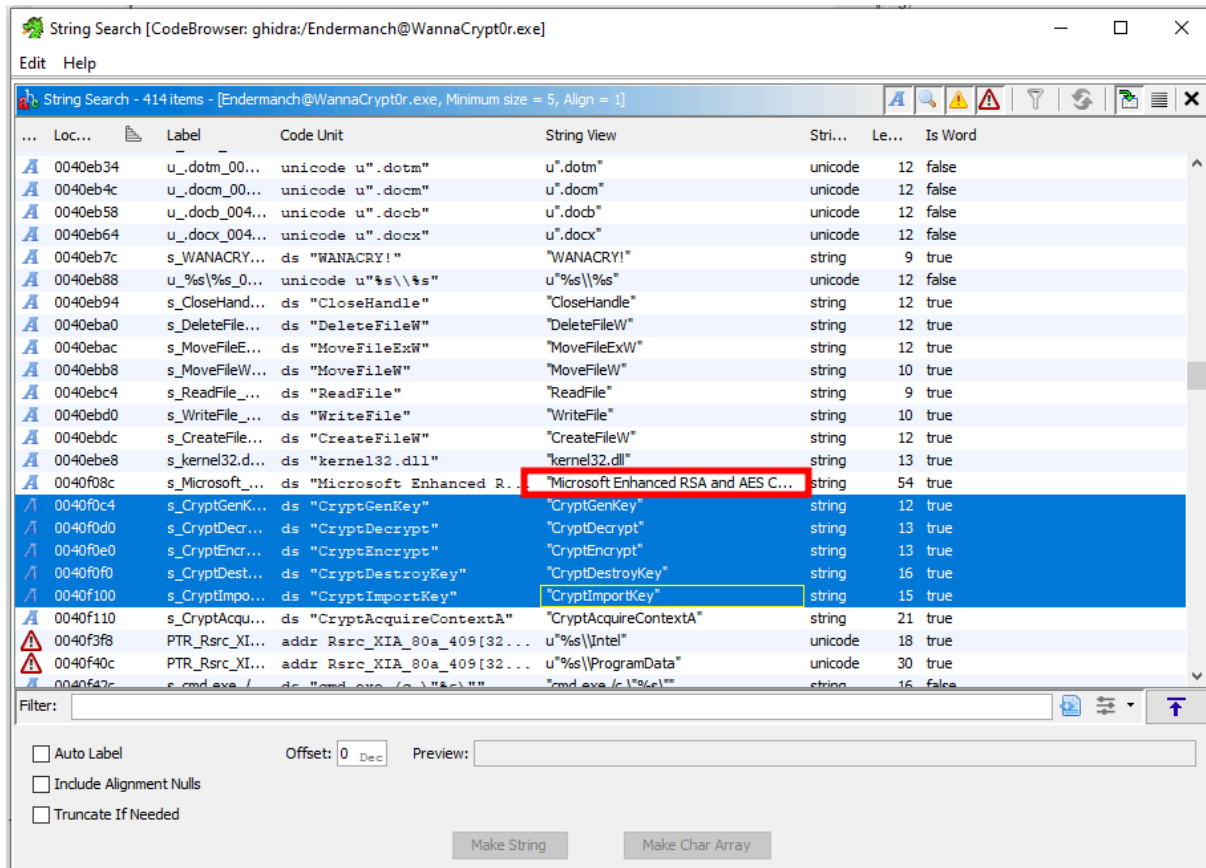


Rapport Analyse wanacry

Fonctionnement du chiffrement

On voit très clairement que wannacrypt utilise RSA et AES



...	Loc...	Label	Code Unit	String View	Stri...	Le...	Is Word
A	0040eb34	u_.dotm_00...	unicode u".dotm"	u".dotm"	unicode	12	false
A	0040eb4c	u_.docm_00...	unicode u".docm"	u".docm"	unicode	12	false
A	0040eb58	u_.docb_004...	unicode u".docb"	u".docb"	unicode	12	false
A	0040eb64	u_.docx_004...	unicode u".docx"	u".docx"	unicode	12	false
A	0040eb7c	s_WANACRY!	ds "WANACRY!"	"WANACRY!"	string	9	true
A	0040eb88	u_%s\\%s_0...	unicode u"%s\\%s"	u"%s\\%s"	unicode	12	false
A	0040eb94	s_CloseHand...	ds "CloseHandle"	"CloseHandle"	string	12	true
A	0040eba0	s_DeleteFile...	ds "DeleteFileW"	"DeleteFileW"	string	12	true
A	0040ebac	s_MoveFileE...	ds "MoveFileExW"	"MoveFileExW"	string	12	true
A	0040ebb8	s_MoveFileW...	ds "MoveFileW"	"MoveFileW"	string	10	true
A	0040ebc4	s_ReadFile_...	ds "ReadFile"	"ReadFile"	string	9	true
A	0040ebd0	s_WriteFile_...	ds "WriteFile"	"WriteFile"	string	10	true
