

باسمه تعالی

## تحلیل فنی باج افزار Desu

## مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، 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 پسوند های 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	۵۴b۵۲۳۴ec۴b۳۶۸۲۶۴۸cf۵۲۸۰۳۹bec۵۹f
SHA-۱	cffac۹۱f۶bdae۷d۸۴۵۸۸a۳۱f۱۶c۵۸c۸dedfcb۳e
SHA-۲۵۶	e۲۰ff۶bf۸۲۹۶۸۴deb۱۸af۱b۱۰۵e۳c۴dab۶۸۷۰fead۰d۲۲۹۶۴۷dc۸ada۹۹bb۶۳fa۷
اندازه فایل	۲۵۴.۵ KB
کامپایلر	VC۸ -> Microsoft Corporation

فایل اجرایی این باج‌افزار دارای هفت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۶۱	۴۰۹۶	۱۷۳۵۷۸	۱۷۴۰۸۰
.rdata	۵.۵۸	۱۸۰۲۲۴	۶۶۹۱۰	۶۷۰۷۲
.data	۳.۳۸	۲۴۹۸۵۶	۷۷۶۴	۴۰۹۶
.gfiles	۳.۰۴	۲۵۸۰۴۸	۷۴۴	۱۰۲۴
.tls	۰.۰۲	۲۶۲۱۴۴	۹	۵۱۲
.rsrc	۶.۲۶	۲۶۶۲۴۰	۱۶۴۰	۲۰۴۸

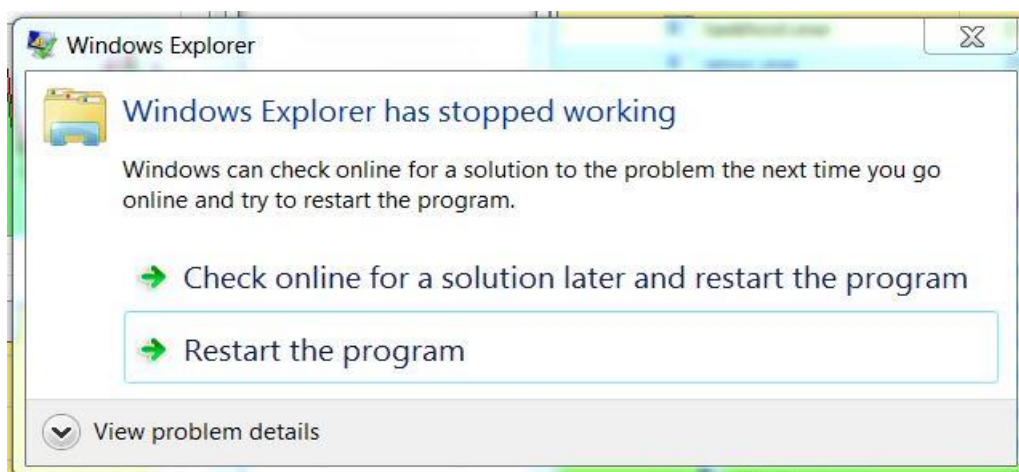
۱۰۷۵۲	۱۰۶۳۶	۲۷۰۳۳۶	۶.۵۶	.reloc
-------	-------	--------	------	--------

## 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 :

۱. @\_DECRYPT\_@.txt
۲. @\_DECRYPT2\_@.txt
۳. @\_DECRYPT3\_@.txt

این باج‌افزار فایل‌ها را با استفاده از الگوریتم رمزنگاری AES ۲۵۶ 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:

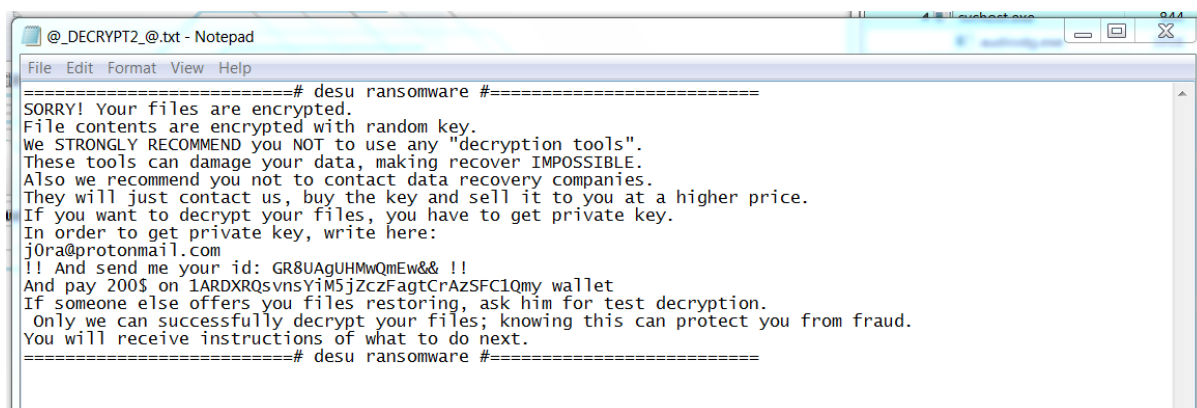


در ادامه فرایند مربوط به اجرای باج‌افزار و پس از پایان رمزگذاری فایل‌های مورد هدف باج‌افزار، فرایند اجرا می‌شود و سیستم ری‌استارت می‌شود و پیغام زیر به نمایش در می‌آید که برای دسترسی به سیستم، قربانی باید رمز عبور را وارد نماید.



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](mailto: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.

