COMMUNICATION : RANSOMWARE WANNACRY

Chers partenaires, / Chers clients,

Une attaque par ransomware s'étend actuellement à grande échelle et a déjà impacté de façon significative les infrastructures informatiques de nombreuses organisations dans le monde entier.

Ce nouveau ransomware et ses potentielles variantes s'appellent communément Wannacry, WannaCrypt, Wanacrypt0r, Wanna decryptor,... Ils visent tous les systèmes d'exploitation de Microsoft pour exploiter une vulnérabilité particulière (MS17-010).

En Mars dernier, Microsoft diffusait un patch pour cette vulnérabilité. Hors ce dernier n'a malheureusement pas été appliqué sur un grand nombre de machines. Du fait de la portée de l'attaque, Microsoft a également diffusé un patch pour les ordinateurs opérant sur Windows XP, non supportés par le précédent patch.

Ce ransomware est particulièrement dangereux car il peut infecter de nouvelles machines, de manière totalement automatique et transparente, en se propageant lui-même via le port 445 TCP (SMB).

Nous vous suggérons de mettre en place les actions suivantes pour bloquer l'infection et vous protéger de futures variantes.

ETAPES GENERALES

Toujours mettre à jour les derniers patchs de vulnérabilité. Microsoft a exceptionnellement développé un patch pour Windows XP également.

Désactivez le support pour SMBV1 sur l'hôte

https://support.microsoft.com/fr-fr/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

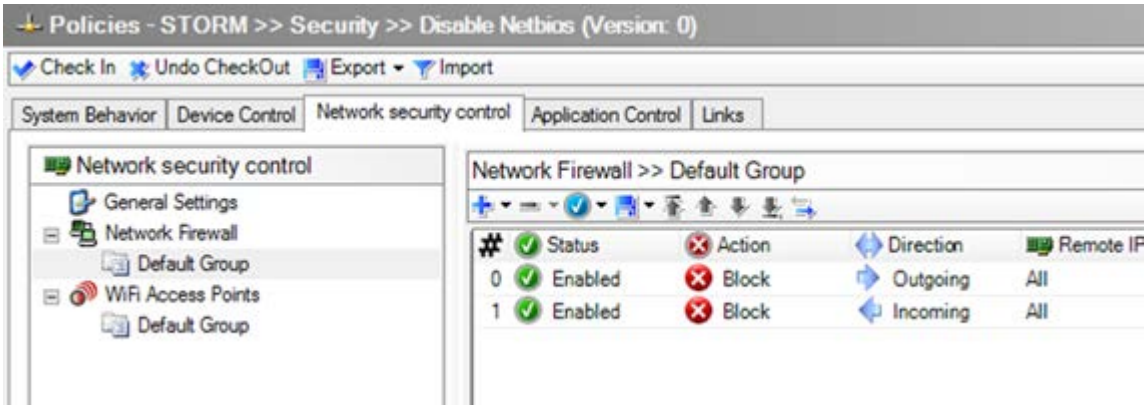
Pour plus d'information de la part de Microsoft :

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

STORMSHIELD ENDPOINT SECURITY

La première étape effectuée par WannaCry consiste à parcourir le réseau pour infecter de nouvelles machines puis d'installer un service lui permettant de chiffrer vos documents.

