باسمه تعالی

تحلیل فنی باج‌افزار

MegaCortex

تاریخ نگارش :

۱۳۹۸/۰۵/۲۹

فهرست مطالب

۱. مقدمه :

باج‌افزارMegacortex برای اولین بار در اوایل ماه مه سال ۲۰۱۹ میلادی مشاهده گردید. این باج‌افزار در همان ابتدای فعالیت خود به سبب حملات گسترده به شبکه‌های سازمان‌ها و کسب و کارها در کشورهای آمریکا، کانادا و بخش غربی قاره اروپا، توجه محققان سایبری را به خود جلب کرد. براساس مشاهدات صورت گرفته، اولین نسخه این باج‌افزار تا ۶۰۰ بیت‌کوین هم درخواست باج می‌دهد که مبلغ قابل توجهی می‌باشد. این باج‌افزار از الگوریتم AES و RSA جهت رمزگذاری فایل‌های سیستم قربانی استفاده می‌کند و پسوند megac0rtx. را به انتهای فایل‌های رمزگذاری شده اضافه می‌نماید. تحلیل پیش رو مربوط به نسخه دوم این باج‌افزار می‌باشد. این نسخه در تاریخ ۲۳ ژوئیه سال جاری میلادی منتشر گردیده است.

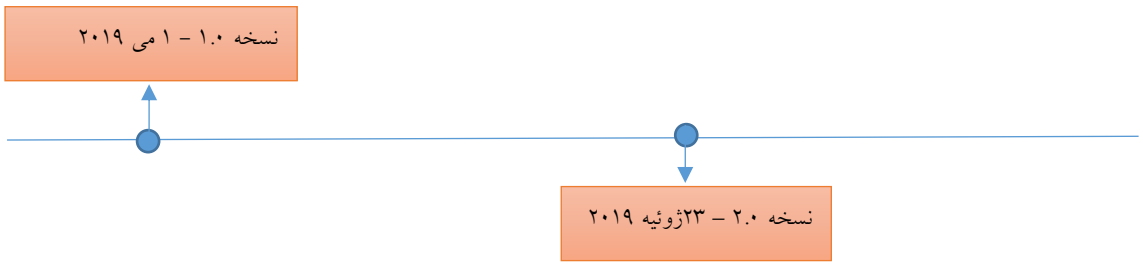
۲. مشخصات فایل اجرایی :

نام فایل	RAND_NAME winnit.exe
MD5	1ef7bfccbd7b044de5680b7e06d2d2a3
SHA-1	8374a845cbb9c13091fb741a119215dc6a5913fb
SHA-256	ea68d92fe813198bf2542ead1b63b943b629fd17f7a625e0a2483ce63121d0fd
نوع فایل	Win32 EXE
اندازه فایل	۹٤٤.٥ کیلوبایت

فایل اجرایی این باج‌افزار دارای ۵ بخش است :

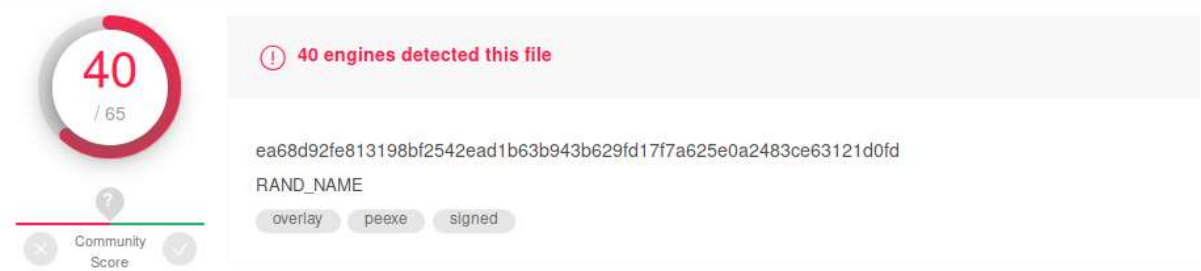
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٦٣	١٣٩٥٢٥	٤٠٩٦	١٣٩٧٧٦
.rdata	٧.٩٣	٨٠٨٠٤٦	١٤٧٤٥٦	٨٠٨٤٤٨
.data	٣.١	٧٥٠٤	٩٥٨٤٦٤	٤٠٩٦
.rsrc	٣.٧٢	١٢٧٢	٩٦٦٦٥٦	١٥٣٦
.reloc	٦.٤٨	٨٨٢٠	٩٧٠٧٥٢	٩٢١٦

۳. شجره‌نامه



٤. میزان تهدید فایل باج‌افزار

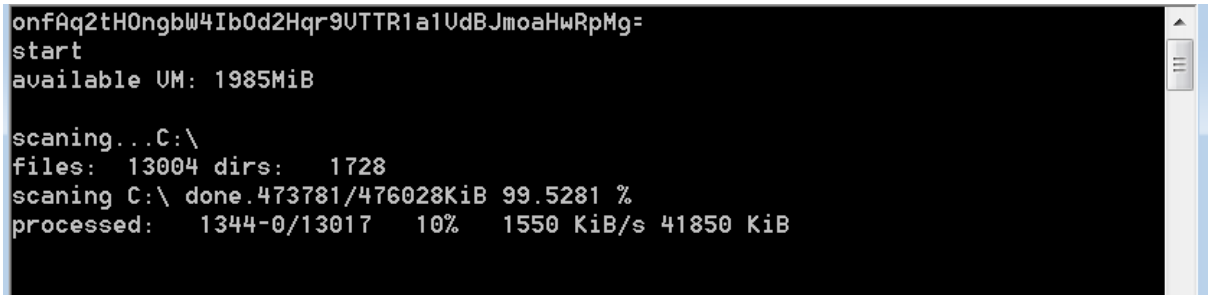
درحال حاضر تعداد ٤٠ مورد از ٦٥ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



