

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2010-08**

---

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-008>

---

### Gestion du document

Référence	CERTA-2010-ACT-008
Titre	Bulletin d'actualité 2010-08
Date de la première version	26 février 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-008.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-008/>

## 1 Durcissement de la configuration des systèmes Windows (1/4)

### 1.1 Introduction

Cet article fait parti d'une série de quatre articles, dont les trois suivants seront publiés dans les trois prochains bulletins d'actualité. Cette suite d'article a pour objectif d'aider à renforcer la configuration des systèmes Windows afin de limiter la surface d'attaque.

### 1.2 Généralités

Régulièrement, des vulnérabilités sont découvertes dans les systèmes d'exploitation. Les codes d'exploitation correspondant sont parfois publiés sur Internet avant la mise à disposition du correctif par l'éditeur concerné. Durcir la configuration des systèmes d'exploitation permet de réduire une partie des risques d'attaques. En effet, dans le cadre d'une stratégie de défense en profondeur, il convient de désactiver les fonctionnalités non utilisées et ainsi de se protéger des vulnérabilités inconnues pouvant toucher des composants superflus.

Cet article commence une série de recommandations ayant pour objectif de durcir la configuration d'un poste Windows client de type Windows XP (représentant actuellement la majorité des postes de travail professionnels), bien que la majorité des recommandations puisse s'appliquer à Windows 2000. Ces recommandations peuvent être mises en œuvre localement sur un poste ou sur un ensemble d'ordinateurs membres d'un domaine Windows, via les stratégies de groupe (GPO). Pour sa facilité de gestion, cette seconde méthode est à préférer aux modifications directes dans la base de registre.

La démarche de durcissement de la configuration des postes de travail a pour but de limiter les risques de compromission à distance ou d'élévation locale de privilèges, favorisant l'exécution d'un programme malveillant. Avant tout, il est essentiel que les utilisateurs n'aient pas les privilèges d'administration, c'est-à-dire membres des groupes locaux « Utilisateurs avec pouvoir » ou « Administrateurs », ou à plus forte raison, membres des groupes administratifs du domaine. La liste des applications nécessitant les droits d'administration doit être établie, afin de déterminer les privilèges effectivement nécessaires à leur fonctionnement et de trouver des moyens pour les contourner (installation d'une version plus récente des logiciels, modification des droits d'accès sur certains répertoires, modification de certaines fonctionnalités des logiciels, ...). À toute fin utile, l'outil `procmon`, distribué par Microsoft<sup>1</sup>, peut être utilisé pour diagnostiquer les tentatives infructueuses d'accès à des ressources par manque de droits.

D'autre part, pour installer plus rapidement des nouveaux postes de travail, l'image d'un poste de référence (*master*) est généralement utilisée. La configuration de cette image doit être formalisée : la traçabilité des modifications apportées au fur et à mesure est importante pour éviter une dérive du paramétrage non maîtrisée. Dans ce cadre, une documentation sur les postes de travail doit être rédigée et doit contenir au minimum :

- les paramètres activés liés au durcissement de la configuration ;
- les incompatibilités rencontrées avec des logiciels utilisés, pouvant empêcher l'application de certains paramètres ;
- la liste des profils utilisateurs nécessitant des configurations spécifiques sur leurs postes (par exemple les administrateurs système) et les différences par rapport à un profil standard ;
- les actions à effectuer et les paramètres à configurer manuellement après l'installation du poste, pour finaliser la configuration des postes de travail.

La configuration de référence doit être régulièrement mise à jour et vérifiée pour éviter un effet de configuration « historique » et obsolète des postes.

### 1.3 Désactivation des sous-systèmes inutilisés

La récente publication d'une vulnérabilité de type élévation de privilèges affectant certaines versions de Microsoft Windows (CERTA-2010-AVI-073<sup>2</sup>) est l'occasion de désactiver les sous-systèmes inutilisés (POSIX, OS/2 et MS-DOS), actuellement caduques. Ces sous-systèmes permettent de supporter d'anciennes applications en leur offrant un environnement d'exécution adapté.

