Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 octobre 2009
N° CERTA-2009-ACT-040

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2009-40**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2009-ACT-040 |
| Titre | Bulletin d'actualité 2009-40 |
| Date de la première version | 02 octobre 2009 |
| 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-2009-ACT-040.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-2009-ACT-040/

## 1 Incidents de la semaine

### Fichier de mots de passe disponible depuis l'Internet

Cette semaine, un correspondant du CERTA a signalé qu'un de ses serveurs de messagerie avait été utilisé pour un envoi massif de messages non sollicités (*spam*). Ces envois ont été réalisés depuis des comptes légitimes du *webmail* de cet organisme.

Les incidents de ce type sont malheureusement assez courants. Ils font généralement suite à l'obtention frauduleuse des identifiants de connexion via des messages faisant croire à une nécessité de mettre à jour ces informations. Les victimes sont dans ce cas redirigées vers un site Web malveillant qui collecte les données.

Cet incident est toutefois différent de ce que l'on rencontre habituellement. En effet, les attaquants ont récupéré les identifiants de connexion en recherchant spécifiquement, à l'aide de moteurs classiques tels que *Google*, des documents contenant des mots de passe en clair.

De tels problèmes n'ont pas de solution simple, même si la vigilance des webmestres et la sensibilisation des utilisateurs permettent d'empêcher ces négligences. Il est toutefois important de signaler ici le rôle du RSSI qui a, par la lecture des journaux de ses serveurs, permis d'identifier immédiatement l'incident et d'en découvrir l'origine.

# 2 Déni de service : des mesures de protection à contractualiser avec ses fournisseurs d'accès

Le déni de service est une des principales malveillances susceptibles de frapper un service exposé à l'Internet. Si la réussite d'une telle attaque n'implique pas la compromission des données d'un site, une indisponibilité peut être gravement pénalisante d'un point de vue opérationnel, par exemple lorsqu'elle touche un service d'infrastructure comme le système de nommage DNS ou des routeurs de cœur de réseau, mais également en termes financier ou d'image de marque pour une entité dont la visibilité sur Internet est cruciale.

Souvent considéré comme un risque résiduel et généralement mal appréhendé y compris par les techniciens, le déni de service doit être pris en compte aux niveaux technique et organisationnel, et suppose des procédures de traitement d'incident qui doivent être contractualisées avec les prestataires d'hébergement et les fournisseurs d'accès à l'Internet. Les méthodes de protection supposent donc des mécanismes de surveillance des sites, afin de déterminer les contre-mesures qui seront les plus adaptées à l'attaque subie. Quelques exemples types suivent.

## 2.1 Déni de service lié à une surcharge excessive (aspiration de contenu, effet « slashdot », ...)

Ce premier cas de figure peut sembler hors sujet mais cette situation est relativement classique. Il ne s'agit pas à proprement parler d'une attaque en déni de service, mais plutôt d'une sollicitation *a priori* légitime mais excessive, qui est susceptible d'engendrer un ralentissement voire une indisponibilité du site.

Les pistes d'amélioration sont notamment les suivantes :