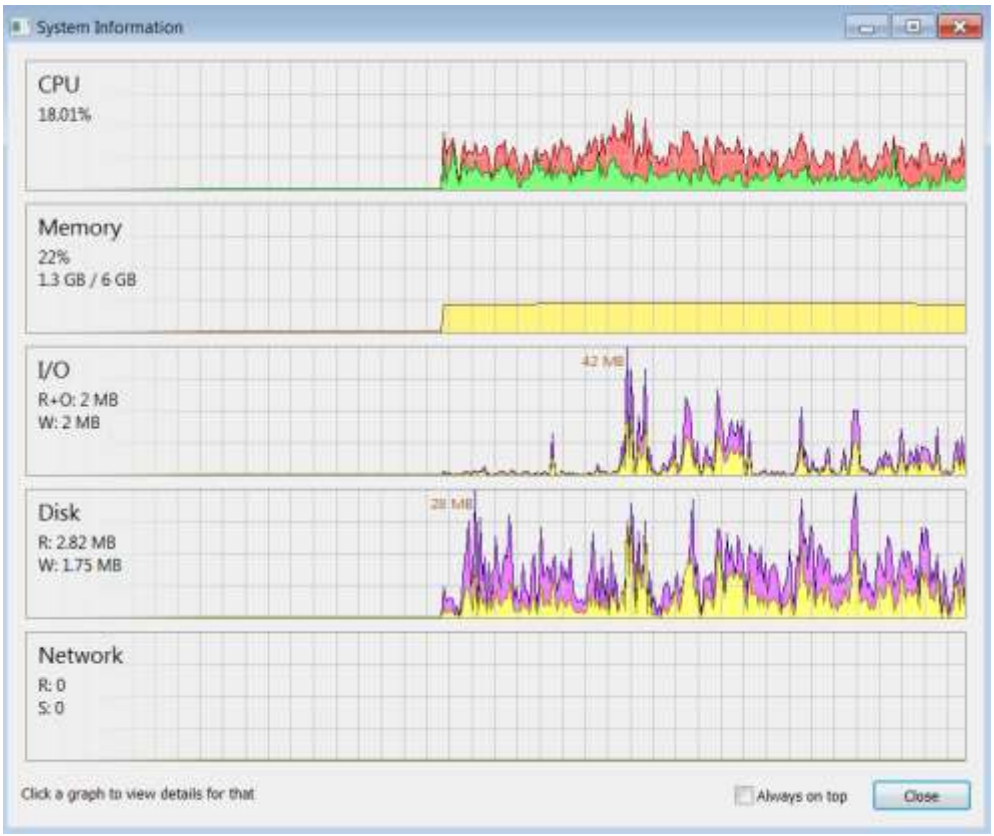
٥. تحلیل پویا

٥-١ آناتومی حمله

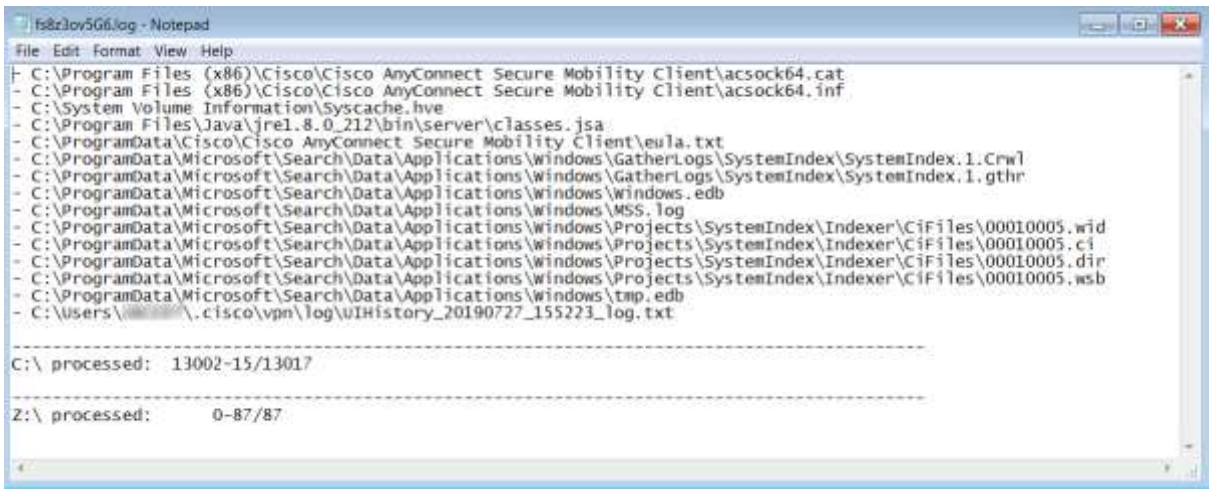
طبق بررسی‌های صورت گرفته، باج‌افزار MegaCortex به محض شروع فعالیت در سیستم قربانی تمام دایرکتوری‌ها را اسکن نموده و سپس شروع به رمزگذاری فایل‌ها می‌نماید. فرآیند رمزنگاری بسته به منابع سیستم قربانی، بین ٥ الی ١٠ دقیقه طول می‌کشد.



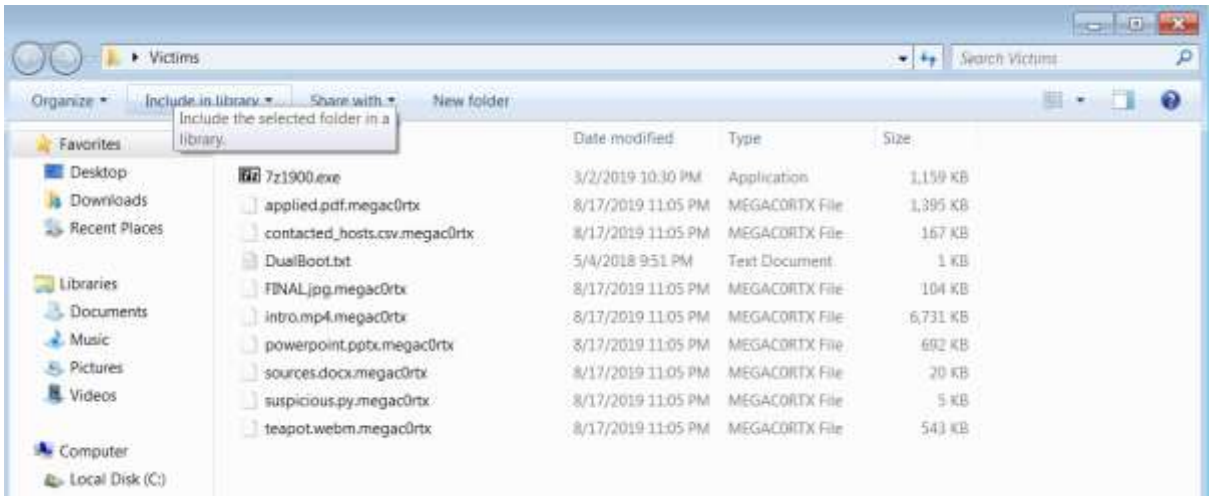
باج‌افزار با بهره‌گیری از منابع سیستم قربانی (CPU، Disk و I/O) فرآیند رمزنگاری را تکمیل می‌کند. همانطور که مشاهده می‌کنید حافظه RAM در یک مقدار ثابت باقی مانده است. بنابراین هرچه توان پردازشی پردازنده سیستم قربانی بالاتر بوده و سرعت خواندن/نوشتن دیسک نیز بیشتر باشد، رمزگذاری نیز سریعتر اتفاق می‌افتد.



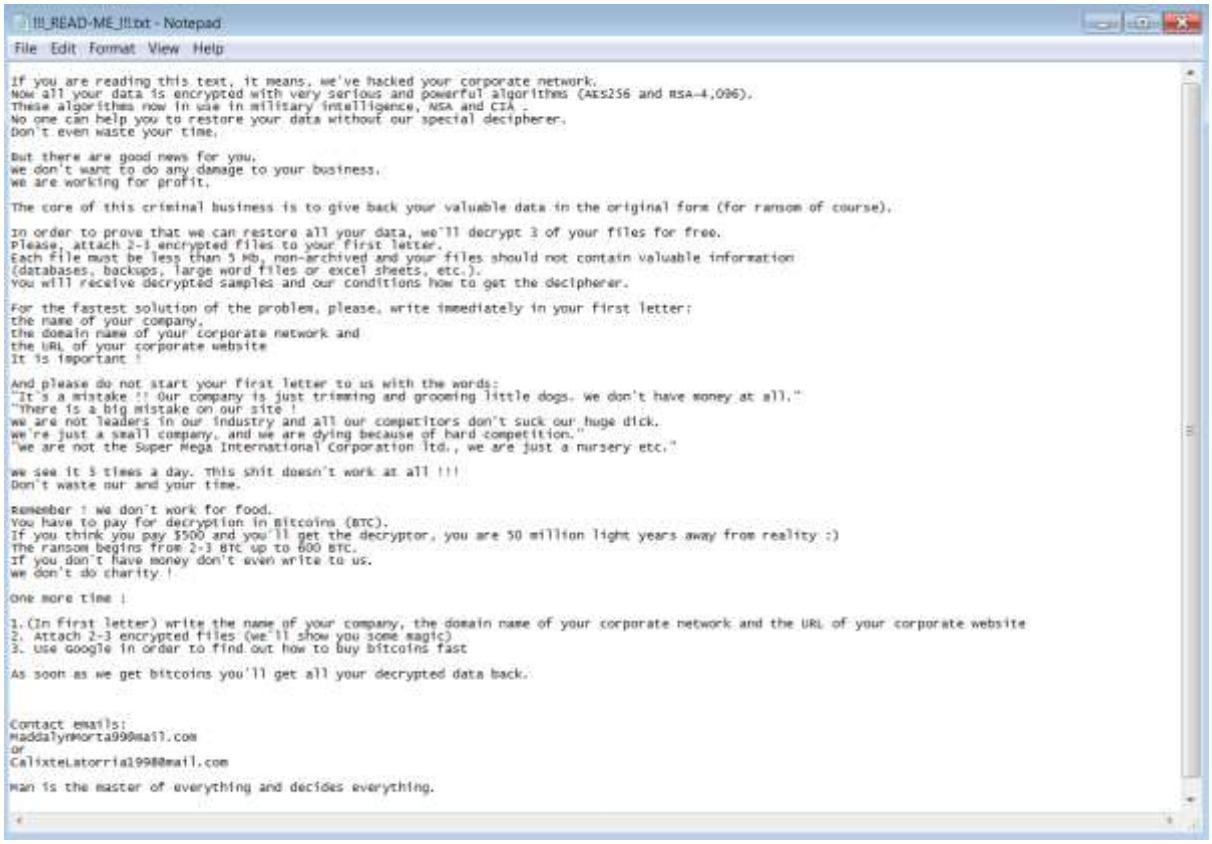
در طول فرآیند رمزنگاری، فایلی با ترکیب xxxxxxxxxx.log نیز در مسیر ریشه درایو اصلی سیستم‌عامل قربانی ایجاد می‌گردد که حاوی لیست فایل‌هایی است که باج‌افزار موفق به رمزگذاری آن‌ها نشده است. محتوای این فایل همزمان با فرآیند رمزنگاری، تکمیل شده و در پایان، تعداد نهایی فایل‌های باقیمانده قابل مشاهده است.



