STREAMSCAN

Cybersécurité pour les moyennes entreprises

ANALYSE DU RANSOMWARE WANNACRY

JUIN 2017 //

Introduction

WannaCryptor, aussi connu sous le nom de WannaCry, est un ransomware apparu le vendredi 12 mai 2017 et qui a instantanément fait la une internationale. Cette grande attention des médias est due aux ravages causés par ce ransomware (hôpitaux paralysés au Royaume-Uni, infections massives chez Fedex, Vodafone, Renault, etc.) ainsi que sa capacité de propagation rarement vue. En effet, plus de 200 000 ordinateurs repartis dans environ 150 pays ont été infectés entre le 12 et le 14 mai 2017.

WannaCry chiffre les fichiers ayant une certaine extension présente sur l'ordinateur infecté (liste non exhaustive) : .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pst, .ost, .msg, .eml, .vsd, .vsdx, .txt, .csv, .rtf, .pdf, etc.

Dans le présent document, nous faisons une analyse du comportement de WannaCry et validons la capacité de notre technologie de détection de brèches de sécurité CDS à le détecter.

Définitions

Pour comprendre la portée et le fonctionnement de WannaCry, il est nécessaire de se familiariser avec quelques définitions et concepts.

Ransomware

Un ransomware est un type de logiciel malicieux (malware) qui chiffre les données sur la machine infectée et demande une rançon pour effectuer le déchiffrement des données.

Ver informatique

Un ver informatique est un programme malveillant similaire à un virus informatique de par son effet malveillant (il cause généralement des dégâts au système qu'il infecte). La différence réside dans la méthode de propagation. Un ver informatique ne nécessite pas l'interaction de l'utilisateur pour se propager. Il utilise les ressources réseau présentes sur le système infecté afin de se propager. Ainsi, une machine infectée pourra en infecter une dizaine voire des centaines d'autres.

Malware zéro-day ou 0-day

Un malware **zéro-d**ay fait référence à un outil malicieux de nouvelles générations qui viennent juste d'apparaître. Les outils de sécurité classiques basés sur des signatures (antivirus, système de détection ou prévention d'intrusions, SIEM, etc.) ne sont pas capables de détecter ce type de cyber menace.

TOR

Protocole internet utilisé pour anonymiser les conversations ou communications sur Internet.

WannaCry = ransomware + ver informatique

La particularité de WannaCry réside dans le fait que c'est un ransomware qui utilise un ver pour se propager. Afin d'infecter de nouvelles cibles et se propager, WannaCry exploite une vulnérabilité critique qui touche le système d'exploitation Windows. Un correctif Microsoft est disponible depuis le 14 mars 2017, soit environ un (1) mois avant l'incident majeur causé par WannaCry (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx).

À titre d'information, la vulnérabilité exploitée par WannaCry concerne le protocole SMB (Server Message Block) et peut mener à l'exécution de code informatique à distance. La quasi-totalité des versions Windows non mises à jour de Windows XP à Windows 10 sont vulnérable.

Méthodologie d'analyse de WannaCry

Pour analyser WannaCry, nous avons mis en place un environnement de test confiné où un ordinateur Windows 7 a été infecté (IP = 192.168.0.186). Le trafic réseau généré par l'ordinateur infecté a été ensuite capturé pour des fins d'analyse.

Nous avons établi deux (2) configurations réseau pour notre analyse. Dans la première configuration, l'hôte infecté avait accès à l'Internet tandis que dans la deuxième l'hôte infecté n'avait aucun accès à Internet.

Deux (2) variantes du ransomware WannaCry ont été analysées : la première version apparue le 12 mai 2017 et une seconde version apparue quelques jours plus tard. L'analyse de la deuxième variante avait pour objectif de se faire une idée de son degré de variation par rapport à la version initiale (nouvelles fonctionnalités, etc.).

Variante 1 analysée (version WannaCry originale)

Nom du fichier : WannaCry.EXE

Hash HA256 : ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

Hash MD5: 84c82835a5d21bbcf75a61706d8ab549

Variante 2 analysée

Nom du fichier: mssecsvc.exe

Hash SHA256:24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

Hash MD5: db349b97c37d22f5ea1d1841e3c89eb4

Analyse de la version originale de WannaCry

Une fois infectée par la première version de WannaCry (version originale), l'hôte Windows 7 scanne le réseau local ainsi que des adresses IP (**générées aléatoirement**) à la recherche de systèmes vulnérables. Les scans se font sur le port **445** (celui associé au service SMB). Si la connexion réussit, WannaCry exécute l'exploit **EternalBlue** pour infecter la machine.

