

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-14

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-2010-ACT-014>

Gestion du document

Référence	CERTA-2010-ACT-014
Titre	Bulletin d'actualité 2010-14
Date de la première version	09 avril 2010
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-2010-ACT-014.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-2010-ACT-014/>

1 Exécution de programmes à partir de documents au format PDF

1.1 Description du problème

Le format de document électronique PDF (*Portable Document Format*) est défini par la norme internationale ISO 32000-1:2008. À la section 12.6, on découvre que le format permet de spécifier le lancement d'applications selon plusieurs critères au moyen du champ */ACTION*.

La norme prescrit aux lecteurs de documents PDF qui veulent se déclarer conformes d'ouvrir effectivement les applications, mais sans préciser les modalités de cette ouverture (section 2.2).

Cette richesse fonctionnelle est à double tranchant.

Le CERTA est informé qu'avant d'exécuter effectivement une telle application :

- le lecteur Adobe Reader affiche une fenêtre d'avertissement, mais le texte de cette fenêtre est partiellement modifiable ;
- le lecteur FoxIt affiche un avertissement uniquement si le correctif datant du 02 avril 2010 est appliqué, mais le texte est aussi partiellement modifiable ;
- d'autres lecteurs, comme evince, n'exécutent pas les applications.

Cette fonctionnalité peut être exploitée de manière malveillante, en particulier en modifiant le texte d'avertissement affiché à l'utilisateur. De plus, un fichier exécutable embarqué dans le document PDF peut être lancé par certains lecteurs. Dans cette hypothèse, l'attaquant peut élargir sa capacité de nuisance. Il n'est pas limité aux programmes déjà présents sur le système.

Il est important de noter que l'inactivation des scripts dans les documents PDF, résolution sage en soi, ne protège pas contre le détournement du lancement d'exécutable à partir de fichiers PDF.

1.2 Limitations sous AdobeReader

Le lecteur AdobeReader donne une possibilité de restreindre le lancement d'applications. La solution pour un utilisateur isolé est de passer par l'interface du lecteur et de suivre l'enchaînement à partir du menu : *Edition -> Préférences -> Gestionnaire des approbations*. La case *Autoriser l'ouverture des pièces jointes non PDF dans des applications externes* ne doit pas être cochée.

Pour un parc d'ordinateurs, le positionnement systématique (script, GPO) à 0 (zéro) de la variable `bAllowOpenFile` de la clef de registre suivante (pour la version 9.0 d'Adobe Reader) est plus opérationnel : `HKCU\Software\Adobe\Adobe Reader\9.0\Originals`

Il est évident que ces mesures peuvent avoir des effets secondaires lorsque des documents PDF sont utilisés pour exécuter des applications tiers.

1.3 Recommandations

Afin de limiter les risques d'exploitation de ces vulnérabilités, le CERTA recommande :

- de lire attentivement les fenêtres d'avertissement lors de la lecture d'un fichier PDF et, au moindre doute, de refuser le lancement de toute action ;
- d'appliquer les correctifs sur les lecteurs de fichiers au format PDF, comme sur tous les autres logiciels. En particulier, il faut appliquer le correctif pour FoxIt mentionné dans l'avis CERTA-2010-AVI-155. Quant à Adobe Reader, l'éditeur prévoit une importante mise-à-jour le 13 avril 2010 ;
- de durcir la configuration de ces lecteurs ;
- de rester informé de l'évolution de ces logiciels ;
- sous réserve de contraintes opérationnelles, d'utiliser un lecteur qui ne lance pas les exécutables à partir des documents PDF.
- de surveiller les journaux et les trafics, entrants et sortants, pour détecter de possibles anomalies.

Pour limiter l'impact du détournement de cette fonctionnalité, il est également important de réduire au maximum les droits accordés à l'utilisateur.

1.4 Documentation

- Avis du CERTA *Vulnérabilité dans Foxit Reader* du 02 avril 2010 : <http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-155/index.html>
- Référence CVE CVE-2009-0836 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0836>
- Référence CVE CVE-2009-4764 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4764>
- Référence CVE CVE-2010-1239 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1239>
- Référence CVE CVE-2010-1240 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1240>

2 Fonctionnalités NTP...

Cette semaine, des chercheurs ont publié leurs travaux sur certaines fonctionnalités méconnues du protocole NTP.