پس از اتمام فرآیند رمزنگاری، پسوند megac0rtx. به انتهای فایل‌های رمزگذاری شده اضافه می‌شود که در تصویر زیر نشان داده شده است. باج‌افزار MegaCortex فایل‌های با پسوند exe. را به دلیل اینکه در لیست سفید باج‌افزار قرار دارد، رمزگذاری نمی‌کند. فایل DualBoot.txt نیز همانطور که در تصویر می‌بینید به دلیل حجم پایین (1KB) رمزگذاری نشده است.



پیغام باج‌خواهی باج‌افزار MegaCortex نیز با نام !!!_READ-ME_!!!.txt بر روی دسکتاپ قرار می‌گیرد که محتوای آن در تصویر زیر قابل مشاهده است.



همانطور که در پیغام باج‌خواهی این باج‌افزار مشخص است، ابتدا به قربانی اطلاع داده شده که تمام فایل‌های موجود در سیستم وی با الگوریتم‌های رمزنگاری AES-256 و RSA-4096 رمزگذاری شده است و تنها راه بازیابی آن‌ها، انجام دستورالعمل‌های ارایه شده در پیغام باج‌خواهی می‌باشد. سپس عنوان شده است که جهت اعتماد و تضمین رمزگشایی فایل‌ها، قربانی می‌تواند تعداد ۳ فایل غیر فشرده و کم‌اهمیت با حجم کمتر از ۵ مگابایت را از طریق ایمیل‌های اشاره شده در متن پیغام برای مهاجم ارسال نموده و نسخه رمزگشایی شده آن‌ها را دریافت نماید. مهاجم در این پیغام رقم متغیر ۳-۲ بیت‌کوین الی ۶۰۰ بیت‌کوین را برای مبلغ باج در نظر گرفته است.

۵-۲ روش انتشار:

همانطور که در بخش مقدمه اشاره شد بنا به گزارش وب‌سایت Bleepingcomputer و به نقل از آزمایشگاه Sophos، در همان ابتدا حملاتی از این باج‌افزار در کشورهای آمریکا، ایتالیا، کانادا، فرانسه، هلند و ایرلند مشاهده شده گردید. محققان این آزمایشگاه‌ها، تروجان‌های Emotet و Qbot را نیز در شبکه‌های آلوده شده به این باج‌افزار مشاهده کرده‌اند اما ارتباط مستقیم این باج‌افزار و انتشار آن توسط این تروجان‌ها را تأیید نکرده‌اند. طبق گزارش قربانیان این باج‌افزار، حملات اصلی بر روی DC (Domain Controller)های دارای آسیب‌پذیری و در معرض خطر انجام شده است.

بر اساس گزارشات بدست آمده، مکانیزم حمله به این صورت است که نرم‌افزاری به نام Cobolt Strike در سرور DC بارگذاری و اجرا می‌شود تا یک Reverse Shell ایجاد کند که این Shell به سیستم مهاجم بازگرداننده می‌شود. سپس مهاجم از طریق این Shell و از راه دور به سرور DC دسترسی پیدا کرده و آن را به گونه‌ای پیکربندی می‌کند که یک کپی از ابزار PsExec، فایل اصلی قابل اجرای باج‌افزار و یک فایل دسته‌ای (batch file) ایجاد و در شبکه توزیع نماید. پس از طی این مراحل، فایل اصلی باج‌افزار توسط فایل دسته‌ای مذکور اجرا می‌شود. طبق اظهارنظر Andrew Brandt محقق آزمایشگاه Sophos، فایل اجرایی باج‌افزار پس از اجرا یک فایل DLL با نام تصادفی درون سیستم قربانی ایجاد می‌کند و سپس این فایل توسط فرآیند rundll32.exe اجرا می‌شود. در واقع، بخش اصلی در رمزگذاری فایل‌های سیستم قربانی همین فایل DLL می‌باشد.

۵-۳ روش جلوگیری:

با توجه به روش‌های نفوذ و انتشار این باج‌افزار، اکیداً توصیه می‌کنیم که سیستم‌عامل‌های خود، مخصوصاً نسخه‌های نصب بر روی سرورها را با وصله‌های امنیتی ارایه شده، به روز رسانی کنید.

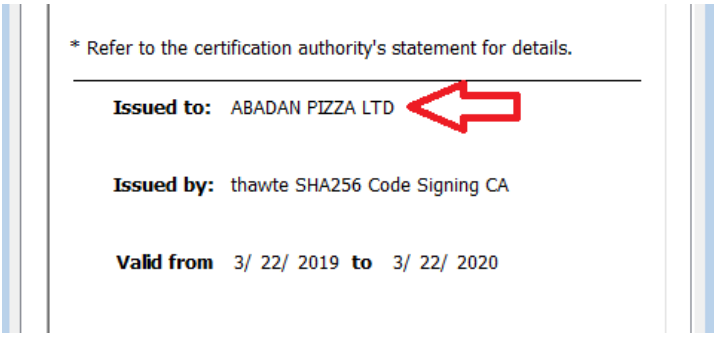
همچنین توصیه می‌شود اقدامات مربوط به امن‌سازی سرویس‌های مایکروسافتی از جمله Active Directory و پروتکل RDP را به طور کامل بر روی سیستم‌های خود انجام دهید و نرم‌افزارهای امنیتی نصب شده درون سیستم عامل خود نظیر آنتی ویروس را، به طور مداوم به روز رسانی کنید.

٦. تحلیل ایستا

٦-١ تحلیل کد

پس از بررسی کد فایل اجرایی باج‌افزار نتایج زیر حاصل گردید. آنتروپی بالای (٧.٨٤) نمونه فایل تحلیل شده در آزمایشگاه نشان می‌دهد که در کدنویسی این باج‌افزار به شدت از تکنیک‌های مبهم‌سازی (Obfuscation) استفاده شده است.

طبق بررسی‌های صورت گرفته، فایل تحلیل‌شده در آزمایشگاه، توسط گواهی (CA) یک شرکت بریتانیایی به نام ABADAN PIZZA LTD امضا (Sign) شده است. از این تکنیک معمولاً برای دور زدن سیستم‌عامل یا آنتی‌ویروس‌ها استفاده می‌شود.



