

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-17

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-017>

Gestion du document

Référence	CERTA-2011-ACT-017
Titre	Bulletin d'actualité 2011-17
Date de la première version	29 avril 2011
Date de la dernière version	–
Source	–
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-017.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-017/>

1 Les réseaux sociaux vecteurs de contenu malveillant

Ces quelques dernières années ont vu l'émergence et la démocratisation sur l'Internet des sites de réseaux sociaux.

Ces plateformes d'échange sont d'ores et déjà connues pour poser différents problèmes d'atteinte à la vie privée, mais représentent également des cibles privilégiées pour la diffusion à grande échelle de contenu malveillant.

Ces codes malveillants profitent largement des liens sociaux entre différents utilisateurs. Par exemple, un message provenant d'un « ami » paraîtra toujours plus légitime que s'il provenait d'un compte inconnu. La technique n'est pas nouvelle, certains logiciels malveillants se propageant par courrier électronique vont chercher leurs cibles dans le carnet d'adresse de la victime initiale afin de gagner en légitimité. Cette technique est amplifiée par le fait que le cercle d'« amis » sur les réseaux sociaux est beaucoup plus étendu que celui d'un carnet d'adresses utilisé pour contacter sa famille et ses collègues de travail par exemple.

La plupart de ces sites invitent chaque utilisateur à apporter sa contribution telle que l'ajout de commentaires, d'images, ou encore inciter d'autres utilisateurs à se rendre sur certaines pages, à s'enregistrer auprès de nouveaux services, à utiliser de nouveaux jeux, etc.

Pour toutes ces raisons, et en prenant en compte le développement très rapide de ces réseaux, beaucoup d'attaquants peuvent être attirés par ce terrain fertile pour diffuser de contenu malveillant au plus grand nombre.

C'est pourquoi, depuis quelques mois, plusieurs vulnérabilités affectant les plus gros réseaux sont découvertes puis corrigées. La technique qui semble être la plus employée est l'injection de code indirecte à distance (ou XSS), qui permet entre autre d'exécuter du code arbitraire dans le contexte de la session d'un utilisateur. Le code peut alors se répliquer par commentaires sur les pages des contacts « amis », propager des messages diffamatoires, collecter des informations sur le profil de la victime ou encore la rediriger vers d'autres sites malveillants.

D'autres méthodes de compromission se développent. Certains liens sur des sites se font passer pour le bouton « J'aime » du site *Facebook* et utilisent des méthodes de détournement de clic (ou *clickjacking*). La victime ayant effectivement cliqué sur ce lien pourra voir son poste compromis, et propagera en même temps ce lien vers ses contacts via le mécanisme classique des notifications « J'aime ».

Enfin, ces sites peuvent aussi être utilisés comme canaux de commande et de contrôle pour certains *botnets*, comme le CERTA l'a présenté dans le bulletin d'actualité CERTA-2009-ACT-045.

Pour toutes ces raisons, le CERTA recommande que les responsables des systèmes d'information s'interrogent sur les politiques d'accès à ces sites.

Documentation

- Bulletin d'actualité CERTA-2010-ACT-045 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-045/>

2 Infection par un *ransomware*

Récemment, le CERTA a reçu une demande d'analyse concernant une machine ayant été infectée par un *ransomware*.

Ce type de code n'est pas nouveau. Il parcourt les documents accessibles et les chiffre. Ensuite, il demande une rançon à l'utilisateur pour qu'il puisse récupérer ses fichiers dans leur état original.

Afin de procéder à une analyse, il est important de conserver l'état de la machine et de réaliser une copie de la mémoire vive et du disque dur. En effet, ces éléments peuvent aider à trouver une méthode de décryptage lorsque le programme présente un défaut dans l'implémentation ou l'utilisation de l'algorithme de chiffrement. De plus, dans un cadre judiciaire, la possible identification de l'attaquant peut également être un moyen de retrouver les éléments permettant de déchiffrer et retrouver ses documents.

Enfin, le CERTA rappelle que l'utilisation régulière de sauvegardes stockées sur des serveurs physiquement séparés reste le meilleur moyen de récupérer ses fichiers.

