باسمه تعالی

تحلیل فنی باج‌افزار

Delphimorix

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور باج‌افزار Delphimorix خبر می‌دهد. بر اساس گزارش وبسایت Id-ransomware.blogspot.ru این باج‌افزار با استفاده از کد باج‌افزار InducVirus توسعه یافته است و نخستین بار در تاریخ ۲۱نوامبر ۲۰۱۸ میلادی مشاهده شده است. به فاصله دو روز بعد از این تاریخ، دوبار به روز رسانی شده است و تحلیل پیش رو مربوط به به‌روزرسانی در تاریخ ۲۳نوامبر می‌باشد.

مشخصات فایل اجرایی :

نام فایل	Project۱.exe
MD۵	eee٦٧٢e٨٠a٦da١٤٩٤٨e٣١٠٥٢٧٦٤٧ece٣
SHA-١	e٦٥٤٤٥f٩٨fb٣e٦c٩a٤٨٨ea٦٧٥a٤٥٠f٠a١٤٣٠f٣٥a
SHA-٢٥٦	٧ff٠٧٩٥٨١bf٣٧٩٢c٩e٠c٣٨c٧٧a٨f١٤afda٦b٧c٨٤a٤b٥٥٦٢٣e٥ff٢٩cdbbcd٠٥b٩
اندازه فایل	١.٣٤ مگابایت

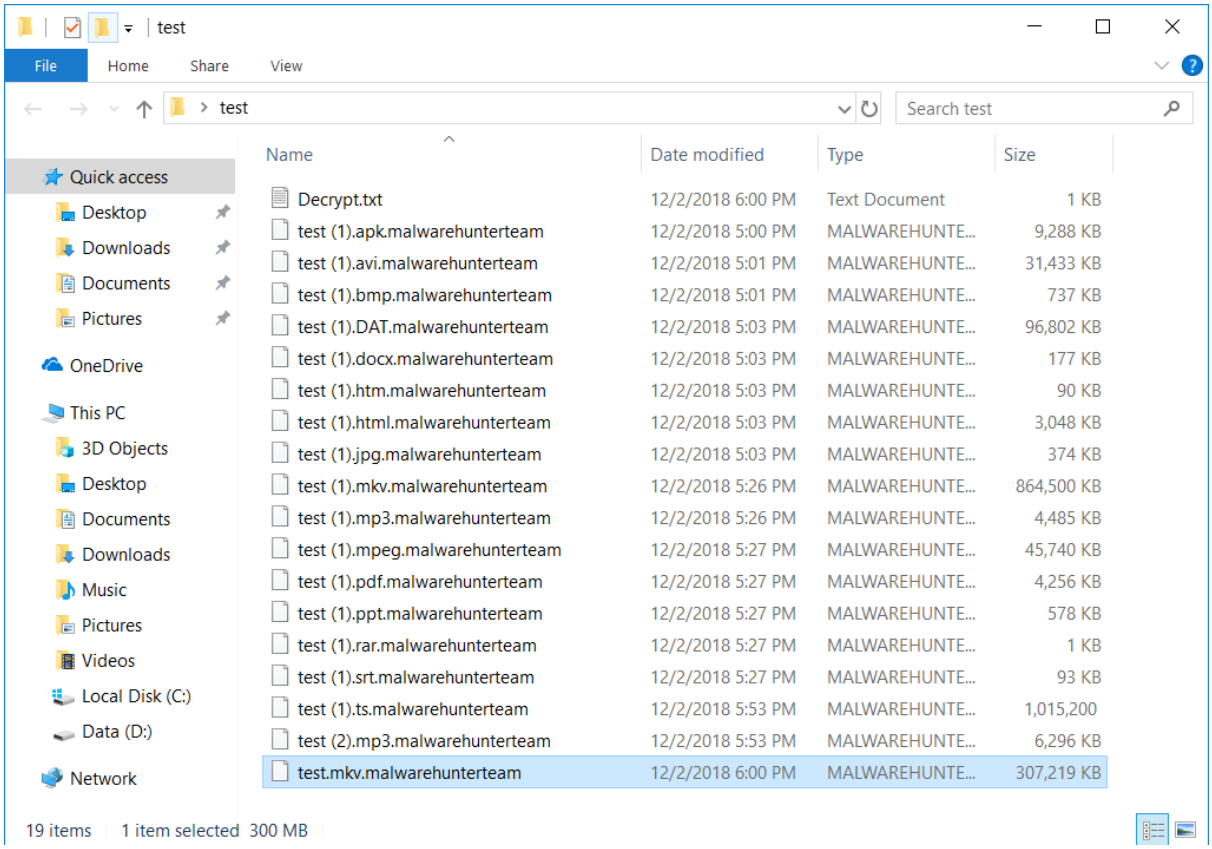
فایل اجرایی این باج‌افزار دارای ۸ بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
CODE	٦.٥١	٤٠٩٦	١٠٧٢٤٢٤	١٠٧٢٦٤٠
DATA	٦.٥٥	١٠٧٧٢٤٨	١٨٦٧٦	١٨٩٤٤
BSS	٠	١٠٩٧٧٢٨	٤٧٤٩	٠
.idata	٤.٩٥	١١٠٥٩٢٠	١٠٢٧٤	١٠٧٥٢
.tls	٠	١١١٨٢٠٨	١٦	٠
.rdata	0.2	١١٢٢٣٠٤	٢٤	٥١٢
.reloc	6.69	١١٢٦٤٠٠	٥٢١٩٢	٥٢٢٢٤
.rsrc	4.17	١١٧٩٦٤٨	٢٥٣٩٥٢	٢٥٣٩٥٢