Les sous-systèmes POSIX et OS/2 ne sont présents que sous Windows 2000 et ne sont plus supportés par défaut à partir de Windows XP. Ainsi, sous Windows 2000, il est conseillé de les désactiver en supprimant les valeurs dénommées `Posix` et `Os2` dans la clé :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session  
Manager\SubSystems.
```

Le sous-système MS-DOS offre quant à lui le support des applications 16 bits. Celles-ci correspondent par exemple à `command.com` et aux applications Windows 16 bits. Bien que ces applications soient rares, une phase d'inventaire et de qualification est recommandée. La désactivation de l'exécution des applications 16 bits peut entraîner des dysfonctionnements d'anciennes applications, cette recommandation devrait être appliquée sur tous les systèmes qui n'utilisent pas d'application 16 bits. Ce sous-système est activé par défaut sur tous les systèmes Windows de type 32 bits.

À partir de Windows 2000, le sous-système peut être désactivé en ajoutant une valeur dénommée *VDMDisallowed* de type *DWORD* dont la donnée vaut *1* dans la clé :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppCompat.
```

<sup>1</sup><http://technet.microsoft.com/fr-fr/sysinternals/bb896645.aspx>

<sup>2</sup><http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-073/>

À partir de Windows XP, ce paramètre peut être positionné *via* les stratégies de groupe. Il se trouve dans la *Configuration ordinateur (Modèles d'administration, Composants Windows, Compatibilité des applications)*, est dénommé « *Empêcher l'accès aux applications 16 bits* » et doit avoir la valeur « *activé* ».

## 2 Un réseau de machines zombies d'un type un peu particulier

Cette semaine des chercheurs ont découvert un code malveillant d'un type un peu particulier. Sa spécificité ne réside pas dans son mode de fonctionnement puisque de ce point de vue il est tout à fait similaire à ce qu'on pourrait trouver dans d'autres réseaux de machines zombies. Ainsi, par exemple, son canal de contrôle s'appuie très classiquement sur le protocole IRC.

La singularité de ce réseau vient du fait que le code malveillant mis en œuvre a pour cible les routeurs grand public et leur système d'exploitation. Ainsi ce code nommé « *Chuck Norris* » s'attaque à des routeurs dont le microgiciel (*Firmware*) est basé sur GNU/Linux, présentant un service d'administration à distance ouvert ainsi qu'un mot de passe faible ou laissé par défaut. Il peut également profiter de vulnérabilités propres au système sur certains types de routeurs.

Plus largement, ce code pourrait infecter tout équipement basé sur l'architecture matérielle MIPS ayant pour système d'exploitation GNU/Linux. Ainsi certains routeurs de FAI ou certains terminaux TV et satellites seraient concernés.

Pour ce qui est de ses possibilités, elles sont très classiques. On trouve des fonctionnalités de capture de trafic, des capacités d'attaque par saturation (DDOS) ou bien encore d'usurpation de serveur DNS légitime afin de rediriger le ou les utilisateurs vers un site malveillant.

Il est à noter que ce code est entièrement résident en mémoire et ne subsiste pas à un redémarrage de l'équipement.

### Recommandations :

Afin d'éviter une compromission par ce type de code, il convient de respecter les recommandations habituelles suivantes :

- désactiver les services d'administration à distance autant que faire se peut ;
- mettre un mot de passe robuste sur le compte administrateur de l'équipement si cela est possible ;
- mettre à jour le microgiciel de l'équipement systématiquement à la publication d'une nouvelle version.

## 3 La technologie DEP (Data Execution Prevention) (1/3)

Au cours des prochains bulletins d'actualité, nous allons faire un tour d'horizon de la technologie *DEP* (ses principes, son administration, ses limites...) Ce premier article a pour but de présenter le principe de fonctionnement de cette technologie.

### 3.1 Qu'est ce que DEP?

*DEP* est une technologie implémentée dans Windows dont le but est de limiter l'exploitation des vulnérabilités logicielles.

Il existe deux types de *DEP*, le *DEP* logiciel sur lequel nous ne nous étendrons pas car il s'agit simplement d'un renforcement des contrôles du mécanisme de gestion des exceptions, et le *DEP* matériel qui sera notre sujet principal.

Le *DEP* matériel utilise une spécificité des processeurs récents :

- AMD (*no-execute page-protection NX*) : implémenté à partir de la famille des Athlon 64;
- Intel (*Execute Disable bit*): implémenté à partir de la famille des Pentium 4.

Ce support matériel permet de marquer une page mémoire comme «non exécutable». Si un programme essaie d'exécuter du code qui se trouve dans une telle page, alors le processeur lèvera une exception (gérée par Windows) qui entraînera, dans la plupart des cas, l'arrêt inopiné de cette application.