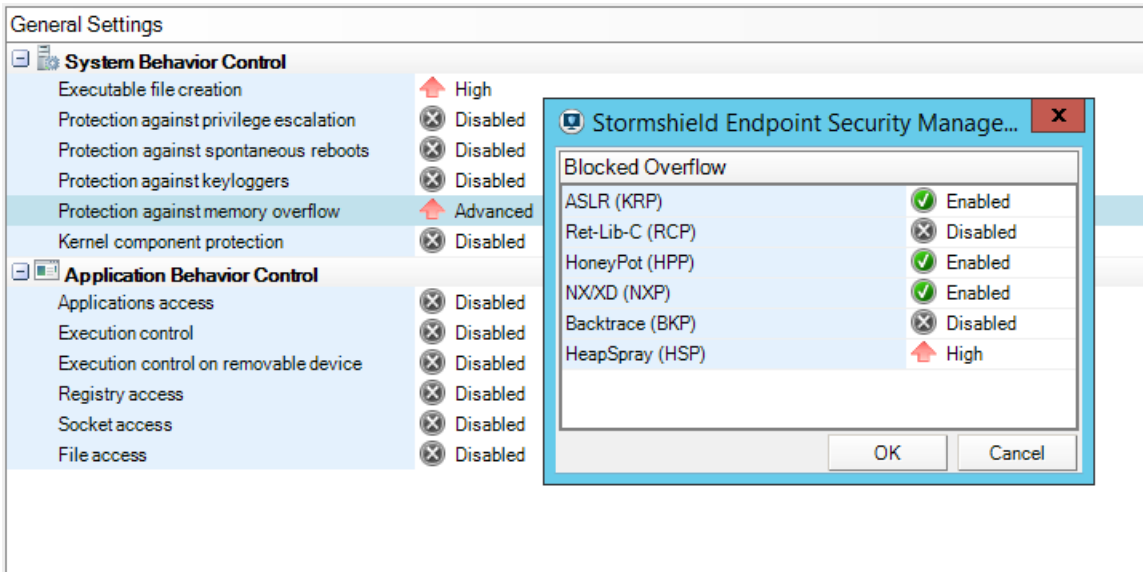
Bloquez le port 445 avec le pare-feu SES



Activez la protection contre la création de fichiers exécutables

Ceci empêchera WannaCry d'installer le service utilisé pour chiffrer vos fichiers.

Positionnez "Protection contre le débordement de mémoire" sur HAUT. Nous sommes persuadés que de nouvelles variantes apparaîtront dans les prochains jours et qu'elles utiliseront des tentatives de dissimulation en combinant différentes méthodes.



Utilisez le filtrage d'extension

Nous vous suggérons de créer un nouvel identificateur d'application appelé « Productivity » et d'y intégrer toutes les applications régulièrement utilisées par votre organisation

App Identifiers

Add | Remove | Rename | Check In | Undo CheckOut | Refresh | Export | Import

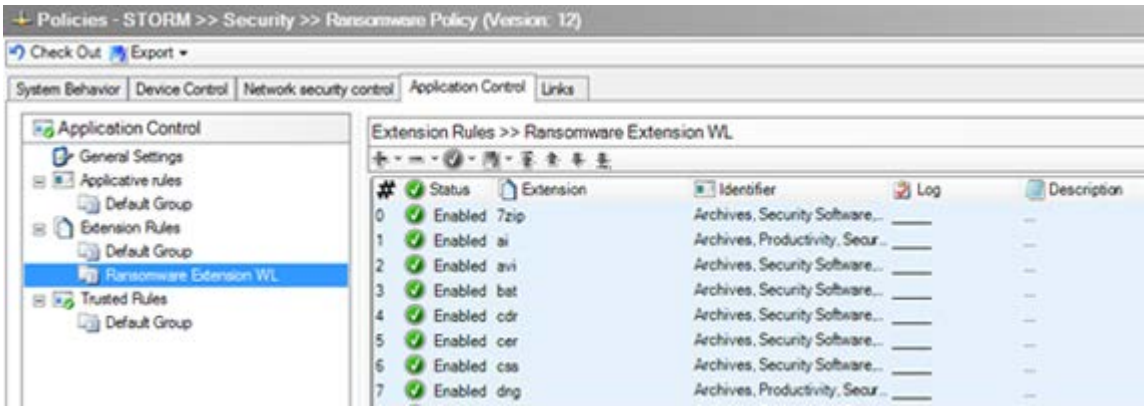
Name	Creation	Last modification	Policy(ies) linked	Comment
Archives	4/19/2017 1:31:10 PM	4/20/2017 12:19:33 PM	2	
Communication	4/19/2017 1:31:11 PM	4/20/2017 12:19:33 PM	2	
Productivity	4/19/2017 1:31:11 PM	4/20/2017 12:38:40 PM	2	
Security Software	4/19/2017 1:31:11 PM	4/20/2017 12:19:33 PM	2	
System Apps	4/19/2017 1:31:11 PM	4/20/2017 12:35:07 PM	2	
Video/Music	4/19/2017 1:31:11 PM	4/20/2017 12:35:12 PM	2	
Web Browser	4/19/2017 1:31:11 PM	4/20/2017 12:19:33 PM	2	

