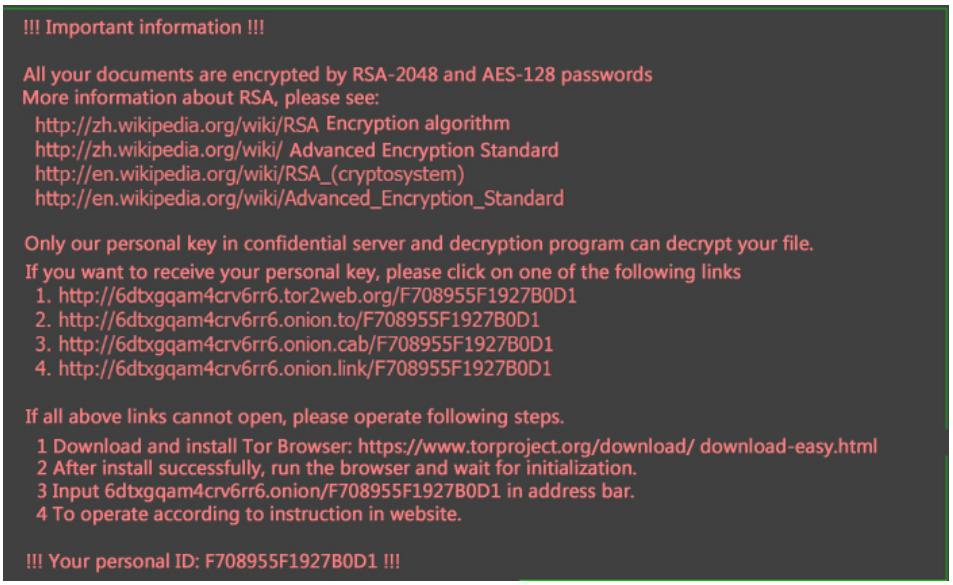
FIRST BITCOIN RANSOMWARE WITH CHINESE PROMPTS "LOCKY"

Antiy CERT



First Edition: 9:26, Feb.18, 2016

Pub Date: 14:04, Feb.19, 2016

Update: 14:04, Feb.19, 2016

Content

1 INTRODUCTION 3
2 SAMPLE ANALYSIS 3
2.1 SAMPLE LABELS 3
2.2 SAMPLE FUNCTIONS 3
2.3 RELATED TECHNIQUE 4
3 CONCLUSION 8
APPENDIX 1: REFERENCES 9
APPENDIX 2: ABOUT ANTIY 9
APPENDIX 3: LOG OF DOCUMENT UPDATE 10

1 Introduction

Antiy CERT found a new kind of ransomware named "Locky" that can encrypt more than 100 kinds of file types through RSA-2048 and AES-128 algorithm, meanwhile, release a ransomware prompt file named _Locky_recover_instructions. txt in every directory with encrypted files. Antiy CERT researchers found that it is a kind of ransomware that transmits by spam mail and is the first Bitcoin ransomware with Chinese prompts.

2 Sample analysis

2.1 Sample labels

Virus name	Trojan/Win32.Locky.a
Original file name	ladybi.exe
MD5	FB6CA1CD232151D667F6CD2484FEE8C8
Processor framework	X86-32
File size	180 KB (184,320 byte)
File format	BinExecute/Microsoft.EXE[:X86]
Timestamp	42B63E17->2005-06-20 11:55:03
Digital signature	NO
Shell	NO
Compiled language	Microsoft Visual C++ 6.0
VT first update time	2016-02-16 10:53:39
VT detect result	41/55

2.2 Sample functions

This ransomware "Locky" racketeers users by kidnapping user data. It encrypts more than 100 kinds of fil e types through RSA-2048 and AES-128 algorithm and release a ransomware prompt file named _Locky_r ecover_instructions. txt in every directory with encrypted files.

