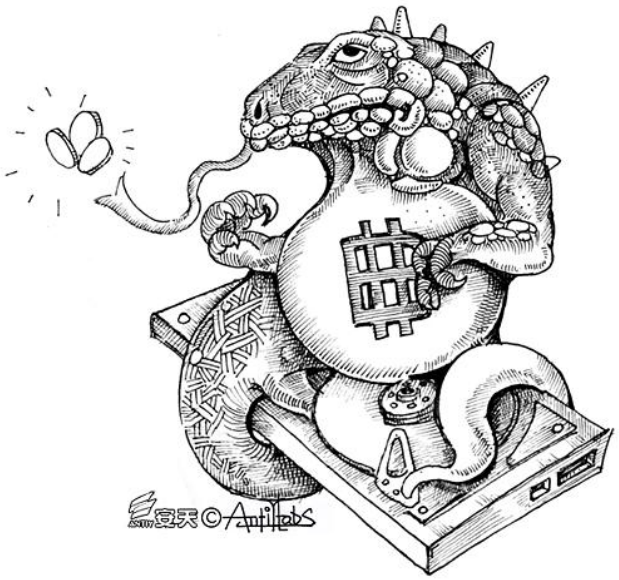
UNCOVERING THE FACE OF RANSOMWARE

——Antiy CERT



CONTENTS

1 Introduction

Recently, more and more security threats posed by ransomware, researchers from Antiy Labs felt obliged to investigate them to uncover the face of ransomware.

September 2013, SecureWorks, the threat response department (CTU) of Dell found a ransomware called CryptoLocker, which was distributed in e-mail attachments, infected computers and encrypted nearly a hundred kinds of files (including spreadsheets, databases , pictures, etc.) and extorted users 300 dollars or 300 euros. It is reported that CryptoLocker had infected 200,000 to 250,000 systems during the first 100 days.

August 2014, *New York Times* reported that about 900,000 Android phones were infected by another ransomware ScarePackage just in a month; it can not only access the camera or the features of your phone, but also pop up messages to accuse you spreading pornography. In order to use you phone normally, you must pay several hundreds of dollars as ransom.

December 2014, researchers from Sophos and ESET found a new ransomware called VirLock or VirRansom, which can self-replicate. It encrypted documents, images, audios, videos and compressed files from compromised computers. In addition, it may lock the screen for copyright infringement and ask for 0.652 Bitcoin (about 159.8US dollars).

If computers are not installed with AV products, they will be infected by traditional virus. In this case, reinstalling operating systems and applications may work. As for the infection of remote control Trojan, users may cut off temporarily to keep safe. However, users will be very sad if the valuable photos on the computers are encrypted by the ransomware. If the encrypted contents are very useful, including thesis with no backup, critical material etc., users have to pay for the ransom. Why can ransomware be so rampant? How does it extort money? What can we do to protect ourselves from this threat? The following part will illustrate these to you. Let's go into the spread means, attack process and defense methods of ransomware.

1.1 What is Ransomware?

Ransomware is a popular kind of Trojan, which can disrupt the normal use of users' data assets and computers resources by harassment, intimidation and even kidnapping user files to extort money from users. The data assets include documents, e-mails, databases, source code, images, and compressed files and so on. The ransom includes real currency, Bitcoin and other virtual currencies. Typically, the author of ransomware will set a specific period for payment, and the number of ransom will be raised over the time. Sometimes, the system still does not work properly and encrypted files are not restored, even if you pay the ransom.

1.2 Main Spread Means

Similar to common Trojans, ransomware are spread by the following ways:

1. spread by web Trojans，once users visit malicious websites, it will be downloaded and run in the background
2. bundle release with other malicious software
3. delivered in the email attachments
4. spread by the removable storage medium

1.3 Signs of Infection

The following behaviors indicate that you have been infected by ransomware:

1. The screens of computers and mobile terminals are locked
2. Disguising as anti-virus software to cheat users to buy the faked AV products
3. Popping up messages as below, saying your files are encrypted, you need to pay some ransom

Figure1 Deceptive message

2 Category

According to the actions of ransomware, it is divided into the following three categories:

1. Affect the normal use of users system. Such as PC Cyborg, QiaoZhaz（Trojan/Win32.QiaoZhaz）etc., they will force users to pay money for normal use of their computers by locking the screen.
2. Intimidate users. Such as FakeAV（Trojan[Ransom]/Win32.FakeAV）etc., they will disguise as anti-virus software to cheat users to buy the faked AV products; Reveton（Trojan[Ransom]/Win32.Foreign）will disguise as law enforcement agencies in the region where users stay, and say they have broken the law to cheat money.
3. Kidnap users' data. This is a common way for current days, and the typical one is CTB-Locker. This malware family（Trojan[Ransom]/Win32.CTBLocker）employs highly sophisticated encryption algorithm to encrypt users' data. Users can not decrypt their data until they pay for the ransom.

Based on specific actions and infected platforms, ransomware includes the following ones:

Result	Action	Platform	Typical Name	Other Name
Affect normal use	Locking screen	Windows	Trojan/Win32.QiaoZhaz	**QiaoZhaz**
		Android	Trojan[rog,sys,fra]/Android.DevLockeer	**DevLockeer**
			Trojan[rog,sys,fra]/Android.Koler	**Koler**
			Trojan[rog,sys,pay]/Android.Locker	**Locker**
	Modifying file associations	Windows	Trojan/Win32.QiaoZhaz	**QiaoZhaz**

Result	Action	Platform	Typical Name	Other Name
	Intercepting phone calls	Android	Trojan[rog,fra,sys]/Android.Cokri	**Cokri**
	Porn popup window	Android	Trojan[rog,sys,fra]/Android.Koler	**Koler**
	Disguising as porn app	Android	Trojan[rog,sys]/Android.simplelock	**simplelock**
Intimidate users	Disguising as AV products	Windows	Trojan[Ransom]/Win32.FakeAV	**FakeAV**
		Android	Trojan[rog,sys]/Android.Svpeng	**Svpeng**
			Trojan[rog,sys]/Android.simplelock	**Simplelock**
	Disguising as law enforcement	Windows	Trojan[Ransom]/Win32.Foreign	**Reveton**
Kidnap user data	Hiding user's files	DOS	Trojan/DOS.AidsInfo	**PC Cyborg**
		Windows	Trojan/Win32.Pluder	**Redplus**
	Deleting user's data	Windows	Trojan/Win32.QiaoZhaz	**QiaoZhaz**
		Android	Trojan[rog,sys,fra]/Android.Koler	**Koler**
	Encrypting user's documents	Windows	Trojan[Ransom]/Win32.CTBLocker	**CTB-Locker**
			Trojan[Ransom]/Win32.Blocker Trojan[Ransom]/Win32.Bitman	**CrytoLocker**
			Trojan[Ransom]/Win32.Locker	**Locker**
		Android	Trojan[rog,sys]/Android.simplelock	**Simplelock**
		Android	Trojan[rog,sys,fra]/Android.Koler	**Koler**
	Encrypting contacts	Android	Trojan[rog,fra,sys]/Android.Cokri	**Cokri**

3 Evolution

3.1 Appearance of Typical Ransomware Families

The earliest known ransomware, named as Trojan/DOS.AidsInfo or PC Cyborg, was designed by Joseph Popp in 1989. This malware is injected into a system as an AIDS Information boot disk, and replaces AUTOEXEC.BAT (a DOS file, locates in the root directory of startup disk, used to describe the commands which are loaded at the system startup) to count when the computers start. Once the system boot times is up to 90 times, the Trojan will hide multiple directories of the disk, and names of all the files in C disk will be encrypted (the system failing in startup). There will be a message popping up on the screen at the moment, saying that the software license has expired and the user needs to pay 189 dollars to Panama for unlocking the system. The author quibbled that this illegal action was for AIDS research when he was indicted.