فایل اجرایی از تابع DllEntryPoint شروع می‌شود.

```
.text:1004CB6D DllEntryPoint   proc near
.text:1004CB6D
.text:1004CB6D hinstDLL        = dword ptr  8
.text:1004CB6D fdwReason       = dword ptr  0Ch
.text:1004CB6D lpReserved      = dword ptr  10h
.text:1004CB6D
.text:1004CB6D                 push    ebp
.text:1004CB6E                 mov     ebp, esp
.text:1004CB70                 cmp     [ebp+fdwReason], 1
.text:1004CB74                 jnz     short loc_1004CB7B
.text:1004CB76                 call    sub_1004D376
.text:1004CB7B
.text:1004CB7B loc_1004CB7B:                           ; CODE XREF: DllEntryPoint+7↑j
.text:1004CB7B                 push    [ebp+lpReserved]
.text:1004CB7E                 push    [ebp+fdwReason]
.text:1004CB81                 push    [ebp+hinstDLL]
.text:1004CB84                 call    sub_1004CA3C
.text:1004CB89                 add     esp, 0Ch
.text:1004CB8C                 pop     ebp
.text:1004CB8D                 retn    0Ch
.text:1004CB8D DllEntryPoint   endp
.text:1004CB8D
```

با استفاده از تابع OpenSCManager امکان دسترسی به پایگاه داده سرویس‌های ویندوزی برای باج‌افزار فراهم می‌شود.

```
push    ebp
mov     ebp, esp
push    0FFFFFFFFh
push    offset sub_10085DE0
mov     eax, large fs:0
push    eax
sub     esp, 4Ch
push    ebx
push    esi
push    edi
mov     eax, ___security_cookie
xor     eax, ebp
push    eax
lea     eax, [ebp+var_C]
mov     large fs:0, eax
lea     ecx, [ebp+var_58]
call    sub_1002BF10
push    0F003Fh             ; dwDesiredAccess
push    0                   ; lpDatabaseName
push    0                   ; lpMachineName
mov     [ebp+var_4], 0
call    ds:OpenSCManagerA
mov     ebx, eax
cmp     ebx, 0FFFFFFFFh
jnz     short loc_1002C456
```

سپس، با استفاده ازتابع EnumServicesStatusExA لیستی از این سرویس‌ها تهیه می‌شود.

```
loc_1002C456:
mov     esi, ds:EnumServicesStatusExA
lea     eax, [ebp+ServicesReturned]
push    0               ; pszGroupName
push    0               ; lpResumeHandle
push    eax             ; lpServicesReturned
lea     eax, [ebp+pcbBytesNeeded]
push    eax             ; pcbBytesNeeded
push    0               ; cbBufSize
push    0               ; lpServices
push    3               ; dwServiceState
push    30h             ; dwServiceType
push    0               ; InfoLevel
push    ebx             ; hSCManager
call    esi ; EnumServicesStatusExA
lea     eax, [ebp+var_D]
push    eax
push    [ebp+pcbBytesNeeded]
lea     ecx, [ebp+lpServices]
call    sub_1002BFA0
mov     edi, [ebp+lpServices]
lea     eax, [ebp+ServicesReturned]
push    0               ; pszGroupName
push    0               ; lpResumeHandle
push    eax             ; lpServicesReturned
lea     eax, [ebp+pcbBytesNeeded]
mov     byte ptr [ebp+var_4], 1
push    eax             ; pcbBytesNeeded
push    [ebp+pcbBytesNeeded] ; cbBufSize
push    edi             ; lpServices
push    3               ; dwServiceState
push    30h             ; dwServiceType
push    0               ; InfoLevel
push    ebx             ; hSCManager
call    esi ; EnumServicesStatusExA
cmp     [ebp+ServicesReturned], 0
mov     [ebp+var_1C], 0
jbe     short loc_1002C513
```

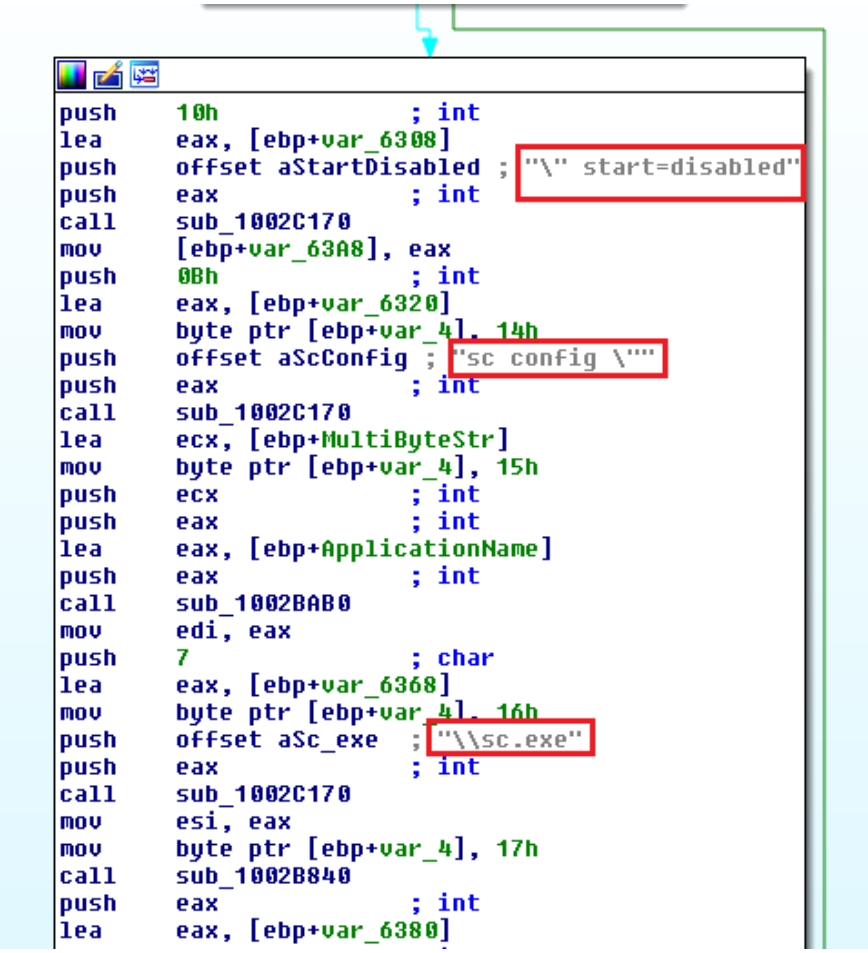
این فرآیند در ابتدای فعالیت فایل باج‌افزار درون سیستم‌عامل قربانی صورت می‌گیرد. علت استفاده از این فرآیند و دسترسی به سرویس‌های درون سیستم‌عامل در واقع غیرفعال نمودن تعدادی از سرویس‌ها می‌باشد که درون کد باج‌افزار تعبیه شده‌اند.

```
mov     [ebp+var_7C], 0Dh
mov     [ebp+var_78], offset aNetsvc ; "NetSvc"
mov     [ebp+var_74], 6
mov     [ebp+var_70], offset aSqlagentNet2 ; "SQLAgent$NET2"
mov     [ebp+var_6C], 0Dh
mov     [ebp+var_68], offset aTpautoconnsvc ; "tpautoconnsvc"
mov     [ebp+var_64], 0Dh
mov     [ebp+var_60], offset aTpvcgateway ; "TPVCGateway"
mov     [ebp+var_5C], 0Bh
mov     [ebp+var_58], offset aVmwarecafcomma ; "VMwareCAFCommAmqpListener"
mov     [ebp+var_54], 19h
mov     [ebp+var_50], offset aVmwarecafmanag ; "VMwareCAFManagementAgentHost"
mov     [ebp+var_4C], 1Ch
mov     [ebp+var_48], offset aTpautoconnsv_0 ; "TPAutoConnSvc"
mov     [ebp+var_44], 0Dh
mov     [ebp+var_40], offset aAdobearmservic ; "AdobeARMservice"
mov     [ebp+var_3C], 0Fh
mov     [ebp+var_38], offset aRscdsvc ; "RSCDsvc"
mov     [ebp+var_34], 7
mov     [ebp+var_30], offset aLrsdrvx ; "LRSDRVX"
mov     [ebp+var_2C], 7
mov     [ebp+var_28], offset aMsvsmon90 ; "msvsmon90"
mov     [ebp+var_24], 9
mov     [ebp+var_20], offset aIdrivert ; "IDriverT"
lea     eax, [ebp+var_8F8]
mov     [ebp+var_1C], 8
mov     [ebp+var_18], offset aMsmq ; "MSMQ "
mov     [ebp+var_14], 5
mov     [ebp+hModule], eax
```

