باسمه تعالی

تحلیل فنی باج‌افزار

GandCrab v۵

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور نسخه جدیدی از باج‌افزار GandCrab خبر می‌دهد. فعالیت این نسخه باج‌افزار از آخرین هفته سپتامبر ۲۰۱۸ میلادی شروع شده است. بر اساس گزارش سایت BleepingComputer این نسخه از باج‌افزار GandCrab، از یک آسیب پذیری به نام ALPC Task Scheduler برای اجرا در سیستم قربانی بهره می‌برد. این آسیب پذیری یک اکسپلویت روز صفر(۰Day) است و زمانی که استفاده شود به فایل‌های اجرایی امکان اجرای دستورات با استفاده از امتیازات کامل سیستم (System privileges) را می‌دهد. تغییرات محسوس این نسخه در پسوند متفاوت اضافه شده به فایل‌ها و همینطور پیغام باج‌خواهی جدید می‌باشد.

مشخصات فایل اجرایی :

نام فایل	o.exe
MD۵	۰۷fadb۰۰٦٤٨٦٩٥٣٤٣٩ce۰۰٩٢٦٥١fd٧a٦
SHA-١	e٤٢٤٣١d٣٧٥٦١cc٦٩٥de۰٣b٨٥e٨e٩٩c٩e٣١٣٢١٧٤٢
SHA-٢٥٦	d٧٧٣٧٨dcc٤٢b٩١٢e٥١٤d٣bd٤٤٦٦cdda۰٥۰dda٩b٥٧٧٩٩a٦c٩٧f٧۰e٨٤٨٩dd٨d۰
اندازه فایل	۱۸۳ کیلوبایت

فایل اجرایی این باج‌افزار دارای ۵ بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٥٧	٤۰٩٦	٧٨٩٦٤	٧٩٣٦۰
.rdata	٤.٥٩	٨٦۰١٦	٢٨٣٨٤	٢٨٦٧٢
.data	٤.٨٦	١١٤٦٨٨	٨۰١١٦	٧٢٧۰٤
.src	٤.٧	١٩٦٦۰٨	٤٨۰	٥١٢
.reloc	٦.٦٥	٢۰۰٧۰٤	٥۰٤٤	٥١٢۰

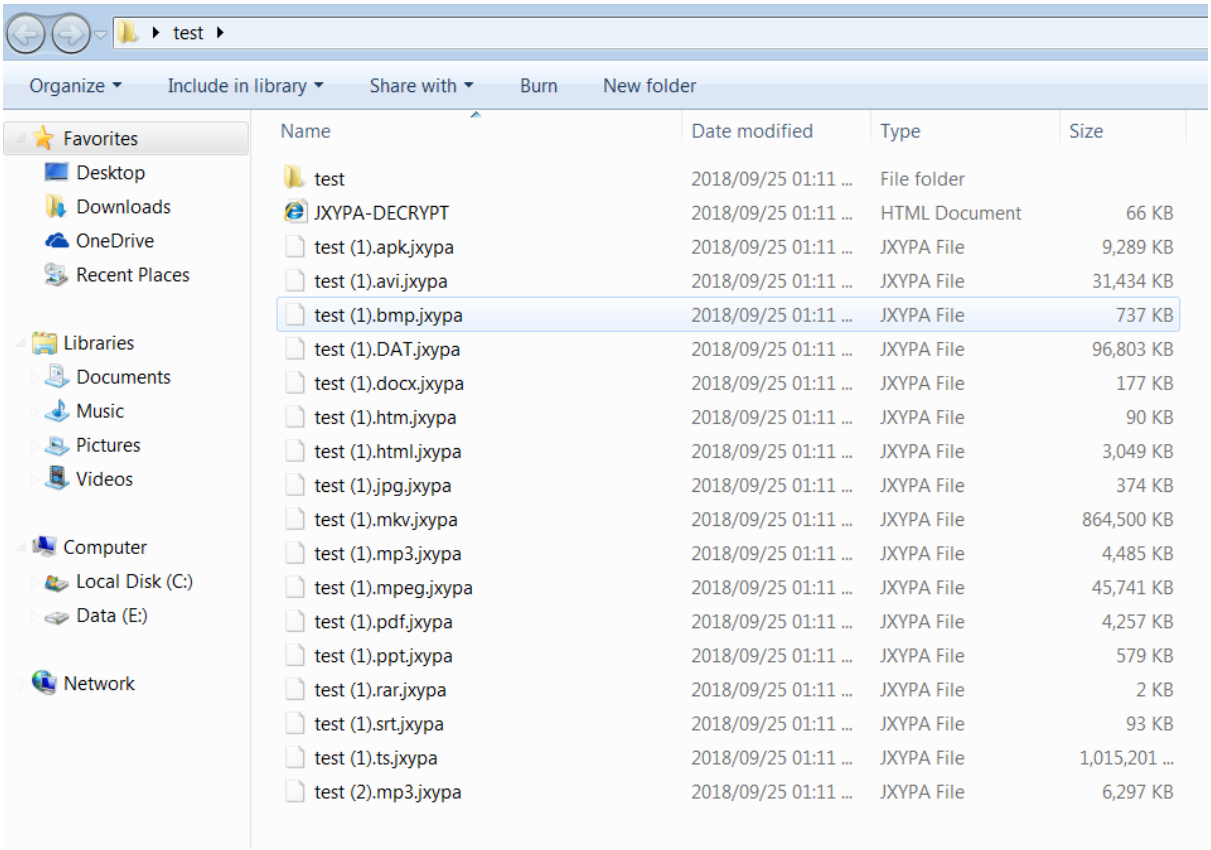
تحلیل پویا :

برای بررسی عمیق‌تر این نسخه از باج‌افزار GandCrab، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. این باج‌افزار به محض اجرا در سیستم قربانی در همان ابتدا از طریق اجرای دستور زیر در محیط cmd، فضای VSS سیستم قربانی را پاک می‌کند:

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

سپس شروع به جست و جوی فایل‌های موردنظر خود کرده و به سرعت آن‌ها را رمزگذاری می‌کند. براساس بررسی‌های انجام شده، این نسخه از باج‌افزار GandCrab، تقریبا تمام انواع فایل‌ها با پسوندهای مختلف را رمزگذاری می‌کند. فایل‌های با نام فارسی نیز توسط باج‌افزار رمزگذاری می‌شوند. فقط فایل‌های درون پوشه Windows سیستم‌عامل، از این باج‌افزار در امان هستند.

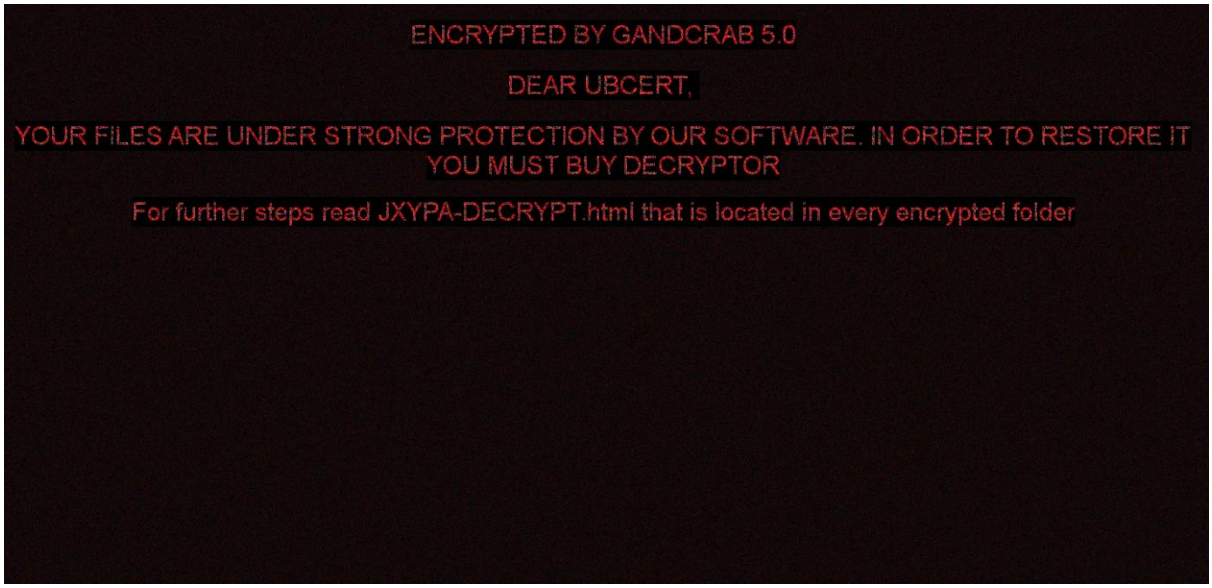
پس از پایان فرآیند رمزگذاری، فایل‌های سیستم قربانی به شکل زیر تغییر پیدا می‌کنند:



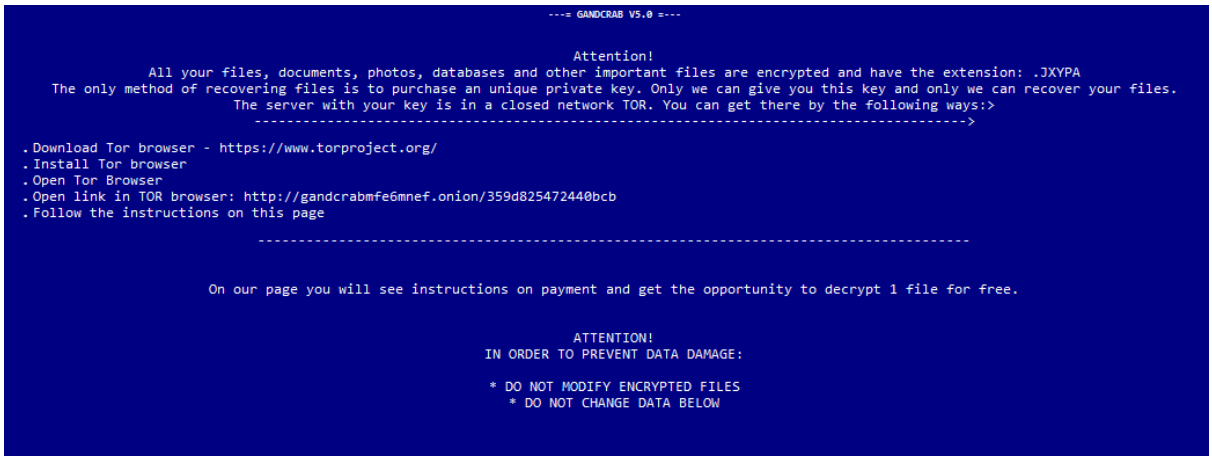
همانطور که در تصویر بالا مشاهده می‌کنید، تمام فایل‌ها با پسوندهای مختلف، توسط باج‌افزار رمزگذاری شده‌اند. به انتهای فایل‌های رمزشده نیز پسوندی با الگوی ۵ کاراکتر تصادفی اضافه شده است. ضمناً درون

هر پوشه‌ای از سیستم‌عامل کـه فـایلی در آن رمزگـذاری شـده باشـد، فایـل پیغـام بـاج‌خـواهی بـا عنـوان JXYPA-DECRYPT.html قرار می‌گیرد. پنج کاراکتر اول عنوان پیغام باج‌خواهی، همان کاراکترهای اضافه شـده به انتهای فایل‌های رمزشده می‌باشند که با هر بار اجرای باج‌افزار، تغییر می‌کنند.

پس از رمزگذاری فایل‌ها، تصویر صفحه نمایش سیستم قربانی به شکل زیر تغییر پیدا می‌کند:



همانطور که در تصویر بالا مشاهده می‌کنید، فایل پیغام باج‌خواهی در هر پوشه حـاوی فایـل‌هـای رمزشـده قرار می‌گیرد. صفحه مربوط به پیغام باج‌خواهی این نسخه از باج‌افزار GandCrab به صورت زیر می‌باشد:



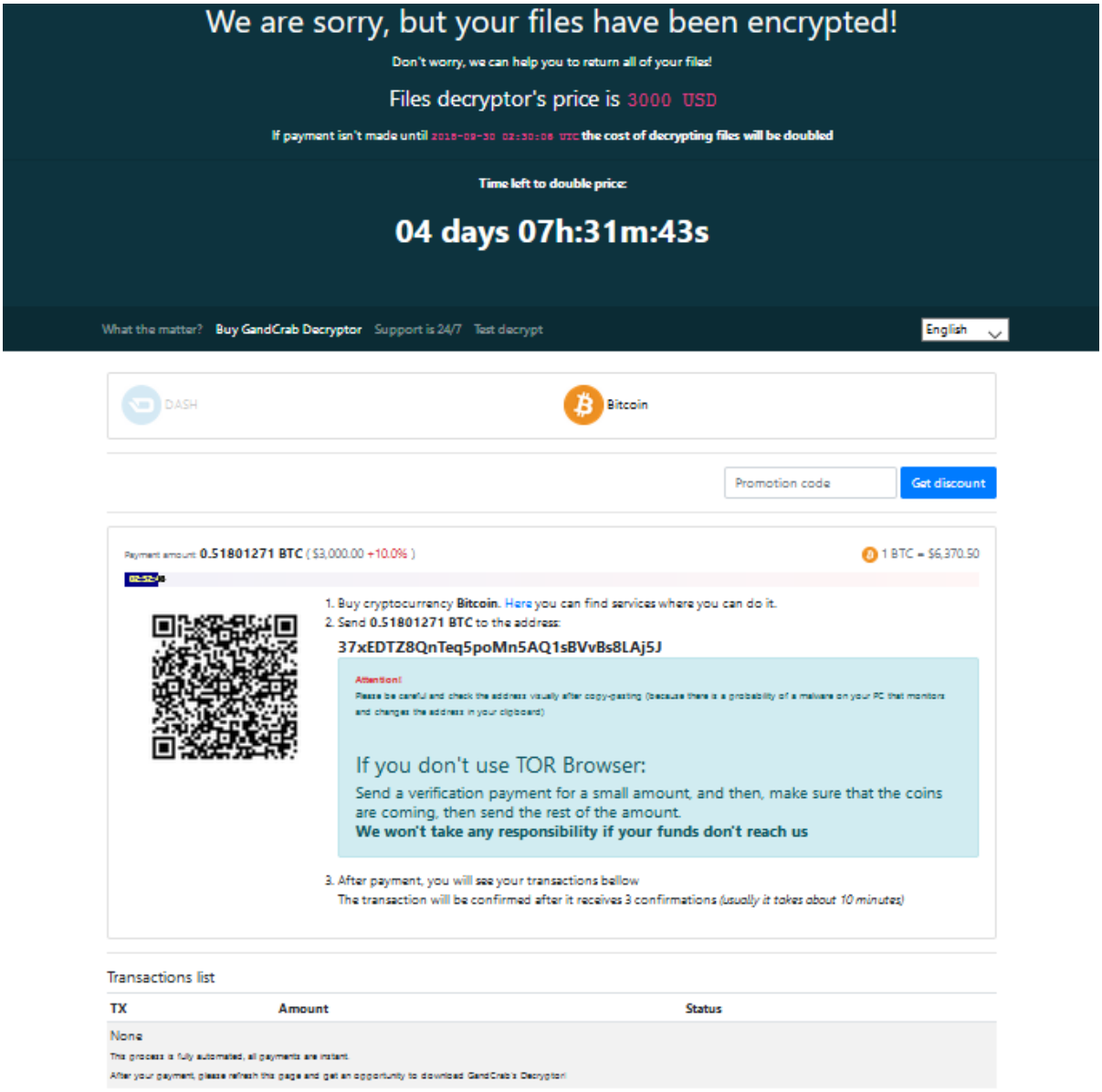
بر اساس تصویر فوق، در بالای این صفحه نام باج‌افزار و نسخه آن کاملا مشهود است. در ادامه عنوان شـده است که تمامی فایل‌ها، اسناد، تصاویر، پایگاه‌های داده ودیگر فایل‌های مهم درون سیستم رمزگذاری شده‌اند و پسوندی که به فایل‌ها اضافه شده است نیز در این پیغام کاملا مشخص است. در ادامه‌ی پیغـام، مهاجمـان تنها راه بازیابی فایل‌ها را خرید کلید خصوصی عنوان کرده‌اند و مدعی شده‌اند که تنها آن‌ها می‌تواننـد کلیـد

را به قربانی بدهند و فایل‌هایش را بازگردانند. سپس قربانی را جهت دریافت کلید به سرور خصوصی خود راهنمایی کرده و عنوان کرده‌اند، تنها از طریق مرورگر Tor قابل دسترسی می‌باشد. آدرسی که جهت ارتباط با قربانی در پیغام باج‌خواهی قرار داده شده است به صورت زیر است:

http://gandcrabmfe٦mnef.onion/٣٥٩d٨٢٥٤٧٢٤٤٠bcb

در انتهای پیغام نیز ذکر شده است که جهت ضمانت یک فایل، به صورت رایگان رمزگشایی می‌شود و همینطور هشدارهایی برای قربانی مبنی بر عدم تغییر فایل‌ها به چشم می‌خورد.

