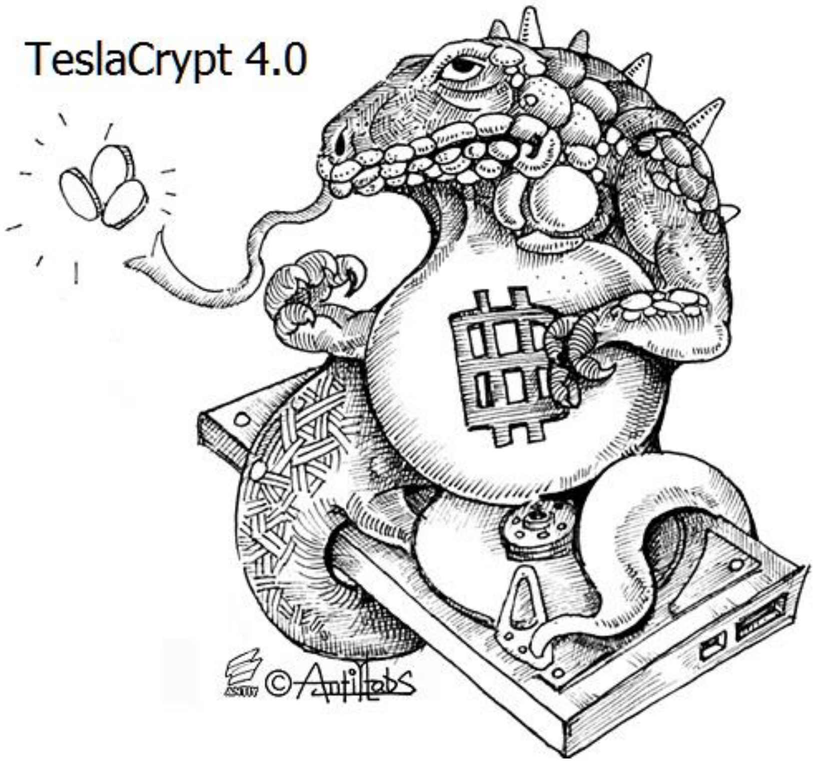
TECHNOLOGICAL AND CHARACTERISTIC ANALYSIS OF NEW VARIANT OF RANSOMWARE FAMILY TESLACRYPT

Antiy CERT



First Edition: 17:44, Apr.7, 2016

Pub Date: 14:23, Apr.8, 2016

Update: 10:07, Apr.8, 2016

Content

1 Introduction

Antiy CERT recently found a new variant of ransomware TeslaCrypt, named TeslaCrypt 4.0, it has many characteristics, such as: do not modify the original file name after encryption, against security tools, own a PDB path, self-start through CMD, use unconventional function call, the same domain name can download multiple ransomware, etc. In particular, common ransomware will modify the extensions of encrypted files after infecting victim hosts, such as TeslaCrypt early version (.vvv,.mp3,.ccc、.abc,.ttt, etc), other ransomware Locky, CTB-Locker（.Locky，.oinpgca）. But the latest variant of TeslaCrypt will do not modify the original file name extensions after encryption.

Ransomware TeslaCrypt was found in February, 2015 [1] which is modified on the basis of Cryptolocker. In its first version, TeslaCrypt claimed to use asymmetric encryption algorithm RSA - 2048, but it actually used symmetrical AES encryption algorithm, and then Cisco released a decryption tool that can decrypt files that is encrypted by TeslaCrypt when key. dat file is found [2];But in the subsequent multiple versions, ransomware TeslaCrypt began to use asymmetric RSA encryption algorithm and the encrypted files cannot decrypt without a key. Antiy CERT found that TeslaCrypt 4.0 emerges in March 2016 and use RSA - 4096 encryption algorithm.

The emergence of ransomware is associated with many factors, and one important factor is the high maturity of anonymous Internet and anonymous payment. After the Spring Festival of 2016, ransomware Locky started to outbreak and many global security vendors have released corresponding reports. Antiy CERT also released “the first Bitcoin ransomware ‘Locky’ with Chinese prompts” [3]. At the end of March 2016, G-data and Trend Micro released the report of Petya ransomware that modifies MBR and encrypts entire hard disk; In early April 2016, Antiy CERT began to track ransomware TeslaCrypt 4.0.

2 Transmitting ways

Ransomware TeslaCrypt uses website drive-by download and E-mail to transmit. Drive-by download is rarely used in domestic, but browser vulnerabilities (Chrome, Firefox, Internet Explorer), Flash vulnerabilities and Adobe Reader vulnerabilities are common ways to transmit; And E-mail is often used to transmit ransomware and multiple ransomware events found by Antiy CERT are also transmitted by E-mail.

