باسمه تعالی

# تحلیل فنی باج‌افزار

# Outsider

## مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور باج‌افزار Outsider خبر می‌دهد. فعالیت این باج‌افزار نخستین بار در تاریخ ۸ دسامبر ۲۰۱۸ میلادی گزارش شده است. براساس نتایج بدست آمده از تحلیل‌ها، سیستم‌هایی که زبان صفحه کلید روسی، بلاروسی یا تاتاری فعال دارند، از رمزگذاری توسط این باج‌افزار در امان هستند. طبق ادعای مهاجم یا مهاجمین، این باج‌افزار از الگوریتم RSA ۱۰۲٤بیتی برای رمزگذاری فایل‌های موردنظر خود استفاده می‌کند.

## مشخصات فایل اجرایی :

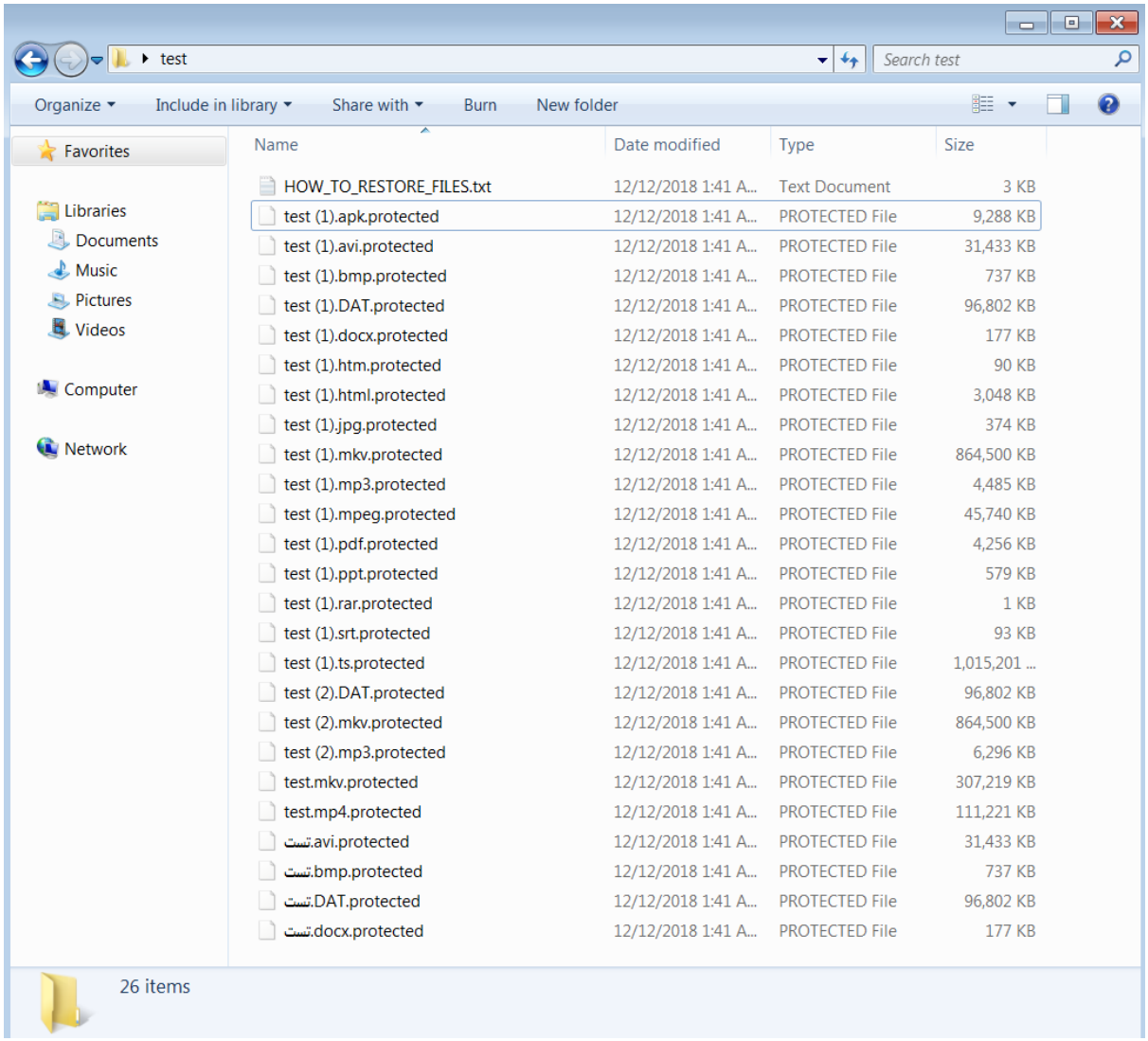
| نام فایل | ۹۰۰.exe |
|---|---|
| MD٥ | ٥a٤٣d٢db٥c٨cc٣b٨ec٢٧٣aa٤٧٠ccc٩٣١ |
| SHA-١ | dfcc٦٨٩٤٥b٩daf٧e٩f٤٩be٤٨٣٧a٦٩٣٤٥٦٠ec٦٣٥f |
| SHA-٢٥٦ | ٢٤٢٤a٧ce٥e٨٨٥bf٤٦٠aeb٨٩٦٨ceab٤٨٠٥٧٨١٣٤٣٠٩٧٣c٥a٢e٢٧d٨٤٦٥٥٣e٧٩٤٠٢c |
| اندازه فایل | ۱۲ کیلوبایت |

فایل اجرایی این باج‌افزار دارای ٤ بخش است :

