باسمه تعالی

بررسی و تحلیل باج افزار

BlackRouter Dark Ransomware

تاریخ نگارش :

۱۳۹۷/۱۰/۳۰

خلاصه:

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از ظهور فعالیت سایبری جدید مهاجمین فارسی زبان در شبکه‌های اجتماعی در زمینه توسعه و انتشار باج‌افزار خبر می‌دهد. طبق آخرین مشاهدات صورت گرفته، این فعالیت در قالب RaaS (باج‌افزار به عنوان یک سرویس) در گروه‌ها و کانال‌های تلگرامی در حال شکل‌گیری و رشد بوده است. با توجه اینکه امروزه کدمنبع اغلب باج‌افزارها در فضای سایبری (از جمله وب تاریک) موجود بوده و قابل سفارشی‌سازی است، معمولاً مهاجمین با دانش متوسط از طریق کلاهبرداری و اخذ مبالغ هنگفت از کاربران ناآگاه و همچنین با تکیه بر روش‌های مهندسی اجتماعی، برای نیل به اهداف خرابکارانه خود از آن‌ها بهره می‌برند. یکی از فعالیت‌های اخیر این افراد در شبکه‌های اجتماعی فارسی‌زبان، تحت عنوان پروژه BlackRouter Dark Ransomware شناخته شده است. فعالیت این پروژه در زمان نگارش این گزارش متوقف گردیده است. لازم به توضیح است که در این گزارش، از ذکر مشخصات و اسامی افراد و گروه‌ها، خودداری گردیده است.

شواهد و یافته‌ها

پروژه BlackRouter Dark Ransomware برای اولین‌بار در تاریخ ۸ دی‌ماه ۹۷ توسط یکی از کاربران در شبکه اجتماعی توییتر مطرح گردید. پس از بررسی‌های صورت گرفته و جست‌وجو در فضای وب، تبلیغات مرتبط با این موضوع در یکی از کانال‌های تلگرامی که در زمینه انتشار انواع نرم‌افزارهای غیر قانونی قفل شکن، فیلترشکن و ... فعالیت داشت، مشاهده گردید. بر اساس شواهد بدست آمده، کاربر مذکور (مهاجم) قصد داشت پروژه خود را در قالب RaaS (باج‌افزار به عنوان سرویس با همکاری مهاجمین همکار و تولید کننده زیرساخت حمله) انتشار و گسترش دهد.

بر اساس اطلاعات گروه اصلی سازندگان باج‌افزار بصورت، جزئیات بیشتری از پروژه مذکور به شرح زیر است:

۱. درآمد از تارگت ها ۸۰ به ۲۰ است که ۸۰ درصدش مال شماست و ۲۰ درصد مابقی درآمد صرف پروژه

۲. تو باج افزار ۲ تا آدرس بیت کوین قرار داده میشه که شامل آدرس شما و آدرس بنده است تارگت موظفه به هردو واریز کنه جلو آدرس ها مبلغ بصورت خودکار تعیین میشه.

۳. مبلغ شروع درخواست از تارگت از ۵۰۰ دلار می باشد هر ۲ روز ۵۰۰ دلار دیگه بهش اضافه میشه و نهایتا به ۵۰۰۰ هزار دلار میرسه

٤. باج افزار تنها در تارگت های خارجی باید استفاده شود و اگر در تارگت ایرانی بزنید مسئولیتش با شماست

۵. تماس تارگت با ما از طریق ایمیله ولی بعد قراره بگیرم ربات تلگرام بزنم چت کنیم با قربانی

٦. ما به اینکه آنتی ویروس ممکنه باج افزار رو تشخیص بده یا نه کار نداریم , مهم اینه باج افزار رو تارگت ران شه و فایلاش قفل شه.

۷. هرچه تارگت بیشتر شانس بیشتر برای بدست آوردن پول

۸. دیکریپتر بصورت خودکار پس از پرداخت برای قربانی ارسال میشه

۹. رو هر تارگتی باج افزار اجرا بشه یک فایل لوگ تو سرورم ایجاد میشه و اطلاعاتشو می تونید ببنید.

