باسمه تعالی

تحلیل فنی باج‌افزار

AnteFrigus

فهرست مطالب

۱. مقدمه :

از اواسط ماه نوامبر سال ۲۰۱۹ میلادی، اخباری مربوط به باج‌افزاری با عنوان AnteFrigus در فضای سایبری منتشر شد. طبق مشاهدات صورت گرفته، این باج‌افزار تنها درایوهای خاصی از سیستم قربانی را مورد هدف قرار داده و هیچ فایلی از درایو C سیستم قربانی را رمزگذاری نمی‌کند. باج‌افزار AnteFrigus از الگوریتم Salsa20 جهت رمزگذاری فایل‌های موردنظر خود استفاده کرده و برای رمزگشایی فایل‌های قربانی، مبلغ ۱۹۹۵ دلار به بیت‌کوین باج درخواست می‌دهد. تحلیل پیش رو، مربوط به یکی از نسخه‌های اخیر منتشر شده از این باج‌افزار می‌باشد.

۲. مشخصات فایل اجرایی آنپک شده:

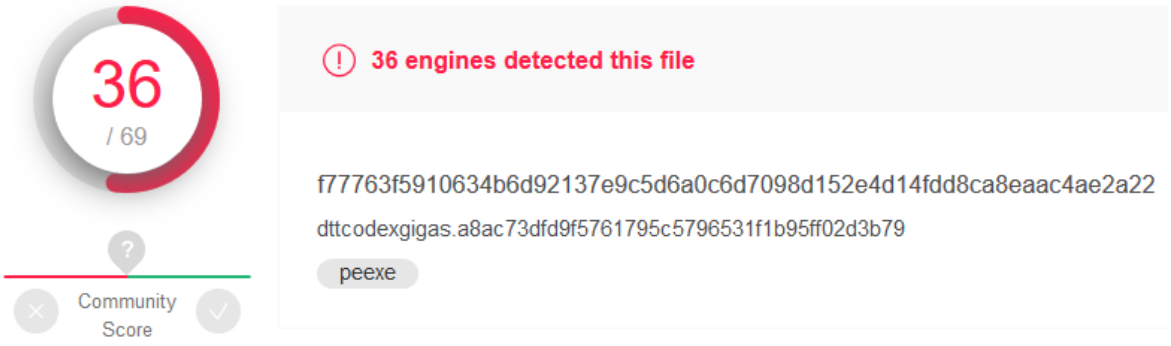
نام فایل	Random
MD5	803ab938b252bb0d9f9572e66cca0392
SHA-1	a8ac73dfd9f5761795c5796531f1b95ff02d3b79
SHA-256	f77763f5910634b6d92137e9c5d6a0c6d7098d152e4d14fdd8ca8eaac4ae2a22
نوع فایل	Win32 EXE
اندازه فایل	٤٤١.٥ مگابایت

۳. شجره‌نامه

تاکنون والدی برای این باج افزار مشاهده نشده است و به نظر می‌رسد باج افزار MedusaLocker با هیچ باج‌افزار دیگری ارتباط و یا شباهت ندارد.

٤. میزان تهدید فایل باج‌افزار

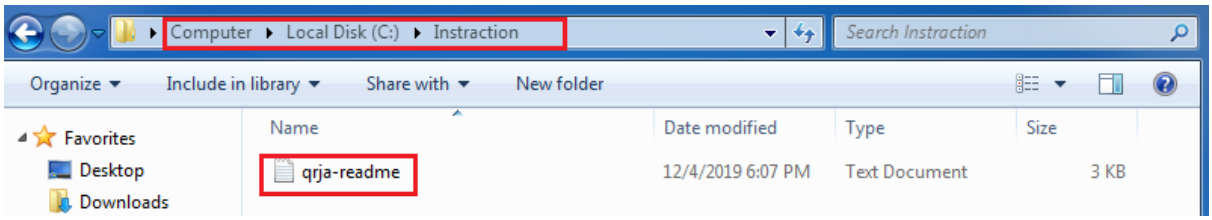
درحال حاضر تعداد ٣٦ مورد از ٦٩ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



۵. تحلیل پویا

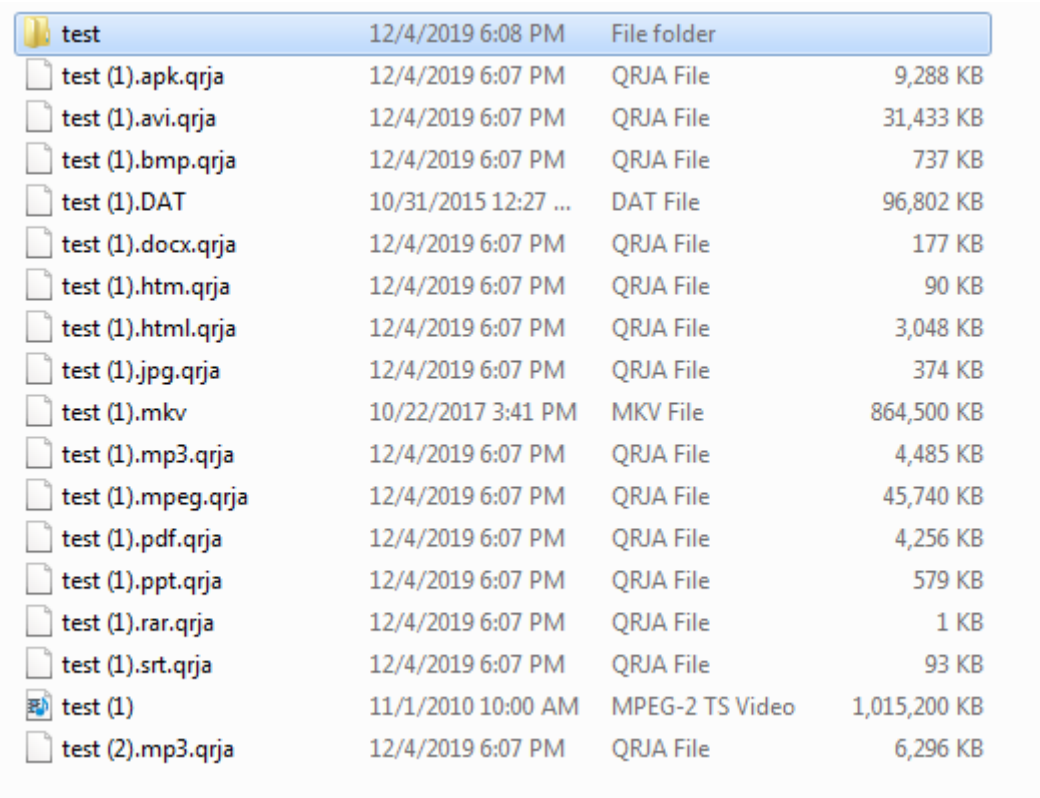
۵-۱ آناتومی حمله:

باج‌افزار AnteFrigus در مدت زمان کمی پس اجرا در سیستم قربانی، پوشه‌ای با عنوان کـه instruction را در درایو C ایجاد می‌کند.