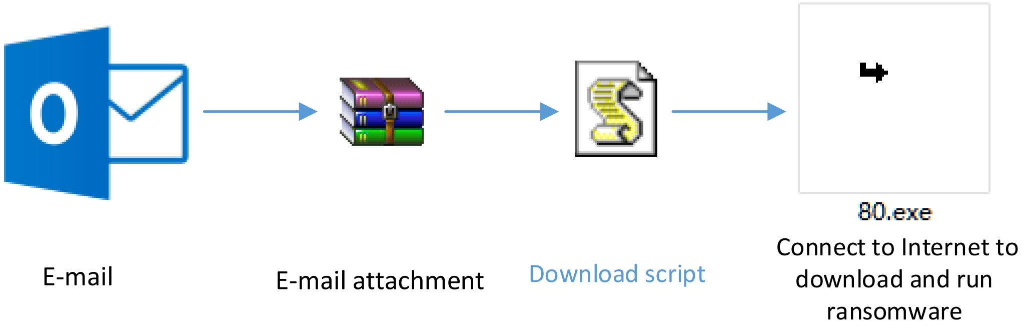


Figure 1 Ransomware transmitted by E-mail

When analyzing TeslaCrypt download addresses, Antiy CERT researchers found that multiple TeslaCrypt 4.0 programs are stored in the same domain name, and file HASH is not identical. For example, domain name http://***pasqq.com can download the TeslaCrypt 4.0 address, as follows:

```
http://***pasqq.com/23.exe
http://***pasqq.com/24.exe
http://***pasqq.com/25.exe
http://***pasqq.com/42.exe
http://***pasqq.com/45.exe
http://***pasqq.com/48.exe
http://***pasqq.com/69.exe
http://***pasqq.com/70.exe
http://***pasqq.com/80.exe
http://***pasqq.com/85.exe
http://***pasqq.com/87.exe
http://***pasqq.com/93.exe
```

In addition, the ransomware addresses in other domain names are the same as above, such as: 23.exe, 24.exe, 25.exe … 93.exe. To April 7, 2016, 14, Antiy CERT found more than 50 domain names with ransomware TeslaCrypt 4.0, part of which have expired.

Part of domain names that can download ransomware TeslaCrypt 4.0:

```
***pasqq.com
***uereqq.com
***ghsqq.com
***rulescc.asia
***rulesqq.com
```

3 Sample analysis

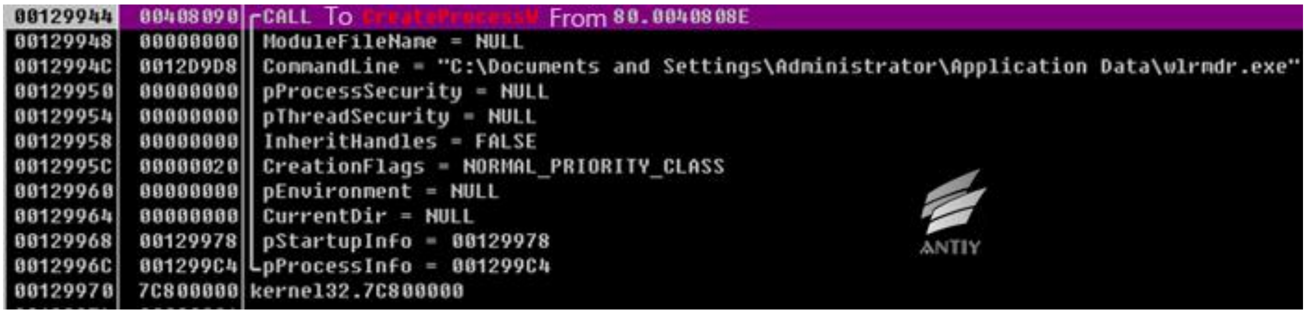
Antiy CERT had found nearly 300 ransomware TeslaCrypt 4.0 in total. The researchers analyzed some newly found samples.

3.1 Sample label

Virus name	Trojan[Ransom]/Win32.Teslacrypt
Original file name	80.exe
MD5	30CB7DB1371C01F930309CDB30FF429B
Processor framework	X86-32
File size	396 KB (405,504 byte)
File format	BinExecute/Microsoft.EXE[:X86]
Timestamp	5704939E -->2016-04-06 12:42:06
Digital signature	NO
Shell	NO
Compiled language	Microsoft Visual C++
VT first upload time	2016-04-06 04:07:00 UTC
VT detect result	28/57

3.2 Use RSA4096 encryption algorithm to encrypt files, but do not modify original file name

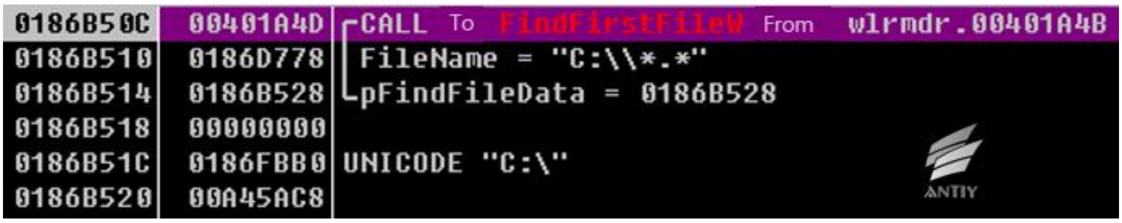
After being executed, it will copy itself to % Application Data % folder, renamed as wlrmdr.exe, set itself property as hiding, and then use CreateProcessW to create process.



```
00129944  00408090 ┌CALL To CreateProcessW From 00.0040808E
00129948  00000000 │ModuleFileName = NULL
0012994C  0012D9D8 │CommandLine = "C:\Documents and Settings\Administrator\Application Data\wlrmdr.exe"
00129950  00000000 │pProcessSecurity = NULL
00129954  00000000 │pThreadSecurity = NULL
00129958  00000000 │InheritHandles = FALSE
0012995C  00000020 │CreationFlags = NORMAL_PRIORITY_CLASS
00129960  00000000 │pEnvironment = NULL
00129964  00000000 │CurrentDir = NULL
00129968  00129978 │pStartupInfo = 00129978
0012996C  001299C4 └pProcessInfo = 001299C4
00129970  7C800000 kernel32.7C800000
```