- concevoir correctement son infrastructure, en termes de :
  - dimensionnement système et réseau en tenant compte des pics de trafic prévisibles : nombre d'équipements, de liens de connectivité, de façon à assurer robustesse et redondance ;
  - localisation et mutualisation de l'hébergement, afin d'évaluer les risques de dommages collatéraux susceptibles d'être causés par une attaque ou une saturation réseau. Par exemple la saturation de la bande passante du serveur Web d'un organisme ne devrait pas avoir d'impact sur son accès Internet en sortie ou sur sa messagerie électronique ;
- réaliser une répartition et un équilibrage de charge par exemple à l'aide des mécanismes suivants :
  - en entrée de l'infrastructure à l'aide d'équipements spécifiques qui travailleront aux niveaux réseau et applicatifs ;
  - à l'aide d'un mécanisme à jeton tournant (*round robin*) basé sur DNS ;
- ajuster finement les paramètres des piles réseaux de ses serveurs et les options de traitement des requêtes des serveurs HTTP, le cas échéant ;
- séparer les contenus statiques et dynamiques publiés, en privilégiant notamment des systèmes et serveurs HTTP minimalistes pour la délivrance des contenus statiques ;
- optimiser ses applications, afin d'éviter que des requêtes ne soient trop coûteuses vis-à-vis du nombre des opérations réalisées (par exemple : nombre de transactions aux bases de données, ou de procédures exécutées par les serveurs d'applications) ou encore de la taille du contenu envoyé (taille des images, contenu multimédia, ...) ;
- gérer la qualité de service de son site, par exemple en limitant la bande passante ou encore le nombre de connexions simultanées en provenance d'une même adresse, avec les limitations d'un tel mécanisme par rapport aux mécanismes de traduction d'adresses ou l'utilisation de relais applicatifs susceptibles de masquer derrière une seule adresse IP, de multiples clients. En dernier recours, un filtrage par adresse IP pourra être mis en œuvre, avec toutes les précautions d'usage que cela suppose, notamment filtrer les adresses sur la base d'une connexion TCP pleinement établie uniquement, afin de limiter les risques d'usurpation ;
- louer ponctuellement (en cas de pic de trafic annoncé) les services d'un réseau de type *CDN* (*Content Delivery Network*), qui effectuera une duplication partielle des sites et permettra une distribution géographique de serveurs cache au plus proche des clients, en combinant géolocalisation sur la base des adresses IP et aiguillage DNS sélectif. L'emploi d'une telle prestation de service devra faire l'objet d'une analyse de risques afin d'estimer sa conformité à la politique de sécurité de l'organisme (en particulier, la perte de confidentialité occasionnée par la réalisation des transactions sur une infrastructure tierce).

## 2.2 Déni de service par malveillance

### 2.2.1 Épuisement des ressources systèmes

Premier cas de figure, l'attaque s'appuie sur les protocoles HTTP ou TCP, avec un établissement de connexion complet, et consiste en l'épuisement des ressources système et non en l'épuisement de la bande passante. Dans ce cas, un filtrage réseau des adresses sources peut être effectué, afin que les connexions TCP ou requêtes HTTP successives soient filtrées en amont et n'atteignent pas les serveurs. Cette détection sera effectuée au niveau des pare-feu, qui détecteront les connexions TCP successives, ou encore au niveau des serveurs frontaux, qui détecteront les requêtes HTTP successives. Cette détection peut être complexe dans la pratique, une attaque de type *slowloris* sur un serveur *Apache* sera difficilement détectable si elle provient d'adresses IP multiples effectuant des connexions « légitimes ». Un agent de surveillance positionné au niveau du serveur Web sera donc le plus à même de détecter une attaque en cours.

Dans tous les cas, ce scénario nécessite anticipation et préparation : des indicateurs de qualité de service (taux de disponibilité des sites, mesure des temps de réponse, ...) et de fonctionnement (indicateurs systèmes, réseaux, ...) devront être définis et surveillés afin de participer à la détection d'incident.

Ce type d'attaque qui porte sur des protocoles connectés nécessite, pour l'attaquant, d'employer une adresse IP qui ne soit pas falsifiée : le filtrage temporaire des adresses incriminées est donc une solution envisageable, en prenant garde au fait que cette contre-mesure ne soit pas elle même un vecteur de déni de service pour la plate-forme. Ce filtrage peut donc être réalisé au niveau de la plate-forme même, ou encore en amont, par l'hébergeur et le fournisseur d'accès (à l'aide d'un mécanisme de routage nul ou *blackhole route*, par exemple, au niveau BGP, via un mécanisme de type *RTBH with uRPF* décrit dans le RFC 5635).

### 2.2.2 Épuisement de la bande passante

Second cas de figure, l'attaque s'appuie sur des protocoles non connectés, type ICMP ou encore UDP, et visent un épuisement de bande passante : la contre-mesure est dans ce cas beaucoup plus complexe, car il n'est théoriquement plus possible de filtrer les adresses IP sources à l'origine des paquets, dans la mesure où elles sont susceptibles d'être falsifiées.