همانطور که قابل مشاهده است، در این پوشه فایلی متنی ایجاد شده است که در واقع همان پیغام باج‌خواهی باج‌افزار می‌باشد. این پیغام، بر روی صفحه دسکتاپ سیستم قربانی نیز ایجاد می‌شود.

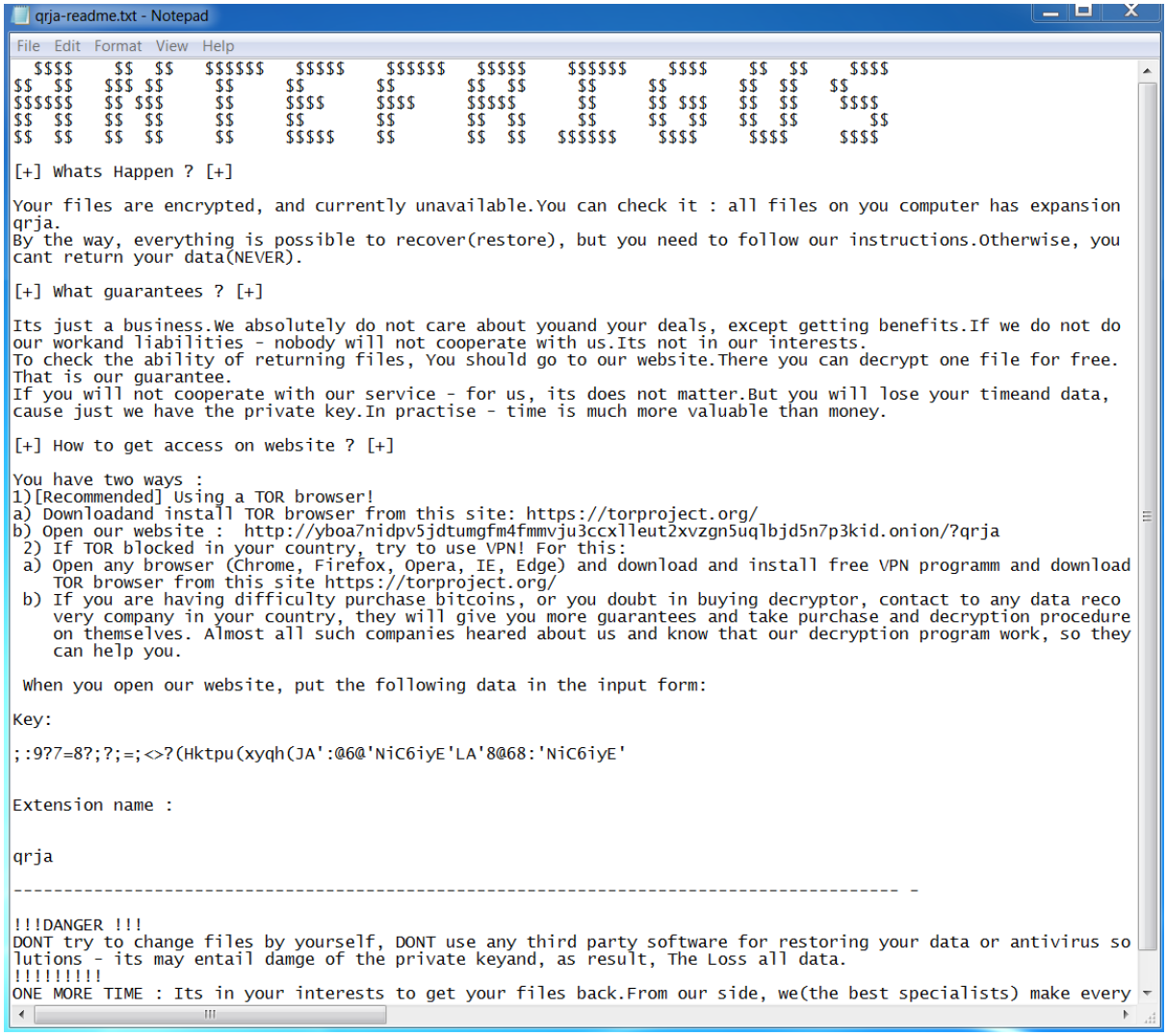
سپس فرآیند رمزگذاری شروع شده و باج‌افزار در مدت زمان کوتاهی تمام فایـل‌هـای مـورد نظـر خـود در سیستم قربانی را رمزگذاری می‌نماید.



test	12/4/2019 6:08 PM	File folder	
test (1).apk.qrja	12/4/2019 6:07 PM	QRJA File	9,288 KB
test (1).avi.qrja	12/4/2019 6:07 PM	QRJA File	31,433 KB
test (1).bmp.qrja	12/4/2019 6:07 PM	QRJA File	737 KB
test (1).DAT	10/31/2015 12:27 ...	DAT File	96,802 KB
test (1).docx.qrja	12/4/2019 6:07 PM	QRJA File	177 KB
test (1).htm.qrja	12/4/2019 6:07 PM	QRJA File	90 KB
test (1).html.qrja	12/4/2019 6:07 PM	QRJA File	3,048 KB
test (1).jpg.qrja	12/4/2019 6:07 PM	QRJA File	374 KB
test (1).mkv	10/22/2017 3:41 PM	MKV File	864,500 KB
test (1).mp3.qrja	12/4/2019 6:07 PM	QRJA File	4,485 KB
test (1).mpeg.qrja	12/4/2019 6:07 PM	QRJA File	45,740 KB
test (1).pdf.qrja	12/4/2019 6:07 PM	QRJA File	4,256 KB
test (1).ppt.qrja	12/4/2019 6:07 PM	QRJA File	579 KB
test (1).rar.qrja	12/4/2019 6:07 PM	QRJA File	1 KB
test (1).srt.qrja	12/4/2019 6:07 PM	QRJA File	93 KB
test (1)	11/1/2010 10:00 AM	MPEG-2 TS Video	1,015,200 KB
test (2).mp3.qrja	12/4/2019 6:07 PM	QRJA File	6,296 KB

