



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 02 septembre 2011
N° CERTA-2011-ACT-035

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-35

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-035>

Gestion du document

Référence	CERTA-2011-ACT-035
Titre	Bulletin d'actualité 2011-35
Date de la première version	02 septembre 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-035.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-035/>

1 Apparition du ver *Morto*

Le ver *Morto* est récemment apparu sur les plates-formes Microsoft Windows. Il se propage en utilisant le protocole RDP (*Remote Desktop Protocol*). Afin d'infecter un poste, ce ver n'exploite pas de vulnérabilité du protocole RDP, il essaie de s'authentifier avec des comptes disposant de mot de passe faible. Le code va en effet tester une liste de noms d'utilisateur communs (*adm, admin, backup, owner...*) avec un dictionnaire restreint de mot de passe.

La présence des fichiers suivants peut indiquer une infection par le ver :

- %windir%/clb.dll ;
- %windir%/clb.dll.bak ;
- %system%/sens32.dll ;
- %windir%/temp/nthsrui.dll ;
- %windir%/offline web pages/cache.txt.

Une augmentation importante du trafic RDP peut également être un signe de la présence du code malveillant. Le ver dispose de fonctionnalités lui permettant d'arrêter les processus liés à des applications de sécurité. Une

description complète des symptômes associés à ce ver peut être trouvée sur la base de connaissances de logiciels malveillants de Microsoft (cf section documentation). Les postes infectés peuvent notamment être utilisés pour réaliser des attaques en déni de service.

Face à cette menace, le CERTA rappelle l'importance de l'utilisation de mots de passe forts. Dans une démarche de défense en profondeur, le CERTA recommande également de faire preuve de prudence lors de l'ouverture de service *RDP* sur l'extérieur, en mettant en place un mécanisme d'authentification forte, ainsi que des règles de filtrage sur adresses IP des machines autorisées à se connecter au service.

Documentation

- Base de connaissance de codes malveillants de Microsoft, Worm:WIN32/Morto.A :
<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fMorto.gen!A>
- Base de connaissance de codes malveillants de Microsoft, Worm:WIN32/Morto.gen!A :
<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fMorto.A>

2 Certificats SSL émis frauduleusement

Cette semaine la presse a relaté la découverte par un internaute d'un faux certificat SSL de serveur, signé par l'autorité de certification néerlandaise DigiNotar.

Cette découverte a été faite alors que l'internaute était victime d'une attaque par interposition (MITM ou *man-in-the-middle*) alors qu'il consultait un serveur Google. En effet le faux certificat de serveur était valable pour les serveurs du domaine google.com.

DigiNotar a confirmé l'émission frauduleuse du certificat et indiqué que d'autres certificats avaient également été émis.

En réponse à cet incident, certains éditeurs (Debian, Microsoft, Mozilla) ont supprimé le certificat de l'autorité DigiNotar de la liste des certificats préinstallés ou l'ont désactivé.

2.1 Documentation

- Bulletin de sécurité Debian DSA 2299 du 31 août 2011 :
<http://www.debian.org/security/2011/dsa-2299>
- Bulletin de sécurité Microsoft 2607712 du 29 août 2011 :
<http://www.microsoft.com/france/technet/security/advisory/2607712.msp>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-34 du 30 août 2011 :
<http://www.mozilla.org/security/announce/2011/mfsa2011-34.html>
- Bulletin du GOVCERT.NL du 31 août 2011 :
<http://www.govcert.nl/english/service-provision/knowledge-and-publication/factsheets/factsheet-fraudulent-issued-security-certificate-discovered.html>
- Billet de l'US-CERT du 30 août 2011 :
http://www.us-cert.gov/current/#fraudulent_diginotar_ssl_certificate

3 Compromission de kernel.org

Le 28 août dernier, une compromission a été détectée sur le site `kernel.org`, hébergeant le code source du noyau Linux. L'intrusion aurait eu lieu un peu plus tôt dans le mois.

Les attaquants ont pu obtenir les droits d'administration du serveur (*root*) mais la méthode utilisée pour l'élévation de privilèges n'est pour l'instant pas connue. L'accès au serveur aurait été effectué au moyen d'un compte utilisateur compromis et un cheval de Troie a été déposé. Celui-ci a été découvert suite à l'apparition de traces suspectes. Celles-ci concernaient un message d'erreur de *Xnest* alors que ce logiciel n'était pas installé sur le serveur.

Une réinstallation complète du serveur est prévue ainsi qu'un audit du code hébergé afin de vérifier l'intégrité de celui-ci. L'ensemble des 448 comptes utilisateurs vont être réinitialisés.

Le CERTA rappelle que la mise en place d'un processus de surveillance des journaux permet dans de nombreux cas de détecter au plus tôt des signes d'intrusion, ce qui a été le cas pour ce serveur.

