Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

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

Paris, le 27 juin 2017
N° CERTFR-2017-ALE-012

Affaire suivie par: CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet: Campagne de maliciels prenant l'apparence d'un rançongiciel à multiples capacités de propagation

Gestion du document

Référence	CERTFR-2017-ALE-012
Titre	Campagne de maliciels prenant l'apparence d'un rançongiciel à multiples capacités de propagation
Date de la première version	27 juin 2017
Date de la dernière version	03 août 2017
Source(s)	-
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

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

Risque(s)

Installation et propagation d'un logiciel malveillant prenant l'apparence d'un rançongiciel, voire, à terme, d'autres logiciels malveillants.

Vecteurs du0027infection

L'ANSSI ne dispose pas à cette heure de preuves relatives au vecteur initial d'infection. L'usage envisagé de la vulnérabilité CVE-2017-0199 semble désormais exclu. Microsoft

indique que le logiciel de paiement de taxe MEDoc pourrait être l'un des vecteurs initiaux d'infection via une mise à jour automatique.

Lorsque le maliciel s'exécute, celui-ci commence par s'attribuer autant de droits que son niveau de privilèges lui permet. Il vérifie ensuite si certains logiciels anti-virus sont présents. S'il possède le privilège `SeDebugPrivilege`, il cherche la présence d'un fichier avant de continuer son exécution. Dans ce cas, celui-ci fait office de ce que l'on appelle communément un killswitch. Le nom de ce fichier est déterminé à partir du nom de l'exécutable malveillant pour lequel l'extension a été retirée. Sur les souches identifiées actuellement, le nom constaté du binaire est C:\Windows\perfc.dat. Par conséquent le fichier vérifié avant exécution est C:\Windows\perfc. Sur ces souches, la présence de ce fichier arrêtera l'exécution du maliciel avant toute action destructrice.

Si ce fichier n'est pas présent, le maliciel va alors modifier le `Master Boot Record` (MBR) afin d'effectuer des actions destructrices au prochain démarrage de la machine. S'il rencontre une erreur lors de cette opération, alors les dix premiers secteurs du disques seront réécrits avec des zéros pour empêcher la machine de démarrer. Ceci est par exemple le cas si le disque a une table de partition GPT (`GUID Partition Table`) au lieu de MBR. L'effet généralement constaté est un écran noir à la place du message de rançon. Dans ce cas, le système est récupérable à condition de reconstruire la table de partition.

Ensuite, il tente de créer une tâche planifiée réalisant un redémarrage de la machine.

Le maliciel va alors commencer à énumérer les équipements présents sur le réseau interne afin de se propager.

Des droits élevés permettent au maliciel de voler les mots de passe locaux soit en utilisant un outil de type Mimikatz en version 32 ou 64 bits, et en faisant appel à l'API CredEnumerateW. Le logiciel malveillant dispose de plusieurs capacités pour se propager sur le réseau :

- en utilisant les identifiants récupérés sur la machine ainsi que l'outil légitime d'administration `PSExec` et du protocole `WMI` ;
- en exploitant des vulnérabilités du protocole SMB (identifiées dans le bulletin MS17-010).

Après avoir tenté de se propager, le maliciel chiffre les fichiers locaux de l'utilisateur en les ciblant en fonction de leur extension. Cette étape est assez longue et dépend du volume de données présentes sur le disque. Une fois le chiffrement terminé, le logiciel malveillant cherche à redémarrer la machine. En fonction des versions de Windows, cela se fera soit par le déclenchement de la tâche planifiée, soit en provoquant une erreur qui débouchera sur un écran bleu dit "de la mort".

Selon le résultat des actions précédentes, la machine :

- redémarrera normalement mais les fichiers seront inaccessibles ;
- ne redémarrera pas ;
- redémarrera avec un message affiché indiquant qu'une vérification de l'intégrité des disques est en cours.

Dans ce dernier cas, le maliciel chiffre la MFT (Master File Table). Il s'agit d'un index des fichiers et répertoires présents sur le disque. Cela a pour conséquence de rendre inaccessibles les fichiers présents sur la machine. Enfin, le maliciel s'installe à la place du secteur de démarrage de Windows afin d'afficher le message de rançon. La clé utilisée pour chiffrer la MFT étant détruite dans le processus, il est impossible d'obtenir son déchiffrement même en échange du

paiement de la rançon.

Résumé des actions du maliciel

Les différentes actions entreprisent par le maliciel sont conditionnés par plusieurs vérifications au cours de son éxecution. Le tableau ci-après synthétise les événements en fonction du contexte d'éxecution du logiciel malveillant, notamment les privilèges dont dispose le processus, le type de secteur d'amorçage ou la présence de logiciel antivirus.

