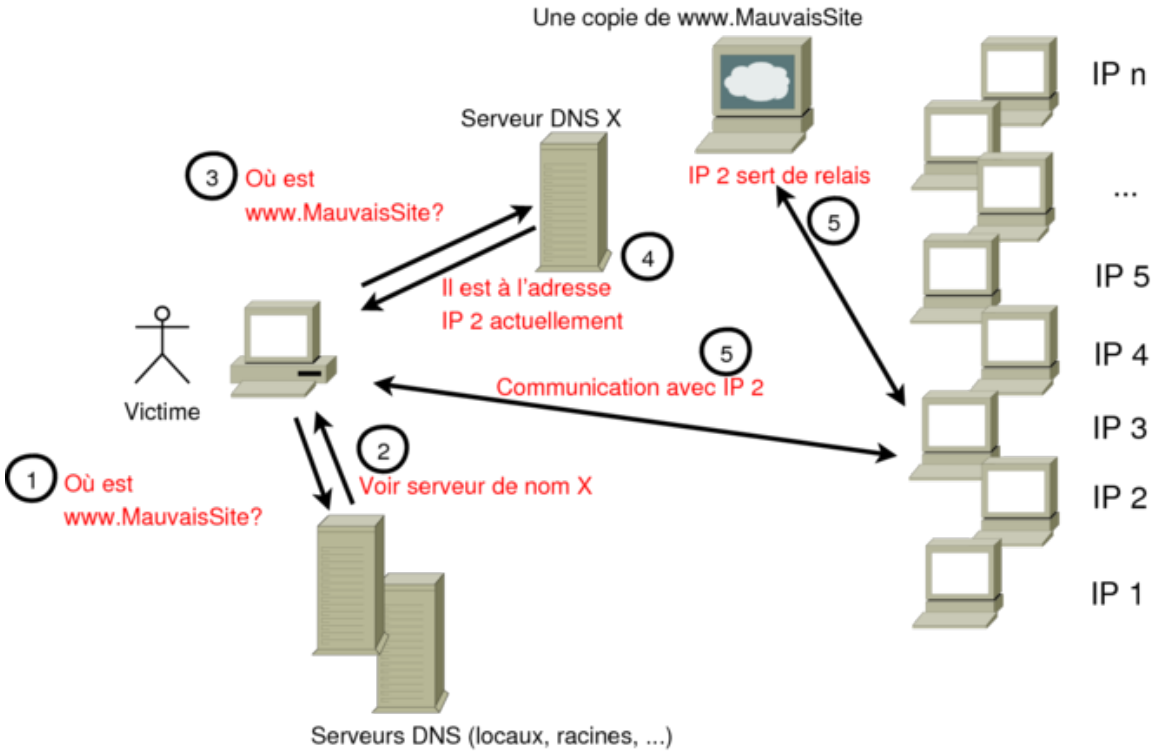

FIG. 1: Architecture possible : un serveur de nom malveillant et plusieurs zombis (IP1..IPn)

Les détails et les nuances de ces architectures restent floues et discutables. Que faut-il néanmoins retenir de cela ?

– l'organisation présentée dans les exemples ci-dessus n'est pas la manifestation d'une malveillance amateur.
– il existe un ensemble de machines compromises pouvant contenir elles-mêmes les codes et les pages malveillantes. Elles peuvent également être de simples relais DNS ou HTTP manipulées par d'autres machines.
– la victime ne voit bien souvent dans ces cas d'architecture qu'une part limitée : les adresses IP avec lesquelles elle communique ne sont souvent qu'un des acteurs. Les rôles respectifs de ces acteurs peuvent changer très fréquemment.

Dans le cas d'un traitement d'incident, le lecteur comprendra donc que fournir comme information une simple adresse IP ou un nom de machine n'est parfois pas suffisant. Il faut collecter et communiquer le maximum d'informations disponibles, afin de rendre l'analyse plus pertinente.

A valeur d'exemple, il est courant d'exporter les journaux d'une interface pour analyse. Il arrive que la résolution de noms se fasse au moment de l'export pour rendre les traces plus lisibles. Des outils comme Wireshark (anciennement Ethereal) font la même chose à la lecture de traces `a posteriori`.

