باسمه تعالی

تحلیل فنی باج افزار Crysis/Dharma[.Bip]

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج‌افزار Crysis/Dharma خبر می‌دهد که پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به .bip تغییر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در اواسط ماه می سال ۲۰۱۸ میلادی شروع شده است. بر خلاف نسخه‌های قبلی خانواده Crysis/Dharma که تمرکز آن‌ها بیشتر بر روی کاربران انگلیسی زبان بود، جامعه هدف این باج‌افزار در حال حاضر مشخص نمی‌باشد. این باج‌افزار از الگوریتم‌های رمزنگاری RSA و AES(Rijndael) برای رمزگذاری فایل‌ها استفاده می‌کند و به جز دایرکتوری‌هایی خاص در درایو اصلی ویندوز که در ادامه به آن اشاره خواهیم نمود، تمام فایل‌های موجود در سیستم قربانی شامل تصاویر، فایل‌های ویدئویی، اسناد، پایگاه داده‌ها و ... را رمزگذاری می‌کند. این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند.

مشخصات فایل اجرایی :

نام فایل	detrimentalnue.exe
MD۵	٥٣c٤٩٢d٧٥٩٦bee٦ad٧c٨a٣fda٧ec٩٠e٧
SHA-١	٠٣ddf٥fdb٣٧c٥b٠a١٢٦٤efb٠٠ca٩d٩٧٦٢٧a٠١dd٦
SHA-٢٥٦	٠٤٤d٣d٣٦c٧e٧٣٧٧e٢٩da٧٦٩٣٩٧b٣e١٧٣b٢١acc٢a٠٧a٦٧٦c٣٧٧d٠٣٣٥c٣٦e٠e٠١f
اندازه فایل	٤٣١ KB
کامپایلر	Microsoft visual C# v٧.٠ / Basic .NET

فایل اجرایی این باج افزار دارای چهار بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٧.٤٢	٨١٩٢	٤٣٥٦٣٦	٤٣٥٧١٢
.sdata	٤.٤١	٤٥٠٥٦٠	٢٣٣٧	٢٥٦٠
.rsrc	٤.١٢	٤٥٨٧٥٢	١٥٠٤	١٥٣٦
.reloc	٠.١	٤٦٦٩٤٤	١٢	٥١٢

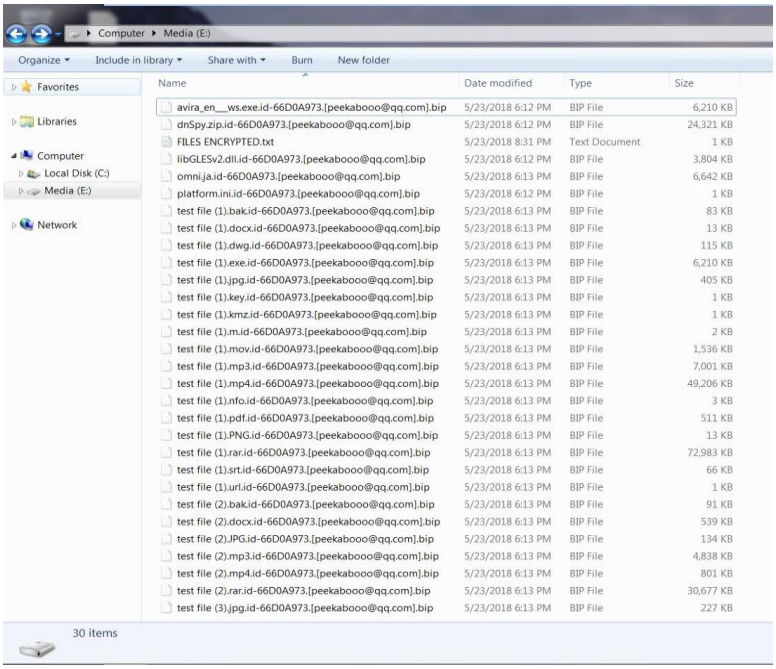
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Crysis/Dharma (.Bip) ، 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، شروع به رمزگذاری فایل‌ها می‌کند و پس از اتمام فرایند رمزگذاری، فایلی با نام FILES ENCRYPTED.txt در کنار فایل‌های رمزگذاری شده و بر روی Desktop ایجاد می‌کند که محتوای آن یک ایمیل به آدرس peekabooo@qq.com می‌باشد که قربانیان جهت رمزگشایی فایل‌ها باید از طریق این ایمیل با مهاجمین ارتباط برقرار نمایند. محتوای این فایل در تصویر زیر قابل مشاهده است :

این باج‌افزار از الگوریتم رمزنگاری AES استفاده می‌کند و به جز دایرکتوری‌های زیر که در درایو اصلی ویندوز وجود دارند، تمام فایل‌ها را رمزگذاری می‌کند.