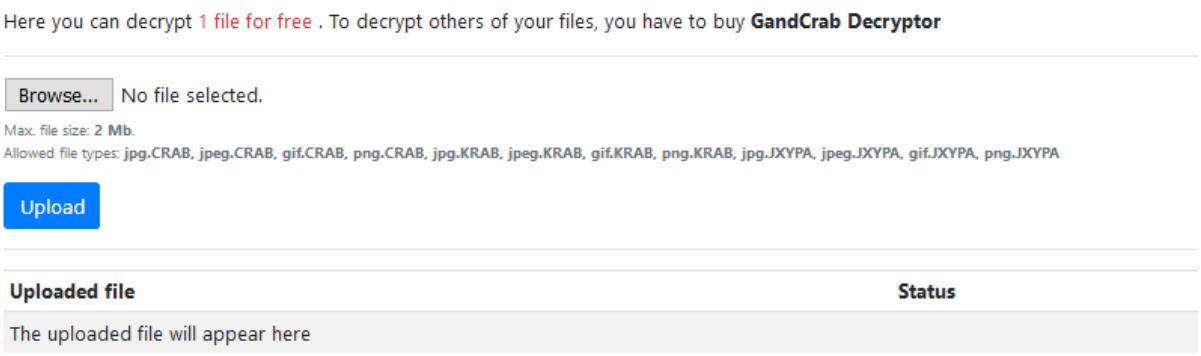
برای کسب اطلاعات بیشتر به آدرس وب سایت مذکور مراجعه کردیم. تصویری که در ادامه مشاهده می‌کنید مربوط به این وب‌سایت می‌باشد که در واقع صفحه پرداخت باج این باج‌افزار است:



همانطور که در تصویر ملاحظه می‌کنید، مبلغ باج جهت رمزگشایی فایل‌ها ۳۰۰۰ دلار درنظر گرفته شده است. البته این مبلغ متغیر می‌باشد و به نقل از یکی از منابع معتبر از ۸۰۰ دلار شروع می‌شود. در ادامه قربانی تهدید شده که اگر در مدت زمانی که به صورت زمان‌سنج در صفحه کاملا مشخص است، این مبلغ پرداخت نشود، به دو برابر افزایش پیدا خواهد کرد. در اواسط صفحه نیز قسمتی جهت انتخاب زبان متن در نظر گرفته شده است که ۷ زبان دیگر غیر از زبان انگلیسی را پشتیبانی می‌کند. روشی که در ادامه برای پرداخت باج در نظر گرفته شده است از طریق بیت‌کوین یا Dash می‌باشد. در قسمت پایین صفحه نیز مبلغ باج ۳۰۰۰ دلار به بیت‌کوین به صورت دقیق ذکر شده است. همینطور آدرس کیف‌پول نیز در ادامه قرار داده

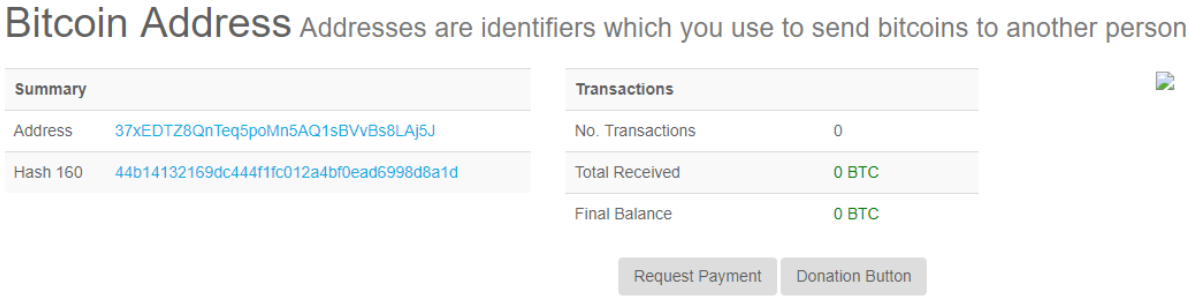
شده است. سپس اشاره شده که اگر قربانی مبلغ باج را پرداخت کند، اطلاعات مربوط به پرداخت خود را در انتهای صفحه مشاهده می‌کند.

قسمت Test decrypt نیز مربوط به رمزگشایی فایل‌ها به صورت رایگان جهت تضمین به قربانی است. نکته جالب آن است که فایل‌هایی که توسط نسخه‌های قبلی این باج‌افزار رمزگذاری شده‌اند نیز، در این نسخه قابل رمزگشایی خواهند بود. تصویر زیر مربوط به این قسمت می‌باشد:



همانطور که در تصویر مشاهده می‌کنید، یک فایل با حجم حداکثر ۲ مگابایت جهت تضمین رمزگشایی، به صورت رایگان رمزگشایی می‌شود. انواع فایل‌ها با پسوندهایی که پشتیبانی می‌شوند نیز در ادامه آمده‌اند. پسوندهای CRAB و KRAB نیز که به ترتیب مربوط به نسخه‌های ۳ و ٤ می‌باشند، در بین آن‌ها وجود دارند.

با دسترسی به آدرس کیف‌پول این باج‌افزار، وضعیت فعالیت آن را مورد بررسی قرار دادیم. خوشبختانه کیف‌پول این باج‌افزار، تاکنون تراکنشی نداشته است. تصویر زیر مربوط به اطلاعات کیف‌پول این باج‌افزار است:



طبق بررسی‌های صورت گرفته، این نسخه از باج‌افزار GandCrab فقط در شرایط اتصال سیستم به اینترنت کار می‌کند و در صورت قطع ارتباط، به صورت غیرفعال در سیستم باقی می‌ماند.

تحلیل ایستا:

قطعه کد زیر مربوط به بخشی از قسمت رمزگذاری می‌باشد. از توابع CryptGenkey، CryptExportkey به ترتیب برای تولید کلید خصوصی جهت رمزگذاری داده‌ها و کلید عمومی استفاده شده است. با توجه به این موضوع و اینکه باج‌افزار تنها در حالت اتصال سیستم به اینترنت کار می‌کند، از دو روش رمزنگاری متقارن و نامتقارن به صورت همزمان برای رمزگذاری داده ها بهره می‌برد. طبق بررسی‌های انجام شده، این باج‌افزار از الگوریتم متقارن Salsa۲۰ و الگوریتم نامتقارن RSA ۲۰۴۸ بیتی جهت رمزگذاری، استفاده می‌کند.

```
.text:00406E54                call    ds:CryptGenKey
.text:00406E5A                push    esi             ; pdwDataLen
.text:00406E5B                push    [ebp+pbData]    ; pbData
.text:00406E5E                mov     esi, ds:CryptExportKey
.text:00406E64                xor     ebx, ebx
.text:00406E66                push    ebx             ; dwFlags
.text:00406E67                push    6               ; dwBlobType
.text:00406E69                push    ebx             ; hExpKey
.text:00406E6A                push    [ebp+phKey]     ; hKey
.text:00406E6D                call    esi ; CryptExportKey
.text:00406E6F                push    [ebp+pdwDataLen] ; pdwDataLen
.text:00406E72                push    [ebp+var_C]     ; pbData
.text:00406E75                push    ebx             ; dwFlags
.text:00406E76                push    7               ; dwBlobType
.text:00406E78                push    ebx             ; hExpKey
.text:00406E79                push    [ebp+phKey]     ; hKey
.text:00406E7C                call    esi ; CryptExportKey
```

در ادامه قطعه کد بالا، از تابع CryptEncrypt برای رمزگذاری داده‌ها استفاده شده است.

```
.text:00406F25                call    ds:CryptGetKeyParam
.text:00406F2B                push    [ebp+dwBufLen]  ; dwBufLen
.text:00406F2E                mov     eax, [ebp+pdwDataLen]
.text:00406F31                push    eax             ; pdwDataLen
.text:00406F32                push    [ebp+arg_0]     ; pbData
.text:00406F35                push    esi             ; dwFlags
.text:00406F36                push    1               ; Final
.text:00406F38                push    esi             ; hHash
.text:00406F39                push    [ebp+phKey]     ; hKey
.text:00406F3C                mov     dword ptr [eax], 0C8h
.text:00406F42                call    ds:CryptEncrypt
.text:00406F48                mov     edi, eax
.text:00406F4A                call    ds:GetLastError
.text:00406F50
```

