WannaCry ou l'histoire d'un ver surmédiatisé

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 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*. Un retiendra en particulier l'attention, il s'agit d'*EternalBlue* qui permet d'exploiter les vulnérabilités SMB décrites ci-dessus.

Suite à ces révélations, de nombreux chercheurs en sécurité s'intéressent à cette divulgation et alertent sur le fait que cette vulnérabilité classée critique pourrait faire l'objet d'un portage en ver et deviendrait alors une menace importante à la sécurité de l'écosystème Windows.

WannaCry

Le 12 Mai, un nouveau logiciel malveillant est découvert, se nommant WannaCry et exploitant MS17-010.

Enregistrement de noms de domaines salutaires

Le 12, après s'être rendu compte de la vérification de disponibilité d'un domaine très inhabituel par le logiciel malveillant, MalwareTech, analyste de logiciels malveillants, a enregistré celui-ci et stoppé la première vague d'attaque. Puis, le lendemain, Matt Suiche a détecté une variante utilisant un autre nom de domaine et enregistré celui-ci aussi. Tous les deux ont contribués à la diminution du nombre d'infection, cependant cela ne fonctionne pas dans la plupart des environnements Entreprise où est souvent utilisé un serveur mandataire ou Proxy car le logiciel ne gérant pas cette exception, leurs enregistrements n'ont aucune incidence dans ce cas précis. De plus, certaines solutions de sécurité bloquaient, au début ces deux domaines par incompréhension.

II. WannaCry

Que fait-il ?

Le logiciel malveillant exploite une faille dans le protocole SMBv1 pour s'installer ensuite, il recherche les hôtes proches. S'il en trouve, il les infecte aussi. Une fois cette première étape effectuée, il va alors chiffrer des documents bien spécifiques et ensuite afficher à l'écran une demande de rançon.

Qui est-il ?

Sa classification en tant que logiciel malveillant ne fait aucun doute dans la communauté, cependant la catégorie d'affectation, elle, est débattue.

Il est constitué de deux phases, l'infection et le chiffrement de fichiers. Pour la première phase, il est alors considéré comme un ver car il n'a pas besoin de programme hôte pour se reproduire. Pour la seconde, il est considéré comme un logiciel de chantage ou rançongiciel.

Ce qui prime est pour moi, le côté ver informatique, le chiffrement des fichiers n'étant que la charge du ver informatique.

La rançon

Après le chiffrement de vos fichiers, il vous est demandé de vous acquitter du paiement d'une rançon d'un montant de 300$ (environ 267€) si vous payez dans les 3 jours. Passé cette échéance, le montant double pour 600$ (environ 535€). Cette rançon est exigée en Bitcoin, une monnaie numérique réputée anonyme. Un guide est disponible pour vous expliquer comment en acquérir et payer la rançon directement sur la fenêtre du logiciel malveillant.

Distribution du logiciel malveillant

Comme nous ne connaissons pas le patient 0, il nous est impossible de confirmer la méthode initiale de distribution. Cependant, pour le reste de l'infection, nous pouvons infirmer le fait d'une distribution par courriel, car la propagation de cette dernière n'est pas due à une campagne d'hameçonnage mais bien à la capacité du ver de se reproduire et d'infecter le réseau local et Internet.

Analyse du logiciel malveillant

Pour étayer mon propos, je me base sur les analyses faites par Amanda Rousseau, Matt Suiche, Zammis Clark et Didier Stevens, tous chercheurs en sécurité.

Description des étapes du logiciel malveillant :

Infection :

- Etablissement d'une connexion SMB
- Test de vulnérabilité MS17-010
- Préparation de la charge encodée en Base64
- Test de vulnérabilité *DoublePulsar*
- Exécution de la charge

Exécution du ver :

- Test de connexion à un domaine
  ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
  iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Il n'est absolument pas conseillé de bloquer ces deux domaines car si la connexion ne réussit pas, le logiciel continue de s'exécuter, autrement non et le logiciel s'interrompt.