"Locky" sample's local behavior: copy itself to system temporary directory %Temp%, and rename as svchost; traverse the files in system, determine whether the file suffix is in the built-in sample list, if it is, encrypt the samples; create prompt file _Locky_recover_instructions.txt in many folders; create file _Locky_recover_instructions.bmp in desktop; And set this file as the desktop background and prompt users how to successfully restore the encrypted files; Add relevant registry keys; Delete system restore snapshot.

- ✓ **copy itself to svchost.exe in %Temp% directory and add startup.**

✓ **The encrypted types are as follows:**

.m4u .m3u .mid .wma .flv .3g2 .mkv .3gp .mp4 .mov .avi .asf .mpeg .vob .mpg .wmv .fla .swf .wav .mp3 .qcow2 .vdi .vmdk .vmx .gpg .aes .ARC .PAQ .tar.bz2 .tbk .bak .tar .tgz .gz .7z .rar .zip .djv .djvu .svg .bmp .png .gif .raw .cgm .jpeg .jpg .tif .tiff .NEF .psd .cmd .bat .sh .class .jar .java .rb .asp .cs .brd .sch .dch .dip .pl .vbs .vb .js .asm .pas .cpp .php .ldf .mdf .ibd .MYI .MYD .frm .odb .dbf .db .mdb .sql .SQLITEDB .SQLITE3 .asc .lay6 .lay .ms11 .sldm .sldx .ppsm .ppsx .ppam .docb .mml .sxm .otg .odg .uop .potx .potm .pptx .pptm .std .sxd .pot .pps .sti .sxi .otp .odp .wb2 .123 .wks .wk1 .xltx .xltm .xlsx .xlsm .xlsb .slk .xlw .xlt .xlm .xlc .dif .stc .sxc .ots .ods .hwp .602 .dotm .dotx .docm .docx .DOT .3dm .max .3ds .xml .txt .CSV .uot .RTF .pdf .XLS .PPT .stw .sxw .ott .odt .DOC .pem .p12 .csr .crt .key

✓ **Do not encrypt files that contains path and file name that contain the following string:**

tmp, Application Data, AppData, Program Files (x86), Program Files, temp, thumbs.db, $Recycle.Bin, System Volume Information, Boot, Windows

✓ **"Locky" registers that added**

HKCU\Software\Locky

HKCU\Software\Locky\id

HKCU\Software\Locky\pubkey

HKCU\Software\Locky\paytext

HKCU\Software\Locky\completed

HKCU\Control Panel\Desktop\Wallpaper "%UserProfile%\Desktop_Locky_recover_instructions.bmp"

✓ **Delete system restoring snapshot**

Delete all Shadow Copies in whole disk through calling vssadmin.exe Delete Shadows /All /Quiet, and make infected system cannot restore by them.

✓ **Internet behavior:**

- Send part information of infected machine to C&C server.
- Download RSA public key from C&C server to prepare for the encryption.
- Upload the encrypted file list.
- To obtain corresponding message according to system language from the server.

2.3 Related technique

2.3.1 Domain generation algorithm

"Locky" samples will use function rdtsc to obtain processor time firstly, make the value and some variables modulo operated, and determine whether the samples visits domains generated by algorithm, or directly accesses to the hard-coded IP address, which can make samples randomly to some extent.


```
if ( v416C5C < 0 )
{
  v19 = __rdtsc();
  v17 = (unsigned int)v19 % v18;
}
v20 = v17 % v18;
v416C5C = v17 + 1;
if ( v17 % v18 >= 6 )
{
  s_IP((int)v4179FC + 28 * (v20 - 6), (int)&v54, 0, 0xFFFFFFFF);
}
else
{
  s_DGA((int)&v49, v20);
  LOBYTE(v69) = 6;
  sub_4053E2(v21);
  sub_405A83(v22, 1);
}
```

