Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mai 2008
N° CERTA-2008-ACT-022

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-22

Gestion du document

Référence	CERTA-2008-ACT-022
Titre	Bulletin d'actualité 2008-22
Date de la première version	30 mai 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-022.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-022/

1 Les incidents de la semaine

1.1 Quand l'historique conduit à l'incident

Cette semaine, le CERTA a traité un incident impliquant une machine infectée par des codes malveillants. Cette machine provient du réseau d'une administration. Les raisons ayant facilité cette compromission sont multiples : correctifs de sécurité non-appliqués, base de signatures d'antivirus obsolète, etc. Et pourtant, loin d'être à l'abandon, cette machine était utilisée pour naviguer sur l'Internet ou lire des courriers électroniques externes, sans aucun filtrage.

Dans un traitement d'incident, il est essentiel de connaître le contexte dans lequel se trouvait la machine. Dans le cadre de cette compromission, le CERTA a appris que non seulement toutes les machines connectées au réseau n'étaient pas à jour mais également qu'aucun filtrage en amont n'était réalisé. Il n'y avait aucune segmentation du réseau : des machines en libre service étaient connectées sur le réseau bureautique à protéger de l'administration. Historiquement, toutes ces machines, avec leurs rôles et besoins différents, sont venues se greffer au fur et à mesure sur le réseau existant sans que l'architecture du réseau ne soit gérée voire repensée.

Le CERTA rappelle que l'application des correctifs de sécurité permet d'éviter que d'anciennes vulnérabilités devenues triviales à exploiter compromettent tout un système d'information. Les logiciels de sécurité qui ne sont

pas maintenus à jour et qui n'ont pas une base de signatures récente sont parfaitement inutiles et peuvent même affaiblir la sécurité globale : comme tout logiciel, ils font l'objet de vulnérabilités. Le CERTA rappelle également qu'il est préférable, dans la mesure du possible, que les réseaux ayant des besoins de sécurité différents soient segmentés.

2 Injections SQL et vulnérabilités Adobe Flash

2.1 Les faits

Des éditeurs d'antivirus ont mentionné dans la soirée du 27 mai 2008 l'exploitation massive d'une vulnérabilité non corrigée et jusqu'alors inconnue du lecteur Adobe Flash. Le CERTA revient dans cet article sur l'événement et les constatations qui ont pu être faites.

Ces activités malveillantes peuvent se découper en phases distinctes : des injections MsSQL massives dans des sites Web vulnérables redirigent les internautes naviguant sur leurs pages vers d'autres sites malveillants. Ces derniers exploitent des vulnérabilités du lecteur Adobe Flash afin de compromettre la machine par le téléchargement et l'installation d'exécutables.

2.2 Injections SQL

Les tentatives d'injections SQL dans des serveurs Web sont courantes et le CERTA fait état dans des bulletins d'actualité précédents de plusieurs cas de compromissions de sites Web par cette méthode. En 2008 :

- Bulletin d'actualité CERTA-2008-ACT-003 du 18 janvier 2008, « Les rumeurs d'activités malveillantes » : http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-003.pdf
- Bulletin d'actualité CERTA-2008-ACT-012 du 21 mars 2008, « Attaques massives de type *SQL Injection* » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-012.pdf
- Bulletin d'actualité CERTA-2008-ACT-017 du 25 avril 2008, « Incidents de la semaine : des compromissions successives » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-017.pdf

Ces dernières semaines, de nombreux sites se sont vus ajouter à leur contenu d'origine des balises `<script>` illégitimes. Ces ajouts ont été réalisés par l'exploitation de vulnérabilités liées aux pages ASP des sites ou par le biais de sites tiers compromis partageant la même base de données. Ces vulnérabilités consistent en un mauvais contrôle des paramètres fournis au serveur, ce qui permet aux attaquants d'exécuter des requêtes MsSQL avec les droits du serveur Web.

Dans le cas présent, ces requêtes ajoutent à tous les champs dans lesquels elles peuvent écrire au format texte une balise `<script>` qui pourra être en principe interprétée par le navigateur du visiteur à son insu. La méthode actuelle d'exploitation de cette vulnérabilité présente l'effet de bord suivant : il arrive que des balises malveillantes se retrouvent dans des sections où les scripts ne sont pas interprétés, comme dans les titres de pages par exemple. Donc, s'il y a apparition de texte étrange tel que `<script src=` ou `<iframe src=` lors de la navigation, cela peut indiquer que le site est compromis.

