

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-21

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-021>

Gestion du document

Référence	CERTA-2011-ACT-021
Titre	Bulletin d'actualité 2011-21
Date de la première version	27 mai 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-021.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-021/>

1 Barres d'outils indésirables

1.1 Description

Les barres d'outils sont des modules ajoutés aux navigateurs Web. Elles existent notamment pour Firefox, Internet Explorer, Opera... Celles-ci proposent des fonctionnalités supplémentaires à l'utilisateur, par exemple un cadre permettant de faire rapidement des recherches.

Le danger est que ces barres d'outils comportent du code qui sera exécuté. Celui-ci peut contenir des vulnérabilités ou réaliser des actions non souhaitées. Certaines barres d'outils peuvent être associées à des logiciels espions (*spywares*) dans le sens où elles vont collecter et transférer des informations sur l'utilisateur, son poste et ses habitudes sans que celui-ci en soit conscient.

De plus, ce type de modules d'extension ne requière généralement pas les droits administrateur pour s'installer.

1.2 Exemples

Les sites conduit.com et predictad.com proposent chacun une plate-forme permettant de développer ses propres barres d'outils. Les modules ainsi développés sont capables d'envoyer silencieusement des données à

des sous-domaines de `conduit.com` et `predictad.com`. Il s'agit là d'une fuite de données non contrôlée, qu'il est préférable de filtrer.

D'autres barres d'outils sont reconnues par certains antivirus comme étant potentiellement dangereuses. Ainsi *Funwebproducts* est vue comme un publiciel par *Bitdefender*. *Widgi Toolbar* est reconnue de même par *Sophos*.

1.3 Mesures envisageables

Pour détecter ce phénomène au niveau réseau, il y a plusieurs possibilités selon les barres d'outils. Par exemple, une recherche des requêtes DNS contenant `conduit.com` ou `predictad.com` ou encore `toolbar.zynga.com` peut être effectuée. Pour l'exemple `conduit.com`, il y a notamment le sous-domaine `alert.services.conduit.com`. Vers ce serveur partent des requêtes HTTP avec la méthode POST, vers des URI `/Alerts/AlertServices.aspx/GetToolbarAlertsInfo` ou encore `/Alerts/AlertServices.aspx/AlertLogin`. Autre exemple pour la toolbar Zynga, une requête HTTP de type GET est envoyée toutes les 5 minutes à l'URL `toolbar.zynga.com/heartbeat.php`. D'autres barres d'outils sont visibles au niveau du *User Agent* du navigateur qu'elles modifient. Par exemple, les *User Agent* vont contenir `WidgiToolbar` ou `FunWebProducts` ou encore `Hotbar`.

De manière générale, il est de bonne pratique que les serveurs Web mandataires contrôlent les *User Agent*, de préférence avec une liste blanche adaptée. Il est aussi possible de mettre en liste noire des domaines utilisés pour la mise à jour de ces barres d'outils. Les utilisateurs doivent également être sensibilisés pour ne pas installer ce genre de logiciels.

Références

- Informations relatives à *Funwebproducts* :
<http://www.bitdefender.com/VIRUS-197041-en-Adware.Bundler.Funwebproducts.M.html>
- Informations relatives à *WidgiToolbar* :
<http://www.sophos.com/en-us/threat-center/threat-analyses/adware-and-puas/WidgiToolbar.aspx>
- Informations relatives à *HotBar* :
http://www.symantec.com/fr/fr/security_response/writeup.jsp?docid=2003-080410-3847-99

2 Faux antivirus malveillants sur Mac OS X

Contrairement à une idée répandue, Mac OS X est également une cible pour les auteurs de programmes malveillants.

Le bulletin d'actualité *CERTA-2011-ACT-018* décrit la mise en place d'une vague d'attaques par redirections involontaires (*drive by downloads*). Cette vague d'attaques est notamment utilisée pour tromper les utilisateurs de Mac OS X, en leur faisant croire que leur poste est infecté, avant de leur proposer un faux antivirus Mac OS X du nom de *Mac Defender* (il peut exister sous d'autres noms). Une fois téléchargé avec *Safari*, ce programme est automatiquement installé si l'option *ouvrir automatiquement les fichiers « fiables »* n'est pas désactivée.

Ce faux antivirus a pour vocation d'extorquer le code de carte de crédit de l'utilisateur. Pour ce faire, il lui fait croire que son poste est compromis en remontant une liste aléatoire de fichiers supposés infectés et en ouvrant des pages Web indésirables. L'utilisateur est alors invité à enregistrer son produit en donnant son numéro de carte de crédit afin de pouvoir « désinfecter » la machine.

Face à cette menace, Apple a réagi en proposant une procédure de suppression manuelle du programme et prévoit de diffuser prochainement une mise à jour permettant d'identifier et de supprimer ce programme dans ses différentes variantes.

- Outre la sensibilisation des utilisateurs à la problématique des faux antivirus, le CERTA recommande :
- l'utilisation d'un compte avec des droits restreints ;
 - la désactivation de l'option *ouvrir automatiquement les fichiers « fiables »* dans *Safari* ;
 - de façon plus générale la ré-installation complète du système après une compromission (cf : *CERTA-2002-INF-002*, Que faire en cas d'intrusion ?).