Trojan[Ransom]/Win32.FakeAV, specialized counterfeit anti-virus software, appeared in 2001, and became popular abroad around 2008. Because its interface was written in English and some domestic anti-virus vendors began using free pricing strategy, it had made little affect in China. FakeAV uses a very deceptive form title during the

cheating period. According to Antiy CERT, it includes over a hundred of titles; the common ones are as bellows:

Form Title
AntiSpyWare2008
AntiVirus2013
Security Defender
ScannRepair
Virus Doctor
Spyware Cleaner
System Care Antivirus
Data Recovery
AVDefender 2014
AVSecurity 2015
Adware Checker

Trojan/Win32.GPcode, a Trojan which can encrypt users' files, appeared in 2005. It can generate warning txt files in the encrypted directories and require the user to purchase a decryption program. The encrypted files include doc, .html, .jpg, .xls, .zip and .rar.

Redplus, coming out in 2006, is the first ransomware in China. It can hide user documents and parcels files, and then pop up a window asking the user to pay ransom into a designated bank account. According to the National Computer Virus Emergency Response Center, there are 581 infections from this malware and its variants. Another ransomware QiaoZhaz emerged in 2007. Once it runs, a message will pop up and say "parts of your files will moved to a locked sector because of using pirated software in your disk, if you want to unlock the files, please contact with liugongs19670519@yahoo.com.cn for purchasing the appropriate software".

3.2 Changes of Payment Method

In the early time, ransom is received by traditionally email, such as Trojan/DOS.AidsInfo will ask victims to email ransom to a designated account. We also observe the malware require victims to pay ransom to a designated bank account such as Trojan/Win32.Pluder, or send messages causing high cost to a designated number such as Trojan[rog,sys,fra]/Android.Koler. The appearance of Bitcoin changes this tradition. Bitcoin can be paid in more subtle ways, so it became a ransomware payment method since 2013. We can say that the appearance of Bitcoin accelerates the speed of ransomware spreading.

3.3 Ransomware for Mobile Terminals

In the late of April 2014, ransomware continued to infect Android system mobile terminals. Koler family, Trojan[rog,sys,fra]/Android.Koler, is an earlier one. Its main actions as following: when the user runs app, it will repeatedly pop up a message saying you are browsing pornographic information, and must pay some money or being punished. For these two years, the most infection rate by ransomware for mobile terminals is in Eastern Europe and Russia, up to 59%; followed by Britain, US and China. The following figure includes the samples of ransomware for mobile terminals around the world captured by Antiy, the number of simplelock.a is almost half of the total.

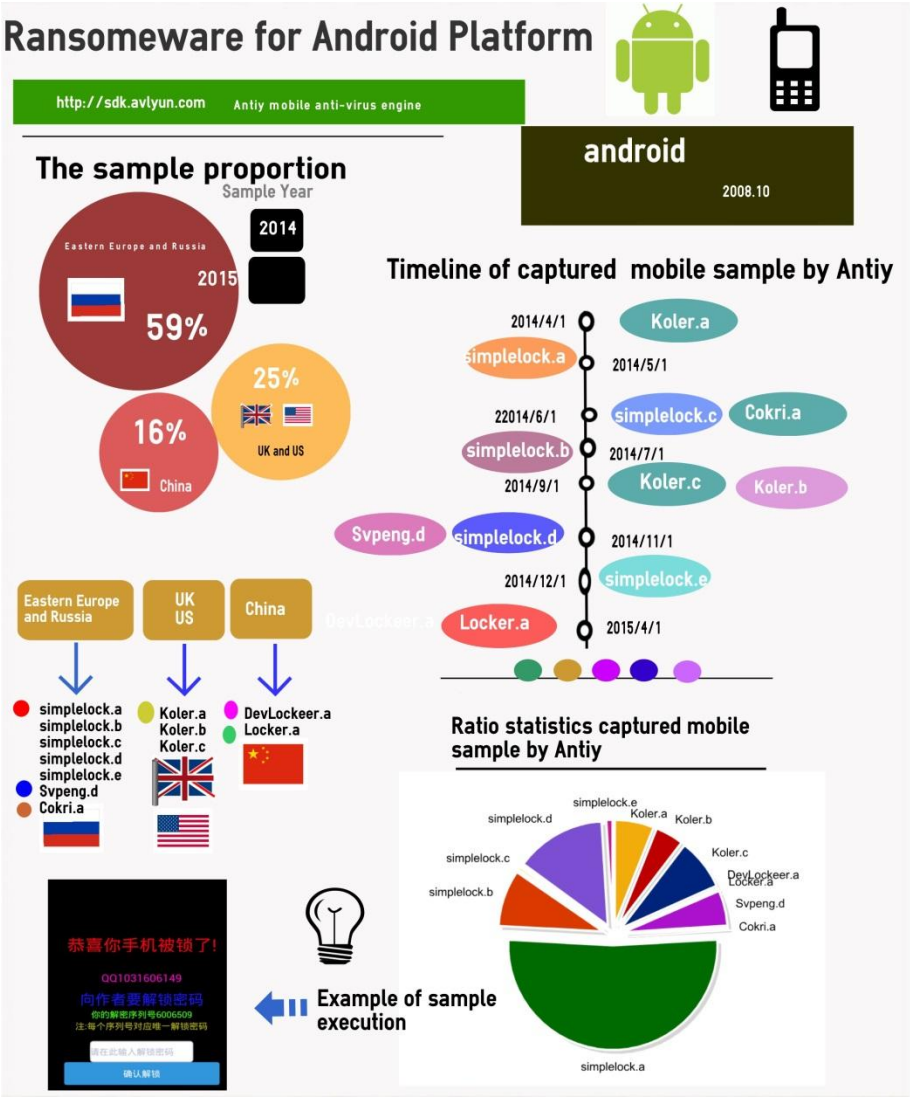


Figure 2 Ransomware for mobile terminals

Typical ransomware for mobile terminals are as follows:

Typical Ransomware for Mobile Terminals		
Home	DevLockeer.a	Set a password for locking screen and extort money
	Locker.a	Top extortion interface and ask users to pay money for unlocking screen
Abroad	Simplelock.a （Eastern Europe and Russia）	Top extortion interface and encrypt files in SD card
	Simplelock.b （Eastern Europe and Russia）	Disguise as AV, require the user to activate the device manager to install; force the extortion interface to the top when the device is running
	Simplelock.c （Eastern Europe and Russia）	Extort money for unlocking screen and encrypt the files in SD card
	Simplelock.d （Eastern Europe and Russia）	Disguise as porn apps and force the extortion interface to the top
	Simplelock.e （Eastern Europe and Russia）	Activate the device manager and top extortion interface

	Svpeng.d （ Eastern Europe and Russia）	Disguise as AV and pop up FBI ransomware interface, take photos of the user and upload device information, top certain interfaces forcibly
	Koler.a（Britain and US）	Unlock the screen and pop up warning message for browsing porn websites
	Koler.b（Britain and US）	Popup window repeatedly, delete system data and all the SD card files, force to set new password for screen lock
	Koler.c（Britain and US）	Pop up warning message for browsing porn websites
	Cokri.a（Eastern Europe and Russia）	Disguise as hot apps，intercept calls and cancel ringtone, encrypt contact, then extort money

3.4 New Threat Trends

January 2015, the variant of Cryptowall family was observed communicating via I2P anonymous network and infected 288 victims in a day. It asked the user to pay Bitcoin after encrypting their data and stole Bitcoin simultaneously. TeslaCrypt and Alpha Crypt respectively appearing in February and April, were observed exploiting the Flash vulnerability recently patched by Adobe, which is also used by CTB-Locker, CryptoWall, TorrentLocker, BandarChor and Angler etc. Among these malware, the most noteworthy one is CTB-Locker. It employs escape techniques to avoid being detected.