### Bitcoin Address

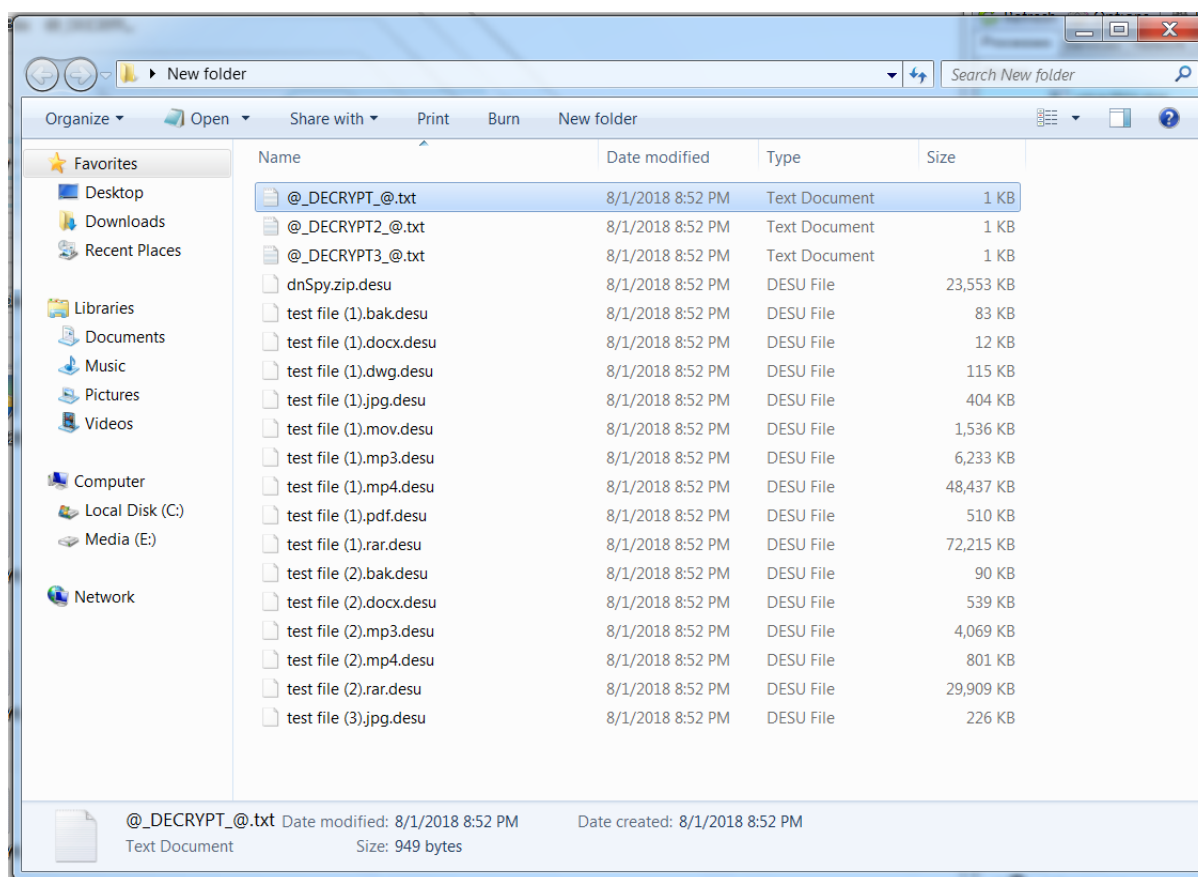
Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1ARDXRQsvnsYiM5jZczFagtCrAzSFC1Qmy	No. Transactions	0
Hash 160	674d91ef8c662be86baacb94f3e535574f3c6303	Total Received	0 BTC
		Final Balance	0 BTC



Request Payment   Donation Button

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 باج‌افزار 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, .xslm, .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 key..... توسط باج‌افزار Desu و... اشاره نمود. همچنین بر اساس بررسی‌های 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 ۴۸۰۰۰۸ بایت ابتدایی آن‌ها را تغییر می‌دهد. تصاویر زیر نمونه‌ای از تغییرات ساختار فایل‌ها را نشان می‌دهد:

قبل از رمزگذاری

```

00000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000 00 00 00 18 66 74 79 70 6d 70 34 32 00 00 00 00
00000001 69 73 6f 6d 6d 70 34 32 00 03 1b 66 6d 6f 6f 76
00000002 00 00 00 6c 6d 76 68 64 00 00 00 00 d3 f3 89 45
00000003 d3 f3 89 45 00 01 5f 90 02 43 29 24 00 01 00 00
00000004 01 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
00000005 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
00000006 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00
00000007 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000008 00 00 00 00 00 00 00 00 00 00 00 03 00 01 e2 c
00000009 74 72 61 6b 00 00 00 5c 74 6b 68 64 00 00 00 03
0000000a d3 f3 89 45 d3 f3 89 45 00 00 00 01 00 00 00 00
0000000b 02 63 29 08 00 00 00 00 00 00 00 00 00 00 00 00
0000000c 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00
0000000d 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00
0000000e 00 00 00 00 40 00 00 00 05 00 00 00 02 d0 00 00
0000000f 00 00 00 24 65 64 74 73 00 00 01 1c 65 6c 73 74
00000010 00 00 00 00 00 00 00 01 02 43 29 08 00 00 0b b8
00000011 00 01 00 00 00 01 dd a4 6d 64 69 61 00 00 00 20
00000012 6d 64 68 64 00 00 00 00 d3 f3 89 45 d3 f3 89 45
00000013 00 01 5f 90 02 63 29 08 55 c4 00 00 00 00 00 47
00000014 68 64 6c 72 00 00 00 00 00 00 00 00 76 69 64 65
00000015 00 00 00 00 00 00 00 00 00 00 00 00 49 53 4f 20
00000016 4d 65 64 69 61 20 66 69 6c 65 20 70 72 6f 64 75
00000017 63 65 64 20 62 79 20 47 6f 6f 67 6c 65 20 49 6e
00000018 63 2e 00 00 01 dd 35 6d 69 6e 66 00 00 24 64
00000019 69 6e 66 00 00 1c 64 72 65 66 00 00 00 00 00
0000001a 00 00 01 00 00 0c 75 72 6c 20 00 00 01 00
          
```

