

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-38

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-038>

Gestion du document

Référence	CERTA-2007-ACT-038
Titre	Bulletin d'actualité 2007-38
Date de la première version	21 septembre 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-038.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-038/>

1 Les serveurs Web, une plate-forme d'attaque intéressante

Au cours d'incidents récents, le CERTA a découvert, sur des serveurs Web compromis, de nombreux robots écrits en php. Ces robots sont tous similaires : ils ont pour fonctionnalité de se rendre sur des canaux irc de serveurs parfois privés et se mettent en attente d'instructions d'attaques.

Le modèle de ces attaques est assez naïf. Elles consistent à donner des ordres de faire des recherches de vulnérabilités en utilisant des moteurs connus (Google, Yahoo!, MSN search, Lycos, etc.). Les vulnérabilités ainsi recherchées concernent toutes des failles connues d'applicatifs Web écrits en php (par exemple, les composants Joomla!, eva-web, etc.). Le robot irc construit une adresse réticulaire (url) en agrégeant le chemin d'un script php (qui va typiquement télécharger et exécuter un robot irc) aux résultats de la recherche. Cette url permet de compromettre les machines dont le nom est retourné par le moteur de recherche.

Ces attaques permettent ainsi de créer un réseau de machines zombie, ou botnet, constitué uniquement de serveurs Web. Les serveurs compromis de cette façon sont généralement utilisés par de nombreux intrus, chacun déposant par la suite des outils. Il n'est donc pas rare de trouver des serveurs Web hébergeant des dizaines de robots irc.

Les robots découverts par le CERTA se connectent généralement sur le port 6667/tcp de serveurs irc. Toutefois, il est possible qu'à l'avenir, ces derniers utilisent d'autres ports pour contourner certaines règles de filtrage.

C'est la raison pour laquelle il est conseillé de mettre en place d'un filtrage en sortie dont le but est d'interdire au serveur Web d'établir n'importe quelle connexion vers d'autres serveurs. Il est également fortement recommandé de consulter régulièrement les journaux des pare-feux ainsi que les journaux d'accès du serveur Web.

2 Problèmes concernant les lecteurs multimédia

2.1 Apple QuickTime

L'alerte du 13 septembre 2007 CERTA-2007-ALE-014 concernant Quicktime et Mozilla Firefox portait sur l'exécution possible de code arbitraire par le navigateur via l'ouverture d'un fichier au format Quicktime spécifiquement construit. La vulnérabilité du côté de Firefox a rapidement été corrigée avec la version 2.0.0.7, qui a désactivé la possibilité d'exécuter des scripts arbitraires avec l'option `-chrome`. Toutefois, un problème existe encore au niveau du lecteur multimédia, du fait :

- qu'il fait appel directement en ligne de commandes à des navigateurs par simple lecture du fichier de données ;
- qu'il semble ne pas filtrer les entrées de l'option `qtnext` ;
- qu'il ne propose à l'utilisateur aucun moyen de désactiver la fonctionnalité `qtnext` et donc des connexions sortantes ou, au minimum, l'exécution de scripts.

En d'autres termes, il n'est pas possible, à la date de rédaction de ce bulletin, de spécifier dans la configuration QuickTime qu'il doit rester passif, et ne pas chercher à initier de connexions. Il ne peut pas fonctionner en simple lecteur multimédia (à moins d'effectuer une autre action, comme débrancher le câble, éteindre la carte WiFi, ou bloquer les connexions sortantes au niveau d'un pare-feu local).

Si l'alerte portait principalement sur la vulnérabilité de Quicktime avec Firefox comme navigateur par défaut, une autre publication montre qu'il est également possible d'utiliser Internet Explorer pour effectuer le même type d'actions. A la date de rédaction de ce bulletin, aucun code de démonstration ne permet de prouver clairement l'exécution de code arbitraire, toutefois il est possible qu'une personne puisse exécuter certaines commandes à distance, comme :

- ouvrir des répertoires ;
- perturber le lecteur et provoquer une erreur.

Le CERTA a choisi de ne pas faire d'alerte pour le moment, mais il est vivement recommandé de rester vigilant et méfiant quant à l'usage d'applications telles que QuickTime ou Microsoft Windows Media Player.