Les injections pointent vers un fichier JavaScript, lui-même appelant une page Web. Celle-ci contient un fichier au format SWF qui charge un autre fichier SWF malveillant.

2.3 Vulnérabilités Flash

Le CERTA a analysé, dès les premières annonces, des échantillons de codes mais n'a pas constaté l'exploitation d'une nouvelle vulnérabilité. La plus récente rencontrée par le CERTA concerne la vulnérabilité trouvée par des chercheurs d'IBM ISS décrite dans le CVE-2007-0071 (CERTA-2008-AVI-197). Il s'agit d'une mauvaise manipulation associée à la structure `DefineSceneAndFrameLabelData` (identifiant de valeur 86 - 0x56 en hexadécimal) d'un fichier SWF, et en particulier à la gestion des nombres de « scènes » annoncés dans le fichier.

Le code exécuté est lui stocké dans l'enregistrement `DEFINEBITS` qui est normalement utilisé pour stocker des données image (JPEG).

```
[HEADER]        File version: 9
[HEADER]        File size: 1541
[HEADER]        Frame rate: 12.000000
[HEADER]        Frame count: 771
```

```
[HEADER]        Movie width: 1.00
[HEADER]        Movie height: 1.00
[045]          4         4 FILEATTRIBUTES
[006]       1024      1028 DEFINEBITS defines id 0682
                 bbox [0.00, 0.00, 0.00, 0.00]
[056]         40      1068 SCENEDESCRIPTION
[009]          3      1071 SETBACKGROUNDCOLOR (ff/ff/ff)
[056]         12      1083 SCENEDESCRIPTION
...
```

En l'état, le CERTA n'est donc pas au courant d'autres vulnérabilités exploitées. Les éditeurs d'antivirus à l'origine du bruit médiatique semblent eux se rétracter et confirmer dans l'ensemble que l'annonce d'un « 0-day » était prématurée.

2.4 Recommandations

2.4.1 Pour les administrateurs de sites Web

Chercher s'il y a compromission

Il faut vérifier que les sites Web ne sont pas compromis : les traces dans les journaux de connexions et dans la base de données sont explicites. Des tentatives d'injection peuvent ressembler à ce qui suit :

```
AAAA-MM-JJ hh:mm:ss /repertoire/page.asp?id=z%20ANd%20char(124)... - 200
AAAA-MM-JJ hh:mm:ss /repertoire/page.asp?id=z%27%20ANd%20char(124)... - 200
```

Une chaîne de caractères est fournie en argument à « id » à la place d'un entier.

Dans la base de données, la présence des chaînes de caractères `<script src` et/ou `<iframe src` dans des champs où elles ne devraient pas se trouver (titres d'articles, numéros de téléphones, etc.) peut permettre de révéler une compromission. Ces chaînes peuvent cependant être obfusquées et se manifestent alors sous la forme d'une chaîne peu lisible et commune à plusieurs tables.

Actions à envisager en cas de compromission

Si un site a été compromis, il est impératif de corriger les vulnérabilités en mettant en place un contrôle plus rigoureux des paramètres. Il faut également nettoyer la base de données. Une solution temporaire peut consister à utiliser un *reverse proxy* afin de filtrer les requêtes Web entrantes (caractères spéciaux, chaînes de type `char()`, etc.).

2.4.2 Pour les utilisateurs

Désactiver les codes dynamiques

Dans le cas présent, le fichier Flash malveillant est téléchargé après exécution par le navigateur d'un code JavaScript. De manière générale, il est préférable de ne pas activer l'interprétation de ces codes (Javascript et Flash) par défaut sur un navigateur. Le bulletin d'actualité CERTA-2008-ACT-016 évoque à cette occasion la richesse de fonctionnalités du format d'une application Flash, et en particulier, depuis la version 9, la mise en oeuvre de ressources réseau de type *socket*.