Ce propos doit être modéré : les attaques en déni de service ne font pas nécessairement usage d'adresses IP falsifiées, dans la mesure où les fournisseurs d'accès ont généralement pour bonne pratique d'interdire en bordure de leurs systèmes autonomes les adresses IP sources qui ne leur sont pas attribuées. En pratique, c'est donc plutôt la multiplication des adresses IP sources, liées à l'utilisation d'un *botnet*, qui rendra difficile ce filtrage que le fait qu'une falsification soit potentiellement réalisée.

Toujours dans ce cas de figure, filtrer le trafic en entrée de la plate-forme hébergée est donc illusoire, dans la mesure où la bande passante allouée par l'opérateur sera déjà saturée et le déni de service sera de toute façon effectif. Les mesures de protection incombent donc au fournisseur d'accès internet, avec lequel il conviendra de contractualiser soigneusement les procédures de détection et de traitement d'incident.

Si cette attaque massive vise explicitement les adresses IP de la plate-forme, il peut être envisagé de basculer le trafic vers un site de secours qui disposerait d'un plan d'adressage IP alternatif, par l'intermédiaire du protocole DNS, en fixant des compteurs d'expiration courts, avec le risque d'un dysfonctionnement temporaire pour les clients d'opérateurs disposant d'une réponse à *TTL* long en cache. Si cette attaque massive suit le nom de domaine, la précédente contre-mesure sera inefficace. Dans une telle situation, la solution la plus immédiate pour l'opérateur sera de *null-router* les adresses IP du site ciblé par l'attaque, en bordure de son réseau (via BGP encore une fois, avec une technique de type filtre *RTBH*), ce qui limitera l'accessibilité du site mais permettra à l'opérateur de préserver sa propre infrastructure. Une nouvelle fois, un filtrage sur les adresses IP impliquées dans l'attaque pourra être mis en œuvre (toujours via BGP et la technique *RTBH with uRPF*).

D'autres solutions sont susceptibles d'être proposées par l'hébergeur et l'opérateur, mais seront de toute façon à contractualiser via le cahier de clauses techniques particulières, qui encadrera la prestation d'hébergement. En particulier, il faudra également surveiller et secourir les éventuels services annexes (DNS, en particulier) nécessaires au bon fonctionnement de la plate-forme, ou encore de prévoir un fonctionnement dégradé en mode France, afin de limiter la connectivité aux seuls internautes français afin de limiter la portée d'une attaque.

## 2.3 Documentation

– RFC 5635 :
http://www.ietf.org/tfc/rfc5635.txt

# 3 Microsoft Security Essentials

Depuis cette semaine, la version finale (1.0) de l'antivirus gratuit de Microsoft dénommé *Microsoft Security Essentials* est disponible en téléchargement sur le site de l'éditeur.

Basé sur le même moteur que *OneCare*, l'antivirus se veut basique et simple d'utilisation. Il remplace l'anti *spyware* gratuit *Windows Defender*, et fait suite à la tentative infructueuse de la part de Microsoft de vendre un produit payant pour les utilisateurs (*Windows Live OneCare*).

Il est à noter que l'utilisation de *Microsoft Security Essentials* semble nécessiter la participation à *Microsoft SpyNet*, l'option n'étant pour le moment pas désactivable. Ceci signifie que certaines informations sur le système, éventuellement personnelles, seront envoyées à l'éditeur (cf. déclaration de confidentialité sur le site de l'éditeur).

Enfin, le CERTA rappelle qu'un logiciel antivirus, s'il peut aider à détecter la présence de codes malveillants, repose sur une base de signatures qui doit être créée par les éditeurs à partir de souches. Dans ce sens, un antivirus sera toujours en retard dans le temps par rapport à l'apparition des codes malveillants. Les utilisateurs et administrateurs ne doivent donc pas se reposer uniquement sur de telles solutions, insister sur des mises à jour régulières des applications utilisées et l'application des bonnes pratiques en matière de sécurité des systèmes d'information.