April 30th 2015, we received an attachment containing CTB-Locker from our user. The user told us he had submitted it to a third party sandbox, and suspected it was specialized in office systems made in China. Having analyzed the email, we found out it did not target Chinese office systems. With the increasing rampancyof ransomware and the new vectors of attacking, this phenomenon cannot be excluded. Most of current ransomware mainly exploit social engineering ways to send mass emails, however, the contents of them are very deceptive, it is too hard to open it. For instance, Threatpost reports that CTB_Locker has begun to spread by sending emails with the subject of “Upgrade to Windows 10 for free”.

3.5 Summary

From AIDS Information Trojan to Locker, it spans over 20 years. Though more and more ransomware continuously emerge, they mainly kidnap users’ data for ransom. The following figure shows the evolution of ransomware from 1989 to 2015, several important times are marked on the left. We can conclude that kinds of ransomware for mobile terminals are increasing over the popularity of Android, and so as of the kinds of that ask victims to pay in the form of Bitcoin.

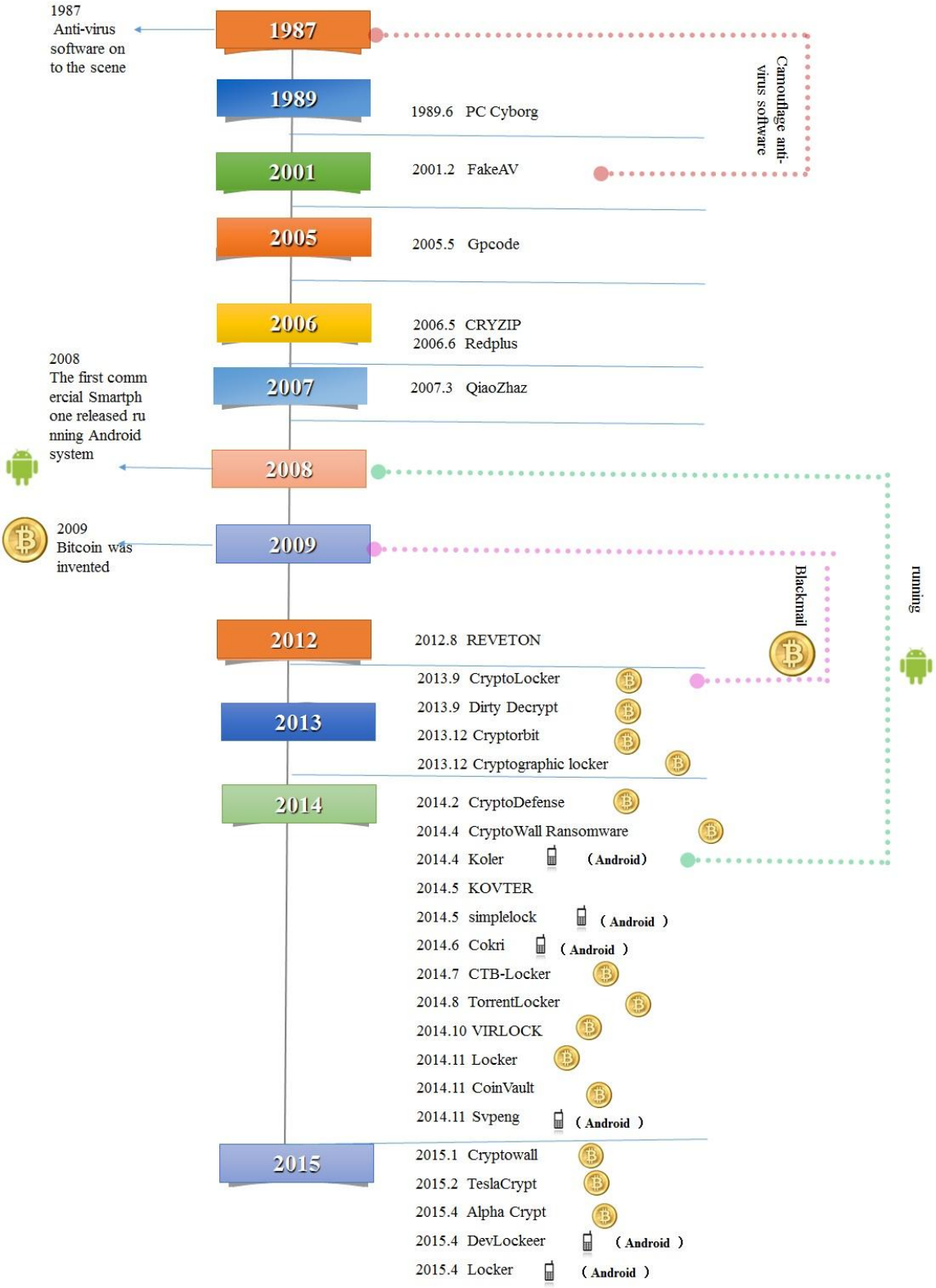


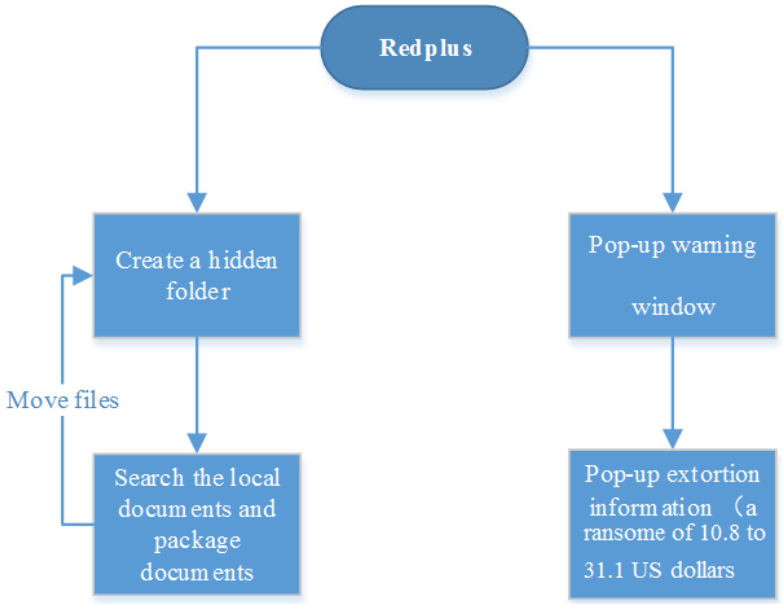
Figure 3 Evolution of ransomware

4 Analysis of Typical Ransomware

Actually, ransomware is a kind of Trojan. We will take typical ransomware for example, describe the attacking process and uncover their faces.