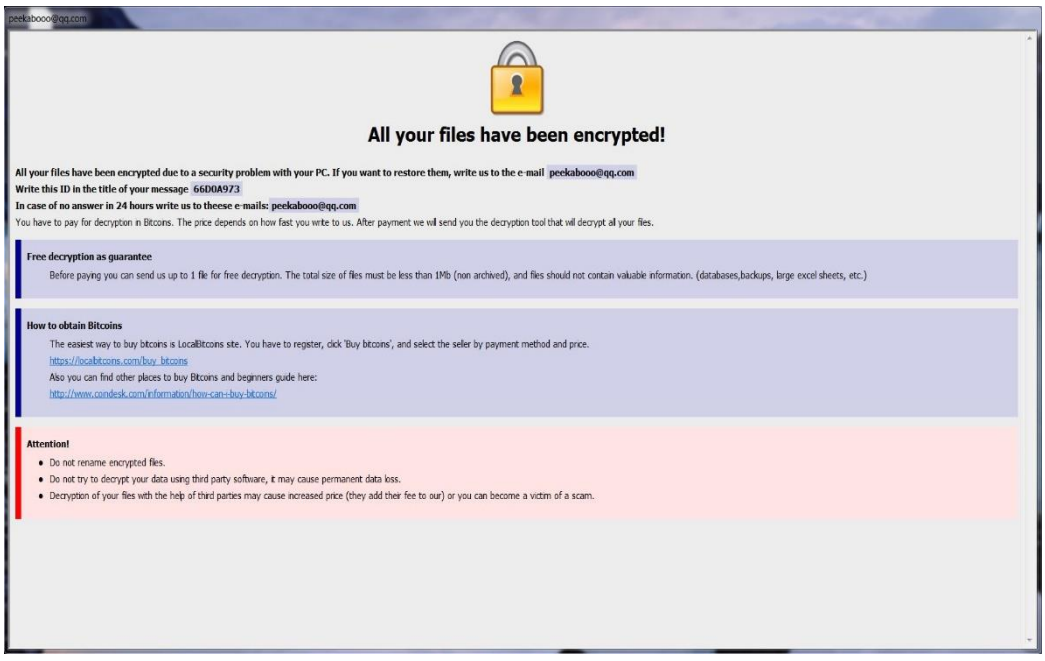
Windows, Common Files\Services, Common Files\SpeechEngines, Common Files\system, DVD Maker, internet explorer, Reference Assemblies, Windows Defender, Windows Journal, Windows Mail, Windows Media Player, windows NT, Windows Photo Viewer, Windows Portable Devices, Windows Sidebar

تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد.



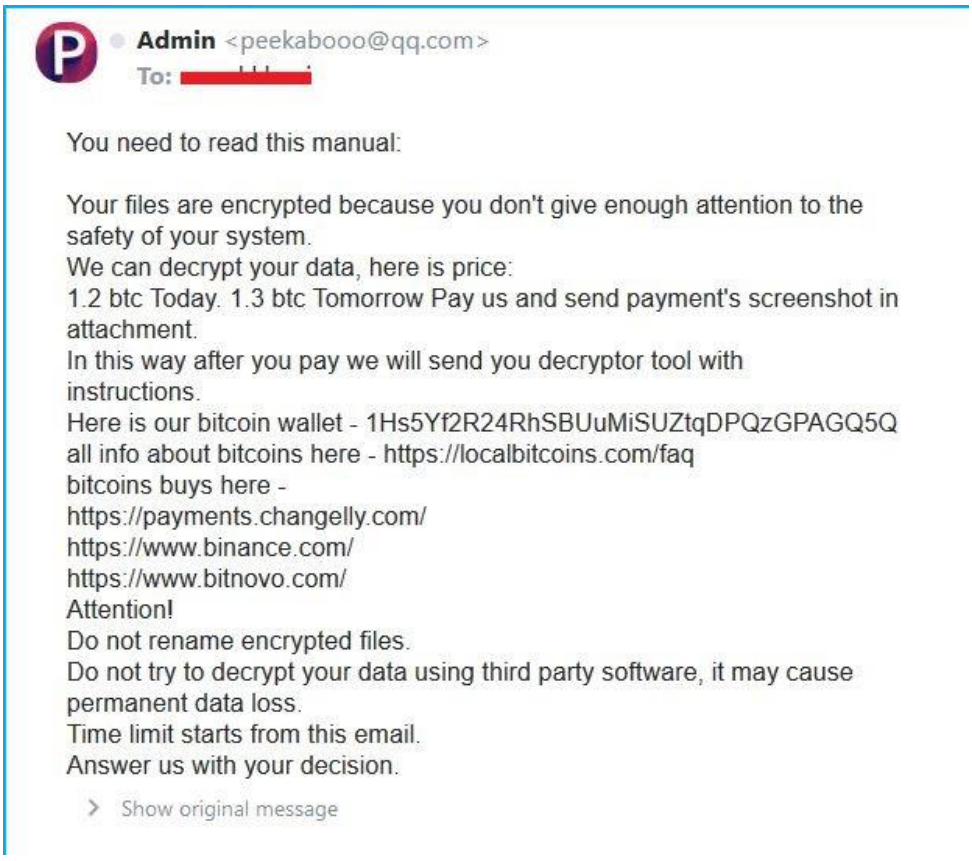
پس از رمزگذاری فایل‌ها، پسوند id-٦٦D٠A٩٧٣.[peekabooo@qq.com].bip. به انتهای فایل های رمزگذاری شده اضافه می‌شود که الگوی این پسوند به شکل id-[id][email].bip. می‌باشد که شامل کد شناسایی قربانی و آدرس ایمیل مربوطه جهت برقراری ارتباط با مهاجمین است.

پس از اتمام فرآیند رمزگذاری، باج‌افزار پیغام باج‌خواهی خود را به نمایش می‌گذارد و به دلیل رمزگذاری دایرکتوری مربوط به نرم‌افزارهای نصب شده بر روی سیستم قربانی، هیچ یک از نرم افزارهای مذکور دیگر قابل استفاده نخواهند بود. تصویر زیر پیغام باج‌خواهی باج افزار Bip Crysis/Dharma. را نشان می‌دهد.



