باسمه تعالی

تحلیل فنی باج افزار Desu

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی Aurora به نام Desu خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در تاریخ ۲۰ ژوئیه ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES ۲۵۶ بیتی برای رمزگذاری استفاده می‌کند و به جز فایل‌هایی با پسوندهای مشخص که در ادامه به آن‌ها اشاره خواهیم نمود، بقیه فایل‌ها را رمزگذاری می‌کند. طبق بررسی‌های انجام شده باج‌افزار Desu نسخه‌ی جدید باج‌افزار AnimusLocker می‌باشد، ریشه‌یابی این باج‌افزار به صورت زیر می‌باشد :

Aurora + Generic Malware > AnimusLocker > Desu

این باج‌افزار پس از رمزگذاری فایل‌ها پسوند آن‌ها را به desu. تغییر می‌دهد و همانند اکثر باج‌افزارها، از قربانیان تقاضای بیت‌کوین می‌کند و طبق اخبار دریافت شده، محققان امنیتی حوزه‌ی باج‌افزار موفق به رمزگشایی فایل‌های رمزگذاری شده توسط این باج‌افزار گردیده‌اند.

مشخصات فایل اجرایی :

نام فایل	memka.exe
MD۵	٥٤b٥٢٣٤ec٤b٣٦٨٢٦٤٨cf٥٢٨٠٣٩bec٥٩f
SHA-۱	cffac٩١f٦bdae٧d٨٤٥٨٨a٣١f١٦c٥٨c٨dedfcbb٣e
SHA-۲۵۶	e٢٠ff٦bf٨٢٩٦٨٤deb١٨af١b١٠٥e٣c٤dab٦٨٧٠fead٠d٢٢٩٦٤٧dc٨ada٩٩bb٦٣fa٧
اندازه فایل	٢٥٤.٥ KB
کامپایلر	VC٨ -> Microsoft Corporation

فایل اجرایی این باج افزار دارای هفت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٦١	٤٠٩٦	١٧٣٥٧٨	١٧٤٠٨٠
.rdata	٥.٥٨	١٨٠٢٢٤	٦٦٩١٠	٦٧٠٧٢
.data	٣.٣٨	٢٤٩٨٥٦	٧٧٦٤	٤٠٩٦
.gfids	٣.٠٤	٢٥٨٠٤٨	٧٤٤	١٠٢٤
.tls	٠.٠٢	٢٦٢١٤٤	٩	٥١٢
.rsrc	٦.٢٦	٢٦٦٢٤٠	١٦٤٠	٢٠٤٨

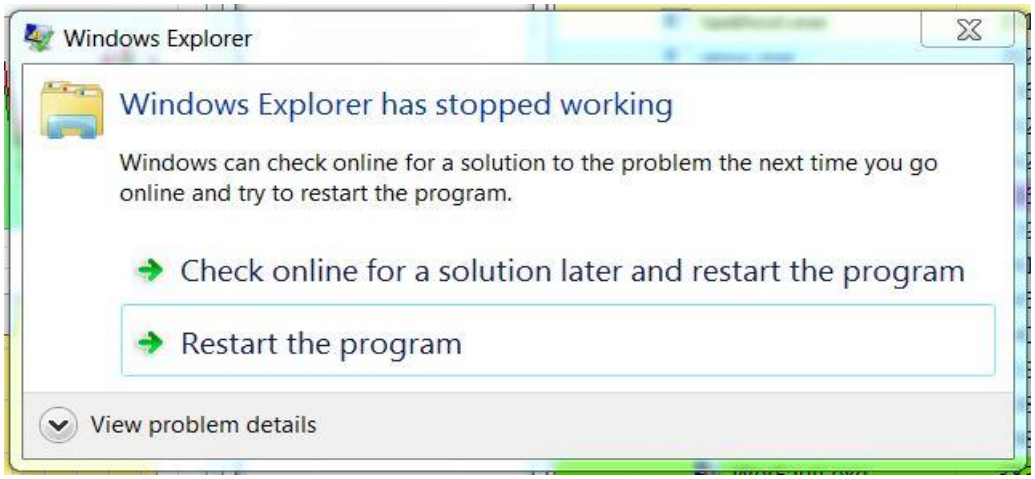
.reloc	٦.٥٦	٢٧٠٣٣٦	١٠٦٣٦	١٠٧٥٢

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Desu، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره در طول اجرا ۳ فایل متنی که محتوای هر یک از آن‌ها شامل پیغام باج‌خواهی می‌باشد را بر روی Desktop و در دایرکتوری‌های مختلف ایجاد می‌کند که نام این فایل‌ها به صورت زیر می‌باشد :

١. @_DECRYPT_@.txt
٢. @_DECRYPT2_@.txt
٣. @_DECRYPT3_@.txt

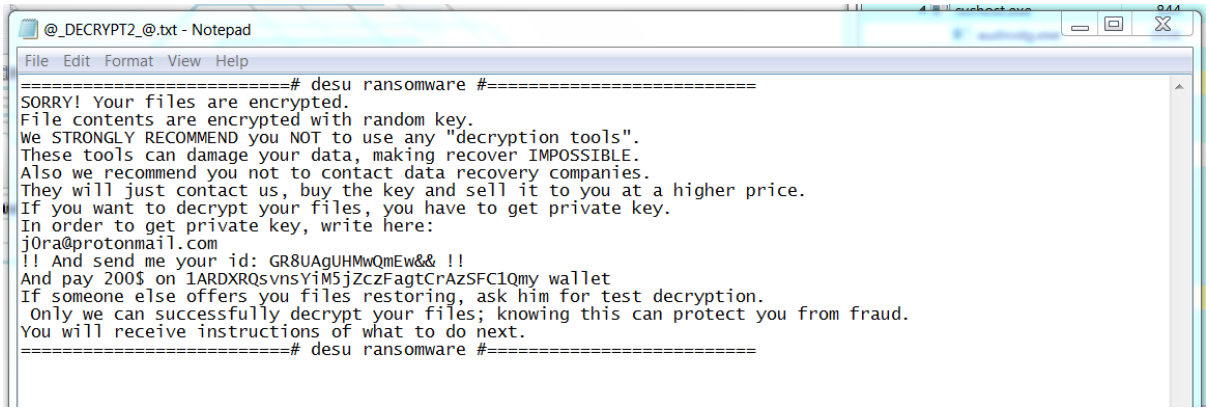
این باج‌افزار فایل‌ها را با استفاده از الگوریتم رمزنگاری AES ٢٥٦ بیتی رمزگذاری کرده و پسوند فایل‌ها را پس از رمزگذاری به desu. تغییر می‌دهد. در حین اجرای باج‌افزار، فعالیت Windows Explorer متوقف می‌شود و پیغام زیر به نمایش در می‌آید:



در ادامه فرایند مربوط به اجرای باج‌افزار و پس از پایان رمزگذاری فایل‌های مورد هدف باج‌افزار، فرایند Cmd.exe اجرا می‌شود و سیستم ری‌استارت می‌شود و پیغام زیر به نمایش در می‌آید که برای دسترسی به سیستم، قربانی باید رمز عبور را وارد نماید.