### 3.2 Pourquoi DEP?

La plupart des tentatives d'exploitation de vulnérabilités passent par l'exécution de code qui réside dans des pages de données (marquées comme "non exécutable" si *DEP* est activé). Voici ci dessous un schéma représentant le chargement d'un tel document :

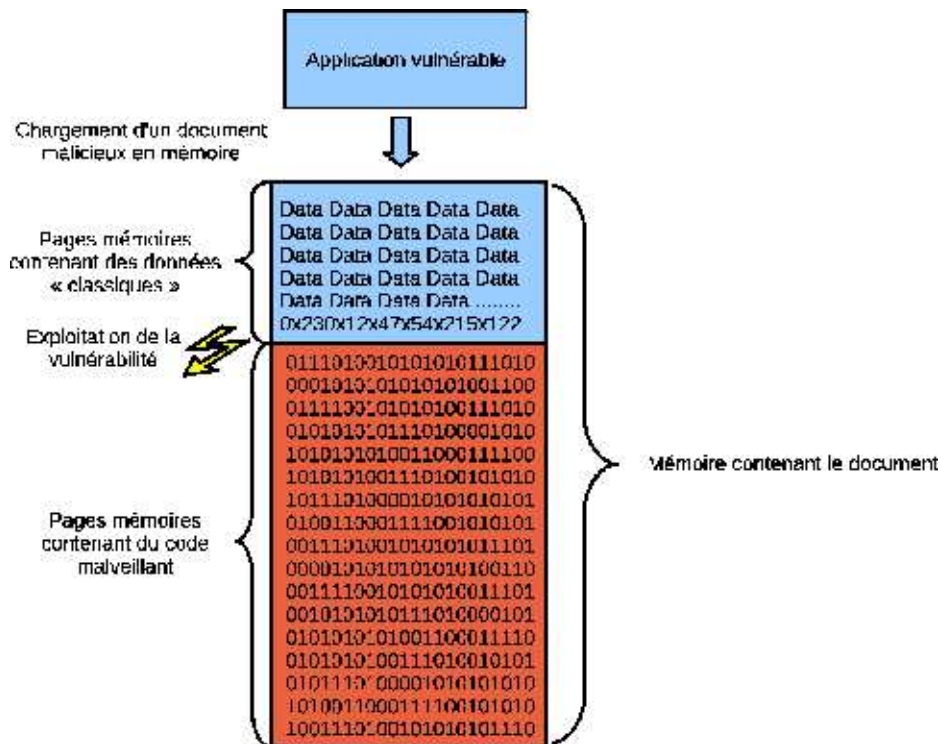


FIG. 1: Représentation du chargement d'un fichier en mémoire

Le but de *DEP*, dans ce cas, sera non pas de corriger la vulnérabilité, mais d'empêcher l'exécution du code malveillant inclus dans le document.

### 3.3 Quels sont les pré-requis

Comme spécifié précédemment, il faut posséder un processeur relativement récent (la plupart des ordinateurs vendus après 2005 sont compatibles). Coté logiciel, il faut être en Windows XP SP2 ou Windows 2003 SP1 (ou supérieur), ces deux *Service Pack* ayant introduit la technologie *DEP*.

### 3.4 Au prochain épisode...

La semaine prochaine, nous nous pencherons sur l'administration et la configuration de *DEP*

## 4 Surfer anonyme sur Internet, qu'en est-il ?

L'anonymat sur Internet est un sujet récurrent. Il trouve sa justification pour les organisations ayant besoin d'un fort besoin de confidentialité, mais aussi pour le particulier soucieux de conserver son droit au respect de la vie privée (article 9 du code civil français). Cette note peut être vu comme une suite à celle du 5 février 2010, à propos du ciblage comportemental sur Internet : <http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-005/>.

A l'occasion de la sortie de l'extension Google Sharing pour Firefox, il est intéressant de rappeler ce qu'est un *proxy* (serveur mandataire) anonyme. Google Sharing sera lui aussi détaillé dans l'article. L'objectif est de dresser un rapide panorama des différentes techniques utilisées par ces serveurs pour apporter cet anonymat, tout relatif, à leurs utilisateurs.

Autant le dire tout de suite, l'anonymat parfait est difficilement atteignable. Même en vous rendant dans un cybercafé avec des lunettes noires et une barbe de plusieurs mois, vous n'écartez pas la possibilité que quelqu'un puisse vous reconnaître et identifier votre connexion. L'anonymat est donc une notion relative.

Il existe essentiellement deux techniques d'anonymisation en utilisant des serveurs mandataires: les *proxys* anonymes solitaires et les réseaux de *proxys* anonymes.

## 4.1 Proxy anonyme

Le *proxy* anonyme solitaire est le plus répandu. Son utilisation est souvent très simple. Beaucoup d'entre eux hébergent un site Web auquel on peut se connecter, site duquel il est possible d'envoyer des requêtes *HTTP* sur l'Internet. La source de la requête *HTTP* vers le site Web devient donc le *proxy* et non plus l'émetteur initial, ce qui permet de rendre invisible l'IP de l'émetteur au site qu'il contacte. Nous venons de prendre l'exemple de requêtes *HTTP*, mais le concept de *proxy* anonyme s'applique à tous types de trafic sur l'Internet.

