Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 octobre 2011
N° CERTA-2011-ACT-042

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-42

Gestion du document

Référence	CERTA-2011-ACT-042
Titre	Bulletin d'actualité 2011-42
Date de la première version	21 octobre 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-042.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-042/

1 Incidents de la semaine

1.1 Une défiguration n'est pas un incident mineur

Dans son activité de veille, le CERTA a repéré la défiguration du site web d'une administration. Celle-ci, prévenue, s'est classiquement retournée vers le prestataire qui a conçu le site et l'héberge. Le site a rapidement recouvré son aspect normal.

Le répit fut de courte durée pour le client. En effet, le serveur étant resté globalement vulnérable, le CERTA a repéré une page de filoutage dans le site soi-disant réparé.

Le CERTA ne répétera jamais assez qu'un incident, même d'apparence superficiel comme une défiguration, doit être traité en profondeur et de manière exhaustive.

Une intrusion est l'illustration visible de la porosité d'un site Web. Il convient de reconstruire complètement et de durcir le serveur lors de la remise en service du site. Dans la négative, des utilisations illicites plus discrètes (site *warez*) ou des portes dérobées peuvent persister.

Par ailleurs, la suppression pure et simple des traces de l'intrusion peut nuire à une enquête si le serveur a servi à des actions contre une autre entité. Ces traces doivent donc être conservées, au moins provisoirement.

1.2 Documentation

- Note d'information du CERTA *Les bons réflexes en cas d'intrusion* :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/
- Note d'information du CERTA *Bonnes pratiques concernant l'hébergement mutualisé* :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/

2 Le code malveillant Duqu

Ce code malveillant (prononcer diou-kiou) a été analysé par plusieurs organismes spécialisés dont les éditeurs d'antivirus (voir section Documentation). Le rapport Symantec a fait des analogies avec le ver Stuxnet, médiatisé en 2010. L'état actuel des analyses doit conduire à une certaine retenue dans la comparaison.

2.1 Points communs

Des blocs de code identiques se retrouvent dans Stuxnet et Duqu. La reprise de blocs de programmes, sources ou compilés, notamment pour les parties utilitaires (référence aux API systèmes, etc.) n'est pas un phénomène nouveau dans le monde des codes malveillants.

Plus intéressant, l'installation d'un pilote (*driver*) malveillant par Duqu est rendue moins visible par l'utilisation d'une signature qui correspond, pour sa vérification, à un certificat valide. Stuxnet a utilisé des certificats correspondant à deux sociétés différentes. Le certificat pour Duqu était produit pour la société taïwanaise C-Media Electronics Incorporated et signé par Verisign. Le détail de la production de cette signature illicite n'est actuellement pas connu. Ce certificat a été révoqué le 14 octobre 2011 selon Symantec. Des variantes se présentent comme des pilotes non signés produits par JMicron Technology Corporation, Adaptech Inc. et IBM.

Les deux codes malveillants tentent des connexions par Internet. Dans l'état des connaissances actuelles, Duqu tente de se connecter à l'adresse IP 206.183.111.97 en HTTP et HTTPS.

Il n'est pas exclu que d'autres adresses soient utilisées, par exemple dans des variantes futures.

2.2 Différences

À la différence de Stuxnet, les variantes de Duqu analysées n'embarquent pas de charge utile visant les systèmes industriels.

Cela ne doit pas faire baisser la vigilance. Duqu ouvre une porte dérobée sur le système compromis. Dès lors, l'attaquant peut utiliser l'ordinateur vulnérable pour attaquer un système informatique classique aussi bien qu'un système industriel.

Un logiciel espion a également été trouvé sur des systèmes infectés avec des fonctions de copie d'informations de configuration et de capture des frappes clavier.

2.3 Documentation

- F-Secure - Description de code malveillant :
  http://www.f-secure.com/v-descs/backdoor_w32_duqu.shtml
- Kaspersky - Blog Securelist :
  http://www.securelist.com/en/blog/208193182/The_Mystery_of_Duqu_Part_One
- McAfee - Blog :
  http://blogs.mcafee.com/mcafee-labs/the-day-of-the-golden-jackal
- Microsoft - Encyclopédie sur les codes malveillants :
  http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan:Win32/Duqu.C&TreatID=-2147316671
- Symantec - Rapport d'analyse :
  http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w"é_duqu_the_precursor_to_the_ne

3 Fausse mise à jour flash…

Un cheval de Troie cible actuellement les utilisateurs de Mac OS X. Celui-ci se fait passer pour une mise à jour du lecteur flash.

En demandant le mot de passe de l'administrateur du système (comportement légitime lors de l'installation d'une application), celui-ci désactive les protections existantes sur le système telles que *XProtectUpdater* permettant de mettre à jour le moteur de détection de malwares inclus dans Mac OS X.

Le CERTA rappelle que le téléchargement de logiciels non hébergés par l'éditeur requiert la plus grande prudence de la part de l'utilisateur et ce, quel que soit le système utilisé.

Documentation

- Description du trojan «Flashback.C» sur le site de l'éditeur F-Secure :
  http://www.f-secure.com/v-descs/trojan-downloader_osx_flashback_c.shtml

4 . . . et mise à jour de l'outil de configuration Adobe Flash Player

Cette semaine Adobe a corrigé une vulnérabilité dans son outil en ligne de configuration des lecteurs Flash. Cette vulnérabilité de type *clickjacking* permet l'activation à distance de la webcam ou du microphone du poste visitant une page Web malveillante.