بعد از رمزگذاری

```

00000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000 68 4a 28 28 09 d2 a2 bd e6 2b 2e 58 54 75 55 d0
00000001 30 86 6b 20 95 6e f8 48 74 f7 bb 65 dc 15 72 6c
00000002 d7 2b 8f 00 ab 5d 5e f0 fd c1 bd 07 70 35 6b e0
00000003 89 28 83 bd 23 b3 dc c6 cb 68 13 e1 82 cd 01 eb
00000004 9e b1 eb 04 c8 0b 31 89 92 34 09 2f 9c 52 35 2d
00000005 0e 39 fa 33 15 47 e8 a7 92 c4 09 2f 9c 52 35 2d
00000006 0e 39 fa 33 15 47 e8 a7 a7 d9 4a e8 cf 8b 19 f9
00000007 0e 39 fa 33 15 47 e8 a7 0e 39 fa 33 15 47 e8 a7
00000008 0e 39 fa 33 15 47 e8 a7 15 97 60 cb 41 aa be f9
00000009 15 21 d7 56 b7 49 84 f1 ba 55 c2 a9 31 93 92 ba
0000000a 80 bf c7 5e 04 69 65 9b af dc c4 03 36 f8 cf 86
0000000b 40 55 f5 91 40 7f fd 7a 0e 39 fa 33 15 47 e8 a7
0000000c 92 34 09 2f 9c 52 35 2d 0e 39 fa 33 15 47 e8 a7
0000000d 92 34 09 2f 9c 52 35 2d 0e 39 fa 33 15 47 e8 a7
0000000e a7 d9 4a e8 cf 8b 19 f9 35 1c 1d 90 88 61 34 8f
0000000f 90 5d ef b0 ac 7b 67 a5 6b 6d 62 dd 8e 3e 7a 22
00000010 b8 75 04 b8 e4 a8 a0 3b 45 c2 a9 31 93 92 ba
00000011 7e 94 c4 48 55 1b 82 1f 03 64 ad 20 36 c8 99 c7
00000012 79 43 59 1b fb 51 c5 9b 80 bf c7 5e 04 69 65 9b
00000013 46 55 ea 52 87 07 e8 c6 6a 7e c0 26 98 8a 53 5f
00000014 fe da c7 25 84 1c ea fe 63 8b 4c 24 cf 0b 8e 31
00000015 0e 39 fa 33 15 47 e8 a7 84 4b ac c3 73 66 52 af
00000016 f2 3a f9 8f fc 00 36 3d d3 42 a6 b9 0f 98 6a dd
00000017 fb 74 c9 ab e2 22 e8 4d 17 91 16 91 a1 b8 f2 f2
00000018 84 05 7d 93 c8 2b d1 93 90 56 49 37 a3 32 61 c4
00000019 40 8e 75 ea 58 b8 ee b3 d8 5c 6c 1e fd 67 64 95
0000001a 9f 0a 50 ea d9 ad 88 83 68 21 a3 ea 50 71 e1 a2
          
```

File Comparison

Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	480,008
Matched	480,007	480,007	49,119,452

تصویر ۱: فایل با حجم بیشتر از ۵۰۰ کیلوبایت که ۸۰۰۰۸ بایت ابتدایی آن رمزگذاری شده است.

قبل از رمزگذاری

```

00000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00004e40 i$($0u$=uTu.-e$
00004e50 .-i$e0Zz7AyCwf5-
00004e60 .sk:0?gFE c.iUyT
00004e70 ad-iP.-NiIR(90
00004e80 a5 3b bc 0a 48 04 d2 c0 0a 4d 76 1d 44 8a 1e 4d
00004e90 7f 80 d7 8d 5a f1 cd d8 f0 fe 15 4e ba a0 86 d0
00004ea0 37 94 a5 6c 03 d5 b0 60 39 e0 53 56 d6 95 e2 37
00004eb0 b1 52 14 35 6f 2a 9e bf 36 c1 ae a7 09 42 12 12
00004ec0 94 80 94 a5 22 80 01 a8 00 06 35 6b 3d ec 6b fc
00004ed0 0d 06 ce ff 00 57 41 db 3a 37 95 ad 47 c8 47 2a
00004ee0 8f 83 9c e3 65 6b 45 6a 84 1d 5b c0 c0 00 72
00004ef0 27 bf 8a 0d 40 6a 00 72 68 a0 ed 9e ae 83 67 2f
00004f00 5f a8 d5 b4 fa dd 46 ad a7 d6 ea 3a de ad 7a 68
00004f10 8e 27 15 d1 ca ee fb 1a 69 c3 3b fa 2b 8a e8 a0 ed
00004f20 0e 27 15 d1 ca ee fb 1a 69 c3 3b fa 2b 8a e8 a0 ed
00004f30 53 9f bd a2 9d dd 14 e6 ef e8 ef 62 b8 ae 3b 3e
00004f40 a3 a3 ac 36 62 ba 29 cd b7 41 38 a7 77 15 c5 71
00004f50 4e fe fe 3a e7 66 82 70 07 6f 1d 73 b3 15 c5 71
00004f60 d8 d5 e1 c0 1d b3 ec 63 b3 ea 38 ff d9
00004f70
00004f80
00004f90
00004fa0
00004fb0
00004fc0
00004fd0
00004fe0
          
```

بعد از رمزگذاری

```

00000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00004e40 ba c7 cd 38 01 11 de f3 52 0b 36 a4 f8 30 40 77
00004e50 4d 35 cd 13 ac 1c 75 dc 94 e1 90 e3 71 4f 1a d2
00004e60 8a 4b 70 05 52 a9 a7 46 de ae e9 32 f6 4e 97 f4
00004e70 da cc 26 91 39 fe ed 01 48 b3 74 e1 f6 c0 b0 a8
00004e80 ad 06 ef 06 6d 6a f6 28 91 89 c3 26 64 0f 53 b3
00004e90 95 d2 5e ed 74 3b 11 d9 bc 9c 34 23 44 de 8a f0
00004ea0 39 15 a4 5e 90 9b 67 ad 59 ac 0f 36 d0 0f 8b 09
00004eb0 25 bb a0 ce 64 41 dd c8 8f 0e 15 7e 89 33 f5 a5
00004ec0 24 8c 96 87 32 b7 d8 3c 0a cb f5 a5 46 94 a7 cb
00004ed0 6b b4 f7 0a 63 84 e2 29 79 d2 7c 86 84 75 4a b3
00004ee0 4b f5 36 10 b7 27 89 be 1f 13 09 29 aa 3a 74 b6
00004ef0 3b 02 dd 5b 71 71 de 02 43 c8 32 16 46 51 40 04
00004f00 ba 68 b0 36 f9 94 93 c1 65 c1 49 f6 9f a7 f7 52
00004f10 7b e1 59 84 b9 d7 d5 74 4d f3 ea f5 68 26 c7 d2
00004f20 1e 1c a2 9a f1 84 be b7 d4 dd 47 3a dd b4 fb 14
00004f30 ae 9d af f1 a5 c0 ef 67 f1 3b 41 d2 0b 42 61 8b
00004f40 51 75 2f a9 43 93 05 c4 7a 9b 2f b6 e0 c7 e6 45
00004f50 5b 87 11 f4 87 75 9c 17 8f f4 82 fa e4 31 bc df
00004f60 fe ce 4b 65 ac 37 6f 53 b3 ea 38 ff d9
00004f70
00004f80
00004f90
00004fa0
00004fb0
00004fc0
00004fd0
00004fe0
          
```