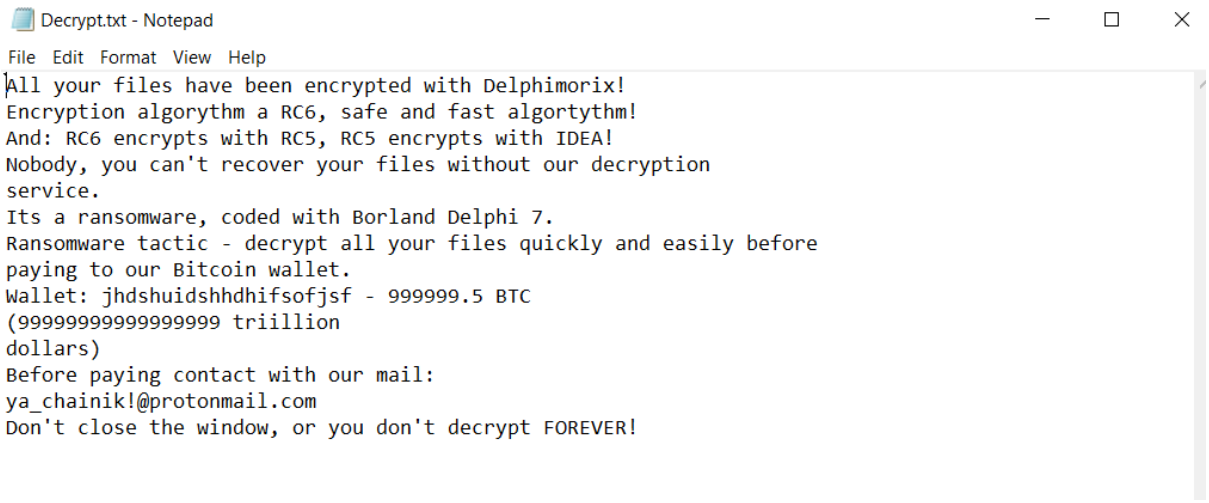
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Delphimorix ، 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 جست و جو و رمزگذاری فایل‌های موردنظر خود می‌کند. فرآیند رمزگذاری این باج‌افزار بسیار طول می‌انجامد. با بررسی‌هایی که همزمان بر روی نمونه فایل‌های رمزشده با نمونه سالم آن‌ها انجام دادیم، متوجه شدیم که این باج‌افزار تمام محتوای فایل‌های مورد هدف خود را رمزگذاری می‌کند. علت طولانی شدن فرآیند رمزگذاری نیز، همین موضوع می‌باشد. همچنین با بررسی‌هایی که بر روی مسیرهای مختلف سیستم‌عامل انجام دادیم، متوجه شدیم فقط فایل‌های موجود بر روی صفحه Desktop سیستم قربانی رمزگذاری می‌شوند. این باج‌افزار تمامی انواع فایل‌های مسیر مذکور، حتی فایل‌های اجرایی با پسوند exe را نیز، رمزگذاری می‌کند.