Un bon *proxy* anonyme supprime tous les éléments pouvant identifier l'émetteur initial de la requête relayée (informations dans l'en-tête de la requête, adresse IP source, etc.), et il permet à l'émetteur initial d'utiliser un protocole de chiffrement (par exemple *TLS/SSL* pour les requêtes applicatives) pour ses communications avec le *proxy*. Le *proxy* utilisera à son tour un chiffrement pour la requête relayée si la cible demandée est en mesure de supporter du trafic chiffré. En général, les *proxys* anonymes ne sont pas appropriés pour visiter les sites Web qui nécessitent des cookies pour fonctionner correctement.

Google Sharing est un exemple de *proxy* anonyme solitaire. Contrairement à ce que son nom pourrait laisser entendre, Google Sharing n'est pas une application Google de plus. C'est une extension pour Firefox redirigeant toutes les requêtes Google de l'utilisateur vers un *proxy* anonyme solitaire. Le but affiché étant d'empêcher le moteur de recherche de récolter des informations sur ses utilisateurs. Le *proxy* anonyme de Google Sharing reçoit donc toutes les requêtes Google (en *HTTPS*) des utilisateurs et les relaie en *HTTP* vers Google après avoir pris soin de les anonymiser. C'est-à-dire après avoir enlevé toutes les informations pouvant identifier l'émetteur de la requête : certains champs de l'en-tête *HTTP*, l'adresse IP source, et bien sûr les *cookies*, c'est pourquoi Google Sharing ne fonctionne pas avec Gmail, ni avec aucune autre application Google nécessitant des *cookies*.

Outre les attaques possibles sur ce type de serveur, le concept de *proxy* anonyme repose sur la confiance que l'on accorde au propriétaire dudit *proxy*. Les informations que le site Web n'aura pas reçues seront détenues par le propriétaire du *proxy*. On se rend bien compte que le problème est en fait déplacé, ce n'est plus le site Web qui détient des informations privées, mais l'intermédiaire censé anonymiser la connexion.

## 4.2 Réseau de proxys anonymes

Comme vu précédemment, un problème évident des *proxys* anonymes est leur dépendance à un unique propriétaire. Les réseaux de *proxys* anonymes ont pour objectif de remédier à cela. L'idée est de former un réseau dans lequel chaque nœud a une connaissance limitée de son environnement, suffisamment limitée pour qu'il soit incapable de reconstruire la requête de l'émetteur initial dans son entier. Ceci nécessite bien évidemment qu'un maximum de propriétaires se partagent les nœuds du réseau, en tout cas assez pour conserver cette propriété de non reconstruction de la requête émetteur par un unique propriétaire.

Ces réseaux mettent en place des protocoles de communication applicatifs qui leurs sont propres, souvent agrémentés de plusieurs couches cryptographiques. L'exemple de réseau anonymisant le plus connu est Tor (<http://www.torproject.org>), mais il en existe d'autres : *I2P*, *GNUnet*, *Freenet*, ...

Tor est le plus populaire des réseaux anonymisants, et malgré la lenteur de connexion caractéristique de ce type de réseau, de nombreuses organisations et produits de sécurité l'utilisent pour véhiculer des données sensibles.

Cependant, bien que ces réseaux remplissent globalement leur rôle, ils ne peuvent pas garantir l'anonymat de tous les canaux d'information circulants entre l'utilisateur et la cible finale, par exemple : le support physique, le contenu actif des réponses *HTML* (*JavaScript*, *Flash*, applique Java, *ActiveX*, ...), les communications ne passant pas par le réseau anonymisant, etc. Ces réseaux ne sont pas non plus dénués de vulnérabilités protocolaires et sont susceptibles de faire l'objet d'attaques.

## 4.3 Limites de ces techniques

Les serveurs mandataires d'anonymisation, qu'ils soient en réseau ou non, peuvent être vulnérables à des attaques extrêmement simples comme l'injection de code client actif dans les pages *HTML* renvoyées en réponse aux utilisateurs, typiquement du *JavaScript* ou une applique Java permettant de récupérer l'adresse IP privée ou publique de l'utilisateur. Ce type d'attaque a notamment été mené contre le réseau *Tor* avec succès et a permis d'obtenir par la suite de nombreuses informations sensibles circulant sur le réseau.