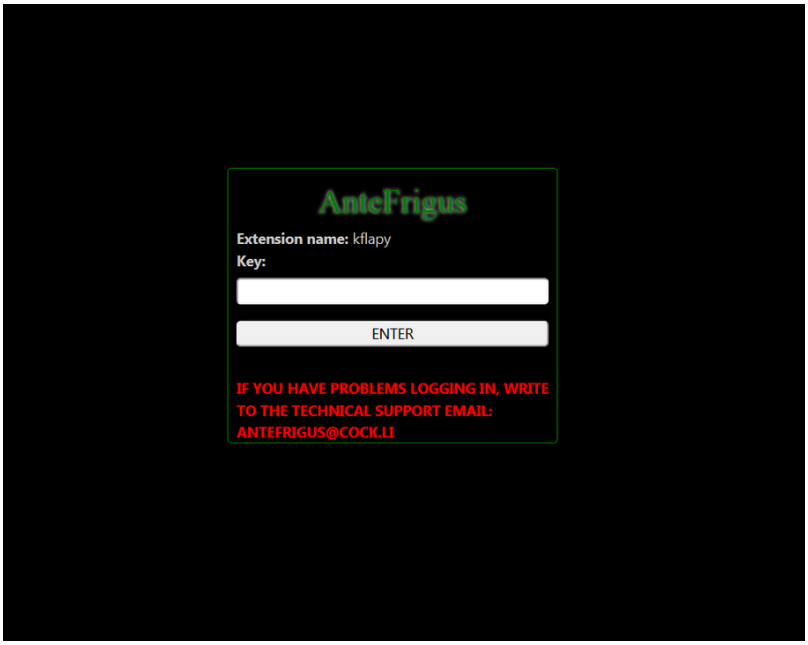
همانطور که قابل مشاهده است، تقریبا تمام انواع فایل‌ها رمزگذاری شده‌اند و به انتهای آن‌ها پسوند تصادفی qrja. اضافه شده است. نتایج بررسی‌های بیشتر نشان داد که پسوند اضافه شده به انتهای فایل‌ها به ابتدای فایل پیغام باج‌خواهی ایجاد شده در سیستم قربانی نیز اضافه می‌شود.

فایل پیغام باج‌خواهی باج‌افزار پس از اتمام فعالیت آن، بر روی صفحه نمایش سیستم قربانی نمایش داده می‌شود.

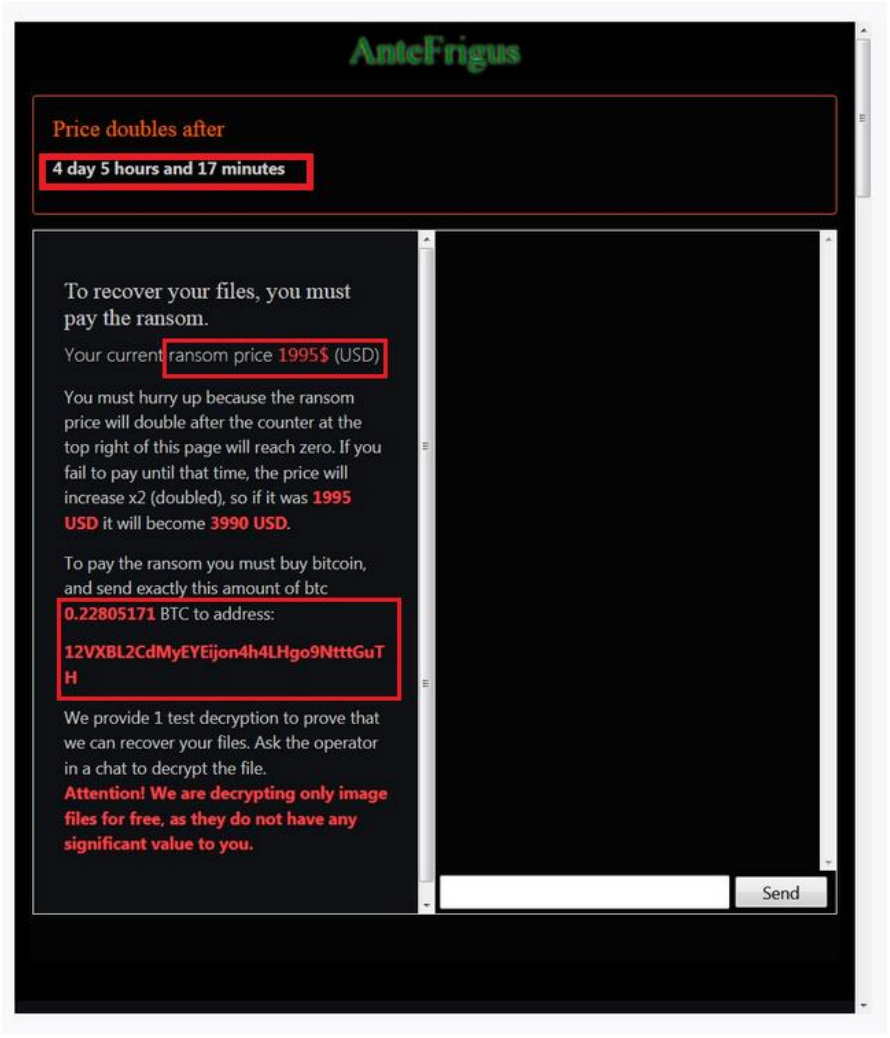


همانطور که در پیغام باج‌خواهی این باج‌افزار قابل مشاهده است در ابتدای پیغام، نام باج‌افزار نوشته شده است. در ادامه، قربانی برای دریافت کلید خصوصی مورد نیاز جهت رمزگشایی فایل‌ها به آدرسی در شبکه دارک‌وب هدایت شده است که فقط از طریق مرورگر Tor قابل دسترس می‌باشد. آدرس صفحه اصلی این مرورگر جهت دانلود نیز، درون پیغام قرار داده شده است.

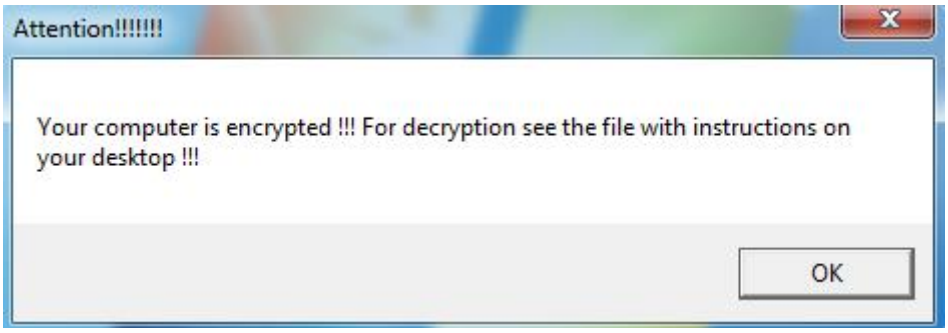
در صفحه اول آدرس عنوان شده در پیغام باج‌خواهی، قربانی باید مقداری که به عنوان Key درون پیغام باج‌خواهی قرار داده شده است را در باکس مشخص شده قرار دهد.



در صورتی که قربانی مشکلی در ورود به صفحه بعد دارد، باید ایمیلی به آدرس ANTEFRIGUS@COCK.LI ارسال کند. پس از ورود مقدار کلید، با کلیک بر روی گزینه ENTER به صفحه بعد هدایت می‌شود.