2.2 Microsoft Windows Media Player

Une autre publication montre un comportement similaire pour le lecteur multimédia Windows Media Player. Au moins une option d'un fichier au format Media Player permet en effet de spécifier une URL à afficher dans le lecteur pendant la lecture du contenu du fichier (HTMLView). Certaines fonctions Javascript semblent filtrées, ce qui limite les possibilités d'exploitation par une personne malveillante. Toutefois, toute connexion sortante présente un risque pour l'utilisateur, et encore plus lorsqu'elle n'est pas maîtrisée et non désactivable comme c'est le cas. Pire encore, le navigateur utilisé est obligatoirement Internet Explorer, ce qui présente un risque majeur dans la mesure où le choix du navigateur est forcé. En effet, toute vulnérabilité d'Internet Explorer serait ainsi potentiellement exploitable via l'ouverture d'un fichier par le lecteur multimédia de Windows, même si l'internaute utilise un navigateur alternatif. Heureusement, les versions 10 et 11 de Windows Media Player provoquent l'affichage d'un avertissement lorsqu'une cette option HTMLView est utilisée. Ces versions ne sont toutefois pas encore mises à jour par défaut excepté sur Windows Vista.

2.3 Ce qu'il faut retenir

D'autres lecteurs multimédia sont probablement affectés par le même type de problème, qui est plus une fonctionnalité qu'une vulnérabilité. La phase de correction n'est pas simple à faire, car la vulnérabilité intervient par l'interaction de deux applications. Les développeurs voient chacun le problème comme un détournement de fonctionnalité de leur application, et ne sont pas toujours prêts à proposer une solution pour éviter le problème.

L'utilisateur est, lui, directement exposé à la vulnérabilité. Il dispose d'applications multimédia incontrôlables, pouvant interpréter beaucoup de choses dans des fichiers aux formats trop riches, sans pour autant pouvoir restreindre cette liberté.

Le CERTA recommande donc l'utilisation d'un lecteur permettant de désactiver ou n'ayant pas ce type de fonctionnalité, ou au minimum permettant l'affichage de fenêtres d'avertissements.

Documentation

Alerte CERTA-2007-ALE-014 du 13 septembre 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-014/index.html>

3 La couche MAC

Des techniques d'attaques détaillées il y a plusieurs années ne sont pas moins dangereuses et inutiles à considérer. Preuve en est avec l'usurpation d'adresses MAC. Le protocole ARP, *Address Resolution Protocol*, se charge de la traduction d'une adresse IP en adresse MAC. L'usurpation, elle, s'appuie sur la propriété de cache, i.e. de stocker temporairement la correspondance entre une adresse IP et une adresse MAC.

Prenons deux machines A et B dans un réseau interne, ainsi qu'une machine voisine, pouvant communiquer avec certaines d'entre elles¹. La machine malveillante annonce ouvertement aux machines voisines (dans sa zone de diffusion *broadcast*) que l'adresse IP A correspond par exemple à sa propre adresse MAC. Si la machine légitime A ne répond pas rapidement, la machine B peut provisoirement stocker cette nouvelle correspondance. Elle échangera donc des données avec la machine malveillante, les trames intégrant la nouvelle adresse. La machine laissée, quant à elle, ne verra pas ce nouveau trafic, car l'adresse MAC de destination ne lui correspondra pas.

Rien de bien nouveau donc. Le CERTA signale cependant que des attaques de ce type ne disparaissent pas, bien au contraire, et peuvent être mises en œuvre dans des codes malveillants. Cela permet de propager divers codes, sans pour autant éveiller l'attention d'administrateurs réseau qui ne surveilleraient que des couches protocolaires plus élevées (journaux du pare-feu par exemple).

Parmi les scénarios possibles :

- 1° une machine est contaminée dans le réseau, d'une manière ou d'une autre ;
- 2° le code malveillant installé écoute le trafic à proximité, et émet des réponses ARP en lieu et place des passerelles de routage ;
- 3° les machines dupées du réseau font transiter leurs requêtes par la machine corrompue ;
- 4° cette dernière relaie les paquets, en modifiant certains paquets particuliers, comme les réponses HTTP. Elle y insère du code malveillant (code javascript par exemple, ou exploitant une vulnérabilité d'un navigateur) ;
- 5° la machine dupée peut alors être à son tour compromise, effectuer une opération similaire, etc.

Ce scénario n'est pas impossible, même s'il ne peut fonctionner que sous certaines conditions. Il permet de propager localement du code malveillant sur un ensemble de machines.

Pour se prémunir de ce genre d'attaques, plusieurs actions doivent être considérées comme :

- cloisonner les réseaux ;
- avoir une politique de filtrage (trafic entrant et sortant) rigoureuse.