Figure 2 Create wlrmdr.exe process

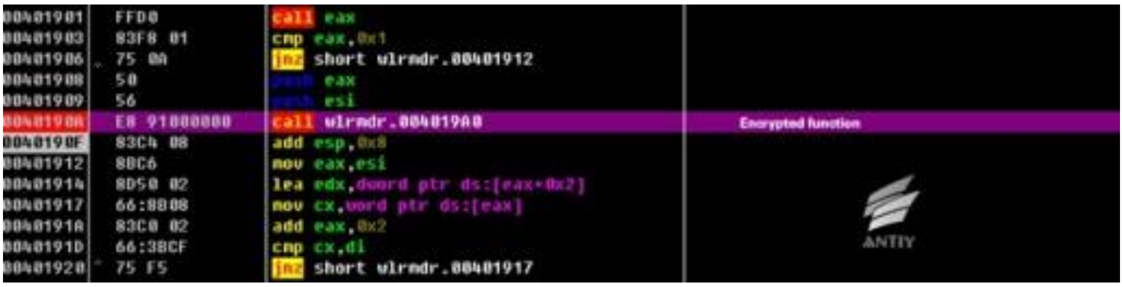
The samples use CreateThreadt to start thread and encrypt all files in disk in the newly created process. First, samples use GetLogicalDriveStringsW to obtain all logical drives and use FindFirstFileW and FindNextFileW to traverse all files and encrypt.



```
0186B50C  00401A4D  ┌CALL To FindFirstFileW From wlrmdr.00401A4B
0186B510  0186D778  │FileName = "C:\\*.*"
0186B514  0186B528  └pFindFileData = 0186B528
0186B518  00000000
0186B51C  0186FBB0  UNICODE "C:\"
0186B520  00A45AC8
```

Figure 3 Traverse files in disk

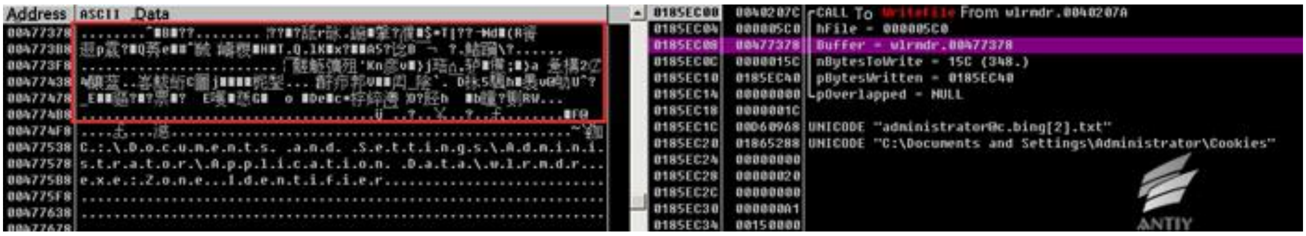
The encrypted function address is 0x0040190A.



```
00401901   FFD0          call eax
00401903   83F8 01       cmp eax,0x1
00401906   75 0A         jnz short wlrmdr.00401912
00401908   50            push eax
00401909   56            push esi
0040190A   E8 91000000   call wlrmdr.004019A0        Encrypted function
0040190F   83C4 08       add esp,0x8
00401912   8BC6          mov eax,esi
00401914   8D50 02       lea edx,dword ptr ds:[eax+0x2]
00401917   66:8B08       mov cx,word ptr ds:[eax]
0040191A   83C0 02       add eax,0x2
0040191D   66:3BCF       cmp cx,di
00401920   75 F5         jnz short wlrmdr.00401917
```

Figure 4 Encrypt the traversed files by calling encrypted function

After encrypting with RSA4096 algorithm, it calls WriteFile to write the encrypted data to the file without modifying file name.

