

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-52

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-052>

Gestion du document

Référence	CERTA-2010-ACT-052
Titre	Bulletin d'actualité 2010-52
Date de la première version	31 décembre 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-052.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-052/>

1 Meilleurs vœux !

L'année 2010 s'achève, c'est donc le moment des bilans et des bonnes résolutions.

Et cette année qui se termine a été particulièrement riche dans le domaine de la SSI. Stuxnet, premier code malveillant ciblant spécifiquement des systèmes informatiques industriels, a fait beaucoup parler de lui. Ce programme informatique n'incorporait pas moins de quatre « 0-day », c'est-à-dire quatre codes d'attaques nouveaux ne disposant pas encore de correctif. Sa capacité à infecter des réseaux déconnectés, en se propageant notamment via des clés de stockage USB lui a, sans doute, permis d'accéder à des réseaux sensibles. Malheureusement, ce scénario d'attaque n'est pas nouveau, et ne peut que nous rappeler les événements de 2009, et le célèbre Conficker.

L'année 2010 a été marquée par une augmentation du nombre d'avis et d'alertes publiés par le CERTA. Pas moins de 639 avis et 21 alertes ont ainsi été diffusés. Les attaques exploitant des vulnérabilités présentes dans les formats bureautiques ont encore eu beaucoup de succès. Le CERTA a pu constater dans les incidents qu'il est amené à traiter la forte augmentation d'attaques par le biais de fichiers PDF plus ou moins spécialement conçus pour son destinataire. Aussi, en cette fin d'année, il ne faut pas relâcher sa vigilance lors de l'ouverture de certains courriels tels les traditionnelles cartes de vœux.

D'un point de vue plus organisationnel, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), dont le CERTA fait partie, a continué sa croissance. Une nouvelle ouverture et des propositions de services à destination des « OIV » (Opérateurs d'Importance Vitale) sont ainsi en train de voir le jour. Le CERTA rappelle également que des postes sont toujours à pourvoir au sein de l'équipe et plus largement au sein de l'ANSSI. Les offres d'emploi sont disponibles à l'adresse suivante : http://www.ssi.gouv.fr/site_rubrique27.html.

Le bulletin d'actualité est, pour le CERTA, le moyen de partager sa vision et son expérience en matière de traitement d'incident. Les retours sur cette production sont toujours bénéfiques. N'hésitez donc pas à nous faire part de vos remarques.

Il ne nous reste désormais plus qu'à vous souhaiter une bonne fin d'année 2010 et une bonne année 2011 et à vous donner rendez-vous l'année prochaine pour continuer ensemble l'effort global de sécurisation de nos systèmes d'information. Très bonne et heureuse année à toutes et à tous !

2 Incident de la semaine

Publicité malveillante sur un site légitime

Cette semaine, le CERTA a été alerté de la compromission de plusieurs machines. Cette compromission s'est manifestée après la mise à jour de la base de signatures de la solution antivirale installée sur les postes de travail.

Après analyse du fichier malveillant, il apparaît que la charge utile téléchargée par ce dernier n'est autre qu'un *BHO (Browser Helper Object)* ayant pour objectif d'insérer des publicités lors de la navigation de l'utilisateur.

Lors de l'inspection de la machine et de son système de fichiers, il est apparu que le fichier malveillant avait été installé grâce à l'exploitation d'une vulnérabilité dans la machine virtuelle *Java* qui n'était pas à jour. Cette exploitation s'est faite par le biais d'une publicité malveillante diffusée sur des sites légitimes.

Le CERTA profite de cet incident pour rappeler deux bonnes pratiques :

- il est important de déployer les mises à jour des applicatifs installés sur un poste de travail au plus tôt. Cette rapidité de validation de mise à jour et d'installer est d'autant plus importante si l'applicatif est présent sur l'ensemble du parc ;
- les publicités sont souvent diffusées par des prestataires externes au site visité. Même si le site visité est considéré de confiance, il est nécessaire de limiter les interactions vers les autres sites pointés, par exemple, par un bandeau publicitaire. Des modules additionnels au navigateur peuvent aider à la limitation de ces interactions.

3 Une base publique de clés privées SSL

Le 19 décembre 2010, un groupe s'intéressant aux équipements embarqués a rendu public une base de données de plus de 2000 clés privées SSL. Il s'agit des clés privées intégrées dans différents microgiciels installés principalement dans des équipements à destination du grand public du type routeur ou point d'accès WiFi. Ces clés sont principalement utilisées par le serveur Web intégré donnant accès à l'interface d'administration de l'équipement, et permettent donc une connexion sécurisée à ce serveur.

Or, comme l'indique le groupe en question, ces clés sont contenues dans les microgiciels des équipements, le plus souvent sans qu'il soit proposé à l'administrateur d'en installer de nouvelles lors de la première mise en route de l'appareil.