تصویر بالا، بخشی از سرویس‌هایی را نشان می‌دهد که درون کد باج‌افزار تعبیه شده‌اند. این لیست شامل ۲۲۲ سرویس می‌باشد که در صورت وجود باید متوقف و غیرفعال شوند و در بین آن‌ها سرویس‌های مربوط به برخی از آنتی‌ویروس‌های معروف نیز یافت می‌شود. لیست مشخص شده دوبار درون کد فراخوانی شده است که ابتدا با اجرای ابزار net.exe در محیط خط فرمان ویندوز و به کمک دستور زیر تمام سرویس‌های فعال موجود در این لیست، متوقف می‌شوند.

net stop "Serveice_Name" /y

سپس، با اجرای دستور sc config "نام سرویس" start= disabled در محیط خط فرمان فرآیند ویندوزی sc.exe غیرفعال می‌شود.



```
push    10h             ; int
lea     eax, [ebp+var_6308]
push    offset aStartDisabled ; "\" start=disabled"
push    eax             ; int
call    sub_1002C170
mov     [ebp+var_63A8], eax
push    0Bh             ; int
lea     eax, [ebp+var_6320]
mov     byte ptr [ebp+var_4], 14h
push    offset aScConfig ; "sc config \""
push    eax             ; int
call    sub_1002C170
lea     ecx, [ebp+MultiByteStr]
mov     byte ptr [ebp+var_4], 15h
push    ecx             ; int
push    eax             ; int
lea     eax, [ebp+ApplicationName]
push    eax             ; int
call    sub_1002BAB0
mov     edi, eax
push    7               ; char
lea     eax, [ebp+var_6368]
mov     byte ptr [ebp+var_4], 16h
push    offset aSc_exe  ; "\\sc.exe"
push    eax             ; int
call    sub_1002C170
mov     esi, eax
mov     byte ptr [ebp+var_4], 17h
call    sub_1002B840
push    eax             ; int
lea     eax, [ebp+var_6380]
```

در ادامه فرآیندهای جاری سیستم‌عامل نیز، همانند سرویس‌ها لیست می‌شوند.

```
EnumProcesses   proc near               ; CODE XREF: sub_1002C770+69↑p

lpidProcess     = dword ptr  4
cb              = dword ptr  8
lpcbNeeded      = dword ptr  0Ch

                jmp     ds:__imp_EnumProcesses
EnumProcesses   endp
```

همچنین، تمام ماژول‌هایی که مربوط به فرآیندهای اشاره شده نیز لیست می‌گردند.

```
EnumProcessModules proc near            ; CODE XREF: sub_1002C770+F8↑p

hProcess        = dword ptr  4
lphModule       = dword ptr  8
cb              = dword ptr  0Ch
lpcbNeeded      = dword ptr  10h

                jmp     ds:__imp_EnumProcessModules
EnumProcessModules endp
```

از لیست فرآیندهای جاری سیستم‌عامل آن دسته که در لیست تعریف شده در کد باج‌افزار قرار دارند، باید متوقف گردند.

```
[ebp+var_84], 0Ch
[ebp+var_80], offset aMsascui_exe ; "msascui.exe"
[ebp+var_7C], 0Bh
[ebp+var_78], offset aMsmpeng_exe ; "msmpeng.exe"
[ebp+var_74], 0Bh
[ebp+var_70], offset aMspmspsv_exe ; "mspmspsv.exe"
[ebp+var_6C], 0Ch
[ebp+var_68], offset aKb891711_exe ; "kb891711.exe"
[ebp+var_64], 0Ch
[ebp+var_60], offset aZavaux_exe ; "zavaux.exe"
[ebp+var_5C], 0Ah
[ebp+var_58], offset aZavcore_exe ; "zavcore.exe"
[ebp+var_54], 0Bh
[ebp+var_50], offset aZillya_exe ; "zillya.exe"
[ebp+var_4C], 0Ah
[ebp+var_48], offset aZlclient_exe ; "zlclient.exe"
[ebp+var_44], 0Ch
[ebp+var_40], offset aVsmon_exe ; "vsmon.exe"
[ebp+var_3C], 9
[ebp+var_38], offset aForcefield_exe ; "forcefield.exe"
[ebp+var_34], 0Eh
[ebp+var_30], offset aIswmgr_exe ; "iswmgr.exe"
[ebp+var_2C], 0Ah
[ebp+var_28], offset aZapro_exe ; "zapro.exe"
[ebp+var_24], 9
[ebp+var_20], offset aZonealarm_exe ; "zonealarm.exe"
[ebp+var_1C], 0Dh
[ebp+var_18], offset aMantispm_exe ; "mantispm.exe"
[ebp+var_14], 0Ch
[ebp+hModule], eax
```

تصویر بالا مربوط به بخشی از فرآیندهای تعریف شده در کد باج‌افزار می‌باشد. لیست کامل تعریف شده شامل ۱۱۱۷ فرآیند می‌باشد که همچون سرویس‌ها، فرآیندهایی مربوط به تعدادی از آنتی‌ویروس‌های سرشناس در این لیست قرار دارد. تمامی این فرآیندها با اجرای دستور زیر متوقف می‌شوند.