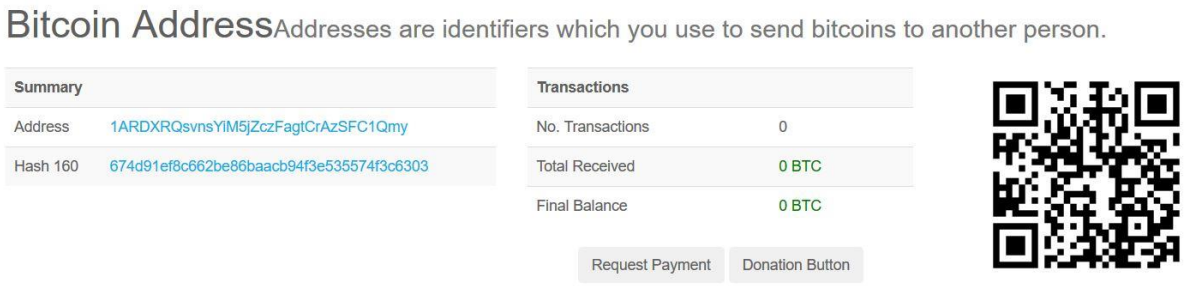
طبق پیغام بالا مهاجمین اعلام نموده‌اند که دسترسی قربانیان به فایل‌ها گرفته شده است و هیچ راهی برای دسترسی به آن‌ها به جز برقراری ارتباط با مهاجمین و پرداخت مبلغ، جهت دریافت رمز عبور وجود ندارد.

تصویر زیر مربوط به پیغام باج‌خواهی ایجاد شده در دایرکتوری‌های مختلف می‌باشد :

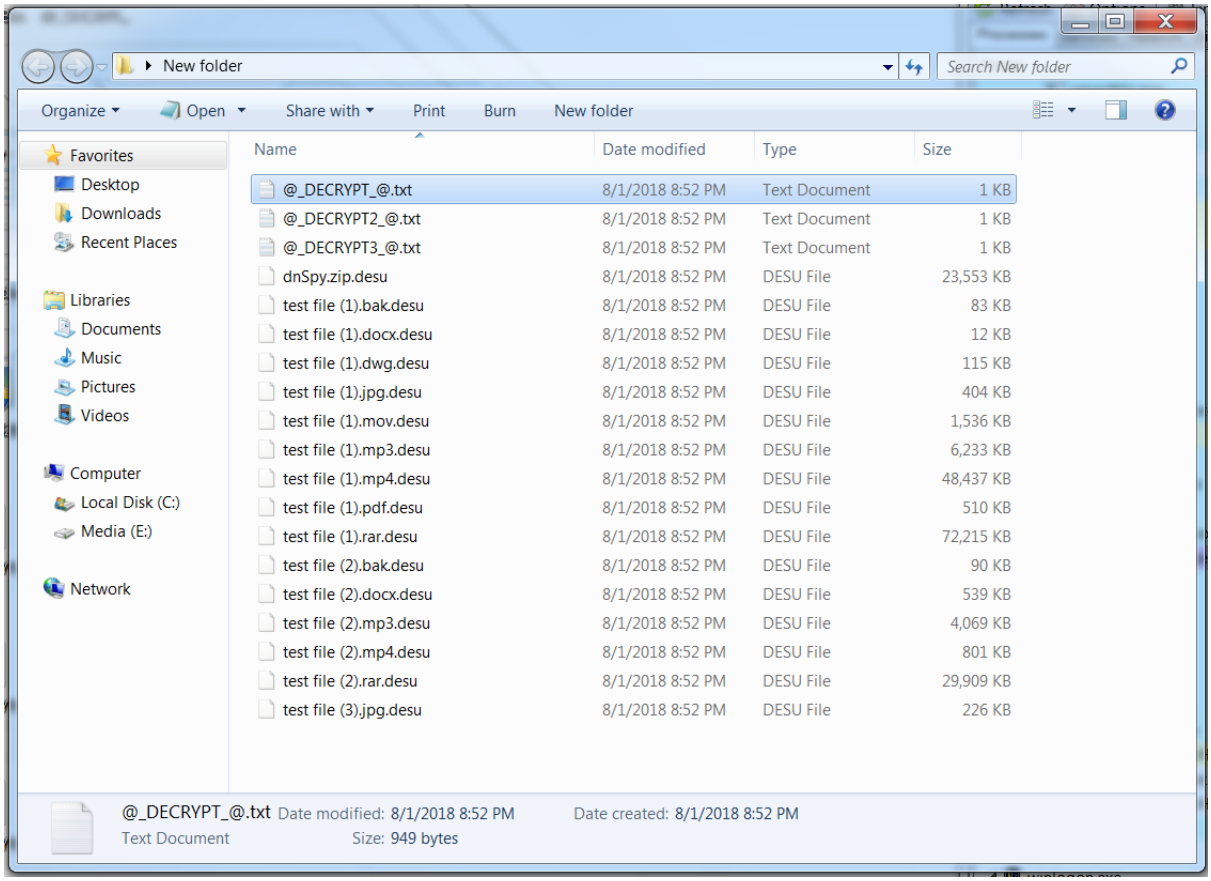


بر اساس پیغام باج‌خواهی مهاجمین اعلام نموده‌اند که فایل‌ها را با استفاده از یک کلید تصادفی رمزگذاری نموده‌اند و یادآور شده‌اند که قربانیان با استفاده از هیچ گونه ابزار رمزگشایی نمی‌توانند فایل‌ها را رمزگشایی نمایند و در صورت سعی به رمزگشایی نمودن فایل‌ها، ممکن است به آن‌ها آسیب برسانند و رمزگشایی آن‌ها را غیرممکن کنند. قربانیان برای رمزگشایی فایل‌ها باید از طریق آدرس ایمیل j0ra@protonmail.com با مهاجمین ارتباط برقرار نمایند و کد شناسایی مربوط به خود را نیز وارد نمایند تا کلید خصوصی را جهت رمزگشایی فایل‌ها خریداری نمایند. در انتهای پیغام باج‌خواهی مهاجمین به قربانیان اعلام نموده‌اند که معادل مبلغ ۲۰۰ دلار را به کیف پول بیت‌کوین به

آدرس 1ARDXRQsvnsYiM5jZczFagtCrAzSFC1Qmy ارسال نمایند. طبق بررسی‌های انجام شده، کیف پول مربوط به این باج‌افزار تاکنون تراکنشی نداشته است.



همانطور که پیشتر اشاره کردیم، این باج‌افزار پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به desu. تغییر می‌دهد، تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج افزار می‌باشد :



همانطور که اشاره شد این باج‌افزار به جز فایل‌هایی با پسوندهای مشخص، باقی فایل‌ها را رمزگذاری می‌نماید. در زیر لیست فایل‌هایی که توسط باج‌افزار رمزگذاری می‌شوند، قابل مشاهده می‌باشد :