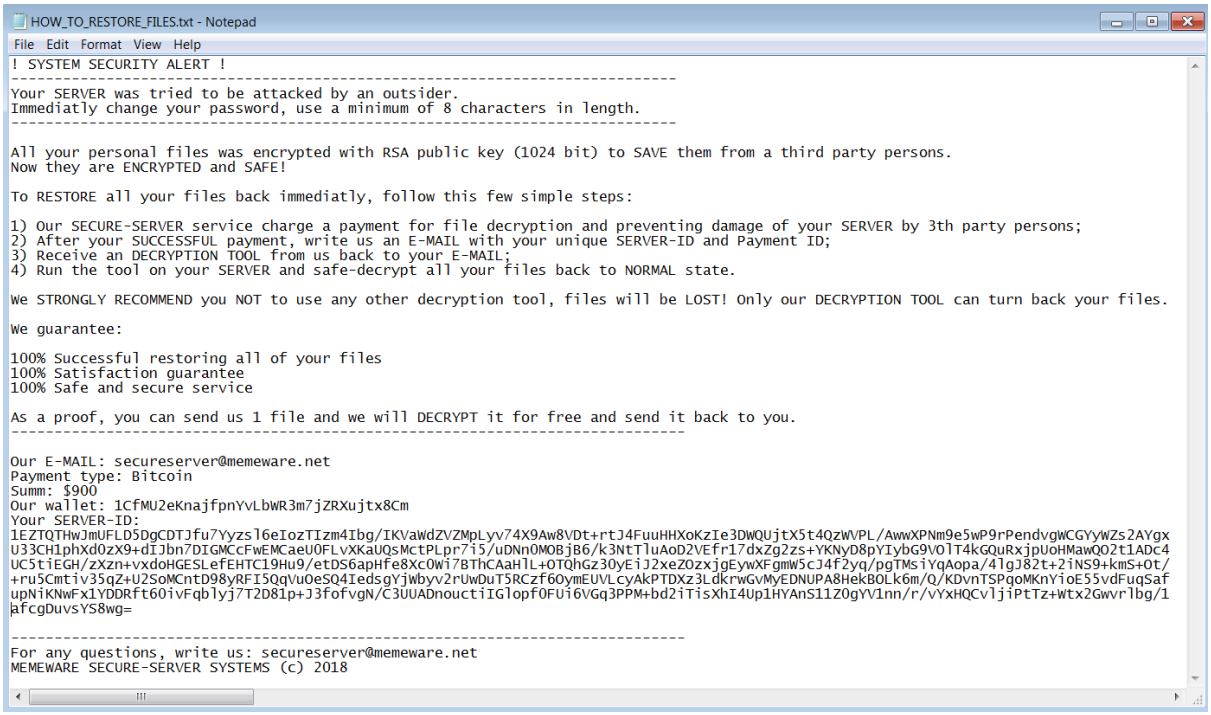
| نام بخش | آنتروپی | آدرس مجازی | اندازه مجازی | اندازه خام |
|---|---|---|---|---|
| .text | ٦.٤٦ | ٤٠٩٦ | ٨٣٢٧ | ٨٧٠٤ |
| .data | 0.32 | ١٦٣٨٤ | ٣٦ | ٥١٢ |
| .idata | 4.75 | ٢٠٤٨٠ | ١٤٨٦ | ١٥٣٦ |
| .reloc | 5.56 | ٢٤٥٧٦ | ٤١٢ | ٥١٢ |

## تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Outsider، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. این باج‌افزار به محض اجرا در سیستم قربانی، شروع به جست‌وجو و رمزگذاری فایل‌های موردنظر خود می‌کند. فایل‌های سیستم قربانی پس از رمزگذاری به شکل زیر تغییر پیدا می‌کنند:




همانطور که مشاهده می‌کنید، تمامی انواع فایل‌ها رمزگذاری شده‌اند و پسوند protected. به انتهای آن‌ها اضافه شده است. همچنین فایل پیغام باج‌خواهی با عنوان HOW_TO_RESTORE_FILES.txt در کنار فایل‌های رمزشده ایجاد شده است. البته این فایل درون هر پوشه حاوی فایل‌های رمزشده نیز، قرار می‌گیرد. با بررسی‌هایی که پس از رمزگذاری فایل‌ها بر روی مسیرهای مختلف سیستم عامل انجام دادیم، متوجه شدیم که این باج‌افزار قدرتمند تمامی انواع فایل‌ها حتی فایل‌های اجرایی با پسوند exe و فایل‌هایی با پسوند غیررایج را نیز، رمزگذاری کرده است. فقط پوشه‌های سیستم‌عامل و Program Files از رمزگذاری در امان مانده بودند. تصویر فایل پیغام باج‌خواهی این باج‌افزار را در ادامه مشاهده می‌کنید:




همانطور که در تصویر بالا مشاهده می‌کنید، در ابتدای این پیغام به شکلی هشدار دهنده عنوان شده است که سرور شما توسط یک outsider مورد حمله قرار گرفته است. فوراً پسورد خود را تغییر دهید، حداقل ۸ کاراکتر طولش باشد. سپس، در ادامه عنوان شده است که فایل‌های شما توسط الگوریتم RSA ۱۰۲٤بیتی رمزگذاری شده‌اند تا آن‌ها را از اشخاص دیگری درصورت دسترسی به سیستم شما، حفظ کنند؛ پس آن‌ها رمزگذاری شده‌اند و در امان هستند. سپس، دستورالعمل رمزگشایی فایل‌ها در ٤ بخش بیان شده است که بر اساس آن قربانی باید مبلغی را برای دریافت ابزار رمزگشایی پرداخت کند و پس از پرداخت موفق، شناسه سرور یا سیستم خود به همراه شناسه پرداخت را به آدرس ایمیل ذکرشده در پیغام ارسال کند سپس ابزار را از طریق این آدرس ایمیل دریافت می‌کند. در انتها باید ابزار را در سرور یا سیستم خود اجرا کند تا فایل‌ها رمزگشایی شوند. در ادامه، ابزار جهت رمزگشایی فایل‌ها تضمین شده است و عنوان شده است که یک فایل به صورت رایگان رمزگشایی می‌شود. در انتهای این پیغام نیز، اطلاعات زیر ذکر شده است:

آدرس ایمیل: secureserver@memeware.net

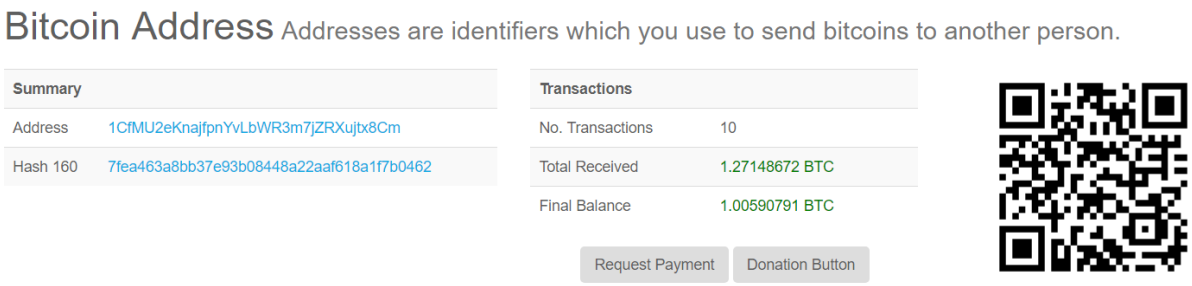
روش پرداخت: بیت‌کوین

مبلغ: ۹۰۰ دلار

آدرس کیف‌پول: ۱CfMU۲eKnajfpnYvLbWR۳mVjZRXujtx۸Cm

شناسه سرور: ۱EZ...

پس از رصد کیف‌پول این باج‌افزار، متوجه شدیم متأسفانه تاکنون تعداد ۱۰ تراکنش داشته است. اطلاعات مربوط به کیف‌پول این باج‌افزار را در تصویر زیر مشاهده می‌کنید:


Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

| Summary | |
|---|---|
| Address | 1CfMU2eKnajfpnYvLbWR3m7jZRXujtx8Cm |
| Hash 160 | 7fea463a8bb37e93b08448a22aaf618a1f7b0462 |

| Transactions | |
|---|---|
| No. Transactions | 10 |
| Total Received | 1.27148672 BTC |
| Final Balance | 1.00590791 BTC |

Request Payment  Donation Button

این باج‌افزار، پس از پایان فرآیند رمزگذاری فایل‌ها، متوقف می‌شود.

## تحلیل ایستا:

پس از تحلیل کد فایل اجرایی باج‌افزار نتایج زیر حاصل گردید:

همانطور که در قسمت قبل توضیح داده شد، این باج‌افزار محتوای پوشه‌های خاصی در سیستم‌عامل را رمزگذاری نمی‌کند. این پوشه‌ها در تصویر زیر قابل مشاهده می‌باشند:

```
.text:00401A14 aWindows:                               ; DATA XREF: .text:off_401BF4↓o
.text:00401A14                 unicode 0, <Windows>,0
.text:00401A24 aProgramFiles:                          ; DATA XREF: .text:00401BF8↓o
.text:00401A24                 unicode 0, <Program Files>,0
.text:00401A40 aProgramFilesX8:                        ; DATA XREF: .text:00401BFC↓o
.text:00401A40                 unicode 0, <Program Files (x86)>,0
.text:00401A68 aRecycle_bin:                           ; DATA XREF: .text:00401C00↓o
.text:00401A68                 unicode 0, <$Recycle.bin>,0
```

فضای VSS سیستم‌عامل، توسط این باج‌افزار حذف می‌شود:

```
.text:00401ADC String2:                                ; DATA XREF: sub_402617+F↓o
.text:00401ADC                 unicode 0, < delete shadows /all /quiet>,0
.text:00401B14                 align 8
.text:00401B18 ; const WCHAR ApplicationName
.text:00401B18 ApplicationName:                        ; DATA XREF: sub_402617+47↓o
.text:00401B18                 unicode 0, <C:\Windows\sysnative\vssadmin.exe>,0
```

پسوند اضافه شده به فایل‌ها پس از رمزگذاری آن‌ها و نام فایل پیغام باج‌خواهی باج‌افزار در قطعه کد زیر قابل مشاهده هستند:

```
.text:00402D36 loc_402D36:                             ; CODE XREF: sub_402C5D+A2Tj
.text:00402D36                 test    al, 0A7h
.text:00402D38                 jz      short loc_402D69
.text:00402D3A                 push    offset a_protected ; ".protected"
.text:00402D3F                 lea     eax, [esp+264h+FindFileData.cFileName]
.text:00402D43                 push    eax
.text:00402D44                 call    ds:StrStrIW
.text:00402D4A                 test    eax, eax
.text:00402D4C                 jnz     short loc_402D69
.text:00402D4E                 push    offset aHow_to_restore ; "HOW_TO_RESTORE_FILES.txt"
.text:00402D53                 lea     eax, [esp+264h+FindFileData.cFileName]
.text:00402D57                 push    eax             ; lpString1
.text:00402D58                 call    ds:lstrcmpW
.text:00402D5E                 test    eax, eax
.text:00402D60                 jz      short loc_402D69
.text:00402D62                 mov     ecx, esi        ; lpExistingFileName
.text:00402D64                 call    sub_4029B8
```

