

باسمه تعالی

تحلیل فنی باج افزار AnimusLocker

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی به نام AnimusLocker خبر می دهد. بررسی ها نشان می دهد که فعالیت این باج افزار در اواخر ماه ژوئن سال ۲۰۱۸ میلادی شروع شده و به نظر می رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می باشد. این باج افزار از الگوریتم رمزنگاری AES ۲۵۶ بیتی برای رمزگذاری استفاده می کند و به جز فایل هایی با پسوندهای مشخص که در ادامه به آن ها اشاره خواهیم نمود، بقیه فایل ها را رمزگذاری می کند. طبق بررسی های انجام شده باج افزار AnimusLocker و باج افزار Aurora از یک خانواده می باشند و ریشه یابی آن ها به صورت زیر می باشد :

Aurora + Generic Malware > AnimusLocker

این باج افزار پس از رمزگذاری فایل ها پسوند آن ها را به animus. تغییر می دهد و همانند اکثر باج افزارها، از قربانیان تقاضای بیت کوین می کند و طبق اخبار دریافت شده، محققان امنیتی حوزه ی باج افزار موفق به رمزگشایی فایل های رمزگذاری شده توسط این باج افزار گردیده اند.

مشخصات فایل اجرایی :

نام فایل	Ransom.exe
MD۵	c9c4711355a76d5b6549cc89946a9b08
SHA-۱	۲۵۱۵۹fcc۵۰۳۲۸۸bfd9۵۶۵۰۰۰b9ae۲4f1fd4e5c8
SHA-۲۵۶	41ff378dcb0c1eacc3766a868c8e0۲4۵۷۸۲c7f849d7e78380c7799b7771f2e2b
اندازه فایل	۳۸۰.۵ KB
کامپایلر	VC۸ -> Microsoft Corporation

فایل اجرایی این باج افزار دارای هفت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۶۱	۴۰۹۶	۱۷۳۴۵۵	۱۷۳۵۶۸
.rdata	۵.۵۹	۱۸۰۲۲۴	۶۷۹۱۲	۶۸۰۹۶
.data	۷.۷۹	۲۴۹۸۵۶	۱۳۳۸۸۰	۱۲۹۰۲۴
.gfids	۳.۱۸	۳۸۵۰۲۴	۷۷۶	۱۰۲۴

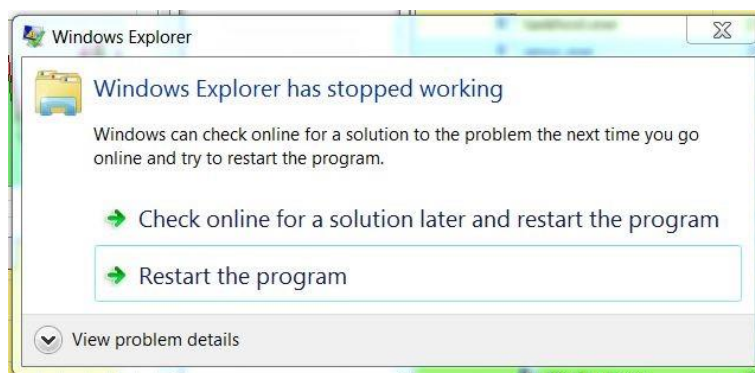
۵۱۲۰	۵۰۲۹	۳۸۹۱۲۰	۰	.tls
۵۱۲	۴۸۰	۳۹۷۳۱۲	۴.۷۲	.rsrc
۱۱۲۶۴	۱۰۸۹۲	۴۰۱۴۰۸	۶.۵۳	.reloc

تحلیل پویا :

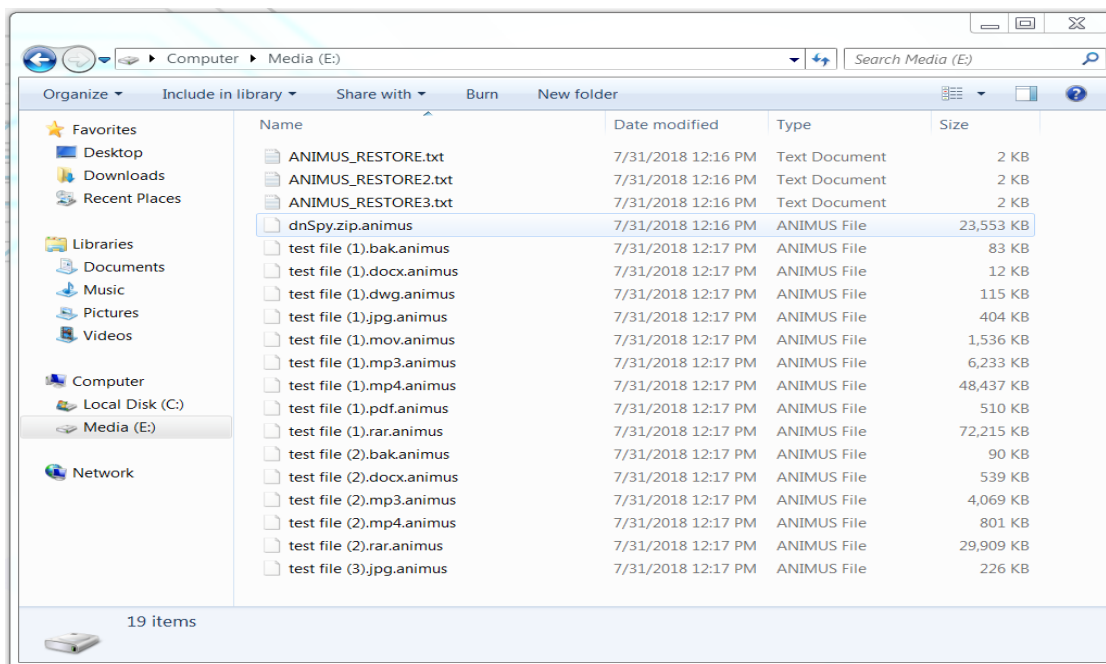
برای بررسی عمیق تر باج افزار AnimusLocker، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج افزار مورد اشاره در طول اجرا ۳ فایل متنی که محتوای هر یک از آنها شامل پیغام باج خواهی می باشد را بر روی Desktop و در دایرکتوری های مختلف ایجاد می کند که نام این فایل ها به صورت زیر می باشد :