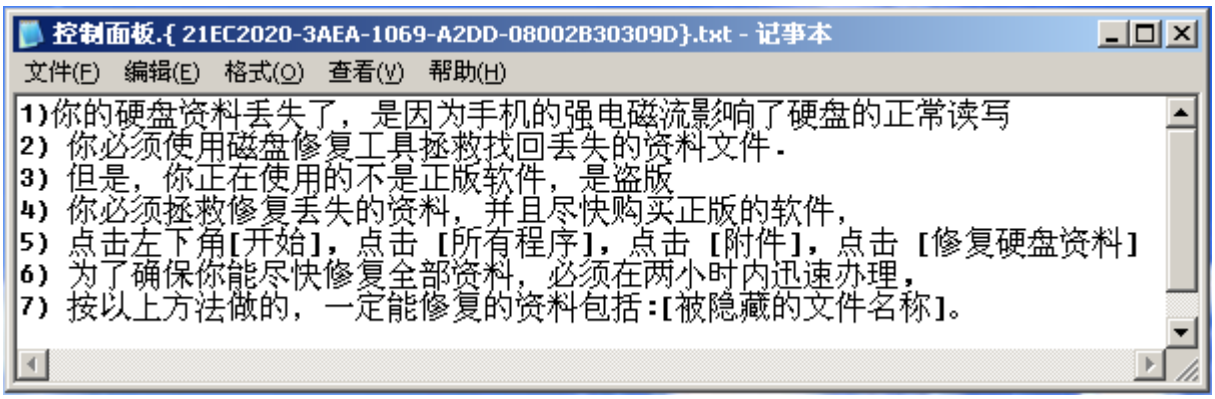
4.1 Redplus

On June 9, 2006, Antiy captured a Trojan called Redplus, which is the first racketeer Trojan in China. It can hide users' document files and asks the ransom from 10.8 to 31.1 US dollars. Once Redplus runs in target systems, the faked dialog box will pop up. Clicking the button OK, then you will see the window for ransom. The main process is as follows:



Redplus asks some money among 70 to 200, and requires the number of money edited into a designated message and then sent it out. For example, the number is 70; the content of the designated message is 00000012020901100006101O#70.

The deceptive tips generated by Redplus like bellows:



The literal meaning of the picture is:

1. The electromagnetic flow is too strong for your cellphone to be used normally, and leads to the loss of your disk data;

2. You must use some repair tools to recover the lost data files;

3. However, the software you are using is pirated but not legitimate;

4. You must repair the lost data and buy legal software;

5. Click the Start button lower left, then choose All Programs-Attachment-Repair disk data;

6. You must finish above work within two hours, or you may not get all the lost data repaired as soon as possible;

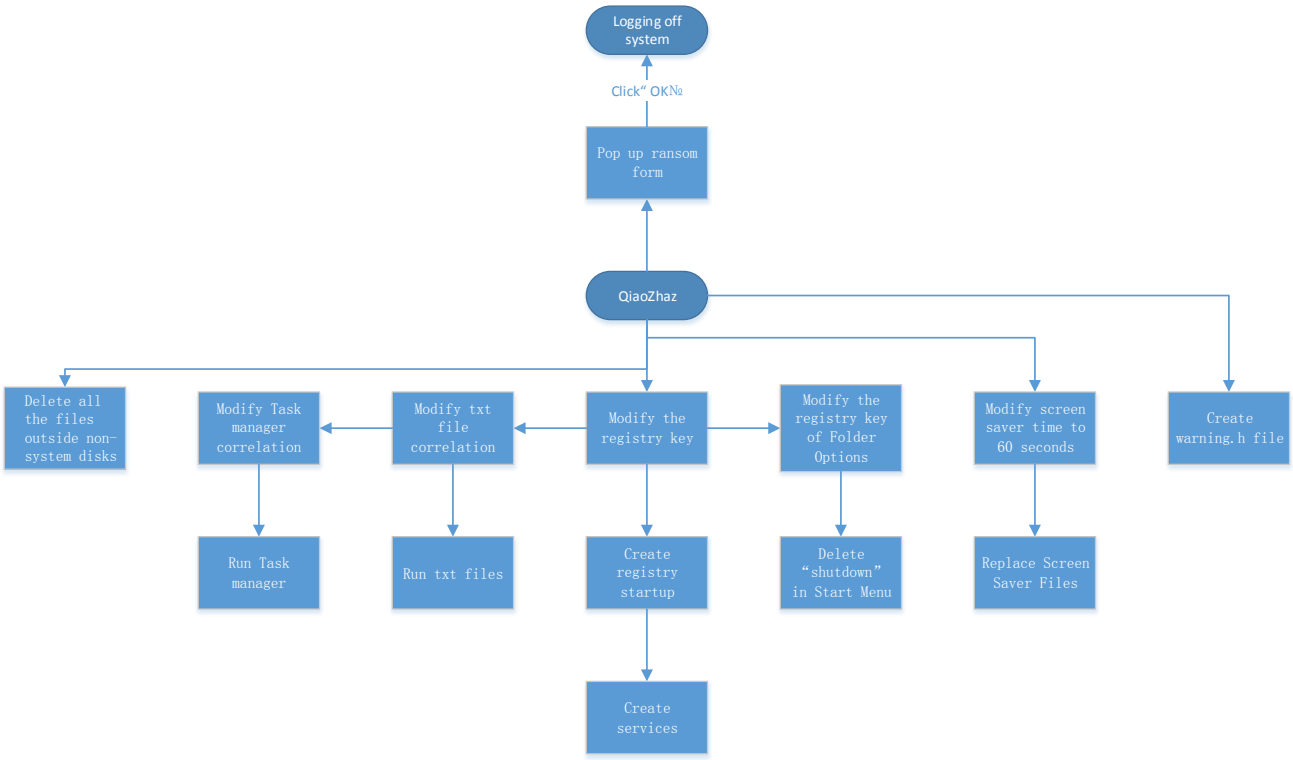
7. Do as what is mentioned above, you will be able to repair the lost data including the hidden file name.

Redplus creates a backup folder in root directory in a local disk, which is hidden and read-only and named "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}". At the same time, it also searches for user documents and packages files on local disks, such as .xls, .doc, .mdb, .ppt, .wps, .zip and .rar, then moves these data to the backup folder. Users will believe their data having lost and pay ransom.

Ouyang XX, the author of Redplus, was arrested in Guangzhou in 2007. He defrauded 7061.05 RMB in 95 attacks. Considering his surrender, he was ultimately sentenced to prison for 4 years.