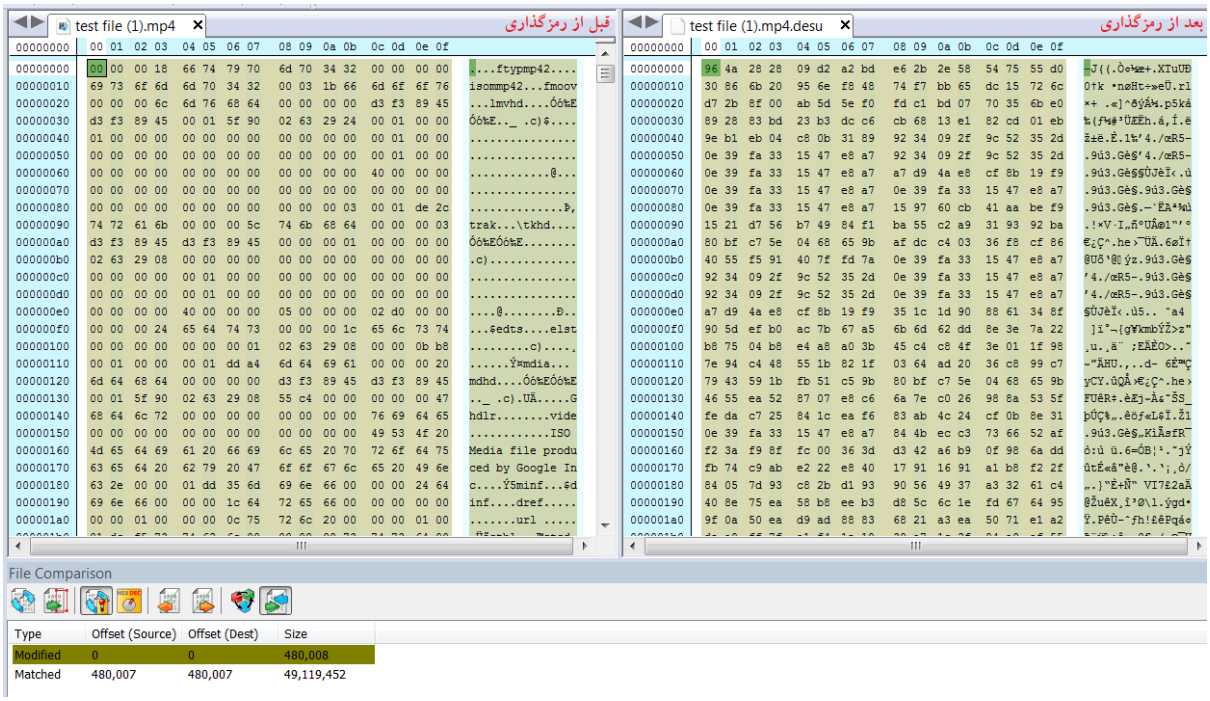
.jnt, .1CD, .dt, .cf, .1c, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pst, .ost, .msg, .eml, .vsd, .vsdx, .txt, .csv, .rtf, .123, .wks, .wk1, .pdf, .dwg, .onetoc2, .snt, .jpeg, .jpg, .docb, .docm, .dot, .dotm, .dotx, .xlsm, .xlsb, .xlw, .xlt, .xlm, .xlc, .xltx, .xltm, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam, .potx, .potm, .edb, .hwp, .602, .sxi, .sti, .sldx, .sldm, .vdi, .vmdk, .vmx, .gpg, .aes, .paq, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd, .bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .p1, .vb, .vbs, .ps1, .bat, .cmd, .js, .asm, .pas, .cpp, .c, .cs, .suo, .sln, .idf, .mdf, .ibd, .myi, .myd, .frm, .odb, .odf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay, .mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots, .ods, .3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .pfx, .der

طبق بررسی‌های صورت گرفته بر روی دو باج‌افزار Desu و AnimusLocker، این دو باج‌افزار در لیست فایل‌های مورد هدف، ایجاد ۳ فایل متنی در دایرکتوری‌های مختلف، نحوه‌ی رمزگذاری فایل‌ها و آدرس ایمیل جهت برقراری با مهاجمین مشابه یکدیگر عمل می‌کنند و از تفاوت‌های این دو باج‌افزار نیز می‌توان به آدرس کیف پول بیت‌کوین، میزان مبلغ باج‌خواهی، که در باج‌افزار Desu به ۲۰۰ دلار افزایش پیدا کرده است و عدم ایجاد فایل ۰۰۰۰۰۰۰۰۰۰.key توسط باج‌افزار Desu و... اشاره نمود. همچنین بر اساس بررسی-های انجام شده اکثر آنتی‌ویروس‌های معتبر، باج‌افزار Desu را همانند باج‌افزار AnimusLocker به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد.

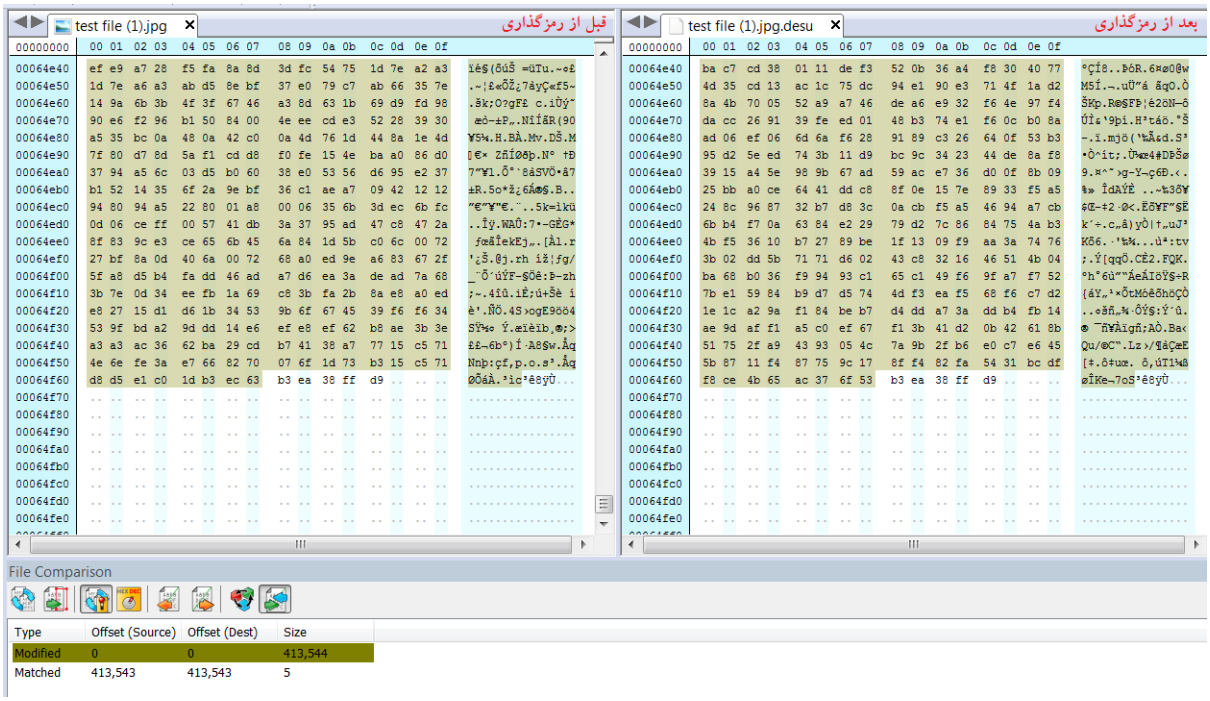
تحلیل ایستا:

پس از تحلیل کد باج‌افزار Desu به نتایج زیر دست پیدا کردیم.

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار Desu ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر نمی‌دهد و با توجه به حجم فایل‌ها رفتار متفاوتی از خود نشان می‌دهد، به این صورت که بیش از ۹۸ درصد ساختار فایل‌هایی که حجم آن‌ها کم‌تر از ۵۰۰ کیلوبایت می‌باشد را تغییر می‌دهد، اما فایل‌هایی که حجم آن‌ها بیشتر از ۵۰۰ کیلوبایت می‌باشند، فقط ٤٨٠٠٠٨ بایت ابتدایی آن‌ها را تغییر می‌دهد. تصاویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد :



تصویر ۱: فایل با حجم بیشتر از ۵۰۰ کیلوبایت که ۴۸۰۰۰۸ بایت ابتدایی آن رمزگذاری شده است.



تصویر ۲: فایل با حجم کمتر از ۵۰۰ کیلوبایت که بیش از ۹۸ درصد ساختار آن تغییر کرده است.