Il est également important de surveiller le trafic à ce niveau. Plusieurs solutions sont disponibles, soit sous forme d'outils indépendants (`arpwatch` sous Linux par exemple), soit sous forme de modules en complément d'un pare-feu ou d'une sonde réseau de détection d'intrusion (IDS). Elles servent principalement à surveiller toute modification visible de l'association IP/MAC. Il faut néanmoins prendre le temps de l'adapter à l'environnement et d'interpréter les retours fournis.

4 Les beaux supports de données amovibles tout neuf ou de retour de réparation

Le CERTA traite fréquemment des incidents (propagation virale en majeure partie) dont l'élément déclencheur est l'insertion d'une clef USB infectée. Ce vecteur d'infection par support de données amovible n'est pas nouveau puisqu'il était l'un des plus fréquents à l'époque où les disquettes étaient encore massivement utilisées. Comme à cette époque, il convient de rester sensible au fait qu'un support amovible représente un élément étranger au système d'information, et par conséquent, reste un élément non sûr jusqu'à preuve du contraire, y compris quand ce support sort de son emballage.

En effet, plusieurs affaires ont eu pour cause d'infection l'insertion d'un support amovible USB fraîchement déballé. Il faut prendre garde que le terme « support de données amovible USB » englobe aussi bien les clés USB, que les disques durs externes, les lecteurs MP3, les appareils photos numériques, les cadres photo, etc.

¹Les réseaux WiFi ne sont pas abordés dans cet article, mais le même scénario d'attaque est tout à fait envisageable dans un tel environnement, car facilité par l'absence d'un périmètre de contrôle physique.

Ce fut ainsi le cas fin 2006 quand une grande marque de baladeur MP3 a vendu une série infectée d'un code malveillant.

Le problème n'est pas tant de savoir comment ce type d'infection peut avoir lieu dans une chaîne de production, mais plutôt de s'assurer que l'on prend les précautions nécessaires permettant de se protéger contre ces supports infectés :

- considérer tout élément extérieur au système d'information comme potentiellement hostile, et donc, le brancher une première fois sur un système non critique, non connecté à un réseau (Internet ou réseau interne) ;
 - désactiver l'exécution automatique (*autorun*). Pour ce faire, sous Windows, changez la valeur *NoDriveTypeAutoRun* de la clef
[HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\Policies\Explorer]
et attribuez-lui la valeur *dword:000000ff* (cf. CERTA-2006-INF-006);
 - vérifier les fichiers présents (y compris les fichiers systèmes et les fichiers cachés) et désinfecter le support ;
- Enfin, vous pouvez contacter le CERTA pour tout contenu suspect que vous trouverez.

Les remarques précédentes sont également valables pour tout geste commercial sous forme de clés USB, cédérom ou autre support de données amovibles.

5 Restauration automatique d'un système

Il existe certaines techniques pour qu'à chaque redémarrage de l'ordinateur, le système d'exploitation et plus largement tout ou partie du contenu du disque dur soit ré-initialisé ou remis dans un état dit « initial ». De prime-abord, cette solution peut être attrayante dans le cadre de la gestion d'un parc informatique homogène. En effet, il suffit d'un redémarrage pour voir l'ordinateur débarrassé des éventuelles installations sauvages, virus... On peut trouver ainsi plusieurs façons de mettre en œuvre ce procédé. Un exemple peut être la récupération du « master » par le réseau. Mais il existe également des solutions matérielles installables dans la machine et qui vont prendre en charge toutes les opérations d'écriture sur le disque. Ainsi, à partir du moment où ce périphérique est installé et configuré dans une machine, les opérations suivantes d'écriture sur le disque seront traitées de façon particulière pour qu'au prochain redémarrage, elles n'aient pas affecté le contenu initial du disque.

Ces solutions posent tout de même des problèmes en terme de sécurité. En effet, lorsque l'on fige le contenu d'un système à un instant donné, il sera impossible d'appliquer des correctifs ultérieurs (problème du « master » vulnérable). Ainsi, à chaque redémarrage, c'est une machine vulnérable que l'on obtient. D'autre part lors d'une analyse *post-mortem*, un simple arrêt de la machine fera « disparaître » un certain nombre d'éléments utiles à l'analyse : dates de dernier accès des fichiers, fichiers contenant une copie du code maveillant ou les fichiers de journalisation... Enfin certains dispositifs utilisent tout de même le disque dur pour enregistrer les modifications temporaires par le biais de fichiers (souvent dans un format propriétaire). Ceci rajoute du « bruit » sur le disque néfaste à une éventuelle autopsie. Ces problématiques doivent être bien prises en compte lors du déploiement de ce genre de technologies dans un parc de machines.

