Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 septembre 2011
N° CERTA-2011-ACT-036

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-36

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-2011-ACT-036`

Gestion du document

Référence	CERTA-2011-ACT-036
Titre	Bulletin d'actualité 2011-36
Date de la première version	09 septembre 2011
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-2011-ACT-036.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-2011-ACT-036/

1 Compromissions furtives de sites Web

Le CERTA a récemment traité une vague de compromissions de sites Web assez furtives. Celles-ci sont discrètes parce qu'elles ne peuvent se constater que dans des circonstances particulières. En effet, le piratage de la machine ne se manifeste que sous la forme d'une redirection conditionnelle. Celle-ci ne s'effectue que lorsque le *referrer* contient des mots-clefs particuliers. Par exemple, en provenant du site de *Google* après avoir recherché un produit pharmaceutique particulier, la visite sur le site Web compromis provoquera la redirection.

Pour forcer les redirections, les attaquants déploient des fichiers `.htaccess` dans l'arborescence des sites Web. Ils ne se contentent d'ailleurs pas de cette modification, puisqu'ils ajoutent également des portes dérobées. La compromission doit donc être traitée avec le plus grand sérieux.

Les administrateurs ont deux moyens pour détecter les incidents de ce genre :

– lire les journaux d'événements, ce qui a pour avantage de dévoiler d'autres problèmes ;

– faire des recherches sur leurs propres sites Web, pour voir ce qu'affiche le moteur de *Google* (ou autre).

En cas d'incident, l'analyse complète du système est préconisée.

2 Mise à jour des autorités de certification

Comme détaillé dans le précédent bulletin d'actualité du CERTA (cf. CERTA-2011-ACT-035), suite à la compromission de l'autorité de certification DigiNotar, de nombreux éditeurs de logiciel ont publié des mises à jour afin de supprimer tout ou partie des certificats émis par cette autorité.

Une liste, non exhaustive, des mises à jour disponibles se trouve dans l'avis CERTA-2011-AVI-493. Adobe fournit également une procédure détaillée (cf. la section Documentation) afin de supprimer manuellement cette autorité de certification de ces programmes via sa solution *Adobe Approved Trust List*.

Le CERTA encourage vivement le déploiement rapide de ces correctifs afin d'empêcher au plus vite des attaques de type *man-in-the-middle* sur les services ciblés par les faux certificats créés pendant la compromission.

Documentation

- Avis CERTA-2011-AVI-493 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-493/
- Procédure de suppression dans les produits Adobe de l'autorité de certification DigiNotar :
  http://blogs.adobe.com/security/2011/09/diginotarremovalaatl.html

3 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/

4 Rappel des avis émis

Dans la période du 02 au 08 septembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-492 : Vulnérabilités dans Symantec Enterprise Vault
- CERTA-2011-AVI-493 : Certificats SSL frauduleux
- CERTA-2011-AVI-494 : Vulnérabilité dans Hitachi Web Serveur
- CERTA-2011-AVI-495 : Vulnérabilité dans les produits Hitachi Cosminexus
- CERTA-2011-AVI-496 : Vulnérabilités dans OpenSSL

– CERTA-2011-AVI-497 : Vulnérabilité dans IBM OmniFind
– CERTA-2011-AVI-498 : Vulnérabilité dans Bluecoat Reporter
– CERTA-2011-AVI-499 : Vulnérabilité dans les commutateurs Cisco Nexus 5000 et 3000 series
– CERTA-2011-AVI-500 : Vulnérabilité dans Xen

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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_rubrique62.html

6 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.

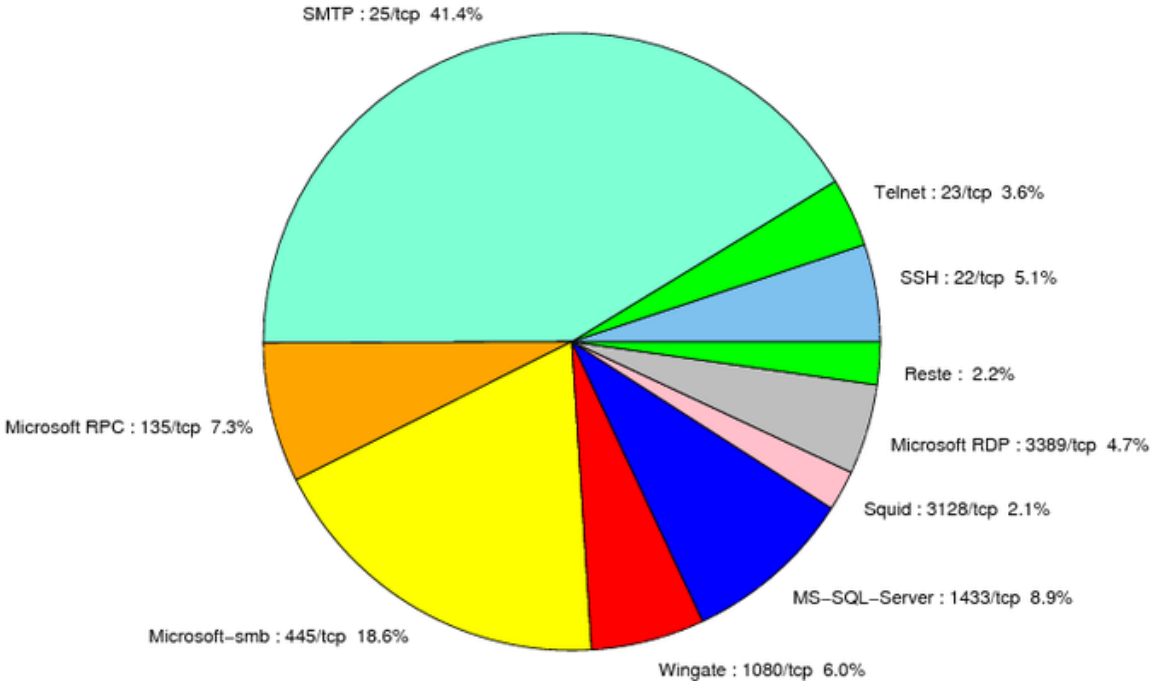

FIG. 1: Répartition relative des ports pour la semaine du 02 au 08 septembre 2011

port	pourcentage
25/tcp	41.36
445/tcp	18.63
80/tcp	17.01
1433/tcp	8.94
135/tcp	7.32
1080/tcp	5.96
22/tcp	5.09
3389/tcp	4.72
23/tcp	3.72
3128/tcp	2.11
3306/tcp	0.74
3127/tcp	0.62
2967/tcp	0.24
4899/tcp	0.12

TAB. 2: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Paquets rejetés 5

Gestion détaillée du document

09 septembre 2011 version initiale.