Cette mise à jour repose sur une modification de l'outil de configuration du lecteur qui se situe sur le site Web d'Adobe. En effet, le CERTA profite de cette actualité pour rappeler que les moyens de modification des paramètres de configuration du lecteur ne résident pas toujours sur le poste de travail. Depuis la version 10.3 d'Adobe Flash Player, il est possible de configurer son lecteur Flash depuis le panneau de configuration Windows ou les préférences Système de Mac OS. Tout utilisateur d'une version antérieure ou d'autres systèmes d'exploitation souhaitant prendre connaissance et/ou modifier les différentes configurations d'Adobe Flash Player doit se rendre à cette adresse :

`http://www.macromedia.com/support/documentation/fr/flashplayer/help/settings_manager01.html`

Documentation

- Publication sur le bloc-notes d'Adobe concernant la modification de la configuration d'Adobe Flash Player :
  http://blogs.adobe.com/psirt/2011/10/clickjacking-issue-in-adobe-flash-player-settings-manager.html

5 Élévation de privilèges d'administrateur local à administrateur de domaine (4ème et dernière partie)

Nous terminons cette série d'articles sur l'élévation de privilèges dans *Active Directory*. Les attaques abordées dans cette série d'articles constituent la grande majorité des moyens utilisés par les attaquants dans les incidents gérés par le CERTA. En aucun cas il ne s'agit ici d'une énumération exhaustive des attaques possibles contre *Active Directory*. De plus, nous nous sommes concentrés sur les aspects relatifs aux faiblesses des déploiements d'*Active Directory*. Nous avons volontairement exclu de notre série d'articles les vulnérabilités induites par l'absence d'une ou plusieurs mises à jour de sécurité ou bien encore par l'utilisation de systèmes d'exploitation obsolètes.

Lent : Rechercher dans le système de fichiers la présence d'informations d'authentification

Attaque :

Lors de la prise de contrôle d'une machine, a fortiori avec les privilèges d'administration, l'attaquant dispose d'un volume important d'information à sa disposition : la base de registre, le système de fichiers, l'accès au réseau de l'entreprise. Avec un minimum de méthode et de patience, il va pouvoir accéder :

- aux mots de passe stockés dans la base de registre ou dans les fichiers de configuration d'applications (VNC, unattend.txt, etc.).
- aux différents scripts accessibles :
  - dans le SYSVOL ;
  - les partages réseau.

Autant de précieuses sources d'informations d'identification que l'attaquant va réutiliser sur d'autres systèmes (SGBD, Application métier, . . .).

Prévention :

Les systèmes « exposés » (portables, serveurs exposés à l'Internet, ordinateurs de bureau) doivent être régulièrement audités afin de déterminer la liste des informations d'identification disponible sur le poste/serveur. De plus, on complètera cet audit par une évaluation de la criticité des informations disponibles sur le réseau, en lecture, par ce poste et par son utilisateur (mots de passe, documents sensibles,...).

Très lent : Attaquer les informations d'identification mises en cache

Attaque :

Sur les machines membres d'un domaine *Active Directory*, par défaut, le système stocke un vérificateur d'information d'authentification (à ne pas confondre avec le condensat du mot de passe). Cette information va permettre au système d'ouvrir une session pour un utilisateur du domaine même sans connectivité à l'*Active Directory*. Ce mécanisme requiert que l'utilisateur se soit connecté interactivement à ce poste en présence d'un contrôleur de domaine.

L'attaque consiste à extraire ces vérificateurs et à les attaquer afin de retrouver le mot de passe de l'utilisateur. Cette attaque est très lente car chaque tentative utilise de nombreuses opérations cryptographiques. De plus, contrairement au condensat du mot de passe, le vérificateur ne peut pas être utilisé pour s'authentifier sur le réseau. Il est nécessaire de « casser » le mot de passe pour s'authentifier.

Prévention :

Une politique de mots de passe forts est une mesure de prévention nécessaire et suffisante pour se prémunir de cette attaque. D'autres alternatives comme la désactivation de ce mécanisme de cache, limitent inutilement l'accès au poste de travail si aucun contrôleur de domaine n'est joignable (ordinateur nomade, problème de connectivité réseau, etc.).

6 Rappel des avis émis

Dans la période du 14 au 20 octobre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-568 : Vulnérabilité dans Cisco TelePresence Video Communication Server
- CERTA-2011-AVI-569 : Multiples vulnérabilités dans Apple iTunes
- CERTA-2011-AVI-570 : Vulnérabilité dans Asterisk
- CERTA-2011-AVI-571 : Vulnérabilités dans VMWare ESX et ESXi
- CERTA-2011-AVI-572 : Vulnérabilités dans phpMyAdmin
- CERTA-2011-AVI-573 : Vulnérabilité dans Cisco Network Admission Control Manager
- CERTA-2011-AVI-574 : Multiples vulnérabilités dans Cisco Adaptive Security Appliances
- CERTA-2011-AVI-575 : Vulnérabilité dans ClamAV
- CERTA-2011-AVI-576 : Vulnérabilités dans Symantec IM Manager
- CERTA-2011-AVI-577 : Vulnérabilités dans Joomla!
- CERTA-2011-AVI-578 : Vulnérabilité dans Opera
- CERTA-2011-AVI-579 : Multiples vulnérabilités dans Moodle
- CERTA-2011-AVI-580 : Vulnérabilités dans Java

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

21 octobre 2011 version initiale.