توضیحات کلی باج افزار

باج افزار نسخه ویندوزه که میتونید هم رو pc بندازیم با ترفند های مختلف

یا میتونین روی سرور های مجازی بندازین

اگه رو pc بندازین احتمال پرداخت تارگت بیشتر هست چون اطلاعاتش حساس تره

اگه بخواین رو سرور بندازین رو سرور هایی بندازین که هاردشون حداقل ٤۰ گیگ استفاده شده باشه

مهم نیست حتما یوزر اصلی باشه رو یوزر guest و بدون دسترسی هم میتونین ران کنین که فقط پوشه user کد نمیشه و زیادم مهم

برای اینکه با تبلیغات تارگت بزنین اول باج افزار رو باید کنید که میتونین با توجه به مطلب کانال فالب رو بزنین که اکثرا سکسی و فالور و ممبر بیشتر تارگت جذب میکنن

شما فقط کافیه باج افزار رو ران کنین

بعد از ران کردن شروع به کد کردن فایل ها میکنه پس مدتی طول میکشه تا کد کنه بعد از اینکه فایل ها قفل شد صفحه ای که در پایین شاتش رو میزارم بالا میاد

خب میرسیم به مقدار باج خواهی

مقدار اولیه باج خواهی ۳۰۰ دلاره که ۳۰ درصد اون میرسه به صاحب پروژه black router و بقیه یعنی ۷۰ درصد ($۲۰۰) میره به والت شما

این مبلغ هر دوروز دوبرابر میشه یعنی بعد از دوروز میشه ۶۰۰ دلار و بعد از دوروز میشه ۱۲۰۰ دلار پرداخت ها نیز در کانال اطلاع رسانی نمایش داده خواهد شد و بالاتر از ۹۶۰۰ دلار نمیره

تارگت ایرانی نزنین جز دردسر چیزی نمیمونه براتون اینو مطمعن باشید

تارگت امریکایی بهترین تارگته به نظر من

بررسی‌ها نشان می‌دهد که مهاجم برای مدیریت باج‌افزار و اعضای گروه خود، دو کانال تلگرامی راه اندازی نموده است. در کانال اول، نمونه‌های باج‌افزار سفارشی سازی شده هر یک از اعضاء با نام مستعار آن‌ها، در اختیار آنان قرار می‌گیرد. اما در کانال دوم که BlackRouter Target Logs نام دارد، رباتی تعبیه شـــده که از آن به منظور دریافت اطلاعات سیستم قربانی استفاده می‌گردد. نمونه اطلاعات ارسالی به این کانال به شرح زیر می‌باشد :

Attacker: [redacted]

Target ID: BFEBFBFF000206A7

Target Name: ACTSERVER

Target OS: Microsoft Windows Server 2008 R2 Standard, 64-bit

Target CPU: Intel:registered: Xeon:registered: CPU E31220 @ 3.10GHz

Target RAM: 16384 MB

Target IP: [redacted]

Target Location: https://www.ip-tracker.org/locator/ip-lookup.php?ip=[redacted]

Target Payout: N/A

لازم به توضیح است که گروه اصلی پروژه BlackRouter Dark Ransomware در زمان شروع حمله، تعداد ۵۵ عضو داشت. این بدین معناست که ۵۵ نمونه فایل باج‌افزار مختلف اما با ویژگی‌های مشابه، برای اعضای گروه سفارشی سازی شده و در حال انتشار در فضای اینترنت بود. با تبلیغات گسترده‌ای که انجام گردید، تعداد اعضاء به سرعت در حال افزایش بود. مدیر گروه مذکور ضمن پاسخگویی به سؤالات اعضای گروه در خصوص پروژه، تأکید زیادی بر استفاده از باج‌افزار خود در اهداف خارج از کشور داشت. از هر یک از اعضاء به محض ورود به گروه و اعلام مشارکت در پروژه، یک نام مستعار و یک آدرس کیف پول بیت‌کوین اخذ می‌گردید. بعداً از این اطلاعات به منظور سفارشی‌سازی نمونه باج‌افزار برای اعضاء استفاده می‌شد.