Documentation

- Bulletin d'actualité CERTA-2011-ACT-018 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-018/>
- Note Apple HT4650 sur la suppression de Mac Defender :
<http://support.apple.com/kb/HT4650>

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 20 au 26 mai 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-303 : Multiples vulnérabilités dans Cisco Unified Operations Manager
- CERTA-2011-AVI-304 : Vulnérabilité dans Cisco Common Services
- CERTA-2011-AVI-305 : Multiples vulnérabilités dans Moodle
- CERTA-2011-AVI-306 : Vulnérabilités dans phpMyAdmin
- CERTA-2011-AVI-307 : Vulnérabilité dans EMC SourceOne Email Management
- CERTA-2011-AVI-308 : Multiples vulnérabilités dans Google Chrome
- CERTA-2011-AVI-309 : Vulnérabilité dans IBM OS/400
- CERTA-2011-AVI-310 : Multiples vulnérabilités dans IBM Lotus Notes
- CERTA-2011-AVI-311 : Vulnérabilité dans Sybase EAServer
- CERTA-2011-AVI-312 : Vulnérabilité dans les contrôleurs Ethernet Intel
- CERTA-2011-AVI-313 : Vulnérabilité dans IBM WebSphere
- CERTA-2011-AVI-314 : Multiples vulnérabilités dans Cisco IOS XR
- CERTA-2011-AVI-315 : Vulnérabilité dans Cisco Content Delivery System Internet Streamer
- CERTA-2011-AVI-316 : Vulnérabilité dans Dovecot

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.

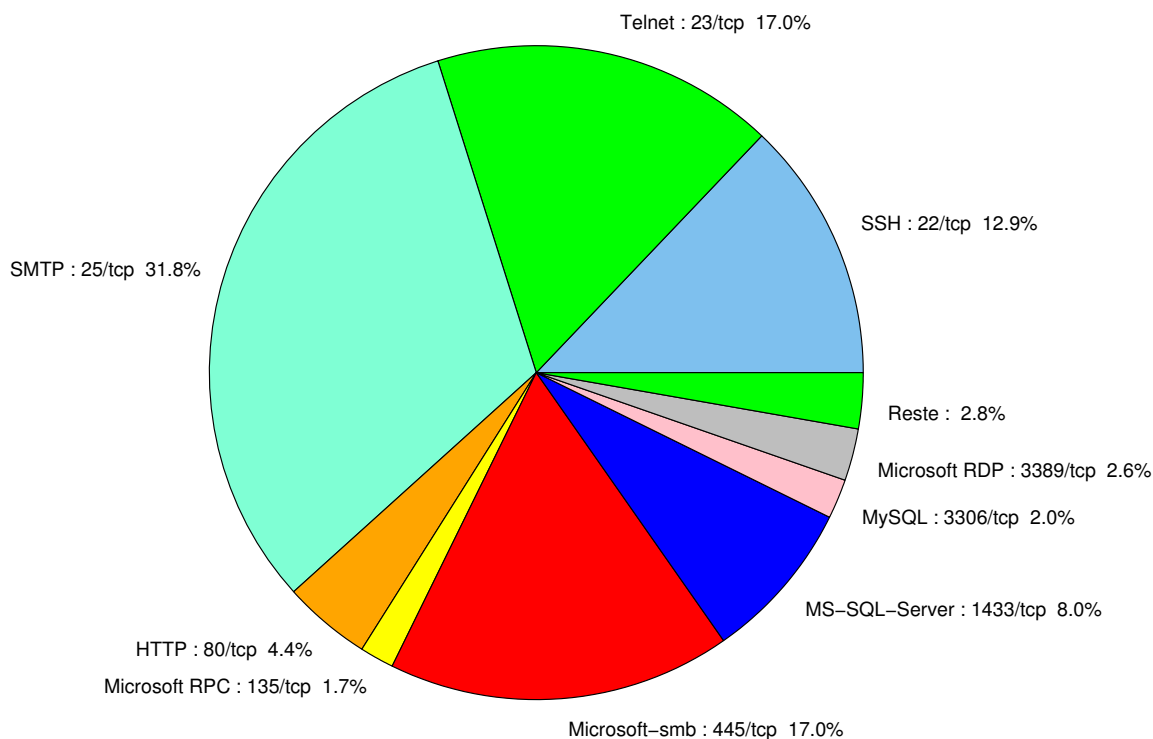


FIG. 1: Répartition relative des ports pour la semaine du 20 au 26 mai 2011

port	pourcentage
80/tcp	105.95
25/tcp	31.82
445/tcp	16.97
22/tcp	12.88
1433/tcp	8
143/tcp	4.8
3389/tcp	2.57
3306/tcp	1.95
135/tcp	1.68
2967/tcp	0.97
3128/tcp	0.88
4899/tcp	0.35
1080/tcp	0.17
1434/udp	0.08

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

27 mai 2011 version initiale.