



# PLEASED TO MEET YOU, MY NAME IS PETYA !

Damien SCHAEFFER

Cyber Security Analyst - m@lwa.re

**mots-clés : MALWARE / MBR / BIOS / CRYPTO / BOOTKIT / REVERSE  
ENGINEERING / RANSOMWARE**

**L**es ransomwares : ces logiciels malveillants prennent en otage vos données personnelles contre remise d'une rançon nous rendent immédiatement la vie pénible si l'on a le malheur de se faire avoir. Très actif depuis le début de l'année, le cas étudié ci-après a la particularité de se loger juste après le BIOS, empêchant alors même le système de démarrer après avoir chiffré le disque.

## Introduction

Le principe de la rançon, déjà utilisé depuis des siècles est depuis l'informatisation de la société aussi mis en pratique dans le monde numérique. Ce ne sont plus des personnes qui sont prises en otage, mais des données rendues inaccessibles par l'utilisation d'un logiciel frauduleux jusqu'au paiement, généralement en Bitcoin.

Ce début d'année a déjà été prolifique pour ce type de logiciels. Apprécier par les pirates notamment dus à leurs principes de fonctionnement assez simple, et au retour sur investissement rapide qui les rendent très rentables. Dans la digne lignée des *CryptoWall*, *CryptoLocker*, *TeslaCrypt*, ou encore *Locky* pour n'en citer que quelques-uns, Petya se distingue par un côté rétro de par son interface en *ASCII art*, mais surtout par son habileté à agir comme un bootkit en se répliquant dans le *Master Boot Record* (MBR) ou dans la *GUID Partition Table* (GPT) suivant le type d'installation, empêchant alors le système de démarrer après avoir préalablement chiffré son contenu.

L'article va se composer de deux parties principales : la première traite de l'exécution du malware jusqu'à son implantation dans le secteur de démarrage, et la seconde du chiffrement du disque jusqu'à son éradication.

## 1 Userland

Une fois n'est pas coutume mon sample comporte un nom à consonance allemande **Bewerbungsmappe-gepackt.exe** (md5:af2379cc4d607a45ac44d62135fb7015), pouvant

se traduire par dossier de candidature compressé. Compressé, car il arbore comme icône celle d'une archive auto extractible de type *SFX*. Cela pourrait servir à cibler un service de ressources humaines d'une entreprise, ou n'importe quel particulier étant un peu trop curieux au vu d'un CV.

Dès son lancement, le malware contrôle s'il dispose des droits administrateurs requis pour l'accès au disque physique. Dans le cas contraire, rien ne se passe, car toutes ses opérations vont se faire à un niveau bas du système, ce qui est l'on peut dire un de ses points faibles ou plus généralement le revers de la médaille d'un bootkit. Pour disposer de tels priviléges, Petya va tout simplement les demander à l'utilisateur via l'élément **trustInfo** du manifeste de l'exécutable.

```

01 : <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
02 :   <security>
03 :     <requestedPrivileges>
04 :       <requestedExecutionLevel
05 :         level="requireAdministrator"
06 :         uiAccess="false"/>
07 :     </requestedPrivileges>
08 :   </security>
09 : </trustInfo>
```

Le payload du malware est une *dll* obfuscée par un *cryptor*, pouvant usurper une archive auto extractible comme un *PDF* dans cet exemple, ou de n'importe quel programme suivant le *packer* utilisé. Son fonctionnement est tout ce qu'il y a de plus standard à savoir dissimuler la charge utile aux antivirus en modifiant le hash d'origine, et en ajoutant des mécanismes rendant plus difficile le reverse engineering ou l'analyse automatisée au sein d'une sandbox. De ce fait et en raison des nombreuses variations existantes, je ne vais pas traiter la déobfuscation et passer directement à l'analyse du payload, stage 1.

Petya cherche à gagner un accès bas niveau au disque physique. Pour ce faire, plusieurs étapes seront nécessaires. Premièrement, comme pour presque n'importe quelle opération sous Windows, un handle est requis et devra être passé aux API de contrôle du disque. Il s'obtient en appelant **kernel32\_CreateFileA** avec comme cible la racine du disque logique, **\.\.\C:** dans notre cas. Cela retournera un handle qui sera donné à la fonction système permettant d'envoyer des commandes à un driver spécifique, **kernel32\_DeviceIoControl**.