بررســی‌های صــورت گرفته نشــان می‌دهد که توســعه دهنگان باج‌افزار مذکور، تیمی متشــکل از چند نفر می‌باشـــند. طبق اظهارات مدیر گروه، تیم مذکور با توســـعه دهندگان باج‌افزار معروف GandCrab نیز در

ارتباط بوده و احتمالاً از دانش آنان برای توسعه باج‌افزار خود بهره می‌برند. به این موضوع بارها در گروه اشاره شده، اما صحت و سقم این ادعا هنوز مشخص نیست.

نکته قابل ملاحظه‌ای که در خصوص نحوه انتشار باج‌افزار BlackRouter وجود دارد این است که ابزاری به نام Celesty Binder توسط توسعه دهندگان باج‌افزار در گروه به اشتراک گذاشته شد که اعضا به کمک آن قادر بودند نمونه‌ی باج‌افزار خود را در پوشش هر فایل یا نرم‌افزار دلخواه خود، ادغام و منتشر نمایند.

مشاهدات حاکی از آن است که در بین اعضای گروه، کاربرانی با دانش هک و کرک وجود دارند که از این باج‌افزار برای پیشبرد اهداف خرابکارانه خود از جمله خودنمایی، انتقام‌جویی و کسب درآمد بهره می‌برند. به گونه‌ای که تنها پس از گذشت ۱۸ ساعت از انتشار باج‌افزار، تعداد ٤٥ سرور مختلف در فضای اینترنت ابتدا توسط اعضا مورد نفوذ قرار گرفته و سپس اطلاعات آن‌ها رمزگذاری گردید.

تحلیل فنی باج‌افزار BlackRouter

پس از تحلیل و اجرای یکی از نمونه‌های باج‌افزار BlackRouter با مشخصات زیر در محیط آزمایشگاهی، نتایج زیر بدست آمد :

نام فایل	SF.exe
MD5	ebad44d2a8c72765aa64bae691458a34
SHA-1	f5a88a9eb718510d5abf3179f1edc19195df576f
SHA-256	f15a3e297b9017c40276ad1c32d606c8beebbf432227b47360f3674bfb60127۱
اندازه فایل	۲/۷۴ MB
پکر	Nulldev v1.0.0-custom

طبق مشاهدات صورت گرفته، باج‌افزار BlackRouter از خانواده باج‌افزار BlackHeart بوده که برای نخستین بار در اواخر ماه آوریل سال ۲۰۱۸ میلادی مشاهده گردید. براساس بررسی‌های صورت گرفته، به نظر می رسد کدهای باج افزار BlackHeart بسیار شبیه به باج افزار Spartacus است. کارشناسان بر این باورند که کد منبع باج‌افزار Spartacus که در اوایل ماه آوریل ۲۰۱۸ شروع به فعالیت کرد، به صورت کیت‌های سازنده (Builder Kit) در دارک‌وب موجود است و افراد می‌توانند با استفاده از آن، باج‌افزاری شبیه باج‌افزار اصلی ولی با ویژگی‌های متفاوت بسازند. بررسی بیشتر کدهای باج‌افزار BlackRouter نشان می‌دهد که مهاجمین از یک App در داخل این باج‌افزار استفاده کرده‌اند. هدف از گنجاندن App در داخل