Ce que certains ont décrié comme une faille est, pour moi, une mesure contre la forensique numérique afin de détecter l'exécution du logiciel malveillant dans un environnement de bac à sable.

- Installation d'un service nommé *mssecsvc2.0* s'affichant comme dans le Gestionnaire des tâches de Windows comme *Microsoft Security Center (2.0) Service*
- Chargement du binaire *tasksche.exe*, enregistrement dans C:\Windows\ et le déplace ensuite vers un sous-répertoire
  Séparation en deux opérations simultanées ensuite :

1. Recherche d'hôtes vulnérables à *EternalBlue*
   - Réseau local LAN
     - Récupération d'une liste de sous-réseau via *GetAdaptersInfo()*
     - Scan de tous les hôtes de la liste (10 hôtes maximum en même temps)
     - Si possibilité d'infection, exécution de la charge (si le temps excède 10 minutes, fin du thread d'infection)
   - Réseau Internet
     - Création de 128 threads
     - Scan d'adresses générées aléatoirement
     - Si le logiciel réussi à se connecter à une adresse IP sur le port 445 alors, un scan du réseau de cette dernière en /24 est alors effectué
     - Si possibilité d'infection, exécution de la charge (si le temps excède 60 minutes, fin du thread d'infection)
2. Le fichier Tasksche.exe qui est un dropper (tout petit fichier qui sert à télécharger un plus gros fichier.) va alors télécharger *XIA.zip*
   - Extraction du fichier XIA.zip avec le mot de passe *WNcry@2ol7*
   - Récupération du fichier *c.wnry* (fichier de configuration)
   - Extraction de la configuration du fichier c.wnry afin de connaître quels sites utiliser pour les communications (Liens TOR en .onion et le lien de téléchargement de Tor browser version 6.5.1 win32 setup)
   - Chargement des 3 adresses des porte-monnaie virtuels bitcoins
   - Cache du répertoire d'extraction du zip et des fichiers.
   - Modifications de la sécurité afin que chaque utilisateur puisse accéder à ce dossier.
   - Préparation de la crypto nécessaire au chiffrement
   - Création d'un mutex : *Global\\MsWinZonesCacheCounterMutex*

Il a été remarqué que s'il existe déjà, le chiffrement des fichiers n'est pas effectué. Cependant, il en existe plusieurs, voici la liste de ceux que j'ai vu passer :

- Global\\MsWinZonesCacheCounterMutexA0
- Global\\MsWinZonesCacheCounterMutexW
- Global\\MsWinZonesCacheCounterMutexA

- Communications sur Tor (probablement pour créer le périphérique et envoyer les clés de déchiffrement correspondantes)

- Création du fichier *@WanaDecryptor@.exe* et sa sauvegarde
- Création du fichier *@Please_Read_Me@.txt*
- Fin des tâches suivantes :
  - Microsoft.Exchange.*
  - MSExchange*
  - sqlserver.exe
  - sqlwriter.exe
  - mysqld.exe

Permet de pouvoir chiffrer les bases de données locales

- Vérification de l'espace libre sur le disque
- Début du chiffrement des fichiers
  - Chiffrement du fichier s'il possède une des extensions suivantes :

