STREAMSCAN
Cybersécurité pour
les moyennes entreprises

ANALYSE DU

# RANSOMWARE NOTPETYA

JUIN 2017 //

## Introduction

Le malware NotPetya vient d'infecter plusieurs ordinateurs à travers le monde, notamment en Ukraine, en France, en Russie et en Angleterre. L'ampleur de cette attaque a fait rappeler au monde les ravages causés par le ransomware WannaCry qui s'était propagé le 12 mai 2017, touchant plus de 200 000 ordinateurs dans plus de 200 pays en quelques jours. StreamScan a publié un livre blanc sur WannaCry. Vous pouvez le consulter à https://www.streamscan.io/fr/2017/Rapport-WannaCrypt0r-FRv1.0.pdf.

Le présent document concerne l'analyse du malware NotPetya qui a sévit le 27 juin 2017.

Note : bien que présentant des similarités avec le ransomware Petya (découvert en avril 2016), NotPetya est bel et bien un nouveau malware.

## Vecteur de propagation de NotPetya

Le vecteur initial d'infection de NotPetya n'est pas encore définitivement connu. De nombreuses sources pointent vers une propagation à travers un logiciel de comptabilité Ukrainien nommé **MeDoc**. Les serveurs de la compagnie Ukrainienne auraient été piratés, et une mise à jour contenant le malware NotPetya aurait été effectuée vers les postes clients (ceci expliquerait la grande propagation du malware en Ukraine qui concentre à lui seul plus de 60% des infections).

## Méthodologie d'analyse du ransomware NotPetya

Afin de cerner le comportement de NotPetya ainsi que ses subtilités, nous l'avons analysé dans un environnement de test.

### Fichier analysé

Hash MD5 : da2b0b17905e8afae0eaca35e831be9e

Hash SHA256 : 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745

### Analyse du malware

L'extraction des chaînes de caractères présents dans le binaire de NotPetya nous donne quelques indices sur son comportement :

- Liste des extensions ciblées par le malware :

'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 ':

Note : NotPetya ne chiffre pas les fichiers un à un comme WannaCry. Il chiffre le fichier MFT contenant les informations nécessaires pour accéder aux fichiers présents sur le disque.

- Présence de fonctions de chiffrement combinant RSA et AES.

‘Microsoft Enhanced RSA and AES Cryptographic Provider’, ‘CryptReleaseContext, CryptAcquireContextA, CryptGenRandom,CryptExportKey,CryptAcquireContextW,CryptSetKeyParam,CryptImportKey,CryptEncrypt,CryptGenKey, CryptDestroyKey’

- Utilisation du service de planifications des tâches pour programmer un arrêt du système infecté

‘schtasks %ws/Create /SC once /TN "" /TR "%ws" /ST %02d:%02d at %02d:%02d %ws shutdown.exe /r /f /RU "SYSTEM"  InitiateSystemShutdownExW’

- Chargement d’une librairie pendant l’exécution de NotPetya et lancement de nouveaux processus.

‘process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\%s\" #1 ‘ :

- Création de nouveaux fichiers par NotPetya : ‘CreateFileA’
- Énumération de informations d’identification de l’utilisateur courant : ‘CredEnumerateW:’

Une analyse des librairies et fonctions importées par NotPetya confirme aussi le comportement de cryptage et les activités réseaux effectuées par le ransomware : CRYPT32.DLL, CRYPTSP.DLL, IPHLPAPI.DLL, LOGONCLI.DLL.

Une fois ces premiers indices identifiés, nous avons procédé à une analyse dynamique de NotPetya. À cet effet, nous avons mis en place un environnement de test confiné où un ordinateur Windows 7 (IP = 10.0.1.3) a été infecté. Le trafic réseau généré par l’ordinateur infecté a été ensuite capturé pour des fins d’analyse.

Au lancement du fichier NotPetya malicieux (dont les HASH MD5 et SHA256 sont indiqués ci-dessus), nous observons la création des processus **SearchProtocolHost.exe** et **SearchFilterHost.exe** qui indiquent une activité de scan lancée par le malware.