Pour passer du disque logique au physique, cette API sera appellée avec **IOCTL\_VOLUME\_GET\_VOLUME\_DISK\_EXTENTS**. Ce paramètre récupère l'emplacement physique d'un volume sur un ou plusieurs disques à savoir **\.\PhysicalDrive0**. Une fois cet emplacement trouvé, l'argument **IOCTL\_DISK\_GET\_PARTITION\_INFO\_EX** renvoie des informations étendues sur le type, la taille, et la nature d'une partition (MBR ou GPT). Précisons encore que l'échantillon étudié se concentre sur le cas d'une infection du MBR, néanmoins le fonctionnement de la variante GPT est similaire.

À ce stade, le malware connaît tout ce dont il a besoin pour accéder et altérer le contenu du disque physique à sa guise. Il commence par copier l'intégralité du MBR d'origine pour être en mesure de le restaurer une fois la rançon payée. Cette zone se trouve dans les 512 premiers bytes d'un disque, dans le secteur **0**. Dès la copie faite, il l'obfusque simplement avec un *XOR* '7'.

```

xor_mbr:
    xor    [esp+eax+0C40h+mbr], '7'
    inc    eax
    cmp    eax, ebp           ; ebp=512
    jb     short xor_mbr

```

Figure 1 : XOR '7' appliqué au MBR.

Le registre **eax** sert ici de compteur : incrémenté à chaque itération, la boucle se répète tant que sa valeur est strictement inférieure à **ebp**, dont la taille est celle d'un secteur de disque (512). Petya remplace ensuite le MBR par un *bootloader* qui lui permettra de charger la version bootkit du malware, aussi appelée *stage 2*.

Il génère en outre la clé de chiffrement symétrique du disque qui sera chiffrée asymétriquement en faisant appel aux courbes elliptiques via les librairies **cryptsp.dll** et **rsaenh.dll**. Cet identifiant unique permettra à l'attaquant de connaître la clé générée sur l'ordinateur de la victime.

Cette dernière sera encodée en *base58* pour faciliter son envoi. Cet algorithme a notamment comme avantage de n'inclure que des caractères alphanumériques, en omettant certains caractères pouvant porter à confusion comme le zéro '0' et le o majuscule 'O', ou comme le L minuscule 'l' et le i majuscule 'I'. Ceci est à préférer lors d'une entrée manuelle de texte, comme ici où la victime devra envoyer cet identifiant à l'attaquant.

Voici ce que donne la clé une fois chiffrée et encodée :

d0P2KsMyxbdwWi8oU8mBcE2Pbd71hxqVDDLkfqNvJWEffA9g498oVAppjcGLMc9HN  
4j6rYwVLKYfae9ja15M8b8R3

Illustré sur la figure ci-dessous, le malware va écrire sur le secteur 54 à 56 les informations suivantes :

- secteur 54 : la clé pour le chiffrement du disque et son identifiant, ainsi que les URLs du site de paiement ;
- secteur 55 : secteur entièrement rempli avec le caractère '7', cela servira pour la validation de la clé ;
- secteur 56 : le MBR d'origine préalablement *XOR* '7'.

```

push  edi
push  54
lea   edx, [esp+0C50h+key_url_id]
lea   ecx, [esp+0C50h+physical_drive_0]
call  write_memory
pop   ecx
pop   edx
test  eax, eax
jz    short fail

push  edi
push  55
lea   edx, [esp+0C50h+sector_7]
lea   ecx, [esp+0C50h+physical_drive_0]
call  write_memory
pop   ecx
pop   edx
test  eax, eax
jz    short fail

push  edi
push  56
lea   edx, [esp+0C50h+mbr]
lea   ecx, [esp+0C50h+physical_drive_0]
call  write_memory
pop   ecx
pop   edx
test  eax, eax
jz    fail

```

Figure 2 : Écriture du malware parmi les premiers secteurs du disque.

Avec maintenant Petya profondément intégré sur le disque dans la zone d'amorçage et les secteurs suivants, le malware va provoquer un redémarrage du système via l'appel à **SeShutdownPrivilege**. L'ordinateur va alors juste s'éteindre brusquement comme lors d'un *blue screen* ou d'une coupure de courant.

Dans l'état actuel du système, il est encore possible de se remettre de l'infection, car les données utilisateur ne sont pas encore chiffrées à la fin du *stage 1*. Il est en outre possible de récupérer la clé de chiffrement symétrique présente dans le MBR en faisant une copie des premiers secteurs du disque jusqu'au secteur 57 compris pour avoir l'intégralité de l'injection.