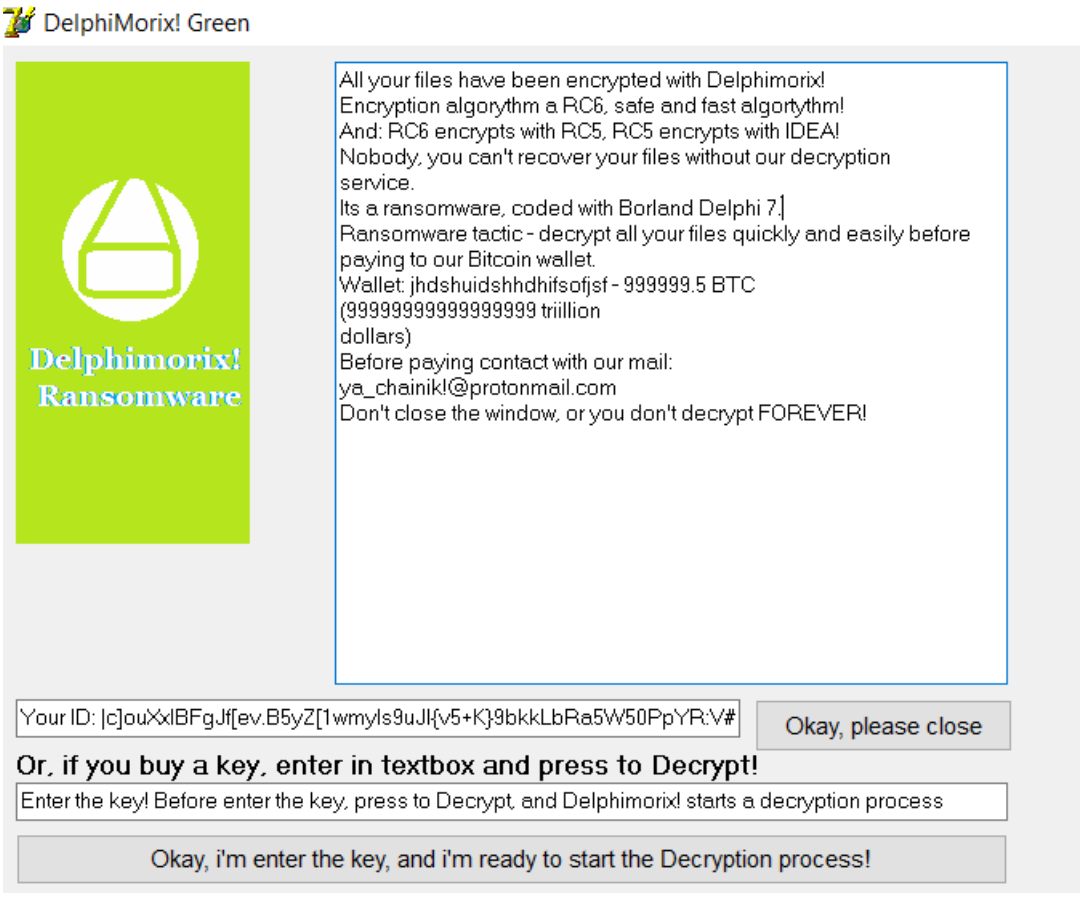
فایل‌های سیستم قربانی پس از رمزگذاری، به شکل زیر تغییر پیدا می‌کنند:



همانطور که مشاهده می‌کنید، تمامی انواع فایل‌ها رمزگذاری شده‌اند و به انتهای آن‌ها پسوند malwarehunterteam. اضافه شده است. همچنین فایل پیغام باج‌خواهی با عنوان Decrypt.txt نیز، درون این پوشه ایجاد شده است. تصویر زیر مربوط به پیغام باج‌خواهی این باج‌افزار است:



همانطور که در ابتدای این پیغام مشاهده می‌کنید، این باج‌افزار خود را Delphimorix معرفی کرده است و عنوان کرده است که تمام فایل‌های قربانی توسط آن رمزگذاری شده‌اند. در ادامه، الگوریتم رمزنگاری باج‌افزار و روش رمزگذاری معرفی شده است و ادعا شده است که هیچکس بدون سرویس رمزگشایی مهاجم یا مهاجمین، قادر به بازیابی فایل‌ها نیست. زبان برنامه نویسی باج‌افزار نیز Delphi ۷ معرفی شده است. نکته جالب در مورد این باج‌افزار این است که عنوان شده است قبل از پرداخت مبلغ باج، تمامی فایل ها به سرعت و به آسانی رمزگشایی خواهند شد. برای باج نیز، مبلغی عجیب معادل ۹۹۹۹۹۹.۵ بیت کوین در نظر گرفته شده است. قربانی باید قبل از پرداخت این مبلغ، به آدرس ya_chainik!@protonmail.com ایمیلی ارسال کند. در انتها نیز، از قربانی خواسته شده است که پنجره‌ای که بر روی صفحه نمایش سیستم نمایان شده است را نبندد. تصویر مربوط به این پنجره را در ادامه مشاهده می‌کنید:



همانطور که مشاهده می‌کنید، متن درون این پنجره با پیغام باج‌خواهی باج‌افزار یکسان است. فقط دو قسمت برای وارد کردن شناسه قربانی و کلید رمزگشایی درنظر گرفته شده است.

تحلیل ایستا:

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

از تابع CreateFile در قطعه کد زیر برای تغییر در فایل استفاده شده است. تابع GetFileSize نیز، برای دریافت اندازه فایل استفاده شده است:

```
CODE:00403168                   push    0
CODE:0040316A                   push    80h
CODE:0040316F                   push    ecx
CODE:00403170                   push    0
CODE:00403172                   push    edx
CODE:00403173                   push    eax
CODE:00403174                   lea     eax, [esi+48h]
CODE:00403177                   push    eax
CODE:00403178                   call    CreateFileA
CODE:0040317D                   cmp     eax, 0FFFFFFFFh
CODE:00403180                   jz      loc_40328E
CODE:00403186                   mov     [esi], eax
CODE:00403188                   cmp     word ptr [esi+4], 0D7B3h
CODE:0040318E                   jnz     loc_403257
CODE:00403194                   dec     word ptr [esi+4]
CODE:00403198                   push    0
CODE:0040319A                   push    dword ptr [esi]
CODE:0040319C                   call    GetFileSize
CODE:004031A1                   inc     eax
CODE:004031A2                   jz      loc_40328E
CODE:004031A8                   sub     eax, 81h
CODE:004031AD                   jnb     short loc_4031B1
CODE:004031AF                   xor     eax, eax
```

در ادامه قطعه کد بالا از تابع SetFilePointer برای حرکت درون فایل استفاده شده است. تابع ReadFile نیـز، برای خواندن محتوای درون فایل همزمان با نتایج تابع SetFilePointer استفاده شده است:

```
CODE:004031B1 loc_4031B1:                             ; CODE XREF: CODE:004031AD↑j
CODE:004031B1                   push    0
CODE:004031B3                   push    0
CODE:004031B5                   push    eax
CODE:004031B6                   push    dword ptr [esi]
CODE:004031B8                   call    SetFilePointer
CODE:004031BD                   inc     eax
CODE:004031BE                   jz      loc_40328E
CODE:004031C4                   push    0
CODE:004031C6                   mov     edx, esp
CODE:004031C8                   push    0
CODE:004031CA                   push    edx
CODE:004031CB                   push    80h
CODE:004031D0                   lea     edx, [esi+14Ch]
CODE:004031D6                   push    edx
CODE:004031D7                   push    dword ptr [esi]
CODE:004031D9                   call    ReadFile
CODE:004031DE                   pop     edx
CODE:004031DF                   dec     eax
CODE:004031E0                   jnz     loc_40328E
CODE:004031E6                   xor     eax, eax
```

