Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 février 2008
N° CERTA-2008-ACT-008

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-08

Gestion du document

Référence	CERTA-2008-ACT-008
Titre	Bulletin d'actualité 2008-08
Date de la première version	22 février 2008
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-008.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-008/

1 Le filoutage ne cible pas que les banques

Cette semaine, le CERTA a rencontré un grand nombre de sites de filoutage dirigés contre les utilisateurs de MSN et Hotmail. Ces pages frauduleuses ont été déposées à la suite d'une compromission ou simplement téléchargées sur des sites web ouverts spécifiquement. Le but de ces filoutages semblait être de récupérer les informations de connexion des utilisateurs des sites `MSN` ou `Hotmail`.

Le CERTA a pris contact avec les hébergeurs pour fermer au plus vite l'accès à ces pages frauduleuses.

Le CERTA rappelle que le filoutage (ou *phishing*) ne cible pas que les organismes bancaires. Cet incident illustre très bien l'étendue des possibilités de ce type de fraude. Même s'il n'est jamais évident de connaître les motivations des attaquants, elles peuvent être les suivantes :

- voler des informations personnelles ;
- usurper l'identité des victimes pour réaliser des méfaits avec le nom de ces dernières ;
- changer les mots de passe de ces comptes pour réaliser un chantage sur les victimes ;
- revendre ces comptes à des organisations criminelles ;
- etc.

Le CERTA rappelle qu'il est préférable de consulter ses courriers au format texte et qu'il ne faut jamais cliquer sur un lien présent dans un courrier électronique. Il est préférable d'écrire soi-même l'adresse de la page désirée dans la barre d'adressage de son navigateur pour éviter les liens masqués ou ambigus, notamment dans les courriels.

Documentation

- Note d'information du CERTA sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/
- Note d'information du CERTA sur les mesures de prévention relatives à la messagerie :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/

2 Surveiller le trafic DNS, une nécessité

2.1 Une étude publiée récemment

Le CERTA a mentionné dans certains bulletins d'actualité l'existence de codes malveillants cherchant à modifier la configuration DNS des postes infectés. L'un des codes, nommé `DNSChanger` a été présenté dans le bulletin CERTA-2007-ACT-052.

La valeur `NameServer` de la base de registres prime toute valeur qui pourrait être fournie par le serveur DHCP. Sa modification est donc une compromission grave.

La nouvelle configuration fait pointer les requêtes des machines compromises vers des serveurs DNS illégitimes et non maitrisés. Ceux-ci sont normalement configurés en mode « ouvert et récursif ». Ce méfait ne vise donc pas directement les serveurs DNS en exploitation.

L'utilisateur a peu de moyens pour détecter ce changement de comportement et pour douter de la réponse DNS reçue.

Une étude récente a été menée sur presque l'ensemble des adresses IPv4 publiques accessibles, afin d'identifier et de quantifier les serveurs illégitimes ou en mode « ouvert récursif » (configuration déconseillée).

17 millions de serveurs récursifs ouverts distincts ont ainsi été recensés. Il s'agit de serveurs autorisant quiconque sur l'Internet à les interroger. Parmi un échantillon de 600.000 d'entre eux, 2% envoient visiblement des réponses erronées et 0,4% redirigent vers des *proxys* anormaux. Une extrapolation sommaire de tous ces chiffres amène à environ 300.000 machines dans l'Internet fournissant des réponses incorrectes ou malveillantes. Ces informations sont conformes à d'autres listes noires obtenues par d'autres biais (relais de spam, machines infectées par le ver Storm, etc.).

Les motivations sont diverses : il peut s'agir de redirections pour afficher des publicités dans le navigateur ou une interprétation d'une erreur de nom de domaine (erreur de frappe au clavier). La précédente redirection peut également diriger vers des sites de filoutage ou des sites ayant des codes exploitant des vulnérabilités par l'intermédiaire du navigateur.

Il ne s'agit pas dans cet article de valider, critiquer ou infirmer les chiffres présentés dans l'étude menée. Il faut retenir que ce problème lié au DNS est bien concret et présente un risque.