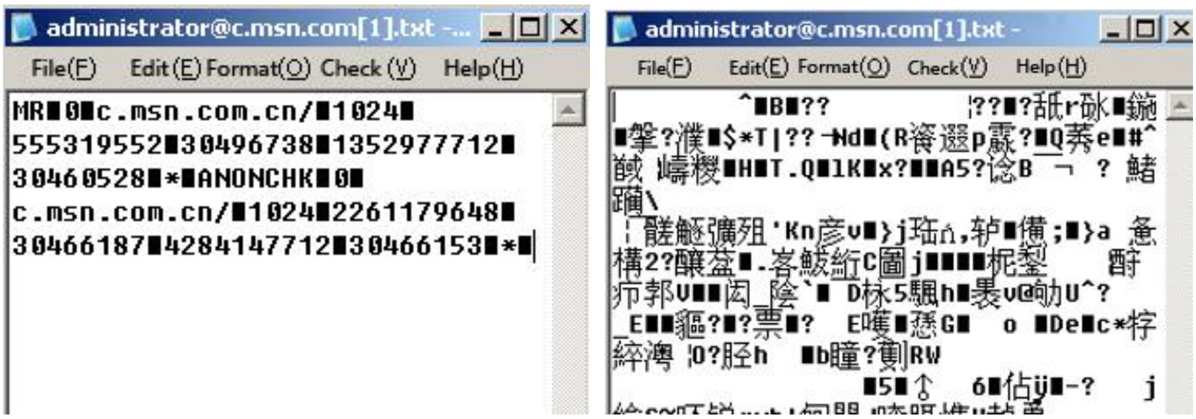


```
Address   ASCII Data
00477378  .........^■B■??.........!??■?舐r砯.鎓■挚?濮■$*T|??-Hd■(R徬
004773B8  遐p覈?■Q莠e■■^虢 嶹樱■H■T.Q.1K■x?■■A5?讫B ¬ ?.鯺躎\?......
004773F8  ...........................┌鞋艇 獷殂'Kn彦v■}j瑶ሰ,轳■儶;■}a 毳構2亿
00477438  ■醾蓋..峇鲅绗C圖j■■■■栀梨... 酐疖郱v■■闵_陰`. D栐5颿h■褬v@劬U^?
00477478  _E■■貙?■?禀■?  E嚄■瑟G■  o ■De■c*梓綷湾 ?0?胫h  ■b瞳?剸RW...
004774B8  ..............................ÿ ..?..X..?..ŧ..........■FØ
004774F8  ....ᠮ...漶.............................................~鎦
00477538  C.:.\.D.o.c.u.m.e.n.t.s. .a.n.d. .S.e.t.t.i.n.g.s.\.A.d.m.i.n.i.
00477578  s.t.r.a.t.o.r.\.A.p.p.l.i.c.a.t.i.o.n. .D.a.t.a.\.w.l.r.m.d.r...
004775B8  e.x.e.:.Z.o.n.e...I.d.e.n.t.i.f.i.e.r.............................
004775F8  ..................................................................
00477638  ..................................................................
00477678
```

```
0185EC00  0040207C  ┌CALL To WriteFile From wlrmdr.0040207A
0185EC04  000005C0  │hFile = 000005C0
0185EC08  00477378  │Buffer = wlrmdr.00477378
0185EC0C  0000015C  │nBytesToWrite = 15C (348.)
0185EC10  0185EC40  │pBytesWritten = 0185EC40
0185EC14  00000000  └pOverlapped = NULL
0185EC18  0000001C
0185EC1C  00D60968  UNICODE "administrator@c.bing[2].txt"
0185EC20  01865288  UNICODE "C:\Documents and Settings\Administrator\Cookies"
0185EC24  00000000
0185EC28  00000020
0185EC2C  00000000
0185EC30  000000A1
0185EC34  00150000
```

Figure 5 Write the encrypted data into file

The comparison of encrypted files:



administrator@c.msn.com[1].txt -...
File(F) Edit(E) Format(O) Check(V) Help(H)
administrator@c.msn.com[1].txt -
File(F) Edit(E) Format(O) Check(V) Help(H)

```
MR■0■c.msn.com.cn/■1024■
555319552■30496738■1352977712■
30460528■*■ANONCHK■0■
c.msn.com.cn/■1024■2261179648■
30466187■4284147712■30466153■*■
```

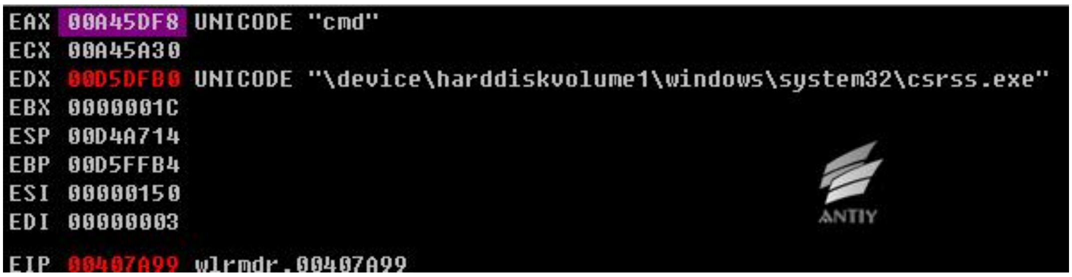
```
        ^■B■??          !??■?舐r砯■鏑
■挚?濮■$*T|??-Hd■(R徬遐p覈?■Q莠e■#^
虢 嶹樱■H■T.Q■1K■x?■■A5?讫B  ¬  ? 鯺
躎\
 ┌鞋艇獷殂'Kn彦v■}j瑶ሰ,轳■儶;■}a 毳
構2?醾蓋■.峇鲅绗C圖j■■■■栀梨     酐
疖郱v■■闵_陰`■ D栐5颿h■褬v@劬U^?
_E■■貙?■?禀■?  E嚄■瑟G■  o ■De■c*梓
綷湾 ?0?胫h  ■b瞳?剸RW
           ■5■ᠮ    6■佔ÿ■-?     j
```

Figure 6 The comparison of encrypted files

3.3 Confrontation security tools

The sample would check whether the system contains process with strings and hide the process so that the users cannot find these tools:

"taskmg "	*Task manager*
"regedi "	*Registry manager*
"procex "	*Process analysis tool*
"msconfi "	*System configuration*
"cmd "	*Command Prompt*



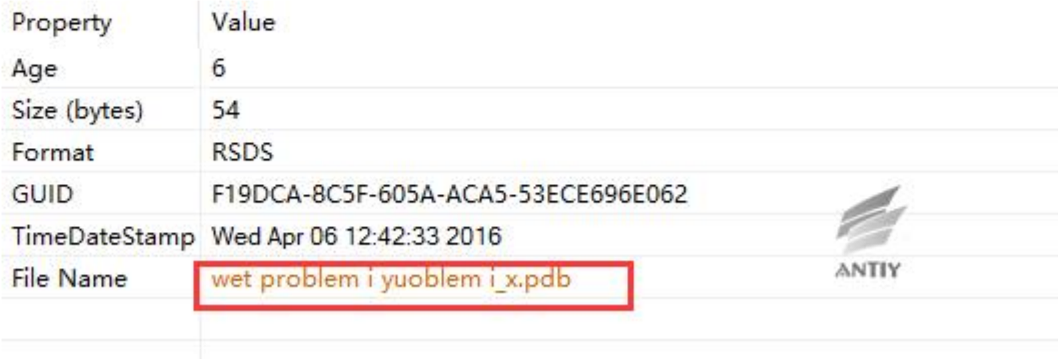
```
EAX 00A45DF8 UNICODE "cmd"
ECX 00A45A30
EDX 00D5DFB0 UNICODE "\device\harddiskvolume1\windows\system32\csrss.exe"
EBX 0000001C
ESP 00D4A714
EBP 00D5FFB4
ESI 00000150
EDI 00000003

EIP 00407A99 wlrmdr.00407A99
```

Figure 7 Hide cmd interface

3.4 With PDB information

The sample has PDB information with the file name "wet problem i yuoblem i_x.pdb".

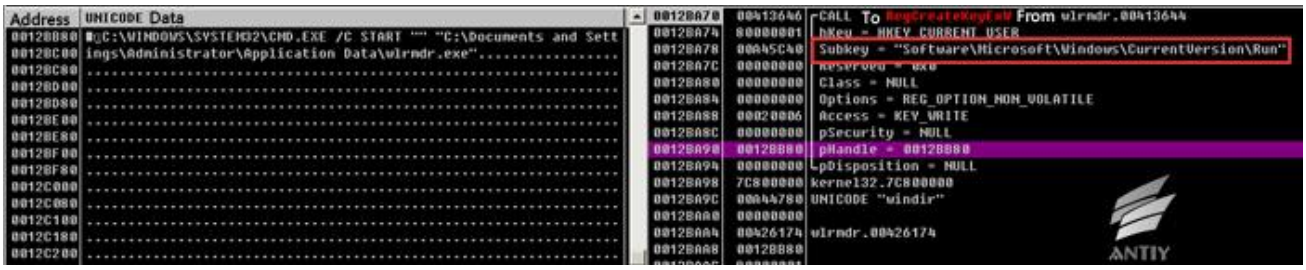


Property	Value
Age	6
Size (bytes)	54
Format	RSDS
GUID	F19DCA-8C5F-605A-ACA5-53ECE696E062
TimeDateStamp	Wed Apr 06 12:42:33 2016
File Name	wet problem i yuoblem i_x.pdb

Figure 8 The debugging information of sample contains PDB information

3.5 Use CMD start-up

The sample calls RegCreateKeyExW, using CMD to start its own code to be written into the registry. Therefore, it can be started with the powerboot.



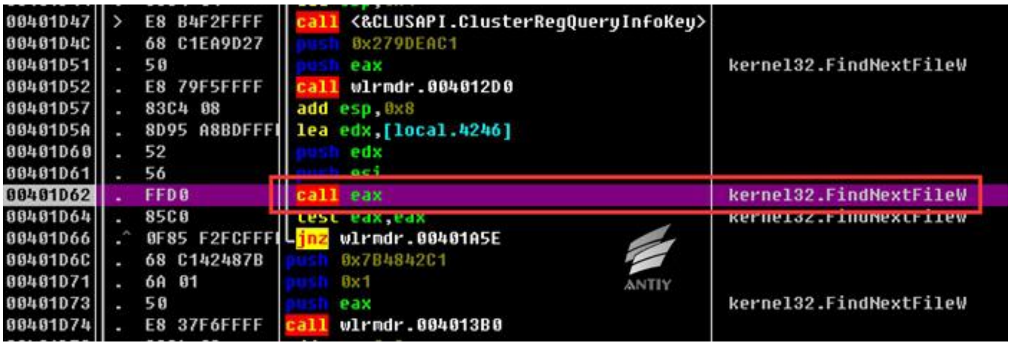
```
Address   UNICODE Data
0012BB80  ■▯C:\WINDOWS\SYSTEM32\CMD.EXE /C START "" "C:\Documents and Sett
0012BC00  ings\Administrator\Application Data\wlrmdr.exe"...................
0012BC80  ................................................................
0012BD00  ................................................................
0012BD80  ................................................................
0012BE00  ................................................................
0012BE80  ................................................................
0012BF00  ................................................................
0012BF80  ................................................................
0012C000  ................................................................
0012C080  ................................................................
0012C100  ................................................................
0012C180  ................................................................
0012C200  ................................................................
```

```
0012BA70  00413646  ┌CALL To RegCreateKeyExW From wlrmdr.00413644
0012BA74  80000001  │hKey = HKEY_CURRENT_USER
0012BA78  00A45C40  │Subkey = "Software\Microsoft\Windows\CurrentVersion\Run"
0012BA7C  00000000  │Reserved = 0x0
0012BA80  00000000  │Class = NULL
0012BA84  00000000  │Options = REG_OPTION_NON_VOLATILE
0012BA88  00020006  │Access = KEY_WRITE
0012BA8C  00000000  │pSecurity = NULL
0012BA90  0012BB80  │pHandle = 0012BB80
0012BA94  00000000  └pDisposition = NULL
0012BA98  7C800000  kernel32.7C800000
0012BA9C  00A44780  UNICODE "windir"
0012BAA0  00000000
0012BAA4  00426174  wlrmdr.00426174
0012BAA8  0012BB80
```