L'un des principaux comportements de la version WannaCry originale tient au fait qu'avant d'encrypter le disque dur de l'hôte infecté et scanner Internet à la recherche de systèmes vulnérables, elle envoie une requête DNS au nom de domaine suivant : **iffefrsodp9ifjaposdfjhgosurijfaewrwergwea.com**.

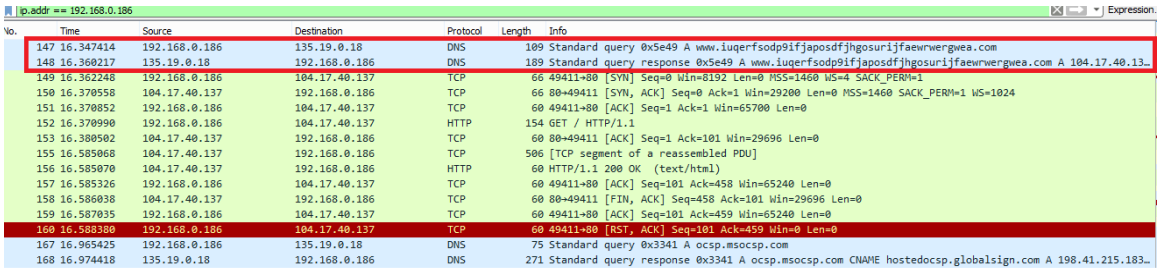


Figure 1. Requête DNS initiée vers le nom de domaine généré aléatoirement

Pour rappel, l'enregistrement de ce nom de domaine par Malwaretech, un chercheur anglais a heureusement permis de ralentir la propagation du ransomware. En effet, comme nous avons pu le constater lors de notre analyse, la version originale de WannaCry ne s'exécute pas si elle ne reçoit pas une réponse à sa requête DNS. Ce nom de domaine agit donc comme un « kill switch ». L'enregistrement du nom de domaine **iffefrsodp9ifjaposdfjhgosurijfaewrwergwea.com** a donc fortement limité l'impact que les créateurs de WannaCry avaient prévu.

Une autre particularité de la version originale de WannaCry est qu'elle installe un client TOR sur la machine infectée afin de communiquer avec des serveurs malicieux distants. De cette manière, toutes les communications (échanges de clés de chiffrement, messages...) sont cryptées.

Un mot sur le nom de domaine ifferfsodp9ifjaposdfjhgosurijfaewrwergwea

À vue d'œil, l'on constate que ce nom de domaine est généré aléatoirement (*random-generated domain*). Cependant, il n'a été généré aléatoirement qu'une seule fois et il est le même pour toutes les copies de la version 1 de WannaCry.

Pour information, l'utilisation de noms de domaines générés aléatoirement est une technique assez utilisée par plusieurs outils malveillants (notamment par des unités de commande et contrôle de malwares -aussi appelés C&C-). Cette méthode rend la traque des serveurs C&C difficile étant donné que le nombre de noms de domaines générés aléatoirement par certains outils malicieux peut atteindre 50.000 par jour (cas du malware Conficker) et qu'un ordinateur infecté peut à lui seul émettre des requêtes vers 500 domaines.

Note : en général, les requêtes vers un nom de domaine généré aléatoirement sont un indicateur de compromission ou de comportement douteux d'un ordinateur.

Ce qu'il faut retenir du comportement de la version originale de WannaCry lorsque le test est réalisé dans un environnement ayant accès à Internet

- Si la requête DNS vers le domaine www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com aboutit, l'exécution du ransomware se termine et le disque dur de l'hôte infecté n'est pas encrypté.
- Si la requête DNS n'aboutit pas, le disque dur est encrypté.