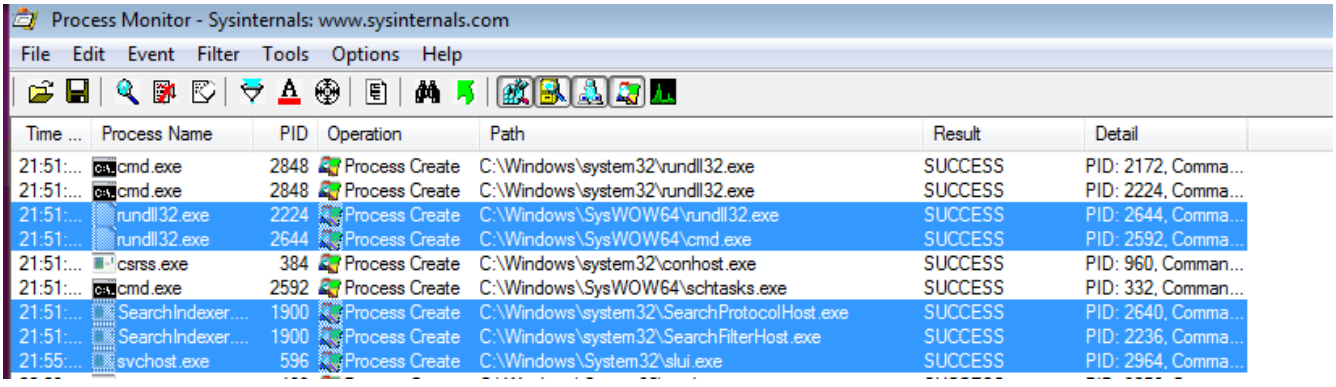



*Figure 1 : lancement des processus SearchProtocolHost.exe et SearchFilterHost.exe et scan du réseau local*

Une analyse de la base des registres de l’hôte infecté permet d’identifier les changements apportés par NotPetya :

```
Keys added: 3
-----------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain
\{8A52F02B-6935-404B-935B-289D5208699B}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
\{8A52F02B-6935-404B-935B-289D5208699B}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{43102B13-5EAF-48BF-AA8A-
C2233960F0F9}

-----------------------------------
Values added: 5
-----------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
\{8A52F02B-6935-404B-935B-289D5208699B}\Path: "\{43102B13-5EAF-48BF-AA8A-C2233960F0F9}"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
\{8A52F02B-6935-404B-935B-289D5208699B}\Triggers:  15 00 00 00 00 00 00 00 01 5F 4B 01 00 00 00 00
00 F4 49 6E 61 F0 D2 01 01 00 00 00 00 00 00 00 F4 49 6E 61 F0 D2 01 38 21 41 00 48 48 48 48 16
EE 6C 83 48 48 48 48 00 48 48 48 48 48 48 48 00 48 48 48 48 48 48 48 01 00 00 00 48 48 48 48 1C 00
00 00 48 48 48 48 01 05 00 00 00 00 00 00 05 15 00 00 00 22 BD 8F FC EE 98 FC 27 2D FF 28 77 E9 03 00
00 48 48 48 48 1A 00 00 00 48 48 48 48 74 00 65 00 73 00 74 00 2D 00 50 00 43 00 5C 00 74 00 65 00
73 00 74 00 00 00 48 48 48 48 48 48 38 00 00 00 48 48 48 48 58 02 00 00 10 0E 00 00 80 F4 03 00 FF
FF FF FF 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 DD DD 00 00 00 00 00 00 01 5F 4B 01 00 00 00 00 00 F4 49 6E 61 F0 D2
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 FF FF FF FF FF
 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
\{8A52F02B-6935-404B-935B-289D5208699B}\DynamicInfo:  03 00 00 00 E1 28 2B F7 47 F0 D2 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{43102B13-5EAF-48BF-AA8A-
C2233960F0F9}\Id: "{8A52F02B-6935-404B-935B-289D5208699B}"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{43102B13-5EAF-48BF-AA8A-
C2233960F0F9}\Index: 0x00000003

-----------------------------------
Values modified: 18
```

*Figure 2 : changements apportés dans la base de registre du système infecté par NotPetya*

Les clés ajoutées à la base de registres confirment que le malware a planifié une tâche qui devrait s'exécuter ultérieurement. En analysant de plus près les tâches planifiées sur la machine infectée, nous constatons la présence d'une tâche planifiée par l'utilisateur courant (test) qui porte le nom **43102b13-5EAF-48BF-AA8A-C2233960F0F9**. Cette tâche planifiée a pour objectif de forcer l'hôte infectée à s'éteindre une (1) heure après l'exécution du malware.