File Comparison

Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	413,544
Matched	413,543	413,543	5

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+71p
.text:0040DD70                                     ; sub_40D2E2+71p ...
.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], 0FFFFFFEh
.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:0040DDB6
.text:0040DDB6 ; ===== S U B R O U T I N E =====
.text:0040DDB6
.text:0040DDB6 sub_40DDB6      proc near                ; CODE XREF: sub_40CFC4:loc_40D0481p
.text:0040DDB6                                     ; sub_40D2E2+561p ...
.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:0040DDCB

```

تابع `IsDebuggerPresent()` که از توابع کتابخانه `Kernel32` می باشد برای جلوگیری از اجرای باج افزار در محیط های دیباگر استفاده می شود تا در هنگام تحلیل با ایجاد خطا در دیباگرها مانع فعالیت گردد. قطعه کد زیر مربوط به این فرایند می باشد :

```

IDA View-A  Hex View-1  Structures  Enums  Imports
.idata:0042C084 extrn SetEvent:dword ; CODE XREF: sub_40D4E1+BF1p
.idata:0042C084 ; DATA XREF: sub_40D4E1+BF1p
.idata:0042C088 ; BOOL __stdcall ResetEvent(HANDLE hEvent)
.idata:0042C088 extrn ResetEvent:dword ; CODE XREF: sub_40D4E1+CB1p
.idata:0042C088 ; DATA XREF: sub_40D4E1+CB1p
.idata:0042C08C ; DWORD __stdcall WaitForSingleObjectEx(HANDLE hHandle, DWORD dwMilliseconds, BOOL bAlertable)
.idata:0042C08C extrn WaitForSingleObjectEx:dword
.idata:0042C08C ; CODE XREF: sub_40D5BF+4E1p
.idata:0042C08C ; DATA XREF: sub_40D5BF+4E1p
.idata:0042C088 ; BOOL __stdcall IsDebuggerPresent()
.idata:0042C088 extrn IsDebuggerPresent:dword ; CODE XREF: sub_40D8C2+D51p
.idata:0042C088 ; sub_411FF7+F81p
.idata:0042C088 ; DATA XREF: ...
.idata:0042C0C4 ; void __stdcall GetStartupInfoW(LPSTARTUPINFO lpStartupInfo)
.idata:0042C0C4 extrn GetStartupInfoW:dword ; CODE XREF: sub_40DCDD+1A1p
.idata:0042C0C4 ; sub_41968C+C1p
.idata:0042C0C4 ; DATA XREF: ...
.idata:0042C0C8 ; BOOL __stdcall QueryPerformanceCounter(LARGE_INTEGER *lpPerformanceCount)
.idata:0042C0C8 extrn QueryPerformanceCounter:dword
.idata:0042C0C8 ; CODE XREF: sub_40DDCB+591p
.idata:0042C0C8 ; DATA XREF: sub_40DDCB+591p

```



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.