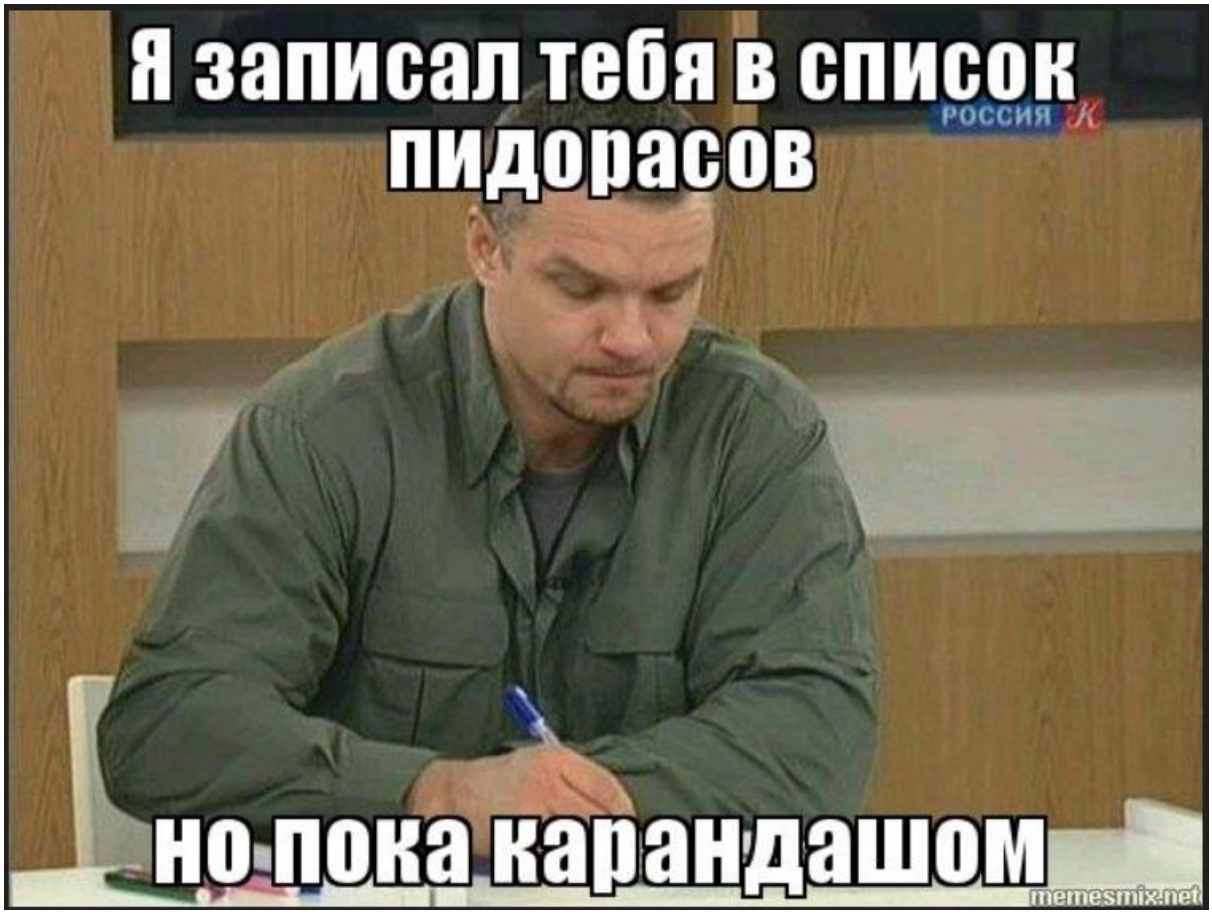
از قطعه کد زیر برای ایجاد و مقدار دهی به رجیستری‌های مورد نیاز باج‌افزار، استفاده شده است:

```
.text:0040495F                call    ds:RegCreateKeyExW
.text:00404965                mov     [ebp-10h], eax
.text:00404968                cmp     dword ptr [ebp-10h], 0
.text:0040496C                jnz     short loc_4049A7
.text:0040496E                push    dword ptr [ebp+8]
.text:00404971                call    ds:lstrlenW
.text:00404977                lea     eax, [eax+eax+2]
.text:0040497B                push    eax
.text:0040497C                push    dword ptr [ebp+8]
.text:0040497F                push    3
.text:00404981                push    0
.text:00404983                push    dword ptr [ebp-14h]
.text:00404986                push    dword ptr [ebp-4]
.text:00404989                call    ds:RegSetValueExW
.text:0040498F                mov     [ebp-18h], eax
.text:00404992                xor     eax, eax
.text:00404994                cmp     dword ptr [ebp-18h], 0
.text:00404998                setz    al
.text:0040499B                mov     [ebp-8], eax
.text:0040499E                push    dword ptr [ebp-4]
.text:004049A1                call    ds:RegCloseKey
```

در ادامه بررسی کد این نسخه از باج‌افزار GandCrab با لینکی مواجه شدیم که با بررسی‌های بیشتر متوجه شدیم تیم پیشتیبانی این باج‌افزار از آن برای تحقیر آزمایشگاه امنیتی AhnLab استفاده کرده است. این لینک با کادر قرمز رنگ در قطعه کد زیر مشخص شده است:

```
.text:00405208                push    offset aXAhnlabHttpMem ; "%X ahnlab http://memesmix.net/media/cre"...
.text:0040520D                lea     eax, [ebp-0C10h]
.text:00405213                push    eax
.text:00405214                call    ds:wsprintfW
.text:0040521A                add     esp, 0Ch
.text:0040521D                lea     eax, [ebp-810h]
.text:00405223                push    eax
.text:00405224                lea     eax, [ebp-0C10h]
.text:0040522A                push    eax
.text:0040522B                lea     eax, [ebp-1010h]
.text:00405231                push    eax
.text:00405232                call    loc_404FB7
.text:00405237                add     esp, 0Ch
.text:0040523A                push    2
.text:0040523C                pop     eax
.text:0040523D                imul    eax, 14h
.text:00405240                xor     ecx, ecx
.text:00405242                mov     [ebp+eax-810h], cx
.text:0040524A                lea     eax, [ebp-810h]
.text:00405250                push    eax
```

آدرس کامل این لینک به صورت http://memesmix.net/media/created/dd•doq.jpg می‌باشد که تصویر یکی از مدیران این آزمایشگاه با عبارتی توهین آمیز به زبان روسی را نمایش می‌دهد. این تصویر به صورت زیر می‌باشد:



همانطور که در ابتدا توضیح دادیم این باج‌افزار هیچ فایلی را در پوشه سیستم عامل ویندوز رمزگذاری نمی‌کند. از قطعه کد زیر برای دریافت مسیر این پوشه در سیستم عامل استفاده شده است. البته باج‌افزار تعدادی از رجیستری‌های مورد نیاز خود را نیز در این مسیر قرار می‌دهد:

```
.text:0040519E          call    ds:GetWindowsDirectoryW
.text:004051A4          push    2
.text:004051A6          pop     eax
.text:004051A7          imul    eax, 3
.text:004051AA          xor     ecx, ecx
.text:004051AC          mov     edx, [ebp-4]
.text:004051AF          mov     [edx+eax], cx
.text:004051B3          push    100h
.text:004051B8          mov     eax, [ebp-4]
.text:004051BB          add     eax, 400h
.text:004051C0          push    eax
.text:004051C1          mov     eax, [ebp-4]
.text:004051C4          add     eax, 604h
.text:004051C9          push    eax
.text:004051CA          mov     eax, [ebp-4]
.text:004051CD          add     eax, 608h
.text:004051D2          push    eax
.text:004051D3          mov     eax, [ebp-4]
.text:004051D6          add     eax, 600h
.text:004051DB          push    eax
.text:004051DC          push    100h
.text:004051E1          mov     eax, [ebp-4]
.text:004051E4          add     eax, 200h
.text:004051E9          push    eax
.text:004051EA          push    dword ptr [ebp-4]
```

از قطعه کد زیر برای تعیین اینکه یک درایو، دیسک قابل جابجایی، ثابت، CD-ROM، دیسک RAM یـا درایـو شبکه می‌باشد، استفاده شده است:

```
.text:004086A2          call    ds:GetDriveTypeW
.text:004086A8          mov     esi, eax
.text:004086AA          cmp     esi, 2
.text:004086AD          jbe     loc_4087A8
.text:004086B3          cmp     esi, 5
.text:004086B6          jz      loc_4087A8
.text:004086BC          xor     eax, eax
.text:004086BE          mov     word ptr [esp+90h+var_60], ax
.text:004086C3          lea     eax, [esp+90h+RootPathName]
.text:004086C7          push    eax             ; lpString2
.text:004086C8          push    dword ptr [ebx+7Ch] ; lpString1
.text:004086CB          call    edi ; lstrcatW
.text:004086CD          push    5Ch
.text:004086CF          pop     eax
```

لیستی از فرآیندهایی که باج‌افزار از آنها استفاده می‌کند، در قطعه کد زیر قابل مشاهده است:

```
.text:00408841                mov     [ebp+lpString1], offset aAvp_exe ; "AVP.EXE"
.text:00408848                mov     [ebp+var_44], offset aEkrn_exe ; "ekrn.exe"
.text:0040884F                mov     [ebp+var_40], offset aAvgnt_exe ; "avgnt.exe"
.text:00408856                mov     [ebp+var_3C], offset aAshdisp_exe ; "ashDisp.exe"
.text:0040885D                mov     [ebp+var_38], offset aNortonantibot_ ; "NortonAntiBot.exe"
.text:00408864                mov     [ebp+var_34], offset aMcshield_exe ; "Mcshield.exe"
.text:0040886B                mov     [ebp+var_30], offset aAvengine_exe ; "avengine.exe"
.text:00408872                mov     [ebp+var_2C], offset aCmdagent_exe ; "cmdagent.exe"
.text:00408879                mov     [ebp+var_28], offset aSmc_exe ; "smc.exe"
.text:00408880                mov     [ebp+var_24], offset aPersfw_exe ; "persfw.exe"
.text:00408887                mov     [ebp+var_20], offset aPccpfw_exe ; "pccpfw.exe"
.text:0040888E                mov     [ebp+var_1C], offset aFsguiexe_exe ; "fsguiexe.exe"
.text:00408895                mov     [ebp+var_18], offset aCfp_exe ; "cfp.exe"
.text:0040889C                mov     [ebp+var_14], offset aMsmpeng_exe ; "msmpeng.exe"
.text:004088A3                call    esi ; VirtualAlloc
.text:004088A5                mov     esi, eax
.text:004088A7                test    esi, esi
.text:004088A9                jnz     short loc_4088B2
```

فرآیندهایی که در قطعه کد بالا مشاهده می‌کنید به ترتیب مربوط به آنتی‌ویروس‌های Kaspersky، ESET، Avira، avast، Norton، McAfee، Panda، Comodo، فایروال Sygate مربوط به شرکت امنیتی Symantec، فایروال Kerio، آنتی ویروس‌های Trend Micro، F-secure، فایروال COMODO و Windows Defenderمی‌باشند که در پس زمینه سیستم عامل اجرا می‌شوند. وجود این فرآیندها در کد باج‌افزار، احتمالا برای توقف آنها پس از نفوذ به سیستم قربانی می‌باشد.

