Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2007
N° CERTA-2007-ACT-028

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-28

Gestion du document

Référence	CERTA-2007-ACT-028
Titre	Bulletin d'actualité 2007-28
Date de la première version	13 juillet 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-028.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-028/

1 Problème de modération des forums et autres

Le CERTA constate que les forums et les applications à contenu interactif (tels que les livres d'or par exemple) sont de plus en plus pollués par des messages à caractère publicitaire pour un produit dont la vente est encadrée, voire interdite ou présentant un caractère diffamatoire, ou d'incitation à la haine, etc. Concrètement, des personnes malintentionnées utilisent toute application web leur permettant de déposer un message, et font de la publicité pour des produits (pornographie, médicament, placement, crédit, diplôme, papiers d'identité, jeu d'argent, contrefaçons de logiciels, etc.) :

- les messages déposés peuvent poser des problèmes juridiques au responsable du site. Pour ce dernier point, vous pouvez lire le document suivant :
  http://www.sante.gouv.fr/htm/pointsur/qualite/ventemed.htm
- la quantité de messages douteux déposés est telle que le contenu légitime du forum en devient illisible ;
- les messages déposés peuvent porter atteinte à l'image du site.

Lors de la mise en place d'un forum ou d'une application comparable, il est recommandé d'envisager la mise en place d'un mécanisme de modération, avec les moyens humains suffisants. Dans certains cas, il est possible

de mettre en place des restrictions, telles que l'obligation de posséder un compte (dont l' ouverture est soumise à l'approbation des modérateurs) avant de pouvoir poster. Il est également important de fermer les applications laissées à l'abandon.

Il est toujours possible de s'aider des moteurs de recherche avec, pour mots-clefs, de nom de domaine et quelques mots spécifiques couramment vus dans les spams.

Il est à noter que l'installation par défaut de certains applicatifs web entraîne parfois la mise en place d'un forum, souvent à l'insu du webmestre. C'est la raison pour laquelle il est important d'être vigilant avec tous ces produits, de bien lire la documentation avant toute installation, et de vérifier que seul le strict nécessaire a été installé.

2 Lettres d'information

Certaines sociétés ou autre organismes proposent de s'abonner à une liste de diffusion pour recevoir des lettres d'information. Il est important que l'internaute qui déciderait de s'abonner à de telles listes soit conscient de risques liés à certains procédés de diffusion des lettres d'information.

Toutes les sociétés ou organismes qui souhaitent publier une lettre d'information n'ont pas obligatoirement un service informatique capable de leur offrir cette prestation. Elles font parfois appel à des entreprises spécialisées. Certaines de ces entreprises utilisent une technologie qui présente des dangers pour les internautes. Le procédé est le suivant :

- supposons que l'on souhaite faire une lettre d'information renvoyant sur le site http://www.certa.ssi.gouv.fr. Par exemple sur les pages suivantes :
  http://certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html
  http://certa.ssi.gouv.fr/site/CERTA-2005-INF-002/index.html
  http://certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- L'entreprise spécialisée dans l'émission de lettres d'information, va envoyer un courrier électronique qui au lieu de pointer directement sur les pages ci-dessus va envoyer sur des pages intermédiaires sous la forme d'URL compliquées ou n'apparait pas le nom du document comme par exemple :
  http://toto.net/r5.aspx?GV1=[chaîne incompréhensible]
  http://titi.net/r/?E=[chaîne incompréhensible]
  (toto et titi remplacent des noms de domaines fréquemmement recontrés dans ce genre de publipostage).

Le CERTA reçoit régulièrement des signalements relatifs à de tels courriers.

Quels sont les problèmes posés par ceux-ci :

- afin de consulter un document sur le site sur lequel il s'est abonné, l'internaute est redirigé vers une autre page ;
- la consultation de cette page est probablement journalisée. Le fait pour un internaute d'accepter que ses consultations soient journalisées par le service auquel il s'abonne n'entraîne pas obligatoirement son adhésion à la journalisation par un tiers ;
- l'internaute ne peut pas vérifier par lui-même avant d'avoir cliqué sur le lien qu'il sera bien redirigé vers le site objet de son abonnement, ouvrant ainsi la voie à :
  - des opérations de filoutage utilisant une technologie similaire (se faisant passer pour des lettres d'information envoyées par une société spécialisée selon ce procédé)
  - des redirections vers des pages malveillantes

Ce ne sont pas les entreprises spécialisées qui présentent en tant que telles un risque mais plutôt la méthode employée (redirection inutile pour l'internaute) dans la mesure ou l'internaute est habitué à des procédés dangereux qui peuvent être réutilisés dans des opérations de filoutage.