En effet, il est prévu dans la norme un certain nombre de commandes auxiliaires permettant d'obtenir des informations sur le fonctionnement du serveur. Il suffit pour s'en convaincre de consulter la page de manuel de la commande `ntpdc` correspondant au client NTP livré avec le serveur standard `ntpd`.

Certains paramètres permettent d'obtenir des informations sur le type de système d'exploitation : *readvar*, les appariements avec d'autres serveurs NTP : *peers* ou *listpeers*, etc.

Mais il a été montré qu'il était possible également, par une utilisation particulière, d'obtenir la liste complète des clients utilisant actuellement un serveur NTP ciblé.

Ainsi si le serveur ne limite pas l'utilisation de ce type de fonctionnalités à certains clients privilégiés, n'importe qui aura accès à ces informations.

Recommandations :

Par défaut, un serveur NTP standard accessible depuis l'Internet mettra à disposition la majorité de ces directives. Il est donc recommandé de limiter l'accès à ces commandes autant que faire se peut. Pour cela plusieurs pistes sont envisageables et complémentaires :

- si cela n'est pas nécessaire, ne pas rendre public sur l'Internet le serveur NTP ou encadrer son utilisation avec une politique de filtrage réseau stricte ;
- restreindre, au niveau du fichier de configuration du serveur, l'accès à certains sous-réseaux uniquement ;
- modifier les options de compilation (ou les sources) du serveur NTP pour que ces directives ne soient pas disponibles dans le binaire *ntpd* final si cela est possible.

3 skipfish - scanner Web

Le scanner de vulnérabilités Web *skipfish* est disponible depuis quelques temps sur Google code. Il permet de cartographier un site depuis une page initiale (*web crawling*) à partir de laquelle il suivra tout les liens trouvés en fonction de paramètres prédéfinis. Il peut aussi tester un certain nombre d'attaques (injection SQL, XSS, inclusion de fichier ...) en se basant sur des mots-clefs. Il est fourni avec des dictionnaires de mots-clefs différents en fonction du panel des tests souhaités.

Les résultats sont présentés en HTML sous forme d'arborescences développables à la demande. Ils sont classés, entre autres, par type de fichiers trouvés (ex: *png*, *jpg*, *gif* ...) et par vulnérabilités plus ou moins critiques. Comme toujours l'utilisation de cet outil présente peu d'intérêt sans une expertise suffisante permettant de comprendre les résultats retournés.

Cet outil est reconnaissable dans les journaux, dans sa configuration par défaut, à son *User-Agent* *Mozilla/5.0 SF/1.26b* (1.26 étant la version) et à ses très nombreuses requêtes. Un test mené sur un serveur dédié de taille modéré (3 CMS, 1 forum, 1 *phpmyadmin*, le tout sans données) avec le dictionnaire de mots-clefs *minimal.wl* a engendré plusieurs gigaoctets de journaux d'accès et d'erreurs. Bien que déclaré comme sans risque, son utilisation sur un serveur en production est à éviter compte tenu des possibilités de déni de service.

3.1 Attention

Le CERTA profite de cet article pour rappeler que la détention et l'utilisation de ce type d'outils est encadré par la loi du 5 janvier 1988 *relative aux atteintes aux systèmes de traitement automatisé de données (STAD)* modifiée par la loi du 21 juin 2004 *pour la confiance dans l'économie numérique*. Les articles 323-1 à 323-3 du code pénal précisent les peines encourues pour l'accès et le maintien frauduleux dans un *STAD*, pour l'entrave à son fonctionnement et la modification ou la suppression de données. Donc, l'utilisation de cet outil de façon non maîtrisée et sans motif légitime est à proscrire, au risque de se retrouver confronté à des problèmes avec la justice.

3.2 Documentation

- Projet skipfish :
<http://code.google.com/p/skipfish/>
- Les articles de loi se trouvent dans le code pénal, livre 3 *Des crimes et des délits contre les biens*, titre 2 *Des autres atteintes aux biens*, chapitre 3 *Des atteintes aux systèmes de traitement automatisé de données* :
<http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT0000060070719>

4 Durcissement de la configuration des systèmes Windows (7/8) : activation des stratégies de restrictions logicielles

Il est possible, à partir de Windows XP, de restreindre l'exécution des programmes selon divers critères, grâce aux stratégies de restrictions logicielles (*Software Restriction Policies*). Une telle politique peut être mise en œuvre dans le but de :

- limiter le risque d'importation involontaire de virus, en particulier par clé USB ou lors d'un téléchargement depuis un site Web ;
- garder une certaine maîtrise des postes de travail en n'autorisant que les programmes professionnels et qualifiés par l'équipe informatique ;
- réduire le risque de compromission d'un poste à l'insu de l'utilisateur, par exemple suite à l'exploitation d'une vulnérabilité logicielle dans le navigateur Internet.