Figure 1 Domain name generation algorithm

The generation of Domain name needs a random number which is conducted according to the date that machine got infected.

```
v23 = 0;
GetSystemTime(&SystemTime);
v3 = __ROR4__(0xB11924E1 * (SystemTime.wYear + 0x1BF5), 5);
v4 = __ROR4__(0xB11924E1 * (v3 + ((unsigned int)SystemTime.wDay >> 1) + 0x27100001), 5);
v5 = __ROR4__(0xB11924E1 * (v4 + SystemTime.wMonth + 0x2709A354), 5);
v6 = __ROL4__(a2 % 6, 21);
v7 = __ROR4__(0xB11924E1 * (v5 + v6 + 0x27100001), 5);
v25 = v7 + 0x27100001;
seed = (v7 + 0x27100001) % 0xBu + 5;
sub_40547C();
v24 = 0;
if ( seed )
{
  do
  {
    v9 = __ROL4__(v25, v2);
    v10 = v20;
    v11 = __ROR4__(-1323752223 * v9, 5);
    v12 = v11 + 655360001;
    v25 = v12;
```

Figure 2 Random value calculation

2.3.2 C&C server

The victim host and server interact with HTTP Post request. The victim host visits main.php in C&C server. Parameters are as follows:

Parameters	Meaning
id	Randomly generated number
act	C&C control server
affid	VIP ID

lang	Language used by computer
corp	Unknown
serv	Unknown
os	Operating system
sp	Fixpack
x64	Whether 64-bit system or not

All requests by victimized hosts are encrypted by hard-coded key in sample and sent to C&C server after encryption. The receive packets are encrypted in the same specific encryption and "Locky" will firstly decrypt operation after receiving encrypted data.

Part information about encrypted packet:

Figure 3 Content of packet

Encryption algorithm when sends packets:


```
if ( *((_DWORD *)lpOptional + 4) )
{
  do
  {
    v7 = *((_DWORD *)lpOptional + 5);
    if ( v7 < 0x10 )
      v8 = lpOptional;
    else
      v8 = *(_BYTE **)lpOptional;
    v9 = v8[v6];
    if ( v7 < 0x10 )
      v10 = lpOptional;
    else
      v10 = *(_BYTE **)lpOptional;
    v11 = __ROR4__(phProv, 5);
    v12 = __ROL4__(v6, 13);
    v10[v6] = v9 ^ (v11 - v12);
    v13 = __ROL4__(v9, v6 & 0x1F);
    v14 = __ROR4__(phProv, 1);
    v15 = v14 + v13;
    v16 = __ROR4__(v6++, 23);
    phProv = (v16 + 0x53702F68) ^ v15;
  }
  while ( v6 < *((_DWORD *)lpOptional + 4) );
}
```

Figure 4 Encryption algorithm

Decryption algorithm of samples when receiving data:

```
v24 = 0;
v25 = 0xAFF49754;
while ( v24 < v58 )
{
  v26 = (int *)v56;
  if ( v59 < 0x10 )
    v26 = &v56;
  v27 = __ROL4__(v25, 3);
  v28 = *((_BYTE *)v26 + v24) - v24 - v27;
  v29 = (int *)v56;
  if ( v59 < 0x10 )
    v29 = &v56;
  *((_BYTE *)v29 + v24) = v28;
  v30 = __ROR4__(v28, 11);
  v31 = __ROL4__(v25, 5);
  v25 = v25 + (v24++ ^ v31 ^ v30) - 0x47CB0D2F;
}
```

Figure 5 Decryption algorithm

2.3.3 Control command

There are four control commands at present, namely, **stats, getkey, report, gettext**.

Command	Function

stats	Send some basic information, such as the number of successfully encrypted files, number and length of files that fail to encrypt.
getkey	RSA public key that used to download encryption from the server.
report	Send encrypted file list to server.
gettext	Obtain information that prompts user how to decrypt, C&C server will return the corresponding language prompt information according to computer language that sent back, such as: send back zh will return Chinese, send back en will return English.

