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 12 mai 2017
N° CERTFR-2017-ALE-010

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Propagation d'un rançongiciel exploitant les vulnérabilités MS17-010

Gestion du document

Référence	CERTFR-2017-ALE-010
Titre	Propagation d'un rançongiciel exploitant les vulnérabilités MS17-010
Date de la première version	12 mai 2017
Date de la dernière version	19 mai 2017
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 - Risque(s)

Installation et propagation d'un logiciel malveillant de type rançongiciel, voire, à terme, d'autres logiciels malveillants.

2 - Vecteurs d'infection

Le vecteur d'infection initial pourrait être un courriel avec une pièce jointe malveillante.

Le programme malveillant ensuite exécuté peut être vu comme constitué de deux parties :

- un composant chargé de la propagation via le réseau en exploitant une vulnérabilité SMB ;
- un rançongiciel.

3 - Systèmes affectés

Sont affectés :

- les sytèmes d'exploitation Windows vulnérables et en réseau maintenus par l'éditeur sur lesquels le correctif MS17-010 n'aurait pas été installé ;
- les sytèmes d'exploitation Windows vulnérables obsolètes et en réseau (Windows XP, Windows Server 2003, Windows 8, Windows Vista, Windows Server 2008, WES09 et POSReady 2009) sur lesquels le correctif KB4012598 n'aurait pas été installé ;
- tous les sytèmes d'exploitation Windows sur lesquels un utilisateur ouvrirait la pièce jointe malveillante.

4 - Résumé

Le CERT-FR constate l'apparition d'un nouveau rançongiciel qui exploite des vulnérabilités d'exécution de code à distance pour se propager. Ces vulnérabilités sont celles décrites dans le bulletin de sécurité MS17-010 (cf. CERTFR-2017-AVI-082, section Documentation).

L'attention est attirée sur le fait que :

- plusieurs variantes du rançongiciel ont pu être distribuées ;
- le composant rançongiciel a pu être remplacé dans certains cas par un composant moins visible.

5 - Contournement provisoire

Recommandations

Le CERT-FR recommande :

- l'application immédiate des mises à jour de sécurité permettant de corriger les failles exploitées pour la propagation (MS17-010 pour les systèmes maintenus par l'éditeur) ;
- le respect des recommandations génériques relatives aux rançongiciels ;
- de limiter l'exposition du service SMB, en particulier sur internet.

Un correctif de l'éditeur est aussi disponible pour les systèmes obsolètes suivants :

- Windows XP SP2 pour processeurs x64 ;
- Windows Server 2003 ;
- Windows XP SP3 pour XPe ;
- Windows XP SP3 ;
- Windows Vista ;
- Windows Server 2008 ;
- WES09 et POSReady 2009 ;

Il peut être téléchargé depuis `https://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598`.

Prévention

De manière préventive, s'il n'est pas possible de mettre à jour un serveur, il est recommandé de l'isoler logiquement, voire de l'éteindre le temps d'appliquer les mesures adaptées de protection.

La désactivation du protocole SMBv1 peut être un plus mais ne saurait remplacer l'installation des correctifs.

Récupération des données chiffrées par WannaCrypt

En cas d'infection par la version actuelle du rançongiciel WannaCrypt sous Windows XP, Windows 2003 et Windows 7 dans ses versions x86, une tentative de déchiffrement de vos données peut être effectuée à l'aide des outils WanaKiwi, ou bien WannaKey accompagné de Wanafork. Ces outils sont disponibles en source ouverte depuis `https://github.com/gentilkiwi/wanakiwi/releases`, `https://github.com/aguinet/wannakey` et `https://github.com/odzhan/wanafork/`.

Cette opération n'est pas garantie de fonctionner mais n'altérera aucun fichier en cas d'échec. Afin d'améliorer les chances de réussite de ces outils, le CERT-FR recommande de suivre les procédures suivantes :

- Le système ne doit pas avoir été redémarré après l'infection, auquel cas les outils cités ci-dessus ne fonctionneront pas;
- Il est déconseillé de manipuler le système après infection, mis à part pour lancer les outils de récupération des données chiffrées.

En cas de réussite, les fichiers chiffrés (.WNCRY) sont gardés intacts et les données déchiffrés sont enregistrées dans des fichiers séparés.

6 - Mesures réactives

Si le code malveillant est découvert sur vos systèmes, le CERT-FR recommande de déconnecter immédiatement du réseau les machines identifiées comme compromises. L'objectif est de bloquer la poursuite du chiffrement et la destruction des documents partagés.

Le CERT-FR recommande aussi d'alerter le responsable sécurité ou le service informatique au plus tôt.

Aussi, le CERT-FR recommande de prendre le temps de sauvegarder les fichiers importants sur des supports de données isolés. Ces fichiers peuvent être altérés ou encore être infectés. Il convient donc de les traiter comme tels. De plus, les sauvegardes antérieures doivent être préservées d'écrasement par des sauvegardes plus récentes.

Le bulletin d'actualité CERTFR-2015-ACT-004 précise de manière plus complète les mesures à appliquer (cf. section Documentation).

7 - Documentation

Concernant le rançongiciel WannaCrypt et les correctifs

- https://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
- https://technet.microsoft.com/fr-fr/library/security/MS17-010
- https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt
- https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targe
- http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-082/index.html
- https://github.com/gentilkiwi/wanakiwi/releases
- https://github.com/aguinet/wannakey
- https://github.com/odzhan/wanafork/

Désactivation de SMBv1

- http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ACT-019/index.html
- https://aka.ms/disablesmb1

Autres

- http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-004/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ACT-016/index.html

Gestion détaillée du document

12 mai 2017 version initiale ;

13 mai 2017 mise à jour ;

19 mai 2017 ajout de la sous-section "Récupération des données chiffrées par WannaCrypt".