در این صفحه که صفحه اصلی پورتال طراحی شده برای باج‌افزار است، مقدار باج و مهلت پرداخت آن مشخص شده است. در صورت عدم پرداخت مقدار باج در مدت زمان تعیین شده، مبلغ آن دوبرابر خواهد شد. آدرس بیت‌کوین مهاجم نیز، جهت پرداخت مبلغ باج در تصویر قابل مشاهده است. همچنین قسمتی جهت پیام دادن درنظر گرفته شده است که قربانی از طریق آن قسمت می‌تواند با مهاجم یا مهاجمین ارتباط برقرار کند. در صورت بستن فایل پیغام باج‌خواهی باج‌افزار که به صورت خودکار بر روی صفحه نمایش سیستم قربانی ظاهر می‌شود، پنجره زیر نمایش داده خواهد شد.



۵-۲ روش انتشار:

براساس گزارش وب‌سایت Bleepingcomputer به نقل از محقق امنیتی با نام مستعار mol69، این باج‌افزار از طریق اکسپلویت کیت RIG منتشر می‌شود.

۵-۳ روش جلوگیری:

با توجه به روش ذکر شده برای انتشار این باج‌افزار توصیه می‌شود که سیستم‌عامل و مرورگرهای خود را به طور مداوم به‌روزرسانی کنید. همچنین، توصیه می‌شود از ورود به سایت‌های نامعتبر اکیداً خودداری کرده و نرم‌افزار آنتی‌ویروس نصب شده بر روی سیستم‌عامل خود را به صورت مداوم به‌روزرسانی کنید.

٦. تحلیل ایستا

بررسی‌های اولیه بر روی فایل اجرایی این باج‌افزار نشان می‌دهد که باج‌افزار Antefrigus بر روی تمامی نسخه‌های سیستم‌عامل ویندوز از ویندوز ویستا به بعد، اجرا خواهد شد.

OS version (major)	0006	Windows Vista
OS version (minor)	0000	
Image version (major)	0000	
Image version (minor)	0000	
Sub system version (major)	0006	
Sub system version (minor)	0000	
Win32 version	00000000	
Size of image	00073000	

۶-۱ تحلیل کد:

بخش‌های کد و داده در فایل اجرایی باج‌افزار Antefrigus با پکر UPX پک شده‌اند.

Nr	Virtual ...	Virtual s...	RAW D...	RAW size	Flags	Name	First bytes (hex)
01	00001000	00049000	00000400	00000000	E0000080	UPX0	!ZERO SIZE!
02 ep	0004A000	0002D000	00000400	0002CC00	E0000040	UPX1	25 F6 DB FF E8 11 00 45 58
03 i...	00077000	00001000	0002D000	00000400	C0000040	.rsrc	00 00 00 00 00 00 00 00

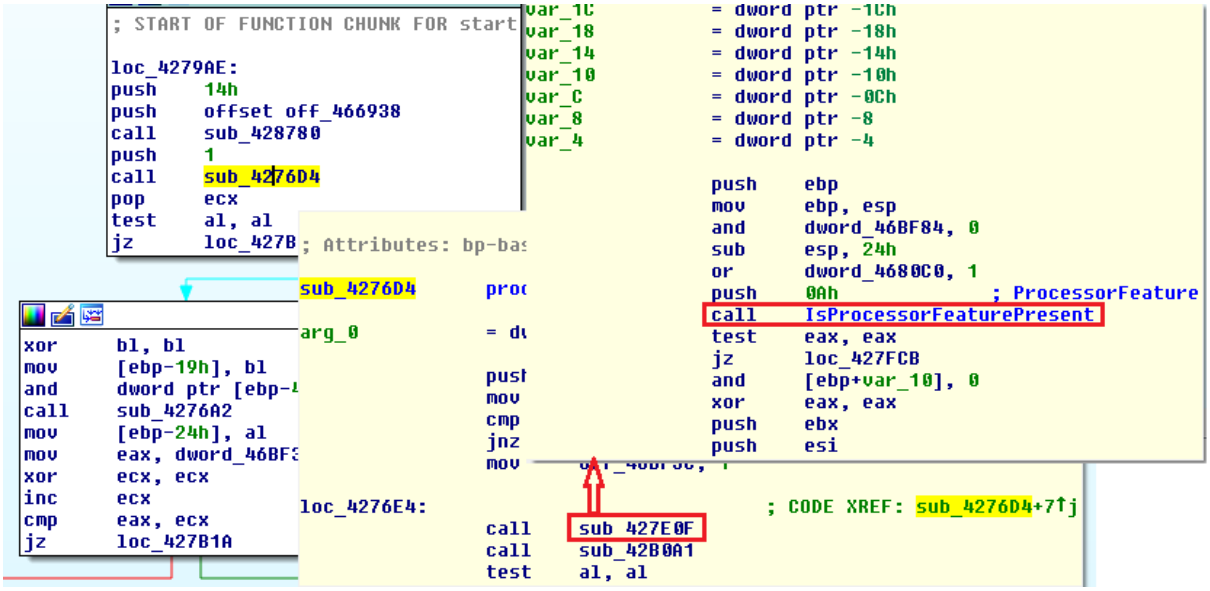
پس از آنپک کردن فایل اجرایی، نتایج زیر حاصل شد.

کد باج‌افزار از تابع start شروع شده و در همان ابتدا، زمان سیستم قربانی دریافت می‌شود.