Ce qu'il faut retenir du comportement de la version originale de WannaCry lorsque le test est réalisé dans un environnement sans accès à Internet

- La requête DNS vers le domaine www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com échoue. WannaCry s'exécute et encrypte le disque dur de l'hôte infecté. Un écran similaire à celui-ci s'affiche sur l'écran de l'utilisateur :

Figure 2. Écran affiché après l'infection d'un hôte par WannaCry

- WannaCry tente ensuite de se connecter à des routeurs TOR, sans succès. Le ransomware poursuit en exécutant des milliers de scans sur des adresses extérieures vers le port 445, le port exploité par la vulnérabilité SMB afin de potentiellement trouver d'autres hôtes Windows vulnérables pour les infecter à leur tour (confère les multiples requêtes SYN initiée par l'hôte infectée dont l'adresse IP est 192.168.0.186).

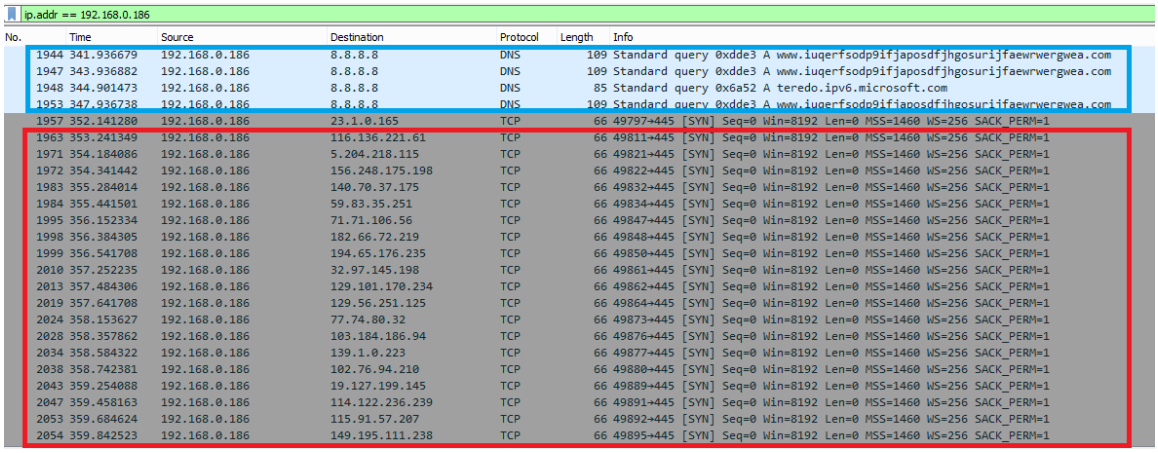


Figure 3. Scans générés par WannaCry pour des fins d'exploitation de la vulnérabilité SMB (port 445)

Capacité du CDS de StreamScan à détecter WannaCry

Détection de la version originale de WannaCry

En analysant les paquets réseau générés par la machine Windows 7 infectée par WannaCry, le module de détection comportemental du CDS de StreamScan a généré une alerte lorsque ladite machine a envoyé la requête DNS vers le domaine www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. Ce module du CDS utilise de l'intelligence artificielle et de l'apprentissage machine (Machine Learning) pour détecter les noms de domaines de ce genre.

Nous sommes donc en mesure de confirmer que le CDS de StreamScan était capable de détecter la première version de WannaCry au jour 0 de son expansion, c'est-à-dire le vendredi 12 mai 2017 (voir figure 4 ci-dessous). Le CDS offre la possibilité de consulter ou télécharger l'ensemble des paquets réseau qui ont permis de générer l'alerte, au format PCAP. Le fichier PCAP téléchargé pourrait être lu par des outils tels que Wireshark ou encore Tcpdump. Il est aussi possible de consulter le contenu des fichiers PCAP directement dans le Dashboard du CDS.

