Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2011
N° CERTA-2011-ACT-028

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-28

Gestion du document

Référence	CERTA-2011-ACT-028
Titre	Bulletin d'actualité 2011-28
Date de la première version	15 juillet 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-028.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-028/

1 Zeus sur mobiles Android

Des chercheurs en sécurité ont récemment détecté une variante du célèbre logiciel malveillant *Zeus* (logiciel d'interception d'identifiants bancaires), infectant les ordiphones utilisant la plate-forme *Android*. Elle se présente sous la forme d'une application de gestion de comptes bancaires.

L'infection par cette variante s'effectue selon un processus en deux étapes :

– le poste de travail de la victime est infecté par une version de *Zeus*. Le logiciel malveillant va alors collecter des informations sur la victime, et essaie notamment de trouver le numéro et le type de téléphone mobile possédé par cette dernière.
– la victime est ensuite contactée par SMS et se voit proposer l'installation de l'application *Android* malveillante.

Une fois installée, cette application écoute et retransmet l'ensemble des messages SMS reçus par l'ordiphone victime vers un serveur Web distant. Ce procédé permet de récupérer les mots de passe uniques transmis par SMS dans le cadre d'un mécanisme d'authentification à double facteur. Ce type de mécanisme est notamment utilisé pour confirmer des virements de fonds effectués en ligne. Cette application avait déja été identifiée sur les plates-formes *BlackBerry*, *Symbian* et *Windows Mobile*.

Face à ce type de menace, le CERTA recommande de faire preuve de prudence lors de l'installation d'applications sur ordiphone en vérifiant notamment la provenance de ces applications.

2 Mises à jour Microsoft du mois de juillet

Microsoft a publié cette semaine quatre bulletins de sécurité pour ses différents logiciels totalisant 22 vulnérabilités corrigées. Parmi ces bulletins, le premier (MS11-053) concerne l'exécution de code à distance via une faille dans le protocole sans fil Bluetooth, deux (MS11-054 et MS11-056) traitent d'élévations de privilèges sous Microsoft Windows et le dernier (MS11-055) concerne l'exécution de code à distance par le biais de documents Visio malveillants. Des codes d'exploitation de certaines vulnérabilités adressées par MS11-054 (élévation de privilèges) et par MS11-055 (exécution de code arbitraire à distance) sont d'ores et déjà disponibles sur l'Internet.

Documentation

- Résumé du bulletin de sécurité Microsoft de juillet 2011 :
  https://www.microsoft.com/france/technet/security/bulletin/ms11-jul.mspx

3 Extension de maintenance pour Mandriva Linux 2010.1 et 2010.2

Le support pour les versions de *Mandriva Linux* 2010.1 et 2010.2, qui aurait dû prendre fin le 8 juillet 2011, a été reconduit. Ainsi, ces deux versions bénéficieront de mises à jour pour une durée supplémentaire de 6 mois.

La prochaine version de *Mandriva*, *Mandriva Linux 2011*, devrait être disponible le 29 août 2011. Aussi, il est judicieux de réfléchir dès maintenant à la migration vers cette version.

Le CERTA rapelle qu'il est recommandé de mettre à jour son système et ces logiciels avant que leur niveau de version ne soit plus maintenu par l'éditeur.

Documentation

- Extension de maintenance pour Mandriva 2010.1 et 2010.2 :
  http://blog.mandriva.com/fr/2011/07/14/extension-de-maintenance-pour-mandriva-2010-1-et-2010-2/

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 8 au 14 juillet 2011, le CERTA a émis les publications suivantes :

– CERTA-2011-AVI-384 : Vulnérabilité dans Hitachi HiRDB
– CERTA-2011-AVI-385 : Vulnérabilité dans Symantec Web Gateway
– CERTA-2011-AVI-386 : Vulnérabilité dans Trend Micro Control Manager
– CERTA-2011-AVI-387 : Vulnérabilité dans la pile Bluetooth des systèmes Windows
– CERTA-2011-AVI-388 : Vulnérabilités dans les pilotes en mode noyau du système Microsoft Windows
– CERTA-2011-AVI-389 : Vulnérabilité dans Microsoft Visio
– CERTA-2011-AVI-390 : Multiples vulnérabilités dans CSRSS de Microsoft Windows
– CERTA-2011-AVI-391 : Vulnérabilité dans Trend Micro Control Manager

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 règlementaire, 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 inexpliqués 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.

