Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 20 avril 2015
N° CERTFR-2015-ACT-016

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-016

1 - Cryptofortress

Cet article rappelle les recommandations à prendre contre les rançongiciels en détaillant le fonctionnement de l'un d'entre eux.

Le CERT-FR a détecté une nouvelle variante dans la famille des rançongiciels : `CryptoFortress`. Ce programme malveillant arrive par les voies classiques de l'ingénierie sociale. Le plus souvent il s'agit d'une pièce jointe à un courriel. Une fois exécuté, il chiffre les fichiers de la victime avant d'exiger une rançon en prétendant que son versement assurera la restauration du système.

Chiffrement des fichiers

Afin de procéder au chiffrement des fichiers, le maliciel utilise l'algorithme de chiffrement symétrique AES. Pour cela il génère sur l'ordinateur de la victime une clé de 256 bits. Cette clé va servir pour le chiffrement de tous les fichiers. Chaque fois qu'un chiffrement est effectué, le fichier en question devient inutilisable.

Les fichiers concernés par le cryptogiciel sont ceux présents dans les disques accessibles via la fonction Windows `GetLogicalDrive`, ainsi que sur les ressources réseau pouvant être obtenues grâce à la fonction `WNetOpenEnum`. Cela concerne tous les disques durs ainsi que les lecteurs réseau, comme les dossiers partagés. Seuls les fichiers ne possédant pas de protection en écriture seront altérés. Chaque fois qu'un fichier est chiffré, le maliciel lui attribue l'extension `.frtrss` et une page de rançon est déposée dans son dossier.

Recouvrement des fichiers

Dans le but de garder la clé AES secrète, le logiciel malveillant utilise l'algorithme de chiffrement asymétrique RSA afin d'en stocker une version chiffrée. Cet algorithme exploite deux clés différentes : une clé publique servant à chiffrer un secret et une clé privée servant à le déchiffrer. La clé publique est embarquée dans l'exécutable et sert à donc chiffrer la clé AES. La clé privée, nécessaire pour le déchiffrement, n'est jamais présente sur l'ordinateur de la victime, mais stocké sur le serveur de l'attaquant. En cliquant sur un des liens présents dans la page de rançon, la victime procède au paiement et envoie la clé AES chiffrée au serveur qui la déchiffre à l'aide de la clé privée. Au final, la clé AES ainsi déchiffrée est théoriquement renvoyée à la victime qui peut alors procéder au déchiffrement de ses fichiers.

Sans la connaissance de la clé privée RSA, il est pratiquement impossible de recouvrer les fichiers. Les raisons sont :

- l'utilisation d'AES avec une clé de 256 bits pour le chiffrement des fichiers ;
- la taille de la clé RSA : 1024 bits, assez importante pour empêcher les tentatives de factorisation ;
- la terminaison du processus et la libération de la mémoire une fois le chiffrement effectué, laissant peu d'espoir quant à l'extraction, a posteriori, de la clé AES ayant servi au chiffrement des fichiers.

CryptoFortress inclut également la possibilité de supprimer les antémémoires de volume (« Volume Shadow Copies »), il n'est donc pas toujours possible de les utiliser pour retrouver les fichiers.

La meilleure solution de recouvrement est donc de restaurer le système avec des sauvegardes réalisées avant l'infection.

Recommandations

Le CERT-FR recommande les actions suivantes :

- effectuer régulièrement des copies de sauvegarde sur des supports déconnectés ;
- sensibiliser les utilisateurs : la plupart de ces messages sont non sollicités, d'un émetteur inconnu et contiennent des fautes d'orthographe ;
- utiliser des restrictions logicielles notamment pour interdire l'exécution de code depuis les répertoires temporaires ;
- mettre à jour les bases de signatures antivirus et des passerelles de messagerie ;
- mettre en place une protection appropriée des partages de fichiers, notamment en positionnant les permissions en lecture seule lorsque c'est possible ;
- appliquer les correctifs de sécurité (système d'exploitation et applications).

Si l'un de vos utilisateurs est victime de ce type de maliciel, le CERT-FR recommande la conduite suivante :

- isoler au plus vite le poste compromis du réseau ;
- identifier le message malveillant et rechercher d'éventuelles copies envoyées à d'autres destinataires afin de les supprimer ;
- reformater le poste client et réinstaller un système sain ;
- restaurer les copies de sauvegarde des fichiers perdus.