از قطعه کد زیر نیز برای نوشتن در فایل استفاده شده است:

```
CODE:00403094 loc_403094:                             ; CODE XREF: unknown_libname_25+A↑j
CODE:00403094                 push    0               ; lpOverlapped
CODE:00403096                 lea     eax, [esp+10h+NumberOfBytesWritten]
CODE:0040309A                 push    eax             ; lpNumberOfBytesWritten
CODE:0040309B                 push    esi             ; nNumberOfBytesToWrite
CODE:0040309C                 mov     eax, [ebx+14h]
CODE:0040309F                 push    eax             ; lpBuffer
CODE:004030A0                 mov     eax, [ebx]
CODE:004030A2                 push    eax             ; hFile
CODE:004030A3                 call    WriteFile
CODE:004030A8                 test    eax, eax
CODE:004030AA                 jnz     short loc_4030B3
CODE:004030AC                 call    GetLastError
CODE:004030B1                 jmp     short loc_4030B5
```

در نهایت با فراخوانی مجدد تابع SetFilePointer و استفاده از تابع SetEndOfFile، برای اضافه نمودن پسوند موردنظر به فایل‌های رمزشده استفاده شده است:

```
CODE:004031F9 loc_4031F9:                             ; CODE XREF: CODE:004031F4↑j
CODE:004031F9                 push    2
CODE:004031FB                 push    0
CODE:004031FD                 sub     eax, edx
CODE:004031FF                 push    eax
CODE:00403200                 push    dword ptr [esi]
CODE:00403202                 call    SetFilePointer
CODE:00403207                 inc     eax
CODE:00403208                 jz      loc_40328E
CODE:0040320E                 push    dword ptr [esi]
CODE:00403210                 call    SetEndOfFile
CODE:00403215                 dec     eax
CODE:00403216                 jnz     short loc_40328E
CODE:00403218                 jmp     short loc_403257
```

از تابع مشخص شده قطعه کد زیر نیز، برای دریافت نوع فایل‌ها استفاده شده است:

```
CODE:00403257 loc_403257:                             ; CODE XREF: CODE:0040318E↑j
CODE:00403257                                         ; CODE:004031EA↑j ...
CODE:00403257                 cmp     word ptr [esi+4], 0D7B1h
CODE:0040325D                 jz      short loc_403276
CODE:0040325F                 push    dword ptr [esi]
CODE:00403261                 call    GetFileType
CODE:00403266                 test    eax, eax
CODE:00403268                 jz      short loc_40327A
CODE:0040326A                 cmp     eax, 2
CODE:0040326D                 jnz     short loc_403276
CODE:0040326F                 mov     dword ptr [esi+20h], offset unknown_libname_25
```

همانطور که در بخش قبل توضیح داده شد، باج‌افزار در انتهای فعالیت خود، تصویر زمینه سیستم قربانی را به رنگ مشکی تغییر می‌دهد. قطعه کد زیر مربوط به این فرآیند می‌باشد:

```
CODE:0042467F loc_42467F:                              ; CODE XREF: Graphics::TCanvas::CreateBrush(void)+2D↑j
CODE:0042467F                 mov     eax, [ebx+14h]
CODE:00424682                 call    sub_423B4C
CODE:00424687                 call    @Graphics@ColorToRGB$qqr15Graphics@TColor ; Graphics::ColorToRGB(Graphics::TColor)
CODE:0042468C                 not     eax
CODE:0042468E                 push    eax             ; COLORREF
CODE:0042468F                 mov     eax, [ebx+4]
CODE:00424692                 push    eax             ; HDC
CODE:00424693                 call    SetBkColor
CODE:00424698                 push    1               ; int
CODE:0042469A                 mov     eax, [ebx+4]
CODE:0042469D                 push    eax             ; HDC
CODE:0042469E                 call    SetBkMode
CODE:004246A3                 pop     ebx
CODE:004246A4                 retn
```

تنظیم پنجره باج‌خواهی باج‌افزار بر روی تصویر زمینه سیستم قربانی نیز، با استفاده از قطعه کد زیر صورت می‌گیرد:

```
CODE:0045E830                 push    ebx
CODE:0045E831                 push    esi
CODE:0045E832                 mov     ebx, eax
CODE:0045E834                 mov     eax, [ebx+30h]
CODE:0045E837                 test    eax, eax
CODE:0045E839                 jz      short loc_45E866
CODE:0045E83B                 push    eax             ; hWnd
CODE:0045E83C                 call    GetLastActivePopup
CODE:0045E841                 mov     esi, eax
CODE:0045E843                 test    esi, esi
CODE:0045E845                 jz      short loc_45E866
CODE:0045E847                 cmp     esi, [ebx+30h]
CODE:0045E84A                 jz      short loc_45E866
CODE:0045E84C                 push    esi             ; hWnd
CODE:0045E84D                 call    IsWindowVisible
CODE:0045E852                 test    eax, eax
CODE:0045E854                 jz      short loc_45E866
CODE:0045E856                 push    esi             ; hWnd
CODE:0045E857                 call    IsWindowEnabled
CODE:0045E85C                 test    eax, eax
CODE:0045E85E                 jz      short loc_45E866
CODE:0045E860                 push    esi             ; hWnd
CODE:0045E861                 call    SetForegroundWindow
```