Figure 9 Use CMD to realize the start-up with powerboot

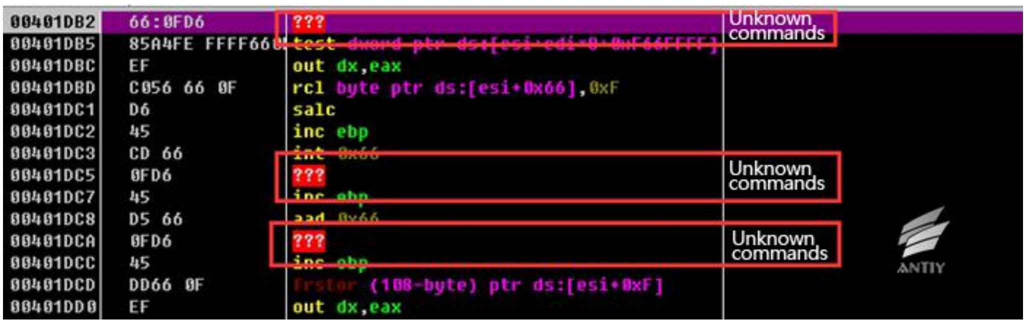
3.6 Use unconventional function call and skip

The sample uses many unconventional function calls and skips to prevent security staff to analyze the virus.



```
00401D47  > E8 B4F2FFFF   call <&CLUSAPI.ClusterRegQueryInfoKey>
00401D4C  . 68 C1EA9D27   push 0x279DEAC1
00401D51  . 50            push eax                                  kernel32.FindNextFileW
00401D52  . E8 79F5FFFF   call wlrmdr.004012D0
00401D57  . 83C4 08       add esp,0x8
00401D5A  . 8D95 A8BDFFFF lea edx,[local.4246]
00401D60  . 52            push edx
00401D61  . 56            push esi
00401D62  . FFD0          call eax                                  kernel32.FindNextFileW
00401D64  . 85C0          test eax,eax                              kernel32.FindNextFileW
00401D66  .^ 0F85 F2FCFFFF└jnz wlrmdr.00401A5E
00401D6C  . 68 C142487B   push 0x7B4842C1
00401D71  . 6A 01         push 0x1
00401D73  . 50            push eax                                  kernel32.FindNextFileW
00401D74  . E8 37F6FFFF   call wlrmdr.004013B0
```

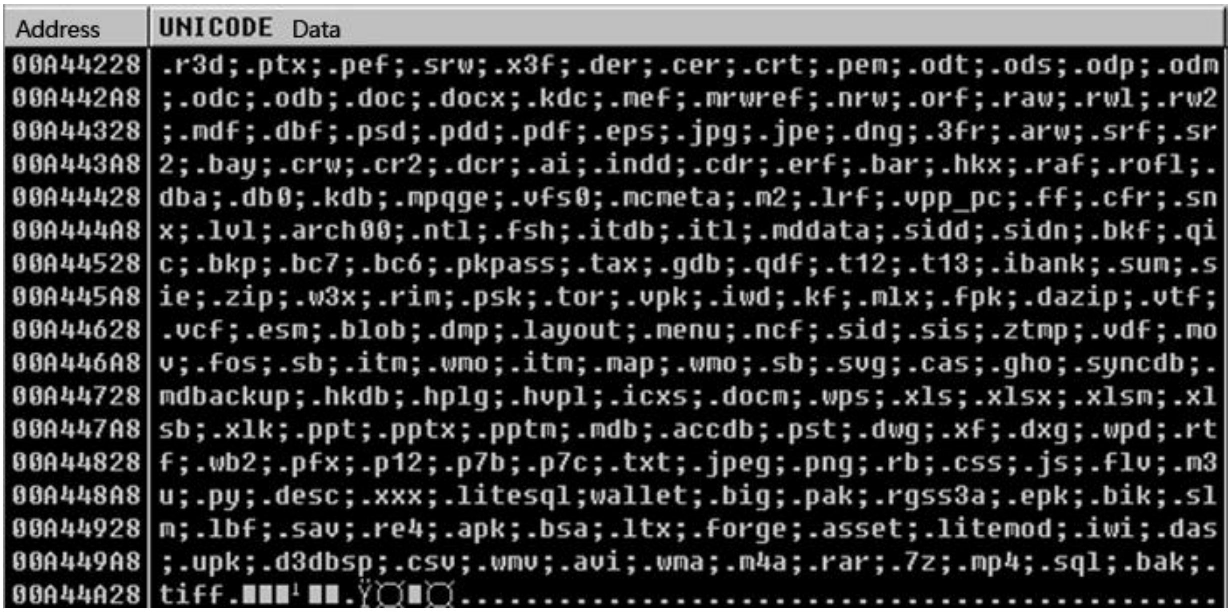
Figure 10 Unconventional function call



```
00401DB2  66:0FD6         ???
00401DB5  85A4FE FFFF660  test dword ptr ds:[esi+edi*8+0xF66FFFF]
00401DBC  EF              out dx,eax
00401DBD  C056 66 0F      rcl byte ptr ds:[esi+0x66],0xF
00401DC1  D6              salc
00401DC2  45              inc ebp
00401DC3  CD 66           int 0x66
00401DC5  0FD6            ???
00401DC7  45              inc ebp
00401DC8  D5 66           aad 0x66
00401DCA  0FD6            ???
00401DCC  45              inc ebp
00401DCD  DD66 0F         frstor (108-byte) ptr ds:[esi+0xF]
00401DD0  EF              out dx,eax
```