بر اساس پیغام باج‌خواهی، یک کد شناسایی منحصربفرد برای هر قربانی وجود دارد که قربانیان برای رمزگشایی فایل‌ها، باید از طریق آدرس ایمیل peekabooo@qq.com با مهاجمین ارتباط برقرار نمایند و بایستی کد شناسایی خود را در قسمت Subject ایمیل وارد نمایند. طبق گفته مهاجمین، مبلغ باج به این بستگی دارد که قربانیان طی چه مدتی پس از رمزگذاری فایل‌ها با مهاجمین ارتباط برقرار نمایند و هر چه دیرتر ارتباط برقرار نمایند مبلغ باج بیشتری در نظر گرفته می‌شود. ضمناً جهت جلب اعتماد قربانیان امکان رمزگشایی تعدادی از فایل‌ها قبل از پرداخت مبلغ باج را نیز فراهم شده است که قربانیان در صورت تمایل، می‌توانند یک فایل با حداکثر حجم ۱ مگابایت را برای رمزگشایی ارسال نمایند. در پیغام باج‌خواهی مهلتی برای پرداخت مبلغ باج در نظر گرفته نشده است و هر گونه تلاش برای رمزگشایی فایل‌ها، به جز پرداخت مبلغ باج باعث از بین رفتن فایل‌ها می‌شود.

پس از برقراری ارتباط با مهاجمین به صورت ناشناس، ابتدا از تعداد سیستم‌های رمزگذاری شده توسط باج‌افزار سوال گردید و سپس پیغام زیر را برای ما ارسال شد.


Admin <peekabooo@qq.com>
To: [redacted]

You need to read this manual:

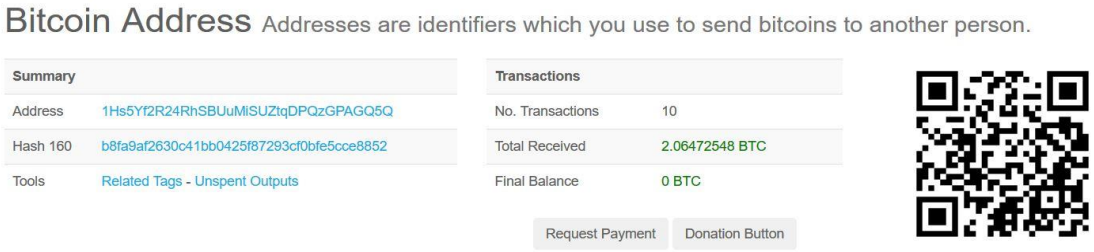
Your files are encrypted because you don't give enough attention to the safety of your system.
We can decrypt your data, here is price:
1.2 btc Today. 1.3 btc Tomorrow Pay us and send payment's screenshot in attachment.
In this way after you pay we will send you decryptor tool with instructions.
Here is our bitcoin wallet - 1Hs5Yf2R24RhSBUuMiSUZtqDPQzGPAGQ5Q
all info about bitcoins here - https://localbitcoins.com/faq
bitcoins buys here -
https://payments.changelly.com/
https://www.binance.com/
https://www.bitnovo.com/
Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Time limit starts from this email.
Answer us with your decision.

Show original message

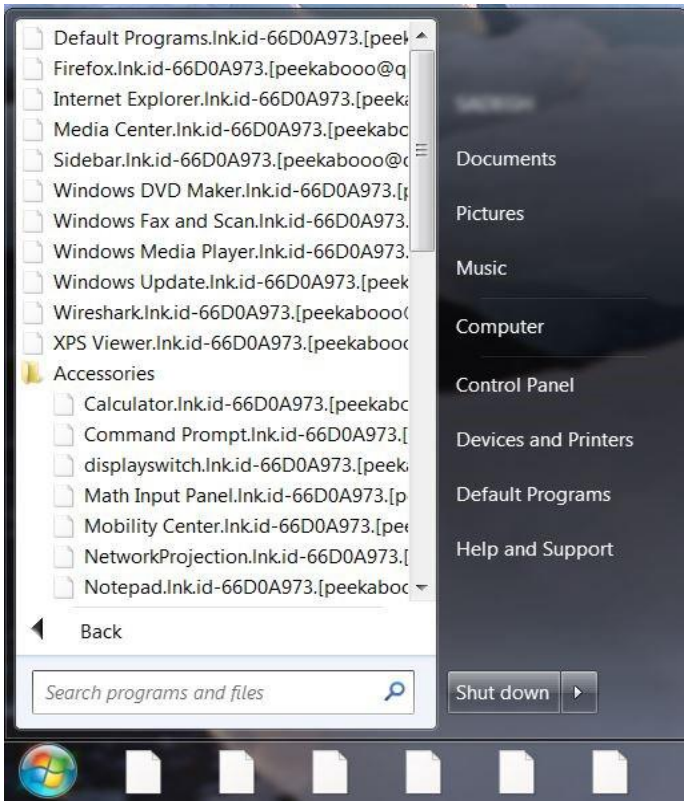
طبق این پیام مبلغ باج، در ابتدا ۱.۲ بیت‌کوین تعیین شده است که که این مبلغ می بایست طی ۲٤ ساعت به کیف پول بیت‌کوین به آدرس ۱Hs٥Yf٢R٢٤RhSBUuMiSUZtqDPQzGPAGQ٥Q پرداخت شود در غیر

اینصورت مبلغ به ۱.۳ بیت‌کوین، برای روز بعد افزایش پیدا می‌کند، بر اساس مذاکرات صورت گرفته با مهاجمین، توانستیم مبلغ باج را به ۰.۷ بیت‌کوین کاهش دهیم.

طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تاکنون تعداد ۱۰ تراکنش برابر با BTC ۲.۰٦٤٧٢٥٤٨ داشته است.



این باج‌افزار فایل‌های موجود در Recycle Bin را نیز حذف می‌نماید و تمام ابزارهای کاربردی مربوط به ویندوز را نیز رمزگذاری می‌کند، همچنین به دلیل رمزگذاری دایرکتوری مربوط به نرم‌افزارهای نصب شده بر روی سیستم قربانی هیچ یک از آن‌ها دیگر قابل استفاده نخواهند بود. تصویر زیر مربوط به رمزگذاری ابزارهای کاربردی ویندوز توسط باج‌افزار می‌باشد :



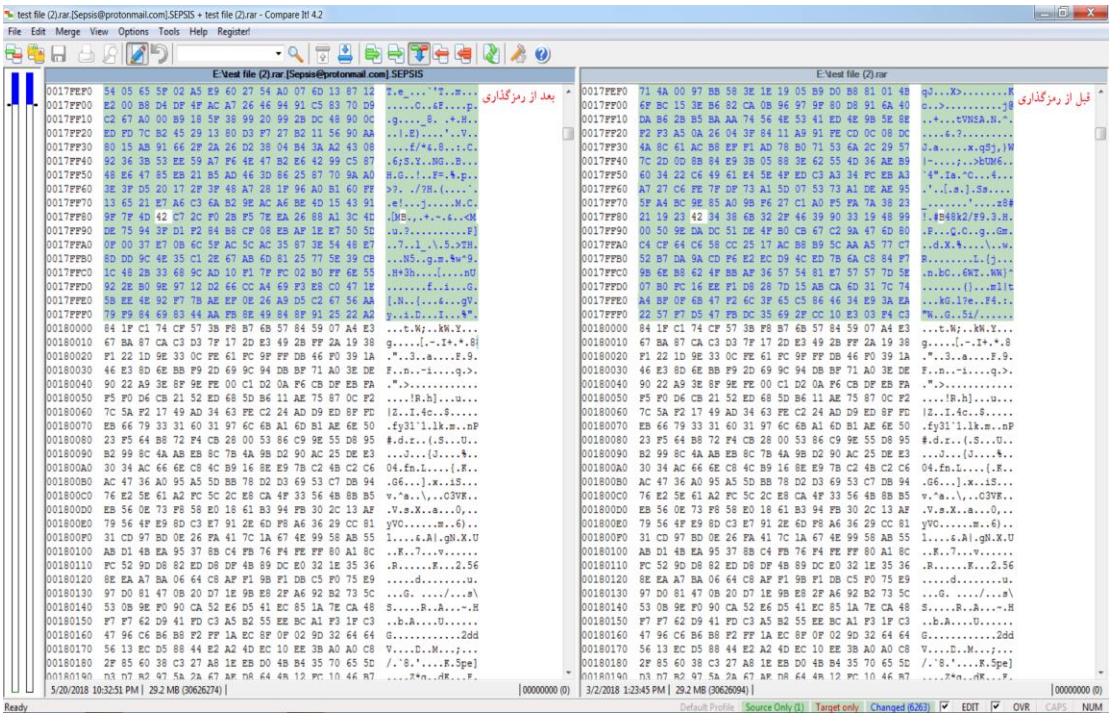
بر اساس مشاهدات صورت گرفته و سوابق نسخه‌های قبلی باج‌افزار Crysis/Dharma ، این نسخه نیز به طور معمول از طریق هک کردن کلمه عبور سرویس ریموت دسکتاپ (RDP) و همچنین هرزنامه ها منتشر می گردد. لذا به مدیران و راهبران شبکه در سازمان ها توصیه می گردد نسبت به امن سازی شبکه خصوصاً RDP اقدام نمایند.

تحلیل ایستا:

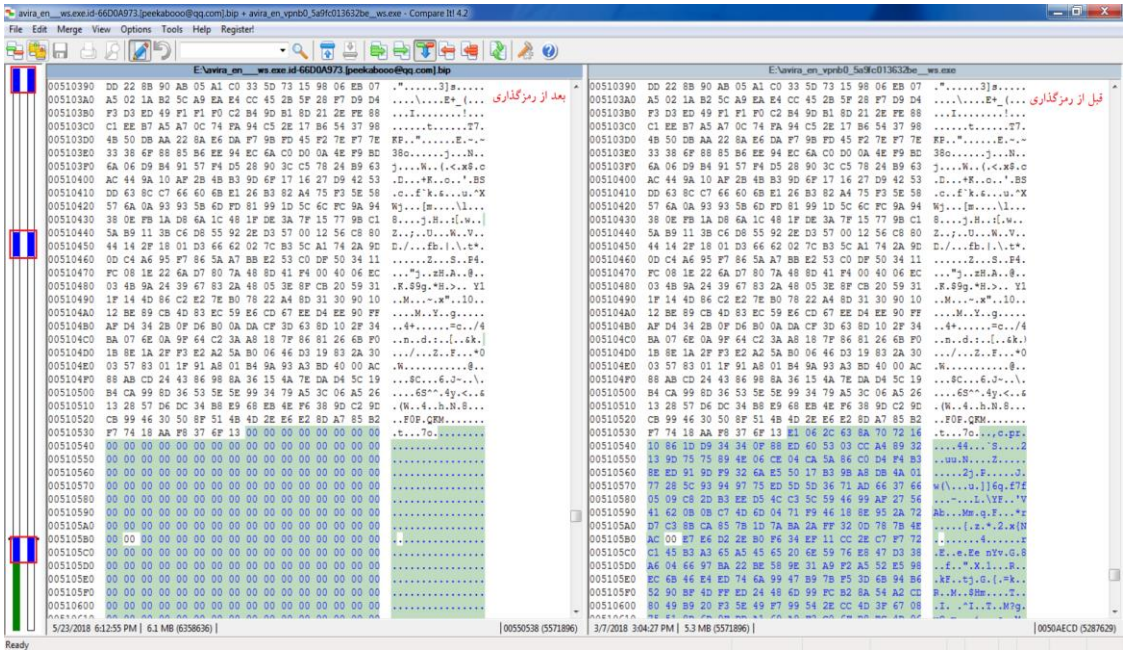
پس از تحلیل کد باج‌افزار Crysis/Dharma (.Bip) به نتایج زیر دست پیدا کردیم.