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 22 au 28 avril 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-247 : Vulnérabilité dans CA SiteMinder
- CERTA-2011-AVI-248 : Vulnérabilités dans CA Output Management Web Viewer
- CERTA-2011-AVI-249 : Multiples vulnérabilités dans Asterisk
- CERTA-2011-AVI-250 : Vulnérabilité dans Adobe Reader et Acrobat
- CERTA-2011-AVI-251 : Vulnérabilité dans des produits d'accès VPN de CheckPoint
- CERTA-2011-AVI-252 : Vulnérabilité dans Webmin
- CERTA-2011-AVI-253 : Vulnérabilité dans Hitachi Web Server
- CERTA-2011-AVI-254 : Vulnérabilité dans Hitachi Web Server
- CERTA-2011-AVI-255 : Vulnérabilité dans WordPress
- CERTA-2011-AVI-256 : Vulnérabilités dans CA Arcot WebFort Versatile Authentication Server
- CERTA-2011-AVI-257 : Vulnérabilité dans HP SiteScope
- CERTA-2011-AVI-258 : Vulnérabilités dans BestPractical RT
- CERTA-2011-AVI-259 : Vulnérabilités dans IBM DB2
- CERTA-2011-AVI-260 : Multiples vulnérabilités dans HP OpenView Storage Data Protector
- CERTA-2011-AVI-261 : Multiples vulnérabilités dans MediaWiki
- CERTA-2011-AVI-262 : Vulnérabilité dans Cisco Wireless Lan Controllers
- CERTA-2011-AVI-263 : Multiples vulnérabilités dans Cisco Unified Communications Manager
- CERTA-2011-AVI-264 : Vulnérabilités dans OpenSUSE Build Service
- CERTA-2011-AVI-265 : Vulnérabilité dans JBoss
- CERTA-2011-AVI-266 : Multiples vulnérabilités dans Google Chrome

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2011-ALE-003-004 : Vulnérabilité dans Adobe Flash Player, Adobe Reader et Acrobat (annonce des dates de publication des correctifs)
- CERTA-2011-AVI-190-002 : Vulnérabilité dans le client DHCP ISC (ajout des bulletins de sécurité Debian, Fedora, Mandriva, NetBSD et Ubuntu)

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 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.

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 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.

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.

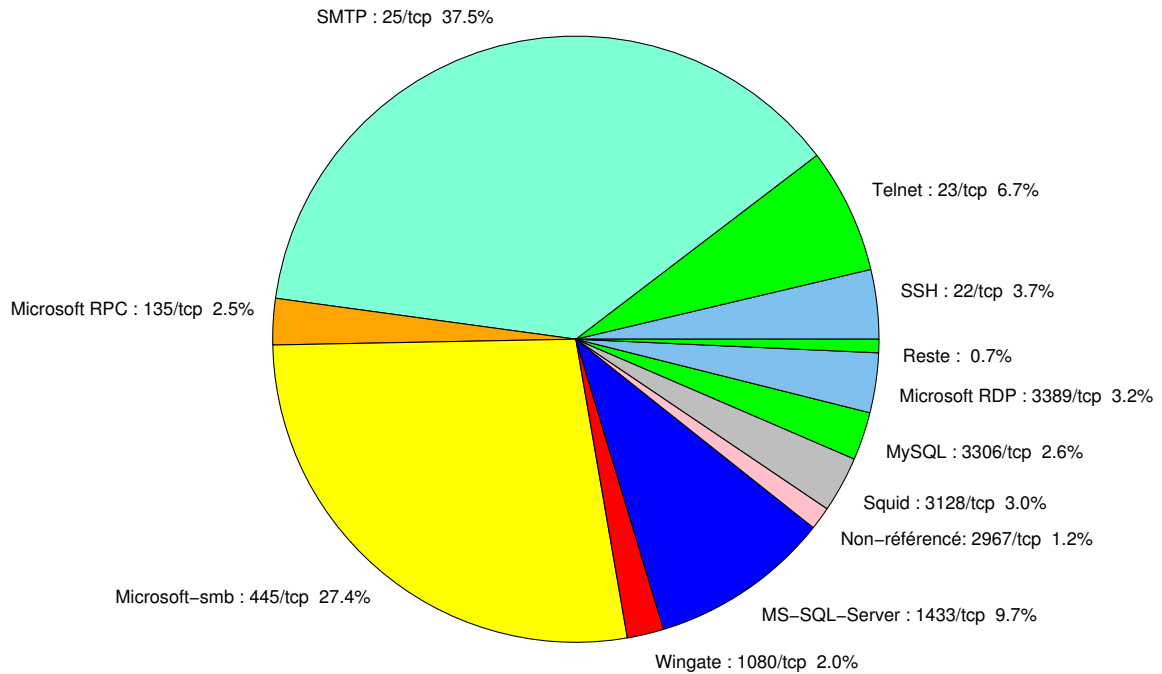


FIG. 1: Répartition relative des ports pour la semaine du 15 au 21 avril 2011

port	pourcentage
25/tcp	37.47
445/tcp	27.41
1433/tcp	9.65
23/tcp	6.67
80/tcp	4.62
22/tcp	3.69
3389/tcp	3.18
3128/tcp	2.97
3306/tcp	2.56
135/tcp	2.46
1080/tcp	1.95
2967/tcp	1.23
21/tcp	0.61
4899/tcp	0.1

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

29 avril 2011 version initiale.