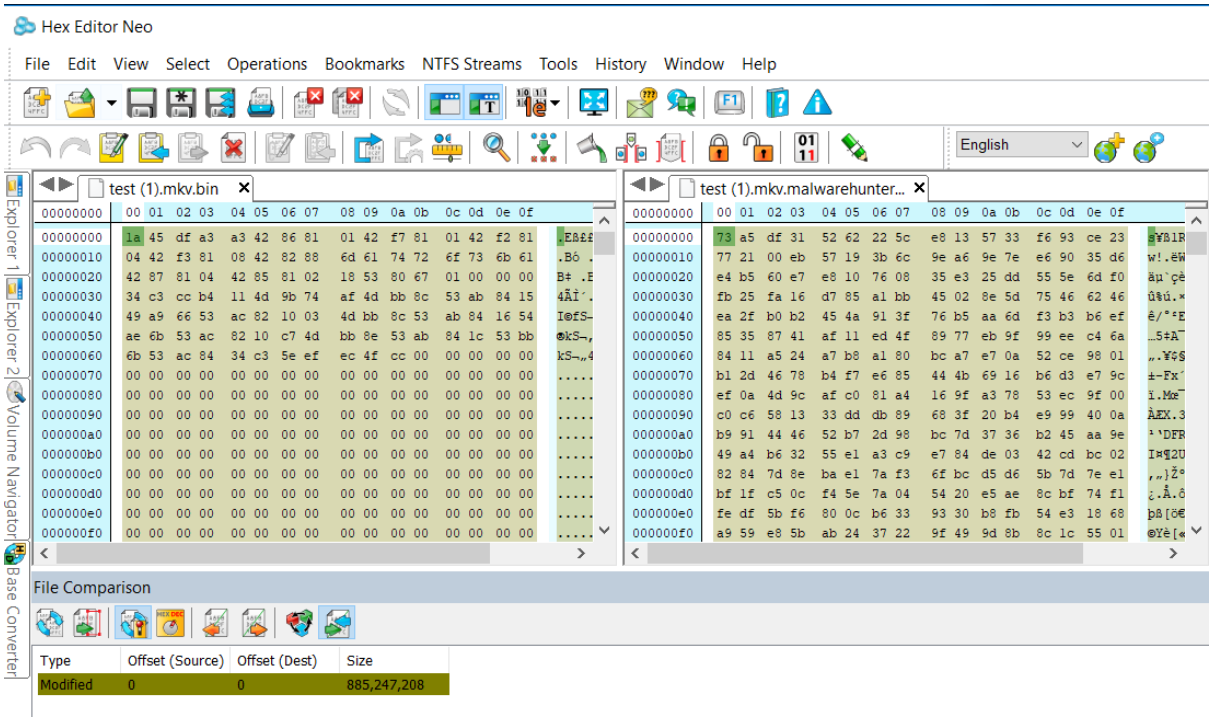
همانطور که در ابتدای بخش تحلیل پویای این باج‌افزار اشاره کردیم، فقط فایل‌های پوشه Desktop سیستم قربانی توسط باج‌افزار رمزگذاری می‌شوند. قطعه کد زیر دریافت محتوای این پوشه را نشان می‌دهد:

```
CODE:004ECBE4 sub_4ECBE4      proc near               ; CODE XREF: sub_4ECBF4+37↓p
CODE:004ECBE4                 push    ebx
CODE:004ECBE5                 mov     ebx, eax
CODE:004ECBE7                 push    ebx
CODE:004ECBE8                 call    SHGetDesktopFolder
CODE:004ECBED                 call    @Comobj@OleCheck$qqrl ; Comobj::OleCheck(long)
CODE:004ECBF2                 pop     ebx
CODE:004ECBF3                 retn
CODE:004ECBF3 sub_4ECBE4      endp
```