Il est préférable de noter soigneusement quand l'opération de résolution des adresses IP a eu lieu. Dans le cas contraire, cela peut ensuite conduire à de mauvaises interprétations.

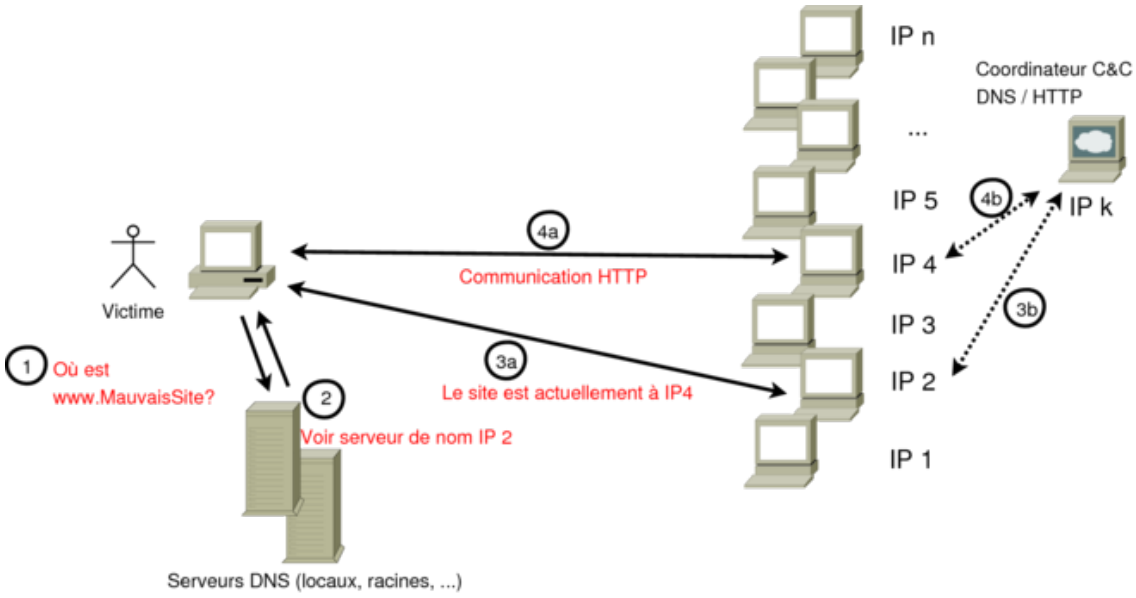

FIG. 2: Architecture possible : zombis (IP1..IPn) servant de mandataires DNS et HTTP

9 Ports observés

Le tableau 3 et la figure 3 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 29 novembre et le 05 décembre 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 30 novembre au 06 décembre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-511 : Vulnérabilités dans Symantec Backup Exec for Windows Server
- CERTA-2007-AVI-512 : Vulnérabilité dans Ruby-GNOME2
- CERTA-2007-AVI-513 : Multiples vulnérabilités de la bibliothèque PCRE
- CERTA-2007-AVI-514 : Vulnérabilité dans Sun Solaris RPC
- CERTA-2007-AVI-515 : Vulnérabilités dans IBM Lotus Notes
- CERTA-2007-AVI-516 : Vulnérabilité dans avast!
- CERTA-2007-AVI-517 : Vulnérabilité de Cairo
- CERTA-2007-AVI-518 : Vulnérabilité dans SonicWall Global VPN Client
- CERTA-2007-AVI-519 : Vulnérabilité dans OpenOfficeorg
- CERTA-2007-AVI-520 : Vulnérabilité de Squid
- CERTA-2007-AVI-521 : Multiples vulnérabilités dans rsync
- CERTA-2007-AVI-522 : Vulnérabilité dans HP OpenView Network Node Manager
- CERTA-2007-AVI-523 : Vulnérabilité dans IBM Tivoli Netcool Security Manager
- CERTA-2007-AVI-524 : Multiples vulnérabilités dans Sun Solaris
- CERTA-2007-AVI-525 : Vulnérabilité dans FreeBSD
- CERTA-2007-AVI-526 : Vulnérabilités dans Novell BorderManager