۱. ANIMUS_RESTORE.txt
۲. ANIMUS_RESTORE۲.txt
۳. ANIMUS_RESTORE۳.txt

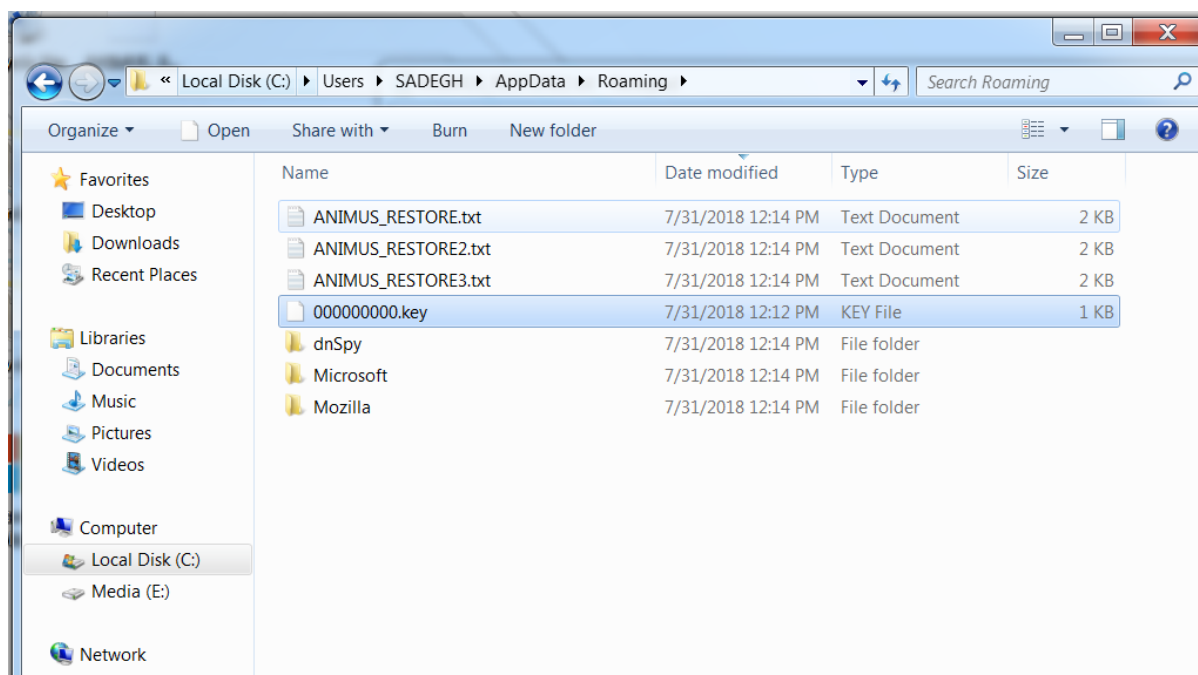
این باج افزار فایل ها را با استفاده از الگوریتم رمزنگاری AES ۲۵۶ بیتی رمزگذاری کرده و پسوند فایل ها را پس از رمزگذاری به animus. تغییر می دهد. در حین اجرای باج افزار، فعالیت Windows Explorer متوقف می شود و پیغام زیر به نمایش در می آید:



پس از آن، فرایند مربوط به اجرای باج افزار خاتمه پیدا می کند و پیغام باج خواهی به نمایش در می آید. تصویر زیر پیغام باج خواهی باج افزار AnimusLocker را نشان می دهد.



فایل key..... در تصویر زیر قابل مشاهده می باشد :



همانطور که اشاره شد این باج افزار به جز فایل هایی با پسوندهای مشخص، باقی فایل ها را رمزگذاری می نماید. در زیر لیست فایل هایی که توسط باج افزار رمزگذاری می شوند، قابل مشاهده می باشد :

.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 مشاهدات صورت گرفته، هنگام اجرای باج افزار AnimusLocker به طور میانگین از ۳۵ الی ۴۵ درصد ظرفیت CPU و ۲۰ درصد ظرفیت حافظه (RAM) استفاده می گردد.

بر اساس بررسی های انجام شده اکثر آنتی ویروس های معتبر، این باج افزار را به عنوان یک تروجان شناسایی نموده اند. لذا احتمال نفوذ باج افزار به سیستم از راه های متداول از جمله هرزنامه ها وجود دارد.

تحلیل ایستا:

پس از تحلیل کد باج افزار AnimusLocker به نتایج زیر دست پیدا کردیم.

طبق بررسی هایی که بر روی فایل های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج افزار AnimusLocker ساختار فایل ها را پس از رمزگذاری به طور کامل تغییر نمی دهد و با توجه به حجم فایل ها رفتار متفاوتی از خود نشان می دهد، به این صورت که تقریباً ۹۸ درصد ساختار فایل هایی که حجم آن ها کم تر از ۵۰۰ کیلوبایت می باشد را تغییر می دهد، اما فایل هایی که حجم آن ها بیشتر از ۵۰۰ کیلوبایت می باشند، فقط ۴۸۰۰۰۸ بایت ابتدایی آن ها را تغییر می دهد. تصاویر زیر نمونه ای از تغییرات ساختار فایل ها را نشان می دهد:

قبل از رمزگذاری | dnSpy.zip

Offset (Source)	Offset (Dest)	Size
0	0	480,008
480,007	480,007	23,637,299

بعد از رمزگذاری | dnSpy.zip.animus

File Comparison

Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	480,008
Matched	480,007	480,007	23,637,299

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

قبل از رمزگذاری | test file (1).bak

Offset (Source)	Offset (Dest)	Size
0	0	84,608
84,607	84,607	7

بعد از رمزگذاری | test file (1).bak.animus

File Comparison

Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	84,608
Matched	84,607	84,607	7