```

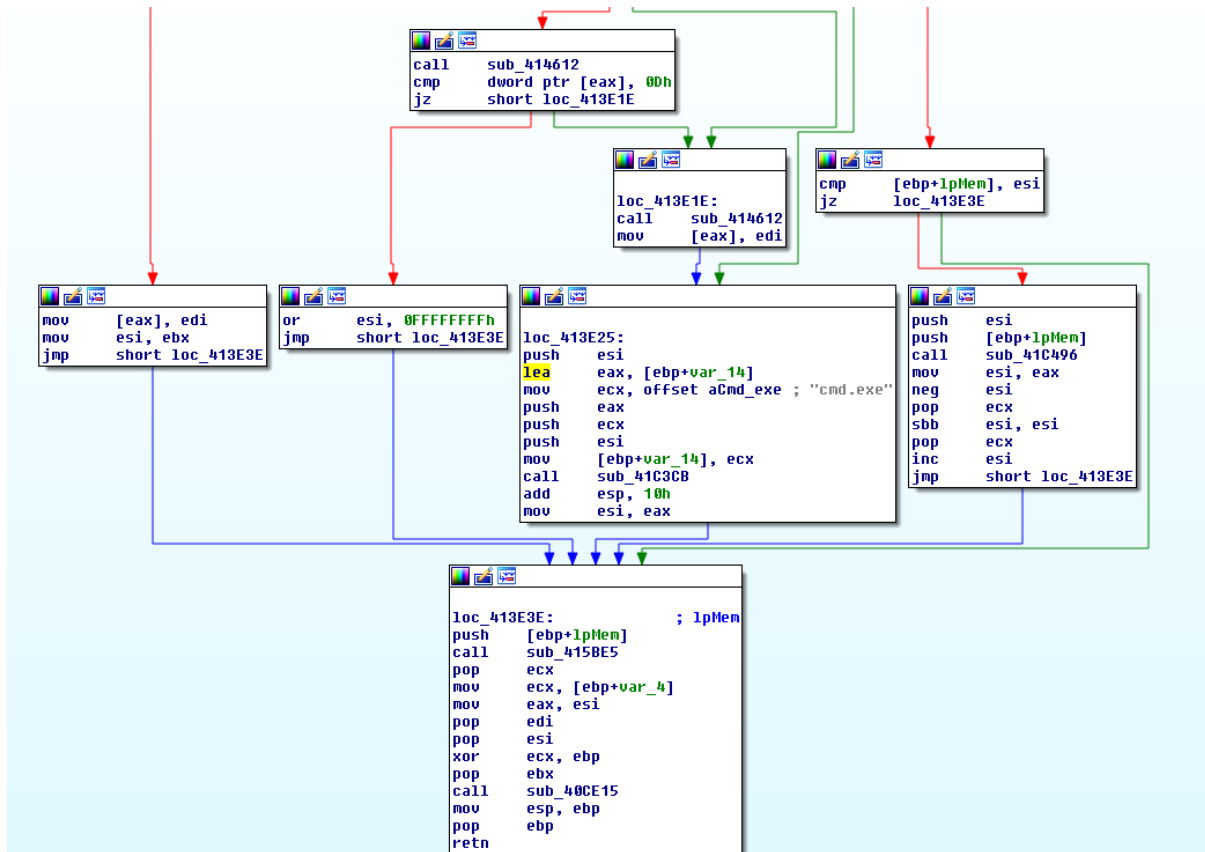
IDA View-A
Hex View-1
Structures
Enums

.text:0040DC18      mov     [ebp+var_288], edi
.text:0040DC1E      mov     [ebp+var_25C], ss
.text:0040DC25      mov     [ebp+var_268], cs
.text:0040DC2C      mov     [ebp+var_28C], ds
.text:0040DC33      mov     [ebp+var_290], es
.text:0040DC3A      mov     [ebp+var_294], fs
.text:0040DC41      mov     [ebp+var_298], gs
.text:0040DC48      pushf
.text:0040DC49      pop     [ebp+var_264]
.text:0040DC4F      mov     eax, [ebp+var_26C]
.text:0040DC52      mov     [ebp+var_26C], eax
.text:0040DC58      lea    eax, [ebp+var_260]
.text:0040DC5B      mov     [ebp+var_260], eax
.text:0040DC61      mov     [ebp+var_324], 10001h
.text:0040DC6B      mov     eax, [eax-4]
.text:0040DC6E      push   50h
.text:0040DC70      mov     [ebp+var_270], eax
.text:0040DC76      lea    eax, [ebp+var_58]
.text:0040DC79      push   esi
.text:0040DC7A      push   eax
.text:0040DC7B      call   sub_40FD80
.text:0040DC80      mov     eax, [ebp+var_58]
.text:0040DC83      add     esp, 0Ch
.text:0040DC86      mov     [ebp+var_58], 40000015h
.text:0040DC8D      mov     [ebp+var_54], 1
.text:0040DC94      mov     [ebp+var_4C], eax
.text:0040DC97      call   ds:IsDebuggerPresent
.text:0040DC9D      push   esi ; lpTopLevelExceptionFilter
.text:0040DC9E      lea    ebx, [eax-1]
.text:0040DCA1      neg     ebx
.text:0040DCA3      lea    eax, [ebp+var_58]
.text:0040DCA6      mov     [ebp+ExceptionInfo.ExceptionRecord], eax
.text:0040DCA9      lea    eax, [ebp+var_324]
.text:0040DCAF      sbb    b1, b1
.text:0040DCB1      mov     [ebp+ExceptionInfo.ContextRecord], eax
.text:0040DCB4      inc    b1
.text:0040DCB6      call   ds:SetUnhandledExceptionFilter
.text:0040DCBC      lea    eax, [ebp+ExceptionInfo]
.text:0040DCBF      push   eax ; ExceptionInfo
.text:0040DCC0      call   ds:UnhandledExceptionFilter
.text:0040DCC6      test   eax, eax
.text:0040DCC8      jnz    short loc_40DCD7
.text:0040DCCA      movzx  eax, b1
.text:0040DCCD      neg    eax
.text:0040DCCF      sbb    eax, eax
.text:0040DCD1      and    dword_43E5AC, eax
.text:0040DCD7      loc_40DCD7: ; CODE XREF: sub_40DBC2+106↑j
.text:0040DCD7      pop    esi
.text:0040DCD8      pop    ebx
.text:0040DCD9      mov    esp, ebp
.text:0040DCDB      pop    ebp
.text:0040DCCD      retn
.text:0040DCDC      sub_40DBC2 endp

0000D070 0040DC70: sub_40DBC2+AE

```

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



قطعه کد زیر مربوط به فرایند ری استارت نمودن سیستم قربانی توسط باج افزار می باشد :

```

IDA View-A
Hex View-1
Structures
Enums
Imports

.text:0040464F
.text:0040464F loc_40464F:          ; CODE XREF: sub_4045D0+79↑j
                mov     eax, ecx
.text:00404651
.text:00404651 loc_404651:          ; CODE XREF: sub_4045D0+7D↑j
                push   0FFFFFFFh
                mov     byte ptr [eax], 0
                lea    eax, [ebp+lpMem]
                push   0
                push   eax
                call   sub_40A0C0
                mov     byte ptr [ebp+var_4], 1
                call   sub_4042F0
                push   offset aCWindowsSystem ; "C:\\Windows\\System32\\shutdown.exe /r "...
                call   sub_413E65
                mov     eax, [ebp+arg_14]
                add     esp, 34h
                cmp     eax, 10h
                jnb    short loc_4046C1
                mov     ecx, [ebp+lpMem]
                inc     eax
                cmp     eax, 1000h
                jnb    short loc_4046B8
                test    cl, 1Fh
                jz     short loc_404694
                call   sub_4121D1
                .text:00404694
    
```

قطعه کد زیر مربوط به قرار دادن ۳ فایل متنی مربوط به پیغام باج خواهی در دایرکتوری های مختلف می باشد:

