Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 février 2012
N° CERTA-2012-ACT-008

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-08

Gestion du document

Référence	CERTA-2012-ACT-008
Titre	Bulletin d'actualité 2012-08
Date de la première version	24 février 2012
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 Virus DNSChanger

Le CERTA informe ses lecteurs d'un risque de coupure d'accès à la plupart des services de l'Internet, à partir du 8 mars 2012, pour les ordinateurs infectés par le virus DNSChanger.

1.1 Rappel sur le DNS

Le protocole DNS, véritable « annuaire » de l'Internet, permet principalement à un système d'exploitation de résoudre la ou les adresses IP (*Internet Protocol*) d'un serveur dont l'utilisateur ne connaît que le nom d'hôte. En effet, sur l'Internet les systèmes ne savent se contacter qu'au moyen de leur adresse IP numérique. Par exemple, un serveur DNS sera capable de répondre à un système l'interrogeant que l'adresse IP du serveur Web du CERTA (nom d'hôte $www.certa.ssi.gouv.fr$) est a cet instant 213.56.176.2.
Ce protocole est donc utilisé dès qu'un système tente d'accéder à un serveur par son nom au lieu de son adresse IP : lors de la connexion à une messagerie, à un site Web, etc. Si ce service n'est plus accessible, les utilisateurs ne pourront plus accéder à aucun serveur Internet, s'ils ne connaissent que leur nom d'hôte.

Pour plus d'informations sur le protocole DNS, vous pouvez vous reporter à la note d'information du CERTA CERTA-2008-INF-002.

1.2 Modification des DNS par un logiciel malveillant

La modification des serveurs DNS utilisés par un poste ou un serveur est exploitée depuis longtemps à des fins malveillantes. En effet, si les requêtes DNS sont émises vers un « annuaire » malveillant, les adresses IP retournées sont contrôlées par l'attaquant, et peuvent pointer vers d'autres serveurs que ceux initialement recherchés.
De nombreuses manipulations sont alors possibles :

- capture et/ou analyse du trafic de l'utilisateur ;
- détournement de courriels ;
- détournement de la navigation vers des sites Web malveillants ;
- fournir de fausses mise à jour de logiciels et donc installer des logiciels malveillants ;
- etc.

Ainsi, de nombreux virus de la classe DNSChanger ont pour fonction principale de modifier frauduleusement un système afin d'en changer les serveurs DNS configurés.

Le travail de plusieurs agences gouvernementales internationales a permis d'identifier un grand nombre d'adresses IP de serveurs DNS malveillants dans les plages d'adresses suivantes :

- 85.255.112.0 à 85.255.127.255 ;
- 67.210.0.0 à 67.210.15.255 ;
- 93.188.160.0 à 93.188.167.255 ;
- 77.67.83.0 à 77.67.83.255 ;
- 213.109.64.0 à 213.109.79.255 ;
- 64.28.176.0 à 64.28.191.255.

Un poste infecté par cette classe de virus aura donc comme serveurs DNS configurés des adresses IP figurant parmis ces intervalles.

1.3 Échéance du 8 mars 2012

Après l'opération « *Ghost Click* » coordonnée par le FBI en novembre 2011, les serveurs malveillants ont été saisis. Afin d'éviter que les utilisateurs compromis perdent leur accès aux services de l'Internet suite à cette coupure, la justice américaine a demandé à ce qu'un consortium international soit créé pour que les serveurs DNS malveillants soient remplacés par des serveurs « bienveillants » répondant aux requêtes par les adresses IP légitimes, pour une période de quatre mois. C'est ainsi que le *DNSChanger Working Group* (ou *DCWG*) a été créé, et gère actuellement ces serveurs DNS de remplacement. Grâce à ces serveurs, les utilisateurs de postes infectés peuvent continuer à résoudre des noms d'hôte de manière conforme.

Ces serveurs de remplacement vont être débranchés le 8 mars 2012. À partir de cette date, tous les systèmes qui ont été infectés par un virus de la classe *DNSChanger* ne pourront donc plus contacter de serveur DNS, et leurs utilisateurs auront alors beaucoup de difficultés pour accéder à la plupart des services disponibles sur l'Internet.

1.4 Recommandations

Pour éviter cette situation, la seule solution est de vérifier dès à présent que son ou ses postes connectés à l'Internet sont bien configurés pour utiliser des serveurs DNS légitimes (généralement ceux fournis par le fournisseur d'accès dans le cadre d'un poste personnel privé). La procédure pour afficher les serveurs DNS utilisés par son poste est à obtenir auprès de l'éditeur du système d'exploitation utilisé.

Toutefois, le *DCWG* fournit sur son site Web (rubrique « *Checkup* », section « *Checking via browser* ») une liste d'adresses permettant de vérifier rapidement si son poste est compromis. Lors de l'accès à un de ces sites, un message apparaissant dans un cadre rouge indique que le poste, ou l'équipement réseau en charge de résoudre les requêtes pour ce poste, utilise des serveurs DNS dont les adresses sont situées dans les intervalles évoqués ci-dessus.