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری توسط باج‌افزار، انجام دادیم شاهد این بودیم که باج‌افزار Crysis/Dharma (.Bip) ساختار تمام فایل‌ها را به یک شکل رمزگذاری نمی‌کند و در مواجهه با فایل‌های مختلف رفتار متفاوتی از خود نشان می دهد. بدین صورت که ساختار بعضی از فایل‌ها که حجم کمی دارند را پس از رمزگذاری کاملا تغییر می‌دهد اما در مورد برخی دیگر از فایل‌ها که حجم

آن‌ها بیشتر می‌باشد، سه بخش ابتدا، میانی و انتهای فایل‌ها را تغییر می‌دهد، نتایج این بررسی‌ها در تصاویر زیر قابل مشاهده است.

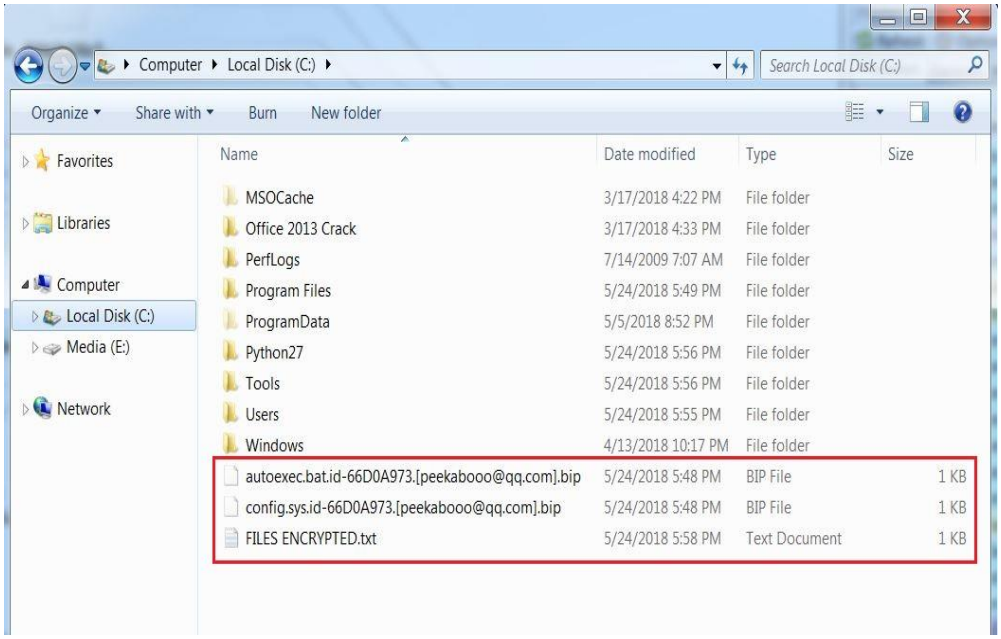


تصویر ۱ تمام ساختار فایل تغییر کرده است.

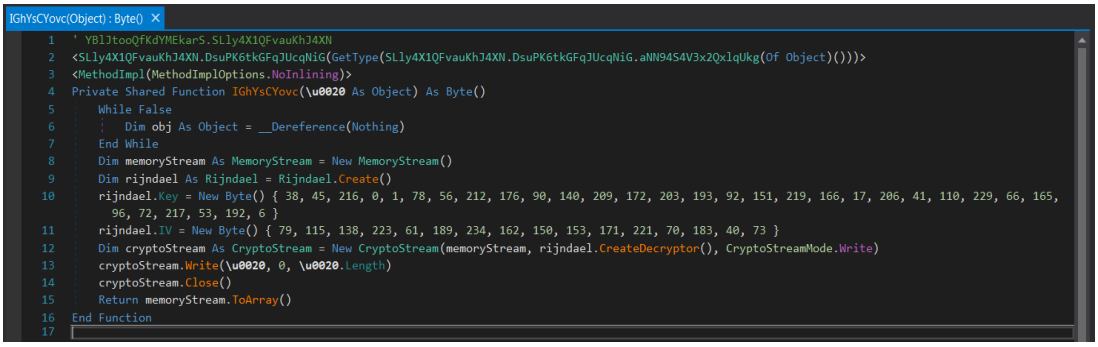


تصویر ۲ سه قسمت ابتدا، میانی و انتها ساختار فایل تغییر کرده است.