قطعه کد زیر مربوط به استفاده از روش‌های مختلف ضد دیس‌اسمبل جهت جلوگیری از بررسی و تحلیل‌های بیشتر توسط محققین می‌باشد :

IDA View-A | Hex View-1 | Structures | Enums

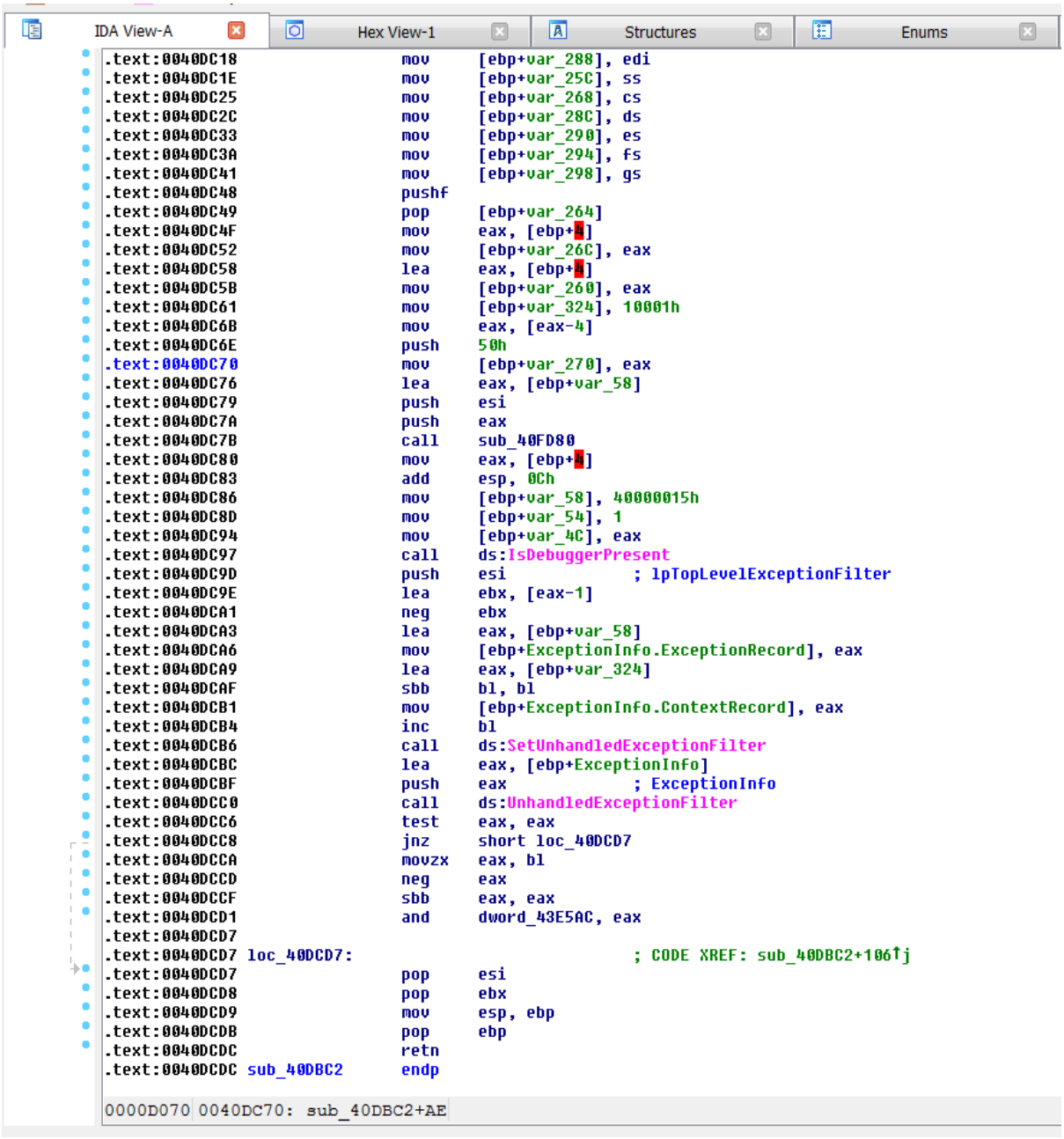
```
.text:0040DD70
.text:0040DD70 ; =============== S U B R O U T I N E =======================================
.text:0040DD70
.text:0040DD70
.text:0040DD70 sub_40DD70      proc near               ; CODE XREF: sub_40CFC4+7↑p
.text:0040DD70                                         ; sub_40D2E2+7↑p ...
.text:0040DD70
.text:0040DD70 arg_4           = dword ptr  8
.text:0040DD70
.text:0040DD70                 push    offset sub_4116F0
.text:0040DD75                 push    large dword ptr fs:0
.text:0040DD7C                 mov     eax, [esp+8+arg_4]
.text:0040DD80                 mov     [esp+8+arg_4], ebp
.text:0040DD84                 lea     ebp, [esp+8+arg_4]
.text:0040DD88                 sub     esp, eax
.text:0040DD8A                 push    ebx
.text:0040DD8B                 push    esi
.text:0040DD8C                 push    edi
.text:0040DD8D                 mov     eax, ___security_cookie
.text:0040DD92                 xor     [ebp-4], eax
.text:0040DD95                 xor     eax, ebp
.text:0040DD97                 push    eax
.text:0040DD98                 mov     [ebp-18h], esp
.text:0040DD9B                 push    dword ptr [ebp-8]
.text:0040DD9E                 mov     eax, [ebp-4]
.text:0040DDA1                 mov     dword ptr [ebp-4], 0FFFFFFFEh
.text:0040DDA8                 mov     [ebp-8], eax
.text:0040DDAB                 lea     eax, [ebp-10h]
.text:0040DDAE                 mov     large fs:0, eax
.text:0040DDB4                 repne retn
.text:0040DDB4 sub_40DD70      endp ; sp-analysis failed
.text:0040DDB4
.text:0040DDB6
.text:0040DDB6 ; =============== S U B R O U T I N E =======================================
.text:0040DDB6
.text:0040DDB6
.text:0040DDB6 sub_40DDB6      proc near               ; CODE XREF: sub_40CFC4:loc_40D048↑p
.text:0040DDB6                                         ; sub_40D2E2+56↑p ...
.text:0040DDB6                 mov     ecx, [ebp-10h]
.text:0040DDB9                 mov     large fs:0, ecx
.text:0040DDC0                 pop     ecx
.text:0040DDC1                 pop     edi
.text:0040DDC2                 pop     edi
.text:0040DDC3                 pop     esi
.text:0040DDC4                 pop     ebx
.text:0040DDC5                 mov     esp, ebp
.text:0040DDC7                 pop     ebp
.text:0040DDC8                 push    ecx
.text:0040DDC9                 repne retn
.text:0040DDC9 sub_40DDB6      endp ; sp-analysis failed
.text:0040DDC9
.text:0040DDCB
```

تابع IsDebuggerPresent() که از توابع کتابخانه Kernel۳۲ می‌باشد برای جلوگیری از اجرای باج‌افزار در محیط‌های دیباگر استفاده می‌شود تا در هنگام تحلیل با ایجاد خطا در دیباگرها مانع فعالیت گردد. قطعه کد زیر مربوط به این فرایند می‌باشد :