4.2 QiaoZhaz

On March 1 and 2, 2007, Antiy respectively captured two viruses and named them QiaoZhaz.c and QiaoZhaz.d. Once you are infected by QiaoZhaz, a message will pop up and say "parts of your files will moved to a locked sector because of using pirated software in your disk, if you want to unlock the files, please contact with liugongs19670519@yahoo.com.cn for purchasing the appropriate software". If users click the button OK, the system will automatically be logged off. The workflow of QiaoZhaz is shown below:



Because of the registry startup entries and services added by QiaoZhaz.c, the system will be logged off after each starting up. The Trojan can remove the Folder Options, so that the functions of Show hidden files, Hide protected system files and Hide extensions for known file types cannot be performed. It can disable Search, Run and

Shutdown in the Start Menu, then users cannot search, command instructions, shut down or log off the system. What's more, it can modify txt file association. Once the user opens the txt, the trojan will be activated. Using the same method to modify the task manager association, it will be activated when users open the task manager. The screen saver time is modified to 60 seconds, over which the user does not operate the computer; the Trojan will run automatically using the Trojan files saved in %system32%. QiaoZhaz.c employs many techniques to avoid being detected, such as closing designated AV software.

QiaoZhaz.d is more odious. Besides the damages as of QiaoZhaz.c, it can also delete all files outside non-system disks. As a result, users must use data recovery software to retrieve the original data. The Trojan creates a file called warning.h in the root directory of each disk to extort money.

March 6, 2007, Antiy released a Registry Repair Tool, which is specially used for QiaoZhaz.

4.3 CryptoLocker

CryptoLocker was first discovered in September 2013, it can nearly infect all the Windows operating systems, including: Windows XP, Windows Vista, Windows 7 and Windows 8. It is spread by email attachments. If the attachment is open, CryptoLocker will encrypt files with certain type by RSA&AES. Thenwindow with ransom message will pop up.

Figure 4 Interface of CryptoLocker

In order to decrypt the files, users must pay 100 or 300 dollars (in the pattern of money pak or Bitcoin) within three or four days.

Types of encrypted files:

*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.eps, *.ai, *.indd, *.cdr, ????????.jpg, ????????.jpe,

img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c

Our analysts test a known sample of CryptoLocker (just with part of the communicating data for the server is out of normal use)and get the result as bellows:

```
POST /home/ HTTP/1.1
Accept: */*
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
Host: otjsqhyceuwmr.info
Content-Length: 192
Cache-Control: no-cache
Pragma: no-cache

......'.Tf.....D`!X=.J.g..8....L.%
...,.t*U..|g..b....t.{.3D...RY....m;..&..........U.......!vZ;....L..
\............|.PO..gl.....,.*...w..?d{..H.j.......t....n.ep...On}...
....HTTP/1.1 405 Not Allowed
Server: nginx
Date: Thu, 11 Jun 2015 03:00:28 GMT
Content-Type: text/html
Content-Length: 568
Connection: close

<html>
<head><title>405 Not Allowed</title></head>