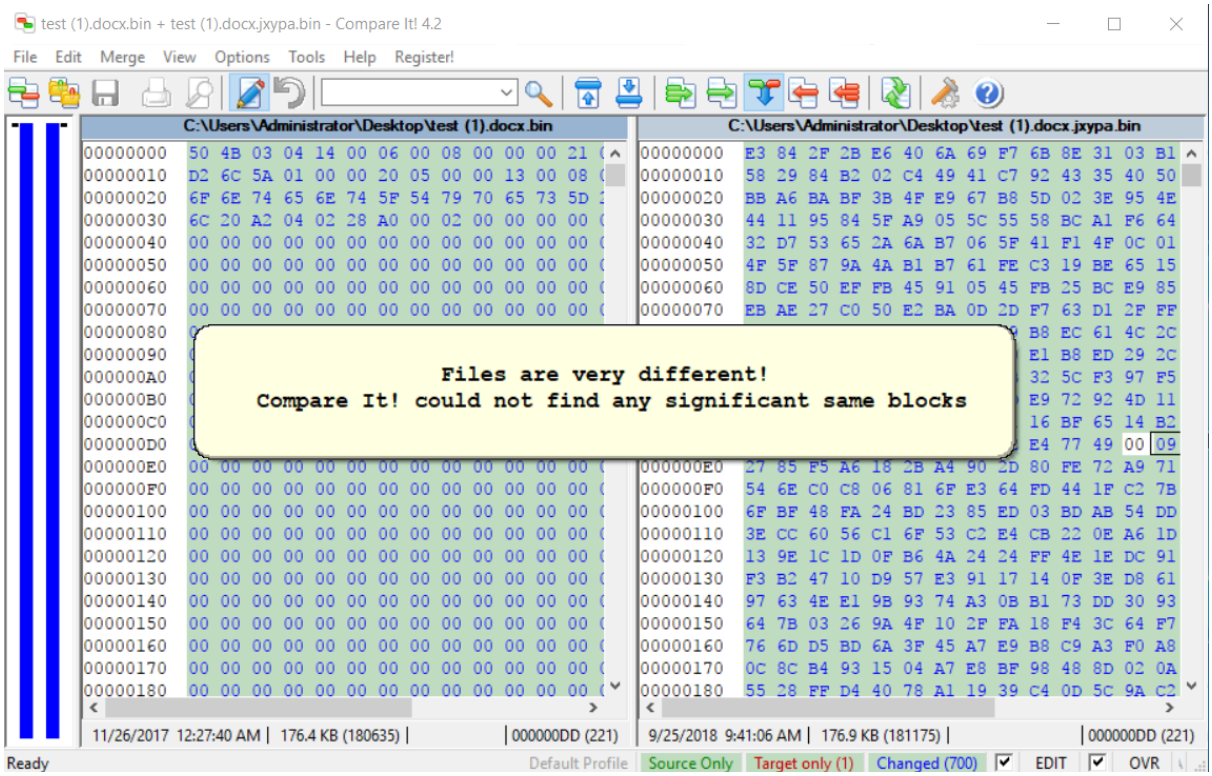
از قطعه کد زیر برای دریافت مسیر پوشه System درون سیستم عامل استفاده شده است. باج‌افزار تعدادی از کلید رجیستری‌های موردنیاز خود را در این مسیر قرار داده و از این محل می‌خواند:

```
.text:00402274                call    ds:GetSystemDirectoryW
.text:0040227A                mov     [ebp-1Ch], eax
.text:0040227D                and     dword ptr [ebp-4], 0
.text:00402281                cmp     dword ptr [ebp-1Ch], 0
.text:00402285                jbe     loc_40238E
.text:0040228B                push    dword ptr [ebp-18h]
.text:0040228E                call    ds:lstrlenW
.text:00402294                mov     esi, eax
.text:00402296                lea     eax, [ebp-0CCh]
.text:0040229C                push    eax
.text:0040229D                call    ds:lstrlenW
.text:004022A3                add     esi, [ebp-1Ch]
.text:004022A6                add     eax, esi
.text:004022A8                lea     ecx, [eax+eax+4]
.text:004022AC                call    sub_4091A1
.text:004022B1                mov     [ebp-4], eax
.text:004022B4                cmp     dword ptr [ebp-4], 0
.text:004022B8                jz      loc_40238E
.text:004022BE                push    dword ptr [ebp-1Ch]
.text:004022C1                push    dword ptr [ebp-4]
```

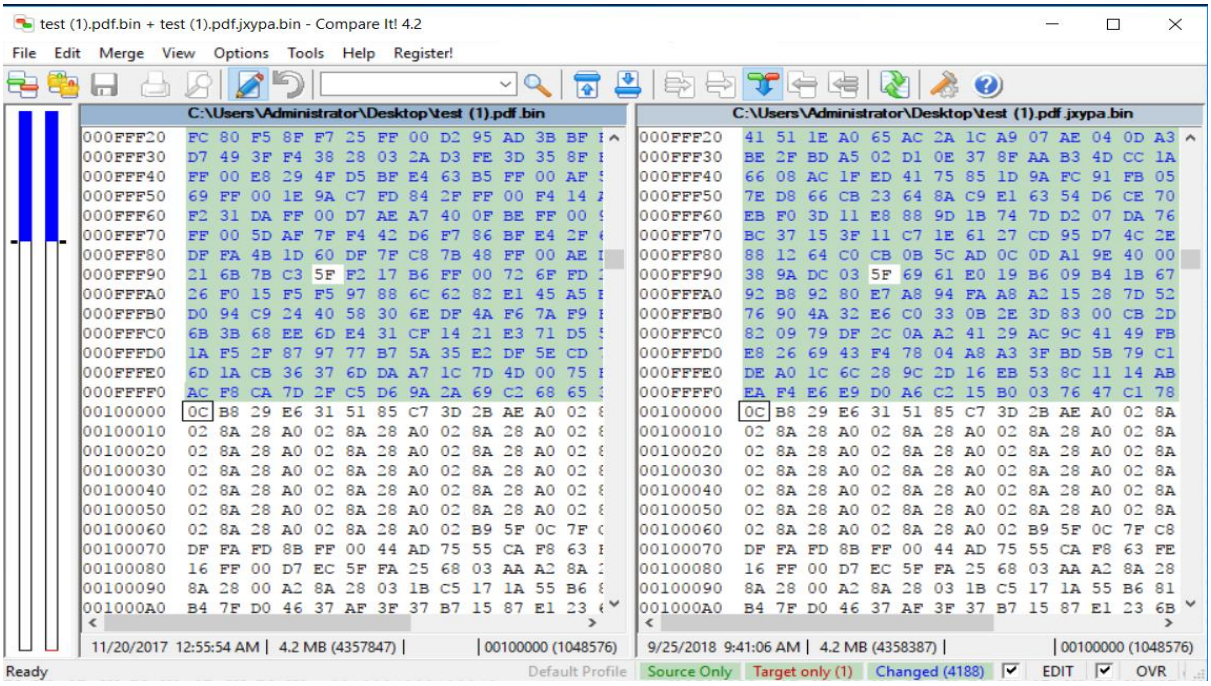
قطعه کد زیر مربوط به رمزگذاری فایل‌ها می‌باشد. قسمت‌های مشخص شده در تصویر، توضیحات مربوط به حجمی از فایل است که رمزگذاری می‌شود:

```
.text:004012F9 loc_4012F9:                             ; CODE XREF: sub_401261+71↑j
.text:004012F9                 mov     eax, [ebp+arg_8]
.text:004012FC                 push    dword ptr [eax+1Ch] ; nNumberOfBytesToLockHigh
.text:004012FF                 push    dword ptr [eax+20h] ; nNumberOfBytesToLockLow
.text:00401302                 push    0               ; dwFileOffsetHigh
.text:00401304                 push    0               ; dwFileOffsetLow
.text:00401306                 push    ebx             ; hFile
.text:00401307                 call    ds:LockFile
.text:0040130D                 push    40h
.text:0040130F                 pop     eax
```

جهت بررسی دقیق مقدار حجم رمزشده از فایل‌ها، نمونه‌هایی رمزشده از آن‌ها را به نمونه سالم آن‌ها مقایسه کردیم. این نسخه از باج‌افزار GandCrab، دقیقا ۱ مگابایت اول هر فایل را رمزگذاری می‌کند و مقدار ۵۳۹ بایت نیز به انتهای هر فایل رمز شده اضافه می‌کند. تصاویر زیر مربوط به نتایج مقایسه دو فایل رمزشده با نمونه سالم آنها می‌باشد:



همانطور که در تصویر بالا مشاهده می‌کنید، این فایل کمتر از ۱ مگابایت حجم داشته و کاملا رمزگذاری شده است.