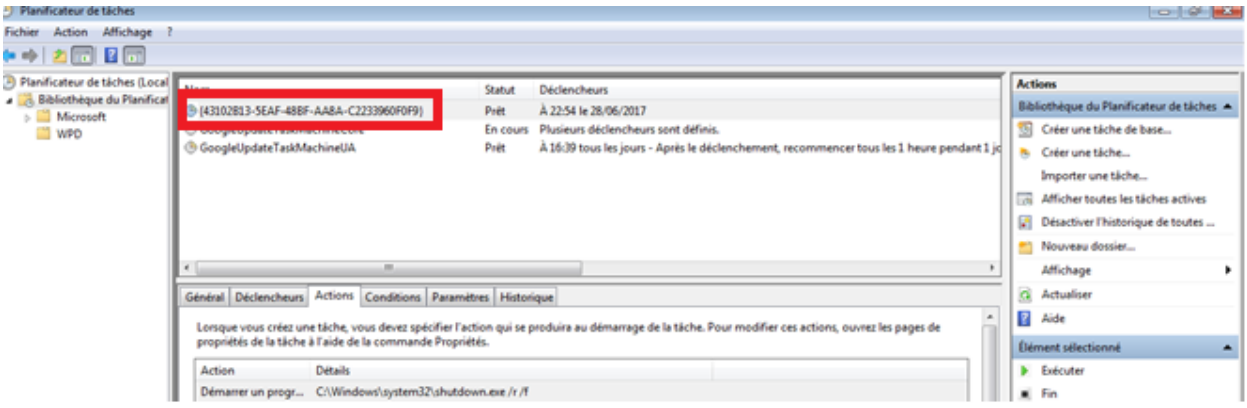
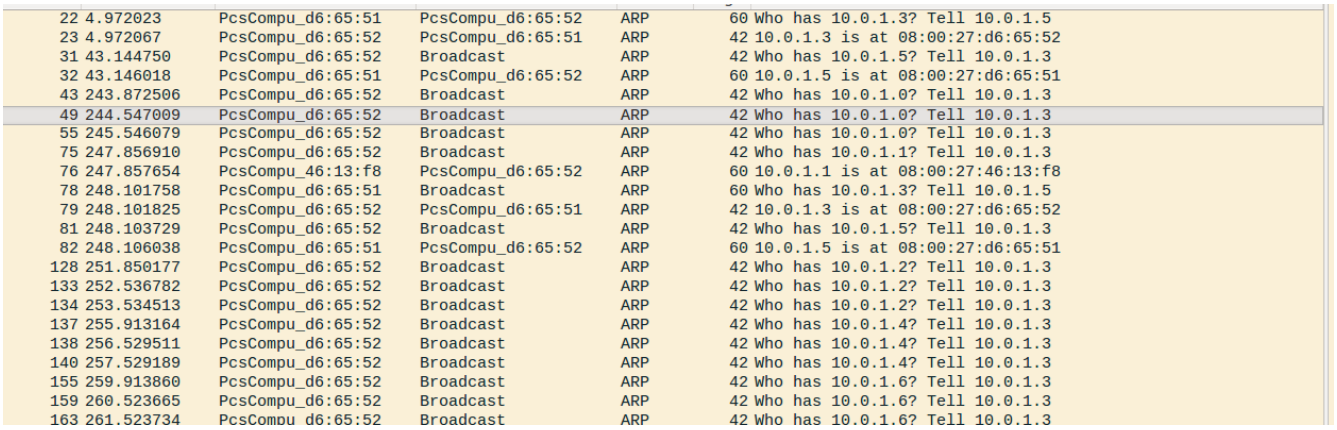