Le versement de la rançon à l'attaquant ne garantit ni le déchiffrement des fichiers ni la sécurité des moyens de paiement utilisés. Il peut notamment entraîner l'installation de maliciels supplémentaires sur le poste utilisé.

2 - Mise à jour mensuelle de Microsoft

Le 14 avril 2015, Microsoft a publié 11 bulletins de sécurité, dont 4 sont considérés comme critiques et 7 comme importants :

- MS15-032 (critique) qui concerne Internet Explorer ;
- MS15-033 (critique) qui concerne Microsoft Office ;
- MS15-034 (critique) qui concerne le pilote HTTP.sys ;
- MS15-035 (critique) qui concerne le moteur de rendu graphique de Windows ;
- MS15-036 (important) qui concerne SharePoint ;
- MS15-037 (important) qui concerne le gestionnaire des tâches de Windows ;
- MS15-038 (important) qui concerne les niveaux d'usurpation d'identité des fils d'exécution ;
- MS15-039 (important) qui concerne les services de base XML ;
- MS15-040 (important) qui concerne les services de fédération Active Directory ;
- MS15-041 (important) qui concerne l'environnement .NET ;
- MS15-042 (important) qui concerne Hyper-V.

Internet Explorer

Dix vulnérabilités ont été corrigées au sein d'Internet Explorer (bulletin MS15-032). Neuf d'entre elles permettent d'exécuter du code arbitraire à distance et huit sont exploitables sur la dernière version du navigateur.

Deux corruptions mémoire, identifiées par les vulnérabilités CVE-2015-1652 et CVE-2015-1666, permettent une exécution de code arbitraire sur toutes les versions d'Internet Explorer de la version 6 à la version 11.

Toutes les versions sont aussi concernées par une vulnérabilité autorisant le contournement de la disposition stochastique de l'espace d'adressage.

Microsoft Office

Le bulletin MS15-033 fait état de cinq vulnérabilités. Quatre d'entres-elles permettent l'exécution de code arbitraire à distance dans le contexte de l'utilisateur actif. Cela concerne plusieurs versions de Microsoft Office, de la version 2007 à la version 2013, et permet une élévation de privilèges grâce à Microsoft Office pour Mac 2011.

A noter que certaines de ces exécutions de code arbitraire à distance concernent aussi la visionneuse Microsoft Word, le pack de compatibilité de Microsoft Office Service Pack 3, les serveurs SharePoint 2010 et 2013, ainsi que Microsoft Office Web Apps dans ses versions 2010 Service Pack 2 et 2013 Service Pack 1.

La vulnérabilité de type corruption mémoire, identifiée CVE-2015-1641, a déjà été observée dans le cadre d'attaques.

Pilote HTTP.sys

La vulnérabilité CVE-2015-1635 mentionnée dans le bulletin MS15-034 touche le service HTTP.sys, notamment utilisé par le serveur web Microsoft IIS.

Ce service souffre d'un mauvais traitement de l'entête HTTP "Range" qui est normalement utilisé par les clients ne souhaitant télécharger qu'une partie d'une ressource mise à disposition par le serveur.

La vulnérabilité est décrite comme une exécution de code arbitraire à distance. Elle permet aussi un déni de service à distance ainsi qu'une potentielle atteinte à la confidentialité des données. Les commandes permettant de causer le déni de service à distance sont très largement diffusées et leur utilisation a déjà été observée sur Internet. Après l'exploitation du déni de service et avant le redémarrage du serveur, il semblerait qu'une partie du contenu de la mémoire du noyau soit incluse à la réponse HTTP.

D'autres services que Microsoft IIS peuvent utiliser le pilote HTTP.sys : il est possible de les lister en faisant afficher une capture instantanée de l'état du service HTTP grâce à la commande `netsh http show servicestate`.

Moteur de rendu graphique de Windows

Le moteur de rendu graphique fait l'objet d'un correctif concernant le traitement des images au format Enhanced Metafile (EMF) qui peut être utilisé pour exécuter du code arbitraire grâce à un fichier volontairement malformé.

Bien que les codes d'exploitation de cette vulnérabilité existant ne soient pas encore publics, le fait que de nombreuses applications clientes, d'Internet Explorer à MS Paint, puissent servir de vecteur à l'exécution de code arbitraire, doit encourager à rapidement appliquer ce correctif.