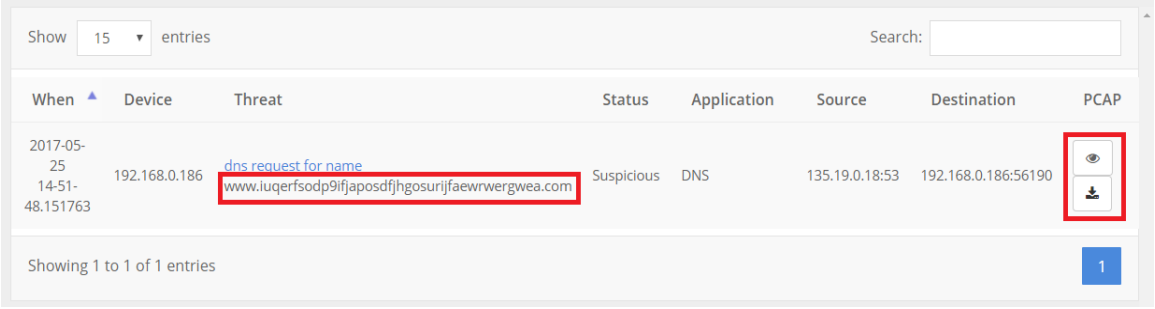


Figure 4. Détection de WannaCry par le CDS de StreamScan

Le module de détection par signatures du CDS a également détecté WannaCry, après mise à jour, suite à la disponibilité des signatures SNORT.