Documentation

- D.Dagon, N.Provos, C.P.Lee, W.Lee, "Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority", février 2008, 15th Annual Network & Distributed System Security Symposium NDSS 2008:
  http://www.citi.umich.edu/u/provos/papers/ndss08_dns.pdf
- Bulletin d'actualité CERTA-2007-ACT-052 du 28 décembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-052.pdf

2.2 Surveillance du trafic DNS

Quelles actions peuvent être entreprises par un administrateur de réseau ?

Les flux DNS sortants du réseau interne doivent être correctement contrôlés. Seuls les serveurs DNS légitimes internes peuvent par exemple initier des requêtes vers leurs homologues dans l'Internet. Les machines ne doivent pas faire cette opération directement. L'observation dans les journaux du pare-feu de telles tentatives est un signe d'une potentielle compromission.

Il est également important de surveiller dans le réseau les requêtes DNS qui circulent, et en particulier les serveurs qui sont destinataires de ces requêtes.

3 Le pare-feu de Windows Vista

Avec la sortie de Windows Vista, Microsoft a inclus un nouveau pare-feu dans son système d'exploitation.

La grande nouveauté du pare-feu est la possibilité d'effectuer du filtrage sortant. Cette fonctionnalité n'est toutefois pas activée par défaut, même si la présence de règles prédéfinies peut laisser penser autrement.

3.1 Activation du filtrage sortant

L'activation du filtrage sortant peut se faire à plusieurs endroits.

- dans les stratégies de groupe : exécuter *gpedit.msc*. Choisir ensuite *Configuration ordinateur*, *Paramètres windows*, *Paramètres de sécurité*, *Pare-feu windows avec fonctions avancées de sécurité*.
- dans la configuration du pare-feu : aller dans *Panneau de configuration*, *Outils d'administration*, *Pare-feu windows avec options avancées de sécurité*.

La stratégie de groupe, même locale, prévaut sur la configuration de l'ordinateur.

On peut voir les options générales du pare-feu, configurables, en suivant le lien *Propriétés du Pare-feu Windows*.

Dans la nouvelle boîte de dialogue, il est possible de paramétrer le filtrage par défaut du pare-feu pour chaque configuration de réseau : privé, public ou domaine. Ainsi, pour activer le filtrage sortant, il faut y mettre l'option *Refuser*. De même, pour le filtrage entrant, on peut confirmer la valeur par défaut en y mettant l'option *Bloquer*. Il est également possible de bloquer complètement toutes les connexions entrantes, ou les autoriser.

Enfin, on peut y choisir d'afficher un message d'avertissement pour indiquer si des applications ont été bloquées (uniquement pour les connexions entrantes), et configurer la journalisation du pare-feu.

3.2 Configuration des règles du pare-feu

Les options *Bloquer* pour le filtrage entrant et *Refuser* pour le filtrage sortant refusent toute connexion qui n'est pas explicitement autorisée dans les règles du pare-feu.

Les règles du pare-feu peuvent être configurées aux mêmes endroits que les options générales du pare-feu. Il en existe deux types : les règles de trafic entrant et les règles de trafic sortant. On peut créer quatre types de règles : programme (on choisit l'exécutable autorisé à communiquer), ports, prédéfinie ou personnalisée. Toutes les règles sont en fait configurables à souhait par la suite, sauf pour les règles prédéfinies.

Voici les différents paramètres applicables à une règle :

- protocole ;
- ports locaux et distants ;
- adresses IP distantes et locale ;
- type d'interface (réseau local, sans-fil...) ;
- profil (public, privé, domaine) ;
- chemin de l'exécutable ou nom du service ;
- nom d'ordinateur ;
- activer ou désactiver la règle, et bloquer ou autoriser les connexions.

Un exemple de règle est ainsi d'autoriser l'exécutable *firefox.exe* à communiquer en sortie vers les ports TCP distants 80 et 443.

Il est important de remarquer que la règle ci-dessus suffit et qu'il n'est pas nécessaire de configurer une règle de flux entrant équivalente. Le pare-feu Windows autorise en effet tout flux entrant relatif à une connexion sortante établie (comme l'option *established* d'iptables sous Linux). Il n'est pas possible de changer cela. Même une règle de filtrage entrant interdisant explicitement à l'exécutable *firefox.exe* de communiquer ne fonctionne pas si nous autorisons un flux en sortie pour cet exécutable.