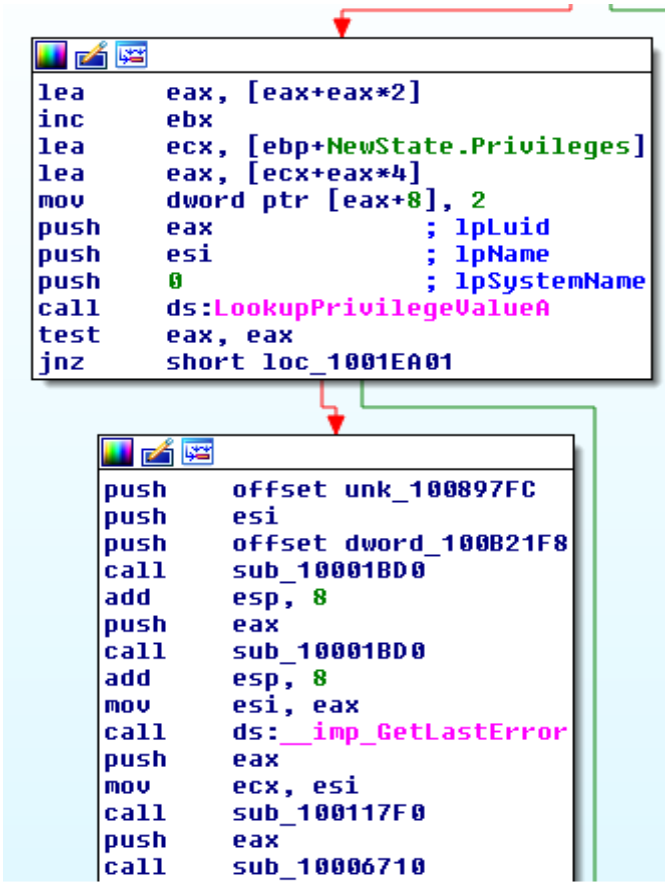
taskkill /IM / نام فایل اجرایی

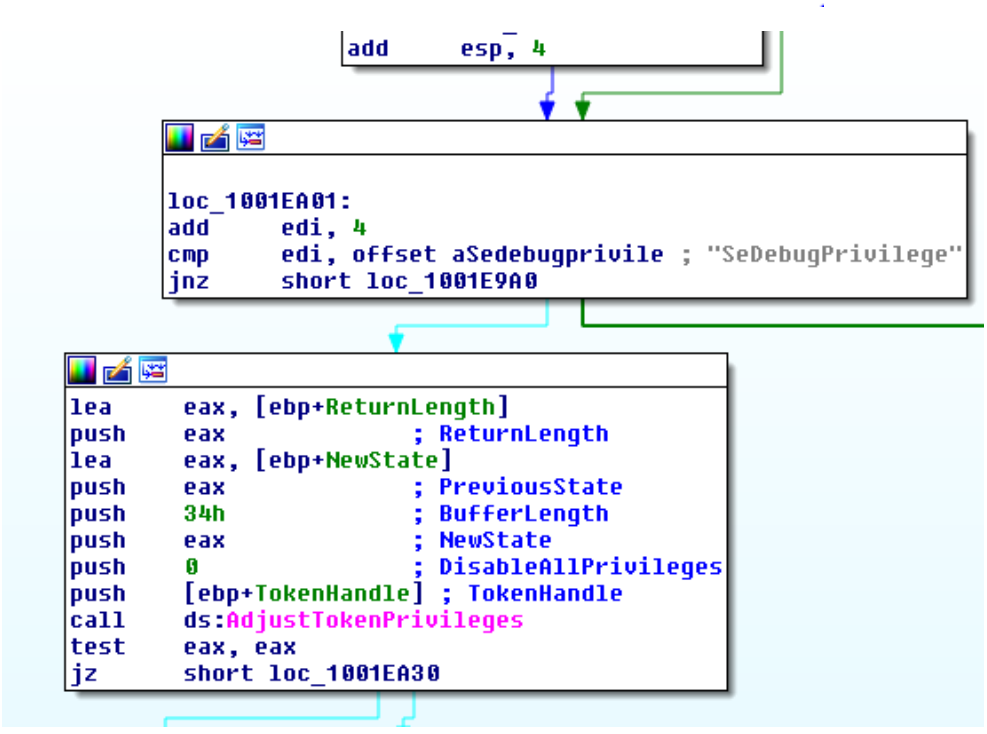
```
push    4
push    offset asc_1008E708 ; "\" /f"
lea     ecx, [ebp+var_6380]
mov     [ebp+var_6370], 0
mov     [ebp+var_636C], 0Fh
mov     [ebp+var_6380], 0
call    sub_1001C320
push    0Eh
push    offset aTaskkillIm ; "taskkill /im \""
lea     ecx, [ebp+lpMem]
mov     byte ptr [ebp+var_4], 4
mov     [ebp+var_6340], 0
mov     [ebp+var_633C], 0Fh
mov     byte ptr [ebp+lpMem], 0
call    sub_1001C320
cmp     [ebp+var_62F4], 10h
lea     eax, [ebp+var_6308]
push    [ebp+var_62F8]
cmovnb  eax, edi
mov     byte ptr [ebp+var_4], 5
push    eax
lea     ecx, [ebp+lpMem]
call    sub_1001BE10
mov     dword ptr [ebp+var_6310], 0
mov     dword ptr [ebp+var_6310+4], 0
movups  xmm0, xmmword ptr [eax]
movups  xmmword ptr [ebp+var_6320], xmm0
movq    xmm0, qword ptr [eax+10h]
movq    [ebp+var_6310], xmm0
mov     dword ptr [eax+10h], 0
mov     dword ptr [eax+14h], 0Fh
mov     byte ptr [eax], 0
push    0Dh
push    offset aTaskkill_exe ; "\\taskkill.exe"
lea     ecx, [ebp+var_6368]
```

با توقف و غیرفعال نمودن این موارد، باج‌افزار دیگر مانعی جهت ادامه‌ی فعالیت در سیستم قربانی ندارد. همانطور که در تحلیل پویا اشاره شد، این باج‌افزار از ابتدای شروع فعالیت خود و همزمان با اجرای مراحل ذکر شده فایلی با ترکیب xxxxxxxxxx.log را نیز، در مسیر درایو C ایجاد می‌کند. قطعه کد زیر مربوط به تولید این فایل می‌باشد.

```
loc_10002925:                           ; CODE XREF: sub_100026C0+205↑j
        test    al, 4
        jnz     loc_10002DCF
        or      eax, 4
        mov     dword_100AF9D4, eax
        push    11h
        push    offset aCFs8z3ov5g6_lo ; "C:\\fs8z3ov5G6.log"
        lea     ecx, [ebp+lpMem]
        mov     byte ptr [ebp+var_4], 4
        mov     [ebp+var_18], 0
        mov     [ebp+var_14], 0Fh
        mov     byte ptr [ebp+lpMem], 0
        call    sub_1001C320
        lea     eax, [ebp+lpMem]
        mov     byte ptr [ebp+var_4], 5
        push    eax             ; lpMultiByteStr
        lea     eax, [ebp+WideCharStr]
        push    eax             ; lpWideCharStr
        call    sub_1002B8B0
        add     esp, 8
        cmp     dword ptr [eax+14h], 8
        mov     ecx, [eax+10h]
        mov     byte ptr [ebp+var_4], 6
        jb      short loc_10002980
        mov     eax, [eax]
```

در ادامه چهار مجوز سیستمی نیز توسط باج‌افزار غیرفعال می‌شوند.





این مجوزها شامل مجوز عیب‌یابی، پشتیبان‌گیری، بازیابی و مالکیت سیستم‌عامل می‌شوند.

```
SeDebugPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeTakeOwnershipPrivilege
```

با اجرای دستور زیر از طریق فرآیند vssadmin.exe فضای VSS سیستم‌عامل نیز پاک می‌شود تا بازگردانی اطلاعات از دست رفته با مشکل روبرو گردد.

```
aVssadminDelete db 'vssadmin delete shadows /all /for=',0
                                        ; DATA XREF: sub_10029520+D3↑o
                align 4
aVssadmin_exe   db '\vssadmin.exe',0    ; DATA XREF: sub_10029520+64↑o
```

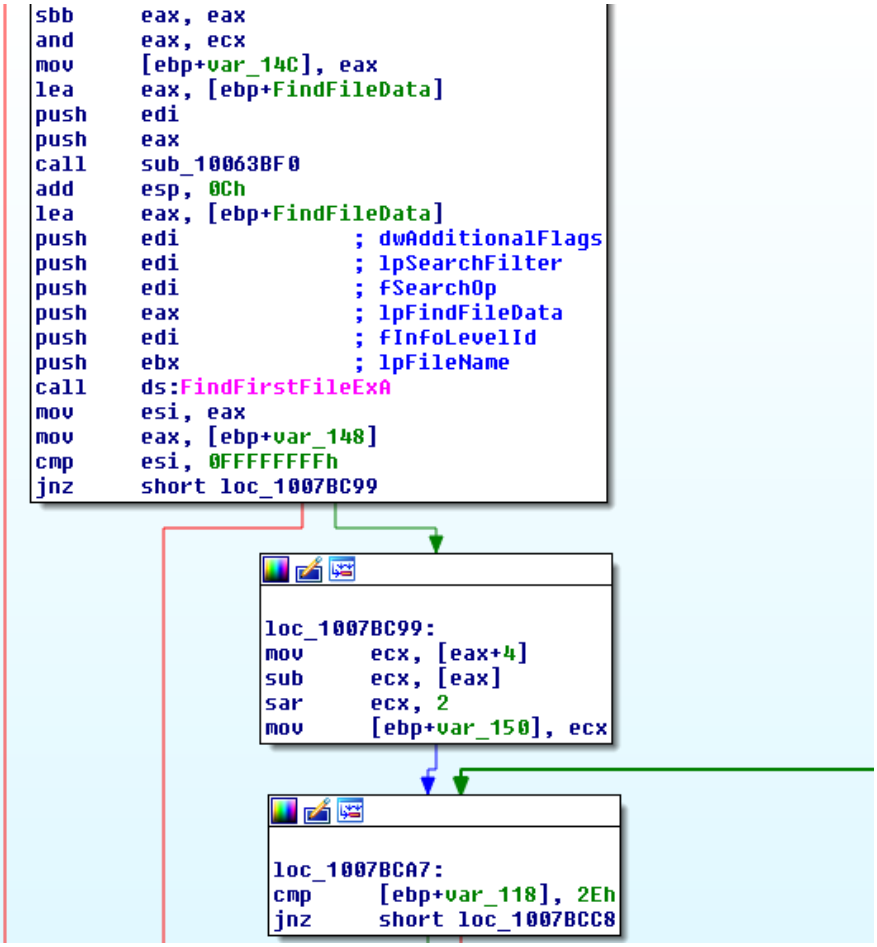
پس از طی این مراحل، اطلاعاتی از سیستم قربانی جمع‌آوری می‌شود.

```
.text:10001000 sub_10001000    proc near               ; DATA XREF: .rdata:100882F4↓o
.text:10001000
.text:10001000 SystemInfo      = _SYSTEM_INFO ptr -24h
.text:10001000
.text:10001000                 push    ebp
.text:10001001                 mov     ebp, esp
.text:10001003                 sub     esp, 24h
.text:10001006                 lea     eax, [ebp+SystemInfo]
.text:10001009                 push    eax             ; lpSystemInfo
.text:1000100A                 call    ds:GetSystemInfo
.text:10001010                 mov     eax, [ebp+SystemInfo.dwAllocationGranularity]
.text:10001013                 mov     dword_100AF958, eax
.text:10001018                 mov     esp, ebp
.text:1000101A                 pop     ebp
.text:1000101B                 retn
.text:1000101B sub_10001000    endp
.text:1000101B
```

```
.text:10001020 sub_10001020    proc near               ; DATA XREF: .rdata:100882F0↓o
.text:10001020
.text:10001020 SystemInfo      = _SYSTEM_INFO ptr -24h
.text:10001020
.text:10001020                 push    ebp
.text:10001021                 mov     ebp, esp
.text:10001023                 sub     esp, 24h
.text:10001026                 lea     eax, [ebp+SystemInfo]
.text:10001029                 push    eax             ; lpSystemInfo
.text:1000102A                 call    ds:GetSystemInfo
.text:10001030                 mov     eax, [ebp+SystemInfo.dwNumberOfProcessors]
.text:10001033                 mov     dword_100AF954, eax
.text:10001038                 mov     esp, ebp
.text:1000103A                 pop     ebp
.text:1000103B                 retn
.text:1000103B sub_10001020    endp
.text:1000103B
```

