

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-18

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-018>

Gestion du document

Référence	CERTA-2011-ACT-018
Titre	Bulletin d'actualité 2011-18
Date de la première version	06 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-018.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-018/>

1 Vague d'attaques par redirections involontaires (*drive-by-downloads*)

1.1 Description du phénomène

Une vague de redirections et de téléchargements involontaires associés à des navigations Web est en cours depuis quelques semaines, avec plusieurs constantes. Le principe est d'amener l'utilisateur, au cours de sa navigation, à contacter un site et à télécharger du code dangereux sur son poste. Ce code s'installera ensuite automatiquement ou par une action directe de l'utilisateur (fenêtre surgissante lui proposant d'installer le code).

L'attaque induit donc bien souvent la compromission d'un site légitime, par exemple en rajoutant un code dynamique JavaScript, forçant le navigateur à envoyer une nouvelle requête vers un autre site lui aussi compromis ou malveillant.

Dans la vague actuellement observée, le premier point commun entre ces téléchargements est la forme des noms de domaine utilisés. Ils contiennent tous les chaînes de caractères `protection` et `scan` et sont des sous-domaines du domaine de premier niveau `.com`. Ils sont également concaténés avec d'autres mots en anglais. Par exemple :

- `scannerprotectionofficesfree.com`
- `desktopscannerprotectionxp.com`

- negativescannerxpprotection.com
- compactscannerprotectionfast.com
- mobilescannerwinprotection.com

Ces sites proposent l'installation d'un faux anti-virus après avoir fait semblant d'analyser la machine et de trouver des virus.

Le deuxième point commun est le format des adresses réticulaires, ou URI. La première page demandée est de la forme :

```
/index2.php?[ :base64: ] { 68 } .
```

L'adresse réticulaire pour télécharger l'exécutable est de la forme :

```
/download.php?[ :base64: ] { 68 }
```

Le paramètre encodé en base64 semble lui toujours commencer par 06abQDY3.

Enfin, les adresses IP des serveurs impliqués appartiennent à différentes plages, sans lien évident. Les exécutables téléchargés sont eux différents à chaque téléchargement (hachés MD5 multiples).

1.2 Mesures envisageables

Pour détecter ce phénomène, il est possible de rechercher dans les journaux des serveurs mandataires Web (et éventuellement dans les journaux DNS) les noms de domaine contenant les chaînes de caractères `protection` et `scan`. La validation des résultats se fait ensuite en observant directement si les adresses réticulaires observées sont de même format que celles précédemment citées, présentant la chaîne `/download.php?06abQDY3`. Il faut alors s'assurer que le contenu téléchargé a été bloqué préventivement (blocage d'exécutables ou antivirus) et qu'il n'a pas été installé sur le poste de l'utilisateur à l'origine involontaire de ce téléchargement.

De manière générale, il ne faut pas accepter le téléchargement d'exécutables au niveau des serveurs Web mandataires, sauf exceptions, par exemple sous forme de liste blanche. Les utilisateurs qui naviguent sur l'Internet doivent le faire à partir d'un système à jour et d'un compte aux droits très restreints, afin d'éviter tout téléchargement et installation involontaire et dangereuse. Les utilisateurs doivent également être sensibilisés pour ne pas tomber dans le piège de ces faux antivirus.

1.3 Références

<http://blog.sucuri.net/2011/04/jquery4html-co-cc-malware-fake-av-redirections.html>

<http://www.sophos.com/support/knowledgebase/article/110379.html>

2 Moteurs de recherche et logiciels malveillants

Les techniques d'optimisation pour les moteurs de recherche (en anglais SEO - *Search Engine Optimization*) sont utilisées pour favoriser le référencement d'un contenu par un moteur de recherche tel que Google ou Bing.

Celles-ci, loin d'être nouvelles, sont de plus en plus utilisées pour référencer des sites malveillants avec des mots-clés légitimes. Souvent lié à l'actualité (comme l'annonce de la mort de Oussama Ben Laden ou l'accident nucléaire de Fukushima), ce référencement abusif se retrouve aussi bien classé que les sites de médias bien connus. Le but de la manoeuvre est de faire installer par l'internaute un logiciel ou un module d'extension malveillant.

Cette semaine, une campagne utilisant le moteur de recherche d'images de Google et relative à la mort de Oussama Ben Laden visait les utilisateurs de Windows et Mac. L'installation d'un faux antivirus était suggérée, après une prétendue infection lors de la redirection vers un site malveillant.

En identifiant le système de leur victime, ces sites malveillants ne se restreignent plus uniquement à Windows et ciblent désormais d'autres systèmes tels que MacOS et des utilisateurs ayant le sentiment d'être jusque là épargnés (à tort).

Le CERTA recommande de prêter une attention particulière aux résultats des moteurs de recherche lors de la navigation afin de ne pas être redirigé vers des sites malveillants.

3 Mise en liste noire de certains certificats SSL frauduleux

Le 25 mars dernier, le CERTA a émis un avis concernant une émission frauduleuse de certains certificats (CERTA-2011-AVI-169).

Les plates-formes susceptibles de recevoir ces mises à jours ne sont pas restreintes aux ordinateurs et serveurs. Les téléphones et les systèmes embarqués peuvent eux aussi être vulnérables.

Microsoft a mis à jour son bulletin de sécurité (254375) en ajoutant, entre autres, les téléphones fonctionnant sous Windows Mobile 6.X et Windows Phone 7.

Le CERTA recommande de procéder à la vérification de l'ensemble des systèmes pouvant interagir avec le système d'information et qui seraient potentiellement vulnérables.