*Figure 3 : planification de l'arrêt de l'hôte (1 heure après son infection)*

## Propagation du malware dans le réseau

Afin d'analyser le mode de propagation de NotPetya, nous avons connecté la machine infectée a un réseau de test où se trouve une autre machine Windows 7 vulnérable à l'exploit **EternalBlue**. Cette machine sera appelée **Victime1** (IP : 10.0.1.5). L'analyse du trafic réseau capturé dans ce réseau de test permet d'établir clairement le mode de propagation de NotPetya qui est le suivant :

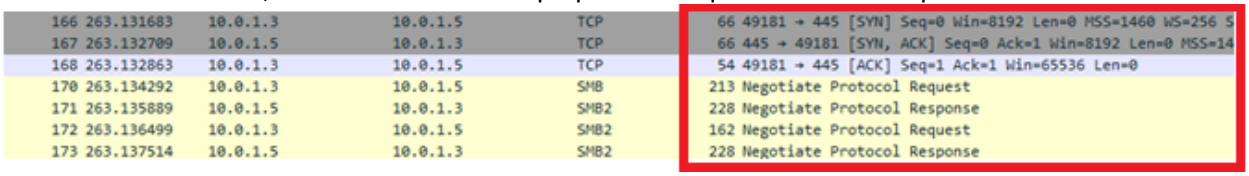
- **Étape 1** : L'hôte infecté émet des requêtes ARP Broadcast afin de scanner le réseau et trouver des machines qui y sont connectées.



| | | | | | | |
|---|---|---|---|---|---|---|
| 22 | 4.972023 | PcsCompu_d6:65:51 | PcsCompu_d6:65:52 | ARP | 60 | Who has 10.0.1.3? Tell 10.0.1.5 |
| 23 | 4.972067 | PcsCompu_d6:65:52 | PcsCompu_d6:65:51 | ARP | 42 | 10.0.1.3 is at 08:00:27:d6:65:52 |
| 31 | 43.144750 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.5? Tell 10.0.1.3 |
| 32 | 43.146018 | PcsCompu_d6:65:51 | PcsCompu_d6:65:52 | ARP | 60 | 10.0.1.5 is at 08:00:27:d6:65:51 |
| 43 | 243.872506 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.0? Tell 10.0.1.3 |
| 49 | 244.547009 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.0? Tell 10.0.1.3 |
| 55 | 245.546079 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.0? Tell 10.0.1.3 |
| 75 | 247.856910 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.1? Tell 10.0.1.3 |
| 76 | 247.857654 | PcsCompu_46:13:f8 | PcsCompu_d6:65:52 | ARP | 60 | 10.0.1.1 is at 08:00:27:46:13:f8 |
| 78 | 248.101758 | PcsCompu_d6:65:51 | Broadcast | ARP | 60 | Who has 10.0.1.3? Tell 10.0.1.5 |
| 79 | 248.101825 | PcsCompu_d6:65:52 | PcsCompu_d6:65:51 | ARP | 42 | 10.0.1.3 is at 08:00:27:d6:65:52 |
| 81 | 248.103729 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.5? Tell 10.0.1.3 |
| 82 | 248.106038 | PcsCompu_d6:65:51 | PcsCompu_d6:65:52 | ARP | 60 | 10.0.1.5 is at 08:00:27:d6:65:51 |
| 128 | 251.850177 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.2? Tell 10.0.1.3 |
| 133 | 252.536782 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.2? Tell 10.0.1.3 |
| 134 | 253.534513 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.2? Tell 10.0.1.3 |
| 137 | 255.913164 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.4? Tell 10.0.1.3 |
| 138 | 256.529511 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.4? Tell 10.0.1.3 |
| 140 | 257.529189 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.4? Tell 10.0.1.3 |
| 155 | 259.913860 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.6? Tell 10.0.1.3 |
| 159 | 260.523665 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.6? Tell 10.0.1.3 |
| 163 | 261.523734 | PcsCompu_d6:65:52 | Broadcast | ARP | 42 | Who has 10.0.1.6? Tell 10.0.1.3 |

*Figure 4 : scan du réseau local afin de trouver des ordinateurs à infecter.*

- **Étape 2** : À la découverte d'une machine connectée au réseau de test (ici l'hôte 10.0.1.5), NotPetya initie la procédure d'infection en exécutant l'exploit EternalBlue exploitant la vulnérabilité MS17-10, comme le montre les paquets SMB que nous avons capturés.