پارامترهای استفاده شده در توابع بالا نشان می‌دهد که تمامی اطلاعات دریافت شده مربوط به CPU سیستم قربانی است. این اطلاعات شامل نوع CPU، تعداد پردازنده‌ها و ... می‌شود.

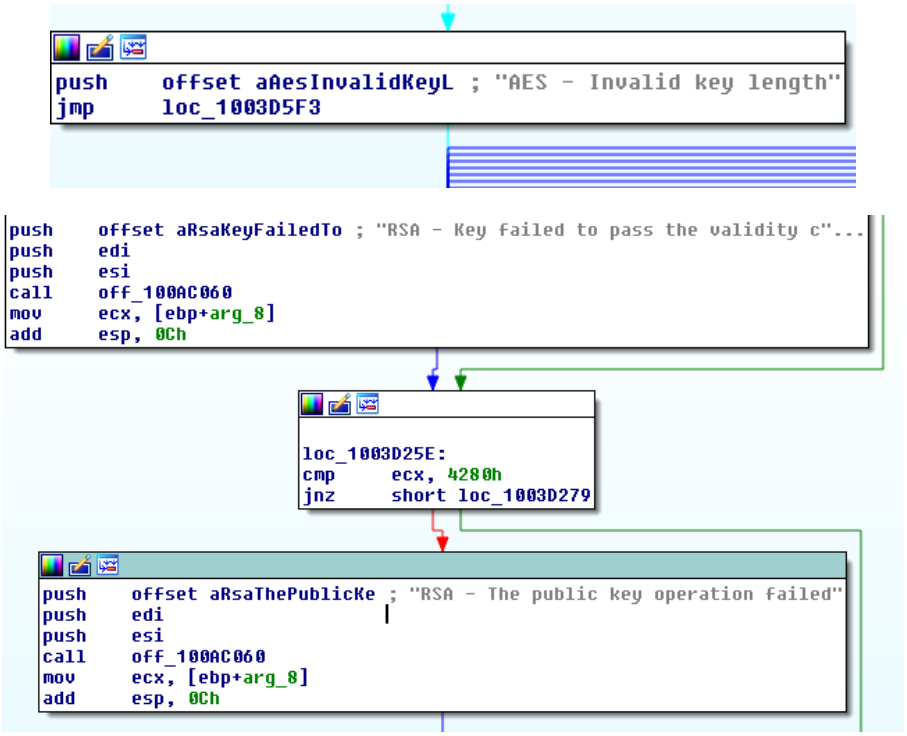
سپس، روند جست وجو و پس از آن رمزگذاری فایل‌ها در سیستم قربانی آغاز می‌شود.



فایل‌های زیر در لیست سفید باج‌افزار قرار دارند و رمزگذاری نمی‌شوند.

```
mov     [ebp+var_C0], offset a_dll ; ".dll"
mov     [ebp+var_BC], 4
mov     [ebp+var_B8], offset a_exe ; ".exe"
mov     [ebp+var_B4], 4
mov     [ebp+var_B0], offset a_sys ; ".sys"
mov     [ebp+var_AC], 4
mov     [ebp+var_A8], offset a_mui ; ".mui"
mov     [ebp+var_A4], 4
mov     [ebp+var_A0], offset a_tmp ; ".tmp"
mov     [ebp+var_9C], 4
mov     [ebp+var_98], offset a_lnk ; ".lnk"
mov     [ebp+var_94], 4
mov     [ebp+var_90], offset a_config ; ".config"
mov     [ebp+var_8C], 7
mov     [ebp+var_88], offset a_manifest ; ".manifest"
mov     [ebp+var_84], 9
mov     [ebp+var_80], offset a_tlb ; ".tlb"
mov     [ebp+var_7C], 4
mov     [ebp+var_78], offset a_olb ; ".olb"
mov     [ebp+var_74], 4
mov     [ebp+var_70], offset a_blf ; ".blf"
mov     [ebp+var_6C], 4
mov     [ebp+var_68], offset a_ico ; ".ico"
mov     [ebp+var_64], 4
mov     [ebp+var_60], offset a_regtransMs ; ".regtrans-ms"
mov     [ebp+var_5C], 0Ch
mov     [ebp+var_58], offset a_devicemetadat ; ".devicemetadata-ms"
mov     [ebp+var_54], 12h
mov     [ebp+var_50], offset a_settingconten ; ".settingcontent-ms"
mov     [ebp+var_4C], 12h
```

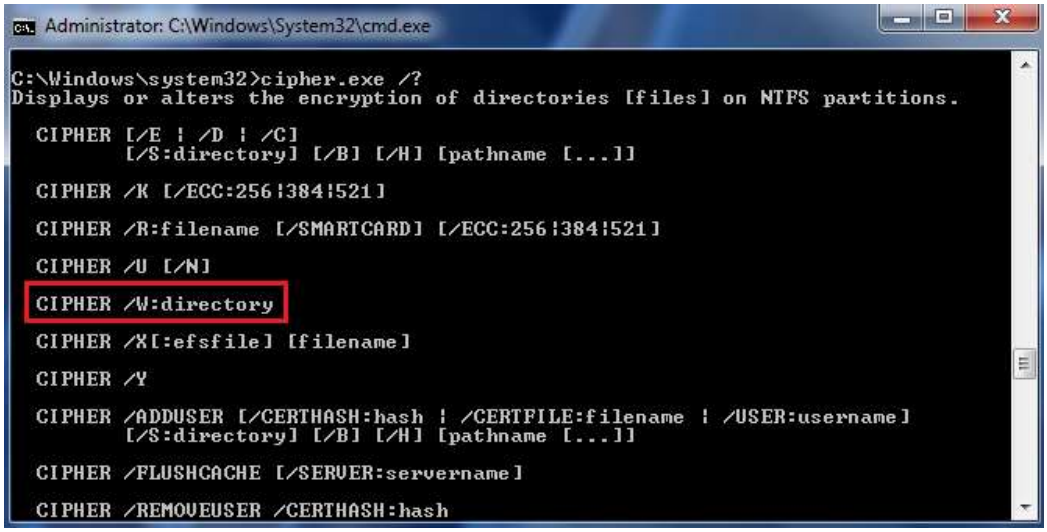
این باج‌افزار، از هر دو الگوریتم AES و RSA در فرآیند رمزنگاری خود بهره می‌برد که در پیغام باج‌خواهی آن نیز اشاره شده است و در بخش قبلی گزارش به محتوای این پیغام اشاره شد. پیغام‌های اخطاری که در صورت اخلال در فرآیند رمزگذاری درون کد قرار گرفته است نیز، صحت این موضوع را نشان می‌دهد.