Mettre à jour, extensions et greffons compris

Il faut vérifier que la version d'Adobe Flash Player utilisée sous Windows est bien celle à jour, i.e. `9.0.124.0`. Ce test n'est pas si simple car un système peut contenir plusieurs instances. Par exemple, un système Windows peut avoir un `Adobe Flash Player ActiveX` et un `Adobe Flash Player plug-in`. Le premier composant n'est utilisé que par Internet Explorer et tout autre logiciel s'appuyant sur les composants du navigateur. Le second, en revanche, est exigé par tout autre navigateur fonctionnant avec des modules, comme Mozilla Firefox ou Opera. Les mises à jour de ses deux composants sont indépendantes et ne sont pas nécessairement automatiques.

Dans le cas où plusieurs navigateurs sont installés sur une machine, il faut donc vérifier pour chacun d'eux la version de Flash Player installée. Une méthode consiste à se rendre avec chacun d'eux sur le site d'Adobe pour vérifier la configuration et télécharger si besoin la dernière disponible :

- Portail de la Sécurité Informatique, « Exploitation massive d'une vulnérabilité liée à la technologie Flash » :
  http://www.securite-informatique.gouv.fr/
- Installation d'Adobe Flash Player :
  http://www.adobe.com/go/getflashplayer
- Vérification de la version Adobe Flash Player utilisée (JavaScript nécessaire) :
  http://kb.adobe.com/selfservice/viewContent.do?externalId=tn_15507&slideId=1
- Lien direct du SWF Adobe de vérification de version :
  http://www.adobe.com/support/flash/ts/documents/test_version/flashplayerversion.swf

Utiliser par défaut un compte aux droits limités

En cas d'infection, l'utilisation d'un compte aux droits limités empêche autant que possible certaines actions du code malveillant. Il faut donc restreindre l'usage d'un compte avec des droits administrateur aux seules tâches de maintenance et d'installation.

2.5 Documentation

- Avis CERTA-2008-AVI-197 du 09 avril 2008, « Vulnérabilités dans Adobe Flash Player » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-197/
- Bulletin d'actualité CERTA-2008-ACT-016 du 18 avril 2008, « Vulnérabilité dans le lecteur Flash » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-016.pdf
- Bulletin de sécurité Adobe APSB08-11 publié le 08 avril 2008 :
  http://www.adobe.com/support/security/bulletins/apsb08-11.html
- Documentation détaillant les spécificités du format SWF :
  http://www.adobe.com/devnet/swf/pdf/swf_file_format_spec_v9.pdf
- Historique des versions de Flash Player :
  http://fpdownload.macromedia.com/get/flashplayer/installers/archive/fp9_archive.zip

3 Les PABX, des machines presque comme les autres

Le but de cet article est d'essayer de faire un parallèle entre les PABX (*Private Automatic Branch eXchange*) et les autres équipements d'un système d'information. Nous allons tenter de montrer que les bonnes pratiques de sécurité sont bien souvent applicables, et cela malgré leurs spécificités.

3.1 Le PABX au sein du système d'information

Les PABX, ou *autocommutateurs privés*, servent à relier un réseau téléphonique local au réseau public. Ils offrent des fonctionnalités telles que la gestion de l'annuaire, les conférences ou les renvois d'appels et ils intègrent maintenant le protocole de voix sur IP ou « VoIP ». Ce sont des machines équipées de processeurs, de disques durs et de logiciels qui peuvent être connectés aux réseaux téléphoniques et informatiques, et cela par un lien avec ou sans fil (DECT *(Digital Enhanced Cordless Telephone)*, WiFi). Les informations confidentielles qui y sont stockées ou qui y transitent, son coût de fonctionnement (communications) et surtout son aspect vital pour le bon fonctionnement d'une majorité des entreprises en font une infrastructure critique des systèmes d'information.

Les PABX étant à cheval entre l'univers de la téléphonie et celui des réseaux informatiques, ils cumulent, pour les attaquants, les attraits de ces deux mondes et ont en plus l'intérêt d'être une passerelle entre les deux. Au niveau téléphonique, ils permettent, entre autres, des communications aux frais de l'entreprise, l'anonymisation de la provenance d'appel et l'écoute des conversations ou des boites vocales. En quelques jours, la facture pour des communications illégitimes peut s'élever à plusieurs dizaines de milliers d'euros (appels vers l'étranger ou vers des numéros surtaxés par exemple). Au niveau informatique, il peut servir de porte d'entrée sur le réseau interne. Les fonctionnalités migrant d'un univers à l'autre et pouvant même être redondantes, le risque d'atteinte à la confidentialité les concerne tout les deux.