Le CERTA recommande

- aux internautes qui souhaitent s'abonner à des listes de diffusion :
  - de s'informer sur le procédé utilisé pour la diffusion de la liste. La consultation d'une archive de la liste de diffusion permet de vérifier la façon dont les liens sont construits. Un lien direct sur la page sera toujours considéré comme plus sûr. Une fois informé, l'internaute peut décider en toute connaissance.
  - d'utiliser des adresses jetables pour l'abonnement à de telles listes, de préférence une pour chaque liste
  - de nettoyer et d'interdire les cookies avant de cliquer sur un lien de ce type

  - de s'assurer que les scripts (Java, JavaScript, ActiveX voire swf) sont bien désactivés dans le logiciel de navigation avant de suivre un lien de ce type
- aux responsables SSI :
  - de continuer à signaler au CERTA de tels envois faisant l'objet de leur étonnement
- aux administrations qui souhaiteraient faire appel à des prestataires pour l'envoi d'une lettre d'information :
  - de s'assurer que la technologie employée soit la plus transparente possible pour les internautes ;
  - de s'assurer que la technologie employée ne donne pas à l'internaute de mauvaises habitudes le rendant plus vulnérable à des opérations de filoutage.

3 Storm Worm

Les bonnes pratiques citées dans la note sur les canulars CERTA-2000-INF-005 restent d'actualité. Ceci se confirme régulièrement, à chaque campagne de pourriels. Certaines sont cependant plus médiatisées que d'autres. Un courrier électronique invitant à contourner la politique de sécurité et à installer un prétendu *patch* sans passer par la chaîne fonctionnelle SSI a été signalé par plusieurs de nos correspondants. La technique n'a rien de nouveau, il s'agit de convaincre l'internaute sous divers prétextes à exécuter un fichier malveillant.

Cette campagne de pourriels signalée prétexte la découverte d'un code malveillant sur la machine du destinataire et l'incite à cliquer sur un lien afin de mettre à jour son ordinateur. Dans sa version actuelle, le pourriel a des sujets de type « Virus detected ! », «Malware Alert ! », «Spyware Detected ! » ou « Worm Activity Detected ! » et est apparemment émis par le « Customer Support Center ». Cette nouvelle diffusion de spam appelant à mettre à jour sa machine (avec un exécutable dénommé Patch.exe) a débuté de façon opportune au moment où Microsoft publiait ses mises à jour mensuelles le 10 juillet 2007.

En cliquant sur le lien l'utilisateur visite un site qui tente d'installer un code malveillant par diverses failles à l'aide d'un code javascript. Si le javascript est désactivé le site propose simplement le fichier en téléchargement direct.

Le CERTA rappelle à cette occasion les points essentiels suivants :

- ne pas faire confiance dans le champ `From:` des messages ;
- ne pas cliquer de façon inconsidérée sur des liens insérés dans les messages ;
- désactiver le javascript par défaut ;
- les mises à jour de sécurité ne sont jamais diffusées de cette manière. Les consignes de mises à jour sont annoncées par l'équipe de soutien informatique ou par le responsable de sécurité.

4 Utilisation du DNS pour orienter des attaques

La presse spécialisée parle d'attaques par `DNS pinning`. De quoi s'agit-il ?

L'objectif de ces attaques consiste à atteindre des machines normalement inaccessibles, en utilisant le navigateur de l'utilisateur comme relais après avoir faussé les réponses du DNS.

Certaines classes d'attaques peuvent s'appuyer sur le protocole en charge de la correspondance entre noms de domaine et adresse réseau IP : le DNS (*Domain Name System*). Elles ne sont pas toutes très récentes, car certaines étaient déjà mentionnées publiquement, comme par l'Université américaine de Princeton en 1996.