در عملیات تخریب فایل‌ها از فرآیند ویندوزی cipher.exe نیز، استفاده شده است.

```
call    sub_1002B840
push    eax             ; lpWideCharStr
lea     eax, [ebp+MultiByteStr]
push    eax             ; lpMultiByteStr
call    sub_1002B920
add     esp, 8
push    0Bh             ; int
push    offset aCipher_exe ; "\\cipher.exe"
mov     ecx, eax
mov     byte ptr [ebp+var_4], 6
call    sub_1001BE10
mov     dword ptr [ebp+var_18], 0
mov     dword ptr [ebp+var_18+4], 0
movups  xmm0, xmmword ptr [eax]
movups  xmmword ptr [ebp+ApplicationName], xmm0
movq    xmm0, qword ptr [eax+10h]
movq    [ebp+var_18], xmm0
mov     dword ptr [eax+10h], 0
mov     dword ptr [eax+14h], 0Fh
mov     byte ptr [eax], 0
sub     esp, 28h
mov     eax, esp
mov     [ebp+var_60], esp
mov     dword ptr [eax], offset off_1008A10C
mov     [eax+24h], eax
lea     eax, [ebp+lpMem]
mov     byte ptr [ebp+var_4], 8
push    edi             ; int
push    eax             ; int
call    sub_1002B920
sub     esp, 10h
mov     byte ptr [ebp+var_4], 9
mov     esi, esp
mov     ecx, eax
mov     [ebp+var_5C], esi
push    0Bh
push    offset aCipherW ; "cipher /W: "
```

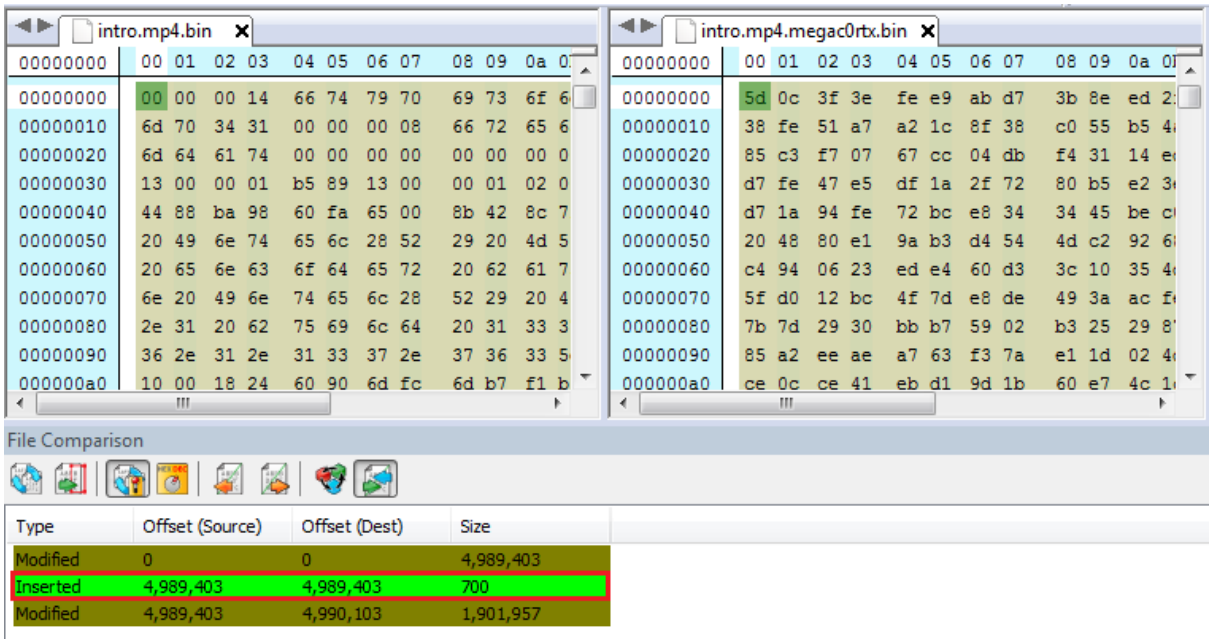
این فرآیند، در واقع یک ابزار خط فرمان می‌باشد که در محیط cmd اجرا می‌شود. دستور مشخص شده در تصویر زیر با بازنویسی فایل‌های حذف شده اقدام به تخریب آنها می‌کند. این عمل با اشغال تمام فضای دیسک توسط فایل‌های بازنویسی شده، بازیابی فایل‌ها را غیر ممکن می‌سازد.



بخشی از متن پیغام باج‌خواهی و همچنین پسوند اضافه شده به انتهای فایل‌ها پس از رمزگذاری، در تصویر زیر قابل مشاهده است.

```
a_megac0rtx:                            ; DATA XREF: sub_1000EC10+17↑o
                                        ; .rdata:a_megac0rtx_ptr↑o
                unicode 0, <.megac0rtx>,0
                align 10h
aIfYouAreReadin db 0Ah                  ; DATA XREF: .rdata:aIfYouAreReadin_ptr↑o
                db 'If you are reading this text, it means, we',27h,'ve hacked your corp'
                db 'orate network.',0Ah
                db 'Now all your data is encrypted with very serious and powerful alg'
                db 'orithms (AES256 and RSA-4,096).',0Ah
                db 'These algorithms now in use in military intelligence, NSA and CIA'
                db ' .',0Ah
                db 'No one can help you to restore your data without our special deci'
                db 'pherer.',0Ah
                db 'Don',27h,'t even waste your time.',0Ah
                db 0Ah
                db 'But there are good news for you.',0Ah
                db 'We don',27h,'t want to do any damage to your business.',0Ah
                db 'We are working for profit.',0Ah
                db 0Ah
                db 'The core of this criminal business is to give back your valuable '
                db 'data in the original form (for ransom of course).',0Ah
                db 0Ah
                db 'In order to prove that we can restore all your data, we',27h,'ll dec'
                db 'rypt 3 of your files for free.',0Ah
                db 'Please, attach 2-3 encrypted files to your first letter.',0Ah
                db 'Each file must be less than 5 Mb, non-archived and your files sho'
                db 'uld not contain valuable information',0Ah
                db '(databases, backups, large word files or excel sheets, etc.).',0Ah
                db 'You will receive decrypted samples and our conditions how to get '
                db 'the decipherer.',0Ah
                db 0Ah
                db 'For the fastest solution of the problem, please, write immediatel'
                db 'y in your first letter:',0Ah
                db 'the name of your company,',0Ah
                db 'the domain name of your corporate network and',0Ah
                db 'the URL of your corporate website',0Ah
```

براساس مشاهدات بدست آمده از مقایسه نمونه چند نمونه فایل رمز شده با نمونه سالم آن‌ها مشاهده گردید که این باج‌افزار تمام محتوای فایل‌ها را تغییر داده و مقدار ۷۰۰ بایت در انتهای هر فایل می‌نویسد.



۶-۲ تحلیل ترافیک شبکه:

با بررسی‌های صورت گرفته بر روی ترافیک ضبط شده در حین فعالیت باج‌افزار MegaCortex هیچ‌گونه ترافیک مرتبط با آن مشاهده نگردید.

۶-۳ رمزگشایی:

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