Une différence importante limite cependant la déclinaison des bonnes pratiques aux PABX. En effet, la journalisation est très limitée. Dans le monde de la téléphonie, elle s'appelle la « taxation » et sert à répartir l'imputation des frais aux différents utilisateurs ou services. Elle trace donc les appels, mais ne garde pas d'informations sur les opérations de maintenance. Par exemple, ajouter un poste ou définir un numéro comme invisible pour la taxation ne laisse pas de trace, si ce n'est dans la configuration elle même. Pour cela le contrôle régulier de la configuration et du *plan de numérotation* est très important.

3.2 Quelques faiblesses des PABX et les bonnes pratiques de sécurité

Plusieurs faiblesses courantes sont présentées ci-dessous pour déterminer comment l'application des bonnes pratiques de sécurité permet de les éviter ou de limiter leur impact.

3.2.1 La ligne de télémaintenance

Description

Les PABX sont souvent maintenus à distance à l'aide d'un modem (interne ou externe) qui répond aux appels entrants. Les identifiants étant généralement triviaux, connaître ce numéro permet la prise de contrôle totale.

Des bonnes pratiques

- *limiter les flux :* il est possible par exemple de ne brancher le modem qu'en cas de besoin, ou d'utiliser des appareils prévus pour ne faire que des rappels vers un numéro préconfiguré ;
- *contrôler les flux :* cet accès étant directement géré par le PABX, il y a très peu d'information dans la journalisation ;
- *utiliser des outils d'authentification forte :* comme les PABX sont souvent mis en place et gérés par des sous-traitants, il faut veiller à ce qu'ils respectent les règles de la PSSI. Souvent, les intervenants jugent plus facile d'utiliser le même mot de passe quel que soit le client. Attention, il arrive qu'une mise à jour remette en place les identifiants par défaut.

3.2.2 L'authentification des abonnées (utilisateurs)

Description

L'authentification des utilisateurs repose sur un code PIN qui est rarement changé. Il peut être utilisé pour configurer son compte, ses renvois ou consulter sa messagerie, et cela depuis l'intérieur ou l'extérieur. Le parcours des condensats (*hash*) de ces codes PIN en montre un grand nombre identiques, correspondant au code par défaut.

Des bonnes pratiques

- *utiliser des mots de passe forts :* lors de l'attribution des postes téléphoniques, comme pour un ordinateur, l'utilisateur devrait saisir un mot de passe respectant des règles de robustesse.

3.2.3 Les fonctionnalités de DISA (*Direct Inward System Access*)

Description

Il existe des fonctionnalités permettant d'appeler le PABX et, moyennant son numéro de poste et son code PIN, d'avoir accès à toutes les fonctionnalités disponibles en interne, par exemple appeler un numéro externe. Dans les faits, cela revient à téléphoner n'importe où, y compris vers de numéros surtaxés, en ne payant que la communication jusqu'au PABX, le reste des coûts étant à la charge de l'entreprise.

Des bonnes pratiques

- *limiter les services à ceux nécessaires :* ces fonctionnalités sont souvent activées par défaut, sans aucune utilité pour l'entreprise. Il faut alors les supprimer.
- *contrôler les flux :* si ces fonctionnalités sont vraiment nécessaires, il est important d'en contrôler leurs utilisations au niveau de la « taxation » et de les limiter via le «plan de numérotation».

3.2.4 Les faiblesses liées au réseau informatique

Pour avoir une vision exhaustive des risques liés au réseau informatique, il faut se reporter aux nombreux articles traitant de la SSI classique. Cependant, un type d'attaque médiatisée concerne les risques liés aux XSS (*Cross Site Scripting*) dans les annuaires. En effet, les utilisateurs pouvant saisir et consulter des informations à l'aide d'interfaces Web, il suffit qu'un champ soit mal contrôlé pour permettre à une personne malveillante d'injecter du code qui compromettrait les ordinateurs des personnes le visualisant. Dans ce cas, les mises à jour des éditeurs doivent être appliquées. De plus, un code d'exploitation publié récemment permet d'exécuter des commandes arbitraires sur un PABX par l'intermédaire d'une vulnérabilité sur l'interface de gestion Web.