- Tricher avec le DNS, « DNS Attack Scenario » :
  http://www.cs.princeton.edu/sip/news/dns-scenario.html
- Tricher avec le DNS et l'aide de Java, « DNS-Based Attack on Java » :
  http://www.cs.princeton.edu/sip/news/dns-spoof.html

Parmi ces attaques, certaines exploitent une propriété particulière des navigateurs, nommée `DNS pinning`. La réponse DNS à une requête portant sur un nom de domaine est une adresse IP, associée à une durée d'expiration. Tant que la durée n'est pas révolue, il n'est pas nécessaire de faire une nouvelle requête. L'adresse IP est considérée comme valide. Après l'expiration, l'adresse IP n'est plus garantie.

Le `DNS pinning` est une propriété de plusieurs navigateurs, qui consiste à garder en « mémoire » la correspondance entre le nom de domaine et l'adresse IP, au-delà de la date d'expiration.

Pour éclairer quelques utilisations malveillantes, voici un scénario fréquemment cité :

1° un utilisateur suit, éventuellement à son insu, un lien vers l'adresse http://SITE_MALVEILLANT.fr.tm

2° le navigateur de l'utilisateur va tout d'abord résoudre le nom de domaine SITE_MALVEILLANT.fr.tm, en envoyant une requête DNS. A la condition où aucun cache ne répond préalablement, c'est le serveur DNS de la personne malveillante qui lui répond, avec une durée d'expiration (*Time to Live*, TTL) de α secondes. Elle lui retourne l'adresse IP du serveur malveillant : W.X.Y.Z. Il peut donc s'y connecter et récupérer la page demandée.

3° la page Web récupérée contient un script Javascript qui effectue, après β secondes ($\beta > \alpha$) les opérations suivantes :

- il utilise l'objet Javascript `XMLHttpRequest` pour forcer le navigateur à charge une autre page sur le site http://SITE_MALVEILLANT.fr.tm.
- comme le TTL a expiré, le script contourne le `DNS pinning`, et oblige le navigateur à effectuer de nouveau une requête DNS.
- cette fois, le serveur DNS malveillant retourne l'adresse IP A.B.C.D du site normalement pas accessible http://MON_INTRANET, par exemple une adresse non routable.

4° le navigateur essaie donc de charger la nouvelle page, non pas à l'adresse W.X.Y.Z, mais à l'adresse A.B.C.D, en croyant toujours communiquer avec http://SITE_MALVEILLANT.fr.tm (champ `Host`).

5° le navigateur reçoit des données du site http://MON_INTRANET, que le script de l'attaquant peut exploiter, grâce à la propriété de réponse de l'objet `XMLHttpRequest` (ou propriété `SOP : same origin policy`). La communication est facilitée par le `DNS pinning` qui maintient alors les correspondances entre adresses.

6° le script chargé à l'étape 3 peut transférer les données capturées vers un site distant.

Dans le cas précédemment cité, la machine de l'utilisateur sert de relais pour lancer des attaques de manière transparente contre le site cible, ici celui de MON_INTRANET.