تصویر ۲: فایل با حجم کمتر از ۵۰۰ کیلوبایت که تقریباً 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
; ===== SUBROUTINE =====
.text:00420E7C ;
.text:00420E7C
.text:00420E7C sub_420E7C      proc near          ; CODE XREF: sub_41C6BA+19C1p
.text:00420E7C      push      0Ch
.text:00420E7E      push      offset unk_43BE88
.text:00420E83      call     sub_40D240
.text:00420E88      and     dword ptr [ebp-1Ch], 0
.text:00420E8C      push     6
.text:00420E8E      call    sub_41510B
.text:00420E93      pop     ecx
.text:00420E94      and     dword ptr [ebp-4], 0
.text:00420E98      push    dword ptr [ebp+8]
.text:00420E9B      call    sub_4206E4
.text:00420EA0      pop     ecx
.text:00420EA1      mov     esi, eax
.text:00420EA3      mov     [ebp-1Ch], esi
.text:00420EA6      mov     dword ptr [ebp-4], 0FFFFFFEh
.text:00420EAD      call    sub_420EBD
.text:00420EB2      mov     eax, esi
.text:00420EB4      call    sub_40D286
.text:00420EB9      retn
.text:00420EB9 sub_420E7C      endp ; sp-analysis failed
; ===== SUBROUTINE =====
.text:00420EBA ;
.text:00420EBA
.text:00420EBA sub_420EBA      proc near          ; DATA XREF: .rdata:0043BEA0j0
.text:00420EBA      mov     esi, [ebp-1Ch]
.text:00420EBA sub_420EBA      endp ; sp-analysis failed
.text:00420EBD

```

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
; sub_4117A3+21f ...
; BOOL __stdcall TerminateProcess(HANDLE hProcess, UINT uExitCode)
; extrn TerminateProcess:dword ; CODE XREF: sub_40C6F8+20f
; sub_4117A3+28f ...
; BOOL __stdcall IsProcessorFeaturePresent(DWORD ProcessorFeature)
; extrn __imp_IsProcessorFeaturePresent:dword
; DATA XREF: IsProcessorFeaturePresentTr
; BOOL __stdcall IsDebuggerPresent()
; extrn IsDebuggerPresent:dword ; CODE XREF: sub_40D048+D5f
; sub_41220A+F8f
; DATA XREF: ...
; void __stdcall GetStartupInfoW(LPSTARTUPINFO lpStartupInfo)
; extrn GetStartupInfoW:dword ; CODE XREF: sub_40D163+1Af
; sub_41A7C5+Cf
; DATA XREF: ...
; BOOL __stdcall QueryPerformanceCounter(LARGE_INTEGER *lpPerformanceCount)
; extrn QueryPerformanceCounter:dword
; CODE XREF: sub_40D445+59f
; DATA XREF: sub_40D445+59f

```

در قطعه کد زیر با استفاده از تابع `IsDebuggerPresent()` اقدام به بررسی محیط دیباگر می کند. اگر نتیجه به دست آمده مثبت باشد (یعنی محیط اجرا دیباگر باشد)، با استفاده از تابع `SetUnhandledExceptionFilter()` باعث ایجاد خطا می شود و از ادامه ی فعالیت جلوگیری می نماید.


```
IDA View-A | Hex View-1 | Structures | Enums
. text: 0040D086 mov [ebp+var_278], ecx
. text: 0040D08C mov [ebp+var_27C], edx
. text: 0040D092 mov [ebp+var_280], ebx
. text: 0040D098 mov [ebp+var_284], esi
. text: 0040D09E mov [ebp+var_288], edi
. text: 0040D0A4 mov [ebp+var_25C], ss
. text: 0040D0AB mov [ebp+var_268], cs
. text: 0040D0B2 mov [ebp+var_28C], ds
. text: 0040D0B9 mov [ebp+var_290], es
. text: 0040D0C0 mov [ebp+var_294], fs
. text: 0040D0C7 mov [ebp+var_298], gs
. text: 0040D0CE pushf
. text: 0040D0CF pop [ebp+var_264]
. text: 0040D0D5 mov eax, [ebp+var_278]
. text: 0040D0D8 mov [ebp+var_26C], eax
. text: 0040D0DE lea eax, [ebp+var_278]
. text: 0040D0E1 mov [ebp+var_260], eax
. text: 0040D0E7 mov [ebp+var_324], 10001h
. text: 0040D0F1 mov eax, [eax-4]
. text: 0040D0F4 push 50h
. text: 0040D0F6 mov [ebp+var_270], eax
. text: 0040D0FC lea eax, [ebp+var_58]
. text: 0040D0FF push esi
. text: 0040D100 push eax
. text: 0040D101 call sub_40F400
. text: 0040D106 mov eax, [ebp+var_278]
. text: 0040D109 add esp, 0Ch
. text: 0040D10C mov [ebp+var_58], 40000015h
. text: 0040D113 mov [ebp+var_54], 1
. text: 0040D11A mov [ebp+var_4C], eax
. text: 0040D11D call ds:IsDebuggerPresent
. text: 0040D123 push esi ; lpTopLevelExceptionFilter
. text: 0040D124 lea ebx, [eax-1]
. text: 0040D127 neg ebx
. text: 0040D129 lea eax, [ebp+var_58]
. text: 0040D12C mov [ebp+ExceptionInfo.ExceptionRecord], eax
. text: 0040D12F lea eax, [ebp+var_324]
. text: 0040D135 sbb b1, b1
. text: 0040D137 mov [ebp+ExceptionInfo.ContextRecord], eax
. text: 0040D13A inc b1
. text: 0040D13C call ds:SetUnhandledExceptionFilter
. text: 0040D142 lea eax, [ebp+ExceptionInfo]
. text: 0040D145 push eax ; ExceptionInfo
. text: 0040D146 call ds:UnhandledExceptionFilter
. text: 0040D14C test eax, eax
. text: 0040D14E jnz short loc_40D15D
. text: 0040D150 movzx eax, b1
. text: 0040D153 neg eax
. text: 0040D155 sbb eax, eax
. text: 0040D157 and dword_45CE78, eax
. text: 0040D15D loc_40D15D: ; CODE XREF: sub_40D048+106↑j
. text: 0040D15D pop esi
. text: 0040D15E pop ebx
. text: 0040D15F mov esp, ebp
. text: 0040D161 pop ebp
. text: 0040D162 retn
. text: 0040D162 sub_40D048 endp
0000C48C 0040D08C: sub_40D048+44
```