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

- CERTA-2007-AVI-391-002 : Vulnérabilité dans GNU Tar
  (ajout de la référence au bulletin de sécurité Mandriva)
- CERTA-2007-AVI-423-002 : Vulnérabilités d'OpenSSL
  (ajout de la référence Blue Coat)
- CERTA-2007-AVI-440-002 : Multiples vulnérabilités dans la machine virtuelle JAVA (JRE) de SUN
  (ajout des références aux bulletins de sécurité SuSE et RedHat)
- CERTA-2007-AVI-502-001 : Vulnérabilités dans Samba
  (ajout références aux bulletins de sécurité Mandriva, Gentoo et Debian)
- CERTA-2007-AVI-509-001 : Vulnérabilités dans Mozilla Firefox
  (ajout des références à Netscape)
- CERTA-2007-AVI-510-001 : Multiples vulnérabilités dans Wireshark
  (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2007-AVI-516-001 : Vulnérabilité dans avast!
  (révision du risque, du résumé et de la description)

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.

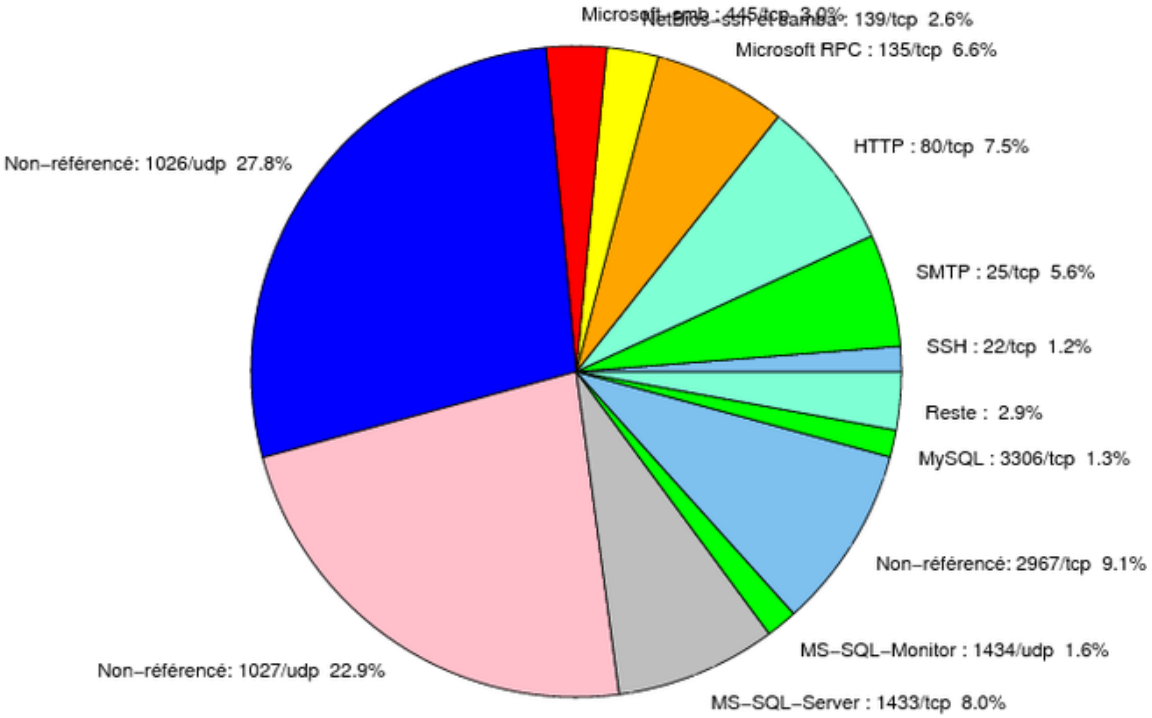

FIG. 3: Répartition relative des ports pour la semaine du 29.11.2007 au 05.12.2007

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
1026/udp	27.76
1027/udp	22.85
2967/tcp	9.11
1433/tcp	7.99
80/tcp	7.47
135/tcp	6.61
25/tcp	5.6
445/tcp	2.98
139/tcp	2.56
1434/udp	1.55
3306/tcp	1.34
22/tcp	1.24
4899/tcp	0.88
1080/tcp	0.72
137/udp	0.36
3128/tcp	0.14
2100/tcp	0.12
3389/tcp	0.11
15118/tcp	0.03
23/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

07 décembre 2007 version initiale.