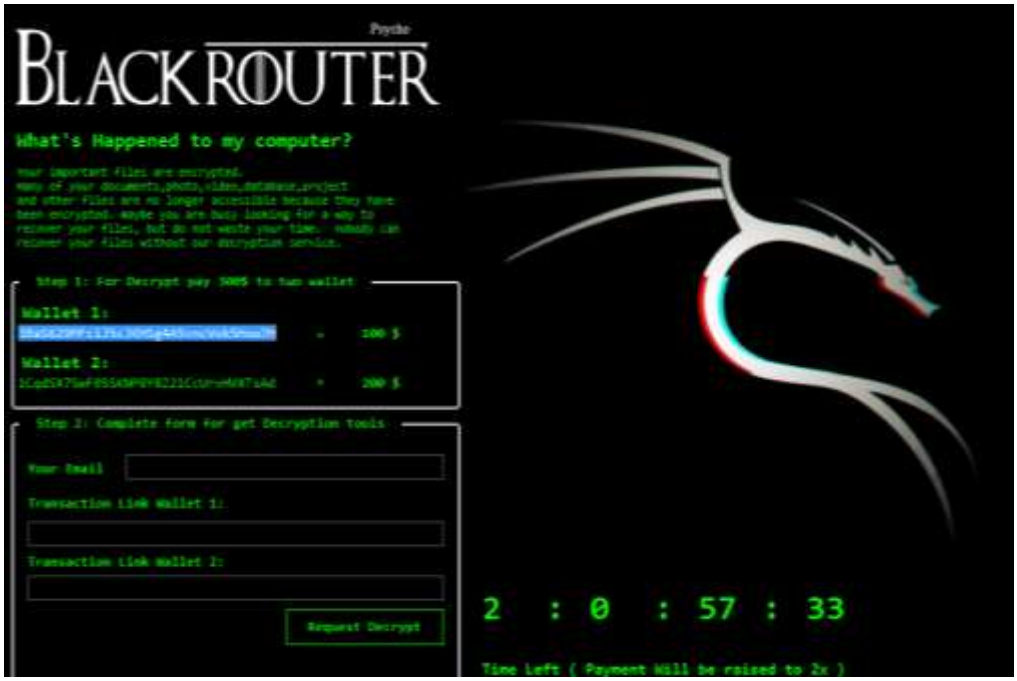
برنامه، برقراری ارتباط با قربانیان از طریق ربات و یا موارد م شابه می‌با شد. این مو ضوع تو سط مهاجم نیز اشاره شده بود.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v1">
    <assemblyIdentity name="MyApplication.app" version="1.0.0.0"/>
  - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    - <security>
      - <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
          <requestedExecutionLevel uiAccess="false" level="asInvoker"/>
        </requestedPrivileges>
      </security>
    </trustInfo>
</assembly>
```

باج‌افزار BlackRouter پس از اجرا در سیستم قربانی، دایرکتوری‌های حساس سیستم را پویش کرده و شروع به رمزگذاری فایل‌ها می‌کند.