Les stratégies de restrictions logicielles permettent d'identifier les programmes exécutables suivant plusieurs critères : leur emplacement sur le système de fichiers, la signature numérique du programme ou une empreinte cryptographique. La politique de restriction peut correspondre à une liste blanche de critères autorisés ou à une liste noire de critères interdits. Il est de plus possible d'exempter les administrateurs locaux de ces restrictions, qui pourront ainsi installer et exécuter d'autres logiciels. Enfin, la liste des extensions identifiant les fichiers exécutables concernés est paramétrable.

D'une manière pragmatique, le critère d'emplacement est le plus simple à mettre en œuvre. Il nécessite tout de même de déterminer au préalable les répertoires de confiance contenant des exécutables légitimes du poste : par défaut, la liste contient `c:\windows`, `c:\windows\system32` et `c:\program files`. Les programmes contenus dans un répertoire autorisé pourront alors être exécutés, ainsi que les programmes présents dans les éventuels sous-répertoires. Il est ensuite nécessaire de déterminer les répertoires dans lesquels les utilisateurs ont les droits d'écriture, par exemple des répertoires temporaires sous `c:\windows`, afin d'ajouter une règle d'interdiction pour chacun de ces répertoires. Les règles les plus spécifiques étant prédominantes, les exécutables d'un sous-répertoire interdit situé dans un répertoire autorisé ne pourront pas être lancés. Pour déterminer les droits d'accès sur un répertoire et ses sous-répertoires, l'outil Microsoft AccessEnum¹ peut être utilisé.

Les stratégies de restrictions logicielles sont configurables à travers la politique locale de sécurité de la machine et éditables *via* le composant enfichable `secpol.msc` (*Paramètres de sécurité, Stratégies de restriction logicielle*). Elles sont ainsi déployables à large échelle *via* GPO et plusieurs profils peuvent être définis pour les différents types d'utilisateurs. Si aucune stratégie n'est définie, il faut en créer une grâce au menu « *Créer de nouvelles stratégies* ». Pour configurer une politique en mode liste blanche de répertoires de confiance, il faut :

- dans la catégorie « *Règles supplémentaires* », spécifier des règles de chemin d'accès de type « non restreint » (exécution autorisée) pour chaque répertoire contenant des applications ;
- dans la catégorie « *Règles supplémentaires* », spécifier des règles de chemin d'accès de type « rejeté » (exécution interdite) pour les éventuels sous-répertoires en écriture pour les utilisateurs ;
- modifier les propriétés de « *Types de fichiers désignés* » pour retirer l'extension « LNK » afin que les raccourcis sur le bureau soient toujours fonctionnels ;
- choisir « *Tous les fichiers logiciels* », pour que les restrictions s'appliquent également aux fichiers DLL (contenant du code exécutable), et « *Tous les utilisateurs exceptés les administrateurs locaux* » dans les propriétés de « *Contrôle obligatoire* » ;
- dans la catégorie « *Niveaux de sécurité* », définir par défaut le niveau « *Rejeté* ».

De cette manière, il ne sera plus possible, pour un utilisateur, d'exécuter des programmes se trouvant par exemple sur une clé USB ou dans son profil (bureau, répertoire de documents personnels, répertoire temporaire, etc.). Bien que les stratégies de restriction logicielle réduisent l'exécution de programmes non désirés, ce mécanisme ne protège pas contre l'exécution de code arbitraire *via* l'exploitation d'une vulnérabilité dans un logiciel. Cependant, les éventuels programmes téléchargés par ce biais ne pourront pas être exécutés au prochain démarrage. Enfin, certains environnements d'exécution de scripts peuvent encore être utilisés (macro VBS, script .Net, etc.).