```
IDA View-A Hex View-1 Structures Enums
.text:004025B0 push ebp
.text:004025B1 mov ebp, esp
.text:004025B3 push 0FFFFFFFh
.text:004025B5 push offset sub_42A4A3
.text:004025B8 mov eax, large fs:0
.text:004025C0 push eax
.text:004025C1 sub esp, 4Ch
.text:004025C4 mov eax, __security_cookie
.text:004025C9 xor eax, ebp
.text:004025CB push eax
.text:004025CC lea eax, [ebp+var_C]
.text:004025CF mov large fs:0, eax
.text:004025D5 lea ecx, [ebp+var_58]
.text:004025D8 call sub_40A000
.text:004025DD push 0Fh
.text:004025DF push offset a@_decrypt_@_tx ; "@_DECRYPT_@.txt"
.text:004025E4 lea ecx, [ebp+var_58]
.text:004025E7 mov [ebp+var_44], 0Fh
.text:004025EE mov [ebp+var_48], 0
.text:004025F5 mov [ebp+var_58], 0
.text:004025F9 call sub_40A4A0
.text:004025FE lea ecx, [ebp+var_40]
.text:00402601 mov [ebp+var_4], 0
.text:00402608 call sub_40A000
.text:0040260D push 10h
.text:0040260F push offset a@_decrypt2_@_t ; "@_DECRYPT2_@.txt"
.text:00402614 lea ecx, [ebp+var_40]
.text:00402617 mov [ebp+var_2C], 0Fh
.text:0040261E mov [ebp+var_30], 0
.text:00402625 mov [ebp+var_40], 0
.text:00402629 call sub_40A4A0
.text:0040262E lea ecx, [ebp+var_28]
.text:00402631 mov byte ptr [ebp+var_4], 1
.text:00402635 call sub_40A000
.text:0040263A push 10h
.text:0040263C push offset a@_decrypt3_@_t ; "@_DECRYPT3_@.txt"
.text:00402641 lea ecx, [ebp+var_28]
.text:00402644 mov [ebp+var_14], 0Fh
.text:0040264B mov [ebp+var_18], 0
.text:00402652 mov [ebp+var_28], 0
.text:00402656 call sub_40A4A0
.text:0040265B push ecx
.text:0040265C mov ecx, offset dword_43EDC8
.text:00402661 mov [ebp+var_4], 2
.text:00402668 call sub_4089D0
.text:0040266D mov byte ptr [ebp+var_10], 0
.text:00402671 lea eax, [ebp+var_10]
.text:00402674 push [ebp+var_10]
.text:00402677 mov dword_43EDC8, 0
.text:00402681 push eax
.text:00402682 lea eax, [ebp+var_58]
.text:00402685 mov dword_43EDC4, 0
.text:0040268F push eax
.text:00402690 mov dword_43EDC8, 0

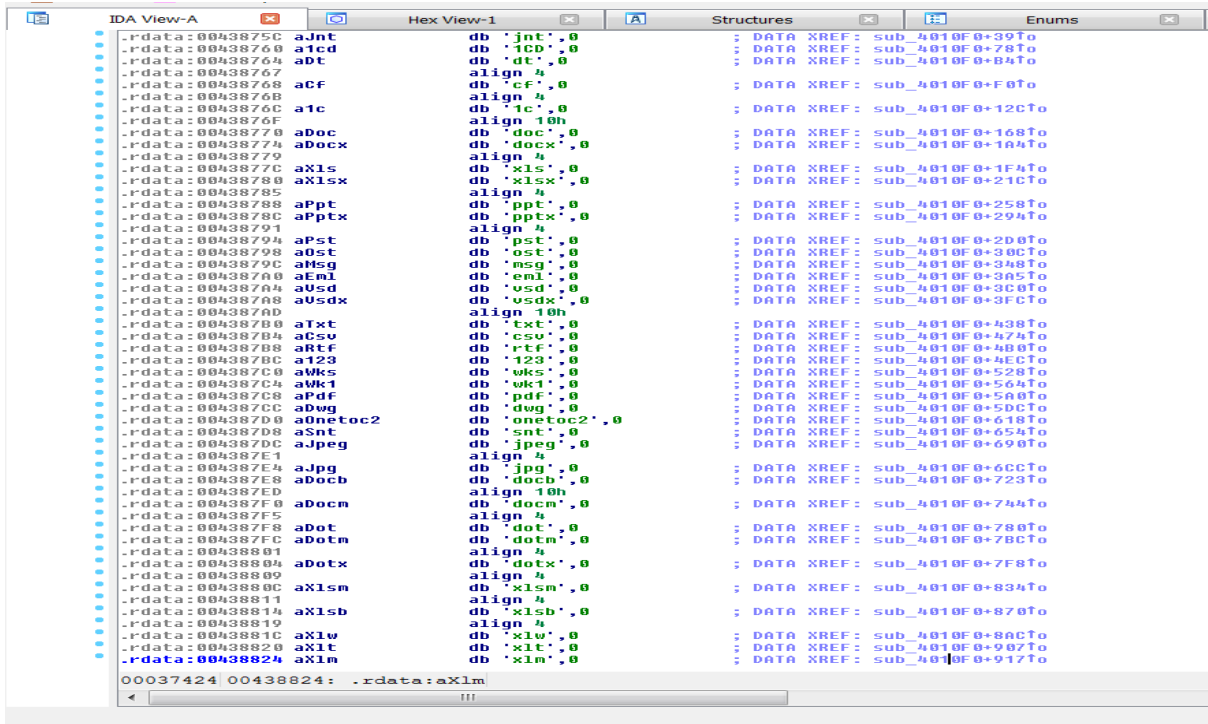
000019B0 004025B0: sub_4025B0
```

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