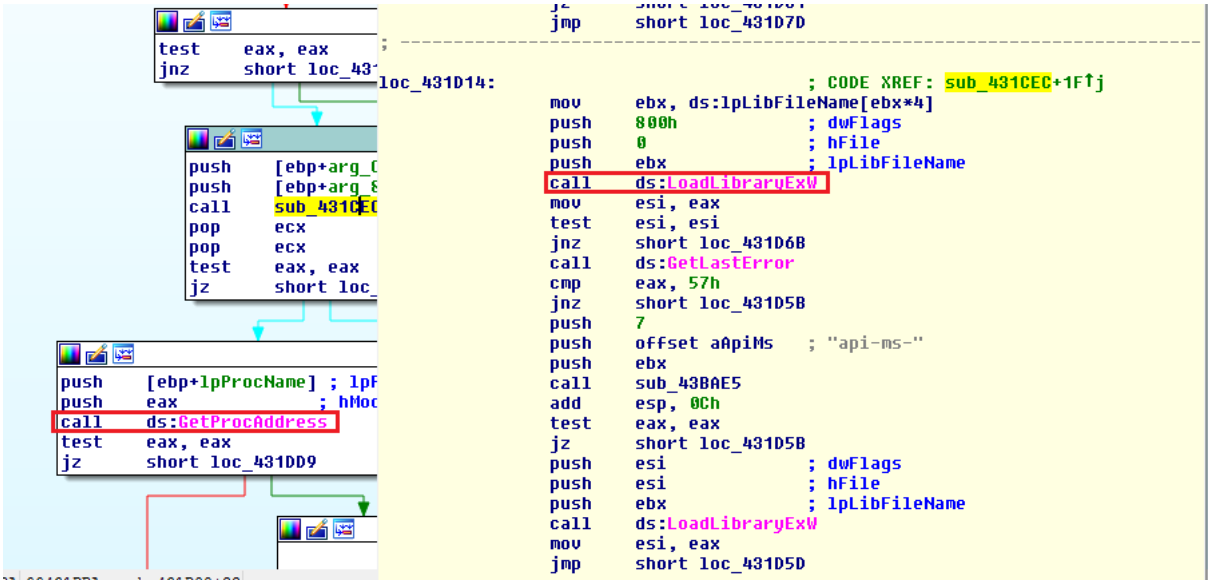
```
public start
start proc near

; FUNCTION CHUNK AT 004279AE SIZE 00000127 BYTES
; FUNCTION CHUNK AT 00427B0A SIZE 00000026 BYTES

call    sub_428828
jmp     loc_4279AE
start endp ; sp-an

; =============== S U B R O U T I N

sub_428828      proc near
                mov     ecx, ___secu
                push    esi
                push    edi
                mov     edi, 0BB40E6
                mov     esi, 0FFFF00
                cmp     ecx, edi
                jz      short loc_42
                test    esi, ecx
                jnz     short loc_42

loc_428842:
                call    sub_4287DB  sub_4287DB
                mov     ecx, eax
                cmp     ecx, edi
                jnz     short loc_428854
                mov     ecx, 0BB40E64Fh
                jmp     short loc_428862

xor
mov

                mov     ebp, esp
                sub     esp, 14h
                and     [ebp+SystemTimeAsFileTime.dwLowDa
                lea     eax, [ebp+SystemTimeAsFileTime]
                and     [ebp+SystemTimeAsFileTime.dwHighD
                push    eax             ; lpSystemTimeAs
                call    ds:GetSystemTimeAsFileTime
                mov     eax, [ebp+SystemTimeAsFileTime.dw
                xor     eax, [ebp+SystemTimeAsFileTime.dw
                mov     [ebp+var_4], eax
                call    ds:__imp_GetCurrentThreadId
                xor     [ebp+var_4], eax
                call    ds:GetCurrentProcessId
                xor     [ebp+var_4], eax
                lea     eax, [ebp+PerformanceCount]
                push    eax             ; lpPerformanceCo
                call    ds:QueryPerformanceCounter
                mov     eax, dword ptr [ebp+PerformanceCo
                lea     ecx, [ebp+var_4]
                xor     eax, dword ptr [ebp+PerformanceCo
                xor     eax, [ebp+var_4]
                xor     eax, ecx
                leave
                retn
                endp
```

همچنین شناسه فایل باج‌افزار و فرآیند والدی که آن را اجرا می‌کند، از طریق توابع GetCurrentProcessId و GetCurrentThreadId جهت آماده سازی فایل باج‌افزار برای اجرا در سیستم قربانی دریافت می‌شود.

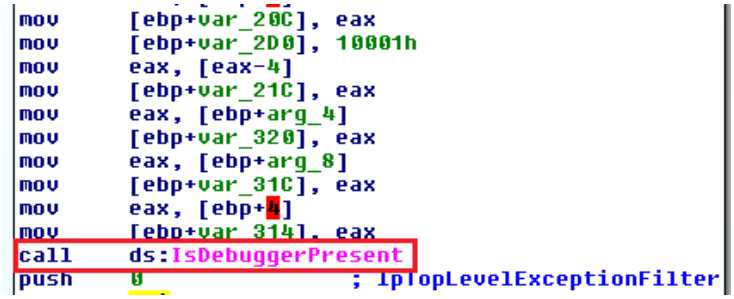
سپس نوع سخت‌افزار سیستم قربانی مشخص می‌شود.



در ادامه کتابخانه‌های استفاده شده در کد باج‌افزار بارگذاری می‌شوند.

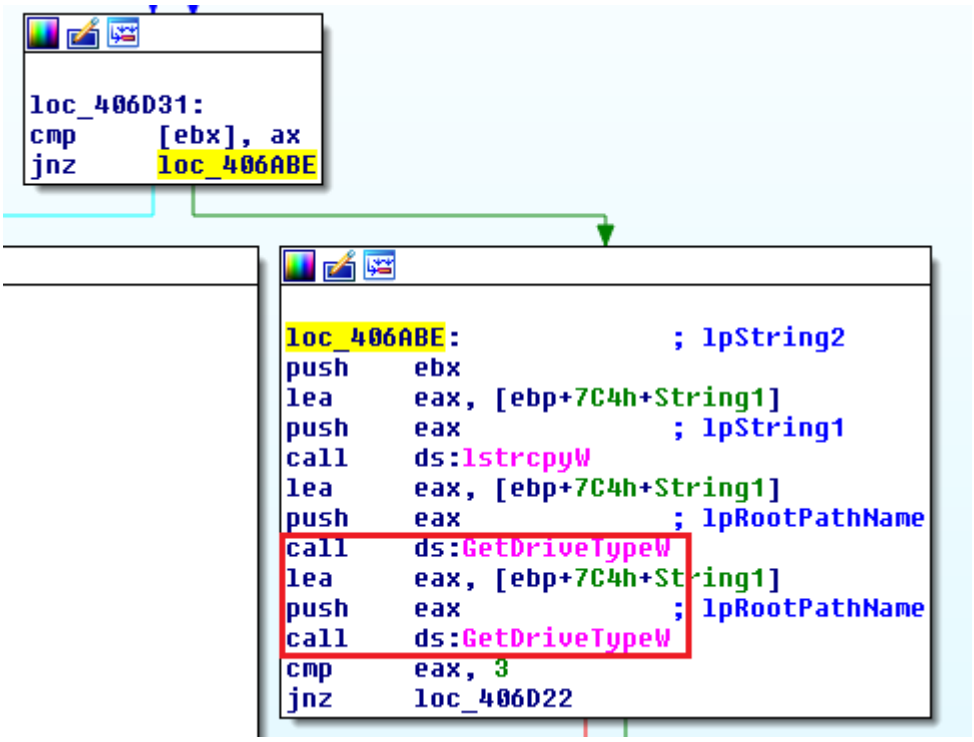


این باج‌افزار، از تابع ضد دیباگ در کد خود بهره برده است و بدون دور زدن تابع ضد دیباگ استفاده شده، امکان دیباگ کد فایل وجود نخواهد داشت.



در ادامه‌ی تابع Start و درون تابعی به نام pause، ابتدا از طریق تابع GetLogicalDriveStringsW نام تمام درایوهای موجود در سیستم قربانی دریافت می‌شود.

سپس در ادامه این فرآیند، نوع درایوهای یافت شده مشخص می‌شود.