همانطور که مشاهده می‌کنید، این فایل ٤.٢ مگابایت حجم دارد که دقیقا ١ مگابایت اول آن رمزشده است. مقایسه فایل‌های با حجم بیشتر نیز، همین نتیجه را نشان داد.

از تابع استفاده شده در قطعه کد زیر، برای بررسی شبکه یا اتصالات موجود با سیستم قربانی، استفاده شده که به نظر می‌رسد این باج‌افزار از طریق شبکه نیز منتشر می‌گردد.

```
.text:00403D59 loc_403D59:                             ; CODE XREF: .text:00403C8D↑j
.text:00403D59                                         ; .text:00403CA7↑j
.text:00403D59                 lea     eax, [ebp-18h]
.text:00403D5C                 push    eax
.text:00403D5D                 push    dword ptr [ebp+8]
.text:00403D60                 push    0
.text:00403D62                 push    1
.text:00403D64                 push    2
.text:00403D66                 call    ds:WNetOpenEnumW
.text:00403D6C                 mov     [ebp-1Ch], eax
.text:00403D6F                 cmp     dword ptr [ebp-1Ch], 0
.text:00403D73                 jnz     loc_403E28
.text:00403D79                 mov     dword ptr [ebp-14h], 1000h
.text:00403D80                 mov     dword ptr [ebp-8], 80h
.text:00403D87                 jmp     short loc_403D90
```

از قطعه کد زیر، برای ایجاد پیغامی که در پس زمینه سیستم قربانی نمایش داده می‌شود، استفاده شده است:

```
loc_40A1D4:                            ; CODE XREF: .text:0040A178↑j
                xor     edx, edx
                mov     ecx, offset aCreatebackgr_0 ; "CreateBackgroundNotifier: GetStrippedEx"...
                call    nullsub_1
```

بخش کوتاهی از این پیغام، با کادر قرمز رنگ در قطعه کد زیر مشخص شده است:

```
.text:00409C6E loc_409C6E:                             ; CODE XREF: .text:00409C4E↑j
.text:00409C6E                 push    offset aDearUser ; "DEAR USER, "
.text:00409C73                 lea     eax, [ebp-0B38h]
.text:00409C79                 push    eax
.text:00409C7A                 call    ds:wsprintfW
.text:00409C80                 pop     ecx
.text:00409C81                 pop     ecx
```

قطعه کدهای زیر مربوط به اتصال اینترنت، دریافت و ارسال درخواست‌های باج‌افزار از طریق پروتکل Http می‌باشد:

```
.text:004066F1                 call    ds:InternetOpenW
.text:004066F7                 mov     [ebp+var_90], eax
.text:004066FD                 test    eax, eax
.text:004066FF                 jz      loc_4067EF
.text:00406705                 push    ebx             ; dwContext
.text:00406706                 push    ebx             ; dwFlags
.text:00406707                 push    3               ; dwService
.text:00406709                 push    ebx             ; lpszPassword
.text:0040670A                 push    ebx             ; lpszUserName
.text:0040670B                 push    50h             ; nServerPort
.text:0040670D                 push    esi             ; lpszServerName
.text:0040670E                 push    eax             ; hInternet
.text:0040670F                 call    ds:InternetConnectW
.text:00406715                 mov     edi, ds:InternetCloseHandle
.text:0040671B                 mov     esi, eax
.text:0040671D                 mov     [ebp+hInternet], esi
.text:00406723                 test    esi, esi
.text:00406725                 jz      loc_4067E5
.text:0040672B                 lea     eax, [ebp+szObjectName]
.text:00406731                 push    offset asc_419E9C ; "/"
.text:00406736                 push    eax             ; LPWSTR
.text:00406737                 call    ds:wsprintfW
.text:0040673D                 pop     ecx
.text:0040673E                 pop     ecx
.text:0040673F                 push    ebx             ; dwContext
.text:00406740                 push    8424F700h       ; dwFlags
.text:00406745                 push    ebx             ; lplpszAcceptTypes
.text:00406746                 push    ebx             ; lpszReferrer
.text:00406747                 push    offset szVersion ; "HTTP/1.1"
.text:0040674C                 lea     eax, [ebp+szObjectName]
.text:00406752                 push    eax             ; lpszObjectName
.text:00406753                 push    offset szVerb   ; "GET"
```

```
.text:00406758                 push    esi             ; hConnect
.text:00406759                 call    ds:HttpOpenRequestW
.text:0040675F                 mov     esi, eax
.text:00406761                 test    esi, esi
.text:00406763                 jz      short loc_4067DD
.text:00406765                 mov     eax, 400h
.text:0040676A                 mov     [ebp+dwBufferLength], eax
.text:00406770
.text:00406770 loc_406770:                             ; CODE XREF: sub_40651B+25C↓j
.text:00406770                 mov     [ebp+var_A0], bl
.text:00406776                 dec     eax
.text:00406777                 jnz     short loc_406770
.text:00406779                 push    ebx             ; dwOptionalLength
.text:0040677A                 push    ebx             ; lpOptional
.text:0040677B                 push    ebx             ; dwHeadersLength
.text:0040677C                 push    ebx             ; lpszHeaders
.text:0040677D                 push    esi             ; hRequest
.text:0040677E                 mov     [ebp+dwIndex], ebx
.text:00406784                 call    ds:HttpSendRequestW
.text:0040678A                 test    eax, eax
.text:0040678C                 jz      short loc_4067DA
.text:0040678E                 lea     eax, [ebp+dwIndex]
.text:00406794                 push    eax             ; lpdwIndex
.text:00406795                 lea     eax, [ebp+dwBufferLength]
.text:0040679B                 push    eax             ; lpdwBufferLength
.text:0040679C                 lea     eax, [ebp+Buffer]
.text:004067A2                 push    eax             ; lpBuffer
.text:004067A3                 push    13h             ; dwInfoLevel
.text:004067A5                 push    esi             ; hRequest
.text:004067A6                 call    ds:HttpQueryInfoA
.text:004067AC                 test    eax, eax
.text:004067AE                 jz      short loc_4067D4
.text:004067B0                 push    offset String2  ; "30x"
.text:004067B5                 lea     eax, [ebp+Buffer]
```

تحلیل ترافیک شبکه :

پس از بررسی ترافیک ایجاد شده بعد از اجرای باج‌افزار، نتایج زیر حاصل گردید:

درخواست‌های DNS:

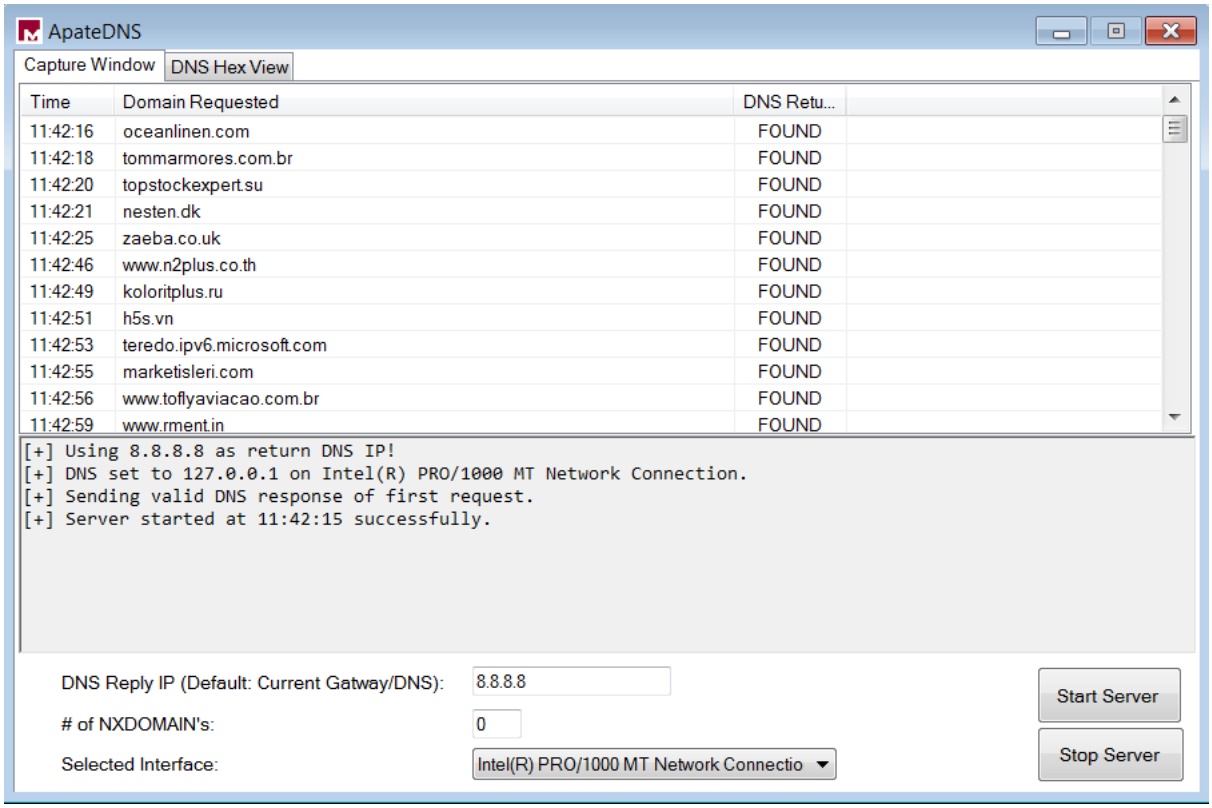
کشور	آدرس آی‌پی	دامنه
--	--	zaeba.co.uk
آمریکا	٦٩.٧٣.١٨٠.١٥١	www.wash-wear.com
برزیل	١٧٩.١٨٨.١١.٣٤	www.toflyaviacao.com.br
آمریکا	١٠٤.٢٤.١٠٤.١٣	www.rment.in
فرانسه	١٧٨.٣٣.٢٣٣.٢٠٢	www.poketeg.com
بلغارستان	١٤٦.٦٦.٧٢.٨٧	www.perfectfunnelblueprint.com