Il est recommandé de désactiver toutes les règles par défaut du pare-feu et de les réactiver ou de créer des règles personnalisées par rapport aux besoins voulus. Pour une navigation usuelle en HTTP / HTTPS, il faudra par exemple créer une règle similaire à celle décrite ci-dessus, et activer la règle prédéfinie de filtrage sortant pour le DNS.

Enfin, pour autoriser les mises à jour Windows :

- créer une règle personnalisée de filtrage sortant ;
- choisir l'exécutable

  `c:\windows\system32\svchost.exe`

  ;

– dans *Personnalisé*, choisir *Appliquer à ce service* et le service Windows Update ;
– confirmer la boîte de dialogue en choisissant « oui » ;
– choisir le protocole TCP et les ports distants 80 et 443 ;
– choisir d'autoriser la connexion et donner un nom à la nouvelle règle.

Documentation

– Note d'information CERTA-2006-INF-001 du 10 janvier 2006 :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001/
– Portail de la Sécurité Informatique, Guide de configuration, « Activer le pare-feu de Windows Vista » :
http://www.securite-informatique.gouv.fr/gp_article233.html

4 Une protection des données privées plutôt paradoxale !

Des sites Internet proposent des outils et méthodes ou une veille attentive afin de limiter la propagation de données personnelles et privées sur l'Internet.

Certains de ces sites sont cependant douteux lorsque l'on examine d'un peu plus leurs modes de fonctionnement. En effet, il arrive que ces sites lancent une quantité impressionnante de *JavaScript* vers d'autres sites ou installent de nombreux *cookies*. Ces sites se permettent en fait de récolter des données et de les diffuser à de nombreux sites distants à l'insu du visiteur.

Ces méthodes de récolte d'informations peuvent être rapprochées des données enregistrées et transmises par les outils de statistiques de fréquentation des sites comme le rappelait le bulletin d'actualité CERTA-2007-ACT-041 du 12 octobre 2007.

Le CERTA recommande donc de bien prêter attention à la qualité de ces sites qui, en prétendant offrir un service, des outils ou de l'information afin de limiter l'envoi de données personnelles sur l'Internet, en profitent pour subtiliser un maximum d'informations à ces visiteurs et pour les envoyer vers des sites distants. Il est également important de se poser la question de la confiance et de la crédibilité que l'on peut accorder à de tels sites, même si ceux-ci prétendent traiter de sécurité et se soucier des données personnelles.

Documentation

– Bulletin d'actualité CERTA-2007-ACT-041 du 12 octobre 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-041/

5 Le partage de connexions sans fil

Un article publié récemment faisait état d'une petite plaisanterie faite par le propriétaire d'un point d'accès Wi-Fi à son voisin s'y étant connecté à son issu. Le propriétaire a en effet entrepris d'inverser toutes les images des pages demandées au cours d'une navigation par la personne connectée sans son accord. Il fournit également gracieusement le code de manipulation des images sur sa page web publique. Malgré l'aspect « bénin » de cette farce, il est possible d'utiliser le même code pour insérer du code malveillant ou du contenu illicite dans les pages visitées par le voisin. Outre le caractère amusant de cette anecdote, le CERTA tient à rebondir sur ce fait divers pour rappeler certaines recommandations et obligations, que l'on soit client d'un accès Wi-Fi ou fournisseur :

– lors d'une connexion à un point d'accès sans fil ouvert, il est important de garder en tête que l'on ne dispose pas de la maîtrise de ce point d'accès. Le propriétaire peut donc à l'insu des utilisateurs filtrer, enregistrer ou manipuler les données transitant par le réseau. Il suffit d'installer des serveurs proxy ou des passerelles pour rediriger et modifier tout ou partie des requêtes et réponses. Il est donc très important de rester très vigilant quant aux données que l'on va échanger via un réseau ou un point d'accès inconnu ou non maîtrisé ;
– il existe également des obligations pour les fournisseurs de ces points d'accès. Le code des postes et des communications électroniques stipule que les fournisseurs d'accès à des réseaux de communication électronique ont dans l'obligation de conserver les traces des activités des utilisateurs pendant un an glissant. Les mêmes contraintes pourraient être mises en place pour tous les autres acteurs de l'Internet dans un projet de réactualisation du code ;