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

```
IDA View-A Hex View-1 Structures Enums
- .text:00402510 push ebp
- .text:00402511 mov ebp, esp
- .text:00402513 push 0FFFFFFFh
- .text:00402515 push offset sub_42A003
- .text:00402518 mov eax, large fs:0
- .text:00402519 push eax
- .text:00402521 sub esp, 4Ch
- .text:00402524 mov eax, __security_cookie
- .text:00402529 xor eax, ebp
- .text:0040252B push eax
- .text:0040252C lea eax, [ebp+var_C]
- .text:0040252F mov large fs:0, eax
- .text:00402535 lea ecx, [ebp+var_58]
- .text:00402538 call sub_40A900
- .text:0040253D push 12h
- .text:0040253F push offset aAnimus_restore ; "ANIMUS_RESTORE.txt"
- .text:00402544 lea ecx, [ebp+var_58]
- .text:00402547 mov [ebp+var_44], 0Fh
- .text:0040254E mov [ebp+var_48], 0
- .text:00402555 mov [ebp+var_58], 0
- .text:00402559 call sub_408A60
- .text:0040255E lea ecx, [ebp+var_40]
- .text:00402561 mov [ebp+var_4], 0
- .text:00402568 call sub_40A900
- .text:0040256D push 13h
- .text:0040256F push offset aAnimus_resto_0 ; "ANIMUS_RESTORE2.txt"
- .text:00402574 lea ecx, [ebp+var_40]
- .text:00402577 mov [ebp+var_2C], 0Fh
- .text:0040257E mov [ebp+var_30], 0
- .text:00402585 mov [ebp+var_40], 0
- .text:00402588 call sub_408A60
- .text:0040258E lea ecx, [ebp+var_28]
- .text:00402591 mov byte ptr [ebp+var_4], 1
- .text:00402595 call sub_40A900
- .text:0040259A push 13h
- .text:004025A1 lea ecx, [ebp+var_28]
- .text:004025A4 mov [ebp+var_14], 0Fh
- .text:004025AB mov [ebp+var_18], 0
- .text:004025B2 mov [ebp+var_28], 0
- .text:004025B6 call sub_408A60
- .text:004025BB push ecx
- .text:004025BC mov ecx, offset dword_45D6C4
- .text:004025C1 mov [ebp+var_4], 2
- .text:004025C8 call sub_40A900
- .text:004025CD mov byte ptr [ebp+var_10], 0
- .text:004025D1 lea eax, [ebp+var_10]
- .text:004025D4 push [ebp+var_10]
- .text:004025D7 mov dword_45D6C4, 0
- .text:004025E1 push eax
- .text:004025E2 lea eax, [ebp+var_58]
- .text:004025E5 mov dword_45D6C8, 0
- .text:004025EF push eax
- .text:004025F0 mov dword_45D6CC, 0
00001910 00402510: sub_402510
```

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

```
IDA View-A Hex View-1 Structures Enums
- .text:00401050 push ebp
- .text:00401051 mov ebp, esp
- .text:00401053 push 0FFFFFFFh
- .text:00401055 push offset sub_42A5C2
- .text:0040105A mov eax, large fs:0
- .text:00401060 push eax
- .text:00401061 mov eax, 1128h
- .text:00401066 call sub_40D5B0
- .text:0040106B mov eax, __security_cookie
- .text:00401070 xor eax, ebp
- .text:00401072 push eax
- .text:00401073 lea eax, [ebp+var_C]
- .text:00401076 mov large fs:0, eax
- .text:0040107C lea ecx, [ebp+var_1134]
- .text:00401082 call sub_40A900
- .text:00401087 push 3
- .text:00401089 push offset aJnt ; "jnt"
- .text:0040108E lea ecx, [ebp+var_1134]
- .text:00401094 mov [ebp+var_1120], 0Fh
- .text:0040109E mov [ebp+var_1124], 0
- .text:004010A8 mov [ebp+var_1134], 0
- .text:004010AF call sub_408A60
- .text:004010B4 lea ecx, [ebp+var_111C]
- .text:004010BA mov [ebp+var_4], 0
- .text:004010C1 call sub_40A900
- .text:004010C6 push 3
- .text:004010C8 push offset a1cd ; "1cd"
- .text:004010CD lea ecx, [ebp+var_111C]
- .text:004010D3 mov [ebp+var_1108], 0Fh
- .text:004010DD mov [ebp+var_110C], 0
- .text:004010E7 mov [ebp+var_111C], 0
- .text:004010EE call sub_408A60
- .text:004010F3 lea ecx, [ebp+var_1104]
- .text:004010F9 mov byte ptr [ebp+var_4], 1
- .text:004010FD call sub_40A900
- .text:00401102 push 2
- .text:00401104 push offset aDt ; "dt"
- .text:00401109 lea ecx, [ebp+var_1104]
- .text:0040110F mov [ebp+var_10F0], 0Fh
- .text:00401119 mov [ebp+var_10F4], 0
- .text:00401123 mov [ebp+var_1104], 0
- .text:0040112A call sub_408A60
- .text:0040112F lea ecx, [ebp+var_10EC]
- .text:00401135 mov byte ptr [ebp+var_4], 2
- .text:00401139 call sub_40A900
- .text:0040113E push 2
- .text:00401140 push offset aCf ; "cf"
- .text:00401145 lea ecx, [ebp+var_10EC]
- .text:0040114B mov [ebp+var_10D8], 0Fh
- .text:00401155 mov [ebp+var_10DC], 0
- .text:0040115F mov [ebp+var_10EC], 0
- .text:00401166 call sub_408A60
- .text:0040116B lea ecx, [ebp+var_10D4]
- .text:00401171 mov byte ptr [ebp+var_4], 3
00000450 00401050: sub_401050
```