```
IDA View-A Hex View-1 Structures Enums
.text:00401129 push offset ajnt ; "jnt"
.text:0040112E lea ecx, [ebp+var_1134]
.text:00401131 mov [ebp+var_1120], 0Fh
.text:0040113E mov [ebp+var_1124], 0
.text:00401148 mov [ebp+var_1134], 0
.text:0040114F call sub_40A4A0
.text:00401154 lea ecx, [ebp+var_111C]
.text:00401157 mov [ebp+var_4], 0
.text:00401161 call sub_40A000
.text:00401166 push 3
.text:00401168 push offset a1cd ; "1CD"
.text:0040116B lea ecx, [ebp+var_111C]
.text:00401173 mov [ebp+var_1108], 0Fh
.text:0040117D mov [ebp+var_110C], 0
.text:00401187 mov [ebp+var_111C], 0
.text:0040118E call sub_40A4A0
.text:00401193 lea ecx, [ebp+var_1104]
.text:00401199 mov byte ptr [ebp+var_4], 1
.text:0040119D call sub_40A000
.text:004011A2 push 2
.text:004011A4 push offset aDt ; "Dt"
.text:004011A8 lea ecx, [ebp+var_1104]
.text:004011B0 mov [ebp+var_10F0], 0Fh
.text:004011B9 mov [ebp+var_10F4], 0
.text:004011C3 mov [ebp+var_1104], 0
.text:004011CA call sub_40A4A0
.text:004011CF lea ecx, [ebp+var_10EC]
.text:004011D5 mov byte ptr [ebp+var_4], 2
.text:004011D9 call sub_40A000
.text:004011DE push 2
.text:004011E0 push offset aCf ; "Cf"
.text:004011E5 lea ecx, [ebp+var_10EC]
.text:004011EB mov [ebp+var_10D8], 0Fh
.text:004011F5 mov [ebp+var_10DC], 0
.text:004011FF mov [ebp+var_10EC], 0
.text:00401206 call sub_40A4A0
.text:0040120B lea ecx, [ebp+var_10D4]
.text:00401211 mov byte ptr [ebp+var_4], 3
.text:00401215 call sub_40A000
.text:0040121A push 2
.text:0040121C push offset a1c ; "1c"
.text:00401221 lea ecx, [ebp+var_10D4]
.text:00401227 mov [ebp+var_10C0], 0Fh
.text:00401231 mov [ebp+var_10C4], 0
.text:00401238 mov [ebp+var_10D4], 0
.text:00401242 call sub_40A4A0
.text:00401247 lea ecx, [ebp+var_10BC]
.text:0040124D mov byte ptr [ebp+var_4], 4
.text:00401251 call sub_40A000
.text:00401256 push 3
.text:00401258 push offset aDoc ; "Doc"
.text:0040125D lea ecx, [ebp+var_10BC]
.text:00401263 mov [ebp+var_10A8], 0Fh
.text:0040126D mov [ebp+var_10AC], 0

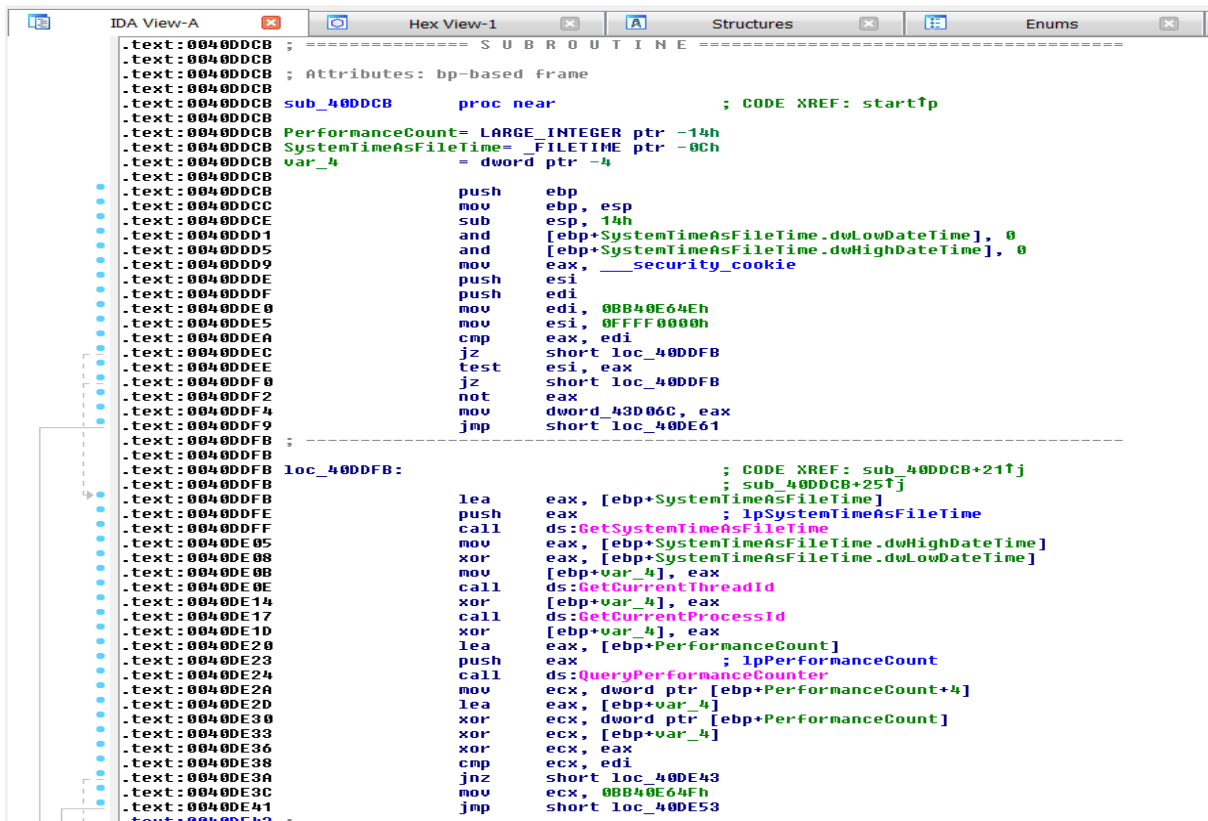
00000529 00401129: sub_4010F0+39
```

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 :



باج افزار Desu فقط از کتابخانه ویندوزی KERNEL۳۲ به همراه توابعی از آن، استفاده می کند، که در زیر قطعه کد مربوط به آن و لیست توابع مورد استفاده قابل مشاهده می باشد :