Dans le cas d'un réseau d'entreprise, il est généralement conseillé d'avoir un seul système autorisé à effectuer des requêtes auprès de serveurs DNS externes et d'appliquer correctement des règles de filtrage pour imposer ce comportement. Dans ce cas, les postes de ce type de réseau ne peuvent pas contacter directement des serveurs DNS distants, et leur compromission aurait déjà été détectée.

Ce type de virus a été propagé par de multiples vecteurs. Il convient donc de maintenir à jour tous les logiciels et modules installés sur son poste, et de rester vigilant lors de l'utilisation de ses logiciels. La modification des

DNS n'étant qu'une des fonctionalités de cette gamme de virus, un poste dont les serveurs DNS ont été modifiés par des adresses de serveurs malveillants doit être considéré comme compromis, et idéalement faire l'objet d'une réinstallation à partir de supports sains.

Ces virus sont également connus pour tenter d'accéder à des interfaces d'administration d'équipement réseau (de type routeur grand public) afin d'y changer également la configuration DNS. Ces équipements propagent à leur tour des serveurs DNS malveillants aux postes qui obtiennent leur configuration réseau (par exemple par DHCP). Dans ce type d'environnement, si un poste a été compromis par un virus du type *DNSChanger*, il est conseillé de vérifier la configuration DNS des équipements réseaux en amont. En cas de découverte d'une compromission de ces équipements, leur reconfiguration à partir d'éléments sains doit alors être réalisée.

Documentation

- DNSChanger Working Group :
  http://www.dcwg.org
- Communiqué de presse du FBI concernant l'opération « Ghost Click »
  http://www.fbi.gov/news/stories/2012/november/malware_110911/DNS-changer-malware.pdf
- Du bon usage des DNS :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002/
- Bulletin d'actualité CERTA-2011-ACT-008 « Exploitation de vulnérabilités d'équipements réseau » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-008/
- Bulletin d'actualité CERTA-2008-ACT-052 « DNS Changer v. 2.0 » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-052/
- Bulletin d'actualité CERTA-2008-ACT-047 « Modification malveillante des résolutions DNS » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-047/

2 Applications pour ordiphones - mise en garde

L'omniprésence des technologies nomades élargit le champ de nuisance des cyberdélinquants. Sur certaines boutiques d'applications pour ordiphones, il existe des applications non officielles qui, selon leur description, permettent de réaliser des téléprocédures (télédéclaration par exemple). Prudence !

Dans le meilleur des cas, l'application est simplement une interface adaptée à l'ordiphone. Elle se limite à relayer les informations entrées par l'utilisateur vers le site Web de l'administration qui héberge la téléprocédure.

Dans un cas beaucoup moins favorable, l'application, interposée entre l'utilisateur et le site Web de l'administration, envoie vers le serveur de l'administration les données entrées et, à l'insu de l'utilisateur de l'ordiphone, envoie en parallèle une copie vers un serveur malveillant. Les applications sur ordiphone représentent une nouvelle technique de filoutage.

Pour ces applications, comme pour les téléchargements de logiciels sur des ordinateurs classiques, le CERTA recommande d'effectuer un minimum de vérifications avant de les télécharger.

Il faut s'assurer du caractère officiel de l'application, si intéressante puisse-t-elle paraître. Cela peut passer par la consultation du site Web de l'organisme qui propose la téléprocédure, qui pourra indiquer s'il existe ou non une application officielle, et pour quels ordiphones. Dans le doute, la prudence commande de ne pas télécharger.

Il est également préférable de vérifier que la boutique de téléchargement depuis laquelle une application est téléchargeable est une boutique officielle pour l'ordiphone.

En complément, les responsables de la communication sont invités à préciser sur leurs sites Web si des applications pour ordiphones ont été développées de manière officielle et sur quelles boutiques elles sont disponibles.

3 Firefox et le support étendu

Un groupe de travail de la fondation Mozilla a travaillé sur une solution « entreprise » du navigateur Firefox. Le résultat est l'adoption d'une version à support étendu dont le cycle de support est plus long que celui de la version standard, c'est à dire 54 semaines contre 6.

Les versions à support étendu auront comme suffixe ESR (*Extended Support Release*). Firefox 10 sert de base à cette première version ESR. La fin de support est programmée pour le 12 février 2013.

Documentation

- Annonce des versions à support étendu de Firefox :
  https://www.mozilla.org/en-US/firefox/organizations/
- Présentation de la version à support étendu de Firefox :
  https://wiki.mozilla.org/Enterprise/Firefox/ExtendedSupport:Proposal

4 Fins de support annoncées

4.1 Firefox 3.6

Dans sa présentation de la version à support étendu de Firefox, la fondation Mozilla rappelle que le support de la branche 3.6 cessera le 24 avril 2012. Cela ne laisse plus que deux mois pour migrer vers une version maintenue.

Documentation

- Présentation de la version à support étendu de Firefox :
  https://wiki.mozilla.org/Enterprise/Firefox/ExtendedSupport:Proposal

4.2 ISC DHCP 3.1-ESV

L'ISC annonce la fin de support de la version 3.1-ESV de son implémentation de serveur DHCP pour le 1^{er} mars 2012.