Documentation

- Avi CERTA-2011-AVI-169 du 24 mars 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-169/>
- Bulletin d'actualité CERTA-2011-ACT-012 du 25 mars 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-012/>
- Bulletin de sécurité Microsoft 2524375 du 23 mars 2011 :
<http://www.microsoft.com/france/technet/security/advisory/254375.msp>

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 29 avril au 05 mai 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-268 : Vulnérabilité dans FFmpeg
- CERTA-2011-AVI-269 : Vulnérabilité dans HP Network Automation
- CERTA-2011-AVI-270 : Vulnérabilité dans Cisco IOS

- CERTA-2011-AVI-271 : Vulnérabilités dans VMware ESX et ESXi
- CERTA-2011-AVI-272 : Vulnérabilité dans des produits BlueCoat
- CERTA-2011-AVI-273 : Vulnérabilité dans Vino
- CERTA-2011-AVI-274 : Vulnérabilités dans HP Insight Control Performance Management
- CERTA-2011-AVI-275 : Vulnérabilités dans Horde

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

- CERTA-2010-AVI-590-002 : Vulnérabilités dans OpenSSL (Ajout de la référence au bulletin de sécurité Oracle Solaris)
- CERTA-2011-AVI-073-002 : Vulnérabilité dans OpenSSL (ajout de la référence au bulletin Fedora (mingw32-openssl))
- CERTA-2011-AVI-098-001 : Multiples vulnérabilités dans Asterisk (ajout de la référence CVE CVE-2011-1147 et du bulletin de sécurité Debian)
- CERTA-2011-AVI-156-001 : Vulnérabilités dans Asterisk (ajout des références CVE CVE-2011-1174, CVE-2011-1175 et du bulletin de sécurité Debian)
- CERTA-2011-AVI-176-001 : Vulnérabilité dans rsync (ajout du bulletin de sécurité Ubuntu)
- CERTA-2011-AVI-196-001 : Vulnérabilité dans SPIP (ajout du bulletin de sécurité Debian)
- CERTA-2011-AVI-249-001 : Multiples vulnérabilités dans Asterisk (ajout de la référence CVE CVE-2011-1599 et du bulletin de sécurité Debian)
- CERTA-2011-AVI-267-002 : Multiples vulnérabilités dans les produits Mozilla (ajout du bulletins de sécurité Ubuntu pour Thunderbird)

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.

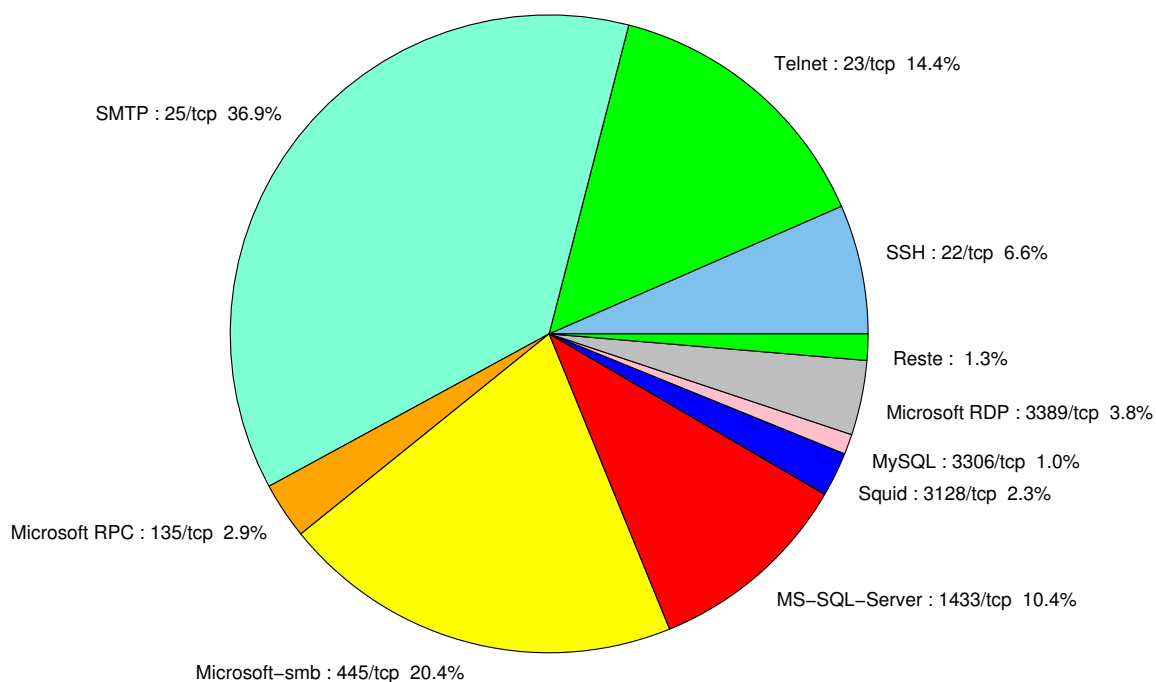


FIG. 1: Répartition relative des ports pour la semaine du 29 avril au 05 mai 2011

port	pourcentage
25/tcp	36.94
445/tcp	20.36
23/tcp	14.43
1433/tcp	10.44
22/tcp	6.55
80/tcp	4.6
3389/tcp	3.88
135/tcp	2.86
3128/tcp	2.25
3306/tcp	1.02
2967/tcp	0.4
21/tcp	0.3
143/tcp	0.2
4899/tcp	0.1

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

06 mai 2011 version initiale.