| | | | | | | |
|---|---|---|---|---|---|---|
| 166 | 263.131683 | 10.0.1.3 | 10.0.1.5 | TCP | 66 | 49181 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S |
| 167 | 263.132709 | 10.0.1.5 | 10.0.1.3 | TCP | 66 | 445 → 49181 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=14 |
| 168 | 263.132863 | 10.0.1.3 | 10.0.1.5 | TCP | 54 | 49181 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 170 | 263.134292 | 10.0.1.3 | 10.0.1.5 | SMB | 213 | Negotiate Protocol Request |
| 171 | 263.135889 | 10.0.1.5 | 10.0.1.3 | SMB2 | 228 | Negotiate Protocol Response |
| 172 | 263.136499 | 10.0.1.3 | 10.0.1.5 | SMB2 | 162 | Negotiate Protocol Request |
| 173 | 263.137514 | 10.0.1.5 | 10.0.1.3 | SMB2 | 228 | Negotiate Protocol Response |

*Figure 5 : infection des ordinateurs vulnérables (voir port 445 SMB)*

## Confirmation de l'infection de l'hôte Victime1

Pour confirmer que le malware NotPetya s'est propagé vers l'hôte Victime1, nous inspectons les tâches planifiées sur cette dernière et constatons qu'elle est infectée.

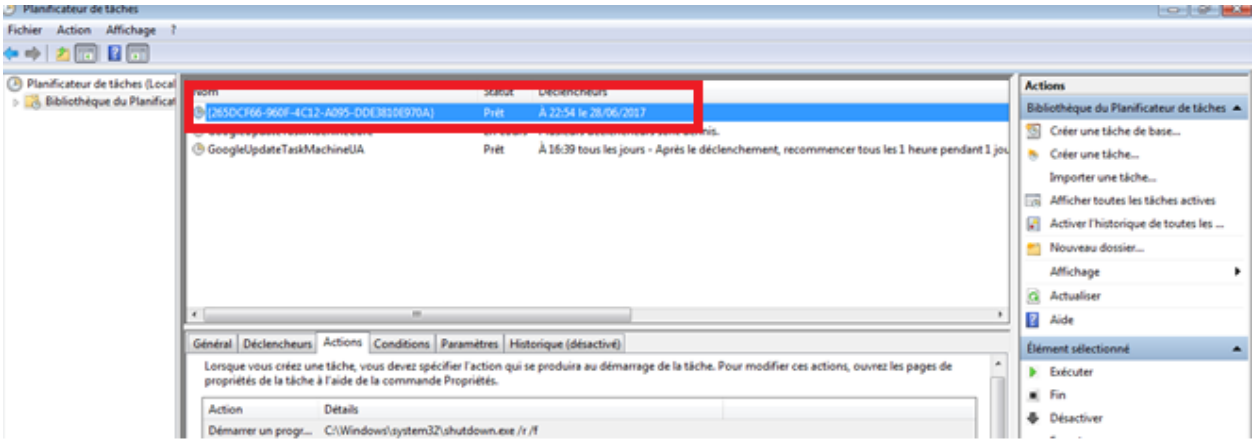
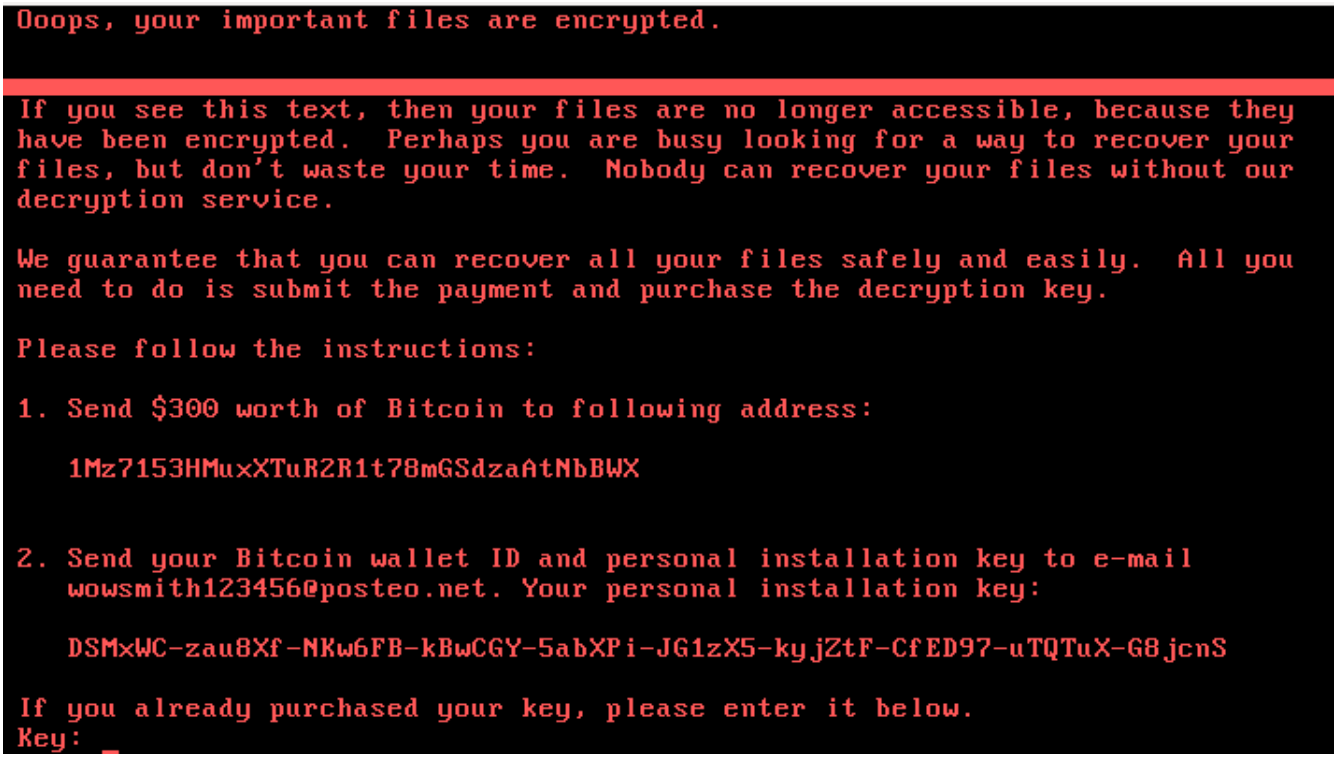