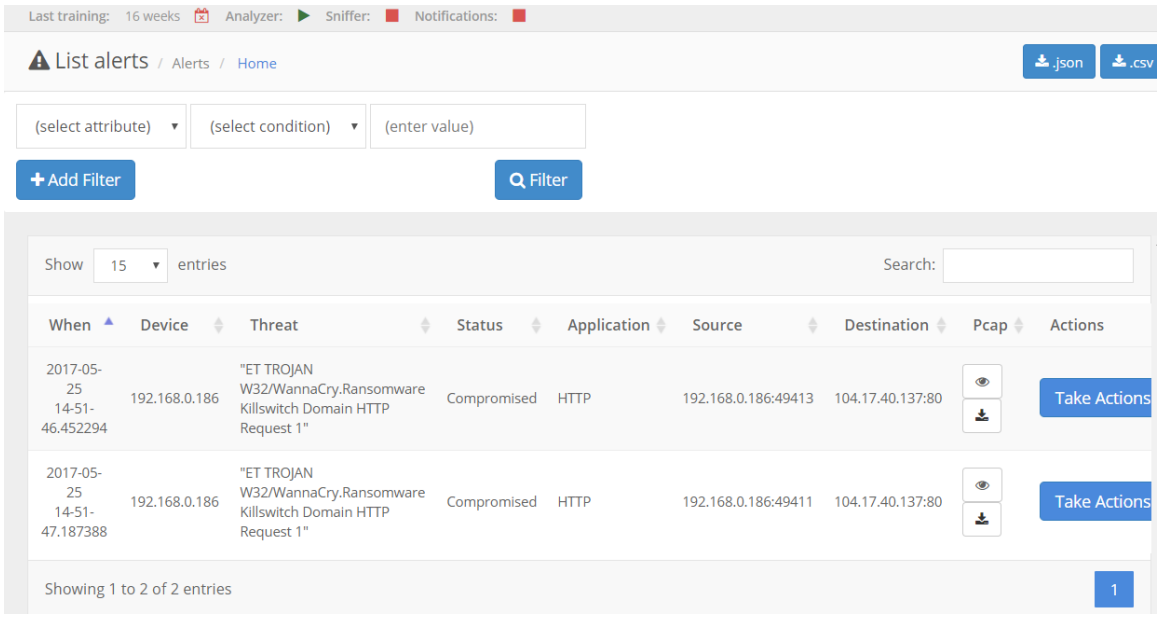


Figure 5. Alertes générées par le module de détection par signatures du CDS

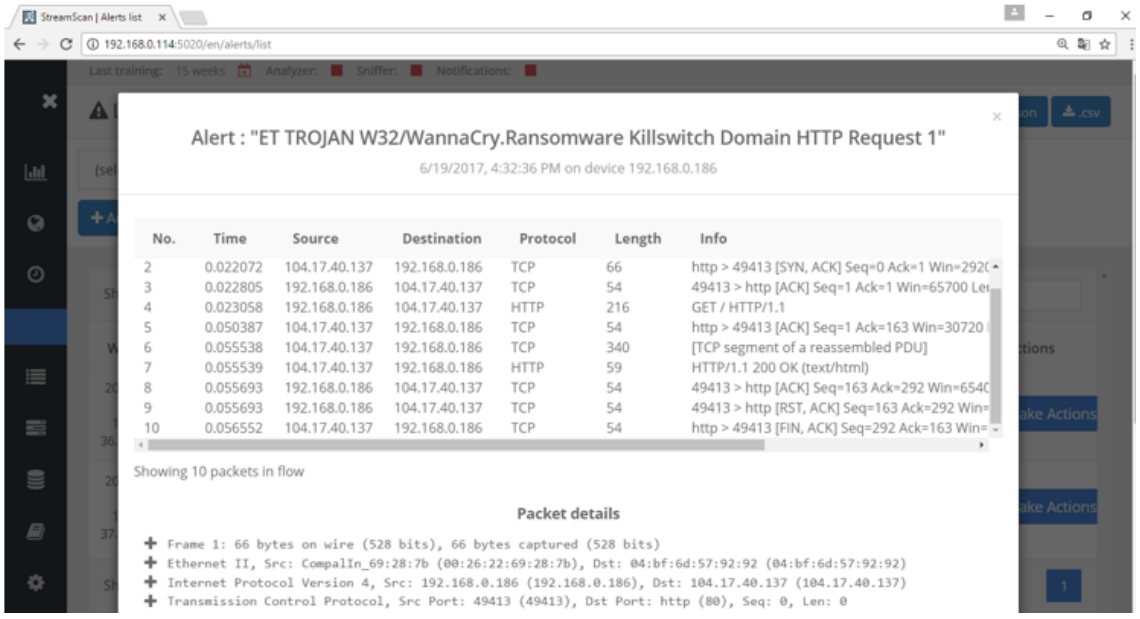


Figure 6. Visualisation des paquets réseau liés aux alertes directement dans son Dashboard du CDS. Il est également possible de les télécharger au format PCAP.

Détection de la version 2 de WannaCry

L'analyse de la deuxième version de WannaCry montre qu'elle ne dispose pas de « kill switch ». Cette variante a donc été repensée pour n'avoir aucune condition d'arrêt. Nous avons aussi constaté que cette version ne dispose pas de fonction « ver » ce qui explique le

fait qu'elle n'essaie pas de se propager en scannant d'autres ordinateurs afin d'exploiter la vulnérabilité SMB.

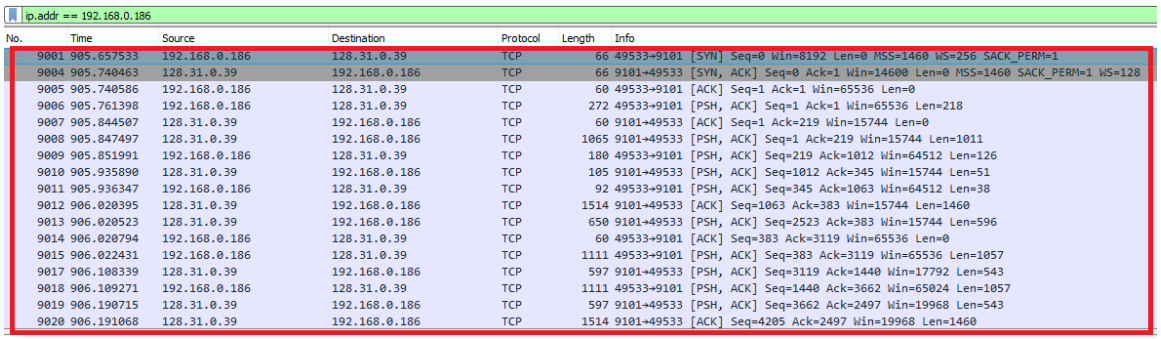
La particularité de cette version de WannaCry réside dans le fait qu'elle initie des requêtes en permanence vers des routeurs TOR. L'on remarque d'utilisation de noms de domaine générés aléatoirement dans les requêtes, tel que montré dans l'image ci-dessous.

Ce qu'il faut retenir du comportement de la version 2 de WannaCry lorsque le test est réalisé dans un environnement n'ayant pas accès à Internet

- WannaCry encrypte le disque de l'ordinateur et tente perpétuellement de se connecter à des routeurs TOR.