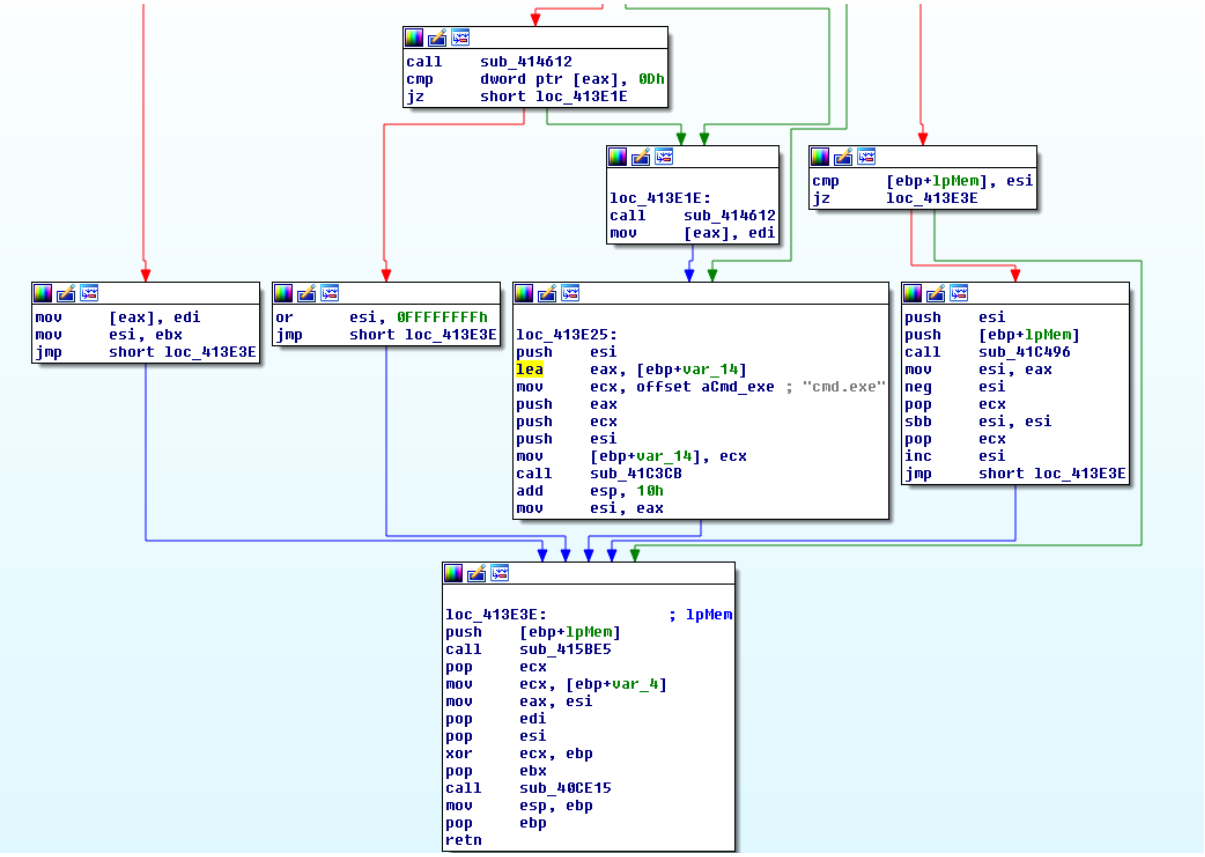
IDA View-A | Hex View-1 | Structures | Enums | Imports

```
.idata:0042C0B4                extrn SetEvent:dword    ; CODE XREF: sub_40D4E1+BF↑p
.idata:0042C0B4                                        ; DATA XREF: sub_40D4E1+BF↑r
.idata:0042C0B8 ; BOOL __stdcall ResetEvent(HANDLE hEvent)
.idata:0042C0B8                extrn ResetEvent:dword  ; CODE XREF: sub_40D4E1+CB↑p
.idata:0042C0B8                                        ; DATA XREF: sub_40D4E1+CB↑r
.idata:0042C0BC ; DWORD __stdcall WaitForSingleObjectEx(HANDLE hHandle, DWORD dwMilliseconds, BOOL bAlertable)
.idata:0042C0BC                extrn WaitForSingleObjectEx:dword
.idata:0042C0BC                                        ; CODE XREF: sub_40D5BF+4E↑p
.idata:0042C0BC                                        ; DATA XREF: sub_40D5BF+4E↑r
.idata:0042C0C0 ; BOOL __stdcall IsDebuggerPresent()
.idata:0042C0C0                extrn IsDebuggerPresent:dword ; CODE XREF: sub_40DBC2+D5↑p
.idata:0042C0C0                                        ; sub_411FF7+F8↑p
.idata:0042C0C0                                        ; DATA XREF: ...
.idata:0042C0C4 ; void __stdcall GetStartupInfoW(LPSTARTUPINFOW lpStartupInfo)
.idata:0042C0C4                extrn GetStartupInfoW:dword ; CODE XREF: sub_40DCDD+1A↑p
.idata:0042C0C4                                        ; sub_41968C+C↑p
.idata:0042C0C4                                        ; DATA XREF: ...
.idata:0042C0C8 ; BOOL __stdcall QueryPerformanceCounter(LARGE_INTEGER *lpPerformanceCount)
.idata:0042C0C8                extrn QueryPerformanceCounter:dword
.idata:0042C0C8                                        ; CODE XREF: sub_40DDCB+59↑p
.idata:0042C0C8                                        ; DATA XREF: sub_40DDCB+59↑r
```

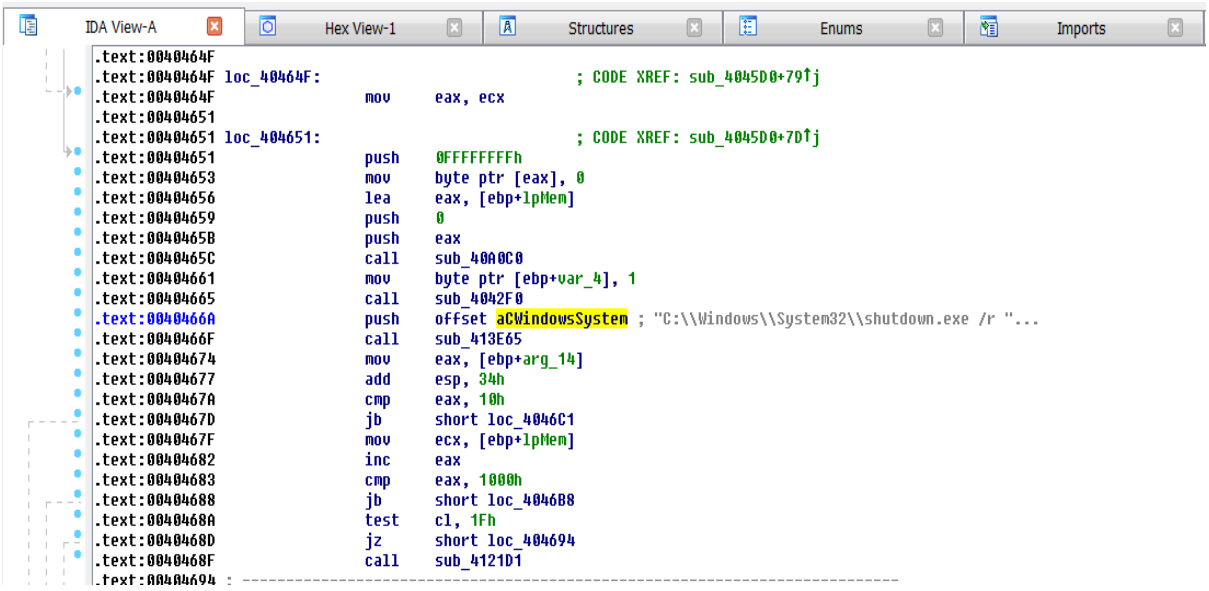
در قطعه کد زیر با استفاده از تابع IsDebuggerPresent() اقدام به بررسی محیط دیباگر می‌کند. اگر نتیجه به دست آمده مثبت باشد(یعنی محیط دیباگر باشد)، با استفاده از تابع SetUnhandledExceptionFilter() باعث ایجاد خطا می‌شود و از ادامه‌ی فعالیت جلوگیری می‌نماید.