متن فایل پیغام باج‌خواهی در تصویر زیر قابل مشاهده است:

```
.text:00401390                 db '------------------------------------------------------------------'
.text:00401390                 db '------------',0Dh,0Ah
.text:00401390                 db 'Your SERVER was tried to be attacked by an outsider.',0Dh,0Ah
.text:00401390                 db 'Immediatly change your password, use a minimum of 8 characters in'
.text:00401390                 db ' length.',0Dh,0Ah
.text:00401390                 db '------------------------------------------------------------------'
.text:00401390                 db '------------',0Dh,0Ah
.text:00401390                 db 0Dh,0Ah
.text:00401390                 db 'All your personal files was encrypted with RSA public key (1024 b'
.text:00401390                 db 'it) to SAVE them from a third party persons. ',0Dh,0Ah
.text:00401390                 db 'Now they are ENCRYPTED and SAFE!',0Dh,0Ah
.text:00401390                 db 0Dh,0Ah
.text:00401390                 db 'To RESTORE all your files back immediatly, follow this few simple'
.text:00401390                 db ' steps:',0Dh,0Ah
.text:00401390                 db 0Dh,0Ah
.text:00401390                 db '1) Our SECURE-SERVER service charge a payment for file decryption'
.text:00401390                 db ' and preventing damage of your SERVER by 3th party persons;',0Dh,0Ah
.text:00401390                 db '2) After your SUCCESSFUL payment, write us an E-MAIL with your un'
.text:00401390                 db 'ique SERVER-ID and Payment ID;',0Dh,0Ah
.text:00401390                 db '3) Receive an DECRYPTION TOOL from us back to your E-MAIL;',0Dh,0Ah
.text:00401390                 db '4) Run the tool on your SERVER and safe-decrypt all your files ba'
.text:00401390                 db 'ck to NORMAL state.',0Dh,0Ah
.text:00401390                 db 0Dh,0Ah
.text:00401390                 db 'We STRONGLY RECOMMEND you NOT to use any other decryption tool, f'
.text:00401390                 db 'iles will be LOST! Only our DECRYPTION TOOL can turn back your fi'
.text:00401390                 db 'les.',0Dh,0Ah
.text:00401390                 db 0Dh,0Ah
.text:00401390                 db 'We guarantee:',0Dh,0Ah
.text:00401390                 db 0Dh,0Ah
.text:00401390                 db '100% Successful restoring all of your files',0Dh,0Ah
.text:00401390                 db '100% Satisfaction guarantee',0Dh,0Ah
.text:00401390                 db '100% Safe and secure service',0Dh,0Ah
.text:00401390                 db 0Dh,0Ah
.text:00401390                 db 'As a proof, you can send us 1 file and we will DECRYPT it for fre'
.text:00401390                 db 'e and send it back to you.',0Dh,0Ah
.text:00401390                 db '------------------------------------------------------------------'
```

از قطعه کد زیر برای یافتن فایل‌ها و مسیرهای مختلف در سیستم‌عامل استفاده شده است:

```
.text:00402C5D FindFileData    = _WIN32_FIND_DATAW ptr -250h
.text:00402C5D lpThreadParameter= dword ptr  8
.text:00402C5D
.text:00402C5D                 push    ebp
.text:00402C5E                 mov     ebp, esp
.text:00402C60                 and     esp, 0FFFFFFF8h
.text:00402C63                 sub     esp, 254h
.text:00402C69                 push    ebx
.text:00402C6A                 mov     ebx, ds:GetProcessHeap
.text:00402C70                 push    esi
.text:00402C71                 push    edi
.text:00402C72                 push    1003Eh          ; dwBytes
.text:00402C77                 push    8               ; dwFlags
.text:00402C79                 call    ebx ; GetProcessHeap
.text:00402C7B                 push    eax             ; hHeap
.text:00402C7C                 call    ds:HeapAlloc
.text:00402C82                 mov     esi, eax
.text:00402C84                 test    esi, esi
.text:00402C86                 jz      loc_402DB9
.text:00402C8C                 push    [ebp+lpThreadParameter]
.text:00402C8F                 push    offset aS       ; "%s\\*"
.text:00402C94                 push    7FFFh
.text:00402C99                 push    esi
.text:00402C9A                 call    ds:wnsprintfW
.text:00402CA0                 add     esp, 10h
.text:00402CA3                 lea     eax, [esp+260h+FindFileData]
.text:00402CA7                 push    eax             ; lpFindFileData
.text:00402CA8                 push    esi             ; lpFileName
.text:00402CA9                 call    ds:FindFirstFileW
.text:00402CAF                 cmp     eax, 0FFFFFFFFh
.text:00402CB2                 jz      loc_402DAD
.text:00402CB8                 mov     ebx, eax
.text:00402CBA
```

از تابع CryptEncrypt در قطعه کد زیر برای رمزگذاری فایل‌ها استفاده شده است. جهت تغییر در محتوای فایل‌ها نیز از تابع CreateFile استفاده شده است:

```
.text:00402A0D loc_402A0D:                             ; CODE XREF: sub_4029B8+5E↓j
.text:00402A0D                 mov     al, [edx+ecx]
.text:00402A10                 mov     [ecx], al
.text:00402A12                 inc     ecx
.text:00402A13                 sub     esi, 1
.text:00402A16                 jnz     short loc_402A0D
.text:00402A18                 push    30h             ; dwBufLen
.text:00402A1A                 lea     eax, [ebp+pdwDataLen]
.text:00402A1D                 push    eax             ; pdwDataLen
.text:00402A1E                 push    edi             ; pbData
.text:00402A1F                 push    esi             ; dwFlags
.text:00402A20                 push    1               ; Final
.text:00402A22                 push    esi             ; hHash
.text:00402A23                 push    phKey           ; hKey
.text:00402A29                 call    ds:CryptEncrypt
.text:00402A2F                 push    esi             ; hTemplateFile
.text:00402A30                 push    80h             ; dwFlagsAndAttributes
.text:00402A35                 push    3               ; dwCreationDisposition
.text:00402A37                 push    esi             ; lpSecurityAttributes
.text:00402A38                 push    1               ; dwShareMode
.text:00402A3A                 push    0C0000000h      ; dwDesiredAccess
.text:00402A3F                 push    ebx             ; lpFileName
.text:00402A40                 call    ds:CreateFileW
.text:00402A46                 mov     [ebp+hFile], eax
.text:00402A49                 cmp     eax, 0FFFFFFFFh
.text:00402A4C                 jz      loc_402C47
.text:00402A52                 mov     [ebp+var_14], esi
.text:00402A55                 mov     [ebp+var_10], esi
```