App Identifiers entries

Add | Modify | Remove

Type	Value	Description
Path / Certificate	*\gimp-*.exe - Gimp.crt (COMODO Code Signing CA 2) (COMODO Code Signin...	Gimp Image Editor
Path / Certificate	*\dreamweaver.exe - Adobe Dreamweaver.crt (Symantec Class 3 Extended Vali...	Adobe Dreamweaver CC
Path / Certificate	*\google photos backup.exe - Google Photo Backup.crt (Symantec Class 3 SHA...	Google Photos Sync App
Path / Certificate	*\acrobat.exe - Adobe Acrobat.crt (Symantec Class 3 Extended Validation Code...	Adobe Acrobat DC
Path / Certificate	*\photoshop.exe - Adobe Photoshop.crt (Symantec Class 3 Extended Validation...	Adobe Photoshop CC
Path / Certificate	*\adobe media encoder.exe - Adobe Premiere / Media Encoder.crt (Symantec Cl...	Adobe Media Encoder CC
Path / Certificate	*\integrator.exe - Office2003-v2.cer (Microsoft Code Signing PCA) (Microsoft Co...	MSOffice 2016 - Office365
Path / Certificate	*\indesign.exe - Adobe Indesign / Adobe Illustrator.crt (Symantec Class 3 Exten...	Adobe Indesign CC
Path / Certificate	*\lightroom.exe - Adobe Lightroom.crt (Symantec Class 3 Extended Validation C...	Adobe Lightroom CC
Path / Certificate	c:\program files*\microsoft office*\office16*.exe - Office2003-v2.cer (Microsoft...	Word
Path / Certificate	*\camtasiastudio.exe - CamtasiaStudio.crt (DigiCert SHA2 Assured ID Code Sig...	Camtasia Studio
Path / Certificate	*\illustrator.exe - Adobe Indesign / Adobe Illustrator.crt (Symantec Class 3 Exten...	Adobe Illustrator
Path / Certificate	*\winscp.exe - Winscp.crt (Symantec Class 3 SHA256 Code Signing CA) (Syma...	WinSCP

L'étape suivante consiste à configurer une liste blanche afin de forcer toutes les données sensibles à n'être gérées que par l'application autorisée. Cette méthode ne bloque pas seulement les tentatives de chiffrement de WannaCry, mais aussi toutes les variantes qui fonctionneraient de façon similaire.

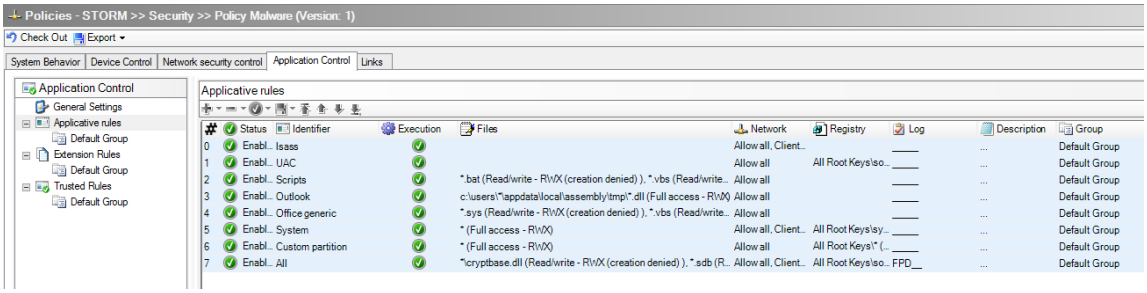


Vous pouvez consulter le guide d'administration pour plus d'information sur les règles d'extension.

Stormshield Endpoint Security peut aussi bloquer la suppression des "shadow copy" en bloquant les appels à vssadmin.exe, ce qui permettra donc de garder une copie de vos fichiers originaux.

Mettez à jour en version V7.2.16

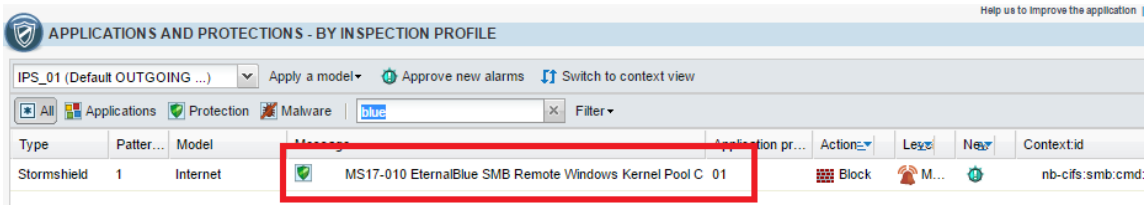
Dans la version V7.2.16, la politique par défaut permet de détecter et de bloquer les logiciels malveillants comme WannaCry.