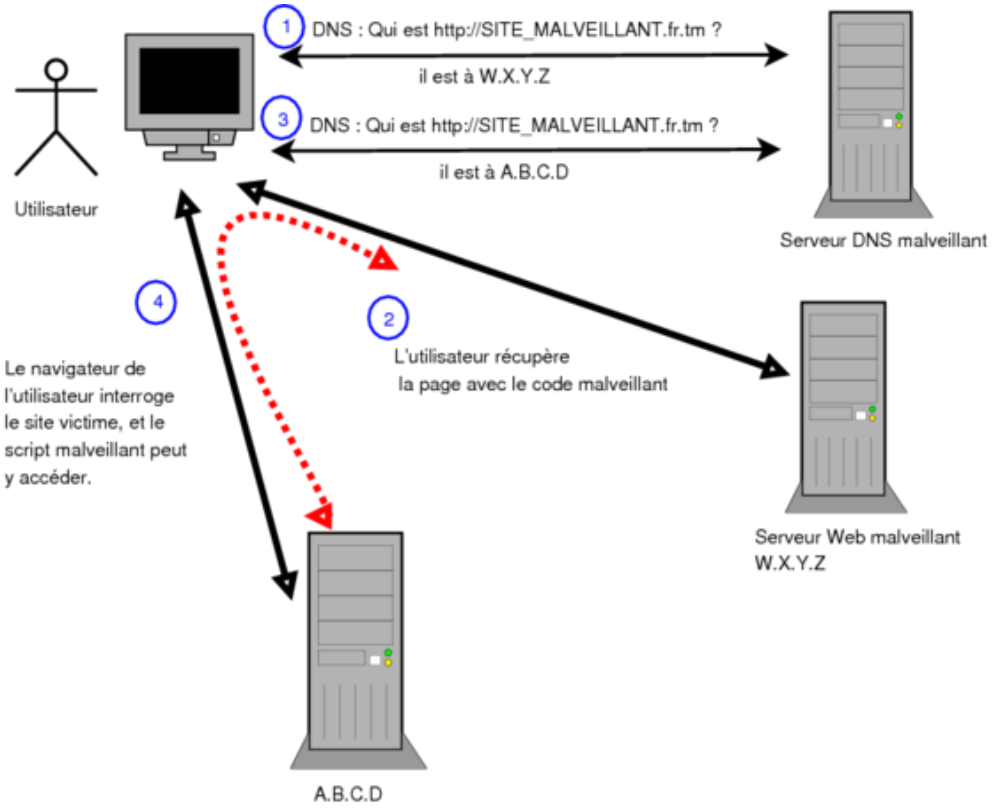

FIG. 1: Schéma illustratif du scénario mentionné

Ces attaques sont également envisageables contre des serveurs Web intermédiaires, ou `proxy`. Tout utilisateur de ce service pour se connecter à l'Internet est alors une victime potentielle.

Quels sont les intérêts pour une personne malveillante ? Cela lui permet d'accéder et éventuellement de modifier les données d'un site que l'utilisateur peut atteindre, ou la configuration d'un équipement :

– ce peut être le cas d'un utilisateur dans un LAN. L'attaquant peut alors naviguer sur des sites intranet du

LAN ;
- comme le scénario précédent, il peut profiter d'autres techniques liées à Javascript, et mentionnées dans des précédents bulletins d'actualité, pour balayer des plages d'adresses, et récupérer des informations sur les machines du LAN ;
- si l'utilisateur est chez lui, connecté par un modem/routeur à l'internet, cette technique permet à la personne malveillante d'accéder à l'interface d'administration, qui est en théorie accessible depuis l'interface réseau interne uniquement.
- l'attaquant peut également interagir avec un serveur sur la machine de l'utilisateur, configuré pour n'accepter que des connexions locales (127.0.0.1 par exemple).

Ces classes d'attaques sont d'autant plus envisageables que plusieurs codes circulant déjà sur l'Internet en simplifient la mise en œuvre.

4.1 Les recommandations du CERTA

- Pour les utilisateurs : plusieurs mesures peuvent être prises pour limiter les risques. La plus évidente correspond à un leitmotiv des bulletins d'actualité du CERTA : il ne faut activer le JavaScript que ponctuellement, quand cela est nécessaire, et sur des sites de confiance. Dans le scénario précédent, l'attaque aurait échoué si l'utilisateur avait désactivé le Javascript avant de se rendre (par accident ?) sur le site http://SITE_MALVEILLANT.fr.tm. Afin de mieux se prémunir contre ce type d'attaques, il est important de désactiver par défaut les autres langages de script, comme Java, ActiveX, ou même FLASH.

  Il est vivement recommandé, quand on est connecté à l'Internet par un modem/routeur, de changer le plan d'adressage interne, ainsi que les identifiants fournis par défaut. Le fait que la page d'administration soit accessible par l'interface réseau interne n'est pas une mesure suffisante.