تصویر ۱

```
IDA View-A Hex View-1 Structures Enums
.rdata:0043827C aJnt db 'jnt',0 ; DATA XREF: sub_401050+39To
.rdata:00438280 a1cd db '1cd',0 ; DATA XREF: sub_401050+78To
.rdata:00438287 adt db 'dt',0 ; DATA XREF: sub_401050+84To
.rdata:00438288 aCf align 4,0 ; DATA XREF: sub_401050+F0To
.rdata:0043828B a1c db '1c',0 ; DATA XREF: sub_401050+12CTo
.rdata:0043828F aDoc align 10h,0 ; DATA XREF: sub_401050+168To
.rdata:00438290 aDocx db 'docx',0 ; DATA XREF: sub_401050+1A4To
.rdata:00438299 align 4,0
.rdata:0043829C aXls db 'xls',0 ; DATA XREF: sub_401050+1F4To
.rdata:004382A0 aXlsx db 'xlsx',0 ; DATA XREF: sub_401050+21CTo
.rdata:004382A5 align 4,0
.rdata:004382A8 aPpt db 'ppt',0 ; DATA XREF: sub_401050+258To
.rdata:004382AC aPptx db 'pptx',0 ; DATA XREF: sub_401050+294To
.rdata:004382B1 align 4,0
.rdata:004382B4 aPst db 'pst',0 ; DATA XREF: sub_401050+2D0To
.rdata:004382B8 a0st db 'ost',0 ; DATA XREF: sub_401050+30CTo
.rdata:004382BC aMsg db 'msg',0 ; DATA XREF: sub_401050+348To
.rdata:004382C0 aEml db 'eml',0 ; DATA XREF: sub_401050+385To
.rdata:004382C4 aUsd db 'usd',0 ; DATA XREF: sub_401050+3C0To
.rdata:004382C8 aUsdx db 'usdx',0 ; DATA XREF: sub_401050+3FCTo
.rdata:004382CD align 10h,0
.rdata:004382D0 aTxt db 'txt',0 ; DATA XREF: sub_401050+438To
.rdata:004382D4 aCsu db 'csu',0 ; DATA XREF: sub_401050+474To
.rdata:004382D8 aRtf db 'rtf',0 ; DATA XREF: sub_401050+4B0To
.rdata:004382DC a123 db '123',0 ; DATA XREF: sub_401050+4E0To
.rdata:004382E0 aWks db 'wks',0 ; DATA XREF: sub_401050+528To
.rdata:004382E4 aWk1 db 'wk1',0 ; DATA XREF: sub_401050+564To
.rdata:004382E8 aPdf db 'pdf',0 ; DATA XREF: sub_401050+5A0To
.rdata:004382EC adwg db 'dwg',0 ; DATA XREF: sub_401050+5D0To
.rdata:004382F0 aOnetoc2 db 'onetoc2',0 ; DATA XREF: sub_401050+618To
.rdata:004382F8 aSnt db 'snt',0 ; DATA XREF: sub_401050+654To
.rdata:004382FC aJpeg db 'jpeg',0 ; DATA XREF: sub_401050+690To
.rdata:00438301 align 4,0
.rdata:00438304 aJpg db 'jpg',0 ; DATA XREF: sub_401050+6CC0To
.rdata:00438308 aDocb db 'docb',0 ; DATA XREF: sub_401050+723To
.rdata:0043830D align 10h,0
.rdata:00438310 aDocm db 'docm',0 ; DATA XREF: sub_401050+744To
.rdata:00438315 align 4,0
.rdata:00438318 aDot db 'dot',0 ; DATA XREF: sub_401050+780To
.rdata:0043831C aDotm db 'dotm',0 ; DATA XREF: sub_401050+7BC0To
.rdata:00438321 align 4,0
.rdata:00438324 aDotx db 'dotx',0 ; DATA XREF: sub_401050+7F8To
.rdata:00438329 align 4,0
.rdata:0043832C aXlsm db 'xlsm',0 ; DATA XREF: sub_401050+834To
.rdata:00438331 align 4,0
.rdata:00438334 aXlsb db 'xlsb',0 ; DATA XREF: sub_401050+870To
.rdata:00438339 align 4,0
.rdata:0043833C aXlw db 'xlw',0 ; DATA XREF: sub_401050+8A0To
.rdata:00438340 aXlt db 'xlt',0 ; DATA XREF: sub_401050+907To
.rdata:00438344 aXlm db 'xlm',0 ; DATA XREF: sub_401050+917To
```

تصویر ۲: بخشی از فایل‌های مورد هدف باج‌افزار

قطعه کد زیر مربوط به ایجاد فایل key..... و قرار دادن آن در دایرکتوری %appdata% می‌باشد:

```
IDA View-A Hex View-1 Structures Enums
.text:00402860 sub_402860 proc near ; DATA XREF: .rdata:0042C1D8J
.text:00402860 push esi
.text:00402861 push offset aappdata ; "appdata"
.text:00402866 call sub_4150B4
.text:0040286B add esp, 4
.text:0040286E mov ecx, offset dword_45D6D0
.text:00402873 mov esi, eax
.text:00402875 call sub_40A900
.text:0040287A mov dword_45D6E4, 0Fh
.text:00402884 mov dword_45D6E0, 0
.text:00402889 mov byte ptr dword_45D6D0, 0
.text:00402895 cmp byte ptr [esi], 0
.text:00402898 jnz short loc_40289E
.text:0040289A xor ecx, ecx
.text:0040289C jmp short loc_4028AC
;
.text:0040289E loc_40289E: mov ecx, esi ; CODE XREF: sub_402860+38fj
.text:004028A0 lea edx, [ecx+1]
.text:004028A3 loc_4028A3: mov al, [ecx] ; CODE XREF: sub_402860+48lj
.text:004028A5 inc ecx
.text:004028A6 test al, al
.text:004028A8 jnz short loc_4028A3
.text:004028AA sub ecx, edx
.text:004028AC loc_4028AC: ; CODE XREF: sub_402860+3cfj
.text:004028AD push ecx
.text:004028AE push esi
.text:004028AF mov ecx, offset dword_45D6D0
.text:004028B3 call sub_408A60
.text:004028B8 push offset sub_42B2E0
.text:004028BD call sub_40CC64
.text:004028C2 add esp, 4
.text:004028C5 pop esi
.text:004028C6 sub_402860 retn
;
.text:004028C7 align 10h
; ===== S U B R O U T I N E =====
.text:004028D0 sub_4028D0 proc near ; DATA XREF: .rdata:0042C1DCJ
.text:004028D5 push offset a000000000_key ; "\\0000000000.key"
.text:004028DA mov edx, offset dword_45D6D0
.text:004028DF call sub_40A580
.text:004028E4 push offset sub_42B370
.text:004028E9 call sub_40CC64
.text:004028EE add esp, 8
.text:004028F1 sub_4028D0 retn
;
00001c60 00402860: sub_402860
```