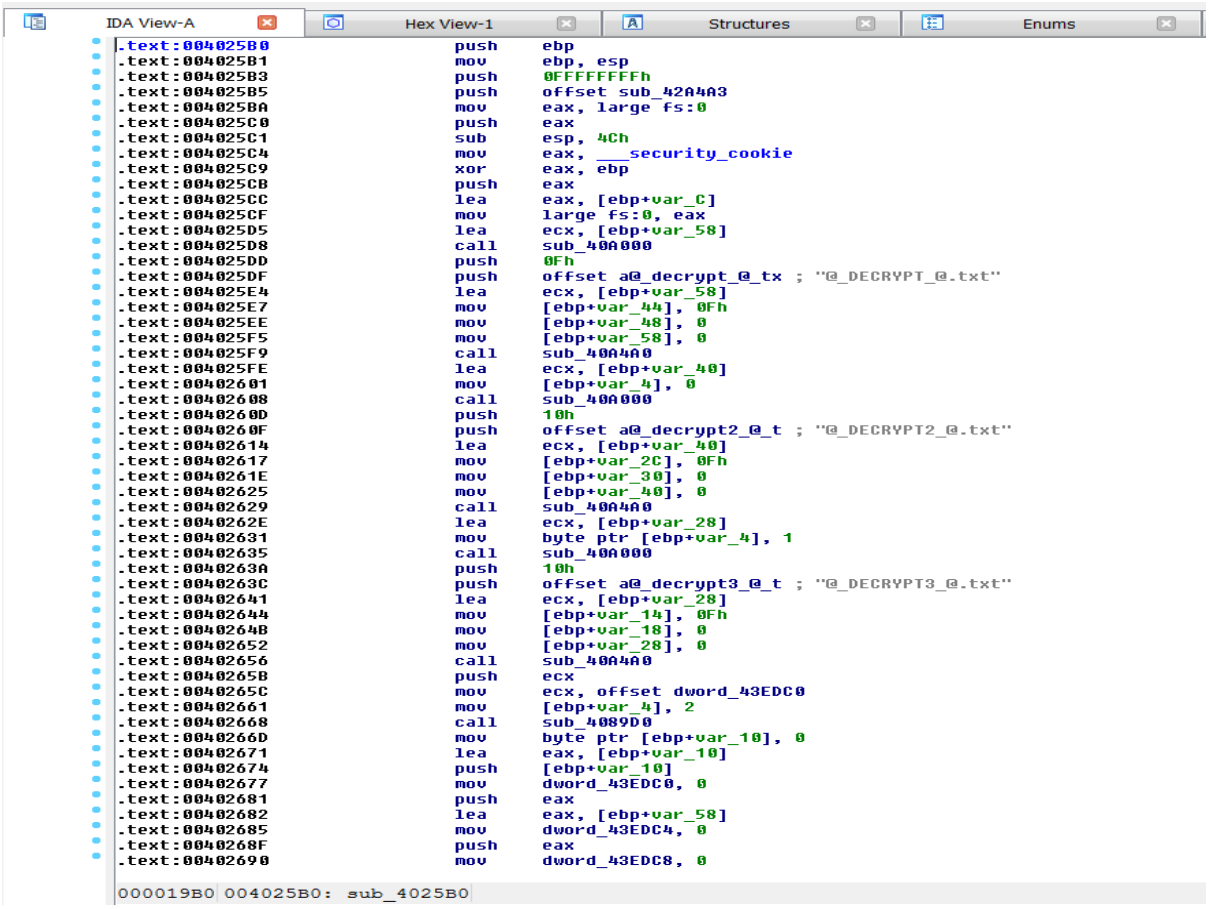
قطعه کد زیر مربوط به فراخوانی فرایند Cmd.exe قبل از ری‌استارت نمودن سیستم توسط باج‌افزار می‌باشد:



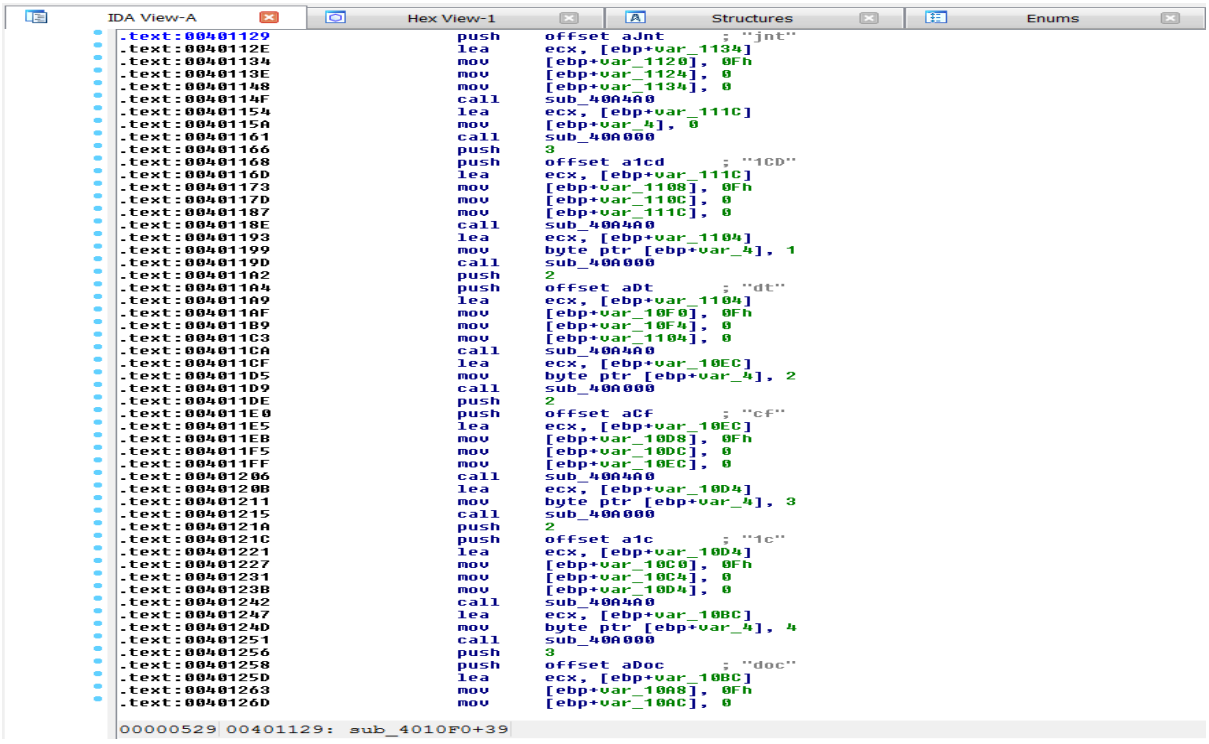
قطعه کد زیر مربوط به فرایند ری‌استارت نمودن سیستم قربانی توسط باج‌افزار می‌باشد :