  L'attaque est possible, car le navigateur garde en cache la résolution de l'adresse, pour la durée de la session HTTP, et malgré le champ TTL. Ainsi, dans l'étape 6, le navigateur continue à associer le site malveillant à l'adresse A.B.C.D. Firefox et Internet Explorer partagent cette propriété. Celle-ci n'est pas toujours configurable dans les navigateurs.
- Pour l'administrateur du réseau :
  - il est important de cloisonner avec précaution les vues pour la résolution de noms. Si un serveur DNS externe retourne une adresse IP dont le serveur est en charge (primaire), ou une adresse IP correspondant à une plage d'adresse IP privées, la réponse doit être rejetée.
  - il est important de vérifier les politiques de filtrage mises en place. Ces attaques fonctionnent, dans le cas d'un proxy, contre tous les sites internes accessibles par le proxy. Le proxy pour les connexions sortantes Web ne doit pas servir pour accéder aux serveurs internes. Un filtrage réseau permet de renforcer cette politique.
  - il est important de filtrer correctement les connexions sortantes. Les flux initiés par les postes clients doivent être restreints et contrôlés.
  - il peut être envisagé d'augmenter la durée de cache des requêtes DNS au niveau du proxy.

5 Sur la cohabitation de deux navigateurs sur un poste de travail

Lors de son installation sur Windows, le navigateur de Mozilla s'enregistre dans la base de registres comme programme responsable du traitement des URL préfixées par "FirefoxURL:".

Cette clé est visible par la méthode suivante :
- Dans le panneau de démarrage, choisir 'Exécuter' ;
- Taper 'regedit' et valider ;
- Dans la fenêtre de l'Editeur du Registre qui s'ouvre, choisir 'Edition', puis 'Rechercher...' ;
- Chercher la chaîne de caractères `FirefoxURL`.

Sous XP, et dans une installation par défaut, la clé en question se présente comme suit :

```
[HKEY_CLASSES_ROOT\FirefoxURL\shell\open\command\]
C:\PROGRA~1\MOZILL~2\FIREFOX.EXE -url "%1" -requestPending
```

Lorsque qu'Internet Explorer rencontre sur une addresse de ce type, il recherche dans la base de registre l'application associée et ouvre donc Firefox en lui passant l'adresse en argument. Ainsi, un clic sur un lien pointant vers « FirefoxURL://adresse.fr » exécuterait la commande :

```
C:\PROGRA~1\MOZILL~2\FIREFOX.EXE -url
```

```
"firefoxurl://addresse.fr" -requestPending
```

Le problème vient du fait que l'adresse passée en paramètre à firefox n'est contrôlée à aucune moment. Au lieu de mettre « adresse.fr », il est possible d'y joindre des arguments, et l'ensemble sera alors interprété par firefox.exe.

Il devient donc possible de modifier la liste des arguments transmis. Certaines options permettant de passer en ligne de commande du code JavaScript dans un « contexte de confiance », il est alors possible d'utiliser ce langage pour exécuter tout type de commande et corrompre la machine.

5.1 Les recommandations du CERTA

Les premières publications de cette vulnérabilité accusaient Internet Explorer. Cependant, les détails fournis par la bibliothèque MSDN sont explicites, et la manipulation du *Protocol Handler* ne contrôle pas la chaîne de caractères transmise. La bibliothèque `urlmon.dll` n'est pas non plus solicitée par Firefox.

A la date de rédaction de cet article, il semblerait donc que le problème provienne bien de Firefox. Quoi qu'il en soit, cette vulnérabilité est intéressante, car elle montre une interaction méconnue et forcée entre deux applications.

Pour contourner provisoirement ce type d'attaque ciblant principalement Internet Explorer il faut donc désactiver le Javascript dans Firefox ! Cela confirme les propos régulièrement mentionnés dans ce bulletin, et qui prônent de désactiver par défaut le JavaScript, pour ne l'utiliser que ponctuellement, pour des sites de confiance.

En complément, il est préférable de désactiver les clés de registre impliquées, en tapant dans l'invite de commandes :

```
reg delete HKCR\FirefoxURL /f
reg delete HKCR\Firefox.URL /f
```

Enfin, il semblerait que certaines extensions comme `NoScript` pour Firefox limitent les risques d'exploitation de cette vulnérabilité. Leur usage est cependant un contournement provisoire en attendant un correctif officiel.