Tableau 2: Résumé des actions du maliciel suivant ses privilèges, le type de secteur d'amorçage, ou la présence de logiciel antivirus

Action	SeDebug	SeTcb	SeShutdown	MBR	GPT	Kaspersky	Symantec/Norton	Commentaires
Vérification du marqueur d'infection (MBR déjà infecté)	requis							Nom du fichier depuis lequel s'exécute le code placé dans le dossier C:\Windows\. Il est souvent observé le fichier C:\Windows\perfc
Infection du MBR	requis			requis		Si Absent		
Ecrasement des dix premiers secteurs du disque dur	requis					Si Présent		Seulement dans le cas ou l'infection du MBR échoue
Planifiifation du redémarrage								Réussite selon le retour de la commande, qui elle-même dépend de la version de Windows
Reconnaissance réseau								
Exécution du dérobeur de mot de passe de type Mimikatz déposé dans le répertoire %TEMP%	requis							
Extraction de PsExec dans le répertoire %WINDIR%	Un des deux	Un des deux						
Extraction de PsExec dans le répertoire %APPDATA%	Absent	Absent						
Création d'un fil d'exécution d'envoi de commandes WMIC								
Élévation locale de privilèges (technique identique que le mouvement latéral)	Si absent et sous conditions							Si le système d'exploitation est parmi : Windows versions 5.1, 5.2 -Windows XP et Windows Server 2003-, 6.0 (Vista, Windows Server 2008), ou 6.1 (Windows 7, Windows Server 2008 R2)
Exploitation des vulnérabilités EternalRomance/EternalBlue							Si absent	
Chiffrement des fichiers sur le disque local								
Ecran bleu ``de la mort'' / Redémarrage forcé			requis					
Effacement des événements windows (wevutil) et journal USN (fsutil)	Si présent ou sous conditions							Si le système est de type Windows 8 et postérieures ou si l'élévation locale de privilèges a réussie; Réussite de la commande selon le retour du processus lancé

Systèmes affectés

Toutes les versions de Windows semblent pouvoir être affectées dans la mesure où des outils d'administration classiques sont utilisés pour la latéralisation. Les serveurs ainsi que les postes

de travail font donc partie du périmètre d'infection possible.

Résumé

Le CERT-FR constate une recrudescence d'activité de maliciel prenant l'apparence d'un rançongiciel possédant une forte capacité de réplication. En particulier, plusieurs échantillons possèdent la capacité de se propager en utilisant aussi bien des codes d'exploitation du protocole SMB que des identifiants légitimes volés sur la machine compromise (à l'aide de `PSExec` et du protocole `WMI`).

Cette capacité de propagation multiple rend potentiellement vulnérables certains réseaux qui, malgré l'application de mises à jour, ne restreignent pas la latéralisation et l'abus d'identifiants.

Solution

Recommandations

Pour empêcher la propagation du maliciel, même en cas d'infection initiale, le CERT-FR recommande d'effectuer les actions suivantes :

- Mettre le processus lsass.exe en PPL (protected process light) sur l'ensemble des postes de travail, des serveurs membres et des contrôleurs de domaine, mesure déployable par GPO via un modèle d'administration récupérable sur le site Web de Microsoft. Cette action rend plus difficile la récupération des empreintes en mémoire et n'est réellement efficace que depuis Windows 8.1 et 2012 R2 ;
- Activer credential guard sur l'ensemble des postes de travail et des serveurs membres, ce qui rend impossible la récupération des empreintes en mémoire, sur Windows 10 et 2016 ;
- Mettre les utilisateurs les plus privilégiés de l'AD dans le groupe protected users ce qui nécessite une extension de schéma AD en 2012 R2. Cette mesure empêche le stockage des empreintes des mots de passe en mémoire, y compris sur les postes Windows 7 s'ils sont à jour (ayant notamment le correctif KB2871997 appliqué) ;
- Ajouter le SID des utilisateurs locaux (S-1-5-114) dans le droit d'authentification interdire l'accès à cet ordinateur par le réseau. Cette mesure peut être déployée par GPO et empêche la réutilisation des mots de passe identiques des comptes locaux ;
- Activer le contrôle de comptes utilisateur (UAC) pour le compte administrateur intégré (par GPO) sur les serveurs et les postes de travail ;
- S'assurer que les utilisateurs n'aient pas de privilèges sur les postes de travail ou activer le contrôle de comptes utilisateur (UAC) en mode Demande de consentement sur le bureau sécurisé.

De manière plus générale, le CERT-FR recommande :

- l'application immédiate des mises à jour de sécurité notamment la mise à jour de sécurité Microsoft MS17-010 (cf. section Documentation) ;
- le respect des recommandations génériques relatives aux rançongiciels : http://www.cert.ssi.gouv.fr/site/CERTFR-2017-INF-001/index.html ;
- de limiter l'exposition du service SMB, en particulier sur internet ;
- respecter le principe de moindre privilège pour les utilisateurs, afin de limiter l'élévation de privilèges et la propagation latérale de l'attaquant ;
- de ne pas payer la rançon.