A	0040ebdc	s_CreateFile...	ds "CreateFileW"	"CreateFileW"	string	12	true
A	0040ebe8	s_kernel32.d...	ds "kernel32.dll"	"kernel32.dll"	string	13	true
A	0040f08c	s_Microsoft_...	ds "Microsoft Enhanced R...	"Microsoft Enhanced RSA and AES C...	string	54	true
A	0040f0c4	s_CryptGenK...	ds "CryptGenKey"	"CryptGenKey"	string	12	true
A	0040f0d0	s_CryptDecr...	ds "CryptDecrypt"	"CryptDecrypt"	string	13	true
A	0040f0e0	s_CryptEncr...	ds "CryptEncrypt"	"CryptEncrypt"	string	13	true
A	0040f0f0	s_CryptDest...	ds "CryptDestroyKey"	"CryptDestroyKey"	string	16	true
A	0040f100	s_CryptImpo...	ds "CryptImportKey"	"CryptImportKey"	string	15	true
A	0040f110	s_CryptAcqu...	ds "CryptAcquireContextA"	"CryptAcquireContextA"	string	21	true
A	0040f3f8	PTR_Rsrc_XI...	addr Rsrc_XIA_00a_409[32...	u"%s\\Intel"	unicode	18	true
A	0040f40c	PTR_Rsrc_XI...	addr Rsrc_XIA_00a_409[32...	u"%s\\ProgramData"	unicode	30	true
A	0040f42c	s_cmd.exe /...	ds "cmd.exe /c \"%s\""	"cmd.exe /c \"%s\""	string	16	false

Filter:

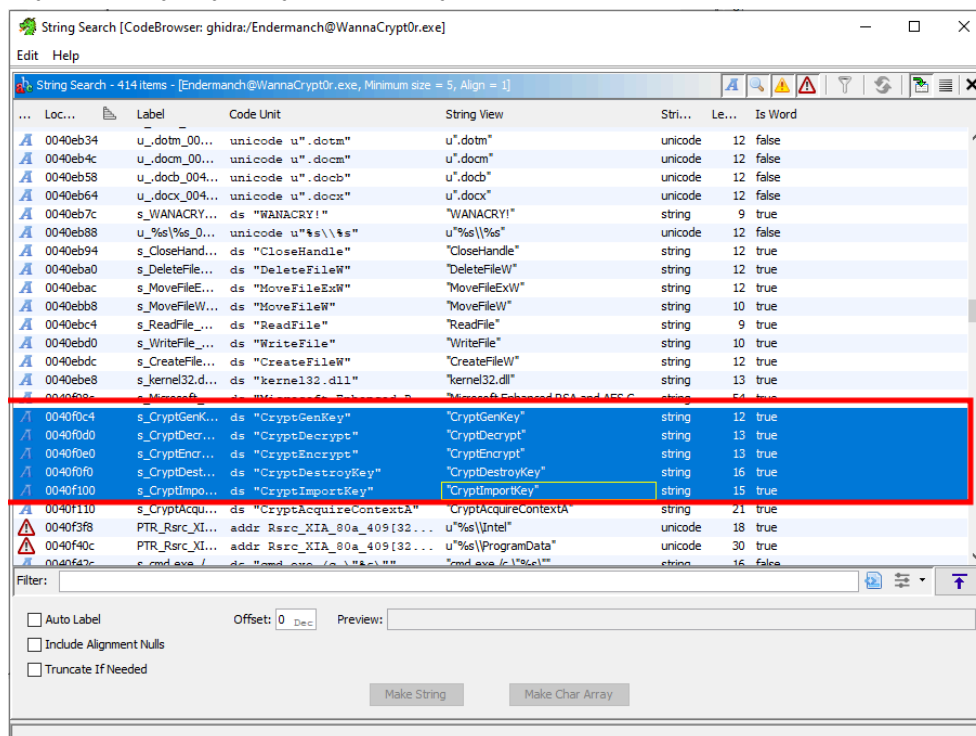
☐ Auto Label Offset: Dec Preview:

☐ Include Alignment Nulls

☐ Truncate If Needed

Fonctions utilisées pour le chiffrement

On peut voir que les fonctions utilisés sont CryptGenKey , CryptDecrypt , CryptEncrypt , CryptDestroyKey , CryptImportKey



Extensions de fichiers ciblées

On peut voir dans le ghidra qu'il cible différents fichiers comme les .mp4 ,.jpeg .iso .png etc

Location	String Value	String Representation	Data Type
0040e714	.avi	u".avi"	unicode
0040e720	.mov	u".mov"	unicode
0040e72c	.mp4	u".mp4"	unicode
0040e738	.3gp	u".3gp"	unicode
0040e744	.mkv	u".mkv"	unicode
0040e750	.3g2	u".3g2"	unicode
0040e75c	.flv	u".flv"	unicode
0040e768	.wma	u".wma"	unicode
0040e774	.mid	u".mid"	unicode
0040e780	.m3u	u".m3u"	unicode
0040e78c	.m4u	u".m4u"	unicode
0040e798	.djvu	u".djvu"	unicode
0040e7a4	.svg	u".svg"	unicode
0040e7b8	.psd	u".psd"	unicode
0040e7c4	.nef	u".nef"	unicode
0040e7d0	.tiff	u".tiff"	unicode
0040e7dc	.tif	u".tif"	unicode
0040e7e8	.cgm	u".cgm"	unicode
0040e7f4	.raw	u".raw"	unicode
0040e800	.gif	u".gif"	unicode
0040e80c	.png	u".png"	unicode
0040e818	.bmp	u".bmp"	unicode
0040e824	.jpg	u".jpg"	unicode
0040e830	.jpeg	u".jpeg"	unicode
0040e83c	.vcd	u".vcd"	unicode
0040e848	.iso	u".iso"	unicode
0040e854	.hackun	u".hackun"	unicode

soit tous ca en résumé

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

URLs contactées par le malware

quand on lance le malware dans un sandbox on remarque que le malware crée un fichier c.wnry

lorsque l'on fait un cat on voit des liens en .onion , ce sont de sites sur darkweb accessible via tor

gx115p7dumjmoqi1pwkphjjcrdfjnxj6lrngx7ekbenv2riucmf.onion

57g7spgrzlojinan.onion

xxlvbrloxvriy2c5.onion

76jdd2ir2embyav4.onion

cwnhwhlz5maq7.onion

https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip

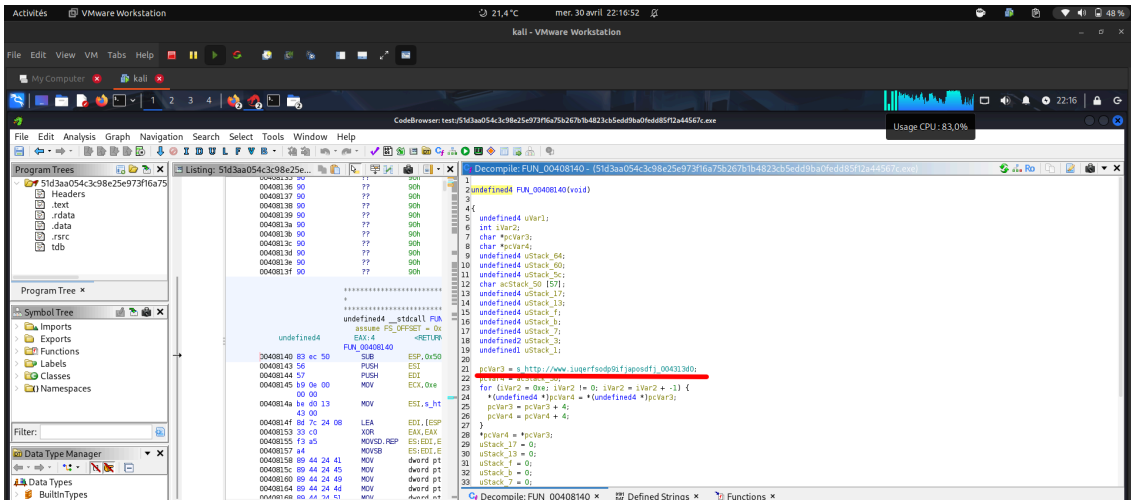
```
MINGW64:/c/Users/maliki/Documents/MalwareDatabase/ransomwares/WannaCrypt0r  
maliki@DESKTOP-UHVM5RN MINGW64 ~/Documents/MalwareDatabase/ransomwares/WannaCrypt0r  
$ cat c.wnry  
hC115p7UMMngoj1pMvkpHijcRdfJNXj6LrLNgx7ekbenv2riucmf.onion;57g7spgrzlojinan.onion;xxlvbrloxvriy2c5.onion;76jdd2ir2embyav47.onion;cwnhwhlz5maq7.onion;https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip
```