Cela peut se faire en démarrant sur un support de donnée externe ou en copiant les données après avoir monté le disque dur depuis autre machine. Le script







- [http://petya37h5tbhyvki\[.\]jonion/a6UWjQ](http://petya37h5tbhyvki[.]jonion/a6UWjQ) ;
- [http://petya5koahsf7sv\[.\]jonion/a6UWjQ](http://petya5koahsf7sv[.]jonion/a6UWjQ).

Pour cette analyse, la première URL a été utilisée. En y accédant via Tor, apparaît un site web au design propre, et aux faux airs de communisme en prenant par exemple la faucille et le marteau comme logo, et **petya ransomware** en écriture rouge et caractères cyrilliques. Il en est de loin très professionnel, avec support multilingue et accès par captcha pour éviter les accès automatisés.

En page d'accueil prend place un compte à rebours, à la fin duquel le montant à payer se verra doubler. En dessous de celui-ci se trouve une section blog, avec des publications de sociétés antivirus comme *trendmicro* ou *gdata* censées accroître la peur et la crédibilité du malware.

La section *payment* du site comporte 4 étapes pour mener à bien une transaction en Bitcoins.

- Step1 : Enter your personal identifier ;
- Step2 : Purchase Bitcoins ;
- Step3 : Do a Bitcoin transaction ;
- Step4 : Wait for confirmation.

Vient ensuite un onglet **FAQ**, censé expliquer ce que Petya vient de faire à votre système et en quoi il est dangereux et robuste, mais est en réalité rempli de fausses informations comme les algorithmes de chiffrement prétendument *RSA 4096* et *AES 256*, ainsi que la publication de vos données sur le *darknet* si le paiement n'est pas effectué. Évidemment, cette propagande est entièrement fausse et n'a que pour but de mettre la pression et inciter à céder au chantage.

La dernière section du site n'est de loin pas la moins intéressante : le support ! Ce dernier faisant partie intégral du *business model* des *ransomwares*. En effet, sans celui-ci les utilisateurs n'arriveraient pas à contacter l'attaquant en cas de soucis. En sachant que

**You (2016-04-05 07:35:16)**

I desperately need my data and therefore I've paid yesterday... Didn't you already received the money?

Please send me the key asap !!

**Support (2016-04-05 09:12:40)**

As you can see here: <https://blockchain.info/address/1L7ewTGGPiISDbpwBwfFWU3DC1H9e2dGSA>

Your bitcoins haven't arrived on our bitcoin address. I recommend you to contact the exchange where you bought your bitcoins.

Figure 8 : Demande de support relativ au paiement de la rançon.

les victimes obtiennent une clé fonctionnelle après leur paiement, de nouveaux utilisateurs leur emboîteront le pas. Mais dans le cas contraire, les futurs acheteurs ne paieront pas sachant que l'opération pourrait ne pas fonctionner. C'est pour cela que le support est primordial dans ce type d'opération.

J'ai donc voulu tenter l'expérience en prétendant avoir payé la veille et n'ayant toujours pas reçu ma clé. Et voilà qu'un peu plus de 1h30 plus tard une réponse me parvient, en me démontrant preuve à l'appui que mon argent n'est pas arrivé sur l'adresse *Bitcoin* du pirate. Ce délai plus que raisonnable peut même être qualifié de court comparé à bon nombre de services clients.

## Conclusion

Ce malware possède un design atypique, complexe, et sophistiqué. Le code démontre en outre l'expérience et l'habileté de son auteur. Cela amène aussi une certaine nouveauté sur le segment des *ransomwares*, avec un déploiement en plusieurs étapes d'abord dans l'espace utilisateur, puis dans le MBR tel un bootkit. À noter que l'utilisation du *secure boot* ou la désactivation du redémarrage automatique en cas de défaillance du système peut permettre de se prévenir du chiffrement du disque.

L'architecture de bas niveau impose quelques limitations, notamment la taille réduite à disposition et l'impossibilité d'utiliser des API, ce qui complique entre autres l'utilisation de la cryptographie. C'est une des raisons pour lesquelles la génération de clés se fait lors de la première étape du malware dans l'espace utilisateur. Cela est néanmoins très intéressant et inhabituel à étudier, comme notamment l'emploi d'*interrupts* comme interface avec le système, les bibliothèques étant indisponibles.