Le sigle ESV à la fin du numéro de version signifie *Extended Support Version*. Pour cette version de ce logiciel, le consortium ISC a rallongé de six mois les quatre années de support garanti pour les versions ESV.

La version 4.1-ESV du serveur DHCP est à support étendu jusqu'en décembre 2012.

Documentation

- Politique de support de l'ISC :
  http://www.isc.org/softwaresupportpolicy
- Annonce de la fin de support d'ISC DHCP 3.1-ESV du 26 janvier 2012 :
  http://www.isc.org/announcement/isc-dhcp-31-esv-end-life-march-1st-2012

5 Vulnérabilité de certains générateurs aléatoires utilisés pour la création de clés RSA

Vulnérabilité et conséquences

Le 14 février 2012, l'*Electronic Frontier Foundation* a publié un message indiquant la découverte par Arjen Lenstra, de l'École Polytechnique Fédérale de Lausanne, d'une vulnérabilité dans certains générateurs d'aléas assurant la génération de clés publiques utilisées sur Internet.

Dans la majeure partie des cas, la vulnérabilité mise en évidence permet à toute personne ayant enregistré une session sécurisée entre un client légitime et un équipement utilisant une clé faible d'en déchiffrer le contenu. L'exploitation est possible *a posteriori*, quel que soit le moment où l'écoute a été réalisée. L'ANSSI considère donc cette vulnérabilité comme très sérieuse. Cette vulnérabilité n'impacte cependant, en première analyse, que les équipements réseau. La sécurité des téléservices sur Internet n'est donc aucunement remise en question.

Cette vulnérabilité illustre une nouvelle fois l'importance d'utiliser des générateurs d'aléas de qualité, conformément aux orientations définies dans le Référentiel général de sécurité (Annexe B.1, voir section Documentation). En effet, dans le cas contraire, les propriétés de sécurité ne peuvent généralement plus être garanties.

Recommandations

En attendant des analyses plus poussées, l'ANSSI recommande très fortement de mettre en place les mesures suivantes dans les plus brefs délais :

- identification et suppression des services (clairs ou HTTPS) des équipements réseau accessibles depuis des réseaux ouverts (et en particulier d'Internet) lorsqu'ils ne sont pas strictement nécessaires ;
- pour les services utiles qui ne peuvent être désactivés, renouvellement systématique des certificats d'authentification utilisés pour la protection des sessions d'administration sécurisées par SSL. Ces certificats doivent être idéalement générés en utilisant des produits qualifiés [1] par l'ANSSI ;
- renouvellement de l'ensemble des mots de passe et authentifiants utilisés pour l'administration de ces services ;
- recherche des possibles compromissions induites par la vulnérabilité par analyse des journaux (connexion d'un administrateur de l'équipement à des heures non habituelles, connexions répétées depuis des adresses IP à l'étranger, etc.).

Ces recommandations doivent être appliquées sur les équipements réseau (serveurs, VPN, routeurs, commutateurs, outils d'administration et de supervision) accessibles depuis des réseaux ouverts.

Par ailleurs, cette affaire est l'occasion de rappeler qu'il convient d'observer la plus grande prudence et de ne pas, dans la mesure du possible, effectuer d'action sensible sur des réseaux publics (*hotspots* WiFi, etc.) lorsque cette opération n'est pas protégée par des moyens alternatifs (IPsec par exemple). En particulier, l'administration d'équipements à distance sur des réseaux ouverts, sans protection par des équipements qualifiés par l'ANSSI, est fortement déconseillée.

Documentation

- Article de A. Lenstra et *al.* :
  http://eprint.iacr.org/2012/064
- Annexes du Référentiel général de sécurité :
  http://references.modernisation.gouv.fr/annexes-du-rgs

6 Rappel des avis émis

Dans la période du 11 février 2012 au 23 février 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-083 : Vulnérabilités dans Citrix XenServer Web Self Service
- CERTA-2012-AVI-084 : Vulnérabilités dans Adobe Flash Player
- CERTA-2012-AVI-085 : Multiples vulnérabilités dans Oracle Java
- CERTA-2012-AVI-086 : Vulnérabilité dans les produits Mozilla
- CERTA-2012-AVI-088 : Vulnérabilités dans Google Chrome
- CERTA-2012-AVI-089 : Vulnérabilité dans Cisco NX-OS
- CERTA-2012-AVI-090 : Vulnérabilité dans Cisco IronPort
- CERTA-2012-AVI-091 : Vulnérabilité dans libvorbis
- CERTA-2012-AVI-092 : Vulnérabilité dans TYPO3
- CERTA-2012-AVI-093 : Vulnérabilité dans phpMyAdmin
- CERTA-2012-AVI-095 : Vulnérabilité dans Python

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

- CERTA-2012-AVI-087-001 : Vulnérabilité dans libpng (ajout de la référence au bulletin Mandriva)
- CERTA-2012-AVI-094-001 : Vulnérabilité dans libxml2 (rectification du lien Mandriva)

1. www.ssi.gouv.fr/fr/produits

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 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.

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 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.

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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique62.html

Gestion détaillée du document

24 février 2012 version initiale.