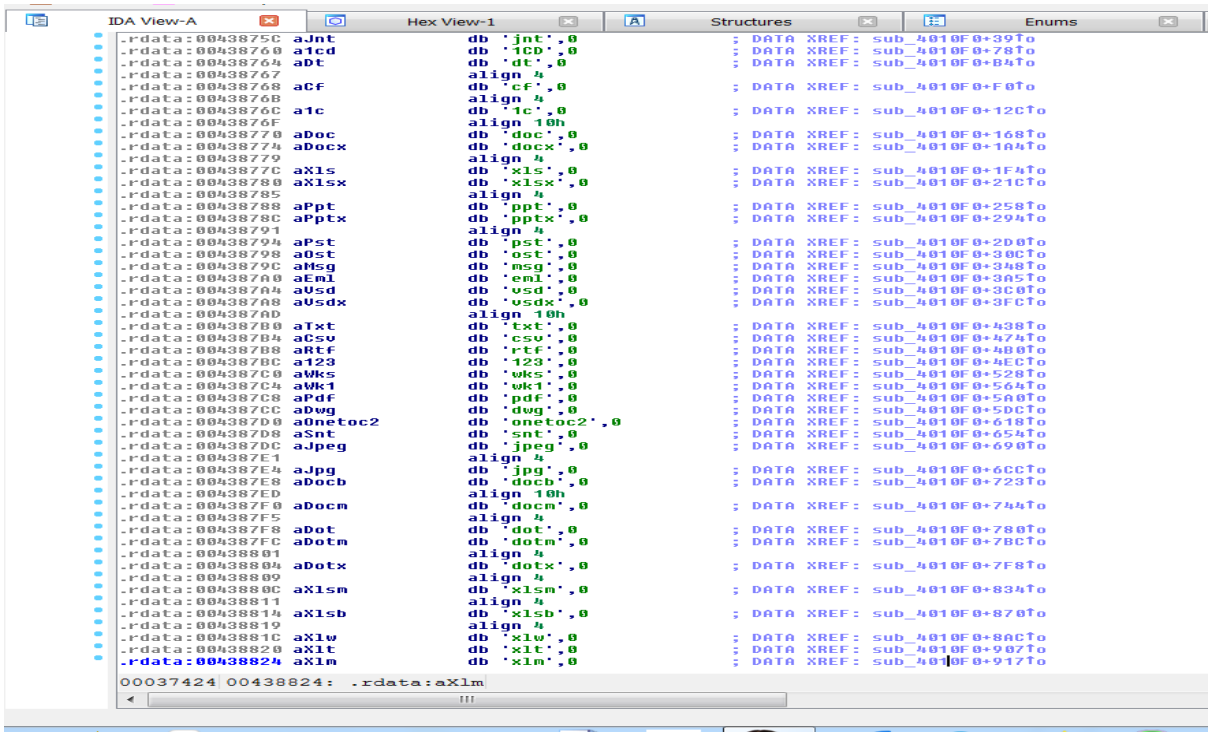
قطعه کد زیر مربوط به قرار دادن ۳ فایل متنی مربوط به پیغام باج‌خواهی در دایرکتوری‌های مختلف می‌باشد:



تصاویر زیر مربوط به بررسی فایل‌ها جهت رمزگذاری و لیست فایل‌های هدف می‌باشد :

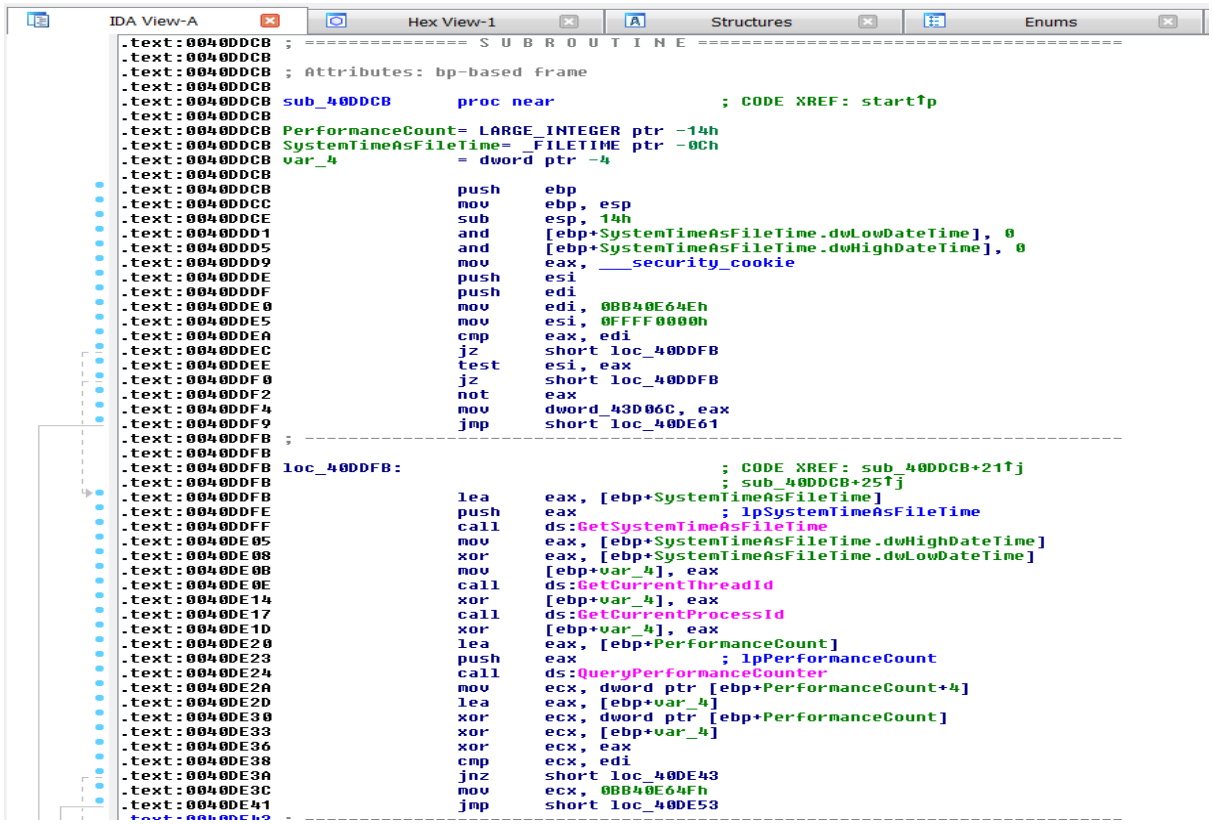


تصویر ۱

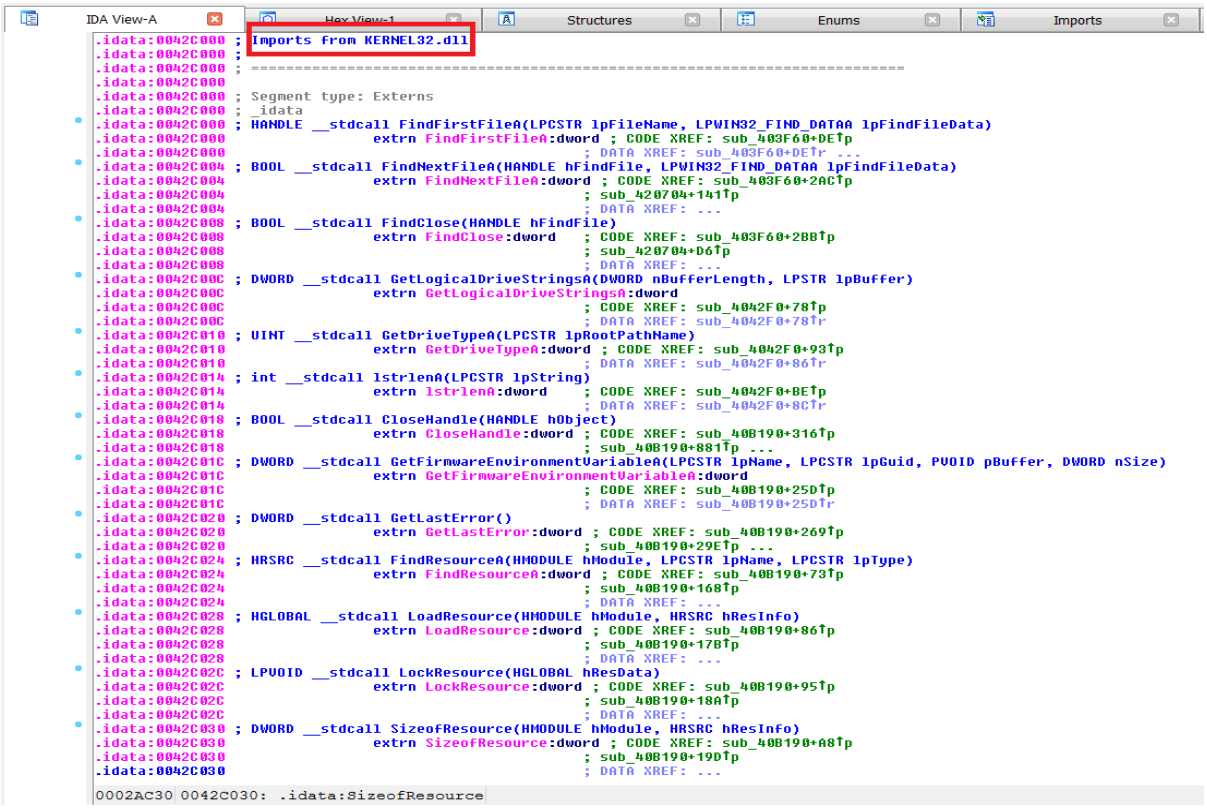


تصویر ۲: بخشی از فایل‌های مورد هدف باج‌افزار

قطعه کد زیر مربوط به بررسی منطقه زمانی کاربران می‌باشد و به نظر می‌رسد باج‌افزار از آن برای هدف قرار دادن کاربرانی خاص استفاده می‌کند :