6 Sécurité de Windows et Computer Security Idendifier

Chaque système d'exploitation Windows installé sur une machine dispose d'un identifiant unique tiré aléatoirement lors de son installation. Cet identifiant ou `SID` (`computer Security IDentifier`) permet, par exemple, d'identifier de façon unique une machine dans un environnement réseau de type « groupe de travail ».

Il est fréquent lors du déploiement de parc informatique d'utiliser des techniques de clonage de machine. Ainsi, à partir d'une machine qualifiée de « Maître » on pourra créer une image qui sera déployée sur toutes les machines du réseau. Or, dans ce cas (clonage), toutes les machines cibles auront le même `SID` ; c'est le propre d'un clone.

Ceci pose un problème car la sécurité (droits d'accès aux fichiers partagés, identification des utilisateurs...) dans un groupe de travail Windows est basée sur ces `SID` et l'identifiant relatif de l'utilisateur ou `RID` (`Relative IDentifier`.

Par exemple, dans un réseau composé de clones, il est impossible de différencier un utilisateur `A` sur une machine `M1` d'un utilisateur `A` sur une machine `M2` puisque `M1` et `M2` ont le même `SID`. Ceci est d'autant plus problématique que les `RID` (identifiants locaux des utilisateurs sur une machine) sont calculés en incrémentant un nombre fixe tiré à l'installation d'une machine. Ainsi dans la mesure où les machines sont clônées leur `RID` initial est le même et leur `SID` également. Une utilisatrice Alice disposera du couple `RID1/SID1` pour s'identifier sur une machine `M1` alors que sur une machine `M2` ce couple `RID1/SID1` sera attribué à Bob. S'il existe des partages réseaux, Bob sera vu comme Alice sur M1 et réciproquement.

Recommandations

Les points suivants permettent de corriger le problème :

- introduire des domaines Windows, afin que la sécurité des ressources ne repose pas sur ce système `SID` ;
- il suffit de renommer la machine dans les propriét'es du « Poste de Travail » pour que le système assigne un nouveau `SID` à la machine ;
- Microsoft met à disposition un outil nommé `NewSID` permettant de modifier le `SID` d'une machine et certaines solutions de clonage proposent un changement de `SID` en option.
  http://www.microsoft.com/france/technet/sysinternals/security/newsid.mspx

7 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 05 et le 12 juillet 2007.

8 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
- Note d'information sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
- Note d'information sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html
- 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 CERTA-2006-INF-006, Risques associés aux clés USB :
  http://www.certa.ssi.gouv.f r/site/CERTA-2000-INF-006/
- Note d'information du CERTA CERTA-2006-INF-009 sur les outils d'indexation et de recherche :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA CERTA-2007-INF-001 sur la gestion des noms de domaine :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
- Note d'information sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002

9 Rappel des avis émis

Dans la période du 06 au 12 juillet 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-285 : Vulnérabilité de Java Web Start
- CERTA-2007-AVI-286 : Vulnérabilité dans HP Instant Support - Driver Check
- CERTA-2007-AVI-287 : Vulnérabilité dans Citrix Presentation Server Client
- CERTA-2007-AVI-288 : Multiples vulnérabilités dans les produits SAP
- CERTA-2007-AVI-289 : Vulnérabilité dans Winpcap
- CERTA-2007-AVI-290 : Vulnérabilités dans GIMP
- CERTA-2007-AVI-291 : Vulnérabilités dans Microsoft Excel
- CERTA-2007-AVI-292 : Vulnérabilité de Microsoft Office Publisher 2007
- CERTA-2007-AVI-293 : Vulnérabilité du pare-feu Microsoft Vista
- CERTA-2007-AVI-294 : Vulnérabilités de Microsoft Active Directory
- CERTA-2007-AVI-295 : Vulnérabilités dans Microsoft NET Framework
- CERTA-2007-AVI-296 : Vulnérabilité dans Microsoft Internet Information Services (IIS)
- CERTA-2007-AVI-297 : Multiples vulnérabiliés du Common Management Agent (CMA) de McAfee
- CERTA-2007-AVI-298 : Vulnérabilité dans 3Com TippingPoint IPS
- CERTA-2007-AVI-299 : Vulnérabilités dans Adobe Flash Player
- CERTA-2007-AVI-300 : Vulnérabilités dans Drupal
- CERTA-2007-AVI-301 : Vulnérabilité dans la machine virtuelle Java de Sun