این باج‌افزار، از الگوریتم RSA ۴۰۹۶بیتی برای رمزگذاری کلید رمزگذاری فایل‌ها استفاده می‌کند. قطعه کد زیر مربوط به این قسمت می‌باشد:

```
.text:00403004 loc_403004:                             ; CODE XREF: start+57↑j
.text:00403004                 push    offset phKey    ; phKey
.text:00403009                 push    ebx             ; dwFlags
.text:0040300A                 push    ebx             ; hPubKey
.text:0040300B                 push    dword ptr [esi+8] ; dwDataLen
.text:0040300E                 push    dword ptr [esi] ; pbData
.text:00403010                 push    hProv           ; hProv
.text:00403016                 call    ds:CryptImportKey
.text:0040301C                 call    sub_401F70
.text:00403021                 mov     edi, eax
.text:00403023                 test    edi, edi
.text:00403025                 jz      short loc_403068
.text:00403027                 mov     ecx, [esi+0Ch]
.text:0040302A                 lea     eax, [ebp+pdwDataLen]
.text:0040302D                 push    200h 4096 Bit   ; dwBufLen
.text:00403032                 push    eax             ; pdwDataLen
.text:00403033                 lea     eax, [ebp+pbData]
.text:00403039                 mov     [ebp+pdwDataLen], ecx
.text:0040303C                 push    eax             ; pbData
.text:0040303D                 push    ebx             ; dwFlags
.text:0040303E                 push    1               ; Final
.text:00403040                 push    ebx             ; hHash
.text:00403041                 push    edi             ; hKey
.text:00403042                 call    ds:CryptEncrypt
.text:00403048                 test    eax, eax
.text:0040304A                 jz      short loc_403061
.text:0040304C                 mov     edx, [ebp+pdwDataLen]
.text:0040304F                 push    ecx
.text:00403050                 lea     ecx, [ebp+pbData]
.text:00403056                 call    sub_401E2F
.text:0040305B                 pop     ecx
.text:0040305C                 mov     lpBuffer, eax
```

طبق ادعای مهاجم یا مهاجمین در پیغام باج‌خواهی، این باج‌افزار از الگوریتم RSA ۱۰۲۴بیتی برای رمزگذاری فایل‌ها استفاده کرده است.

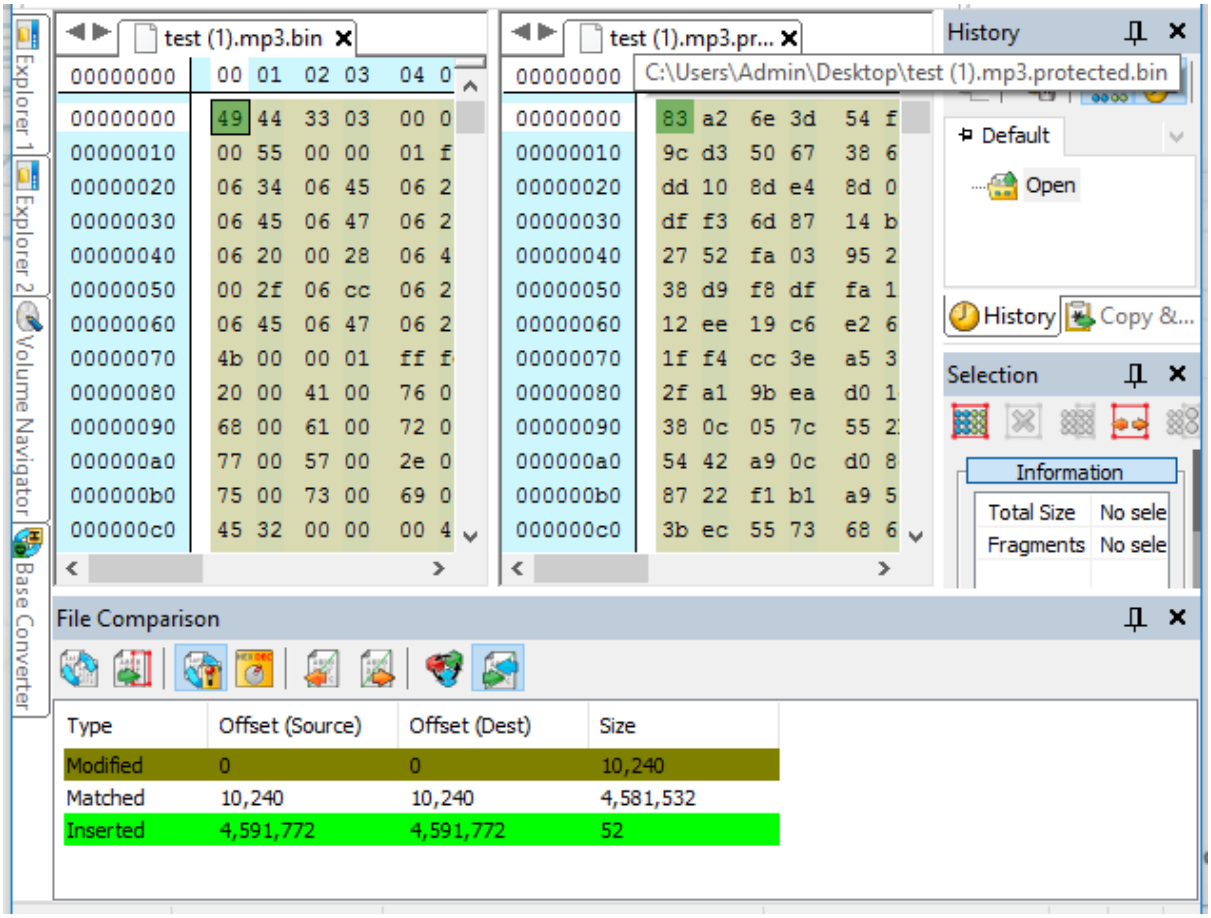
از قطعه کد زیر برای خواندن محتوای درون فایل‌ها استفاده شده است:

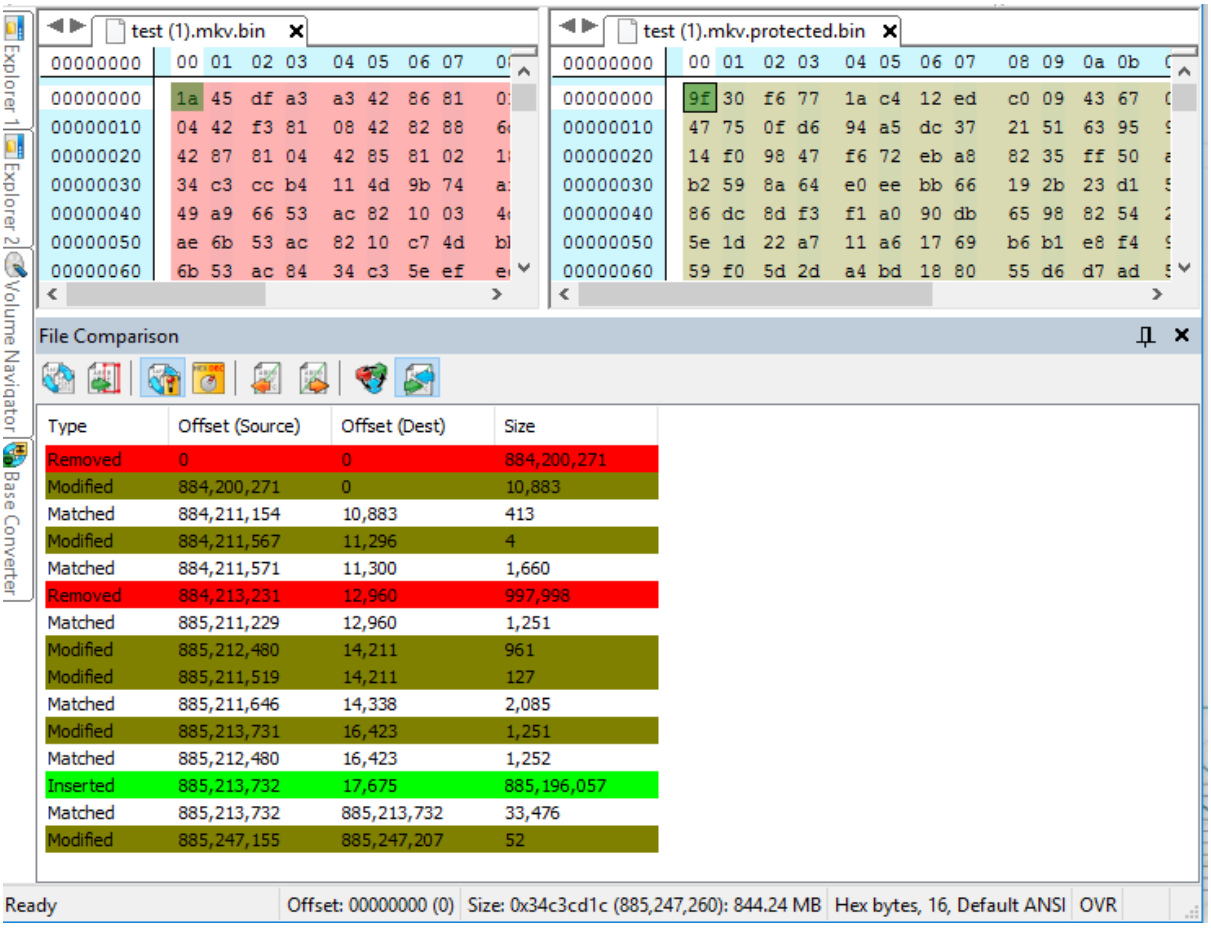
```
.text:00402AE1 loc_402AE1:                             ; CODE XREF: sub_4029B8+1D4↓j
.text:00402AE1                 xor     eax, eax
.text:00402AE3                 push    eax             ; lpOverlapped
.text:00402AE4                 lea     eax, [ebp+NumberOfBytesRead]
.text:00402AE7                 push    eax             ; lpNumberOfBytesRead
.text:00402AE8                 push    2800h10240 Byte ; nNumberOfBytesToRead
.text:00402AED                 push    ebx             ; lpBuffer
.text:00402AEE                 push    edi             ; hFile
.text:00402AEF                 call    ds:ReadFile
.text:00402AF5                 mov     ecx, [ebp+NumberOfBytesRead]
.text:00402AF8                 xor     eax, eax
.text:00402AFA                 mov     [ebp+var_10], ecx
.text:00402AFD                 cmp     ecx, eax
.text:00402AFF                 jbe     short loc_402B5B
.text:00402B01                 mov     edi, eax
```