*Figure 6 : infection de l'hôte **Victime1** par propagation de NotPetya*

Au démarrage de l'ordinateur **Victime1**, l'écran indiquant l'infection et la demande de rançon apparait :



## Conclusion

L'analyse du mode de collecte des rançons mis en place par les auteurs de NotPetya nous laisse perplexes quant à leur motivation financière. En effet, il est demandé aux victimes d'envoyer un courriel à une adresse (**wowsmith123456@posteo.net**) rendue publique. Les auteurs de malware ne pouvaient pas ignorer que ladite boite de courriel serait désactivée sitôt l'infection médiatisée. Les plaintes de victimes auraient aussi conduit à la désactivation de cette boite de courriel.

Comme il fallait s'y attendre, la boite de courriels **wowsmith123456@posteo.net** a été désactivée. De ce fait, les victimes qui souhaiteraient payer la rançon (opération que nous déconseillons vivement) ne pourraient même pas le faire. Pour un malware de ce niveau de sophistication, cette impasse (qui s'apparente à une erreur de débutant), est incompréhensible et aberrante.

Nous en concluons que le but de NotPetya est de rendre inaccessibles de manière définitive les données qui ont été chiffrées. NotPetya a donc un but destructif et des zones d'ombre persistent sur la volonté de ses auteurs à faire passer leur malware pour un ransomware.

## Recommandation

La propagation rapide du malware NotPetya prouve encore une fois l'importance des mises à jours et de l'application des patchs de sécurité. En effet, ce nouveau malware s'est propagé de la même façon que WannaCry en exploitant la même vulnérabilité dont le patch est disponible depuis Mars 2017.


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