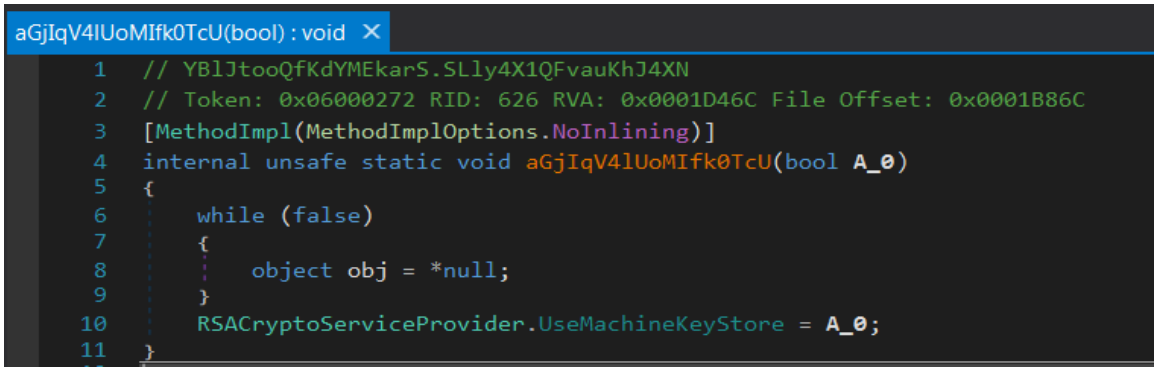
برخی از فایل‌های ایجاد شده توسط باج‌افزار، در تصویر زیر قابل مشاهده می‌باشد :



نسخه‌های ابتدایی این باج‌افزار از الگوریتم رمزنگاری AES برای رمزگذاری فایل‌ها استفاده می‌کردند. پس از بررسی بر روی کدمنبع این نسخه از باج‌افزار، همانطور که قبلا نیز اشاره نمودیم از الگوریتم‌های رمزنگاری RSA و AES (Rijndael) برای رمزگذاری فایل‌ها استفاده می‌کند، این مورد در تصاویر زیر قابل مشاهده می‌باشد :



تصویر ۱



تصویر ۲

```
RSACryptoServiceProvider
namespace System.Security.Cryptography
{
    // Token: 0x02000281 RID: 641
    [ComVisible(true)]
    public sealed class RSACryptoServiceProvider : RSA, ICspAsymmetricAlgorithm
    {
        // Token: 0x06002279 RID: 8825
        [SecurityCritical]
        [SuppressUnmanagedCodeSecurity]
        [DllImport("QCall", CharSet = CharSet.Unicode)]
        private static extern void DecryptKey(SafeKeyHandle pKeyContext, [MarshalAs(UnmanagedType.LPArray)] byte[] pbEncryptedKey, int
          cbEncryptedKey, [MarshalAs(UnmanagedType.Bool)] bool fOAEP, ObjectHandleOnStack ohRetDecryptedKey);

        // Token: 0x0600227A RID: 8826
        [SecurityCritical]
        [SuppressUnmanagedCodeSecurity]
        [DllImport("QCall", CharSet = CharSet.Unicode)]
        private static extern void EncryptKey(SafeKeyHandle pKeyContext, [MarshalAs(UnmanagedType.LPArray)] byte[] pbKey, int cbKey, [MarshalAs
          (UnmanagedType.Bool)] bool fOAEP, ObjectHandleOnStack ohRetEncryptedKey);

        // Token: 0x0600227B RID: 8827 RVA: 0x0007BBDD File Offset: 0x00079DDD
        [SecuritySafeCritical]
        public RSACryptoServiceProvider() : this(0, new CspParameters(24, null, null, RSACryptoServiceProvider.s_UseMachineKeyStore), true)
        {
        }

        // Token: 0x0600227C RID: 8828 RVA: 0x0007BBF7 File Offset: 0x00079DF7
        [SecuritySafeCritical]
        public RSACryptoServiceProvider(int dwKeySize) : this(dwKeySize, new CspParameters(24, null, null,
          RSACryptoServiceProvider.s_UseMachineKeyStore), false)
        {
        }
```

تصویر ۳

بر اساس قطعه کدهای زیر، باج افزار فایل‌های مختلف را مورد بررسی قرار می‌دهد که آیا دارای پسوند خاصی هستند و آن‌ها را تغییر می‌دهد.

```
jINKm3WpX9Zx4qHPsM(object) : bool
// fgVWeFuSqBu8ZespR2.Va5su2KJrNbMiR40Z2
// Token: 0x0600000F RID: 15 RVA: 0x00007784 File Offset: 0x00005B84
[MethodImpl(MethodImplOptions.NoInlining)]
internal unsafe static bool jINKm3WpX9Zx4qHPsM(object A_0)
{
    while (false)
    {
        object obj = *null;
    }
    return Path.HasExtension(A_0);
}
```

تصویر ۱: بررسی پسوند فایل‌ها

```
Path
// Token: 0x06001903 RID: 6403 RVA: 0x00052AD0 File Offset: 0x00050CD0
[__DynamicallyInvokable]
public static bool HasExtension(string path)
{
    if (path != null)
    {
        Path.CheckInvalidPathChars(path, false);
        int num = path.Length;
        while (--num >= 0)
        {
            char c = path[num];
            if (c == '.')
            {
                return num != path.Length - 1;
            }
            if (c == Path.DirectorySeparatorChar || c == Path.AltDirectorySeparatorChar || c == Path.VolumeSeparatorChar)
            {
                break;
            }
        }
    }
    return false;
}
```