Le CERT-FR rappelle l'importance de ces correctifs de sécurité et recommande de les appliquer dès que possible.

Documentation

- https://technet.microsoft.com/library/security/MS15-032
- https://technet.microsoft.com/library/security/MS15-033
- https://technet.microsoft.com/library/security/MS15-034
- https://technet.microsoft.com/library/security/MS15-035
- https://technet.microsoft.com/library/security/MS15-036
- https://technet.microsoft.com/library/security/MS15-037
- https://technet.microsoft.com/library/security/MS15-038
- https://technet.microsoft.com/library/security/MS15-039
- https://technet.microsoft.com/library/security/MS15-040
- https://technet.microsoft.com/library/security/MS15-041

3 - Rappel des avis émis

Dans la période du 13 au 19 avril 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-146 : Multiples vulnérabilités dans les produits Juniper
- CERTFR-2015-AVI-147 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2015-AVI-148 : Multiples vulnérabilités dans les produits Cisco

- CERTFR-2015-AVI-149 : Multiples vulnérabilités dans les produits Huawei
- CERTFR-2015-AVI-150 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2015-AVI-151 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2015-AVI-152 : Vulnérabilité dans Microsoft Windows
- CERTFR-2015-AVI-153 : Multiples vulnérabilités dans le moteur de rendu graphique de Microsoft
- CERTFR-2015-AVI-154 : Multiples vulnérabilités dans Microsoft SharePoint Server
- CERTFR-2015-AVI-155 : Vulnérabilité dans le gestionnnaire des tâches de Microsoft Windows
- CERTFR-2015-AVI-156 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2015-AVI-157 : Vulnérabilité dans Microsoft XML Core Services
- CERTFR-2015-AVI-158 : Vulnérabilité dans Microsoft Active Directory Federation Services
- CERTFR-2015-AVI-159 : Vulnérabilité dans Microsoft .NET
- CERTFR-2015-AVI-160 : Vulnérabilité dans Microsoft Windows Hyper-V
- CERTFR-2015-AVI-161 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2015-AVI-162 : Multiples vulnérabilités dans les produits F5
- CERTFR-2015-AVI-163 : Vulnérabilité dans Red Hat JBoss
- CERTFR-2015-AVI-164 : Multiples vulnérabilités dans le noyau Linux de Red-Hat
- CERTFR-2015-AVI-165 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2015-AVI-166 : Multiples vulnérabilités dans les produits Adobe
- CERTFR-2015-AVI-167 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2015-AVI-168 : Vulnérabilité dans BlueCoat ProxySG
- CERTFR-2015-AVI-169 : Multiples vulnérabilités dans Oracle Solaris
- CERTFR-2015-AVI-170 : Multiples vulnérabilités dans Oracle Database Server
- CERTFR-2015-AVI-171 : Multiples vulnérabilités dans Oracle PeopleSoft
- CERTFR-2015-AVI-172 : Multiples vulnérabilités dans Oracle Java
- CERTFR-2015-AVI-173 : Multiples vulnérabilités dans Oracle MySQL
- CERTFR-2015-AVI-174 : Multiples vulnérabilités dans les produits Oracle Sun Systems
- CERTFR-2015-AVI-175 : Vulnérabilité dans Cisco IOS XR
- CERTFR-2015-AVI-176 : Vulnérabilité dans Cisco Secure Desktop
- CERTFR-2015-AVI-177 : Multiples vulnérabilités dans IBM AIX et Virtual I/O Server
- CERTFR-2015-AVI-178 : Vulnérabilité dans ProFTPD
- CERTFR-2015-AVI-179 : Vulnérabilité dans Asterisk
- CERTFR-2015-AVI-180 : Vulnérabilité dans GnuTLS
- CERTFR-2015-AVI-181 : Multiples vulnérabilités dans BlueCoat Malware Analysis Appliance (MAA)
- CERTFR-2015-AVI-182 : Vulnérabilité dans IBM InfoSphere BigInsights
- CERTFR-2015-AVI-183 : Vulnérabilité dans IBM Domino
- CERTFR-2015-AVI-184 : Vulnérabilité dans IBM Security Privileged Identity Manager Virtual Appliance
- CERTFR-2015-AVI-185 : Multiples vulnérabilités dans IBM Security Network Intrusion Prevention System

Gestion détaillée du document

20 avril 2015 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-016`