Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 mai 2012
N° CERTA-2012-ACT-021

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-21

Gestion du document

Référence	CERTA-2012-ACT-021
Titre	Bulletin d'actualité 2012-21
Date de la première version	25 mai 2012
Date de la dernière version	–
Source	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Filoutage par carte pré-payée

Le CERTA a reçu de nouvelles réclamations concernant un type de filoutage un peu particulier.

Dans le schéma habituel d'attaque, l'internaute est incité à suivre une redirection vers un site malveillant ou compromis qui demande alors de renseigner le numéro de carte bancaire de la victime. Dans ce cas, son navigateur est susceptible de lever une alerte si le site visité est inscrit dans une liste « anti-hameçonnage ».

Dans ce nouveau schéma d'attaque, le message envoyé réclame à l'internaute un paiement (facture, amende, ...) en utilisant un système de carte pré-payée. La victime est invitée à acheter un coupon de paiement et à en renvoyer le code à une adresse de messagerie spécifique. Dans ce type de scénario, les listes « anti-hameçonnage » évoquées précédement se révèlent donc inopérantes.

Le CERTA rappelle que l'envoi d'information permettant la réalisation d'une transaction bancaire doit amener l'utilisateur à la plus grande vigilance. En particulier, il convient par principe de considérer comme suspecte, toute demande de paiement reçue par courrier électronique.

Ces courriels malveillants peuvent être signalés aux forces de l'ordre au travers du site du ministère de l'intérieur : `http://www.internet-signalement.gouv.fr`.

2 Google et DNSChanger

Google annonce, sur son *blog* dédiée à la sécurité, qu'une notification est désormais envoyée aux internautes infectés par le code malveillant *DNSChanger*. Cette notification revêt la forme d'un message informatif affiché en haut de la page des résultats d'une recherche *Google*.

Si l'intention de *Google* est louable, elle peut générer certains problèmes, car :

- le message délivré par *Google* est alarmiste et similaire à ceux utilisés par les « faux antivirus » ;
- la notification comporte un lien cliquable. Des attaquants pourraient imiter le message de *Google* et inclure un lien vers un code malveillant. Des utilisateurs dont la machine n'est pas infectée par *DNSChanger* pourraient ainsi céder à la panique et compromettre leur poste.

Le CERTA recommande aux utilisateurs qui verraient le message de *Google* de ne pas cliquer sur le lien qu'il contient et :

- en environnement professionnel, de prévenir leur RSSI ;
- pour les particuliers, de confirmer une éventuelle infection en consultant les sites du groupe de lutte contre ce code malveillant, le *DNS Changer Working Group* (DCWG).

Documentation

- Message posté sur le *blog* de sécurité de *Google* :
  http://googleonlinesecurity.blogspot.co.uk/2012/05/notifying-users-affected-by-dnschanger.html
- Site de détection du DCWG :
  http://www.dcwg.org/detect/

3 Rappel des avis émis

Dans la période du 18 au 24 mai 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-282 : Vulnérabilité dans IBM Cognos
- CERTA-2012-AVI-283 : Multiples vulnérabilités dans RealPlayer
- CERTA-2012-AVI-284 : Multiples vulnérabilités dans Apple QuickTime
- CERTA-2012-AVI-286 : Multiples vulnérabilités dans HP-UX
- CERTA-2012-AVI-287 : Vulnérabilité dans HP OpenVMS
- CERTA-2012-AVI-288 : Multiples vulnérabilités dans Symantec Web Gateway
- CERTA-2012-AVI-289 : Vulnérabilité dans IBM Rational Change
- CERTA-2012-AVI-290 : Multiples vulnérabilités dans Moodle
- CERTA-2012-AVI-291 : Vulnérabilités dans Symantec Endpoint Protection
- CERTA-2012-AVI-292 : Multiples vulnérabilités dans Wireshark

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

- CERTA-2012-AVI-285-001 : Vulnérabilités dans OpenOffice et LibreOffice (Ajout de la vulnérabilité concernant la référence CVE CVE-2012-2334)

4 Actions suggérées

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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

Gestion détaillée du document

25 mai 2012 version initiale.