– CERTA-2007-AVI-302 : Vulnérabilité dans Sun Java Secure Socket Extension
– CERTA-2007-AVI-304 : Vulnérabilité dans Cisco Unified Communications Manager
– CERTA-2007-AVI-305 : Vulnérabilité dans AIX d'IBM
– CERTA-2007-AVI-306 : Vulnérabilité de ClamAV
– CERTA-2007-AVI-307 : Multiples vulnérabilités de AVG Antivirus
– CERTA-2007-AVI-308 : Multiples vulnérabilités dans Apple QuickTime
– CERTA-2007-AVI-309 : Multiples vulnérabilités des produits Symantec
– CERTA-2007-AVI-310 : Vulnérabilité dans la commande rcp sous Sun Solaris

10 Actions suggérées

10.1 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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

11 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.

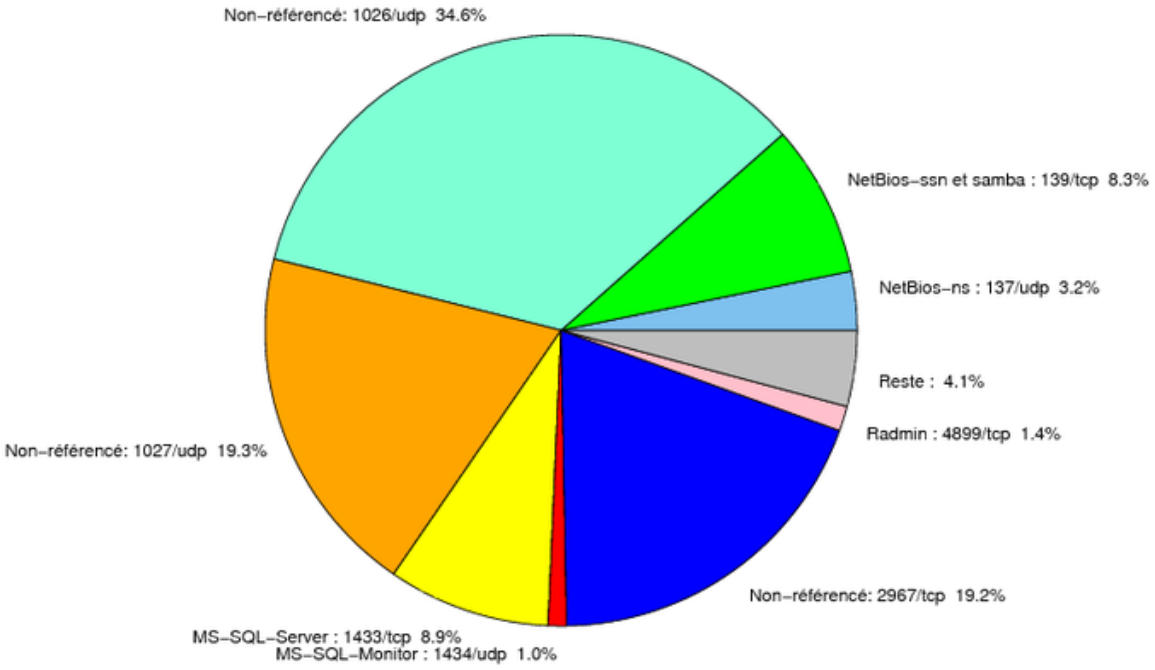

FIG. 2: Répartition relative des ports pour la semaine du 05.07.2007 au 12.07.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE

2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

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

port	pourcentage
1026/udp	34.57
1027/udp	19.3
2967/tcp	19.19
1433/tcp	8.87
139/tcp	8.32
137/udp	3.21
4899/tcp	1.35
1434/udp	1
22/tcp	0.95
1080/tcp	0.74
21/tcp	0.61
3128/tcp	0.37
3306/tcp	0.23
443/tcp	0.2
80/tcp	0.18
3389/tcp	0.15
11768/tcp	0.1
15118/tcp	0.06
9898/tcp	0.03
5554/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

13 juillet 2007 version initiale.