www.n۲plus.co.th	۲۰۲.۴۳.۴۵.۱۸۱	تایلند
www.mimid.cz	۱۷۸.۲۳۸.۳۷.۱۶۲	جمهوری چک
www.macartegrise.eu	--	
www.lagouttedelixir.com	۵۱.۶۸.۵۰.۱۶۸	انگلستان
www.krishnagrp.com	۱۸۴.۱۶۸.۲۲۱.۹۴	آمریکا
www.ismcrossconnect.com	۲۱۳.۱۸۶.۳۳.۱۸۶	فرانسه
www.himmerlandgolf.dk	۹۴.۲۳۱.۱۰۹.۲۳۹	دانمارک
www.groupwine.fr	۸۷.۹۸.۱۵۴.۱۴۶	فرانسه
www.fabbfoundation.gm	--	--
www.cakav.hu	۸۰.۷۷.۱۲۳.۲۳	مجارستان
www.billerimpex.com	۲۱۷.۱۶۰.۰.۲۳۴	آلمان
wpakademi.com	۵۰.۸۷.۵۸.۱۶۵	آمریکا
vjccons.com.vn	۱۷۱.۲۴۴.۳۴.۱۶۷	ویتنام
unnatimotors.in	۱۰۳.۱۰۷.۱۷.۱۰۲	هند
topstockexpert.su	--	--
top-۲۲.ru	۸۷.۲۳۶.۱۹.۱۳۵	روسیه
tommarmores.com.br	۱۹۱.۲۵۲.۵۱.۳۷	برزیل
test.theveeview.com	۶۶.۹۶.۱۴۷.۶۷	آمریکا
smbardoli.org	۱۰۴.۲۷.۱۸۷.۱۱۳	آمریکا
simetribilisim.com	۹۴.۷۳.۱۴۸.۱۸	ترکیه
sherouk.com	۲۰۹.۱۸۲.۲۰۸.۲۴۵	آمریکا
royal.by	۹۳.۱۲۵.۹۹.۱۲۱	بلاروس
relectrica.com.mx	۶۷.۲۲۷.۲۳۶.۹۶	آمریکا
pp-panda۷۴.ru	۸۷.۲۳۶.۱۶.۲۹	روسیه
picusglancus.pl	۱۸۵.۱۳۵.۸۸.۱۰۵	لهستان
perovaphoto.ru	۹۲.۵۳.۹۶.۲۰۱	روسیه
ocsp.trust-provider.com	۱۷۸.۲۵۵.۸۳.۱	انگستان
ocsp.int-x۳.letsencrypt.org	۱۰۴.۸۶.۱۱۱.۱۷۶	آمریکا

ocsp.comodoca٤.com	٢.١٨.٦٦.١٩	محدوده اتحادیه اروپا
oceanlinen.com	٧٧.١٠٤.١٤٤.٢٥	بلغارستان
nesten.dk	١٠٤.٢٨.٣١.١٦٠	آمریکا
mrngreens.com	٤٥.٦٤.١٠٤.١٤٠	هند
mauricionacif.com	١٠٤.٢٨.٢٩.١٤٢	آمریکا
marketisleri.com	٨٩.٢٥٢.١٨٧.٧٢	ترکیه
lucides.co.uk	٢١٧.١٦٠.٠.٢٧	آلمان
krasnaypolyana١٢٣.ru	٩٥.٢١٣.١٧٣.١٧٣	روسیه
koloritplus.ru	٨٧.٢٣٦.١٦.٢٠٨	روسیه
isrg.trustid.ocsp.identrust.com	--	--
hoteltravel٢٠١٨.com	١٣٧.٧٤.٢٣٨.٣٣	فرانسه
hanaglobalholding.com	--	--
h٥s.vn	١٠٣.٢٧.٢٣٨.٣١	ویتنام
graftedinn.us	٤٥.٣٣.٩١.٧٩	آمریکا
goodapd.website		--
evotech.lu	٢١٣.١٨٦.٣٣.١٧	فرانسه
dna-cp.com	١٨٨.٦٤.١٨٤.٩٠	انگستان
diadelorgasmo.cl	١٩٢.١٦٣.٢٣٤.٤٠	آمریکا
devdev.com.br	١٨٦.٢٠٢.١٥٣.١٥٨	برزیل
cyclevegas.com	٧٠.٤٠.١٩٧.٩٦	آمریکا
cevent.net	١٧٣.٢٤٧.٢٤٢.١٣٣	آمریکا
boatshowradio.com	١٠٧.١٧٨.١١٣.١٦٢	آمریکا
blokefeed.club	١٠٤.٢٤.١٠٣.١٥٣	آمریکا
bloghalm.eu	٢١٧.١٧٤.١٤٩.١٣٠	بلغارستان
big-game-fishing-croatia.hr	١٠٤.٢٧.١٦٣.٢٤١	آمریکا
bethel.com.ve	١٠٤.٣١.٧٦.٩٥	آمریکا
bellytobabyphotographyseattle.com	--	--

aurumwedding.ru	--	--
asl-company.ru	۸۷.۲۳۶.۱۶.۳۱	روسیه
alem.be	۱۸۸.۱۶۵.۵۳.۱۸۵	فرانسه
acbt.fr	۲۱۳.۱۸۶.۳۳.۳	فرانسه
٦chen.cn	۲۲۳.۲٦.٦۲.۷۲	هنگ کنک

تصویر زیر مربوط به تعدادی از این آدرس‌ها می‌باشد:



میزبان‌هایی که باج‌افزار با آن‌ها ارتباط برقرار کرده است:

کشور	دامنه	نام پروتکل	شماره پورت	آدرس میزبان
آلمان	www.billerimpex.com	TCP	۸۰	۲۱۷.۱٦۰.۰.۲۳٤
آلمان	www.billerimpex.com	TCP	٤٤۳	۲۱۷.۱٦۰.۰.۲۳٤
--	--	TCP	۸۰	٥۲.۲۹.۱۹۲.۱۳٦
فرانسه	www.poketeg.com	TCP	۸۰	۱۷۸.۳۳.۲۳۳.۲۰۲
روسیه	perovaphoto.ru	TCP	۸۰	۹۲.٥۳.۹٦.۲۰۱

روسیه	asl-company.ru	TCP	۸۰	۸۷.۲۳۶.۱۶.۳۱
بلغارستان	www.perfectfunnelblueprint.com	TCP	۸۰	۱٤٦.٦٦.۷۲.۸۷
آمریکا	www.wash-wear.com	TCP	۸۰	٦۹.۷۳.۱۸۰.۱٥۱
روسیه	pp-panda۷٤.ru	TCP	۸۰	۸۷.۲۳٦.۱٦.۲۹
آمریکا	cevent.net	TCP	۸۰	۱۷۳.۲٤۷.۲٤۲.۱۳۳
فرانسه	alem.be	TCP	۸۰	۱۸۸.۱٦٥.٥۳.۱۸٥
آمریکا	boatshowradio.com	TCP	۸۰	۱۰۷.۱۷۸.۱۱۳.۱٦۲
آمریکا	boatshowradio.com	TCP	٤٤۳	۱۰۷.۱۷۸.۱۱۳.۱٦۲
انگستان	dna-cp.com	TCP	۸۰	۱۸۸.٦٤.۱۸٤.۹۰
فرانسه	acbt.fr	TCP	۸۰	۲۱۳.۱۸٦.۳۳.۳
آمریکا	wpakademi.com	TCP	۸۰	٥۰.۸۷.٥۸.۱٦٥
مجارستان	www.cakav.hu	TCP	۸۰	۸۰.۷۷.۱۲۳.۲۳
جمهوری چک	www.mimid.cz	TCP	۸۰	۱۷۸.۲۳۸.۳۷.۱٦۲
هنگ کنگ	٦chen.cn	TCP	۸۰	۲۲۳.۲٦.٦۲.۷۲
بلغارستان	oceanlinen.com	TCP	۸۰	۷۷.۱۰٤.۱٤٤.۲٥
برزیل	tommarmores.com.br	TCP	۸۰	۱۹۱.۲٥۲.٥۱.۳۷
آمریکا	nesten.dk	TCP	۸۰	۱۰٤.۲۸.۳۱.۱٦۰
تایلند	www.n۲plus.co.th	TCP	۸۰	۲۰۲.٤۳.٤٥.۱۸۱
روسیه	koloritplus.ru	TCP	۸۰	۸۷.۲۳٦.۱٦.۲۰۸
ویتنام	h٥s.vn	TCP	۸۰	۱۰۳.۲۷.۲۳۸.۳۱
ترکیه	marketisleri.com	TCP	۸۰	۸۹.۲٥۲.۱۸۷.۷۲
ترکیه	marketisleri.com	TCP	٤٤۳	۸۹.۲٥۲.۱۸۷.۷۲
برزیل	www.toflyaviacao.com.br	TCP	۸۰	۱۷۹.۱۸۸.۱۱.۳٤
آمریکا	www.rment.in	TCP	۸۰	۱۰٤.۲٤.۱۰٤.۱۳
انگلستان	www.lagouttedelixir.com	TCP	۸۰	٥۱.٦۸.٥۰.۱٦۸
آمریکا	www.krishnagrp.com	TCP	۸۰	۱۸٤.۱٦۸.۲۲۱.۹٤
آمریکا	www.krishnagrp.com	TCP	٤٤۳	۱۸٤.۱٦۸.۲۲۱.۹٤
آمریکا	big-game-fishing-croatia.hr	TCP	۸۰	۱۰٤.۲۷.۱٦۳.۲٤۱