قطعه کد زیر مربوط به بررسی منطقه زمانی کاربران می باشد و به نظر می رسد باج افزار از آن برای هدف قرار دادن کاربرانی خاص استفاده می کند :

```
.text:00420BF0 mov edi, edi
.text:00420BF2 push ebp
.text:00420BF3 mov ebp, esp
.text:00420BF5 sub esp, 10h
.text:00420BF8 push ebx
.text:00420BF9 push esi
.text:00420BFA call sub_42065A
.text:00420BFF mov esi, eax
.text:00420C01 xor ebx, ebx
.text:00420C03 lea eax, [ebp+var_4]
.text:00420C06 mov [ebp+var_4], ebx
.text:00420C09 push eax
.text:00420C0A mov [ebp+var_8], ebx
.text:00420C0D mov [ebp+var_C], ebx
.text:00420C10 call sub_4206B8
.text:00420C15 pop ecx
.text:00420C16 test eax, eax
.text:00420C18 jnz loc_420D40
.text:00420C1E lea eax, [ebp+var_8]
.text:00420C21 push eax
.text:00420C22 call sub_420660
.text:00420C27 pop ecx
.text:00420C28 test eax, eax
.text:00420C2A jnz loc_420D40
.text:00420C30 lea eax, [ebp+var_C]
.text:00420C33 push eax
.text:00420C34 call sub_42068C
.text:00420C39 pop ecx
.text:00420C3A test eax, eax
.text:00420C3C jnz loc_420D40
.text:00420C42 push dword_45D514 ; lpMem
.text:00420C48 call sub_416035
.text:00420C4D mov dword_45D514, ebx
.text:00420C53 mov [esp+1Ch+lpTimeZoneInformation], offset TimeZoneInformation ; lpTimeZoneInformation
.text:00420C5A call ds:GetTimeZoneInformation
.text:00420C60 cmp eax, 0FFFFFFFh
.text:00420C63 jz loc_420D1C
.text:00420C69 imul ecx, TimeZoneInformation.Bias, 3Ch
.text:00420C70 mov edx, TimeZoneInformation.StandardBias
.text:00420C76 push edi
.text:00420C77 xor edi, edi
.text:00420C79 inc edi
.text:00420C7A mov dword_45D518, edi
.text:00420C7D mov [ebp+var_4], ecx
.text:00420C80 mov ebx, TimeZoneInformation.StandardDate.uMonth, bx
.text:00420C83 cmp ebx, short loc_420C94
.text:00420C8A jz short loc_420C94
.text:00420C8C imul eax, edx, 3Ch
.text:00420C8F add ecx, eax
.text:00420C91 mov [ebp+var_4], ecx
.text:00420C94 loc_420C94:
.text:00420C94 mov [esp+1Ch+lpTimeZoneInformation], offset TimeZoneInformation ; CODE XREF: sub_420BF0+9Atj
.text:00420C97 cmp ebx, short loc_420C83
.text:00420C99 jz short loc_420C83
.text:00420C9B mov eax, TimeZoneInformation.DaylightBias
.text:00420CA2 test eax, eax
.text:00420CA4 jz short loc_420C83
.text:00420CA6 sub ebx, eax
.text:00420CA8 mov [ebp+var_8], edi
0001FFF2 00420BF2: sub_420BF0+2
```