Malgré tout ce professionnalisme et le design élaboré du malware, Petya tend à avoir manqué sa cible. Ce genre de bootkit pouvant être insérés discrètement au plus profond du système relève plus des APT (*Advanced Persistent Threat*) que des *ransomwares*. En effet, ces derniers en *userland* font potentiellement plus de dégâts, en pouvant aussi chiffrer des périphériques externes ou réseaux par exemple. Ils requièrent en outre des droits élevés pour pouvoir s'infiltrer dans le secteur de démarrage, en comparaison des *ransomwares* standards.

Notons encore l'arrivée de Mischa, une version mise à jour corrigeant quelques lacunes de Petya, notamment en terme de cryptographie, et propose une solution alternative de chiffrement des données utilisateur en *userland* en cas d'exécution par un utilisateur disposant de droits limités.

Finalement, relevons encore les clins d'œil à l'univers de James Bond, plus particulièrement à l'opus *GoldenEye*, avec entre autres Petya, Janus en bas de page sur le site de paiement, ou encore le *XOR '7*, du MBR. ■



# PROFESSIONNELS !

DÉCOUVREZ NOS OFFRES D'ABONNEMENTS ...  
...EN VOUS CONNECTANT À L'ESPACE DÉDIÉ AUX PROFESSIONNELS SUR :

**www.ed-diamond.com**

## PDF COLLECTIFS PRO

OFFRE	ABONNEMENT	Réf	1 - 5 lecteurs	6 - 10 lecteurs	11 - 25 lecteurs			
			Tarif TTC	Réf	Tarif TTC	Réf	Tarif TTC	
PROMC2	6 <sup>e</sup> MISC		<input type="checkbox"/> PRO MC2/5	168,-	<input type="checkbox"/> PRO MC2/10	336,-	<input type="checkbox"/> PRO MC2/25	672,-
PROMC+2	6 <sup>e</sup> MISC + 2 <sup>e</sup> HS		<input type="checkbox"/> PRO MC+2/5	216,-	<input type="checkbox"/> PRO MC+2/10	432,-	<input type="checkbox"/> PRO MC+2/25	864,-

PROFESSIONNELS :  
N'HÉSitez PAS À  
NOUS CONTACTER  
POUR UN DEVIS  
PERSONNALISÉ PAR  
E-MAIL :  
[abopro@ed-diamond.com](mailto:abopro@ed-diamond.com)  
OU PAR TÉLÉPHONE :  
03 67 10 00 20

## ACCÈS COLLECTIFS BASE DOCUMENTAIRE PRO

OFFRE	ABONNEMENT	Réf	1 - 5 connexion(s)	6 - 10 connexions	11 - 25 connexions			
			Tarif TTC	Réf	Tarif TTC	Réf	Tarif TTC	
PROMC+3	MISC + HS		<input type="checkbox"/> PRO MC+3/5	177,-	<input type="checkbox"/> PRO MC+3/10	354,-	<input type="checkbox"/> PRO MC+3/25	708,-
PROH+3	GLMF + HS + LP + HS + OS		<input type="checkbox"/> PRO H+3/5	447,-	<input type="checkbox"/> PRO H+3/10	894,-	<input type="checkbox"/> PRO H+3/25	1788,-

Les abréviations des offres sont les suivantes : LM = GNU/Linux Magazine France HS = Hors-Série LP = Linux Pratique OS = Open Silicium

SÉLECTIONNEZ VOTRE OFFRE DANS LA GRILLE CI-DESSUS ET RENVOYEZ CE DOCUMENT COMPLET À L'ADRESSE CI-DESSOUS !

Voici mes coordonnées postales :

Société :	
Nom :	
Prénom :	
Adresse :	
Code Postal :	
Ville :	
Pays :	
Téléphone :	
E-mail :	



Les Éditions Diamond  
Service des Abonnements  
10, Place de la Cathédrale  
68000 Colmar – France  
Tél. : + 33 (0) 3 67 10 00 20  
Fax : + 33 (0) 3 67 10 00 21

Vos remarques :

Je souhaite recevoir les offres promotionnelles et newsletters des Éditions Diamond.  
 Je souhaite recevoir les offres promotionnelles des partenaires des Éditions Diamond.  
En envoyant ce bon de commande, je reconnais avoir pris connaissance des conditions générales de vente des Éditions Diamond à l'adresse internet suivante : [boutique.ed-diamond.com/content/3-conditions-generales-de-ventes](http://boutique.ed-diamond.com/content/3-conditions-generales-de-ventes) et reconnais que ces conditions de vente me sont opposables.