.doc,.docx,.docb,.docm,.dot,.dotm,.dotx,.xls,.xlsx,.xlsm,.xlsb,.xlw,.xlt,.xlm,.xlc,.xltx,.xltm,.ppt,.pptx,.pptm,.pot,.pps,.ppsm,.ppsx,.ppam,.potx,.potm,.pst,.ost,.msg,.eml,.edb,.vsd,.vsdx,.txt,.csv,.rtf,.123,.wks,.wk1,.pdf,.dwg,.onetoc2,.snt,.hwp,.602,.sxi,.sti,.sldx,.sldm,.sldm,.vdi,.vmdk,.vmx,.gpg,.aes,.ARC,.PAQ,.bz2,.tbk,.bak,.tar,.tgz,.gz,.7z,.rar,.zip,.backup,.iso,.vcd,.jpeg,.jpg,.bmp,.png,.gif,.raw,.cgm,.tif,.tiff,.nef,.psd,.ai,.svg,.djvu,.m4u,.m3u,.mid,.wma,.flv,.3g2,.mkv,.3gp,.mp4,.mov,.avi,.asf,.mpeg,.vob,.mpg,.wmv,.fla,.swf,.wav,.mp3,.sh,.class,.jar,.java,.rb,.asp,.php,.jsp,.brd,.sch,.dch,.dip,.pl,.vb,.vbs,.ps1,.bat,.cmd,.js,.asm,.h,.pas,.cpp,.c,.cs,.suo,.sln,.ldf,.mdf,.ibd,.myi,.myd,.frm,.odb,.dbf,.db,.mdb,.accdb,.sql,.sqlitedb,.sqlite3,.asc,.lay6,.lay,.mml,.sxm,.otg,.odg,.uop,.std,.sxd,.otp,.odp,.wb2,.slk,.dif,.stc,.sxc,.ots,.ods,.3dm,.max,.3ds,.uot,.stw,.sxw,.ott,.odt,.pem,.p12,.csr,.crt,.key,.pfx,.der

---

- Communications sur Tor
- Suppression des copies de volumes cachés

Entreprises et administrations touchées par l'attaque

Sans vouloir faire une liste exhaustive, voici un bout de liste des entreprises et des administrations ayant communiqué dessus :

- ✓ National Healthcare System (GB)
- ✓ NISSAN (GB)
- ✓ Telefonica (ES)
- ✓ Iberdrola and Gas Natural (ES)
- ✓ Portugal Telecom (PRT)
- ✓ FedEx (US)
- ✓ Ministère des affaires Etrangères Russe (RU)
- ✓ Deutsche Bahn (DE)
- ✓ Hitachi
- ✓ Groupe aéronautique LATAM
- ✓ PetroChina (CN)
- ✓ Q-Park

- ✓ Renault (!?)
- ✓ Les chemins de fer russes (RU)

Pour une liste plus complète :
https://en.wikipedia.org/wiki/WannaCry_cyber_attack#List_of_affected_organizations

Cependant, celle-ci ne sera jamais exhaustive car certaines entreprises ne déclarent pas cet incident pour ne pas causer d'atteinte d'image à leurs produits, marques ou services.

Correctifs et remédiation

Mise à jour

La plus simple consiste à faire la mise à jour MS17-010, disponible pour bon nombre de systèmes d'exploitation car Microsoft a rendu la mise à jour fonctionnelle même sur XP qui n'est, pour rappel, plus supporté actuellement.

Lien de téléchargement de la mise à jour :

http://www.catalog.update.microsoft.com/search.aspx?q=4012598

Cependant, pour plusieurs raisons qui sont évoquées plus bas, certains ne peuvent appliquer ces mises à jour pour diverses contraintes.

Mutex

Ajouter les mutex décrits plus hauts, cela stopperait l'exécution du logiciel malveillant

Restrictions

Restrictions du trafic sur le port 445 en TCP via les ACLs des routeurs

Utilisation des capacités des pare-feu sur les postes de travail pour limiter les communications entre les postes de travail.

Récupérer ses fichiers (avec de la chance)

Il existe un outil qui permet de récupérer ses fichiers sous de strictes conditions. Je ne l'ai pas testé personnellement mais j'ai lu plusieurs fois que cela fonctionnait.

Un post du blog de MalwaresBytes détaille le processus :

https://blog.malwarebytes.com/cybercrime/2017/05/wannadecrypt-your-files/

Désactiver SMBv1

Cf : https://technet.microsoft.com/en-us/library/security/ms17-010#Vulnerability%20Information

III. Médiatisation à outrance

Médias

L'attaque a été, du moins à mon sens, surmédiatisée. Pourquoi cette surmédiatisation ? Il y a eu une médiatisation suite à l'annonce du NHS, puis cela s'est enchaîné avec la consigne de Telefonica à destination de ses employés, d'éteindre tous les ordinateurs. Puis, réactions en chaîne suite à la mise à disposition de la carte en temps réel des infections par le chercheur en sécurité, MalwareTech. Suite à ça, une quantification des attaques était disponible et les médias s'en sont emparé. On a subi les éditions spéciales jusqu'au Journal de 20 Heures, les journalistes allant jusqu'à parler de cyberattaque mondiale sans précédent.