Certains PABX ont publié une liste de leurs objectifs de sécurité en vue d'une évaluation certification. Des documents sont disponibles aux adresses suivantes :

- Alcatel OmniPCX :
  http://www.ssi.gouv.fr/fr/politique_produit/catalogue/inventaire/pdf/Alcatel%20OmniPCX.pdf
- Resix NetxSERV :
  http://www.ssi.gouv.fr/fr/politique_produit/catalogue/inventaire/pdf/netxservcs.pdf

3.3 Conclusion

Les PABX sont des infrastructures critiques des SI auxquelles il faut prêter une grande attention. Une première approche possible pour vérifier et augmenter leur niveau de sécurité est d'essayer d'y appliquer les bonnes pratiques sécuritaires telles que :

- limiter et contrôler les flux par la mise en place de filtrage et de journalisation (enregistrement et analyse) ;
- limiter et contrôler les services ;
- mettre à jour lorsqu'un qu'un correctif est disponible ;
- imposer l'utilisation d'identifiants forts ;
- sensibiliser les utilisateurs ;
- faire respecter la PSSI aux sous-traitants.

4 Les téléphones mobiles

4.1 Vulnérabilité dans certains téléphones mobiles

Le fabricant Motorola a récemment publié une mise à jour de sécurité pour le *firmware* mis en oeuvre dans les modèles RAZR de téléphone portable. Cette nouvelle version de *firmware* corrige une vulnérabilité dans le moteur de traitement des images qui permet une exécution de code arbitraire au moyen d'une image spécifiquement construite. Ainsi, un individu malveillant peut envoyer un message multimédia (MMS) à une personne afin de l'inciter à ouvrir l'image attachée et compromettre son équipement. Cette technique peut également se faire via Bluetooth.

L'éditeur Motorola propose une mise à jour de sécurité aux utilisateurs de téléphones portables ayant une version vulnérable. Cependant, celle-ci peut risquer de porter atteinte au bon fonctionnement de l'appareil dans le cas où le système d'exploitation a été modifié pour et/ou par les opérateurs de téléphonie mobile.

La mise à jour de sécurité est disponible à l'adresse suivante :
http://direct.motorola.com/hellomoto/NSS/update_my_software.asp

4.2 Une nouvelle technologie dans les téléphones mobiles

De plus en plus de fabricants de téléphones mobiles équipent leurs produits avec une nouvelle technologie de communication sans fil de courte portée. Cette technologie porte le nom de *Near Field Communication* (NFC). Celle-ci, dont la portée théorique est de quelques centimètres, est une extension de la technologie utilisée dans les composants RFID (Radio Frequency Identification). Elle est destinée à offrir à l'utilisateur de nombreuses interactions pour régler des transactions, emprunter les transports en commun, servir de porte-monnaie électronique... Ce ne sont là que quelques exemples voués à être concrétisés.

Certains groupes de chercheurs en sécurité ont d'ores et déjà commencé à étudier les faiblesses liées à cette technologie. Par conséquent, il n'est pas exclu de voir, à terme, des annonces de vulnérabilités.

Cette nouvelle technologie de communication NFC vient s'inscrire à une liste déjà longue d'autres technologies non filaires : GSM, GPRS, Wi-Fi, Bluetooth, IrDA... Le CERTA rappelle donc la nécessité d'utiliser ces technologies de communication de façon responsable, sachant que les équipements utilisant ces technologies font

parfois l'objet de vulnérabilités (corrigées ou non) et que la mise à jour de leur système d'exploitation et de leurs applications n'est pas toujours triviale ni même parfois possible.

5 Les services de *DNS* dynamiques

Les services de *DNS* dynamiques permettent d'associer un nom de domaine fixe à une adresse IP qui elle ne l'est pas. Ces services sont généralement conçus afin de permettre aux personnes ayant une adresse IP changeant à chaque nouvelle connexion (par exemple des clients *ADSL*) d'avoir un nom de domaine invariable associé.