همانطور که در بخش قبل اشاره شد، این باج‌افزار محتوای درایوهای خاصی از سیستم قربانی را رمزگذاری می‌کند. لیست این درایوها در تصویر زیر قابل مشاهده است.

```
push    offset aE       ; "E:"
push    ecx
lea     ecx, [ebp+7C4h+var_354]
call    loc_40BAEF
push    offset aD       ; "D:"
push    ecx
lea     ecx, [ebp+7C4h+var_34C]
mov     byte ptr [ebp+7C4h+var_7C8], 30h
call    loc_40BAEF
push    offset asc_46088C ; "F:"
push    ecx
lea     ecx, [ebp+7C4h+var_344]
mov     byte ptr [ebp+7C4h+var_7C8], 31h
call    loc_40BAEF
push    offset aI       ; "I:"
push    ecx
lea     ecx, [ebp+7C4h+var_33C]
mov     byte ptr [ebp+7C4h+var_7C8], 32h
call    loc_40BAEF
push    offset aU       ; "U:"
push    ecx
lea     ecx, [ebp+7C4h+var_334]
mov     byte ptr [ebp+7C4h+var_7C8], 33h
call    loc_40BAEF
push    offset aG       ; "G:"
push    ecx
```

در ادامه این روند و پس از دریافت تمام اطلاعات درایوهای موجود در سیستم قربانی، اطلاعاتی همچون نام کاربر فعال سیستم دریافت می‌شود.

```
call    ds:GetUserNameW
lea     eax, [ebp+7C4h+Buffer]
push    eax
lea     ecx, [ebp+7C4h+var_384]
call    sub_40920C
push    8
pop     ebx
mov     byte ptr [ebp+7C4h+var_7C8], 0Bh
lea     ecx, [ebp+7C4h+var_384]
cmp     [ebp+7C4h+var_370], ebx
mov     eax, [ebp+7C4h+var_374]
cmovnb  ecx, [ebp+7C4h+var_384]
lea     eax, [ecx+eax*2]
lea     ecx, [ebp+7C4h+var_384]
cmovnb  ecx, [ebp+7C4h+var_384]
push    ecx
push    eax
push    ecx
lea     ecx, [ebp+7C4h+var_42C]
call    sub_40B9D2
xor     eax, eax
mov     [ebp+7C4h+var_358], 0Fh
mov     [ebp+7C4h+var_35C], eax
mov     byte ptr [ebp+7C4h+var_36C], al
lea     eax, [ebp+7C4h+var_42C]
mov     byte ptr [ebp+7C4h+var_7C8], 0Dh
```

سپس، فایل پیغام باج‌خواهی باج‌افزار بر روی صفحه دسکتاپ سیستم قربانی ایجاد می‌شود.

```
mov     edx, offset aCUsers ; "C:/Users/"
lea     ecx, [ebp+7C4h+var_820]
call    sub_40B5CC
mov     byte ptr [ebp+7C4h+var_7C8], 0Eh
mov     [esp+894h+lpMultiByteStr], offset aDesktop ; "/Desktop/"
push    eax
lea     eax, [ebp+7C4h+var_838]
push    eax
call    sub_40B5B0
add     esp, 0Ch
lea     ecx, [ebp+7C4h+var_2C4]
mov     byte ptr [ebp+7C4h+var_7C8], 0Fh
push    ecx
mov     ecx, eax
call    sub_4092C8
push    eax
lea     ecx, [ebp+7C4h+var_7EC]
call    sub_409309
mov     byte ptr [ebp+7C4h+var_7C8], 10h
push    offset aReadme_txt ; "-readme.txt"
lea     eax, [ebp+7C4h+var_7EC]
push    eax
lea     eax, [ebp+7C4h+var_850]
push    eax
call    sub_40B5B0
lea     ecx, [ebp+7C4h+var_36C]
add     esp, 0Ch
cmp     ecx, eax
jz      short loc_406EA1
```

تصویر زیر بخشی از متن پیغام باج‌خواهی باج‌افزار را نشان می‌دهد که پس از ایجاد فایل پیغام، درون آن قرار می‌گیرد.

```
push    offset a2IfTorBlockedI ; "\r\n 2) If TOR blocked in your country,"...
lea     eax, [ebp+7C4h+var_36C]
mov     byte ptr [ebp+7C4h+va
push    eax
lea     eax, [ebp+7C4h+var_82
push    eax
call    sub_40B5B0
add     esp, 0Ch
lea     ecx, [ebp+7C4h+var_32
mov     byte ptr [ebp+7C4h+va
push    ecx
mov     ecx, eax
call    sub_4092C8
push    eax
lea     ecx, [ebp+7C4h+var_8(
call    sub_409309
push    offset aExtensionName
lea     eax, [ebp+7C4h+var_8(
mov     byte ptr [ebp+7C4h+va
push    eax
lea     eax, [ebp+7C4h+var_83
push    eax

a2IfTorBlockedI db 0Dh,0Ah              ; DATA XREF: pause+86C↑o pause+ABE↑o
                db ' 2) If TOR blocked in your country, try to use VPN! For this:',0Dh,0Ah
                db ' a) Open any browser (Chrome, Firefox, Opera, IE, Edge) and downl'
                db 'oad and install free VPN programm and download TOR browser from t'
                db 'his site https://torproject.org/ ',0Dh,0Ah
                db '   b) If you are having difficulty purchase bitcoins, or you doubt'
                db ' in buying decryptor, contact to any data recovery company in you'
                db 'r country, they will give you more guarantees and take purchase a'
                db 'nd decryption procedure on themselves. Almost all such companies '
                db 'heared about us and know that our decryption program work, so the'
                db 'y can help you.',0Dh,0Ah
                db 0Dh,0Ah
                db ' When you open our website, put the following data in the input f'
                db 'orm:',0Dh,0Ah
                db 0Dh,0Ah
                db 'Key:',0Dh,0Ah
                db 0Dh,0Ah,0
a_ByTheWayEvery db '.',0Dh,0Ah          ; DATA XREF: pause+817↑o
                db 'By the way, everything is possible to recover(restore), but you n'
                db 'eed to follow our instructions.Otherwise, you cant return your da'
```

علاوه بر پیغام باج‌خواهی پنجره‌ای با عنوان زیر نیز، برای قربانی نمایش داده می‌شود که در بخش قبل به آن اشاره شد.

```
push    offset Caption  ; "Attention!!!!!!!"
push    offset Text     ; "Your computer is encrypted !!! For decr"...
push    ebx
call    ds:MessageBoxW
push    offset aPause
call    sub_4342EA
pop     ecx
lea     ecx, [ebp+7C4h+v
call    sub_4059E4
mov     byte ptr [ebp+7C
cmp     [ebp+7C4h+var_32
jnz     loc_4077F8

; const WCHAR Caption
Caption:                                ; DATA XREF: sub_405684+16↑o pause+C85↑o
                unicode 0, <Attention!!!!!!!>,0
                align 10h
; const WCHAR aSomeOfTheFiles
aSomeOfTheFiles:                        ; DATA XREF: sub_405684+1B↑o
                unicode 0, <Some of the files are encrypted, in order to decrypt them>
                unicode 0, < go to the C:/Instraction/ file and read the instructions>
                unicode 0, < !!!>,0
```