باج‌افزار Desu فقط از کتابخانه ویندوزی KERNEL۳۲ به همراه توابعی از آن، استفاده می‌کند، که در زیر قطعه کد مربوط به آن و لیست توابع مورد استفاده قابل مشاهده می‌باشد :



KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll
UnhandledExceptionFilter	LCMapStringW	SetUnhandledExceptionFilter	GetStdHandle
FreeEnvironmentStringsW	lstrlenA	IsProcessorFeaturePresent	WaitForSingleObject
InitializeSListHead	GetConsoleCP	DecodePointer	GetDriveTypeA
GetLocaleInfoW	GetEnvironmentStringsW	SetEnvironmentVariableA	SetEndOfFile
SetStdHandle	WaitForSingleObjectEx	TerminateProcess	EncodePointer
GetCPInfo	SizeofResource	GetModuleHandleExW	GetExitCodeProcess
WriteFile	GetCurrentProcessId	ReadConsoleW	DeleteCriticalSection
GetSystemTimeAsFileTime	LockResource	GetCurrentThreadId	GetCurrentProcess
HeapReAlloc	GetCommandLineW	WriteConsoleW	GetConsoleMode
GetStringTypeW	WideCharToMultiByte	InitializeCriticalSectionAndSpi	IsValidLocale
GetOEMCP	HeapSize	nCount	GetProcAddress
GetLogicalDriveStringsA	GetCommandLineA	HeapFree	CreateEventW
LoadResource	RaiseException	EnterCriticalSection	CreateFileW
FindClose	TlsFree	FreeLibrary	GetFileType
TlsGetValue	SetFilePointer	QueryPerformanceCounter	TlsSetValue
SetLastError	ReadFile	GetTickCount	CreateFileA
IsDebuggerPresent	CloseHandle	TlsAlloc	ExitProcess
HeapAlloc	GetACP	FlushFileBuffers	LeaveCriticalSection
GetModuleFileNameA	GetModuleHandleW	RtlUnwind	GetLastError
EnumSystemLocalesW	GetFileAttributesExW	GetStartupInfoW	FindFirstFileExA
LoadLibraryExW	CreateProcessA	SetEvent	FindFirstFileA
MultiByteToWideChar	IsValidCodePage	GetUserDefaultLCID	ResetEvent
GetFirmwareEnvironmentVari	FindResourceA	GetProcessHeap	FindNextFileA
ableA	MoveFileExW	CompareStringW	SetFilePointerEx

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم باز می‌شوند :

۱.	*\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\ImageFileExecutionOptions\996E.exe*
۲.	*\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option*
۳.	*\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers*
٤.	*\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled*
٥.	*<HKLM>\System\CurrentControlSet\Control\Terminal Server*
٦.	*<HKLM>\System\CurrentControlSet\Control\Session Manager*
۷.	*<HKLM>\System\CurrentControlSet\Control\SafeBoot\Option*
۸.	*<HKLM>\System\CurrentControlSet\Control\DeviceClasses*

طبق بررسی‌های انجام شده مهاجمین از کلید شماره ۱ جهت قابلیت توسعه دادن به باج‌افزار استفاده نموده‌اند، کلید شماره ۳ جهت پیاده سازی سیاست‌های محدودیت نرم‌افزار استفاده شده است، کلید شماره ۵ جهت فعالسازی سرویس ریموت دسکتاپ (RDP) و کلید شماره ۸ جهت به دست آوردن اطلاعاتی راجع به رابط‌های سیستم استفاده می‌شده است.

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار Desu نشدیم.

نتایج بدست آمده از اجرای باج‌افزار بر روی سیستم دارای آنتی‌ویروس بومی پادویش :

طبق بررسی‌های صورت گرفته، آنتی‌ویروس پادویش در حالت عادی، این باج‌افزار را به عنوان یک فایل مخرب شناسایی می‌کند و آن را در همان ابتدا حذف می‌نماید، تصویر زیر مربوط به بررسی صورت گرفته با استفاده از آنتی‌ویروس پادویش می‌باشد :

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۷ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه بومی ویروس کاو قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن desu.bin

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.14.2	✔	Clean
f_secure	11.00	ii	Dangerous: Trojan.GenericKD.31098949
kaspersky	5.5	ii	Dangerous: Trojan-Ransom.Win32.Agent.jbo
eset	4.5.3.38239	ii	Dangerous: Win32/Filecoder.NNP
drweb	11.0.1.1607061217	ii	Dangerous: Trojan.Siggen7.55992
clam_av	0.99.2	✔	Clean
comodo	1.1.268025.1	ii	Dangerous: Malware
bitdefender	11.0.1.18	ii	Dangerous: Trojan.GenericKD.31098949
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Trojan Horse

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۳ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.31098949	AegisLab	W32.Troj.Ransom.Filecoder!c
AhnLab-V3	Trojan/Win32.FileCoder.C2624466	ALYac	Trojan.Ransom.AnimusLocker
Arcabit	Trojan.Generic.D1DA8845	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	TR/FileCoder.zxehh
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Trojan.GenericKD.31098949
Comodo	.UnclassifiedMalware	CrowdStrike Falcon	malicious_confidence_100% (W)
Cyren	W32/Trojan.BDCL-1372	DrWeb	Trojan.Siggen7.55992
Emsisoft	Trojan.FileCoder (A)	Endgame	malicious (high confidence)
eScan	Trojan.GenericKD.31098949	ESET-NOD32	a variant of Win32/Filecoder.NNP
F-Secure	Trojan.GenericKD.31098949	Fortinet	W32/Filecoder.NNP!tr
GData	Win32.Trojan-Ransom.Filecoder.P@gen	Ikarus	Trojan-Ransom.FileCoder
K7AntiVirus	Trojan (00516bfc1)	K7GW	Trojan (00516bfc1)
Kaspersky	Trojan-Ransom.Win32.Agent.jbo	Malwarebytes	Ransom.FileCryptor
McAfee	Artemis!54B5234EC4B3	McAfee-GW-Edition	BehavesLike.Win32.Generic.dh
NANO-Antivirus	Trojan.Win32.FileCoder.ffpibu	Palo Alto Networks	generic.ml
Panda	Trj/Genetic.gen	Qihoo-360	Win32/Trojan.3e8
Rising	Ransom.Genasom!8.293 (CLOUD)	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Trojan Horse
TACHYON	Ransom/W32.Desu.260608	Tencent	Win32.Trojan.Raas.Auto
TrendMicro	Ransom_ANIMUS.THGBCAH	TrendMicro-HouseCall	Ransom_ANIMUS.THGBCAH
VBA32	TrojanRansom.Agent	Zillya	Trojan.Filecoder.Win32.7967
ZoneAlarm	Trojan-Ransom.Win32.Agent.jbo	Antiy-AVL	Clean