¹<http://technet.microsoft.com/fr-fr/sysinternals/bb897332.aspx>

5 Bonnes pratiques d'administration sous Windows : L'ouverture de session

Cet article est le premier d'une série qui va nous permettre de rappeler quelques bonnes pratiques d'administration sous Windows. En effet une grande partie de la sécurité d'un système d'information repose sur son administration. Aujourd'hui nous allons nous pencher sur l'ouverture de session (ou *login* interactif) et ses travers...

5.1 L'ouverture de session ou pourquoi s'en passer

Avec la généralisation des techniques type *Terminal Server / Remote Desktop*, le réflexe veut souvent que l'on ouvre une session à distance sur une machine pour l'administrer.

Cette méthode est certes très pratique mais aussi excessivement dangereuse...

En effet lors d'une ouverture de session de multiples mécanismes sont mis en œuvre, par exemple de nombreux programmes vont être lancés automatiquement via :

- les clés Run dans la base de registre :
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- les programmes du menu « Démarrer » :
C:\Documents and Settings\USERXXX\Menu Démarrer\Programmes\Démarrage
- les extensions du « Shell » ;
- les tâches planifiées ;
- etc...

Or, ces entrées sont évidemment très utilisées par les logiciels malveillants pour s'exécuter automatiquement, et ce, avec les droits de l'utilisateur connecté.

Outre ces entrées, certains logiciels malveillants qui s'exécutent typiquement dans un service, peuvent récupérer le jeton de sécurité de l'utilisateur connecté à la session interactive (ou à une session *Terminal Server*). Ce jeton peut alors servir à se faire passer pour l'utilisateur connecté, et permettre ainsi d'exécuter du code avec tous les droits de cet utilisateur.

On imagine alors facilement les dégâts que cela peut provoquer si un utilisateur de type « Administrateur du domaine » ouvre une session interactive sur une machine infectée...

L'exemple type est le ver *Conficker* : de très nombreux parcs de machines ont été infectés parce qu'un administrateur du domaine ouvrait une session sur une machine infectée, donnant ainsi les droits administrateur du domaine au code malveillant, qui en profitait pour se répliquer sur toutes les machines du domaine via les partages administratifs (C\$, IPC\$), sans même avoir besoin d'utiliser la moindre faille...

5.2 L'ouverture de session : les alternatives

Heureusement, il y a d'autres moyens d'administrer une machine à distance sans avoir besoin d'ouvrir une session interactive en tant qu'administrateur.

5.2.1 Les MMC, regedit, etc...

Windows possède de nombreux outils d'administration accessible via les MMC (*Microsoft Management Console*).

L'une des plus utiles est la MMC « Gestion de l'ordinateur » (lancer `compmgmt.msc`). Celle-ci permet, entre autres, de gérer :

- les journaux d'événements de la machine ;
- les dossiers partagés ;
- les utilisateurs et groupes locaux ;
- les périphériques ;
- les disques ;
- les services.

Et comme pour beaucoup de *MMC*, ceci est valable pour la machine locale mais aussi pour une machine distante (click droit sur « Gestion de l'ordinateur (local) » et « Se connecter à un autre ordinateur ... »).

Vous pouvez aussi accéder aux fichiers distants via les partages administratifs :

\\NomDeLaMachine\c\$

L'outil *Regedit* permet, quant à lui, d'éditer la base de registre de machines distantes (menu « Fichier », « Connexion au registre réseau... »).

5.2.2 RunAs ou « Exécuter en tant que »

Les outils précédemment cités permettent déjà de couvrir un large besoin en termes d'administration d'une machine. Il peut cependant rester des cas (rares) où l'ouverture d'une session interactive est obligatoire. Dans ce cas il faudra s'attacher à ouvrir une session en tant qu'utilisateur sans pouvoir puis démarrer une fenêtre de commandes via l'utilitaire *RunAs*.

L'ouverture d'une session interactive avec un compte administrateur local est aussi possible, mais dans ce cas il faut vérifier que le couple « Administrateur local » / « Mot de Passe » utilisé est unique sur chaque machine.

Nous reviendrons d'ailleurs en détail sur ce point la semaine prochaine.