Figure 11 Unconventional skip

3.7 The encrypted file format of TeslaCrypt 4.0



```
Address   UNICODE Data
00A44228 .r3d;.ptx;.pef;.srw;.x3f;.der;.cer;.crt;.pem;.odt;.ods;.odp;.odm
00A442A8 ;.odc;.odb;.doc;.docx;.kdc;.mef;.mrwref;.nrw;.orf;.raw;.rwl;.rw2
00A44328 ;.mdf;.dbf;.psd;.pdd;.pdf;.eps;.jpg;.jpe;.dng;.3fr;.arw;.srf;.sr
00A443A8 2;.bay;.crw;.cr2;.dcr;.ai;.indd;.cdr;.erf;.bar;.hkx;.raf;.rofl;.
00A44428 dba;.db0;.kdb;.mpqge;.vfs0;.mcmeta;.m2;.lrf;.vpp_pc;.ff;.cfr;.sn
00A444A8 x;.lvl;.arch00;.ntl;.fsh;.itdb;.itl;.mddata;.sidd;.sidn;.bkf;.qi
00A44528 c;.bkp;.bc7;.bc6;.pkpass;.tax;.gdb;.qdf;.t12;.t13;.ibank;.sum;.s
00A445A8 ie;.zip;.w3x;.rim;.psk;.tor;.vpk;.iwd;.kf;.mlx;.fpk;.dazip;.vtf;
00A44628 .vcf;.esm;.blob;.dmp;.layout;.menu;.ncf;.sid;.sis;.ztmp;.vdf;.mo
00A446A8 v;.fos;.sb;.itm;.wmo;.itm;.map;.wmo;.sb;.svg;.cas;.gho;.syncdb;.
00A44728 mdbackup;.hkdb;.hplg;.hvpl;.icxs;.docm;.wps;.xls;.xlsx;.xlsm;.xl
00A447A8 sb;.xlk;.ppt;.pptx;.pptm;.mdb;.accdb;.pst;.dwg;.xf;.dxg;.wpd;.rt
00A44828 f;.wb2;.pfx;.p12;.p7b;.p7c;.txt;.jpeg;.png;.rb;.css;.js;.flv;.m3
00A448A8 u;.py;.desc;.xxx;.litesql;wallet;.big;.pak;.rgss3a;.epk;.bik;.sl
00A44928 m;.lbf;.sav;.re4;.apk;.bsa;.ltx;.forge;.asset;.litemod;.iwi;.das
00A449A8 ;.upk;.d3dbsp;.csv;.wmv;.avi;.wma;.m4a;.rar;.7z;.mp4;.sql;.bak;.
00A44A28 tiff.■■■¹■■.ÿ¤■¤...................................
```

Figure 12 3.7 The encrypted file format of TeslaCrypt 4.0

4 Summary

The ransomware poses great threats to both individual users and enterprises. The encrypted files cannot be restored, which will bring great loses for users. If you want to solve the threat problems of ransomware, you should install security products, protection and backup products. In addition, users should pay more attention to the mails that they have received, open the email attachments or click the links carefully, especially the emails from strangers.

Antiy Intelligent Endpoint Protection System (IEP) can prevent the ransomware from encrypting files when users clicked to operate the ransomware by mistake.

Antiy Threat Analysis System (PTA) can identify unknown ransomware automatically.