تصویر ۲: کدمنبع تابع HasExtension()

```
WSJGNRtMRstfRbcJ97T(object, object) : o...
1   // EIJDRrjQqUpfFZedhv.dYImq0ivxCXESadYxj
2   // Token: 0x060000E3 RID: 227 RVA: 0x0000C8FC File Offset: 0x0000ACFC
3   [MethodImpl(MethodImplOptions.NoInlining)]
4   internal unsafe static object WSJGNRtMRstfRbcJ97T(object A_0, object A_1)
5   {
6       while (false)
7       {
8           object obj = *null;
9       }
10      return Path.ChangeExtension(A_0, A_1);
11  }
12
```

تصویر ۳: تغییر پسوند فایل‌ها

```
Path
8
9   namespace System.IO
10  {
11      // Token: 0x0200019C RID: 412
12      [ComVisible(true)]
13      [__DynamicallyInvokable]
14      public static class Path
15      {
16          // Token: 0x060018E3 RID: 6371 RVA: 0x00051D08 File Offset: 0x0004FF08
17          [__DynamicallyInvokable]
18          public static string ChangeExtension(string path, string extension)
19          {
20              if (path != null)
21              {
22                  Path.CheckInvalidPathChars(path, false);
23                  string text = path;
24                  int num = path.Length;
25                  while (--num >= 0)
26                  {
27                      char c = path[num];
28                      if (c == '.')
29                      {
30                          text = path.Substring(0, num);
31                          break;
32                      }
33                      if (c == Path.DirectorySeparatorChar || c == Path.AltDirectorySeparatorChar || c == Path.VolumeSeparatorChar)
34                      {
35                          break;
36                      }
37                  }
38                  if (extension != null && path.Length != 0)
39                  {
40                      if (extension.Length == 0 || extension[0] != '.')
41                      {
42                          text += ".";
43                      }
44                      text += extension;
45                  }
46                  return text;
47              }
48              return null;
49          }
```

تصویر ٤: کدمنبع تابع ChangeExtension()

باج‌افزار Crysis/Dharma (.Bip) فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می‌کند.

mscoree.dll
_CorExeMain

بر اساس بررسی‌های صورت گرفته، باج‌افزار Crysis/Dharma (.Bip) پس از اجرا، فرایندهای زیر را ایجاد می‌کند :

detrimentalnue.exe

- detrimentalnue.exe
  - cmd.exe
    - mode.com
    - vssadmin.exe vssadmin delete shadows /all /quiet

باج‌افزار Bip Crysis/Dharma. فرایند vssadmin.exe را به منظور حذف shadow copy و فرایند mode.com را نیز جهت نمایش پیغام باج‌خواهی اجرا می‌کند.

کلیدهای رجیستری زیر توسط باج‌افزار به سیستم افزوده می‌شود :

```
HKLM\SYSTEM\ControlSet٠٠١\services\VSS\Diag\SwProvider_{b٥٩٤٦١٣٧-٧b٩f-٤٩٢٥-af٨٠-٥١abd٦٠b٢٠d٥}

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\SwProvider_{b٥٩٤٦١٣٧-٧b٩f-٤٩٢٥-af٨٠-٥١abd٦٠b٢٠d٥}
```

همچنین مقادیر رجیستری زیر زیر به سیستم قربانی اضافه می‌شوند :

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\٠٤٤d٢d٣٦c٧e٧٣٧٧e٢٩da٧٦٩٣٩٧b٢e١٧٢b٢١acc٢a
٠٧a٦٧٦c٢٧٧d٠٣٣٥c٣٦e٠e٠١f.exe:
"C:\Windows\System٣٢\٠٤٤d٢d٣٦c٧e٧٣٧٧e٢٩da٧٦٩٣٩٧b٢e١٧٢b٢١acc٢a٠٧a٦٧٦c٢٧٧d٠٣٣٥c٣٦e٠e٠١f.exe"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\C:\Windows\System٣٢\Info.hta:"mshta.exe"C:\Windows\System٣٢\Info.hta""

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\C:\Users\SADEGH\AppData\Roaming\Info.hta:"mshta.exe "C:\Users\SADEGH\AppData\Roaming\Info.hta""

HKLM\SOFTWARE\Microsoft\Windows Search\RebuildIndex: ٠x٠٠٠٠٠٠٠٣

HKU\S١٥٢١٥٤٩٥٣٤٨٨٥١٠٨٤٣١١٥٩٨٣١١٥١٣٧١٠٢١٠٠٠\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF٥CDACE٢٤F٤F٩١٧٨٩٩٢٦F٤١٧٤٩EA}\Count\P:\Hfref\FNQRTU\Qrfxgbc\٠٤٤q٢q٣٦pVrV٣٧٧r٢٩qnV٦٩٣٩٧o٢٢١٧٢o٢١npp٢n٠Vn٦V٦p٣٧٧q٠٣٣op٣٦r٠r٠١s.rkr: ٠٠ ٠٠ ٠٠ ٠٠ ٠١ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٠ ٠٨٠ BF ٠٠ ٠٠ ٨٠ BF ٠٠ ٠٠ ٨٠ BF ٠٠ ٠٠ ٨٠ BF ٠٠ ٠٠ ٨٠ BF ٠٠ ٠٠ ٨٠ BF ٠٠ ٠٠ ٨٠ BF ٠٠ ٠٠ ٨٠ BF ٠٠ ٠٠ ٨٠ BF FF FF FF FF C٠ ٤C CB DC ٩B F٢D٣٠١ ٠٠ ٠٠ ٠٠ ٠٠