Ce qu'il faut retenir du comportement de la version 2 de WannaCry lorsque le test est réalisé dans un environnement ayant accès à Internet

- WannaCry encrypte le disque de l'ordinateur et se connecte à des routeurs TOR distants.


ip.addr == 192.168.0.186

No.	Time	Source	Destination	Protocol	Length	Info
9001	905.657533	192.168.0.186	128.31.0.39	TCP	66	49533→9101 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
9004	905.740463	128.31.0.39	192.168.0.186	TCP	66	9101→49533 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
9005	905.740586	192.168.0.186	128.31.0.39	TCP	60	49533→9101 [ACK] Seq=1 Ack=1 Win=65536 Len=0
9006	905.761398	192.168.0.186	128.31.0.39	TCP	272	49533→9101 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=218
9007	905.844507	128.31.0.39	192.168.0.186	TCP	60	9101→49533 [ACK] Seq=1 Ack=219 Win=15744 Len=0
9008	905.847497	128.31.0.39	192.168.0.186	TCP	1065	9101→49533 [PSH, ACK] Seq=1 Ack=219 Win=15744 Len=1011
9009	905.851991	192.168.0.186	128.31.0.39	TCP	180	49533→9101 [PSH, ACK] Seq=219 Ack=1012 Win=64512 Len=126
9010	905.935890	128.31.0.39	192.168.0.186	TCP	105	9101→49533 [PSH, ACK] Seq=1012 Ack=345 Win=15744 Len=51
9011	905.936347	192.168.0.186	128.31.0.39	TCP	92	49533→9101 [PSH, ACK] Seq=345 Ack=1063 Win=64512 Len=38
9012	906.020395	128.31.0.39	192.168.0.186	TCP	1514	9101→49533 [ACK] Seq=1063 Ack=383 Win=15744 Len=1460
9013	906.020523	128.31.0.39	192.168.0.186	TCP	650	9101→49533 [PSH, ACK] Seq=2523 Ack=383 Win=15744 Len=596
9014	906.020794	192.168.0.186	128.31.0.39	TCP	60	49533→9101 [ACK] Seq=383 Ack=3119 Win=65536 Len=0
9015	906.022431	192.168.0.186	128.31.0.39	TCP	1111	49533→9101 [PSH, ACK] Seq=383 Ack=3119 Win=65536 Len=1057
9017	906.108339	128.31.0.39	192.168.0.186	TCP	597	9101→49533 [PSH, ACK] Seq=3119 Ack=1440 Win=17792 Len=543
9018	906.109271	192.168.0.186	128.31.0.39	TCP	1111	49533→9101 [PSH, ACK] Seq=1440 Ack=3662 Win=65024 Len=1057
9019	906.190715	128.31.0.39	192.168.0.186	TCP	597	9101→49533 [PSH, ACK] Seq=3662 Ack=2497 Win=19968 Len=543
9020	906.191068	128.31.0.39	192.168.0.186	TCP	1514	9101→49533 [ACK] Seq=4205 Ack=2497 Win=19968 Len=1460

Figure 7. L'hôte infecté ù des connexions distantes avec des routeurs TOR.

Capacité du CDS de StreamScan à détecter la version 2 de WannaCry

Tout comme pour la première version de WannaCry, le CDS est en mesure de détecter la version 2, en s'appuyant toujours sur son module comportemental qui, en plus de détecter plusieurs autres comportements anormaux, est capable de détecter les noms de domaines générés aléatoirement (*en* analysant les requêtes TOR).