Les clés ont été obtenues pour la plupart à partir des microgiciels du projet à source ouverte *DD-WRT*. En connaissant par exemple la version précise de ce microgiciel, il est facile de trouver la clé privée utilisée par cette version dans la base de données. Il est également possible pour un attaquant d'obtenir la clé publique fournie par le certificat du serveur Web, ou en interceptant une connexion chiffrée à l'interface d'administration. Il pourra alors vérifier si la clé privée associée est connue. Si c'est le cas, il pourra alors déchiffrer la communication, et obtenir par exemple les identifiant d'accès à l'interface.

Ce type d'attaque n'est pas nouveau. Elle repose sur le principe qu'il est possible à une tierce personne d'avoir accès aux paramètres privés. L'outil récemment rendu public permet en revanche de faciliter cette recherche de la clé privée dans des cas précis.

Pour éviter de s'exposer à cette attaque, les fabricants devraient installer dans chaque équipement un certificat différent, ou demander à l'administrateur d'en générer un lui-même et qui sera propre à cet équipement.

4 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/>

5 Rappel des avis émis

Dans la période du 24 au 30 décembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-631 : Vulnérabilité dans HP StorageWorks Modular Smart Array
- CERTA-2010-AVI-632 : Vulnérabilité dans HP Insight Diagnostics Online Edition
- CERTA-2010-AVI-633 : Vulnérabilité dans HP DDMI
- CERTA-2010-AVI-634 : Vulnérabilité dans Pidgin
- CERTA-2010-AVI-635 : Vulnérabilités dans Django
- CERTA-2010-AVI-636 : Vulnérabilité dans IBM WebSphere Registry and Repository
- CERTA-2010-AVI-637 : Vulnérabilité dans IBM Tivoli Access Manager for e-business

Durant la même période, l'avis suivant a été mis à jour :

- CERTA-2010-AVI-585-001 : Vulnérabilités dans les produits Mozilla (ajout des références aux bulletins Fedora)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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

7 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.

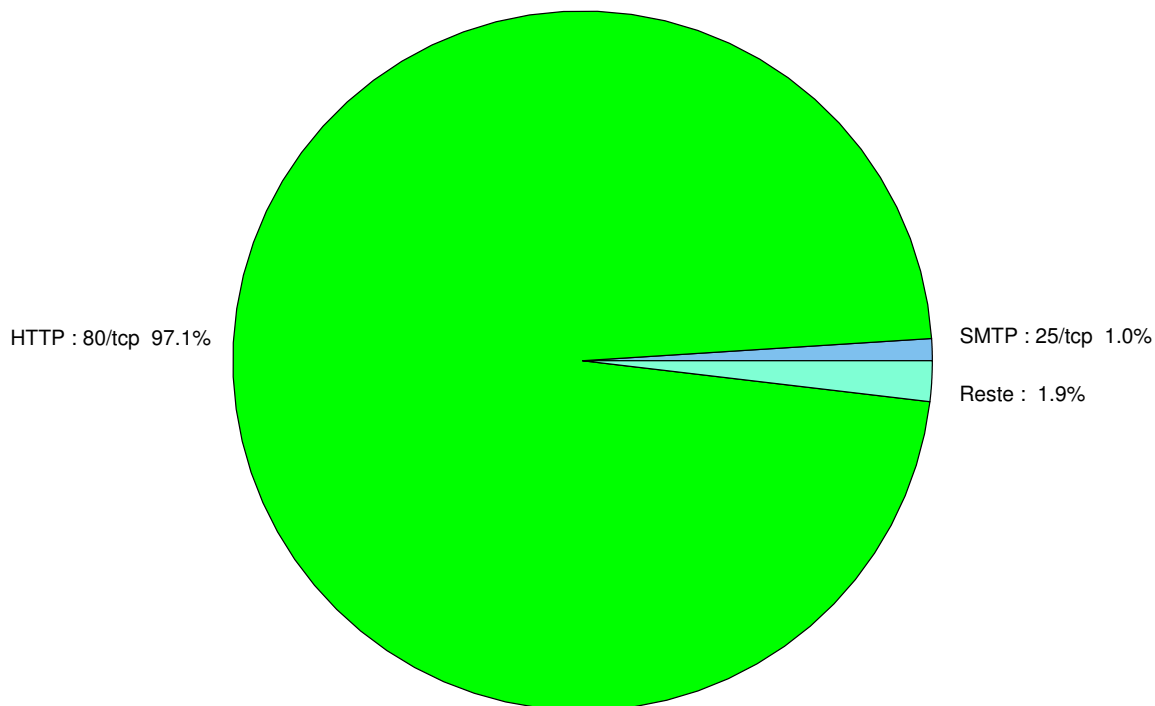


FIG. 1: Répartition relative des ports pour la semaine du 24 au 30 décembre 2010

port	pourcentage
80/tcp	97.31
25/tcp	1
1433/tcp	0.46
445/tcp	0.39
2967/tcp	0.2
23/tcp	0.13
135/tcp	0.11
3306/tcp	0.09
3389/tcp	0.07
1434/udp	0.02

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

31 décembre 2010 version initiale.