```
145     private static readonly string string_5 = Environment.GetFolderPath(Environment.SpecialFolder.System);
146
147     // Token: 0x04000060 RID: 96
148     private static readonly string string_6 = Path.GetPathRoot(Class0.string_5);
149
150     // Token: 0x04000061 RID: 97
151     [CompilerGenerated]
152     [DebuggerBrowsable(DebuggerBrowsableState.Never)]
153     private static readonly string string_7;
154
155     // Token: 0x04000062 RID: 98
156     public static readonly string string_8 = Environment.GetFolderPath(Environment.SpecialFolder.Desktop);
157
158     // Token: 0x04000063 RID: 99
159     private static readonly string string_9 = Environment.GetFolderPath(Environment.SpecialFolder.MyComputer);
160
161     // Token: 0x04000064 RID: 100
162     private static readonly string string_10 = Environment.GetFolderPath
163       (Environment.SpecialFolder.DesktopDirectory);
164
165     // Token: 0x04000065 RID: 101
166     private static readonly string string_11 = Environment.GetFolderPath(Environment.SpecialFolder.Favorites);
167
168     // Token: 0x04000066 RID: 102
169     private static readonly string string_12 = Environment.GetFolderPath(Environment.SpecialFolder.Personal);
170
171     // Token: 0x04000067 RID: 103
172     private static readonly string string_13 = Environment.GetFolderPath(Environment.SpecialFolder.MyMusic);
173
174     // Token: 0x04000068 RID: 104
175     private static readonly string string_14 = Environment.GetFolderPath(Environment.SpecialFolder.History);
176
177     // Token: 0x04000069 RID: 105
178     private static readonly string string_15 = Environment.GetFolderPath(Environment.SpecialFolder.Personal);
```

پیغام باج‌خواهی باج‌افزار BlackRouter به صورت زیر است :