Appendix 1: References

[1] Uncovering the Face of Ransomware

http://www.antiy.net/p/uncovering-the-face-of-ransomware/

[2] http://www.freebuf.com/sectool/66060.html

http://blogs.cisco.com/security/talos/teslacrypt

[3] First Bitcoin ransomware with chinese prompts“locky”

http://www.antiy.net/p/first-bitcoin-ransomware-with-chinese-promptslocky/

Appendix 2: More than 50 domains that spread ransomware found by Antiy CERT

marvellrulescc.asia	witchbeherеqq.com	ohelloguymyff.com
arendroukysdqq.com	isityouereqq.com	joecockerhereff.com
blablaworldqq.com	jeansowghsqq.com	howisittomorrowff.com
fromjamaicaqq.com	marvellrulesqq.com	giveitalltheresqq.com
goonwithmazerqq.com	greetingseuropasqq.com	giveitallhereqq.com
gutentagmeinliebeqq.com	grandmahereqq.com	ohelloguyzzqq.com
hellomississmithqq.com	mafiawantsyouqq.com	jeansowghtqq.com
hellomisterbiznesqq.com	spannflow.com	grandaareyoucc.asia
hellomydearqq.com	ohelloguyqq.com	imgointoeatnowcc.com
helloyoungmanqq.com	bonjovijonqq.com	washitallawayff.com
howareyouqq.com	joecockerhereqq.com	greetingsjamajcaff.com
invoiceholderqq.com	itsyourtimeqq.su	hpalsowantsff.com
itisverygoodqq.com	blizzbauta.com	ohellowruff.com
lenovomaybenotqq.com	yesitisqqq.com	ohelloweuqq.com
lenovowantsyouqq.com	thisisitsqq.com	ujajajgogoff.com
mafianeedsyouqq.com	soclosebutyetqq.com	ohiyoungbuyff.com
mommycantakeff.com	isthereanybodyqq.com	helloyungmenqq.com
thisisyourchangeqq.com	ohelloguyff.com	

Appendix 3: The C&C address found by Antiy CERT

addagapublicschool.com/binfile.php

kel52.com/wp-content/plugins/ajax-admin/binstr.php

closerdaybyday.info/wp-content/plugins/google-analytics-for-wordpress/vendor/composer/installers/tests/Composer/Installers/Test/binfile.php

coldheartedny.com/wp-content/plugins/wordpress-mobile-pack/libs/htmlpurifier-4.6.0/library/HTMLPurifier/DefinitionCache/Serializer/URI/binfile.php

thejonesact.com/wp-content/themes/sketch/binfile.php

theoneflooring.com/wp-content/themes/sketch/binfile.php

mahmutersan.com.tr/wp-content/plugins/contact-form-maker/images/02/03/stringfile.php

myredhour.com/blog//wp-content/themes/berlinproof/binstr.php

controlfreaknetworks.com/dev/wp-content/uploads/2015/07/binstr.php

sappmtraining.com/wp-includes/theme-compat/wcspng.php

controlfreaknetworks.com/dev/wp-content/uploads/2015/07/wcspng.php

vtechshop.net/wcspng.php

sappmtraining.com/wp-includes/theme-compat/wcspng.php

shirongfeng.cn/images/lurd/wcspng.php

198.1.95.93/~deveconomytravel/cache/binstr.php

helpdesk.keldon.info/plugins/editors/tinymce/jscripts/tiny_mce/plugins/inlinepopups/skins/clearlooks2/img/binfile.php

hotcasinogames.org/binfile.php

goldberg-share.com/wp-content/plugins/contact-form-7/includes/js/jquery-ui/themes/smoothness/images/binfile.php

opravnatramvaji.cz/modules/mod_search/wstr.php

studiosundaytv.com/wp-content/themes/sketch/binfile.php

theoneflooring.com/wp-content/themes/sketch/binfile.php

hotcasinogames.org/binfile.php

pcgfund.com/binfile.php

kknk-shop.dev.onnetdigital.com/stringfile.php

forms.net.in/cgi-bin/stringfile.php

casasembargada.com/wp-content/plugins/formcraft/php/swift/lib/classes/Swift/Mime/HeaderEncoder/stringfile.php

csskol.org/wp-content/plugins/js_composer/assets/lib/font-awesome/src/assets/font-awesome/fonts/stringfile.php

grosirkecantikan.com/wp-content/plugins/contact-form-7/includes/js/jquery-ui/themes/smoothness/images/binarystings.php

naturstein-schubert.de/modules/mod_cmscore/stringfile.php

vtc360.com/wp-content/themes/vtc360_maxf3d/ReduxFramework/ReduxCore/inc/extensions/wbc_importer/demo-data/Demo2/binarystings.php

starsoftheworld.org/cgi-bin/binarystings.php

holishit.in/wp-content/plugins/wpclef/assets/src/sass/neat/grid/binarystings.php

minteee.com/images/binstr.phpnewculturemediablog.com/wp-includes/fonts/wstr.php

drcordoba.com/components/bstr.php

Appendix 4: About Antiy

Starting from antivirus engine research and development team, Antiy now has developed into an advanced security product supplier with four research and development centers, nationwide detection and monitoring ability as well as products and services covering multiple countries. With a fifteen-year continual accumulation, Antiy has formed massive security knowledge and promoted advanced products and solutions against APT with integrated application of network detection, host defense, unknown threat identification, data analysis and security visual experiences. With the recognition of technical capacity by industry regulators, customers and partners, Antiy has consecutively awarded qualification of national security emergency support unit four times and one of the six of CNNVD first-level support units. Antiy detection engine for mobile is the first Chinese product that obtained the first AV – TEST (2013) annual awards and more than ten of the world's famous security vendors choose Antiy as their detection partner.

More information about antivirus engine: http://www.antiy.net