Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 juillet 2011
N° CERTA-2011-ACT-026

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-26

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-026`

Gestion du document

Référence	CERTA-2011-ACT-026
Titre	Bulletin d'actualité 2011-26
Date de la première version	01 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.

1 Incidents de la semaine

1.1 Divulgations de données d'authentification

Au cours des dernières semaines, différents groupes d'attaquants se sont fait remarquer sur l'Internet en revendiquant diverses intrusions. Ces groupes ont notamment divulgué sur des sites publics les informations d'authentification de milliers d'utilisateurs, compromettant de fait la sécurité du site mais aussi la sécurité des utilisateurs, ces derniers ayant pu utiliser les mêmes informations d'authentification sur différents sites.

L'utilisation de sites publics par des attaquants n'est cependant pas une nouveauté. En effet, il existe, depuis plusieurs années, des logiciels espions, et notamment des enregistreurs de frappe clavier, qui se servent de ces sites afin d'extraire les données qu'ils ont capturées. Il est ainsi possible d'accéder en ligne à des journaux de capture comprenant des informations sensibles comme des mots de passe ou des numéros de cartes bancaires. Afin de limiter l'impact de ce type de fuite de données, le CERTA recommande :

- d'utiliser des mots de passe différents pour chaque service requerrant une authentification ;
- de changer régulièrement ses mots de passe ;
- de mettre en place une politique de filtrage des sites publics utilisés pour faire de l'extraction de données (sites de type *pastebin*).

1.2 Vigilance de l'utilisateur, une ligne de défense

Cette semaine, le CERTA a traité un incident dont l'impact a été limité grace à la vigilance de l'utilisateur.

Ce dernier reçoit un premier courriel dont l'objet est l'un des sujets de travail de cet utilisateur et l'adresse d'expéditeur a la forme d'une adresse personnelle de l'un de ses interlocuteurs. Ce sont des ficelles classiques de l'ingéniérie sociale, largement reprises dans les attaques ciblées. Par ce message, il peut obtenir un document PDF qui apparaît vide avec indication que le support des javascripts est désactivé. Cela a de quoi mettre la puce à l'oreille.

Un deuxième courriel, avec le même objet et le même corps de message, mais semblant émaner d'une adresse personnelle d'un autre interlocuteur, lui parvient peu de temps après. Cette fois, notre utilisateur écrit à son interlocuteur, expéditeur apparent, non pas par la fonction de réponse, mais en utilisant l'adresse légitime qu'il connaît. Cet interlocuteur lui confirme alors l'imposture.

Ces quelques minutes de vérification ont évité de gros souci à notre utilisateur et à son service. Le document piégé contient et installe un exécutable qui tente ensuite des connexions vers un serveur externe. Bref, le schéma classique des attaques dont la presse se fait régulièrement l'écho.

Le CERTA rappelle souvent dans ses recommandations la nécessaire vigilance lors de la réception de courriels d'expéditeurs inconnus, ou même d'expéditeurs connus, quand la réception est inattendue, ou que des incohérences apparaissent : langue utilisée, utilisation inhabituelle d'une adresse personnelle, objet sans rapport avec les sujets normalement traités avec l'expéditeur...

La détection de telles anomalies est très difficile à remplir par un équipement technique. La vigilance de l'utilisateur est irremplaçable. Un courriel sur une adresse connue et fiable ou un appel téléphonique de vérification peuvent épargner bien des heures d'investigations et de restauration, voire peuvent éviter des fuites d'informations sensibles.

2 Attaques via des périphériques externes

Cette semaine, la société de sécurité *Netragard* a décrit un mécanisme d'attaque intéressant. Il s'agit en fait d'une évolution de la classique clé USB piégée qui, une fois branchée, va infecter le système. Ici, il s'agit d'une souris USB qui intègre un micro contrôleur simulant le comportement d'un clavier. Une fois connecté au système, ce périphérique envoie des séquences de touches au poste afin d'exécuter un programme embarqué dans la souris et, ainsi, installer une porte dérobée.

Cette attaque montre le danger que représente la connection d'un périphérique sur un poste de travail. Aussi, il est recommandé de ne pas connecter de périphériques d'origine inconnue ou douteuse à un poste de travail et ce, quel que soit le type du périphérique.