طبق بررسی‌های صورت گرفته، باج‌افزار AnteFrigus از الگوریتم رمزنگاری Salsa20 جهت رمزگذاری فایل‌های موردنظر خود در سیستم قربانی استفاده می‌کند.

```
a_?av?Concretep db '.?AV?$ConcretePolicyHolder@USalsa20_Policy@CryptoPP@@V?$AdditiveC'
                db 'ipherTemplate@V?$AbstractPolicyHolder@UAdditiveCipherAbstractPoli'
                db 'cy@CryptoPP@@VSymmetricCipher@2@@CryptoPP@@@2@UAdditiveCipherAbst'
                db 'ractPolicy@2@@CryptoPP@@',0
off_469784      dd offset off_45507C    ; DATA XREF: .rdata:off_463014↑o
```

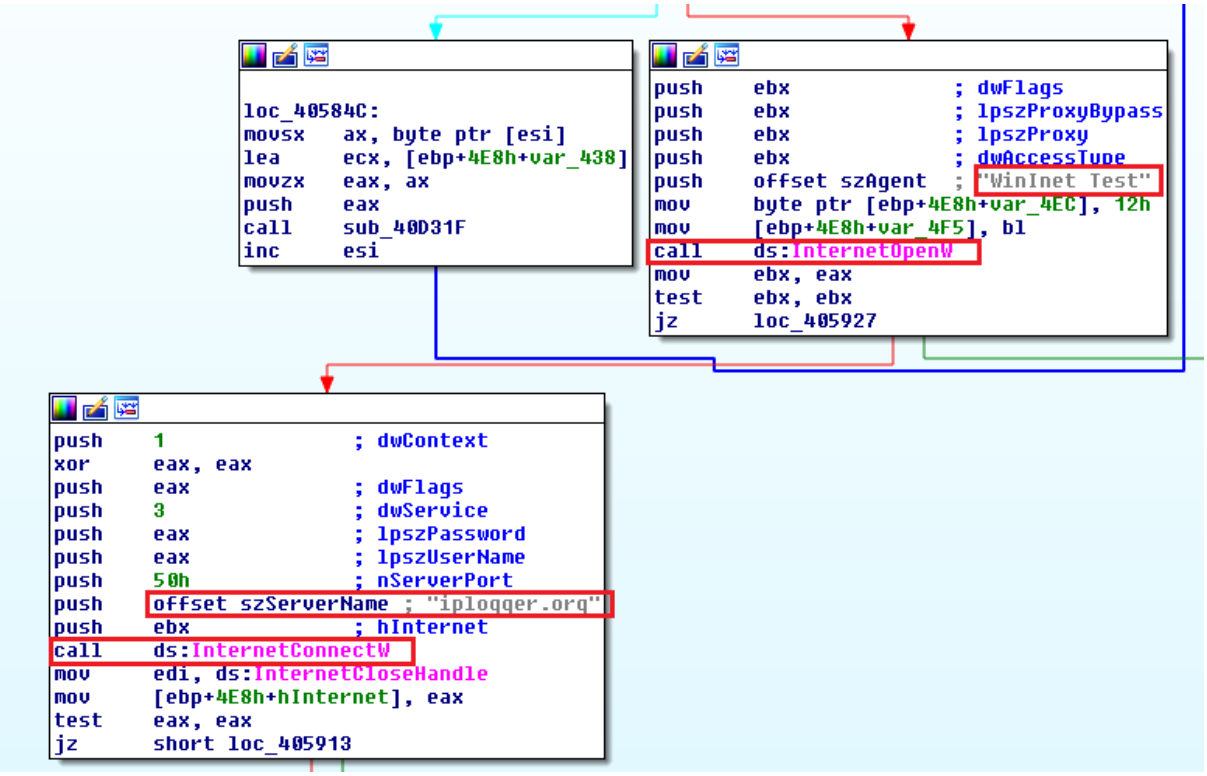
فایل‌های زیر حین فرآیند رمزگذاری بررسی نمی‌شوند.

```
                db 'dll',0
                db '386',0
                db 'adv',0
                db 'ani',0
                db 'big',0
                db 'bat',0
                db 'bin',0
                db 'cab',0
                db 'cmd',0
                db 'com',0
                db 'cpl',0
                db 'cur',0
pack            db 'deskthemepack',0
                align 10h
                db 'diagcab',0
                db 'diagcfg',0
                db 'diagpkg',0
                db 'drv',0
                db 'exe',0
                db 'hlp',0
                db 'icl',0
                db 'icns',0
```

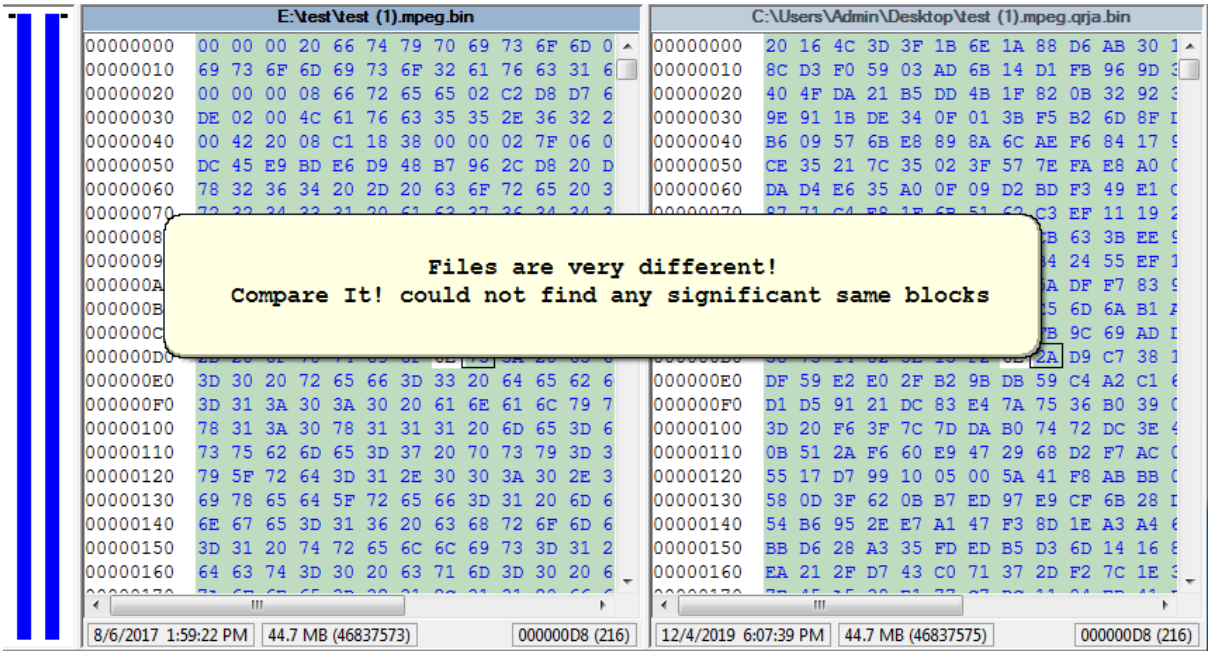
لیست کامل این فایل‌ها به صورت زیر است:

.adv, .ani, .bat, .big, .bin, .cab, .cmd, .com, .cpl, .cur, .deskthemepack, .diagcab, .diagcfg, .diagpkg, .dll, .drv, .exe , .hlp, .hta, .icl, .icns , .ico, .ics, .idx, .key, .ldf, .lnk, .lock, .mod, .mpa, .msc, .msi, .msp,. msstyles, .msu, .nls, .nomedia, .ocx, .pck, .prf, .rom, .rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .wpx

باج‌افزار AnteFrigus برای یافتن آدرس آی‌پی و موقعیت جغرافیایی سیستم قربانی با دامنه iplogger.org ارتباط برقرار می‌کند.