### Documentation

– Téléchargement de Microsoft Security Essentials :
http://www.microsoft.com/security_essentials/default.aspx

# 4 Un contrôle d'ordinateurs zombies imagé

Un *botnet*, ou « réseau d'ordinateur zombies », est composé de machines compromises attendant des ordres pour agir. Ainsi le contrôleur du réseau peut demander aux ordinateurs sous son contrôle de participer à des campagnes de pourriels, de mener des attaques en déni de service ou de propager du code malveillant. Cependant, pour que cela fonctionne il faut que les machines reçoivent un ordre. S'il est assez courant que celles ci utilisent l'IRC ou une requête HTTP pour attendre leurs directives, une nouvelle méthode a été abordée cette semaine. Il s'agit encore d'une requête HTTP mais qui ne charge plus du texte mais une image, ou ce qui y ressemble.

En effet, la requête demande un fichier *JPEG* et le serveur répond un contenu qu'il annonce comme étant une image (*HTTP content-Type Header:image/jpeg*), qui commence comme une image (les 32 octets d'un entête *JPEG*) mais qui continue avec des commandes obscurcies qui seront utilisées par le code malveillant en attente d'instruction. Ces commandes ne formant pas une image correcte, il est possible d'identifier ce type d'échange en cherchant les images malformées.

# 5 Chrome Frame

La société `Google` a publié au mois d'août 2009, une extension (*plugin*) nommée `Google Frame` destinée aux navigateurs de `Microsoft Internet Explorer 6` et `Internet Explorer 7`. Celle-ci a pour effet d'installer dans le contexte du navigateur le moteur de rendu `Webkit` en plus du moteur de rendu classique d'`Internet Explorer` à savoir `Trident`. Il est ainsi possible pour l'utilisateur d'utiliser en parallèle deux moteurs de rendu.

C'est à la charge du concepteur de la page web de définir un marqueur particulier qui indiquera au navigateur d'utiliser `Google Frame` à la place de `Trident`. Ainsi, c'est le contenu de la page web qui déclenchera ou pas l'activation de tel ou tel autre moteur.

Selon `Google`, cela permettrait aux utilisateurs d'`Internet Explorer` d'effectuer une migration « en douceur » vers leur propre navigateur : `Google Chrome` qui utilise nativement `Webkit` pour fonctionner.

Il n'est pas du propos de cet article d'argumenter sur la qualité ou la robustesse de tel ou tel moteur de rendu. En revanche, il convient de noter que l'ajout ou le remplacement d'un moteur de rendu dans un navigateur n'est pas sans conséquence sur la sécurité du navigateur « accueillant ». On ne s'attardera pas non plus, ici, sur la version 6 d'`Internet Explorer` qui est plutôt en fin de cycle de vie. Par contre, la version 7 d'`Internet Explorer` est encore très fréquemment utilisée et n'a pas encore été supplantée par la version 8. On pourra donc s'interroger sur les effets de l'ajout d'un tel *plugin* dans ce navigateur.

De manière générale, le fait d'installer une extension dans un navigateur, quel qu'il soit, fait que sa surface d'attaque s'en trouve augmentée. Rajouter un moteur de rendu en tant qu'extension revient à ajouter toutes les vulnérabilités potentielles inhérentes à ce moteur.

Ce faisant, l'utilisateur doit également bien avoir conscience que lorsqu'une vulnérabilité touchera `Google Chrome`, il faudra très certainement qu'il mette à jour l'extension `Chrome Frame` pour `Internet Explorer`.

On peut aussi s'interroger légitimement sur la façon dont seront gérées les données de connexions ou les fichiers de mise en cache. Quel rôle sera dévolu à quel moteur ou quel composant ? Comment fonctionnera la manipulation des certificats et du secret dans le navigateur avec deux moteurs différents ?