STORMSHIELD NETWORK SECURITY

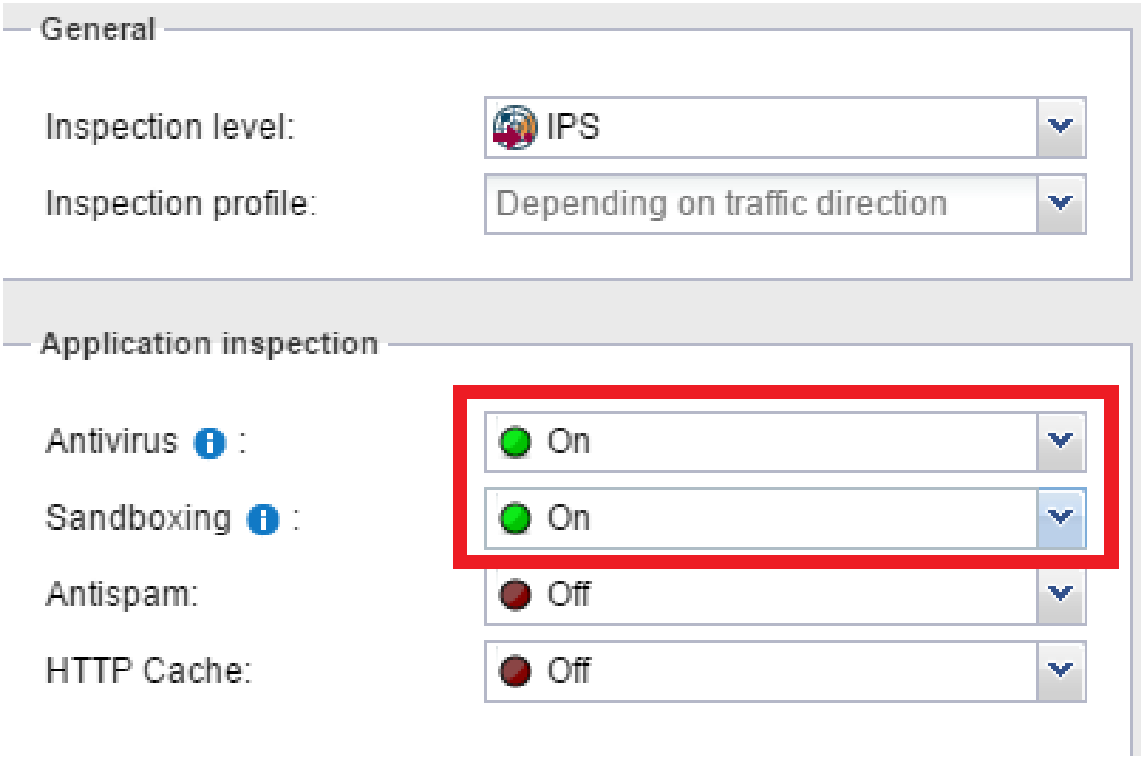
Activez la protection contre l'exploitation de l'exploit EternalBlue dans l'IPS

Cette protection est activée par défaut. Vérifiez bien que votre moteur IPS est à jour et que la protection est activée dans les deux directions (entrantes et sortantes).

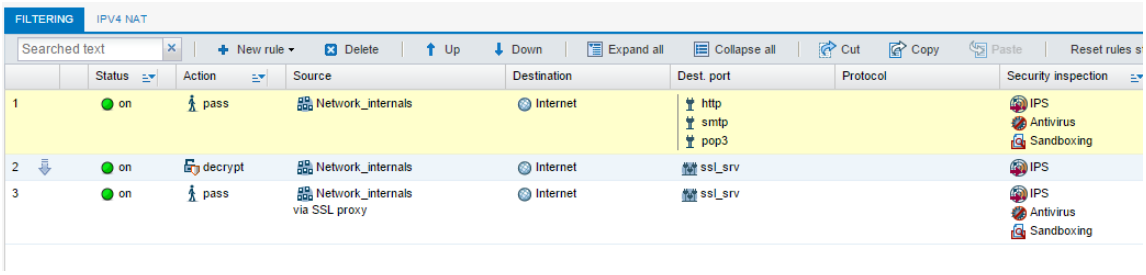


Activez l'option Breach Fighter (si vous avez souscrit à cette option)

Notre « sandbox » en mode cloud détecte et bloque ce ransomware. Elle détectera et bloquera également toutes les futures variantes si une tentative de diffusion via courrier électronique était lancée.