– les actions entreprises par les personnes externes au réseau ne sont pas toujours maîtrisées. Dans le cas où une personne n'ayant pas d'arrière pensée malveillante laisse son point d'accès ouvert, sa connexion peut être exploitée à de mauvaises fins par des tiers. Il est donc important de retenir que c'est la personne propriétaire de la connexion qui sera la première inquiétée en cas de problème.

Le CERTA tient donc à attirer l'attention sur les risques inhérents à l'utilisation d'un tel type de moyen d'accès à l'Internet et les obligations légales à respecter lors de la mise à disposition de ces moyens d'accès au public.

– Note d'information CERTA-2002-REC-002, « Sécurité des réseaux sans-fil (Wi-Fi) » : http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/
– Portail de la Sécurité Informatique, « Configurer une connexion Wi-Fi en WPA2 avec Windows XP » : http://www.securite-informatique.gouv.fr/gp_article234.html
– Portail de la Sécurité Informatique, « Configurer une connexion Wi-Fi en WPA2 (ou WPA) avec Windows Vista : http://www.securite-informatique.gouv.fr/gp_article194.html

6 La VOIP et le saut de VLAN

6.1 Présentation

Un VLAN (*Virtual Local Area Network*) est un procédé défini dans la norme Ethernet 802.1q, pour isoler logiquement plusieurs réseaux. Il est utilisé entre autres pour diviser un réseau accueillant le trafic de téléphonie sur IP et celui des données classiques. Il permet la mise en place d'une qualité de service (QoS). Il permet aussi, normalement, de sécuriser le réseau en cloisonnant les services et les appareils y accédant. Un saut de VLAN consiste à accéder illégitimement à un flux, par exemple en faisant passer un ordinateur pour un téléphone.

6.2 Méthode

Dans un déploiement de téléphonie sur IP les combinés sont associés à un VLAN et certains modèles utilisent le protocole CDP (*Cisco Discovery Protocol*) pour se déclarer automatiquement. En branchant un ordinateur et en analysant les paquets Ethernet multicast il est possible de trouver l'identifiant de VLAN utilisé (VVID).

En configurant une interface réseau avec le bon VVID il est possible de demander une adresse IP via le DHCP du VLAN. Si elle est obtenue, alors le saut est réussi. En effet une requête DHCP sans avoir spécifié de VLAN positionnerait par défaut la machine dans le réseau de données alors que là, elle est identifiée dans le VLAN de la téléphonie. Ensuite, la liste des machines et services atteignables dépendra de la configuration réseau globale. Dans certain cas, l'absence de séparation ou de contrôle entre les réseaux voix et données permet d'accéder à toute l'infrastructure du réseau testé.

6.3 Conclusion

Plusieurs méthodes pour éviter cette technique de saut sont possibles:

– activer le filtrage par les adresses MAC pour contrôler les appareils se connectant ;
– utiliser le protocole 802.1x, l'accès aux ports d'un *switch* nécessitant alors des identifiants ;
– cloisonner les réseaux, en particulier si des terminaux de téléphonie sont non surveillés et placés dans des locaux publics.

7 Moteurs de recherche : tests de vulnérabilités indirects

Les moteurs de recherche offrent souvent l'occasion d'optimiser les recherches au moyen d'expressions régulières ou de raccourcis. Ces services, forts utiles, peuvent également servir à des fins plus malveillantes, afin de trouver plus rapidement un ensemble de sites indexés et souffrant d'une vulnérabilité commune.