همانطور که در تصویر بالا مشاهده می‌کنید، مقدار حجمی که از فایل‌ها خوانده می‌شود، مشخص شده است. در ادامه و در قطعه کد زیر، همین مقدار که در هر فایل نوشته می‌شود نیز، مشخص شده است:

```
.text:00402BCB          lea     eax, [ebp+NumberOfBytesRead]
.text:00402BCE          push    eax             ; lpNumberOfBytesWritten
.text:00402BCF          push    4               ; nNumberOfBytesToWrite
.text:00402BD1          lea     eax, [ebp+Buffer]
.text:00402BD4          push    eax             ; lpBuffer
.text:00402BD5          push    [ebp+hFile]     ; hFile
.text:00402BD8          call    ds:WriteFile
.text:00402BDE          xor     eax, eax
.text:00402BE0          push    eax             ; lpOverlapped
.text:00402BE1          lea     eax, [ebp+NumberOfBytesRead]
.text:00402BE4          push    eax             ; lpNumberOfBytesWritten
.text:00402BE5          push    30h             ; nNumberOfBytesToWrite
.text:00402BE7          push    edi             ; lpBuffer
.text:00402BE8          push    [ebp+hFile]     ; hFile
.text:00402BEB          call    ds:WriteFile
.text:00402BF1          push    [ebp+hFile]     ; hObject
.text:00402BF4          call    ds:CloseHandle
.text:00402BFA          push    1003Eh          ; dwBytes
.text:00402BFF          push    8               ; dwFlags
.text:00402C01          call    esi ; GetProcessHeap
.text:00402C03          push    eax             ; hHeap
.text:00402C04          call    ds:HeapAlloc
.text:00402C0A          mov     esi, eax
.text:00402C0C          test    esi, esi
.text:00402C0E          jz      short loc_402C45
.text:00402C10          push    offset a_protected ; ".protected"
.text:00402C15          push    ebx
.text:00402C16          push    offset aSS      ; "%s%s"
.text:00402C1B          push    7FFFh
.text:00402C20          push    esi
.text:00402C21          call    ds:wnsprintfW
.text:00402C27          add     esp, 14h
.text:00402C2A          push    esi             ; lpNewFileName
.text:00402C2B          push    ebx             ; lpExistingFileName
.text:00402C2C          call    ds:MoveFileW
```

همانطور که مشاهده می‌کنید، در هر فایل مقدار ۱۰۲۴۰بایت برابر با مقدار خوانده شده، نوشته می‌شود. با بررسی‌هایی که بر روی نمونه فایل‌های رمزشده و نمونه سالم آن‌ها انجام دادیم، متوجه شدیم این باج‌افزار دقیقا معادل همین مقدار از هر فایل را تغییر می‌دهد. البته این موضوع در رابطه با فایل‌های با حجم چند صد مگابایت صدق نمی‌کند و تغییرات در فایل‌های با این حجم کاملا متغیر و نامنظم است. نتایج مربوط به مقایسه دو نمونه فایل با حجم‌های مختلف در ادامه مشاهده می‌کنید:


test (1).mp3.bin
test (1).mp3.pr...
C:\Users\Admin\Desktop\test (1).mp3.protected.bin
History
Default
Open
History
Copy &...
Selection
Information
Total Size
No sele
Fragments
No sele
Explorer 1
Explorer 2
Volume Navigator
Base Converter
File Comparison
Type
Offset (Source)
Offset (Dest)
Size
Modified 0 0 10,240
Matched 10,240 10,240 4,581,532
Inserted 4,591,772 4,591,772 52


test (1).mkv.bin
test (1).mkv.protected.bin
Explorer 1
Explorer 2
Volume Navigator
Base Converter
File Comparison
Type
Offset (Source)
Offset (Dest)
Size
Removed 0 0 884,200,271
Modified 884,200,271 0 10,883
Matched 884,211,154 10,883 413
Modified 884,211,567 11,296 4
Matched 884,211,571 11,300 1,660
Removed 884,213,231 12,960 997,998
Matched 885,211,229 12,960 1,251
Modified 885,212,480 14,211 961
Modified 885,211,519 14,211 127
Matched 885,211,646 14,338 2,085
Modified 885,213,731 16,423 1,251
Matched 885,212,480 16,423 1,252
Inserted 885,213,732 17,675 885,196,057
Matched 885,213,732 885,213,732 33,476
Modified 885,247,155 885,247,207 52
Ready
Offset: 00000000 (0)
Size: 0x34c3cd1c (885,247,260): 844.24 MB
Hex bytes, 16, Default ANSI
OVR

باج‌افزار Outsider زبان صفحه کلید سیستم‌های مورد حمله خود را بررسی می‌کند و در صورتی که سیستمی دارای یکی از زبان‌های روسی، بلاروسی و تاتاری در زبان‌های صفحه کلید خود باشد، درون آن اجرا نمی‌شود. قطعه کد زیر مربوط به این قسمت می‌باشد:

```
t:004027AC                push    ebp
t:004027AD                mov     ebp, esp
t:004027AF                sub     esp, 10h
t:004027B2                call    ds:GetUserDefaultLangID
t:004027B8                mov     ecx, 419h
t:004027BD                movzx   eax, ax
t:004027C0                mov     [ebp+var_8], ecx
t:004027C3                cmp     ax, cx
t:004027C6                jz      loc_40288D
t:004027CC                add     ecx, 26h
t:004027CF                cmp     ax, cx
t:004027D2                jz      loc_40288D
t:004027D8                mov     ecx, 423h
t:004027DD                mov     [ebp+var_C], ecx
t:004027E0                cmp     ax, cx
t:004027E3                jz      loc_40288D
t:004027E9                dec     ecx
t:004027EA                mov     [ebp+var_10], ecx
t:004027ED                cmp     ax, cx
t:004027F0                jz      loc_40288D
t:004027F6                mov     ecx, 444h
t:004027FB                cmp     ax, cx
t:004027FE                jz      loc_40288D
t:00402804                push    ebx
t:00402805                mov     ebx, ds:GetKeyboardLayoutList
t:0040280B                xor     eax, eax
t:0040280D                push    esi
t:0040280E                push    edi
t:0040280F                push    eax             ; lpList
t:00402810                push    eax             ; nBuff
t:00402811                mov     [ebp+var_1], al
t:00402814                call    ebx ; GetKeyboardLayoutList
```