نتایج بررسی‌ها بر روی نمونه فایل‌های رمزشده با نمونه سالم آن‌ها پس از پایان فعالیت باج‌افزار در سیستم قربانی نشان می‌دهد که این باج‌افزار، فایل‌های با حجم حداکثر ۵۰ مگابایت را به طور کامل رمزگذاری می‌کند.



فایل‌های با حجم بیشتر از مقدار مذکور رمزگذاری نخواهند شد.

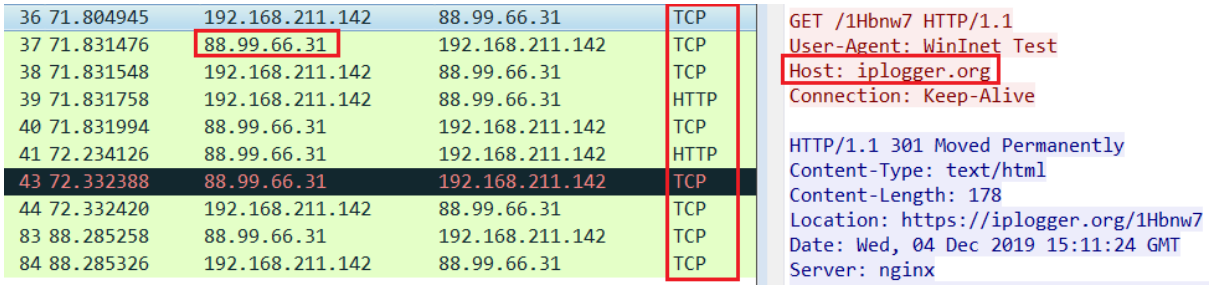
۶-۲ تحلیل ترافیک شبکه:

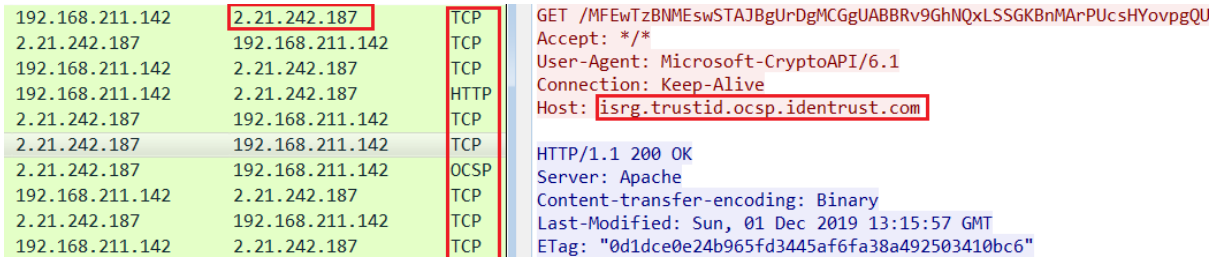
پس از بررسی ترافیک شبکه ایجاد شده حین اجرای باج‌افزار، نتایج زیر حاصل شد.

میزبان‌هایی که باج‌افزار با آن‌ها ارتباط برقرار کرده است:

کشور	پروتکل	شماره پورت	دامنه	آدرس آی‌پی
آلمان	TCP,HTTP	۸۰،۴۳۳	iplogger.org	۸۸.۹۹.۶۶.۳۱
محدوده اتحادیه اروپا	TCP,HTTP	۸۰	isrg.trustid.ocsp.identrust.com	۲.۲۱.۲۴۲.۱۸۷
آمریکا	TCP,HTTP	۸۰	ocsp.int-x3.letsencrypt.org	۷۲.۲۴۷.۱۷۸.۱۶

تصاویر زیر مربوط به ترافیک ایجاد شده و جزییات ارتباطات باج‌افزار می‌باشد.





192.168.211.142	72.247.178.16	TCP	GET /MFMwUTBPME0wSzAJBgUrDgMCGgUABBR%2B5mrncpqz%2FPiiIGI
72.247.178.16	192.168.211.142	TCP	1.1
192.168.211.142	72.247.178.16	TCP	Accept: */*
192.168.211.142	72.247.178.16	HTTP	User-Agent: Microsoft-CryptoAPI/6.1
72.247.178.16	192.168.211.142	TCP	Connection: Keep-Alive
72.247.178.16	192.168.211.142	OCSP	Host: ocsp.int-x3.letsencrypt.org
72.247.178.16	192.168.211.142	TCP	
192.168.211.142	72.247.178.16	TCP	HTTP/1.1 200 OK
72.247.178.16	192.168.211.142	TCP	Server: nginx
192.168.211.142	72.247.178.16	TCP	Content-Type: application/ocsp-response
			Content-Length: 527

تصویر زیر مربوط به درخواست‌های HTTP باج‌افزار می‌باشد.

6	301	HTTP	iplogger.org	/1Hbnw7	178	no-stor...	text/html	2c8b2e9249e4320d59c3fb0a3bc3f2599a9c35ac919a0918ad3f2f8a7a433ecd:7900
7	200	HTTP	Tunnel to	iplogger.org:443	0			2c8b2e9249e4320d59c3fb0a3bc3f2599a9c35ac919a0918ad3f2f8a7a433ecd:7900
8	200	HTTP	isrg.trustid.ocsp.identrust.com	/MFEwTzBNMEswSTAJBgU...	1,398	public, ...	application/ocsp-response	2c8b2e9249e4320d59c3fb0a3bc3f2599a9c35ac919a0918ad3f2f8a7a433ecd:7900
9	200	HTTP	ocsp.int-x3.letsencrypt.org	/MFMwUTBPME0wSzAJBg...	527	public, ...	application/ocsp-response	2c8b2e9249e4320d59c3fb0a3bc3f2599a9c35ac919a0918ad3f2f8a7a433ecd:7900

۶-۳ رمزگشایی:

در حال حاضر، هیچ‌گونه ابزاری جهت رمزگشایی فایل‌های رمزشده توسط این باج‌افزار، ارایه نشده است.