Une attaque pas si énorme

Sauf que, si on remet en perspective cette attaque avec le passé, celle-ci est insignifiante. Comme l'ont rappelé les intervenants des podcasts dédiés à la sécurité informatique que sont NoLimitSecu et ComptoirSecu, par le passé, des attaques informatiques ont déjà infecté bien plus de personnes que WannaCry. Prenons par exemple le ver *ILoveYou*, qui selon les estimations de l'époque, aurait infecté plus de 10 millions de périphériques, WannaCry fait pâle figure avec ses quelques 400 000 infectés.

Des entreprises peu scrupuleuses

Je ne compte plus le nombre de courriels que certains confrères et moi avons reçu où l'on nous explique que la solution miracle et boule de cristal X solutionne tout. Si on est un peu critique vis-à-vis de ces messages, envoyés le jour même voire pour certains dans l'heure du premier article de presse généraliste, de sociétés vendant des solutions ou prestations liées de près ou de loin à la sécurité, on s'aperçoit très vite que ces dernières n'ont pas réellement compris cette infection quand elles nous proposent de lutter avec des solutions filtrant les messages électroniques.

Une incompétence flagrante vraiment ?

Mais ce qui m'a le plus exaspéré, c'est les personnes qui traitaient tous les gens touchés comme des simplets responsables de leurs malheur. Si certains peuvent être effectivement responsables, d'autres sont contraints. Pour avoir travaillé dans des postes où justement je gérais les mises à jour et la sécurité, il peut y avoir des raisons pour lesquelles des mises à jour n'étaient pas installées au moment de l'attaque. Pour n'en citer que quelques exemples :

- Des professionnels dont le métier n'est pas la sécurité et qui se servent de l'informatique en tant qu'outil de travail, ne s'en soucient pas, tant que ça marche, on ne touche pas.
- Les entreprises ou administrations n'ayant pas forcément les effectifs nécessaires ou les moyens.
- Les professionnels ayant des machines-outils où le poste informatique est livré avec l'ordinateur où s'exécute une application métier très contraignante. Certains constructeurs utilisant le protocole SMBv1 pour de la transmission de flux entre machines spécifiques ou autres contraintes.
- Le temps de test des mises à jour. Certaines entreprises testent les correctifs avant de les déployer en masse car ceux-ci peuvent conduire à des interruptions de service suite à leur installation. Pour rappel, en 2016, un correctif distribué par Microsoft a généré des BSOD, engendrant des pertes de service problématiques.
- …

Attribution

Nous avons vu fleurir une attribution plus ou moins assumée par des fournisseurs de logiciels de sécurité cette semaine. Cette attribution est basée sur des analyses de similarités de code partagé entre *WannaCry* et *Contopee*, un logiciel malveillant qui serait relié au groupe *Lazarus*. Cependant, de ce que j'ai pu en lire, ces similarités sont infimes et pourrait plus laisser à supposer que des parties du code ont été reprises.

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.