همانطور که در قسمت قبل توضیح داده شد، این باج‌افزار پس از پایان فعالیت خود در سیستم قربانی متوقف می‌شود. قطعه کد مربوط به این قسمت را در تصویر زیر مشاهده می‌کنید:

```
.text:004028D2 loc_4028D2:                             ; CODE XREF: sub_402893+82↓j
.text:004028D2                push    ds:off_401C0C[edi] ; lpString2
.text:004028D8                lea     eax, [ebp+pe.szExeFile]
.text:004028DE                push    eax             ; lpString1
.text:004028DF                call    ds:lstrcmpW
.text:004028E5                test    eax, eax
.text:004028E7                jnz     short loc_40290F
.text:004028E9                push    [ebp+pe.th32ProcessID] ; dwProcessId
.text:004028EF                push    eax             ; bInheritHandle
.text:004028F0                push    1               ; dwDesiredAccess
.text:004028F2                call    ds:OpenProcess
.text:004028F8                mov     ebx, eax
.text:004028FA                cmp     ebx, 0FFFFFFFFh
.text:004028FD                jz      short loc_40290F
.text:004028FF                push    0               ; uExitCode
.text:00402901                push    ebx             ; hProcess
.text:00402902                call    ds:TerminateProcess
.text:00402908                push    ebx             ; hObject
.text:00402909                call    ds:CloseHandle
```

## تحلیل ترافیک شبکه :

پس از اجرای باج‌افزار در محیط آزمایشگاهی و سندباکس‌های آنلاین و بررسی ترافیک شبکه ایجاد شده، هیچگونه ترافیک مشکوکی مربوط به باج‌افزار مشاهده نکردیم. این باج‌افزار در حالت آفلاین بدون هیچ مشکلی اجرا می‌شود.

## خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد مورد ٤٤ از ٧٠ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

| | | | |
|---|---|---|---|
| Ad-Aware | Gen:Heur.Zard.2 | AhnLab-V3 | Malware/Gen.Generic.C2883682 |
| ALYac | Trojan.Ransom.Filecoder | Arcabit | Trojan.Zard.2 |
| Avast | Win32:Malware-gen | AVG | Win32:Malware-gen |
| Avira | HEUR/AGEN.1036376 | BitDefender | Gen:Heur.Zard.2 |
| Bkav | W32.AIDetectVM.malware | Comodo | Malware@#bhu02exbarru |
| CrowdStrike Falcon | malicious_confidence_70% (W) | Cybereason | malicious.b5c8cc |
| Cylance | Unsafe | DrWeb | Trojan.Encoder.26800 |
| Emsisoft | Gen:Heur.Zard.2 (B) | eScan | Gen:Heur.Zard.2 |
| ESET-NOD32 | a variant of Win32/Filecoder.NTL | F-Secure | Gen:Heur.Zard.2 |
| Fortinet | W32/Filecoder.NTL!tr | GData | Gen:Heur.Zard.2 |
| Ikarus | Trojan-Ransom.FileCoder | K7AntiVirus | Trojan ( 005425ed1 ) |
| K7GW | Trojan ( 005425ed1 ) | Kaspersky | Trojan-Ransom.Win32.Cryptor.cdk |
| Malwarebytes | Ransom.FileCryptor | MAX | malware (ai score=87) |
| McAfee | Artemis!5A43D2DB5C8C | McAfee-GW-Edition | BehavesLike.Win32.Upatre.lm |
| Microsoft | Trojan:Win32/Occamy.C | NANO-Antivirus | Trojan.Win32.Encoder.fkxgvm |
| Palo Alto Networks | generic.ml | Panda | Trj/GdSda.A |
| Qihoo-360 | Win32/Trojan.Ransom.1bd | Rising | Malware.Heuristic!ET#92% (RDM+:cmRtazojBVocGRHxtt3j2XfLN... |
| Sophos AV | Mal/EncPk-ZC | Sophos ML | heuristic |
| Symantec | ML.Attribute.HighConfidence | Tencent | Win32.Trojan.Cryptor.Swbb |
| Trapmine | malicious.moderate.ml.score | TrendMicro | Ransom.Win32.OUTSIDER.THABAOAH |
| TrendMicro-HouseCall | Ransom.Win32.OUTSIDER.THABAOAH | VBA32 | BScope.Trojan.Dynamer |
| VIPRE | Trojan.Win32.Generic!BT | ZoneAlarm | Trojan-Ransom.Win32.Cryptor.cdk |

## خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ٤ مورد از ١٤ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

**نتایج اسکن:**

| آنتی ویروس | نتیجه اسکن | |
|---|---|---|
| comodo | ii | Dangerous |
| drweb | ii | Dangerous<br>Trojan.Encoder.26800 |
| eset | ii | Dangerous<br>a variant of Win32/Filecoder.NTL trojan |
| avast | ii | Dangerous<br>Win32:Malware-gen\|PE3-D82C48DF00001D459A15AF557B790400\|troj;Win32:Evo-gen |
| sophos | ii | Dangerous<br>Mal/EncPk-ZC |
| fprot | ✓ | Clean |
| پادویش | ✓ | Clean |
| symantec | ii | Dangerous<br>Heur.AdvML.C |
| kaspersky | ii | Dangerous |
| escan | ii | Dangerous<br>Gen:Heur.Zard.2(DB) |
| clamav | ✓ | Clean |
| fsecure | ii | Dangerous<br>Gen:Heur.Ransom.Imps.1 |
| mcafee | ✓ | Clean |
| bitdefender | ii | Dangerous |