Documentation

- Annonce sur le site kernel.org :
<http://www.kernel.org>

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 25 août au 01 septembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-473 : Vulnérabilité dans SAP NetWeaver
- CERTA-2011-AVI-474 : Vulnérabilité dans IBM Rational ClearCase et ClearQuest
- CERTA-2011-AVI-475 : Multiples vulnérabilités dans phpMyAdmin versions 33.0 à 3.4.3.2
- CERTA-2011-AVI-476 : Vulnérabilités dans Xerox FreeFlow Print Server
- CERTA-2011-AVI-477 : Vulnérabilités dans Cisco Intercompany Media Engine
- CERTA-2011-AVI-478 : Vulnérabilités dans Cisco Unified Communications Manager
- CERTA-2011-AVI-479 : Vulnérabilité dans Cisco Unified Communications Manager et Cisco Unified Presence Server
- CERTA-2011-AVI-480 : Vulnérabilité dans Squid
- CERTA-2011-AVI-481 : Vulnérabilité dans le routeur Wifi Asus RT-N56U
- CERTA-2011-AVI-482 : Vulnérabilité dans DotNetNuke
- CERTA-2011-AVI-483 : Vulnérabilité dans IBM Tivoli Storage Productivity Center
- CERTA-2011-AVI-484 : Vulnérabilité dans IBM Tivoli Federated Identity Manager
- CERTA-2011-AVI-485 : Vulnérabilité dans Apache Tomcat
- CERTA-2011-AVI-486 : Vulnérabilités dans Opera
- CERTA-2011-AVI-487 : Multiples vulnérabilités dans HP-UX Veritas Enterprise Administrator
- CERTA-2011-AVI-488 : Vulnérabilité dans Cisco NX-OS

- CERTA-2011-AVI-489 : Vulnérabilité dans IBM WebSphere Application Server Community Edition
- CERTA-2011-AVI-490 : Vulnérabilité dans Apache httpd
- CERTA-2011-AVI-491 : Vulnérabilité dans IBM WebSphere Application Server Administrative Console

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

- CERTA-2011-AVI-461-001 : Vulnérabilités dans PHP (ajout du correctif de la version 53.8 du 23 août 2011.)

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.

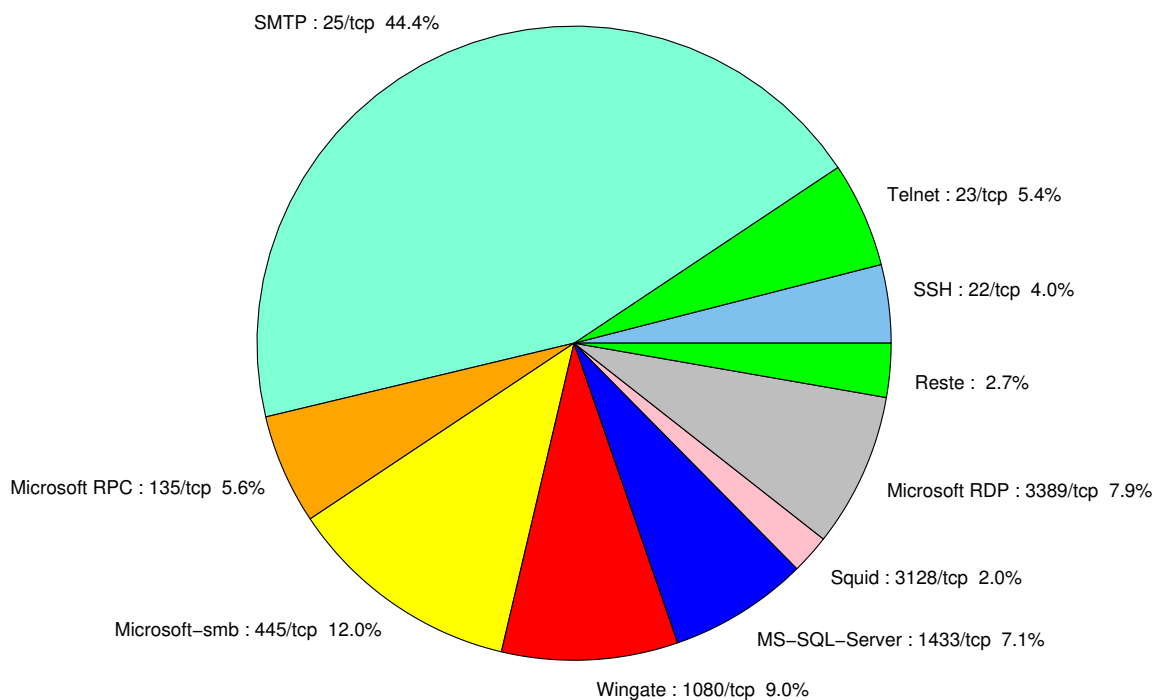


FIG. 1: Répartition relative des ports pour la semaine du 25 août au 01 septembre 2011

port	pourcentage
25/tcp	44.38
80/tcp	16.2
445/tcp	11.97
1080/tcp	8.97
3389/tcp	7.85
1433/tcp	7.1
135/tcp	5.61
23/tcp	5.36
22/tcp	3.99
3128/tcp	1.99
4899/tcp	0.99
21/tcp	0.74
3306/tcp	0.62
1434/udp	0.24
2967/tcp	0.12

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

02 septembre 2011 version initiale.