بر اساس پیغام باج‌خواهی، دو مبلغ و دو کیف پول مختلف برای پرداخت باج در نظر گرفته شده است. کیف پول اول متعلق به تو سعه دهنده باج‌افزار و کیف پول دوم متعلق به فرد منت شر کننده می‌با شد. پس از پرداخت مبالغ باج ۱۰۰ و ۲۰۰ دلار در آدرس کیف پول‌های تعیین شده و بعد از وارد کردن ایمیل در کادر مشخص شده ابزار رمزگشایی در اختیار قربانی قرار می‌گیرد. مهلت پرداخت باج دو روز درنظر گرفته شده است و پس از آن مبلغ باج خواهی دوبرابر می شود. ضمناً قربانیان می‌بایست مبلغ باج ۱۰۰ دلار را به آدرس کیف پول اول و ۲۰۰ دلار به آدرس کیف پول دوم ارسال نمایند.

3BaS629MFciJ5cJKHSg4A5vncVok5Hxw7H

3BaS629MFciJ5cJKHSg4A5vncVok5Hxw7H

Total Received:	0.00105000
Total Sent:	0.00105000
Final Balance:	0.00000000
Total transactions:	2

Recent transactions:

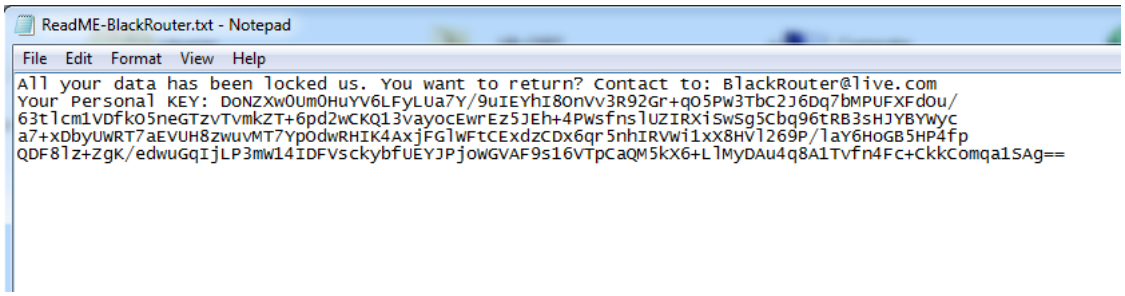
	Date ▼	Amount	Balance
	2018-12-19 17:30:09	-0.00105000	0.00000000
	2018-12-19 09:42:34	0.00105000	0.00105000

تصویر۱ : آدرس و تراکنش کیف پول اول

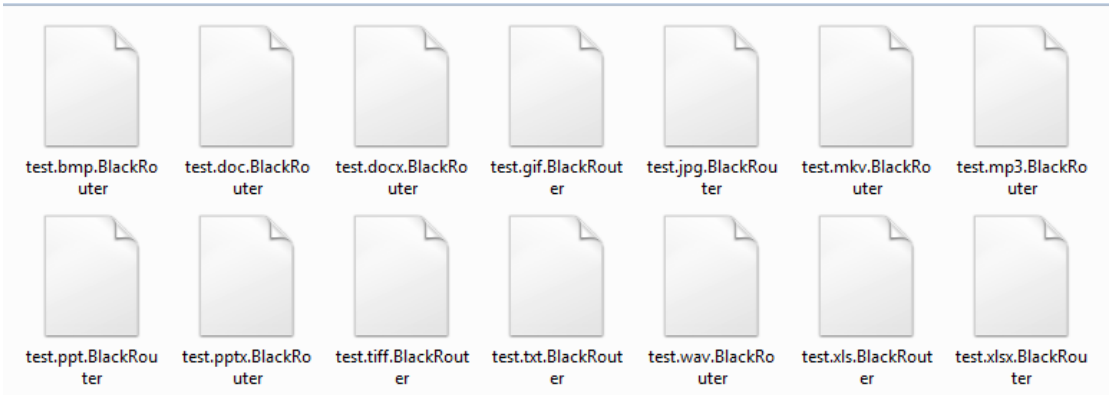
1CqdSX7SwFB5SKNP8Y8Z21CcUrvHVXTsAd

تصویر۱ : آدرس و تراکنش کیف پول دوم

فایل متنی پیغام باج‌خواهی که در تمام مسیرهای رمزگذاری شده ایجاد می‌گردد به صورت زیر می‌باشد:



باج‌افزار BlackRouter پس از رمزگذاری، پسوند BlackRouter. را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند.تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد:

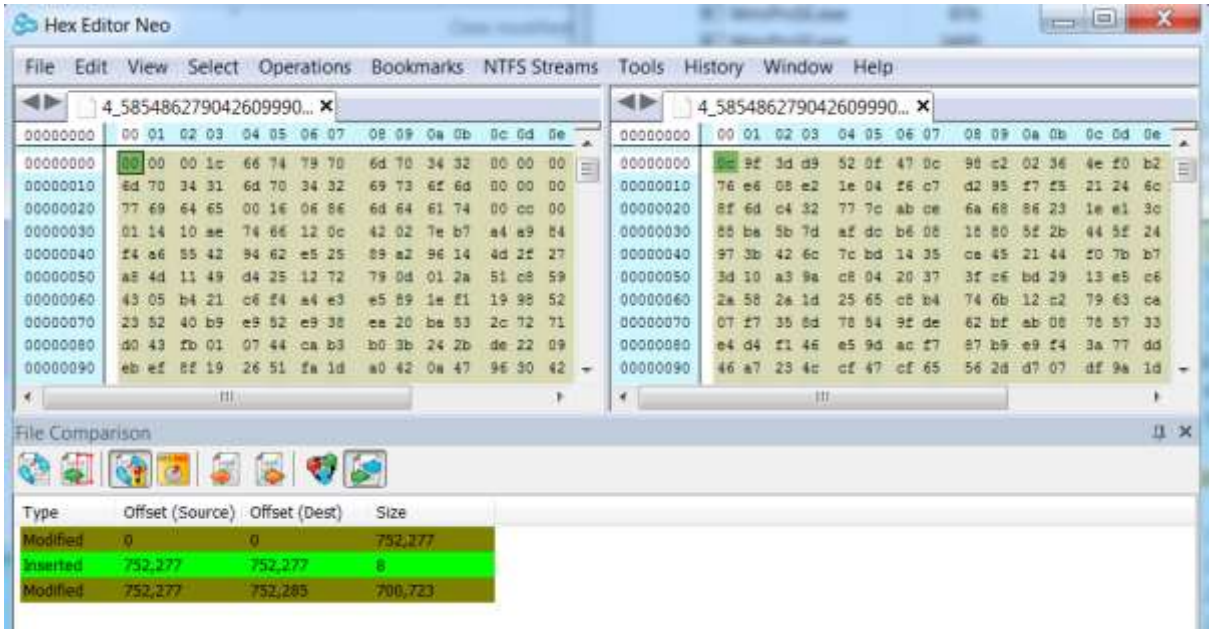


طبق بررسی صورت‌گرفته، باج‌افزار BlackRouter، پسوندهای زیر را مورد هدف قرار می‌دهد:

".exe", ".der", ".pfx", ".key", ".crt", ".csr", ".p12", ".pem", ".odt", ".sxw", ".stw", ".3ds", ".max", ".3dm", ".ods", ".sxc", ".stc", ".dif", ".slk", ".wb2", ".odp", ".sxd", ".std", ".sxm", ".sqlite3", ".sqlitedb", ".sql", ".accdb", ".mdb", ".dbf", ".odb", ".mdf", ".ldf", ".cpp", ".pas", ".asm", ".cmd", ".bat", ".vbs", ".sch", ".jsp", ".php", ".asp", ".java", ".jar", ".class", ".mp3", ".wav", ".swf", ".fla", ".wmv", ".mpg", ".vob",

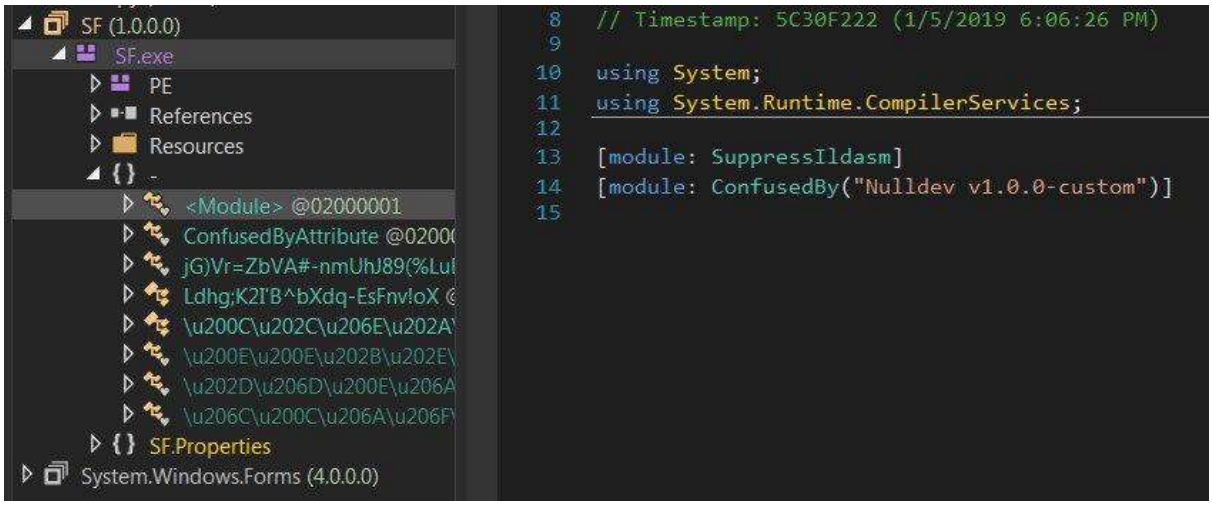