6 Les messageries instantanées, risques immédiats ?

6.1 Constatation

Les messageries instantanées (IM) sont souvent installées sur des postes. Elles peuvent être fournies avec une distribution particulière d'un système d'exploitation, mais sont souvent installées *a posteriori* par l'utilisateur, en fonction de celles de ces contacts.

Il n'est donc pas rare de trouver des installations de celles-ci sur des machines en cours d'analyse.

L'objectif de cette publication est de bien faire comprendre que cela peut engendrer des risques complémentaires importants.

Comme de nombreuses applications, les logiciels de messagerie se sont vus doter de fonctionnalités au fil des mois. Outre une messagerie texte instantanée, il est maintenant possible de :

- gérer du trafic audio et video, par le biais d'une webcam ou d'un microphone ;
- utiliser la messagerie comme moyen de téléphonie sur IP ;
- télécharger et interpréter des chaînes de caractères avec des « émo-icônes » ;
- offrir des espaces de partage de fichiers ;
- échanger des données sous un format quelconque ;

- interpréter des adresses (URL) ;
- écrire des messages dans un format dynamique ou interprété (HTML, Javascript) ;
- envoyer des actions pré-définies sur l'ordinateur distant ;
- stocker des listes de contacts, avec leurs informations personnelles ;
- utiliser la messagerie comme outil de rapport d'événement (*reporting*) ;
- conserver par défaut un historique des conversations et toute autre transaction.
- etc.

La liste ci-dessus n'est pas exhaustive, les logiciels pouvant évoluer très rapidement.

6.2 Les risques

Le lecteur aura bien compris, avec le paragraphe précédent, que les logiciels de messagerie offrent une surface d'attaque très large pour les personnes malveillantes. Voici à titre d'information, quelques vulnérabilités recensées en 2007 :

- pour MSN Messenger : CVE-2007-2931, CVE-2007-4579, CVE-2007-3436 ;
- pour Cerulean Studios Trilian : CVE-2007-3305, CVE-2007-3833, CVE-2007-3832, CVE-2007-2479, CVE-2007-2478, CVE-2007-2118 ;
- pour aMSN (Alvaro's Messenger) : CVE-2007-2195 ;
- pour Pidgin/Gaim : CVE-2007-3841 ;
- pour AIM (AOL Instant Messenger) : CVE-2007-4901, CVE-2007-3833, CVE-2007-3832, CVE-2007-3437, CVE-2007-3350, CVE-2007-1904 ;
- pour Yahoo Messenger : CVE-2007-5017, CVE-2007-4635, CVE-2007-4515, CVE-2007-4391, CVE-2007-3928, CVE-2007-3638, CVE-2007-3148, CVE-2007-3147, CVE-2007-1680, CVE-2007-0868, CVE-2007-0768 ;
- pour Jabber Server : CVE-2007-3910, CVE-2007-0903 ;
- pour iChat : CVE-2007-3748, CVE-2007-2390, CVE-2007-0710, CVE-2007-0614, CVE-2007-0021 ;
- pour mIRC : CVE-2007-4402, CVE-2007-4401.

Il y a plus d'une centaine de clients disponibles gratuitement sur l'Internet, supportant les protocoles courants. Plusieurs logiciels combinent des clients différents, et mettent en œuvre des protocoles différents. Ils cumulent ainsi plusieurs vulnérabilités. Par ailleurs, la mise à jour n'est pas toujours immédiate. Leur installation engendre enfin régulièrement des exceptions dans les règles de pare-feux locales, ce qui crée également des portes d'entrées intéressantes pour les codes malveillants.

A cette liste s'ajoutent des risques classiques de messagerie, comme l'incitation à cliquer sur un lien pour visiter une page malveillante ou installer un code de type « cheval de Troie ». Le côté « instantané » et « multiplexé » (plusieurs conversations en même temps) réduit le temps de réflexion.

Il faut bien comprendre que des codes malveillants circulent sur l'Internet en permanence, pour exploiter la plupart des vulnérabilités citées précédemment. Certains sont médiatisés, d'autres moins.

Le CERTA ne publie pas régulièrement d'avis sur ces applications, mais tient à rappeler le risque potentiel qu'elles peuvent faire courir aux systèmes sur lesquelles elles sont installées.

Il est possible de déployer en interne sa propre architecture de messagerie, en accord avec la politique de sécurité en vigueur. Si cette option n'est pas nécessaire, alors il est vivement recommandé d'éviter l'utilisation de telles applications, et de sensibiliser les utilisateurs sur le sujet.