Par ailleurs, le CERTA recommande souvent lors d'alertes d'utiliser des navigateurs alternatifs. Avec une telle extension, `Internet Explorer` présentera un risque double de ne plus être utilisable. Par ailleurs comme le choix du moteur à utiliser dépend du contenu de la page visitée, il est facile pour un attaquant de déclencher l'utilisation du composant vulnérable.

On pourrait argumenter sur le fait que l'utilisation d'une telle extension apporte à des navigateurs vieillissants des améliorations en termes de sécurité comme une boîte à sable (*sandbox*) par exemple. Mais, dans ce cas, ne vaut-il pas mieux utiliser un autre navigateur complet plutôt qu'une solution hybride dont on ne maîtrise pas forcément le comportement ?

# 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 26 septembre au 01 octobre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-404 : Vulnérabilité de Snort
- CERTA-2009-AVI-405 : Vulnérabilité dans Apple iTunes
- CERTA-2009-AVI-406 : Vulnérabilité du noyau Linux
- CERTA-2009-AVI-407 : Vulnérabilité de Apple Xsan
- CERTA-2009-AVI-408 : Multiples vulnérabilités dans IBM HTTP Server
- CERTA-2009-AVI-409 : Vulnérabilité de BlackBerry
- CERTA-2009-AVI-410 : Vulnérabilité dans IBM Lotus Connections
- CERTA-2009-AVI-411 : Vulnérabilité dans IBM Informix Dynamic Server

– CERTA-2009-AVI-412 : Vulnérabilités dans IBM DB2
– CERTA-2009-AVI-413 : Vulnérabilités dans HP-UX
– CERTA-2009-AVI-414 : Vulnérabilité dans le navigateur Google Chrome
– CERTA-2009-AVI-415 : Vulnérabilité dans Novell NetWare
– CERTA-2009-AVI-416 : Vulnérabilité dans HP StorageWorks
– CERTA-2009-AVI-417 : Vulnérabilités dans IBM AIX

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

– CERTA-2009-AVI-259-001 : Vulnérabilité du serveur Samba (ajout de la référence au bulletin de sécurité Sun)
– CERTA-2009-AVI-384-001 : Vulnérabilité de FreeRADIUS (ajout des références aux bulletins RedHat et Ubuntu)

# 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 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.

## 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 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.

### 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_rubrique63.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.