".mpeg", ".asf", ".avi", ".mov", ".mp4", ".mkv", ".flv", ".wma", ".mid", ".m3u", ".m4u", ".svg", ".psd", ".tiff", ".tif", ".raw", ".gif", ".png", ".bmp", ".jpg", ".jpeg", ".iso", ".backup", ".zip", ".rar", ".tgz", ".tar", ".bak", ".ARC", ".vmdk", ".vdi", ".sldm", ".sldx", ".sti", ".sxi", ".dwg", ".pdf", ".wk1", ".wks", ".rtf", ".csv", ".txt", ".msg", ".pst", ".ppsx", ".ppsm", ".pps", ".pot", ".pptm", ".pptx", ".ppt", ".xltm", ".xltx", ".xlc", ".xlm", ".xlt", ".xlw", ".xlsb", ".xlsm", ".xlsx", ".xls", ".dotm", ".dot", ".docm", ".docx", ".doc", ".ndf" , ".pdf" , ".ib" , ".ibk "

تصویر زیر مقایسه دو نمونه فایل، قبل و بعد از رمزگذاری را نشان می‌دهد :



طبق مشاهدات صورت گرفته ساختار فایل مورد نظر، تماماً پس از رمزگذاری باج‌افزار تغییرمی‌کند.

باج‌افزار مورد اشـــاره که با آنتروپی نســـبتاً بالایی (در اینجا ۸) پک شـــده، از روش ConfuserEx برای مبهم‌سازی کد و جلوگیری از مهندس معکوس توسط تحلیلگران بدافزار استفاده نموده است.



ascii	16	-	-	-	-	n/a	set_IsBackground
ascii	17	-	-	-	-	n/a	get_CurrentThread
ascii	14	-	-	-	-	n/a	get_IsAttached
ascii	9	-	-	-	-	n/a	IsLogging
ascii	11	-	-	-	-	n/a	get_IsAlive
ascii	10	-	-	-	-	n/a	get_Module
ascii	7	-	-	-	-	n/a	Marshal
ascii	12	-	-	-	-	n/a	GetHINSTANCE
ascii	22	-	-	-	-	n/a	get_FullyQualifiedName
ascii	9	-	-	-	-	n/a	get_Chars
ascii	14	-	-	-	-	n/a	GetElementType
ascii	14	-	-	-	-	n/a	CreateInstance
ascii	9	-	-	-	-	n/a	GetString
ascii	6	-	-	-	-	n/a	Intern
ascii	11	-	-	-	-	n/a	op_Equality
ascii	4	-	-	-	-	n/a	Math
ascii	21	-	-	-	-	n/a	Nulldev v1.0.0-custom
ascii	10	-	-	-	-	n/a	Copyright
ascii	6	-	-	-	-	n/a	2017
ascii	26	-	-	-	-	n/a	.NETFramework,Version=v4.0
ascii	20	-	-	-	-	n/a	FrameworkDisplayName
ascii	16	-	-	-	-	n/a	.NET Framework 4
ascii	7	-	-	-	-	n/a	1.0.0.0

طبق نتایج بدست آمده از تحلیل کد، الگوریتم رمزنگاری مورد استفاده توسط باج‌افزار، ترکیبی و از نوع AES و RSA-2048 در حالت EBC می‌باشد. لذا بدون کلید خصوصی مهاجم، احتمال رمزگشایی فایل‌ها تقریباً غیرممکن است.