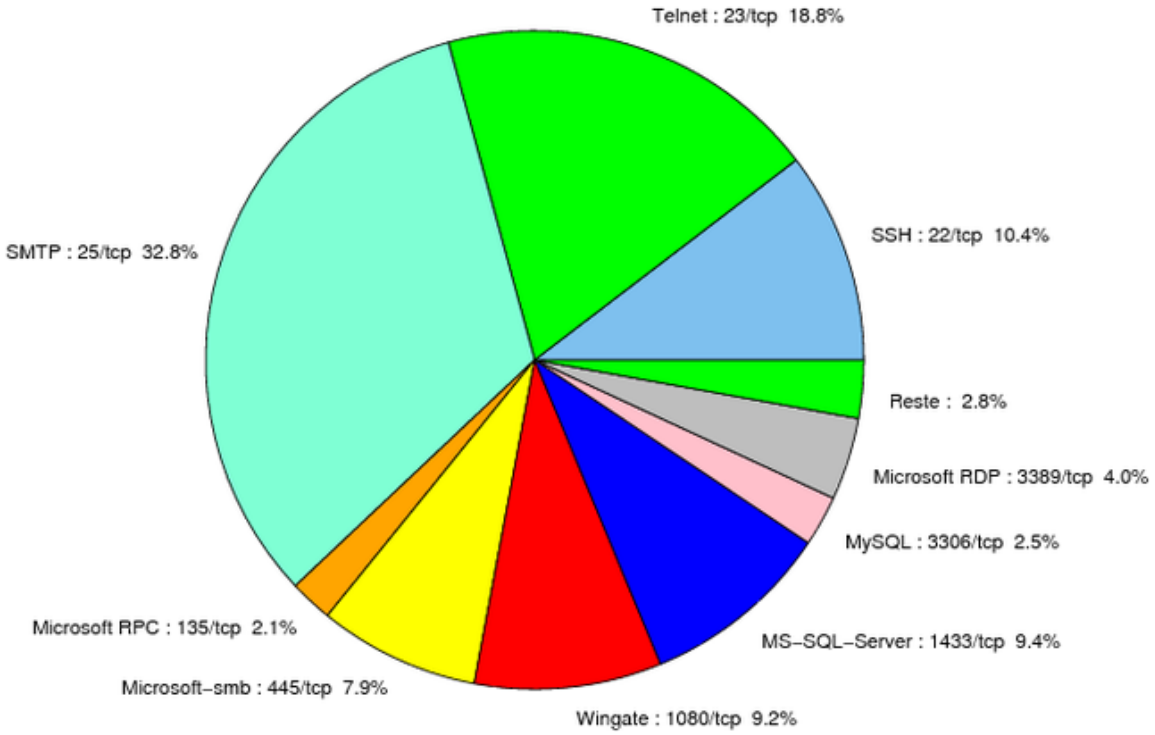

FIG. 1: Répartition relative des ports pour la semaine du 8 au 14 juillet 2011

port	pourcentage
25/tcp	32.81
80/tcp	26.93
23/tcp	18.93
22/tcp	10.38
1433/tcp	9.37
1080/tcp	9.19
445/tcp	7.9
3389/tcp	4.04
3306/tcp	2.48
135/tcp	2.11
2967/tcp	0.91
4899/tcp	0.82
21/tcp	0.18
5000/tcp	0.09

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

15 juillet 2011 version initiale.