

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-15

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-2009-ACT-015>

Gestion du document

Référence	CERTA-2009-ACT-015
Titre	Bulletin d'actualité 2009-15
Date de la première version	10 avril 2009
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-2009-ACT-015.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-2009-ACT-015/>

1 L'inclusion locale

1.1 Présentation

Cette semaine, le CERTA a traité un incident de sécurité relatif à la compromission d'un serveur Web. Cet incident a été révélé par la présence de contenu malveillant (du filoutage ou *phishing*). L'analyse des journaux a ensuite permis de mettre en évidence la présence et l'utilisation d'un outil malveillant de prise de contrôle à distance (un *PHP Shell*). Le téléchargement de ce fichier est en fait directement visible dans les journaux, l'attaquant a modifié dans sa requête Web le champ réservé à la présentation de la version de son navigateur (le *UserAgent*). L'attaque a ensuite consisté à inclure le fichier `/proc/self/environ` présent localement sur le serveur. Cette technique a permis à l'attaquant de contourner la mesure de protection qui se limitait à interdire l'inclusion de fichiers distants.

Cette attaque, aussi connue sous le nom de *Local File Inclusion*, est largement automatisée dans les codes malveillants. Il est pourtant assez simple de s'en prémunir. Il faut :

- appliquer les correctifs de sécurité des applications et autres CMS utilisés ;
- contrôler et valider systématiquement le contenu d'une variable avant de l'utiliser ;

- protéger (voir interdire) l'accès aux ressources locales comme `/proc/self/environ` dévoilant la configuration du serveur.

Dans le cas d'hébergements mutualisés, toutes ces précautions sont rarement le fait de l'hébergeur. Le CERTA invite donc ses lecteurs à suivre ces bonnes pratiques afin de limiter les désagréments. Cet incident montre une nouvelle fois l'importance de la bonne gestion des journaux pour faciliter la compréhension de l'incident.

1.2 Documentation

- Note d'information du CERTA sur la gestion des journaux d'événements : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005/>
- Note d'information du CERTA sur le bon usage de PHP : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

2 Intrusion FTP

Le CERTA a traité cette semaine un incident dont le scénario est le suivant :

1. une machine est infectée par un code malveillant ;
2. l'utilisateur de cette machine se connecte au serveur FTP *ftp.domain.tld* et s'authentifie auprès de lui. Les identifiants de connexion sont interceptés par le code malveillant qui les transmet à un serveur distant sous contrôle d'attaquants ;
3. un robot d'attaque se connecte quelque temps plus tard au serveur *ftp.domain.tld* et rejoue les identifiants de connexion. Il liste ensuite tous les fichiers des répertoires auxquels il a accès et télécharge (méthode RETR) tous les fichiers au format HTML. Il modifie quelques uns de ces fichiers en ajoutant du `javascript` et un `iframe` malveillants, puis il réinstalle (méthode STOR) ces fichiers. La durée de l'attaque est de l'ordre de quelques secondes ;
4. plusieurs connexions font suite à cette attaque et il est difficile de dire s'il s'agit de robots ou non.

Après la découverte de cet incident, la réaction des administrateurs a été de modifier le mot de passe du compte FTP accédé frauduleusement. Cette décision peut paraître saine, mais elle ne suffit pas. En effet, le point de départ de cet incident est l'infection du client FTP. Le nouveau mot de passe positionné peut lui aussi être saisi par le code malveillant.

Dans un cas comme celui-ci, il est absolument indispensable de désactiver complètement le compte utilisé frauduleusement, tant que l'on n'a pas découvert quel poste client est infecté (il peut y en avoir plusieurs pour certains comptes partagés). D'autre part, dans la mesure où l'origine légitime des connexions FTP est connue (par exemple une adresse IP bien déterminée), il est particulièrement judicieux de mettre en place du filtrage afin de restreindre les accès.

3 Winemmem, un code malveillant original

3.1 Le fait

Cette semaine, un éditeur de solution antivirus a reporté l'existence d'une variante d'un code malveillant aux méthodes plutôt singulières. En effet, ce code malveillant réussit à s'insérer à l'intérieur d'une archive auto-extractible ou un fichier d'installation d'une application tout en passant les différents contrôles d'intégrité inclus dans ces différents formats.

3.2 La technique

Le code malveillant, nommé *Winemmem* par un éditeur d'antivirus, réussit à se camoufler grâce aux données supplémentaires (aussi appelée *overlay*) du format *PE* contenues dans les fichiers auto-extractibles et autres installateurs d'applications. Il réécrit la section code de l'application originale et réalloue une taille aléatoire de code du début de la section code et de l'*OEP* à la fin du fichier, augmentant ainsi la taille des données supplémentaires. Le virus ne crée pas de nouvelle section et ne modifie pas l'entête *PE*. Afin de prendre la main lors de l'exécution du fichier infecté, le code malveillant réécrit le code original au point d'entrée (*entry point*).

À l'exécution du fichier compromis, le virus intercepte l'*API CreateFileA()* et recherche un fichier au format *PE* dans le répertoire *Program Files*. Il parcourt alors le fichier à la recherche d'une *dll* associée. Le code malveillant

copie alors la *dll* dans le répertoire du fichier exécutable associé et l'infecte en modifiant l'*entry point* et en ajoutant sa charge utile à la fin de la dernière section. Il est ensuite capable de partir à la recherche de nouveaux fichiers exécutables sur des périphériques amovibles ou de récupérer de nouveaux codes d'une machine distante dès lors qu'il a été lancé.