Méthode d'arrêt du malware

Le malware est connu pour avoir un kill switch mais comment trouvé ce kill switch ?
grace a strings our peste il est affiché directement

```
(kali@kali)-[~/Téléchargements]  
$ pestr 51d3aa054c3c98e25e973f16a75b267b1b4823cb5edd9ba0fedd85f12a44567c.exe |grep http  
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwff.com  
<head><meta http-equiv="content-type" content="text/html; charset=  
<asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">  
^[[A  
(kali@kali)-[~/Téléchargements]  
$ strings 51d3aa054c3c98e25e973f16a75b267b1b4823cb5edd9ba0fedd85f12a44567c.exe |grep http  
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwff.com  
<asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">  
(kali@kali)-[~/Téléchargements]
```

On le retrouve également dans le ghidra lorsque que l'on va dans l'entré principale on remarque que le lien du kill switch est présent



on le retrouve également sur le wireshark dans les requêtes DNS lors de l'attaque

1	0.000000	192.168.253.133	192.168.253.132	DNS	84 Standard query 0x53d3 A win10.ipv6.microsoft.com
2	0.000181	192.168.253.132	192.168.253.133	DNS	100 Standard query response 0x53d3 A 192.168.253.132
3	0.973896	192.168.253.133	192.168.253.132	DNS	109 Standard query 0x6f1f A www.iuqerfsodp9ifajaposdfjhgosurijfaewrwergrwea.com
4	0.974025	192.168.253.132	192.168.253.133	DNS	125 Standard query response 0x011f A 192.168.253.132
5	0.981195	192.168.253.133	192.168.253.132	TCP	66 49573 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

Propagation du malware

Lorsque l'on lance le malware et que l'on effectue une capture Wireshark sur le réseau de la VM, on remarque qu'il envoie des requêtes via SMB à toutes les adresses IP du réseau local en incrémentant les numéros d'hôtes. Cela est visible à travers les requêtes ARP.

568	40.390618	00:0c:29:4c:2e:38	ff:ff:ff:ff:ff:ff	ARP	60 Who has 192.168.253.148? Tell 192.168.253.133
569	40.390619	00:0c:29:4c:2e:38	ff:ff:ff:ff:ff:ff	ARP	60 Who has 192.168.253.149? Tell 192.168.253.133
570	40.390621	00:0c:29:4c:2e:38	ff:ff:ff:ff:ff:ff	ARP	60 Who has 192.168.253.150? Tell 192.168.253.133
571	40.390622	00:0c:29:4c:2e:38	ff:ff:ff:ff:ff:ff	ARP	60 Who has 192.168.253.151? Tell 192.168.253.133
572	40.390684	00:0c:29:4c:2e:38	ff:ff:ff:ff:ff:ff	ARP	60 Who has 192.168.253.152? Tell 192.168.253.133
573	40.408250	192.168.253.133	221.84.158.168	TCP	66 49814 > 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
574	40.436948	192.168.253.133	192.168.253.132	DNS	84 Standard query 0x747b A win10.ipv6.microsoft.com
575	40.437058	192.168.253.132	192.168.253.133	DNS	100 Standard query response 0x747b A 192.168.253.132
576	40.467830	192.168.253.133	96.34.190.214	TCP	66 49815 > 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
577	40.468504	00:0c:29:4c:2e:38	ff:ff:ff:ff:ff:ff	ARP	60 Who has 192.168.253.165? Tell 192.168.253.133
578	40.593390	192.168.253.133	164.224.16.13	TCP	66 49819 > 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
579	40.629970	192.168.253.1	224.0.0.251	MDNS	82 Standard query 0x0000 PTR googlecast.tcp.local, "QU" question
580	40.640082	192.168.253.133	133.98.196.239	TCP	66 49820 > 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
581	40.656304	00:0c:29:4c:2e:38	ff:ff:ff:ff:ff:ff	ARP	60 Who has 192.168.253.166? Tell 192.168.253.133
582	40.781612	00:0c:29:4c:2e:38	ff:ff:ff:ff:ff:ff	ARP	60 Who has 192.168.253.167? Tell 192.168.253.133