این باج‌افزار، مدتی پس از پایان فرآیند رمزگذاری، خود را از سیستم قربانی حذف می‌کند. قطعه کد مربوط به آن را در ادامه مشاهده می‌کنید:

```
CODE:00409C70                push    ebx
CODE:00409C71                mov     ebx, eax
CODE:00409C73                mov     eax, ebx
CODE:00409C75                call    @System@@LStrToPChar$qqrx17System@AnsiString
CODE:00409C7A                push    eax             ; lpFileName
CODE:00409C7B                call    DeleteFileA
CODE:00409C80                cmp     eax, 1
CODE:00409C83                sbb     eax, eax
CODE:00409C85                inc     eax
CODE:00409C86                pop     ebx
CODE:00409C87                retn
```

با بررسی چند نمونه فایل رمزشده با نمونه سالم آن‌ها متوجه شدیم که این باج‌افزار تمام محتوای فایل‌های موردنظر خود را رمزگذاری می‌کند. در ادامه تصویر مربوط به نتیجه مقایسه یک نمونه از این فایل‌ها با نمونه سالم آن را مشاهده می‌کنید:



تحلیل ترافیک شبکه :

پس از اجرای باج‌افزار در محیط آمایشگاهی و سندباکس‌های آنلاین و بررسی نتایج ترافیک شبکه ایجاد شده در آن‌ها، هیچگونه ترافیک مشکوکی مربوط به باج‌افزار مشاهده نکردیم.

خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد ٤٠ مورد از ٦٩ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.31366334	AegisLab	Trojan.Win32.Crypmod.4!c
AhnLab-V3	Malware/Gen.Generic.C2852210	ALYac	Trojan.GenericKD.31366334
Arcabit	Trojan.Generic.D1DE9CBE	Avast	FileRepMalware
AVG	FileRepMalware	Avira	TR/FileCoder.fcray
BitDefender	Trojan.GenericKD.31366334	CAT-QuickHeal	Trojan.Crypmod
CrowdStrike Falcon	malicious_confidence_90% (W)	Cylance	Unsafe
Cyren	W32/GenBl.EEE672E8!Olympus	DrWeb	Trojan.Encoder.26774
Emsisoft	Trojan.FileCoder (A)	eScan	Trojan.GenericKD.31366334
ESET-NOD32	a variant of Win32/Filecoder.NTK	F-Secure	Trojan.GenericKD.31366334
Fortinet	W32/Generic.NTK!tr	GData	Trojan.GenericKD.31366334
Ikarus	Trojan-Ransom.FileCoder	K7AntiVirus	Trojan (00541e781)
K7GW	Trojan (00541e781)	Kaspersky	HEUR:Trojan-Ransom.Win32.Crypmod.gen
McAfee	Artemis!EEE672E80A6D	McAfee-GW-Edition	BehavesLike.Win32.Dropper.th
Microsoft	Trojan:Win32/Zpevdo.B	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.709
Rising	Ransom.Crypmod!8.DA9 (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	Trojan.Gen.2	Trapmine	malicious.high.ml.score
TrendMicro	Ransom_Crypmod.R002C0WKP18	TrendMicro-HouseCall	Ransom_Crypmod.R002C0WKP18
Webroot	W32.Trojan.GenKD	ZoneAlarm	HEUR:Trojan-Ransom.Win32.Crypmod.gen

سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۷ مورد از ۱۴ 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	
clamav	✓	Clean
kaspersky	✓	Clean
bitdefender	ii	Dangerous
mcafee	✓	Clean
eset	ii	Dangerous a variant of Win32/Filecoder.NTK trojan
comodo	✓	Clean
fsecure	ii	Dangerous Trojan.GenericKD.31366334
sophos	✓	Clean
fprot	✓	Clean
drweb	ii	Dangerous Trojan.Encoder.26774
پادویش	✓	Clean
symantec	ii	Dangerous Trojan.Gen.2
avast	ii	Dangerous
escan	ii	Dangerous Trojan.GenericKD.31366334(DB)