آمریکا	big-game-fishing-croatia.hr	TCP	٤٤٣	١٠٤.٢٧.١٦٣.٢٤١
انگلستان	ocsp.trust-provider.com	TCP	٨٠	١٧٨.٢٥٥.٨٣.١
محدوده اتحادیه اروپا	ocsp.comodoca٤.com	TCP	٨٠	٢.١٨.٦٦.١٩
آمریکا	mauricionacif.com	TCP	٨٠	١٠٤.٢٨.٢٩.١٤٢
فرانسه	www.ismcrossconnect.com	TCP	٨٠	٢١٣.١٨٦.٣٣.١٨٦
آمریکا	test.theveeview.com	TCP	٨٠	٦٦.٩٦.١٤٧.٦٧
آمریکا	relectrica.com.mx	TCP	٨٠	٦٧.٢٢٧.٢٣٦.٩٦
آمریکا	relectrica.com.mx	TCP	٤٤٣	٦٧.٢٢٧.٢٣٦.٩٦
آمریکا	bethel.com.ve	TCP	٨٠	١٠٤.٣١.٧٦.٩٥
آمریکا	bethel.com.ve	TCP	٤٤٣	١٠٤.٣١.٧٦.٩٥
ویتنام	vjccons.com.vn	TCP	٨٠	١٧١.٢٤٤.٣٤.١٦٧
بلغارستان	bloghalm.eu	TCP	٨٠	٢١٧.١٧٤.١٤٩.١٣٠
آمریکا	cyclevegas.com	TCP	٨٠	٧٠.٤٠.١٩٧.٩٦
بلاروس	royal.by	TCP	٨٠	٩٣.١٢٥.٩٩.١٢١
بلاروس	royal.by	TCP	٤٤٣	٩٣.١٢٥.٩٩.١٢١
دانمارک	www.himmerlandgolf.dk	TCP	٨٠	٩٤.٢٣١.١٠٩.٢٣٩
دانمارک	www.himmerlandgolf.dk	TCP	٤٤٣	٩٤.٢٣١.١٠٩.٢٣٩
فرانسه	hoteltravel٢٠١٨.com	TCP	٨٠	١٣٧.٧٤.٢٣٨.٣٣
هلند	picusglancus.pl	TCP	٨٠	١٨٥.١٣٥.٨٨.١٠٥
هند	unnatimotors.in	TCP	٨٠	١٠٣.١٠٧.١٧.١٠٢
هند	unnatimotors.in	TCP	٤٤٣	١٠٣.١٠٧.١٧.١٠٢
روسیه	krasnaypolyana١٢٣.ru	TCP	٨٠	٩٥.٢١٣.١٧٣.١٧٣
آمریکا	smbardoli.org	TCP	٨٠	١٠٤.٢٧.١٨٧.١١٣
آمریکا	blokefeed.club	TCP	٨٠	١٠٤.٢٤.١٠٣.١٥٣
فرانسه	evotech.lu	TCP	٨٠	٢١٣.١٨٦.٣٣.١٧
برزیل	devdev.com.br	TCP	٨٠	١٨٦.٢٠٢.١٥٣.١٥٨
برزیل	devdev.com.br	TCP	٤٤٣	١٨٦.٢٠٢.١٥٣.١٥٨

آمریکا	graftedinn.us	TCP	۸۰	٤٥.۳۳.۹۱.۷۹
روسیه	top-۲۲.ru	TCP	۸۰	۸۷.۲۳٦.۱۹.۱۳٥
ترکیه	simetribilisim.com	TCP	۸۰	۹٤.۷۳.۱٤۸.۱۸
آمریکا	sherouk.com	TCP	۸۰	۲۰۹.۱۸۲.۲۰۸.۲٤٥
آلمان	lucides.co.uk	TCP	۸۰	۲۱۷.۱٦۰.۰.۲۷
آمریکا	diadelorgasmo.cl	TCP	۸۰	۱۹۲.۱٦۳.۲۳٤.٤۰
آمریکا	diadelorgasmo.cl	TCP	٤٤۳	۱۹۲.۱٦۳.۲۳٤.٤۰
فرانسه	www.groupwine.fr	TCP	۸۰	۸۷.۹۸.۱٥٤.۱٤٦
هند	mrngreens.com	TCP	۸۰	٤٥.٦٤.۱۰٤.۱٤۰

خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد ٤۳ مورد از ٦۷ 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.GandCrab4.8CBC6992	ALYac	Generic.Ransom.GandCrab4.8CBC6992
Antiy-AVL	Trojan[Ransom]/Win32.GandCrab	Arcabit	Generic.Ransom.GandCrab4.8CBC6992
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/FileCoder.evrob	BitDefender	Generic.Ransom.GandCrab4.8CBC6992
ClamAV	Win.Ransomware.Gandcrab-6667060-0	CrowdStrike Falcon	malicious_confidence_100% (D)
Cybereason	malicious.37561c	Cylance	Unsafe
Cyren	W32/Trojan.UERA-7181	Emsisoft	Generic.Ransom.GandCrab4.8CBC6992 (B)
Endgame	malicious (high confidence)	eScan	Generic.Ransom.GandCrab4.8CBC6992
ESET-NOD32	a variant of Win32/Filecoder.GandCrab.D	F-Secure	Generic.Ransom.GandCrab4.8CBC6992
Fortinet	W32/Filecoder_GandCrab.D!tr	GData	Generic.Ransom.GandCrab4.8CBC6992
Ikarus	Trojan-Ransom.GandCrab	K7AntiVirus	Trojan (00536a1e1)
K7GW	Trojan (00536a1e1)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Ransom.GandCrab	MAX	malware (ai score=100)
McAfee	Ran-GandCrabv4!07FADB006486	McAfee-GW-Edition	BehavesLike.Win32.Generic.ch
NANO-Antivirus	Trojan.Win32.Filecoder.fifjpt	Palo Alto Networks	generic.ml
Panda	Generic Suspicious	Qihoo-360	HEUR/QVM20.1.13E4.Malware.Gen
Rising	Ransom.GandCrab!8.F355 (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	ML.Attribute.HighConfidence	Tencent	Win32.Trojan.Filecoder.Ija
TrendMicro	Ransom_GANDCRAB.THOIBEAH	TrendMicro-HouseCall	Ransom_GANDCRAB.THOIBEAH
VBA32	BScope.TrojanRansom.Cryptor	Webroot	W32.Trojan.Gen
ZoneAlarm	HEUR:Trojan.Win32.Generic		

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر از ۱۱ مورد آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو،٤ مورد قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن
d77378dcc42b912e514d3bd4466cdda050dda9b57799a6c97f70e8489dd8c8d0.exe

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.15.0	✔	Clean
f_secure	11.00	ii	Dangerous: Generic.Ransom.GandCrab4.8CBC6992
kaspersky	5.5	i	Suspicious: HEUR:Trojan.Win32.Generic
eset	4.5.3.38826	ii	Dangerous: Win32/Filecoder.GandCrab.D
drweb	11.0.1.1607061217	✔	Clean
clam_av	0.99.2	ii	Dangerous: Win.Ransomware.Gandcrab-6667060-0
comodo	1.1.268025.1	✔	Clean
bitdefender	11.0.1.18	ii	Dangerous: Generic.Ransom.GandCrab4.8CBC6992
avast	2.1.2	✔	Clean
symantec	7.9.0.30	i	Suspicious: Heur.AdvML.B