Portefeuilles Bitcoin utilisés

Les 3 portefeuilles bitcoin utilisés sont ici

Defined Strings - 381 items				
Location	String Value	String Representation	Data Type	
0040eb58	.docb	u".docb"	unicode	
0040eb64	.docx	u".docx"	unicode	
0040eb70	.doc	u".doc"	unicode	
0040eb7c	WANACRY!	"WANACRY!"	ds	
0040eb88	%s\\%s	u"%s\\%s"	unicode	
0040eb94	CloseHandle	"CloseHandle"	ds	
0040eba0	DeleteFileW	"DeleteFileW"	ds	
0040ebac	MoveFileExW	"MoveFileExW"	ds	
0040ebb8	MoveFileW	"MoveFileW"	ds	
0040ebc4	ReadFile	"ReadFile"	ds	
0040ebd0	WriteFile	"WriteFile"	ds	
0040ebdc	CreateFileW	"CreateFileW"	ds	
0040ebe8	kernel32.dll	"kernel32.dll"	ds	
0040f08c	Microsoft Enhanced RSA and AES Cr...	"Microsoft Enhanced RSA and AES C...	ds	
0040f0c4	CryptGenKey	"CryptGenKey"	ds	
0040f0d0	CryptDecrypt	"CryptDecrypt"	ds	
0040f0e0	CryptEncrypt	"CryptEncrypt"	ds	
0040f0f0	CryptDestroyKey	"CryptDestroyKey"	ds	
0040f100	CryptImportKey	"CryptImportKey"	ds	
0040f110	CryptAcquireContextA	"CryptAcquireContextA"	ds	
0040f120	end of file "0x"	"end of file "0x"	ds	
0040f440	115p7UMMngoj1pMvkpHijcRdfJNXj6...	"115p7UMMngoj1pMvkpHijcRdfJNXj6..."	ds	
0040f464	12t9YDPgwueZ9NyMgw519p7AA8isj...	"12t9YDPgwueZ9NyMgw519p7AA8isj..."	ds	
0040f488	13AM4VW2dhxYgXeQepoHkHSQuy6...	"13AM4VW2dhxYgXeQepoHkHSQuy6..."	ds	
0040f4b4	Global\WslWinZonesCacheCounterMu...	Global\WslWinZonesCacheCounter...	ds	
0040f4d8	tasksche.exe	"tasksche.exe"	ds	
0040f4e8	TaskStart	"TaskStart"	ds	

```
Decompile: FUN_00401e9e - (ed01ebfbc9eb5bbea545af4d...  
1  
2 void FUN_00401e9e(void)  
3  
4 {  
5     int iVar1;  
6     undefined local_31c [178];  
7     char local_26a [602];  
8     char *local_10 [3];  
9  
10    local_10[0] = s_13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb_0040f488;  
11    local_10[1] = s_12t9YDPgwueZ9NyMgw519p7AA8isjr6S_0040f464;  
12    local_10[2] = s_115p7UMMngoj1pMvkpHijcRdfJNXj6Lr_0040f440;  
13    iVar1 = FUN_00401000(local_31c,1);  
14    if (iVar1 != 0) {  
15        iVar1 = rand();  
16        strcpy(local_26a,local_10[iVar1 % 3]);  
17        FUN_00401000(local_31c,0);  
18    }  
19    return;  
20 }  
21
```