6 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=1937>
- 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/>

7 Rappel des avis émis

Dans la période du 02 au 08 avril 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-154 : Vulnérabilité dans Firefox
- CERTA-2010-AVI-155 : Vulnérabilité dans Foxit Reader
- CERTA-2010-AVI-156 : Multiples vulnérabilités dans CA XOsoft
- CERTA-2010-AVI-157 : Vulnérabilité dans Emacs
- CERTA-2010-AVI-158 : Multiples vulnérabilités dans ClamAV
- CERTA-2010-AVI-159 : Vulnérabilité dans MediaWiki

- CERTA-2010-AVI-160 : Vulnérabilités dans VMware ESX Server

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

- CERTA-2009-AVI-448-003 : Vulnérabilités dans Xpdf et dérivés (ajout du bulletin de sécurité Debian pour Xpdf)
- CERTA-2010-AVI-093-001 : Vulnérabilité dans Asterisk (ajout de la référence CVE)
- CERTA-2010-AVI-161-001 : Multiples vulnérabilités dans McAfee Email Gateway (correction du lien vers les notes de mise à jour)

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique67.html

9 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.

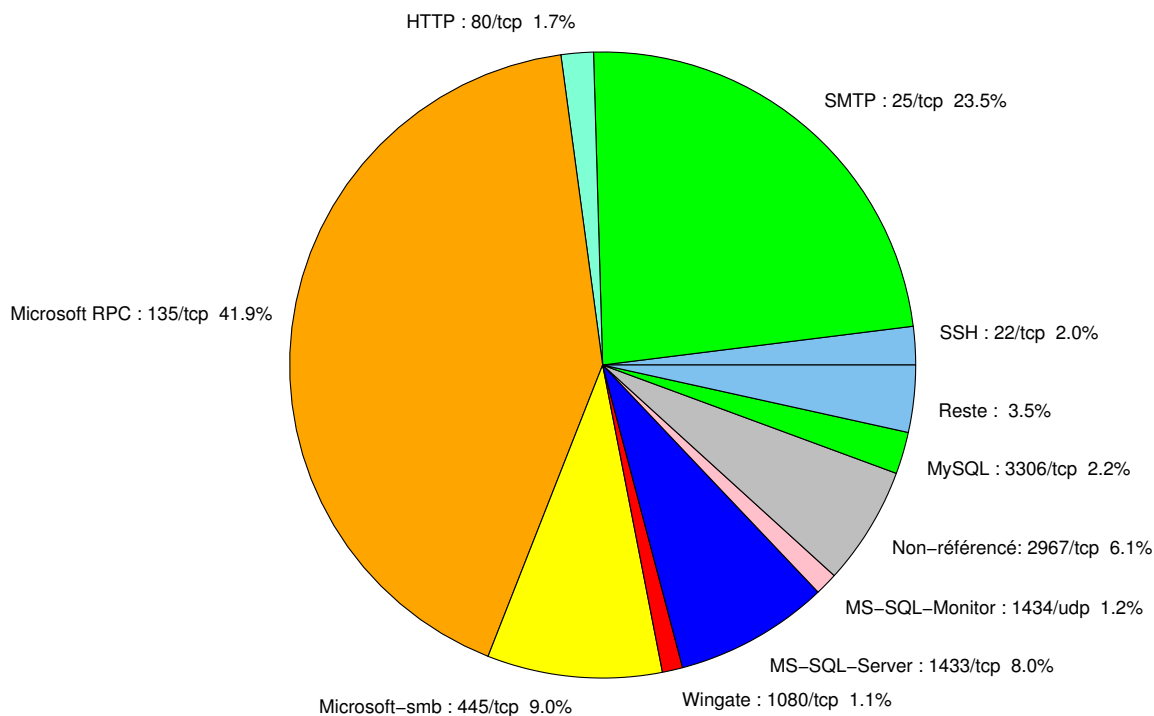


FIG. 1: Répartition relative des ports pour la semaine du 02 au 08 avril 2010

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 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
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	–	– CERTA-2007-AVI-008
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 CERTA-2007-AVI-321
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 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
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 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
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
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
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	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

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

port	pourcentage
135/tcp	41.9
80/tcp	26.57
25/tcp	23.48
445/tcp	9.08
1433/tcp	7.97
2967/tcp	6.11
3306/tcp	2.16
22/tcp	1.97
1434/udp	1.17
1080/tcp	1.05
4899/tcp	0.67
3389/tcp	0.49
3127/tcp	0.43
139/tcp	0.18
15118/tcp	0.12
2100/tcp	0.06

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

09 avril 2010 version initiale.