Documentation

- Attack of the computer mouse :
  http://www.h-online.com/security/news/item/Attack-of-the-computer-mouse-1270018.html

3 Mise à jour de Thunderbird

La version 5.0 finale de *Thunderbird* est désormais disponible. Elle vient remplacer la version 3.1. Afin de garder un système à jour, il est recommandé de faire évoluer les clients de messagerie vers cette version.

Cette mise à jour reprend le nouveau système de numérotation mis en place dernièrement par *Mozilla* pour son navigateur Web *Firefox*.

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 24 au 30 juin 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-369 : Multiples vulnérabilités dans Mac OS X
- CERTA-2011-AVI-370 : Vulnérabilité dans Joomla!
- CERTA-2011-AVI-371 : Vulnérabilités dans Asterisk
- CERTA-2011-AVI-372 : Vulnérabilité dans des boitiers VPN Arkoon
- CERTA-2011-AVI-373 : Vulnérabilité dans libcurl
- CERTA-2011-AVI-374 : Multiples vulnérabilités dans Google Chrome
- CERTA-2011-AVI-375 : Vulnérabilité dans Novell File Reporter

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

- CERTA-2011-AVI-351-001 : Vulnérabilité dans le client SMB de Microsoft (ajout d'effets secondaires possibles)

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.

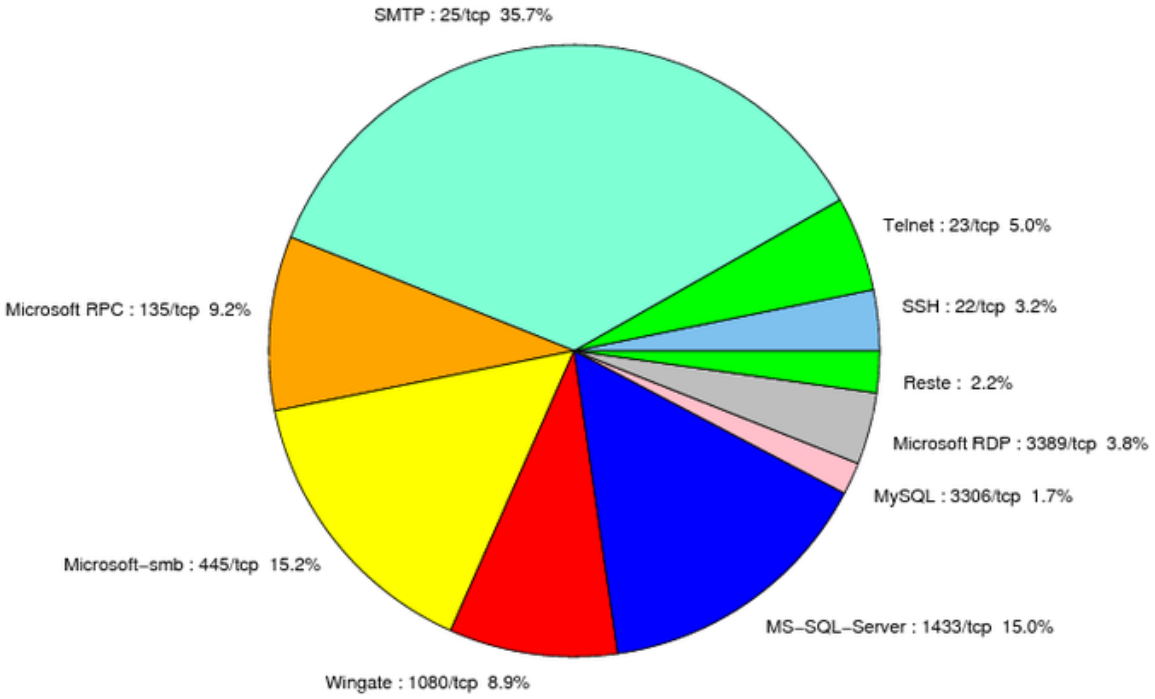

FIG. 1: Répartition relative des ports pour la semaine du 24 au 30 juin 2011

port	pourcentage
25/tcp	35.73
445/tcp	15.21
1433/tcp	15.01
135/tcp	9.2
1080/tcp	8.9
80/tcp	5.8
23/tcp	5
3389/tcp	3.9
22/tcp	3.2
3306/tcp	1.7
3128/tcp	0.7
21/tcp	0.6
2967/tcp	0.5
4899/tcp	0.4

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

01 juillet 2011 version initiale.