L'expression *Google Hack* a été attribuée à ces opérations dans le moteur de recherche Google. Des sites et des documents proposent logiquement les « formules » adaptées, ainsi que les trucs et astuces pour optimiser les requêtes. Des vulnérabilités sont par exemple régulièrement publiées sur des composants utilisés pour construire un site. Ces vulnérabilités sont exploitables en commençant par trouver les sites utilisant ces composants. Si

l'indexation du site trahit leurs présences, alors ils apparaîtront dans des résultats de moteur de recherche de la forme :

```
search: page_caractéristique_du_module_vulnérable + site:.fr
```

La recherche se limite ici aux seuls sites `.fr`.

Des sites listent ces requêtes. Récemment, l'un d'entre eux propose une interface pour tester à partir de ces requêtes si un domaine ou un site particulier est présent dans les résultats du moteur de recherche. Cette opération peut être vue comme une recherche de vulnérabilités indirecte, où le moteur de recherche sert d'intermédiaire pour identifier les vulnérabilités du site visé.

Comme tout outil lié à la sécurité, ces applications peuvent être considérées comme un danger, ou moyen complémentaire de tester la robustesse de son site. Néanmoins, cette méthode présente différents inconvénients qu'il est important de connaître :

- l'interface s'installe sur le poste de l'utilisateur. Une fois le nom du site cible entré, l'interface génère un très gros volume de requêtes vers le moteur de recherche pour identifier si le site ressort dans le résultat de certains « hacks ». Le moteur de recherche n'est pas complètement passif, et peut considérer qu'il s'agit d'un abus du service rendu, et donc bloquer l'accès au domaine ou au service pour cette adresse. Si cela est gênant pour un particulier, cela le sera encore davantage dans le cas d'un réseau NATé.
- les requêtes sont servies à l'utilisateur à partir des « hacks ». Il s'agit de détection de vulnérabilités exprimées sous forme de signatures. Les résultats retournés sont sujets à des faux-positifs et des faux-négatifs, dont la proportion n'est pas estimée *a priori*.
- les « hacks » effectués ne sont pas directement visibles. Seule l'interprétation du résultat apparaît. Ils ne sont cependant pas tous pertinents.

Ce genre d'interface est dangereux, mais présente l'avantage de confirmer l'importance de mettre à jour et de surveiller les journaux des sites. Ces activités peuvent parfois être visibles en observant les champs `Referer` dans les journaux, ou en testant directement les tentatives dans le moteur de recherche, après avoir considéré les effets de bord que cela peut engendrer.

Cette méthode indirecte est assez pernicieuse, car la recherche de vulnérabilités est effectuée par le moteur de recherche. L'administrateur du site ne peut y faire grand chose, le filtrage de domaine ou d'adresse n'y faisant rien. Il peut éventuellement limiter les indexations faites par un fichier `robots.txt` par exemple.

La meilleure garantie de non compromission de son site réside dans une mise à jour sérieuse des applications utilisées, et une limite raisonnable des modules et autres logiciels atteignables par des requêtes externes (modules des gestionnaires de contenus en particulier).

8 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 14 et le 21 février 2008.

9 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/

10 Rappel des avis émis

Dans la période du 15 au 21 février 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-084 : Vulnérabilité de PCRE
– CERTA-2008-AVI-085 : Vulnérabilité des produits F-Secure
– CERTA-2008-AVI-086 : Multiples vulnérabilités dans Joomla!
– CERTA-2008-AVI-087 : Multiples vulnérabilités dans Adobe Flash Media Server
– CERTA-2008-AVI-088 : Multiples vulnérabilités dans MySQL
– CERTA-2008-AVI-089 : Vulnérabilité dans Cisco Unified Communications Manager
– CERTA-2008-AVI-090 : Vulnérabilité dans HP Ignite-UX et DynRootDisk
– CERTA-2008-AVI-091 : Multiples vulnérabilités dans les équipements Cisco Unified IP Phone
– CERTA-2008-AVI-092 : Multiples vulnérabilités dans Dokeos
– CERTA-2008-AVI-093 : Vulnérabilité dans sendfile sous FreeBSD
– CERTA-2008-AVI-094 : Multiples vulnérabilités dans Claroline
– CERTA-2008-AVI-095 : Vulnérabilité d'IBM DB2
– CERTA-2008-AVI-096 : Vulnérabilités dans Kerio MailServer
– CERTA-2008-AVI-097 : Multiples Vulnérabilités dans Opera
– CERTA-2008-AVI-098 : Multiples vulnérabilités du noyau Linux