Concrètement, si le fournisseur d'accès n'a pas pour politique d'attribuer une adresse IP fixe ou si ses abonnés ont fait le choix de ne pas avoir d'adresse IP fixe, les utilisateurs vont se voir attribuer une adresse IP différente très fréquemment. Afin de disposer d'un nom unique toujours accessible, les services de *DNS* dynamiques identifient la nouvelle adresse IP et l'associent au nom de domaine créé par l'utilisateur. Cette association est généralement faite via une application client installée sur le poste de l'utilisateur.

Les noms de domaines sont sous la tutuelle du service de *DNS* dynamique et prennent la forme :
`partie_personnalisée.nom_du_service_DNS_dynamique.tld`

Le service de *DNS* dynamique est ainsi l'autorité pour les sous-domaines et gère l'association adresse IP/nom de domaine.

Ce service a été détourné de son objectif premier afin d'offrir la possibilité d'associer, à tour de rôle, différentes machines (donc différentes adresses IP) à un nom de domaine unique. Les auteurs de programmes malveillants peuvent ainsi mettre le nom de domaine fixe dans le code et changer la machine vers laquelle le nom pointe. Cela permet de gérer un ensemble de machines de diffusion de codes malveillants et/ou de récolter de données. Ainsi les chances de perturber le fonctionnement du code malveillant par le nettoyage de l'une de ces machines diminuent. Cette technique est à rapprocher d'un fonctionnement des réseaux d'ordinateurs zombies communément appelé *FastFlux* et fonctionnant sur le même principe.

Le CERTA recommande donc de rester vigilant lors de l'inspection de journaux de connexions sortantes sur l'apparition de noms de domaine liés à ce type de service. Même si les domaines associés sont loin d'être tous malveillants, ils sont à surveiller car des individus malintentionnés profitent de ces services et ces derniers apparaissent régulièrement dans les connexions établies par des machines compromises.

6 Rootkits pour IOS

Récemment, a été rendu public un ensemble d'éléments techniques mettant en évidence la faisabilité de créer des *rootkits* pour `IOS`. Pour mémoire, `IOS` est le système d'exploitation embarqué dans la plupart des équipements `Cisco`. Il a été montré qu'il était possible de faire fonctionner un logiciel masquant l'activité d'un utilisateur ayant la maîtrise du `rootkit`. En l'état, il n'est possible d'installer le code malveillant qu'en modifiant un `IOS` existant puis en le plaçant sur l'équipement choisi (principalement via `TFTP`). Ce dernier point pourrait paraître rassurant car il faut un accès privilégié pour réaliser l'opération. Cependant, et comme cela a été relevé par plusieurs chercheurs, c'est sans compter sur la pratique de certains administrateurs. Ceux-ci, plutôt que de payer et de télécharger une nouvelle version officielle d'`IOS` préférent en recupérer une gratuitement depuis des sources tierces plus ou moins douteuses...

Recommandations

En la matière, les recommandations sur les mises à jour sont les mêmes que celles s'appliquant aux systèmes plus conventionnels comme leur aquisition à partir de sources officielles certes payantes mais fiables a priori.

La vérification de l'intégrité de certains fichiers est également une bonne pratique, certains constructeurs fournissant par exemple sur leur site des condensats de certains fichiers-clés.

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 22 et le 29 mai 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 23 au 29 mai 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-260 : Vulnérabilité dans Alcatel OmniPCX Office
- CERTA-2008-AVI-261 : Vulnérabilité d'un préprocesseur de Snort
- CERTA-2008-AVI-262 : Multiples vulnérabilités dans GnuTLS
- CERTA-2008-AVI-263 : Vulnérabilité dans HP-UX
- CERTA-2008-AVI-264 : Vulnérabilité dans IBM Lotus Sametime
- CERTA-2008-AVI-265 : Vulnérabilité de Nagios
- CERTA-2008-AVI-266 : Vulnérabilités dans Trillian
- CERTA-2008-AVI-267 : Multiples vulnérabilités d'AIX
- CERTA-2008-AVI-268 : Multiples vulnérabilités du serveur SSH des équipements Cisco
- CERTA-2008-AVI-269 : Multiples Vulnérabilités dans Cisco Service Control Engine
- CERTA-2008-AVI-270 : Vulnérabilité dans SAP Web Application Server
- CERTA-2008-AVI-271 : Vulnérabilité dans Core FTP
- CERTA-2008-AVI-272 : Vulnérabilité dans Xerox WorkCentre
- CERTA-2008-AVI-273 : Vulnérabilités d'EMC AlphaStor
- CERTA-2008-AVI-274 : Vulnérabilité dans Sun Java System Web Server
- CERTA-2008-AVI-276 : Vulnérabilité dans Samba
- CERTA-2008-AVI-277 : Vulnérabilités dans OpenSSL
- CERTA-2008-AVI-278 : Mutliples vulnérabilités dans Apple Mac OS X
- CERTA-2008-AVI-279 : Vulnérabilité dans Symantec Backup Exec System Recovery Manager
- CERTA-2008-AVI-280 : Vulnérabilités dans Mambo
- CERTA-2008-AVI-281 : Vulnérabilité dans CiscoWorks Common Services
- CERTA-2008-AVI-282 : Vulnérabilité dans libxslt