این باج افزار از کتابخانه های ویندوزی به همراه توابعی از هر کدام از کتابخانه ها استفاده می کند، در تصویر، استفاده از این کتابخانه ها به خوبی قابل مشاهده است، همچنین لیست کامل این کتابخانه ها به همراه توابع مورد استفاده نیز در ادامه ی متن آمده است.

```
.idata:0042C000 Imports from ADVAPI32.dll
-----
.idata:0042C000 Segment type: Externs
.idata:0042C000 .idata
.idata:0042C000 LSTATUS __stdcall RegCreateKeyEx(HKEY hKey, LPCWSTR lpSubKey, DWORD Reserved, LPCWSTR lpClass, DWORD dwOptions, REGSAM samDesired, const LPSECURITY_ATTRIBUTES lp
    extrn RegCreateKeyEx: dword ; CODE XREF: sub_404280+AA1p
    ; DATA XREF: sub_404280+111p
.idata:0042C004 LSTATUS __stdcall RegSetValueEx(HKEY hKey, LPCWSTR lpValueName, DWORD dwType, const BYTE *lpData, DWORD cbData)
    extrn RegSetValueEx: dword ; CODE XREF: sub_404280+F11p
    ; DATA XREF: sub_404280+111p
.idata:0042C008 LSTATUS __stdcall RegOpenKeyEx(HKEY hKey, LPCWSTR lpSubKey, DWORD ulOptions, REGSAM samDesired, PHKEY phkResult)
    extrn RegOpenKeyEx: dword ; CODE XREF: sub_405A70+681p
    ; DATA XREF: sub_405A70+681p
.idata:0042C00C LSTATUS __stdcall RegDeleteValue(HKEY hKey, LPCWSTR lpValueName)
    extrn RegDeleteValue: dword ; CODE XREF: sub_405A70+781p
    ; DATA XREF: sub_405A70+781p
.idata:0042C010 LSTATUS __stdcall RegCloseKey(HKEY hKey)
    extrn RegCloseKey: dword ; CODE XREF: sub_404280+1091p
    ; sub_405A70+851p
    ; DATA XREF: ...
.idata:0042C018 Imports from KERNEL32.dll
.idata:0042C018 .idata
.idata:0042C018 DWORD __stdcall GetLogicalDriveStringsA(DWORD nBufferLength, LPSTR lpBuffer)
    extrn GetLogicalDriveStringsA: dword
    ; CODE XREF: sub_4058A0+701p
    ; DATA XREF: sub_4058A0+701p
.idata:0042C01C BOOL __stdcall FindClose(HANDLE hFindFile)
    extrn FindClose: dword ; CODE XREF: sub_405680+1011p
    ; sub_42113D+D61p
    ; DATA XREF: ...
.idata:0042C020 SIZE_T __stdcall HeapSize(HANDLE hHeap, DWORD dwFlags, LPCVOID lpMem)
    extrn HeapSize: dword ; CODE XREF: sub_428873+281p
    ; DATA XREF: sub_428873+281p
.idata:0042C024 BOOL __stdcall ReadConsole(HANDLE hConsoleInput, LPVOID lpBuf, DWORD nNumberOfCharsToRead, LPDWORD lpNumberOfCharsRead, PCONSOLE_READCONSOLE_CONTROL lpInpu
    extrn ReadConsole: dword ; CODE XREF: sub_425C1C+2B01p
    ; DATA XREF: sub_425C1C+2B01p
.idata:0042C028 int __stdcall lstrlenA(LPCSTR lpString)
    extrn lstrlenA: dword ; CODE XREF: sub_4058A0+9C1p
    ; DATA XREF: sub_4058A0+941p
.idata:0042C02C BOOL __stdcall FindNextFile(HANDLE hFindFile, LPWIN32_FIND_DATA lpFindFileData)
    extrn FindNextFile: dword ; CODE XREF: sub_405680+1C21p
    ; sub_42113D+1111p
    ; DATA XREF: ...
.idata:0042C030 DWORD __stdcall GetModuleFileNameW(HMODULE hModule, LPWSTR lpFileName, DWORD nSize)
    extrn GetModuleFileNameW: dword ; CODE XREF: sub_405A70+261p
    ; DATA XREF: sub_405A70+261p
.idata:0042C034 UINT __stdcall GetDriveType(LPCSTR lpRootPathName)
    extrn GetDriveType: dword ; CODE XREF: sub_4058A0+911p
    ; DATA XREF: sub_4058A0+7E1p
```

ADVAPI۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll
RegCreateKeyExW	GetStdHandle	FindClose	TlsAlloc	HeapSize
RegOpenKeyExA	GetDriveTypeW	TlsGetValue	FlushFileBuffers	RaiseException
RegDeleteValueA	FileTimeToSystemTime	GetFullPathNameW	RtlUnwind	TlsFree
RegCloseKey	GetDriveTypeA	SetLastError	FreeLibrary	ReadFile
RegSetValueExW	SetEndOfFile	PeekNamedPipe	GetStartupInfoW	CloseHandle
	EncodePointer	IsDebuggerPresent	GetUserDefaultLCID	IsValidCodePage
	SystemTimeToTzSpecificLocalTime	HeapAlloc	GetProcessHeap	ResetEvent
	DeleteCriticalSection	GetModuleFileNameA	CompareStringW	FindNextFileA
	GetCurrentProcess	EnumSystemLocalesW	FindFirstFileExA	IsValidLocale
	GetConsoleMode	LoadLibraryExW	FindFirstFileA	GetProcAddress
	UnhandledExceptionFilter	MultiByteToWideChar	ExitProcess	CreateEventW
	FreeEnvironmentStringsW	SetFilePointerEx	LeaveCriticalSection	CreateFileW
	InitializeSListHead	MoveFileExW	GetLastError	GetFileType
	GetLocaleInfoW	DecodePointer	LCMapStringW	TlsSetValue
	GetLogicalDriveStringsA	TerminateProcess	lstrlenA	SetStdHandle
	GetTimeZoneInformation	ReadConsoleW	GetConsoleCP	GetCPIInfo
	QueryPerformanceCounter	GetCurrentThreadId	WaitForSingleObjectEx	WriteFile
	GetModuleHandleExW	WriteConsoleW	GetCurrentDirectoryW	
	SetEnvironmentVariableA	InitializeCriticalSection	GetCurrentProcessId	
	IsProcessorFeaturePresent	AndSpinCount	GetCommandLineW	
	SetUnhandledExceptionFilter	HeapFree	WideCharToMultiByte	
	GetModuleFileNameW	EnterCriticalSection	GetSystemTimeAsFileTime	
	GetEnvironmentStringsW	SetEvent	HeapReAlloc	
	GetACP	GetModuleHandleW	GetStringTypeW	
		GetCommandLineA	GetOEMCP	

بر اساس بررسی‌های صورت گرفته، این باج‌افزار پس از اجرا فقط یک فرایند ایجاد می‌کند :

- Ransom.exe

پس از خاتمه فرایند مربوط به باج‌افزار فرایند notepad.exe ایجاد می‌شود و پیغام باج‌خواهی به نمایش در می‌آید.

کلیدهای رجیستری زیر توسط باج‌افزار در سیستم باز می‌شوند :

۱.	<i> Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\ImageFileExecutionOptions\996E.exe</i>
۲.	<i> Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option</i>
۳.	<i> Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers</i>
۴.	<i> REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodelIdentifiers\TransparentEnabled</i>
۵.	<i> REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers</i>

طبق بررسی‌های انجام شده مهاجمین از کلید شماره ۱ جهت قابلیت توسعه دادن به باج‌افزار استفاده نموده‌اند و کلید شماره ۳ نیز جهت پیاده سازی سیاست‌های محدودیت نرم‌افزار استفاده شده است.