Prévention

De manière préventive, s'il n'est pas possible de mettre à jour une machine, 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.

Détection

Les règles Yara suivantes sont fournies afin de permettre la détection d'un logiciel malveillant relatif à la campagne en cours.

```
rule MS17_010_RANSOMWARE_perfc_xor_strings {
```

meta:
author = "ANSSI"
version = "1.0"
description = "Rule to detect MS17_010 ransomware"

strings:
// PC NETWORK PROGRAM 1.0 xor 0x72
$a = {70 22 31 52 3C 37 26 25 3D 20 39 52 22 20 3D 35 20 33 3F 52 43 5C 42
72 70 3E 33 3C 3F 33 3C 43 5C 42 72 70 25 1B 1C 16 1D 05 01 52 14}

// \\123.12.31.2\IPC$ xor 0x75
$b = {75 29 75 29 75 44 75 47 75 46 75 5B 75 44 75 47 75 5B 75 46 75 44 75
5B 75 47 75 29 75 3C 75 25 75 36 75 51 75 75 75 4A 4A 4A 4A 4A 75}

// payload1 shellcode entrypoint xor 0x64
$c = {2C ED 84 02 E7 80 94 25 33 25 32 25 31 25 30 37 35 36 31 33 32 34 34
8C D8 62 64 64 2C ED}

condition:
1 of them
}

```
rule MS17_010_RANSOMWARE_Kaspersky_PetrWrap {
 meta:
 copyright = "Kaspersky Lab"
 description = "Rule to detect PetrWrap ransomware samples"
 last_modified = "2017-06-27"
 author = "Kaspersky Lab"
 hash = "71B6A493388E7D0B40C83CE903BC6B04" version = "1.0"
```

strings:
$a1 =
"MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXE
jfO2n2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2Dt
X4GRKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITD
bDDmdrRIiUEUw6o3pt5pNOskfOJbMan2TZu" fullword
wide
$a2 = ".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.
djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.

php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.
vmdk.vmsd.vmx.vsdx.vsv.work.xls" fullword wide
$a3 = "DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER
CABLE IS PLUGGED"
fullword ascii
$a4 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" fullword ascii
$a5 = "wowsmith123456@posteo.net." fullword wide

condition:
uint16(0) == 0x5A4D and
filesize < 1000000 and any of them
}

```
rule MS17_010_RANSOMWARE_FireEye_perfc_clear_strings {
meta:version="1.1"
 //filetype="PE"
 author="Ian.Ahl@fireeye.com @TekDefense, Nicholas.Carr@mandiant.com
 @ItsReallyNick"
 date="2017-06-27"
 description="Probable PETYA ransomware using ETERNALBLUE, WMIC, PsExec"
strings:
 // DRIVE USAGE
 $dmap01 = "\\\\.\\PhysicalDrive" nocase ascii wide
 $dmap02 = "\\\\.\\PhysicalDrive0" nocase ascii wide
 $dmap03 = "\\\\.\\C:" nocase ascii wide
 $dmap04 = "TERMSRV" nocase ascii wide
 $dmap05 = "\\admin$" nocase ascii wide
 $dmap06 = "GetLogicalDrives" nocase ascii wide $dmap07 = "GetDriveTypeW" nocase ascii wide
```

// RANSOMNOTE
$msg01 = "WARNING: DO NOT TURN OFF YOUR PC!" nocase ascii wide
$msg02 = "IF YOU ABORT THIS PROCESS" nocase ascii wide
$msg03 = "DESTROY ALL OF YOUR DATA!" nocase ascii wide
$msg04 = "PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED" nocase ascii
wide
$msg05 = "your important files are encrypted" ascii wide
$msg06 = "Your personal installation key" nocase ascii wide
$msg07 = "worth of Bitcoin to following address" nocase ascii wide
$msg08 = "CHKDSK is repairing sector" nocase ascii wide
$msg09 = "Repairing file system on " nocase ascii wide
$msg10 = "Bitcoin wallet ID" nocase ascii wide
$msg11 = "wowsmith123456@posteo.net" nocase ascii wide
$msg12 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" nocase ascii wide
$msg_pcre = /(en|de)crypt(ion|ed\.)/

// FUNCTIONALITY, APIS
$functions01 = "need dictionary" nocase ascii wide
$functions02 = "comspec" nocase ascii wide
$functions03 = "OpenProcessToken" nocase ascii wide
$functions04 = "CloseHandle" nocase ascii wide
$functions05 = "EnterCriticalSection" nocase ascii wide
$functions06 = "ExitProcess" nocase ascii wide
$functions07 = "GetCurrentProcess" nocase ascii wide
$functions08 = "GetProcAddress" nocase ascii wide
$functions09 = "LeaveCriticalSection" nocase ascii wide
$functions10 = "MultiByteToWideChar" nocase ascii wide
$functions11 = "WideCharToMultiByte" nocase ascii wide
$functions12 = "WriteFile" nocase ascii wide
$functions13 = "CoTaskMemFree" nocase ascii wide