<body bgcolor="white">
<center><h1>405 Not Allowed</h1></center>
<hr><center>nginx</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Figure 5 Communication of CryptoLocker

December 2013, ESET published an article on the emerging Cryptolocker 2.0 and Cryptolocker, and made a comparison of their techniques [4]:

	Cryptolocker	Cryptolocker 2.0
Virus name from ESET	Win32/Filecoder.BQ	MSIL/Filecoder.D, MSIL/Filecoder.E
Developing language	C++	C#
Payment method	Monepak,Ukash,cashU,Bitcoin	Bitcoin
Encryption algorithm	RSA-2048	RSA-4096
Encryption algorithm (for C&C Communication)	RSA	AES
C&C Address	Hard-coded and dynamically generated random domain	Hard-coded

Techniques used by CryptoLocker are almost concluded in CTB-Locker, so we will make the detailed analysis in section 4.4.

4.4 CTB-Locker

CTB-Locker is an abbreviation of Curve-Tor-Bitcoin Locker，it is a kindof ransomware family whichhas greater impactin the world currently,mainly spreads through email attachments. It uses high-strength encryption algorithm, encrypting system documents, pictures, databases, etc.After encryption, CTB-Locker will pop-up the ransom

window and modify the desktop background; then prompt users to pay 8 Bitcoins within 96 hours (about 10,000 yuan). Otherwise, it will destroy user files.The family has been always active abroad, anddomestic victims also appear in succession. Another feature of the family is using onion routing (Tor) to obtain ransom through completely anonymous Bitcoin transactions, which makes it difficult to trace the author of ransomware.

The figure of typical attack process is as follows：

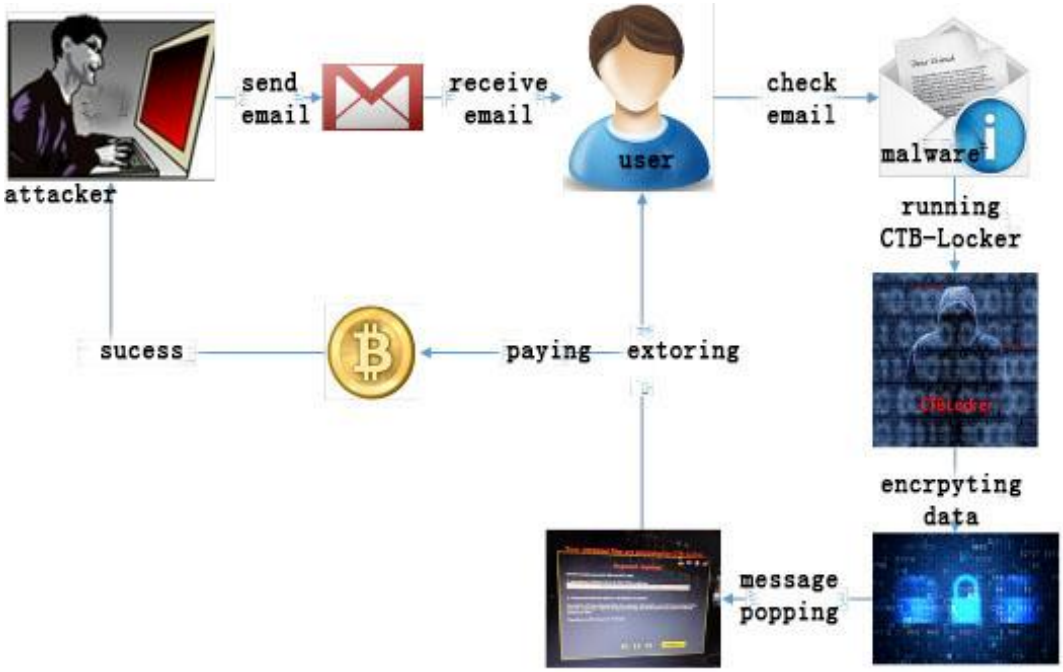


Figure 6 Attacking process of CTB-Locker

Analysts of Antiy CERT extracted a sample randomly and executed it, then a window extorting money popped up.

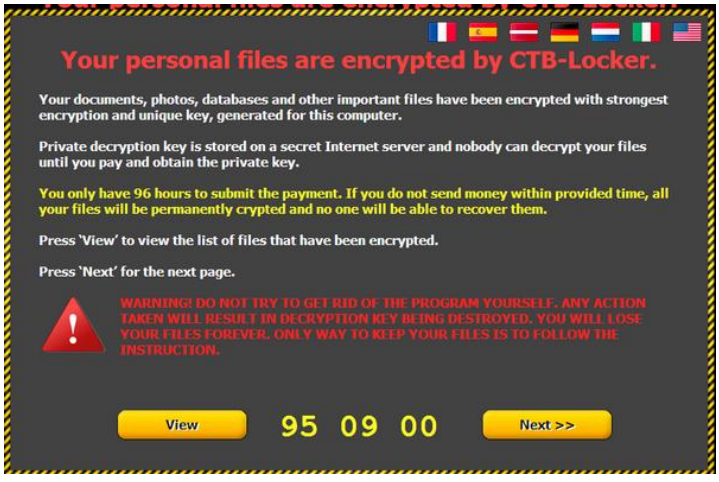


Figure 7 Extortion screen of CTB-Locker

At the same time, it also modified the desktop background, telling the user how to download and install Tor browser, and how to access their ransom payment webpage by Tor browser.

Figure 8 CTB-Locker requires the user to install Tor browser

According to the analysis of the sample, we can understand the general execution process of CTB-Locker, as shown in the figure below:

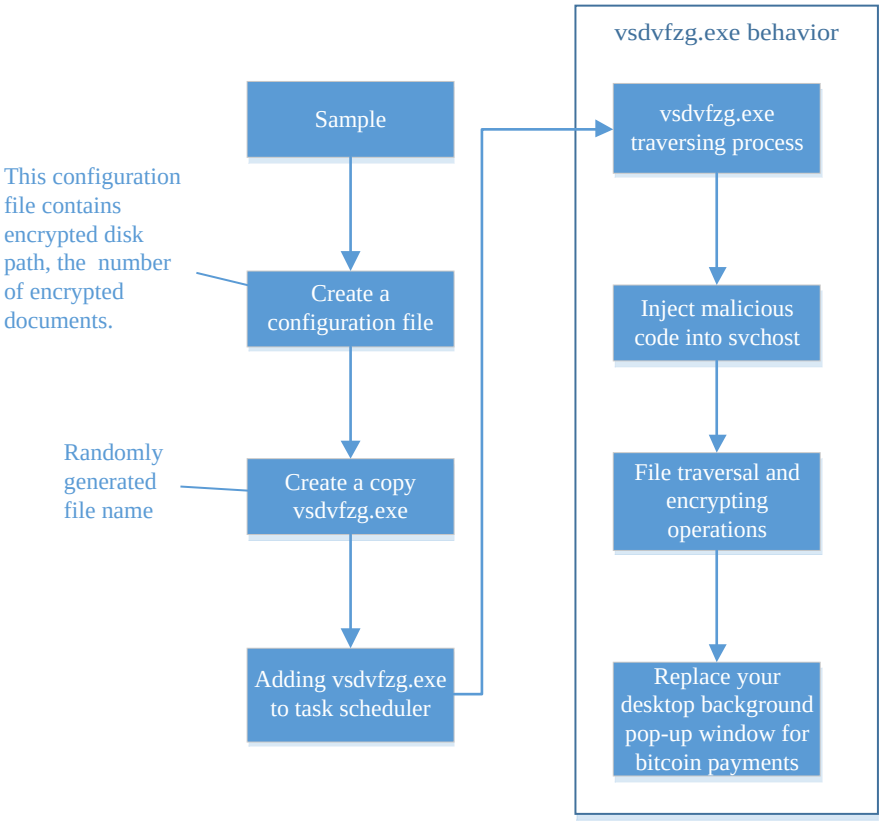


Figure 9 The general execution process of CTB-Locker

During file traversal process, the sample will encrypt the files which have the following extensions:

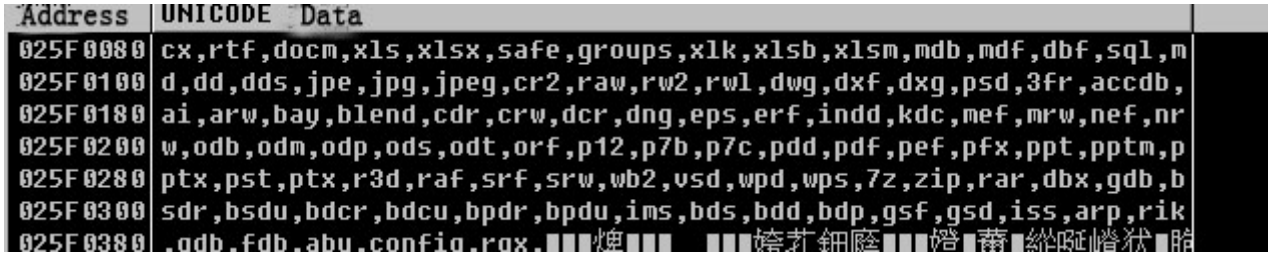


Figure 10 Decrypted file extensions data of CTB-Locker

The encryption part is more critical, so we explain it as emphasis.

First, the sample will move the file (with suffix.tmp) to be encrypted to the temporary directory by calling MoveFileEx. Then filling a buffer depends on the file time and the current system files running time or other information. Computing SHA256 and making it as the session private key. It will use the Elliptic curve Diffie-Hellman (ECDH) algorithm computing to generate a session public key(session public key); then generate a session shared key with master public keys in configuration file using ECDH algorithm. Computing SHA256of theshared session and the value will be AES encryption KEY. Related codes are as follows:

```
lea     eax, [ebp+50h+var_104]
push    eax
lea     eax, [ebp+50h+var_124]
push    eax
lea     eax, [ebp+50h+var_B4] ; Generating session public key
push    eax
call    sub_25F63FF
push    offset najzljf_data
lea     eax, [ebp+50h+var_124]
push    eax
lea     eax, [ebp+50h+var_164] ;  Session shared secret
push    eax
call    sub_25F63FF
lea     eax, [ebp+50h+var_144]
push    eax
lea     eax, [ebp+50h+var_164]
push    20h ; ' '
push    eax
call    Sha256          ;  Computing sha256
mov     edi, [ebp+50h+arg_1C] ; Encryped key
```

It should be noted that the AES key to be saved to a parameter of the function for the caller, but the caller just saved five AES keys. This is the reason why CTB-Locker isstill able to decrypt five files in offline mode.CTB-Locker reads the file, encrypts it with AES after it compressed by ZLIB. The encrypted data are written starting the head offset 0x30 of a temporary file, it will write the data0x30 to the head of the temporary file after being encrypted. The beginning 0x20 byte is the session public key. Five AES keys, the number of encrypted files, encrypted disks and other information will be saved in the configuration file.

4.5 Ransomware for mobile platform

In April 2014, ransomware for mobile platforms began to appear abroad, and the similar software appeared in China before long. Currently, the ransom patterns ofmobile platform both home and abroad include RMB, Q coins, dollars, rubles, etc.; the ways of fraud include screenlocking, file encryption, contactsencryption and so on.

According to information, thousands of phones have been infected in China since such software broke out. The development of ransomware will be a serious threat to user's mobile phone and data.

Domestic ransomware usually camouflage game plugs or pay cracked software, lock screen when users click it. The users must addthe QQ number left on the screen as a friend and pay ransom to “the friend” if they want to unlock screens.

The following is a real case of this kind of ransomware. Victim's phone is locked, and designated QQ number shows on the mobile phone screen. The user is required to add it as a friend and pay a ransom to unlock screen.

Users will be prompted to answer authentication questions after adding the QQ number. In this case，we can see the relevant information of the extortionists, its relevant identity information can be seen in the personal information, but we cannot guarantee its authenticity.

Figure 11 Fraud process diagram

Corresponding text translations of the picture:

The literal meaning of the picture is:

Congratulations！ Your phone has been unlocked.

QQ 1031606149

Asking for the password.

Decryption serial number is 6006509.

Note: each serial number corresponds to the only unlocking password.

Confirm to unlock

You will add a friend (1031606149), and you are wanted to answer the following questions:

No.1: Crack & bypass, intercept, unlock?

No.2: Do you have an Alipay or Tenpay account?

No.3: or other payment methods you have?

Unlock

Interception source codes (kill-free); incorporating two APKs as one; kinds of little funny software; if you send the request to add friends but with no response, please call 1838508254.

Time for QQ: 6 years

Profile: Male; Horse; Capricorn; O-type blood

Birthdate: January 1

Location: Yiyang Hainan province, China

Email: 1031606149@qq.com

Telephone number: 13800051501

You will send me the unlocking password after getting the money, right?

Yes.

What is your account and how much you charge?

*Alipay account: 183*****440 (Wen Zhaojun)*

20RMBs.

After adding friends, the author of the ransomware will chat with the victim and ask 20 yuan as ransom, and require the user to transfer the moneyto a designated PayPal account, only doing this, he will give the password for unlocking screen. It is understood that the author also cheat other Android mobile phone users, and they still failed to get the unlock password after paying ransom.Moreover, the interception Trojan functionality will be added to steal users' Paypal and wealth accounts. Sometimes, victims may pay ransom many times but with no unlocking passwords, evenadded to blacklist by the authors of the ransomware.

5 Protection: what should we do?

5.1 SecurityRecommendations and Solutions

For PC users, we suggest them to do as bellows to protect themselvesfrom being affected by ransomware:

1. Back up important files in time;
2. Apply software patches as soon as they become available;
3. Bookmark trusted websites and access these websites via bookmarks;
4. Keep alert to emails of untrusted sources, and do not open attachments or links in untrusted emails;
5. Scan your system regularly with anti-malware.

For mobile terminal users of Android platform, recommendationsare as following:

1. Install mobile anti-virus software（for example LBE security master, AntiyAVL Pro ,etc.）;
2. Download mobile app from reliable Android Market.

Mobile terminal users who have already been infected by ransomware can try the following ways:

1. If the phone roots and opens USB scheduling model，malicious applications can be deleted directly after entering the adb shell.

2. If you lock the screen with the system password，some phones may try to use the function of recovering the password.

3. Enter safe mode of the mobile phone to remove malicious applications.The mainstream way getting into

safe mode for Android phones is to hold down the [Power Key] button boot until the LOGO or operators appear on the screen, keep press on the [The volume reduction] button. If it works, the words "Safe Mode" will appear at the left bottom of the lock screen. Then you can uninstallmalware normally.

5.2 Defensive Approaches forOrdinary Users

According to the analysis above, ransomware withsophisticated encryption ways to kidnap user data will pose a serious threat to user data security and it is extremely important to defense. Ordinary users can download special defense products such as CryptoMonitor to keep safe. (CryptoMonitor, based on the behavior detection results, tries to prevent your data when ransomware attempt to encrypt them[5]).