The prompt in Chinese:

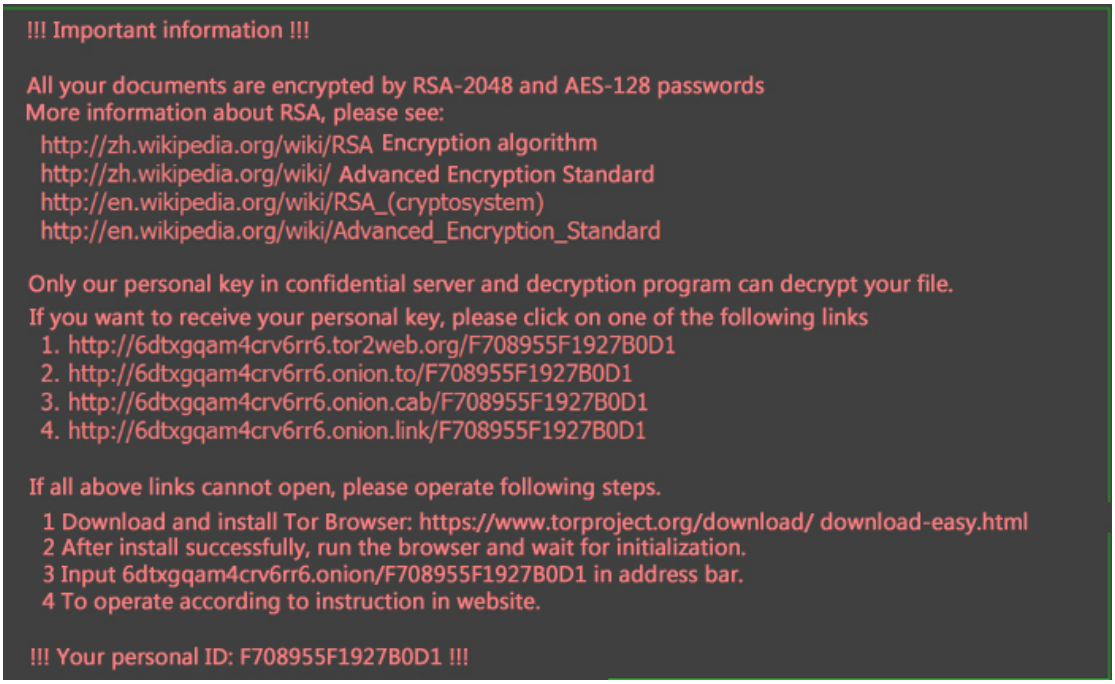


Figure 5 Prompt content

3 Conclusion

Through the analysis of Antiy CERT, the function of ransomware "Locky" is basically identical as the function of ransomware that analyzed before [1]. Ransomware can bring huge benefits to attackers, because it uses Bitcoin to trade that is difficult to track. Once the users are infected by ransomware, they can only decrypt by payment or discard these files. Antiy CERT reminds mass users that even the payment cannot fully guarantee to completely restore the encrypted files. To prevent data being encrypted, defense of ransomware is essential and users should form good habit of Internet use and do not perform unknown documents.

The purpose of "Locky" is the same as other software, which asks users for money by encrypting user data. What is unlike to other ransomware, it is the first Bitcoin ransomware with a Chinese prompt, showing that targets of ransomware are expanding gradually and will develop more localized versions.

Antiy CERT predicts that China will be attacked more by similar ransomware in future. Therefore, how to defense ransomware becomes one of the important tasks to defend network security.

Appendix 1: References

[1] Uncover of real ransomware

http://www.antiy.com/response/ransomware.html

Appendix 2: 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

Appendix 3: log of document update

Update time	Version	Content
2016-02-18 09:26	V1.0	Writing
2016-02-19 14:04	V1.1	Modification
yyyy-mm-dd 00:00		
yyyy-mm-dd 00:00		