Pour ne pas lever une alerte lors du contrôle d'intégrité des fichiers, le code malveillant restaure les données originales. Pour cela, il intercepte les fonctions d'une *API* contenue dans *ntoskrnl.exe* qui normalement empêche l'écriture ou la suppression d'un fichier en cours d'exécution ou verrouillé par un processus.

Le code malveillant contient également une routine d'interception des *API* *ExitProcess()* et *ExitWindowsEx()* afin de se recopier dans un fichier à la fermeture de l'exécution du fichier infecté ou de Microsoft Windows.

Cette technique permet à ce code malveillant de n'être reconnu que par très peu d'antivirus et peut poser des problèmes pour la désinfection.

3.3 Les recommandations

Le CERTA rappelle qui est important de n'exécuter que des fichiers de confiance. Il est ainsi recommandé de télécharger les installateurs sur le site de l'éditeur et de vérifier, lorsque celle-ci est disponible, la signature du fichier avant son exécution.

4 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 02 et le 09 avril 2009.

5 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=1935>
- 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/>

6 Rappel des avis émis

Dans la période du 03 au 10 avril 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-128 : Vulnérabilité dans Moodle

- CERTA-2009-AVI-129 : Vulnérabilité dans Asterisk
- CERTA-2009-AVI-130 : Multiples vulnérabilités dans Joomla!
- CERTA-2009-AVI-131 : Vulnérabilités de ClamAV
- CERTA-2009-AVI-132 : Vulnérabilité dans Novell NetIdentity
- CERTA-2009-AVI-133 : Vulnérabilités dans Kerberos

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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, la DCSSI dispose d'un centre de formation :

<http://www.ssi.gouv.fr/fr/formation/>

8 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.

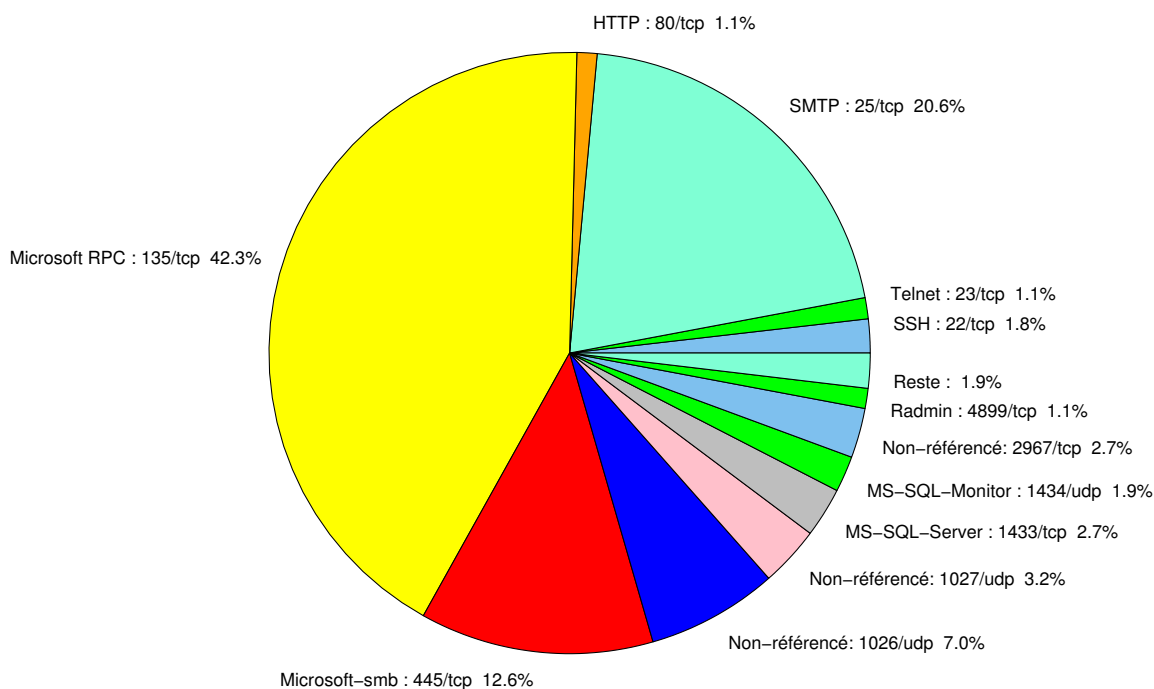


FIG. 1: Répartition relative des ports pour la semaine du 02 au 09 avril 2009

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	– CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283

				CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
135/tcp	42.35
25/tcp	20.57
445/tcp	12.56
1026/udp	7.04
1027/udp	3.24
2967/tcp	2.67
1434/udp	1.93
22/tcp	1.81
80/tcp	1.3
23/tcp	1.25
4899/tcp	1.08
21/tcp	0.45
3389/tcp	0.34
137/udp	0.28
3128/tcp	0.17
3306/tcp	0.11

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	7
3	Paquets rejetés	8

Gestion détaillée du document

10 avril 2009 version initiale.