5.3 Defensive Approaches for EnterpriseUsers

For enterprise users, they can follow the next five steps to keep away from ransomware: warning, prevention, protection, handling and auditing. Firstly, unknown applications found by enterprise users should be submittedtotheircloud platforms automatically; and identifying them by feature detection and virtual execution so as to detect malicious programs in time. Secondly, IT managers can set the host computer of great value file resource to critical computer or restricted computers. Thus they can apply to the trusted baseline (whitelist) to find out ransomware or other suspicious programs andprevent malicious behaviors. Thirdly, they can use security document measures to protect the documents with great value. Finally, they can trace malicious samples over the entire networkthrough the clouds traceabilityto facilitate post-audit and assess the damage.

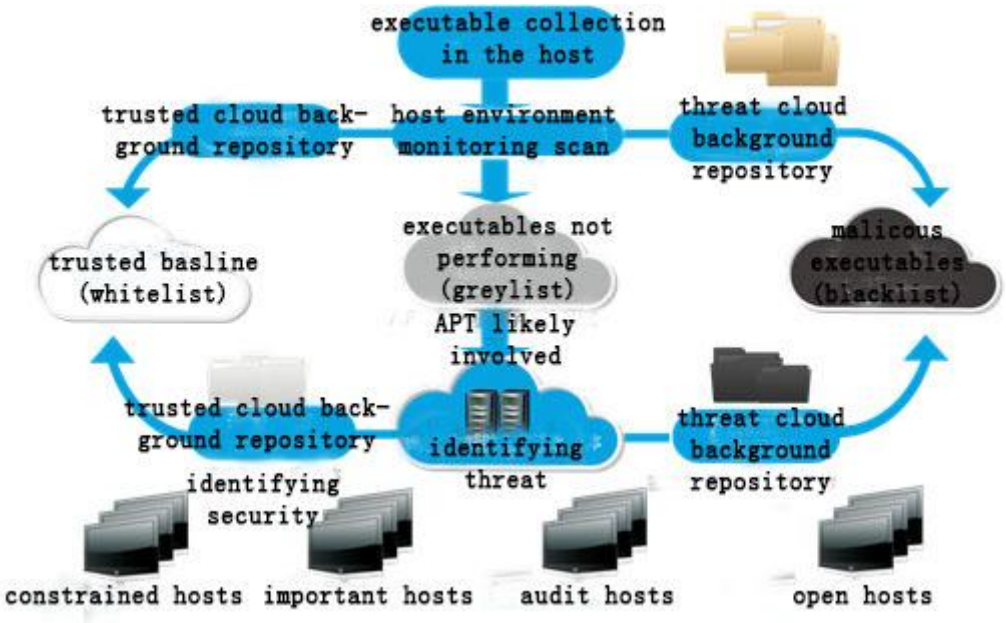


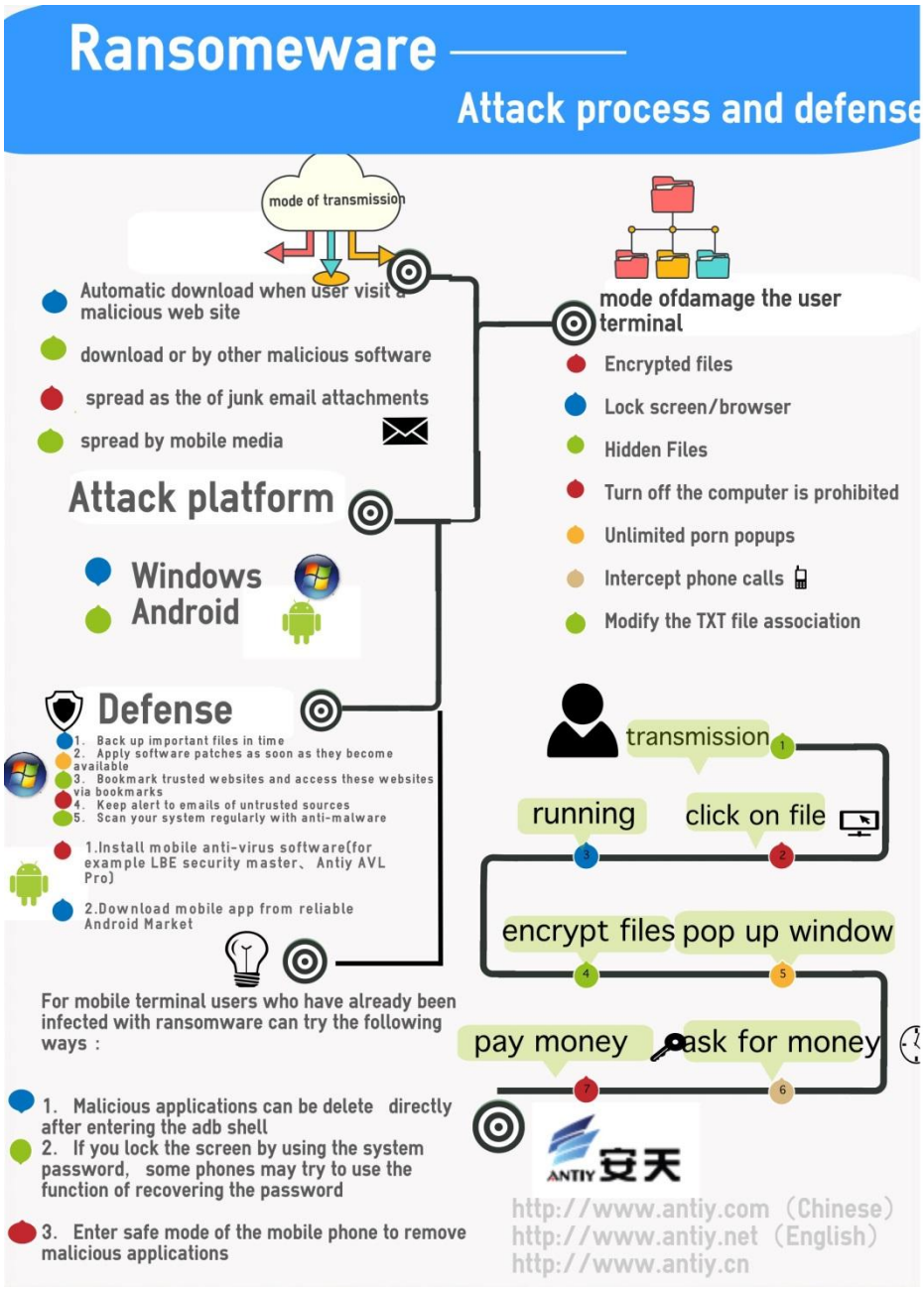
Figure 12 Enterprise security products of Antiy work process

6 Conclusion

Though ransomware is not so sophisticated, it can make serious damages on data assets. We should never overlook its effect.

By the end of May 2015, the author of Locker apolygized to the public and published its database, then provided the automatic decryption program for victims. According to some statistics, the database records 62,703 ransomware events. If the ransom is 0.1 Bitcoin (about 27.3 US dollars) and gets paid every time, the total ransom will be up to 1.551 million US dollars. With the huge illegal incomes, it is likely that there will be more and more malware writers to develop ransomware. Payment methods like Bitcoin are difficult to track, so the authors of ransomware will be more emboldened.

Greek soldiers jumpped out of trojans, kill the men in the sleep and open the gate. The hidden forces flooded into Troy and burnt it into ashes. At this time, the Trojans regret not take Laocoon's advice, but it was too late ..... For the common infections by virus and trojan, users can make system in the safe state again by installing AV software even after being infected. For the ransomware kidnapping users' data, AV software, focused on system security rather than reliable defense and detection ability, will be useless. To keep away from ransomware, one of the most effective way is to install tools focusing on data security respectively, such as the tool we discussed above. We can also deploy the security products suitable for the enterprise if we work for the organization, which will protect our important documents more efficiently and more easily.



Appendix A：References

[1] CryptoLocker Ransomware

http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/

[2] 恶意勒索软件 ScarePackage 肆虐美国 Android 用户需小心提防(Malicious ransomeware ScarePackage plague USA Android users need to be careful)

http://www.cnbeta.com/articles/322803.htm

[3] 新型恶意勒索软件 VirLock (New malicious ransomeware VirLock)
http://netsecurity.51cto.com/art/201412/462202.htm

[4] Cryptolocker 2.0 – New Version, or Copycat?
http://www.welivesecurity.com/2013/12/19/cryptolocker-2-0-new-version-or-copycat/

[5] Easy Sync CryptoMonitor
https://easysyncsolutions.com/CryptoMonitorDetails

[6] CryptoLocker Ransomware Information
http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

[7] Ransomware would you pay up?
https://nakedsecurity.sophos.com/2012/09/25/ransomware-would-you-pay-up/

[8] Ransomware
http://www.trendmicro.com/vinfo/us/security/definition/ransomware

[9] Cryptowall ransomeware
http://translate.google.com.hk/translate?langpair=auto%7Czh-CN&u=http://www.enigmasoftware.com/cryptowallransomware-removal/

[10] Crytplocker_Update_RevD
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25203/en_US/Cryptolocker_Update_RevD.pdf

[11] RANSOMWARE - KollAH.F OUTBREAK
https://sites.google.com/site/alonjb/ransomwareinternalpublication

[12] Ransomware: Kovter infections on the rise
http://www.csoonline.com/article/2156408/malware-cybercrime/ransomware-kovter-infections-on-the-rise.html

[13] 'Reveton' ransomware upgraded with powerful password stealer
http://www.pcworld.com/article/2466980/reveton-ransomware-upgraded-with-powerful-password-stealer.html

[14] Inside a ‘Reveton’ Ransomware Operation
http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

[15] “攻击 WPS 样本”实为敲诈者(“Attack the WPS sample ”is a blackmailer actually)
http://www.antiy.com/response/CTB-Locker.html

[16] 部分利用社工技巧的群发邮件样本关联分析(Part of groupmail samples correlation analysis using social engineering)
http://www.antiy.com/response/Upatre.html

[17] 勒索软件 CTB-Locker 核心原理的一些疑问和分析(Some doubt and analysis about core principle of ransomeware CTB-Locker)
http://www.freebuf.com/articles/system/57918.html

[18] Windows 10 Upgrade Spam Carries CTB-Locker Ransomware
https://threatpost.com/windows-10-upgrade-spam-carries-ctb-locker-ransomware/114114

Appendix B：About Antiy

Antiy Labs is a vender of antivirus engine and solution and founded in 2000. Now, it has four research and development centers, monitoring and early warning capabilitiescoveragethroughout the country, and provides security products and services for many foreign countries. With fifteen years accumulation, Antiy owns a massive security threat repository.With the experience of network detection, host defense, unknown threats identification, big data analytics and visual security, it launches advanced products and solutions response to Advanced Persistent Threat (APT).

Antiy technical strength has been recognized by professional administrative organizations, customers and partners. It has won the security emergency supporting qualification for last four years, and becomeone of the six top-level CNNVD support units. Antiy Mobile Detection Engine is the only Chinese product which gets the world's first AV-TEST (2013) annual awards; more than ten well-known security vendorsall over the world have chosen to work with us.

For more information about the anti-virus engine please visit：	http://www.antiy.com（Chinese） http://www.antiy.net（English）
For more information about Antiy anti-APT related products, please visit：	http://www.antiy.cn