7 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 13 et le 20 septembre 2007.

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 14 au 20 septembre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-404 : Vulnérabilité de Qt
- CERTA-2007-AVI-405 : Vulnérabilités multiples d’OpenOffice
- CERTA-2007-AVI-406 : Vulnérabilité de OmniPCX Entreprise
- CERTA-2007-AVI-407 : Vulnérabilité dans Firefox
- CERTA-2007-AVI-408 : Vulnérabilité de WinSCP

Le CERTA a également mis à jour l’alerte suivante :

- CERTA-2007-ALE-014 : Vulnérabilité dans Apple QuickTime

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 réglementaire, 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 inexplicables 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.

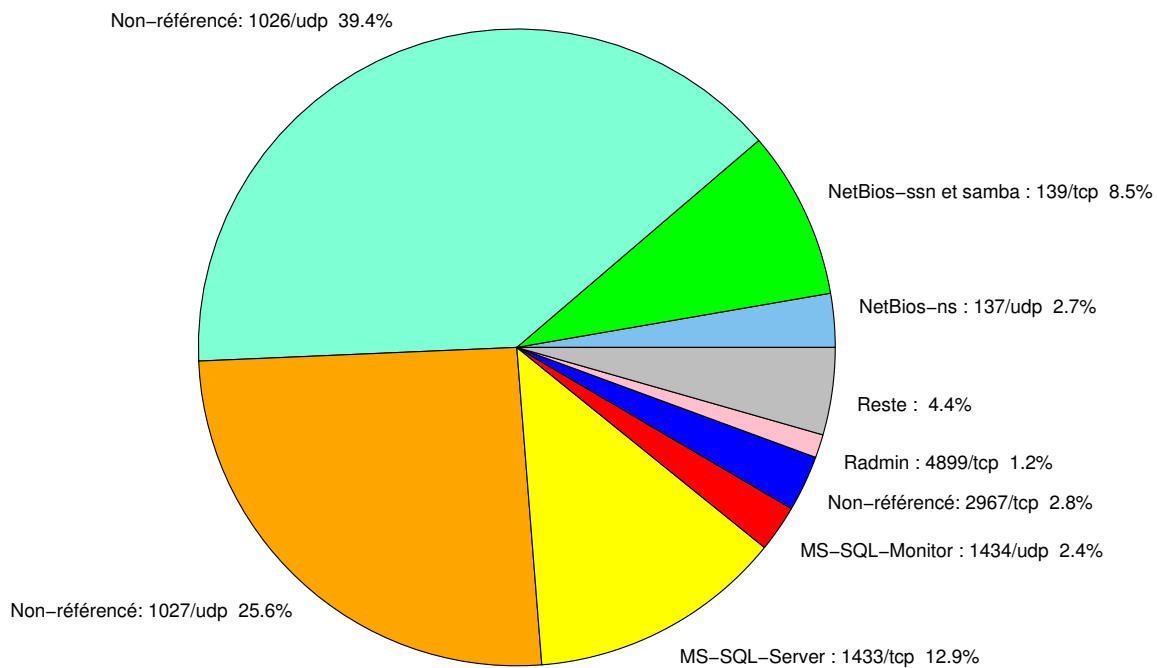


FIG. 1: Répartition relative des ports pour la semaine du 13.09.2007 au 20.09.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	-	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	-	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	-	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	-	CERTA-2004-AVI-384
80	TCP	HTTP	-	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	-	-
111	TCP	Sunrpc-portmapper	-	CERTA-2003-AVI-052
119	TCP	NNTP	-	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	-	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	-	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	-	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338
143	TCP	IMAP	-	CERTA-2005-AVI-185
389	TCP	LDAP	-	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	-	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	-	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338
1023	TCP	-	Serveur ftp de Sasser.E	-
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	-	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	-	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	-	CERTA-2005-ALE-002

2381	TCP	–	HP System Management	CERTA-2006-AVI-248
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310

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

port	pourcentage
1026/udp	39.42
1027/udp	25.56
1433/tcp	12.93
139/tcp	8.54
2967/tcp	2.83
137/udp	2.72
1434/udp	2.36
4899/tcp	1.18
22/tcp	0.97
1080/tcp	0.67
3306/tcp	0.56
3128/tcp	0.52
21/tcp	0.45
25/tcp	0.41
23/tcp	0.24
80/tcp	0.22
143/tcp	0.15
15118/tcp	0.07
9898/tcp	0.03
5554/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	10
3	Paquets rejetés	11

Gestion détaillée du document

21 septembre 2007 version initiale.