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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

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

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

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 oeuvre (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 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.

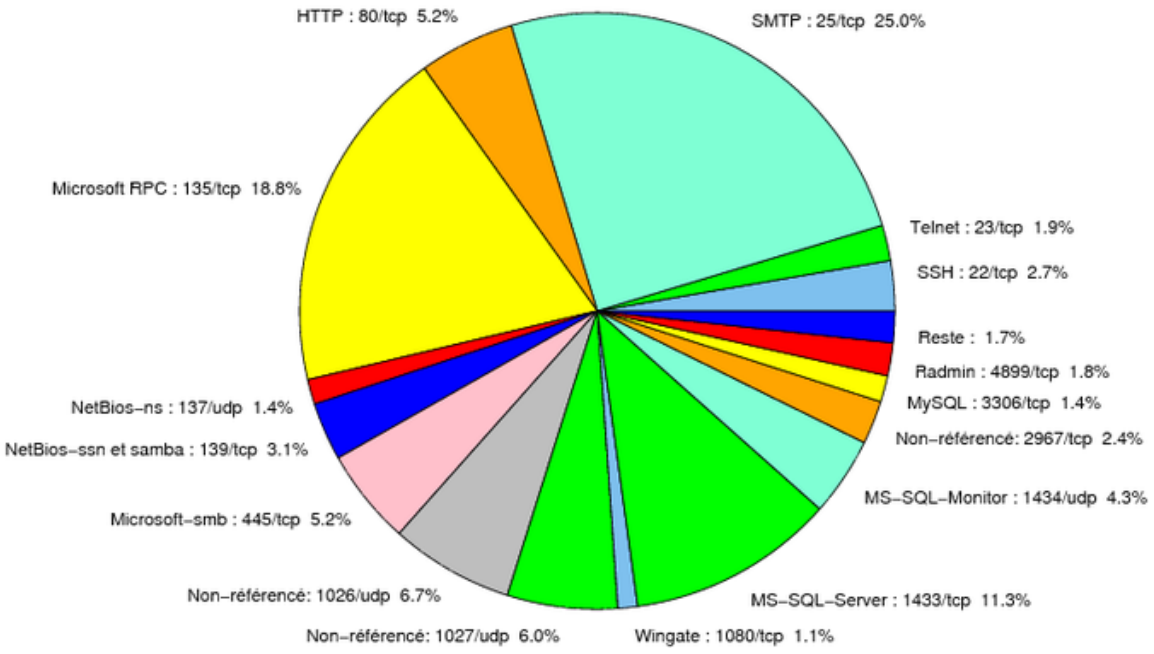

FIG. 1: Répartition relative des ports pour la semaine du 22.05.2008 au 29.05.2008

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
25/tcp	25.03
135/tcp	18.83
1433/tcp	11.26
1026/udp	6.7
1027/udp	5.99
80/tcp	5.77
445/tcp	5.2
1434/udp	4.27
139/tcp	3.13
22/tcp	2.71
2967/tcp	2.35
23/tcp	1.92
4899/tcp	1.78
3306/tcp	1.42
137/udp	1.35
1080/tcp	1.06
3128/tcp	0.64
143/tcp	0.42
21/tcp	0.28
3389/tcp	0.14
9898/tcp	0.07

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

30 mai 2008 version initiale.