HKU\S١٥٢١٥٤٩٥٣٤٨٨٥١٠٨٤٣١١٥٩٨٣١١٥١٣٧١٠٢١٠٠٠\Software\Classes\LocalSettings\MuiCache\٢C\٥٢C٦٤BV E\@%systemroot%\system٣٢\timedate.cpl,-٥١: "Date and Time"

HKU\S١٥٢١٥٤٩٥٣٤٨٨٥١٠٨٤٣١١٥٩٨٣١١٥١٣٧١٠٢١٠٠٠\Software\Classes\LocalSettings\MuiCache\٢C\٥٢C٦٤BV E\@%ProgramFiles%\Windows Sidebar\sidebar.exe,-١٠١٢: "Add Desktop Gadgets that display personalized slideshows, news feeds, and other customized information."
```

HKU\S-۱-۵-۲۱-۱۵۴۹۵۳۴۸۸-۵۱۰۸۴۳۱۱۵۹-۸۳۱۱۵۱۳۷-۱۰۲۱۰۰۰\Software\Classes\LocalSettings\MuiCache\۲۴\۵۲C۶۴B۷E\@%ProgramFiles%\DVD Maker\DVDMaker.exe,-۶۳۳۸۵: "Burn pictures and video to DVD."

HKU\S-۱-۵-۲۱-۱۵۴۹۵۳۴۸۸-۵۱۰۸۴۳۱۱۵۹-۸۳۱۱۵۱۳۷-۱۰۲۱۰۰۰\Software\Classes\LocalSettings\MuiCache\۲۴\۵۲C۶۴B۷E\@%windir%\system۳۲\FXSRESM.dll,-۱۱۵: "Send and receive faxes or scan pictures and documents."

HKU\S-۱-۵-۲۱-۱۵۴۹۵۳۴۸۸-۵۱۰۸۴۳۱۱۵۹-۸۳۱۱۵۱۳۷-۱۰۲۱۰۰۰_Classes\LocalSettings\MuiCache\۲۴\۵۲C۶۴B۷E\@%systemroot%\system۳۲\timedate.cpl,-۵۱: "Date and Time"

HKU\S-۱-۵-۲۱-۱۵۴۹۵۳۴۸۸-۵۱۰۸۴۳۱۱۵۹-۸۳۱۱۵۱۳۷-۱۰۲۱۰۰۰_Classes\LocalSettings\MuiCache\۲۴\۵۲C۶۴B۷E\@%ProgramFiles%\Windows Sidebar\sidebar.exe,-۱۰۱۲: "Add Desktop Gadgets that display personalized slideshows, news feeds, and other customized information."

HKU\S-۱-۵-۲۱-۱۵۴۹۵۳۴۸۸-۵۱۰۸۴۳۱۱۵۹-۸۳۱۱۵۱۳۷-۱۰۲۱۰۰۰_Classes\LocalSettings\MuiCache\۲۴\۵۲C۶۴B۷E\@%ProgramFiles%\DVD Maker\DVDMaker.exe,-۶۳۳۸۵: "Burn pictures and video to DVD."

HKU\S-۱-۵-۲۱-۱۵۴۹۵۳۴۸۸-۵۱۰۸۴۳۱۱۵۹-۸۳۱۱۵۱۳۷-۱۰۲۱۰۰۰_Classes\LocalSettings\MuiCache\۲۴\۵۲C۶۴B۷E\@%windir%\system۳۲\FXSRESM.dll,-۱۱۵: "Send and receive faxes or scan pictures and documents."

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 Bip Crysis/Dharma. نشدیم.

شناسایی :

در حال حاضر تعداد ۴۳ مورد از ٦٤ 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.40242380	AegisLab	Ml.Attribute.Gen!c
ALYac	Trojan.Ransom.Crysis	Arcabit	Trojan.Generic.D2660CCC
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Kryptik.rrsjw	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Trojan.GenericKD.40242380
CAT-QuickHeal	Trojan.IGENERIC	Comodo	UnclassifiedMalware
Cyren	W32/Trojan.ZWGI-1399	DrWeb	Trojan.Encoder.3953
Emsisoft	Trojan.GenericKD.40242380 (B)	Endgame	malicious (high confidence)
eScan	Trojan.GenericKD.40242380	ESET-NOD32	a variant of MSIL/Kryptik.NUQ
F-Secure	Trojan.GenericKD.40242380	Fortinet	MSIL/Kryptik.NLS!tr
GData	Trojan.GenericKD.40242380	Ikarus	Trojan-Ransom.Dharma
K7AntiVirus	Trojan (0052edd41)	K7GW	Trojan (0052edd41)
Kaspersky	Trojan.Win32.Scarsi.atia	Malwarebytes	Ransom.Crysis
MAX	malware (ai score=97)	McAfee	Ransom-O
McAfee-GW-Edition	Ransom-O	Palo Alto Networks	generic.ml
Panda	Trj/RnkBend.A	Qihoo-360	Trojan.Generic
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Trojan.Gen.2
Tencent	Win32.Trojan.Scarsi.Swky	TrendMicro	TROJ_GEN.R002C0OEH18
TrendMicro-HouseCall	TROJ_GEN.R002C0OEH18	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Trojan.Gen	Yandex	Trojan.Scarsi!kOeeHJ4hGoY
ZoneAlarm	Trojan.Win32.Scarsi.atia	AhnLab-V3	Clean