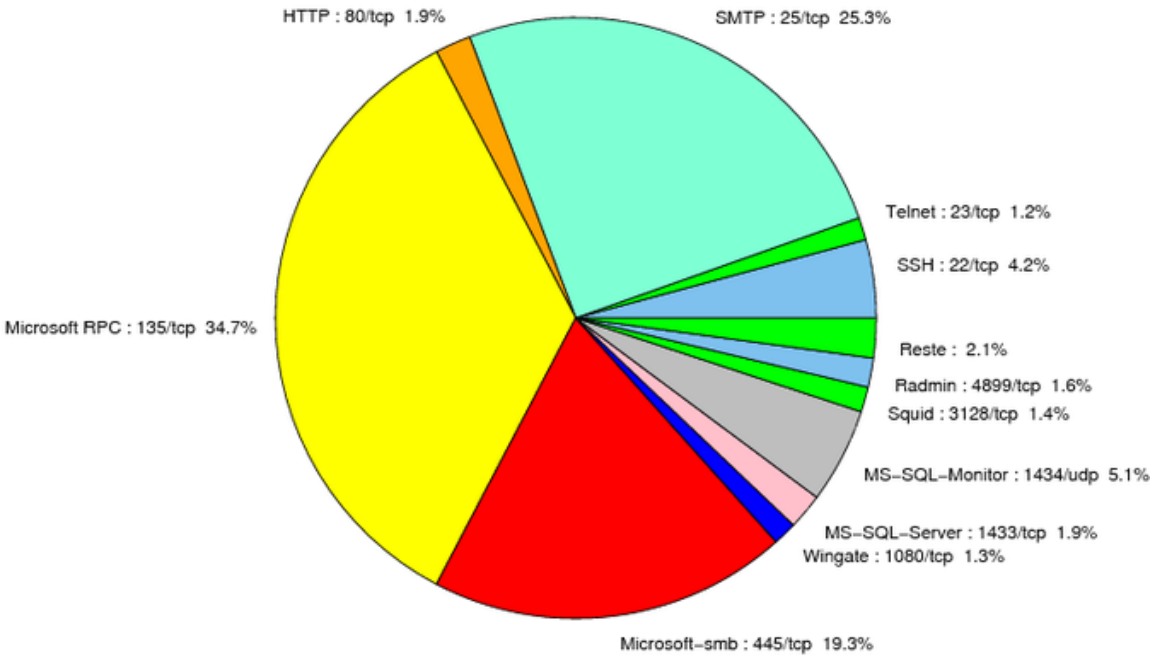


FIG. 1: Répartition relative des ports pour la semaine du 26 septembre au 01 octobre 2009

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|---|---|---|---|---|
| 21 | TCP | FTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 23 | TCP | Telnet | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>CERTA-2007-ALE-005-001 |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 106 | TCP | MailSite Email Server | – | –<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |

| | | | | |
|---|---|---|---|---|
| | | | | http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT |
| 143 | TCP | IMAP | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 389 | TCP | LDAP | – | http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT |
| 427 | TCP | Novell Client | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 443 | TCP | HTTPS | – | http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT |
| 445 | TCP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT |
| 445 | UDP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 1023 | TCP | – | Serveur ftp de Sasser.E | – |
| 1080 | TCP | Wingate | MyDoom.F | http://www.certa.ssi.gouv.fr/site/CERT |
| 1433 | TCP | MS-SQL-Server | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 1434 | UDP | MS-SQL-Monitor | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 2100 | TCP | Oracle XDB FTP | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 2381 | TCP | HP System Management | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 2512 | TCP | Citrix MetaFrame | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 2513 | TCP | Citrix MetaFrame | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 2745 | TCP | – | Bagle | – |
| 2967 | TCP | Symantec Antivirus | Yellow Worm | http://www.certa.ssi.gouv.fr/site/CERT |
| 3104 | TCP | CA Message Queuing | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 3127 | TCP | – | MyDoom | – |
| 3128 | TCP | Squid | MyDoom | http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT |
| 3268 | TCP | Microsoft Active Directory | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 3306 | TCP | MySQL | – | – |
| 4899 | TCP | Radmin | – | – |
| 5000 | TCP | Universal Plug and Play | Bobax, Kibuv | http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT |
| 5151 | UDP | IPSwitch WS_TP | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 5151 | TCP | ESRI ArcSDE | – | http://www.certa.ssi.gouv.fr/site/CERT |
| 5554 | TCP | SGI ESP HTTP | Serveur ftp de Sasser | – |
| 5900 | TCP | VNC | – | http://www.certa.ssi.gouv.fr/site/CERT<br>http://www.certa.ssi.gouv.fr/site/CERT |
| 6014 | TCP | IBM Tivoli Monitoring | – | http://www.certa.ssi.gouv.fr/site/CERT |

| | | | | |
|---|---|---|---|---|
| 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<br>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<br>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 |
|---|---|
| 135/tcp | 34.66 |
| 25/tcp | 25.33 |
| 445/tcp | 19.28 |
| 1434/udp | 5.12 |
| 22/tcp | 4.19 |
| 80/tcp | 2.13 |
| 1433/tcp | 1.92 |
| 4899/tcp | 1.56 |
| 3128/tcp | 1.35 |
| 1080/tcp | 1.28 |
| 23/tcp | 1.2 |
| 2967/tcp | 0.99 |
| 3389/tcp | 0.64 |
| 21/tcp | 0.28 |
| 3306/tcp | 0.14 |
| 42/tcp | 0.07 |

TAB. 3: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**02 octobre 2009** version initiale.