Ces systèmes anonymisants sont des serveurs comme les autres, ils peuvent être compromis par une attaque au même titre que n'importe quel autre serveur sur l'Internet. Aussi, certains sont malveillants et peuvent infecter les utilisateurs.

Enfin, il n'est pas rare que la police saisisse ce type de serveur pour les besoins d'une enquête, de nombreux délits étant commis en utilisant des services d'anonymisation.

Le CERTA recommande donc la plus grande prudence dans l'utilisation de ce type de service.

## 5 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/>

## 6 Rappel des avis émis

Dans la période du 19 au 25 février 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-088 : Vulnérabilité dans l'antivirus Avast!
- CERTA-2010-AVI-089 : Vulnérabilité dans Adobe Download Manager
- CERTA-2010-AVI-090 : Vulnérabilité dans WordPress
- CERTA-2010-AVI-091 : Vulnérabilités dans TYPO3

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

- CERTA-2010-AVI-077-001 : Multiples vulnérabilités dans Google Chrome (ajout des références CVE)
- CERTA-2010-AVI-082-001 : Vulnérabilités dans Mozilla Firefox (ajout des références aux bulletins Debian, Fedora, Mandriva, RedHat et Ubuntu)
- CERTA-2010-AVI-087-001 : Multiples vulnérabilités dans plusieurs produits Symantec (ajout d'une troisième vulnérabilité)

## 7 Actions suggérées

### 7.1 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.

## **7.2 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.

## **7.3 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.

## **7.4 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.

## **7.5 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.

## **7.6 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.

## **7.7 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](http://www.ssi.gouv.fr/site_rubrique67.html)

## 8 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

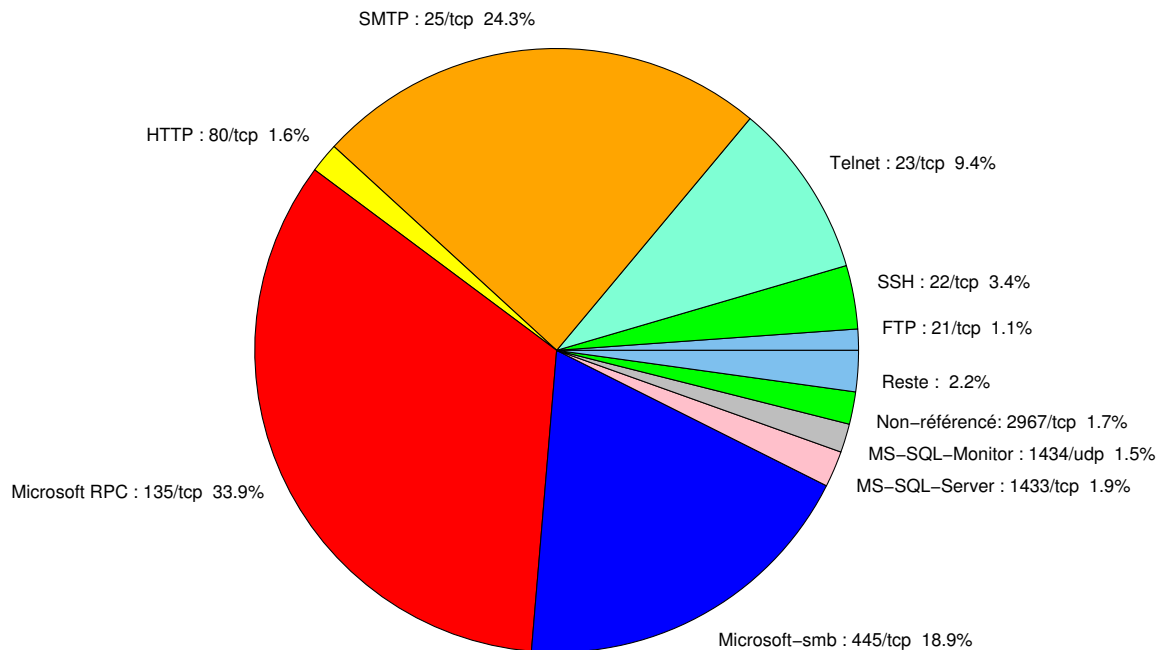


FIG. 2: Répartition relative des ports pour la semaine du 19 au 25 février 2010

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	33.86
25/tcp	24.26
445/tcp	18.93
23/tcp	9.4
22/tcp	3.4
1433/tcp	1.93
2967/tcp	1.73
80/tcp	1.6
1434/udp	1.53
21/tcp	1.13
4899/tcp	0.93
3389/tcp	0.46
3128/tcp	0.33
3306/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

26 février 2010 version initiale.