```

Imports from KERNEL32.dll
-----
; Segment type: Externs
; idata
; idata:0042C000
; HANDLE __stdcall FindFirstFileA(LPCSTR lpFileName, LPWIN32_FIND_DATA lpFindFileData)
; extrn FindFirstFileA:dword ; CODE XREF: sub_403F60+DEtp
; ; DATA XREF: sub_403F60+DEtp ...
; idata:0042C004
; BOOL __stdcall FindNextFileA(HANDLE hFindFile, LPWIN32_FIND_DATA lpFindFileData)
; extrn FindNextFileA:dword ; CODE XREF: sub_403F60+2ACtp
; ; sub_420704+141tp
; ; DATA XREF: ...
; idata:0042C008
; BOOL __stdcall FindClose(HANDLE hFindFile)
; extrn FindClose:dword ; CODE XREF: sub_403F60+2BBtp
; ; sub_420704+D6tp
; ; DATA XREF: ...
; idata:0042C00C
; DWORD __stdcall GetLogicalDriveStringsA(DWORD nBufferLength, LPSTR lpBuffer)
; extrn GetLogicalDriveStringsA:dword
; ; CODE XREF: sub_4042F0+78tp
; ; DATA XREF: sub_4042F0+78tp ...
; idata:0042C010
; UINT __stdcall GetDriveTypeA(LPCSTR lpRootPathName)
; extrn GetDriveTypeA:dword ; CODE XREF: sub_4042F0+93tp
; ; DATA XREF: sub_4042F0+86tp ...
; idata:0042C014
; int __stdcall lstrlenA(LPCSTR lpString)
; extrn lstrlenA:dword ; CODE XREF: sub_4042F0+BEtp
; ; DATA XREF: sub_4042F0+8Ctp ...
; idata:0042C018
; BOOL __stdcall CloseHandle(HANDLE hObject)
; extrn CloseHandle:dword ; CODE XREF: sub_408190+316tp
; ; sub_408190+881tp ...
; idata:0042C01C
; DWORD __stdcall GetFirmwareEnvironmentVariableA(LPCSTR lpName, LPCSTR lpGuid, PVOID pBuffer, DWORD nSize)
; extrn GetFirmwareEnvironmentVariableA:dword
; ; CODE XREF: sub_408190+25Dtp
; ; DATA XREF: sub_408190+25Dtp ...
; idata:0042C020
; DWORD __stdcall GetLastError()
; extrn GetLastError:dword ; CODE XREF: sub_408190+269tp
; ; sub_408190+29Etp ...
; idata:0042C024
; HRSRC __stdcall FindResourceA(HMODULE hModule, LPCSTR lpName, LPCSTR lpType)
; extrn FindResourceA:dword ; CODE XREF: sub_408190+73tp
; ; sub_408190+168tp
; ; DATA XREF: ...
; idata:0042C028
; HGLOBAL __stdcall LoadResource(HMODULE hModule, HRSRC hResInfo)
; extrn LoadResource:dword ; CODE XREF: sub_408190+86tp
; ; sub_408190+17Btp
; ; DATA XREF: ...
; idata:0042C02C
; LPVOID __stdcall LockResource(HGLOBAL hResData)
; extrn LockResource:dword ; CODE XREF: sub_408190+95tp
; ; sub_408190+18Atp
; ; DATA XREF: ...
; idata:0042C030
; DWORD __stdcall SizeofResource(HMODULE hModule, HRSRC hResInfo)
; extrn SizeofResource:dword ; CODE XREF: sub_408190+88tp
; ; sub_408190+19Dtp
; ; DATA XREF: ...
0002AC30 0042C030: .idata:SizeofResource
  
```

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
GetFirmwareEnvironmentVariableA	FindResourceA	GetProcessHeap	FindNextFileA
	MoveFileExW	CompareStringW	SetFilePointerEx

کلیدهای رجیستری زیر توسط باج افزار در سیستم باز می شوند :

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\CodelIdentifiers
۴. \REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodelIdentifiers\TransparentEnabled
۵. <HKLM>\System\CurrentControlSet\Control\Terminal Server
۶. <HKLM>\System\CurrentControlSet\Control\Session Manager
۷. <HKLM>\System\CurrentControlSet\Control\SafeBoot\Option
۸. <HKLM>\System\CurrentControlSet\Control\DeviceClasses

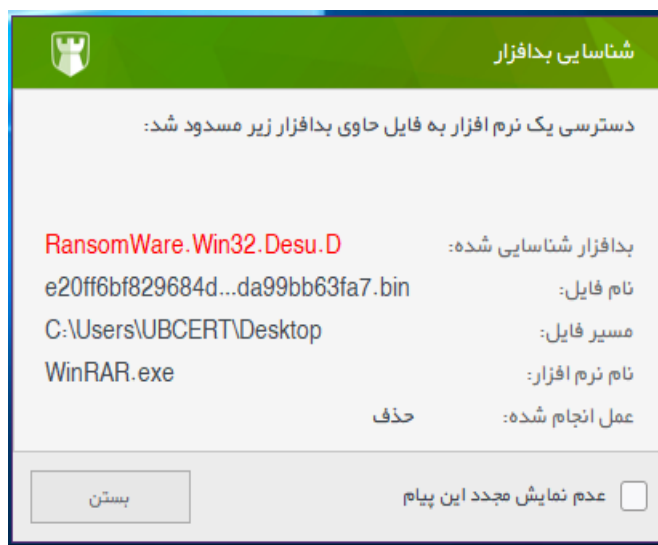
طبق بررسی های انجام شده مهاجمین از کلید شماره ۱ جهت قابلیت توسعه دادن به باج افزار استفاده نموده اند، کلید شماره ۳ جهت پیاده سازی سیاست های محدودیت نرم افزار استفاده شده است، کلید شماره ۵ جهت فعالسازی سرویس ریموت دسکتاپ (RDP) و کلید شماره ۸ جهت به دست آوردن اطلاعاتی راجع به رابط های سیستم استفاده می شده است.

### تحلیل ترافیک شبکه :

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

### نتایج بدست آمده از اجرای باج افزار بر روی سیستم دارای آنتی ویروس بومی پادویش :

طبق بررسی های صورت گرفته، آنتی ویروس پادویش در حالت عادی، این باج افزار را به عنوان یک فایل مخرب شناسایی می کند و آن را در همان ابتدا حذف می نماید، تصویر زیر مربوط به بررسی صورت گرفته با استفاده از آنتی ویروس پادویش می باشد :



## خروجی سامانه ویروس کاو 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 و آن را حذف یا غیرفعال می کنند.

### نتیجه اسکن desu.bin

آنتی ویروس	نسخه آنتی ویروس	نتیجه اسکن
پادویش	2.3.190.2675	✓
sophos	9.14.2	✓
f_secure	11.00	ii
kaspersky	5.5	ii
eset	4.5.3.38239	ii
drweb	11.0.1.1607061217	ii
clam_av	0.99.2	✓
comodo	1.1.268025.1	ii
bitdefender	11.0.1.18	ii
avast	2.1.2	✓
symantec	7.9.0.30	ii

## خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۳ مورد از ۶۶ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

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