```
Private Function smethod_2(string_0 As String, byte_0 As Byte()) As Byte()
    Dim result As Byte()
    Using rsacryptoServiceProvider As RSACryptoServiceProvider = New RSACryptoServiceProvider(2048)
        rsacryptoServiceProvider.PersistKeyInCsp = False
        rsacryptoServiceProvider.FromXmlString(string_0)
        result = rsacryptoServiceProvider.Encrypt(byte_0, True)
    End Using
    Return result
End Function
```

```
Public Function smethod_0(byte_0 As Byte(), string_0 As String) As Byte()
    Dim rijndaelManaged As RijndaelManaged = New RijndaelManaged()
    Dim array As Byte() = New Byte(31) {}
    Dim sourceArray As Byte() = New MD5CryptoServiceProvider().ComputeHash(Encoding.ASCII.GetBytes(string_0))
    Array.Copy(sourceArray, 0, array, 0, 16)
    Array.Copy(sourceArray, 0, array, 15, 16)
    rijndaelManaged.Key = array
    rijndaelManaged.Mode = CipherMode.ECB
    Dim cryptoTransform As ICryptoTransform = rijndaelManaged.CreateEncryptor()
    Return cryptoTransform.TransformFinalBlock(byte_0, 0, byte_0.Length)
End Function
```

در حال حاضر تعداد ۲۹ مورد از ۶۹ آنتی ویروس موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Variant.Ransom.BlackHeart.4	AegisLab	Trojan.Win32.BlackHeart.4!c
ALYac	Gen:Variant.Ransom.BlackHeart.4	Arcabit	Trojan.Ransom.BlackHeart.4
Avast	FileRepMalware	AVG	FileRepMalware
BitDefender	Gen:Variant.Ransom.BlackHeart.4	CAT-QuickHeal	Trojan.YakbeexMSIL.ZZ4
CrowdStrike Falcon	malicious_confidence_100% (W)	Cybereason	malicious.eb7185
Cylance	Unsafe	Cyren	W32/Trojan.VUGT-8331
Emsisoft	Gen:Variant.Ransom.BlackHeart.4 (B)	Endgame	malicious (high confidence)
eScan	Gen:Variant.Ransom.BlackHeart.4	F-Secure	Gen:Variant.Ransom.BlackHeart.4
GData	Gen:Variant.Ransom.BlackHeart.4	Kaspersky	HEUR:Trojan-Ransom.MSIL.Encoder.gen
McAfee	Artemis!E8AD44D2A8C7	McAfee-GW-Edition	BehavesLike.Win32.Backdoor.vc
Microsoft	Trojan:Win32/Occamy.C	Palo Alto Networks	generic.ml
Qihoo-360	Win32/Trojan.Ransom.eb7	SentinelOne	static engine - malicious
Sophos ML	heuristic	Symantec	ML.Attribute.HighConfidence
Trapmine	malicious.high.ml.score	TrendMicro-HouseCall	TROJ_GEN.R002H09A519
ZoneAlarm	HEUR:Trojan-Ransom.MSIL.Encoder.gen	Acronis	Clean