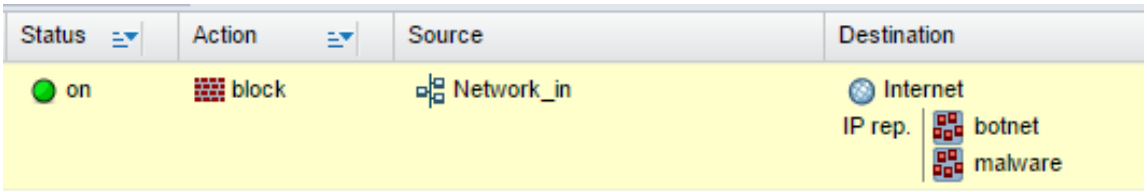


N'oubliez pas de décrypter le traffic SSL afin de permettre le fonctionnement de la « Sandbox ».



Bloquez l'accès aux botnets connus

Ceux-ci sont utilisés pour propager le ransomware donc le fait de les bloquer vous aidera à vous protéger contre de futures variantes.



Filtrage d'URL

Ce ransomware essaie de contacter deux domaines non enregistrés qui agissent comme un interrupteur (kill-switch) et qui permettent de bloquer l'action du malware à distance. Ce mécanisme peut également servir à déterminer si la machine ciblée est réelle ou s'il s'agit d'une « sandbox ». Le code malveillant est écrit afin qu'il exécute son action (c.-à-d. qu'il chiffre vos fichiers) s'il n'y a pas de réponse du domaine. Si le domaine répond, le ransomware ne chiffrera pas vos fichiers. Si les domaines WannaCry sont bloqués, il continuera à chiffrer, même si l'interrupteur a été activé. Pour cette raison, nous ne recommandons pas le filtrage des URL concernées pour prévenir la propagation de l'infection.

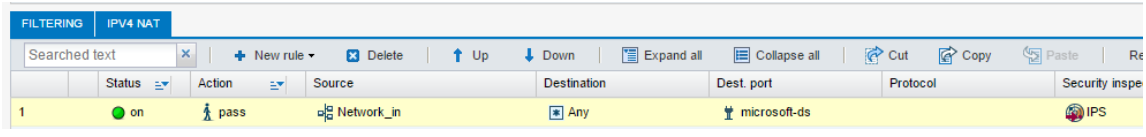
Même si le filtrage d'URL est toujours de façon générale une bonne pratique, nous vous suggérons de vérifier que les deux domaines WannaCry suivants (c.-à-d. « kill-switches) sont accessibles depuis vos différents réseaux internes, **en ne bloquant ne pas** :

hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com et hxxp://ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com (replace hxxp by http of course)

Créez des règles de filtrage

Il est important de segmenter votre réseau et de bloquer le trafic sur le port 445 lorsque cela est possible.

De manière générale, la segmentation est toujours une bonne pratique pour éviter la propagation de logiciels malveillants.



STORMSHIELD VISIBILITY CENTER

Vous pouvez utiliser Stormshield Visibility Center pour vérifier si les machines de votre réseau ont été effectivement impactées.

Si des connexions vers les sites ci-dessous sont visibles dans votre tableau de bord SNS, cela signifie que vous êtes probablement infecté.

hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

hxxp://ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
hxxp:// www[.]ayylmaoTJHSSTasdfasdfasdfasdfasdfasdfasdf[.]com

La même approche peut être utilisée lorsque vous affichez le tableau de bord de SES, si vous constatez des activités anormales des processus et extensions suivants.

C:\WINDOWS\tasksche.exe

C:\WINDOWS\taskdl.exe

C:\WINDOWS\taskse.exe

C:\WINDOWS\@WanaDecryptor@.exe

Et tous les fichiers avec les extensions *.WNCRYPT, .WNRY, .WCRY, .WNCRY, .WNCRYT*

L'équipe Stormshield

---

www.stormshield.eu

STORMSHIELD

Stormshield, filiale à 100% d'Airbus Defence and Space, propose des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).