کلید رجیستری زیر توسط باج افزار در سیستم تنظیم می شود :

\\REGISTRY\\USER\\S-1-5-21-1482476501-1645522239-1417001333-500\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\MSFEEEditor

قطعه کد زیر مربوط به تنظیم شدن این کلید می باشد که برای اجرای دائمی و در هر بار اجرای سیستم از آن استفاده می شود و نام فایل مورد استفاده که در قسمت Run رجیستری ثبت می شود MSFEEEditor می باشد :

```

.text:00404307 add esp, 3Ch
.text:0040430A lea eax, [ebp+phkResult]
.text:00404310 push 0 ; lpdwDisposition
.text:00404312 push eax ; phkResult
.text:00404313 push 0 ; lpSecurityAttributes
.text:00404315 push 2001Fh ; samDesired
.text:0040431A push 0 ; dwOptions
.text:0040431C push 0 ; lpClass
.text:0040431E push 0 ; Reserved
.text:00404320 push offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVe"...
.text:00404325 push 80000001h ; hKey
.text:0040432A call ds:RegCreateValueEx ; const MCHAR SubKey ; DATA XREF: sub_404280+80f0
.text:00404330 mov esi, eax ; SubKey: unicode 0, <Software\\Microsoft\\Windows\\CurrentVersion\\Run>,0
.text:00404332 neg esi
.text:00404334 sbb esi, esi
.text:00404336 add esi, 1
.text:00404339 jz short loc_40437E
.text:0040433B lea ecx, [ebp+Data]
.text:00404341 lea edx, [ecx+2]
.text:00404344 loc_404344: ; CODE XREF: sub_404280+CD4j
.text:00404344 mov ax, [ecx]
.text:00404347 add ecx, 2
.text:0040434A test ax, ax
.text:0040434D jnz short loc_404344
.text:0040434F sub ecx, edx
.text:00404351 sar ecx, 1
.text:00404353 lea eax, ds:2[ecx*2]
.text:0040435A push eax ; cbData
.text:0040435B lea eax, [ebp+Data]
.text:00404361 push eax ; lpData
.text:00404362 push 1 ; dwType
.text:00404364 push 0 ; Reserved
.text:00404366 push offset ValueName ; "MSFEEEditor"
.text:0040436B push [ebp+phkResult] ; hKey
.text:00404371 call ds:RegSetValueEx
.text:00404377 mov esi, eax
.text:00404379 neg esi
.text:0040437B sbb esi, esi
.text:0040437D inc esi
.text:0040437E loc_40437E: ; CODE XREF: sub_404280+B9Tj
.text:0040437E mov eax, [ebp+phkResult]
.text:00404384 test eax, eax
.text:00404386 jz short loc_40438F
.text:00404388 push eax ; hKey
.text:00404389 call ds:RegCloseKey
.text:0040438F loc_40438F: ; CODE XREF: sub_404280+106Tj
.text:0040438F mov ecx, [ebp+var_4]
.text:00404392 mov eax, esi
.text:00404394 xor ecx, ebp
.text:00404396 pop esi
.text:00404397 call sub_40C4A6
.text:0040439C mov esp, ebp
.text:0040439E pop ebp
.text:0040439F retn
.text:0040439F sub_404280 endp
0000370A 0040430A: sub_404280+8A
    
```

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 باج افزار AnimusLocker نشدیم.

خروجی سامانه VirusTotal :





در حال حاضر تعداد ۵۰ مورد از ۶۷ 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.31018237	AegisLab	W32.Troj.Ransom.Filecoderic
ALYac	Trojan.Ransom.AnimusLocker	Antiy-AVL	Trojan(Dropper)/Win32.Dorgam
Arcabit	Trojan.Generic.D1D94CFD	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.GenericKD.31018237	CAT-QuickHeal	Trojan.Genasom
ClamAV	Win.Trojan.Agent-6595906-0	Comodo	TrojWare.Win32.Filecoder.-NNP
CrowdStrike Falcon	malicious_confidence_100% (W)	Cylance	Unsafe
Cyren	W32/Trojan.YKJD-1659	DrWeb	Trojan.Encoder.25651
Emsisoft	Trojan.GenericKD.31018237 (B)	Endgame	malicious (moderate confidence)
eScan	Trojan.GenericKD.31018237	ESET-NOD32	a variant of Win32/Filecoder.NNP
F-Secure	Trojan.GenericKD.31018237	Fortinet	W32/Filecoder.NNP!tr
GData	Win32.Trojan-Ransom.Filecoder.P@gen	Ikarus	Trojan-Ransom.FileCoder
Jiangmin	TrojanDropper.Dorgam.ry	K7AntiVirus	Trojan (005173491)
K7GW	Trojan (005173491)	Kaspersky	Trojan-Dropper.Win32.Dorgam.xiy
Malwarebytes	Ransom.FileCryptor	MAX	malware (ai score=94)
McAfee	Generic.dvr	McAfee-GW-Edition	BehavesLike.Win32.PUPXBE.fc
Microsoft	Trojan:Win32/Occamy.C	NANO-Antivirus	Trojan.Win32.Dorgam.feapqk
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	HEUR/QVM10.2.2661.Malware.Gen	Rising	Trojan.Filecoder!8.68 (CLOUD)
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Trojan Horse
Tencent	Win32.Trojan.Filecoder.Tbii	TrendMicro	Ransom_ANIMUS.THGOBAH
TrendMicro-HouseCall	Ransom_ANIMUS.THGOBAH	VBA32	TrojanDropper.Dorgam
Webroot	W32.Trojan.Gen	Yandex	Trojan.DR.Dorgam!tdFIMgVG6fk
Zillya	Dropper.Dorgam.Win32.951	ZoneAlarm	Trojan-Dropper.Win32.Dorgam.xiy

خروجی سامانه ویروس کاو مرکز ماهر :

در حال حاضر تعداد ۸ 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 AnimusLocker.exe

آنتی ویروس	نسخه آنتی ویروس	نتیجه اسکن
پادوبش	2.3.190.2675	
sophos	9.14.2	
f_secure	11.00	
kaspersky	5.5	
eset	4.5.3.38121	
drweb	11.0.1.1607061217	
clam_av	0.99.2	
comodo	1.1.268025.1	
bitdefender	11.0.1.18	
avast	2.1.2	
symantec	7.9.0.30	