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

– CERTA-2007-AVI-435-001 : Vulnérabilité dans HP System Management Homepage
(ajout de la référence CVE)
– CERTA-2008-AVI-056-001 : Vulnérabilité dans la pile IPv6 du projet KAME
(ajout de la référence au bulletin de FreeBSD)

11 Actions suggérées

11.1 Respecter la politique de sécurité

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

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

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

11.2 Concevoir une architecture robuste

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

11.3 Appliquer les correctifs de sécurité

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

11.4 Utiliser un pare-feu

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

11.5 Analyser le réseau

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

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

11.6 Réagir aux incidents de sécurité

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

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

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

11.7 Former et sensibiliser les utilisateurs

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

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

12 Les bulletins d'actualité

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

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

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

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

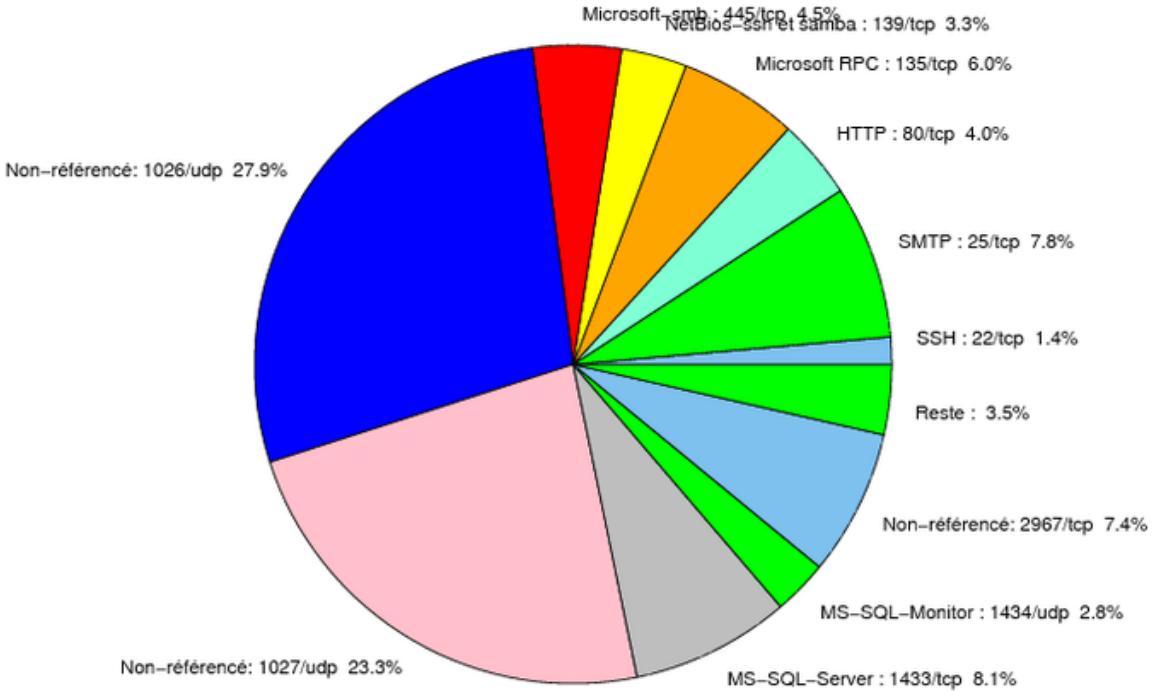

FIG. 1: Répartition relative des ports pour la semaine du 14.02.2008 au 21.02.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
80/tcp	65.85
1026/udp	27.9
1027/udp	23.26
1433/tcp	8.06
25/tcp	7.78
2967/tcp	7.39
135/tcp	6.03
445/tcp	4.52
139/tcp	3.31
1434/udp	2.77
22/tcp	1.37
137/udp	0.96
1080/tcp	0.89
4899/tcp	0.87
21/tcp	0.37
3128/tcp	0.18
2100/tcp	0.11
111/tcp	0.05
143/tcp	0.03

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

22 février 2008 version initiale.