$functions14 = "NamedPipe" nocase ascii wide
$functions15 = "Sleep" nocase ascii wide // imported, not in strings

// COMMANDS
// -- Clearing event logs & USNJrnl
$cmd01 = "wevtutil cl Setup" ascii wide nocase
$cmd02 = "wevtutil cl System" ascii wide nocase
$cmd03 = "wevtutil cl Security" ascii wide nocase
$cmd04 = "wevtutil cl Application" ascii wide nocase
$cmd05 = "fsutil usn deletejournal" ascii wide nocase
// -- Scheduled task
$cmd06 = "schtasks " nocase ascii wide
$cmd07 = "/Create /SC " nocase ascii wide
$cmd08 = " /TN " nocase ascii wide
$cmd09 = "at %02d:%02d %ws" nocase ascii wide
$cmd10 = "shutdown.exe /r /f" nocase ascii wide
// -- Sysinternals/PsExec and WMIC
$cmd11 = "-accepteula -s" nocase ascii wide
$cmd12 = "wmic"
$cmd13 = "/node:" nocase ascii wide
$cmd14 = "process call create" nocase ascii wide

condition:
(uint16(0) == 0x5A4D)
and 3 of ($dmap*)
and 2 of ($msg*)
and 9 of ($functions*)
and 7 of ($cmd*)
}

Marqueurs

Les éléments suivants sont identifiés en source ouverte comme étant de possibles marqueurs de compromission.

```
71b6a493388e7d0b40c83ce903bc6b04
0df7179693755b810403a972f4466afb
42b2ff216d14c2c8387c8eabfb1ab7d0
e285b6ce047015943e685e6638bd837e
e595c02185d8e12be347915865270cca
3b7331b99da80dcb5a0f5c14d384b49c
3d451bcaa800833115abf90c0954ac3b
710bd936a07bd3b146bdb170c317438c
8a241cfcc23dc740e1fadc7f2df3965e
9ed3bdaeb95e1084db73f39414b4f2b9
a92f13f3a1b3b39833d3cc336301b713
af2379cc4d607a45ac44d62135fb7015
b968c302c6fd56bbf7da3cc72bb31fa6
d0a0e16f1f85db5dfac6969562923576
e068ee33b5e9cb317c1af7cecc1bacb5
f11998e3849632b67a45a7186523f682
0487382a4daf8eb9660f1c67e30f8b25
415fe69bf32634ca98fa07633f4118e1
```

L'ANSSI confirme que les empreintes md5 suivantes sont liées à la campagne en cours :

```
71b6a493388e7d0b40c83ce903bc6b04
0df7179693755b810403a972f4466afb
42b2ff216d14c2c8387c8eabfb1ab7d0
e285b6ce047015943e685e6638bd837e
```

Le domaine et l'adresse IP suivante sont associés au serveur de mise à jour du logiciel MeDoc

identifié comme ayant distribué une version du maliciel.

```
upd.me-doc.com.ua
92.60.184.55
```

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, sans toutefois les éteindre. 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.

Comme le maliciel récupère les mots de passe, il est donc nécessaire de changer les mots de passe des sauvegardes avant de les restaurer. Si cela n'est pas possible, on peut aussi changer le mot de passe après la réinstallation, mais impérativement avant de rebrancher la machine sur le réseau.

Documentation

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-2017-INF-001/index.html
- 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
- https://technet.microsoft.com/fr-fr/library/security/MS17-010
- https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

Gestion détaillée du document

le 27 juin 2017
version initiale ;
le 28 juin 2017 à 01h30
mise à jour ;
le 28 juin 2017 à 11h00
mise à jour des informations sur le vecteur initial d'infection, ajout de marqueurs, modification des éléments limitant la propagation ;
le 28 juin 2017 à 20h15
mise à jour, ajouts de recommandations ;
le 28 juin 2017 à 23h00
mise à jour, ajouts de la chronologie de l'infection, retraits des marqueurs réseau ;
le 29 juin 2017 à 19h00

mise à jour, modification des mesures réactives, correction d'erreurs, confirmation de la destruction de la clé servant à chiffrer la MFT.

le 30 juin 2017 à 17h00

mise à jour, ajout d'un tableau récapitulant les actions du maliciel, ajout de marqueurs.

le 04 juillet 2017

modifications mineures.

le 07 juillet 2017

clôture de l'alerte.

le 03 août 2017

correction du marqueur upd.me-doc.com.ua.