IV. Conséquences

Générales

- Mises à jour en urgence sur des systèmes difficiles à mettre à jour en temps normal.
- Information de la population aux risques que présentent ce type de logiciels.
- Information et plus largement, responsabilisation des conseils d'administration des entreprises et des patrons aux problématiques de sécurité pouvant toucher la situation économique, l'image et les services de leur société.
- Distribution au plus grand nombre de cet exploit via la plateforme Metasploit. Cela va augmenter la simplicité de la mise en œuvre de l'attaque et donc augmenter leur nombre.
- Microsoft a distribué en « urgence » un correctif pour bon nombre de ses logiciels touchés, même ceux qui ne sont plus officiellement supportés. Si dans un premier temps cela paraît bienvenu, cela pourrait aussi devenir un argument contre la mise à jour des anciennes versions de Windows en arguant que « S'il y a un gros problème, Microsoft sortira un correctif en urgence, on est tranquille ».
- Le groupe *ShadowBrokers*, à l'origine de la divulgation compte continuer ses agissements et propose à partir du mois de Juin un abonnement à ce qui semble être une archive chaque mois de nouvelles failles.
- Pertes économiques et d'activités suite à l'attaque

Juridique

Le parquet de Paris a lancé une enquête de flagrance dès le vendredi 12 Mai 2017 pour "accès et maintien frauduleux dans des systèmes de traitement automatisé de données", "entraves au fonctionnement" et "extorsions et tentatives d'extorsions". Suite à ça, il apparaît que des nœuds Tor ont été saisis en relation avec cette attaque car ils auraient servi de relais pour les transmissions du logiciel malveillant. De plus, Interpol et Europol ont mobilisé des équipes de spécialistes pour lutter contre cette infection.

Microsoft et NSA

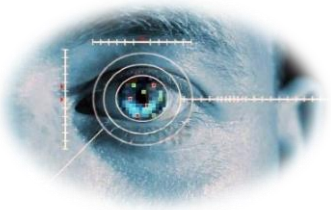
Cette attaque a relancé un débat qui n'avait jusqu'à présent pas trouvé écho dans la presse généraliste. Il concerne comment les agences de renseignements et entreprises privées peuvent garder les vulnérabilités critiques de type 0day en leur possession. En effet, cette faille aurait été volé par le groupe *ShadowBrokers* à une entité secrète de la NSA. Là où le bât blesse, c'est que si la NSA est incapable de garder en sécurité ses outils, c'est une mise en danger des réseaux et des systèmes si ces armes sont récupérées. Suite à cette attaque, Microsoft a relancé son idée de Convention de Genève 2.0 pour demander à ce que des failles critiques de ce type soient remontées aux constructeurs afin qu'ils puissent délivrer des correctifs pour celles-ci. Mais ne nous faisons pas trop d'illusions, ces vulnérabilités sont des armes bien trop précieuses pour ces agences, il y a que très peu de chance que cette initiative réussisse, cependant elle mérite d'être saluée.

V. Webographie

- https://technet.microsoft.com/en-us/library/security/ms17-010#Vulnerability%20Information
- https://support.microsoft.com/fr-fr/help/4013389/title
- http://www.catalog.update.microsoft.com/search.aspx?q=4012598
- https://steemit.com/shadowbrokers/@theshadowbrokers/oh-lordy-comey-wanna-cry-edition
- https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation
- https://github.com/x0rz/EQGRP_Lost_in_Translation
- https://medium.com/@shadowbrokerss
- https://en.wikipedia.org/wiki/WannaCry_cyber_attack#List_of_affected_organizations
- https://blog.comae.io/wannacry-the-largest-ransom-ware-infection-in-history-f37da8e30a58
- https://blog.comae.io/wannacry-new-variants-detected-b8908fefea7e
- https://blog.comae.io/wannacry-links-to-lazarus-group-dcea72c99d2d
- https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d
- https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/
- https://blog.malwarebytes.com/cybercrime/2017/05/wannadecrypt-your-files/
- https://blog.didierstevens.com/2017/05/14/quickpost-wannacrys-mutex-is-mswinzonescachecountermutexa0-digit-zero-at-the-end/
- https://blog.didierstevens.com/2017/05/13/quickpost-wcry-killswitch-check-is-not-proxy-aware/
- https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis
- https://baesystemsai.blogspot.fr/2017/05/wanacrypt0r-ransomworm.html
- https://www.countercept.com/our-thinking/analyzing-the-doublepulsar-kernel-dll-injection-technique/

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