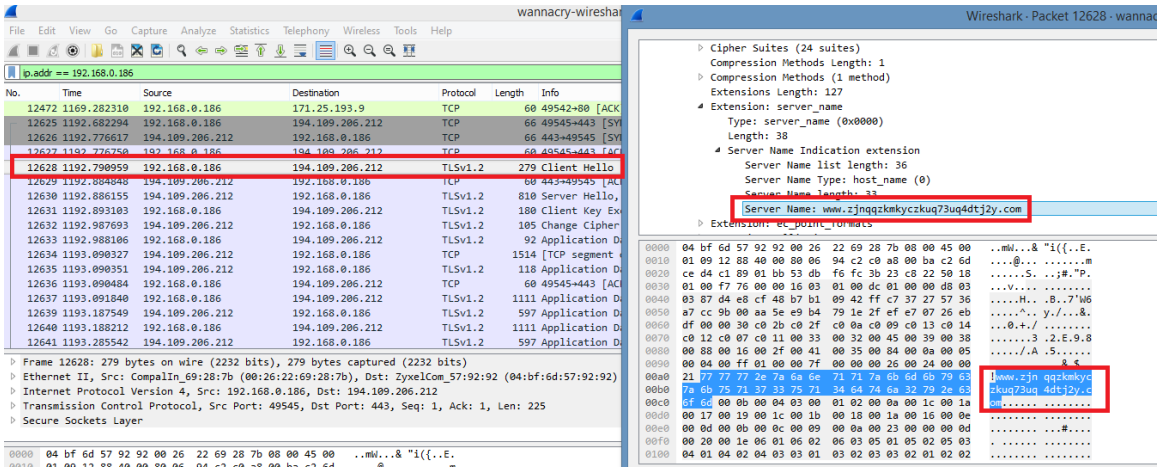


Figure 8. Identification de noms de domaines générés aléatoirement dans le trafic TOR

Réponse active du CDS suite à la détection de WannaCry

Le CDS peut être configuré en **mode actif** pour prendre action lorsqu'une compromission ou un comportement anormal (ou douteux) est détecté dans un réseau. Ainsi, le CDS peut :

- **Interagir avec un coupe-feu** pour bloquer la source d'une compromission. Dans le cas de WannaCry, le CDS peut bloquer l'IP de l'ordinateur infecté, ce qui aurait eu pour conséquence de l'isoler du réseau et de l'empêcher de scanner d'autres ordinateurs internes ou distants pour se propager. Pour l'entreprise, ceci évite que d'autres ordinateurs internes du réseau soient infectés (forte réduction de l'impact potentiel de l'incident).
- **Interagir avec un NAC** (Network Access Control) lorsqu'un ordinateur est infecté ou à un comportement douteux. Ceci aura pour conséquence l'isolation dudit ordinateur du réseau.

Quelques recommandations

Nous faisons les recommandations suivantes pour minimiser le risque d'infection par des malwares zero-day :

- Mieux gérer les vulnérabilités du réseau et s'assurer d'appliquer les correctifs de sécurité
- Ne pas utiliser de systèmes d'exploitation non supportés (ex : Windows XP)
- Ne pas se fier uniquement aux outils de sécurité basés sur des signatures (IDS/IPS, SIEM, antivirus, etc.) pour détecter les cybermenaces. L'exposition du nombre de malwares (ex : 200 000 nouveaux virus détectés par jour en 2013, contre 1.8 million par jour en 2016!) rend ces outils de plus en plus inefficaces.

- Considérer de plus en plus les outils de sécurité comportementaux (tel que le CDS de StreamScan) dans le processus de sécurisation des réseaux informatiques. En plus de détecter les malwares et cyber menaces connus, le CDS détecte les comportements anormaux ou douteux dans votre réseau, incluant les infections ou compromissions par des nouvelles générations de malwares. **Pour rappel, les malwares et les cybermenaces de type zero-day sont ceux qui ont le plus d'impact sur les entreprises.**

Évolution de WannaCry

L'analyse et l'observation des deux (2) versions WannaCry laissent présager l'apparition de nouvelles versions, plus ou moins sophistiquées et complexes.

Au cours des mois à venir, nous recommandons d'accorder une attention très particulière aux communications TOR entrantes ou sortantes des réseaux informatiques. Par défaut, ces communications doivent être considérées comme étant suspectes et une action rapide devra être prise.

Nous attirons l'attention sur le fait qu'en matière de détection d'outils malicieux, les requêtes vers des noms de domaines générés aléatoirement sont des signes importants de compromission ou d'infections. Il est donc important de toujours prendre action lorsqu'un ordinateur du réseau essaie de communiquer avec ce genre de domaine.

StreamScan Détection et Réponse Gérées conçues pour vous

Cet article vous a été présenté par StreamScan. Notre solution de détection et réponse gérées (DRG) combine notre technologie innovante CDS et le soutien de notre équipe de pirates éthiques pour fournir la sécurité réseau dont votre organisation a besoin, à un coût nettement inférieur à celui des frais de licence des logiciels ou de la constitution d'une équipe de sécurité interne.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment StreamScan MDR peut vous aider à protéger votre entreprise ou votre organisation.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment le DRG de StreamScan peut vous aider à protéger votre entreprise ou votre organisation.

Courriel : demo@streamscan.ai
Téléphone : +1 (650) 264-9702
www.streamscan.ai