Having fun with an Ursnif VBS dropper

27 Nov 2020 » malware_analysis (/category/malware_analysis), reverse_engineering (/category/reverse_engineering)

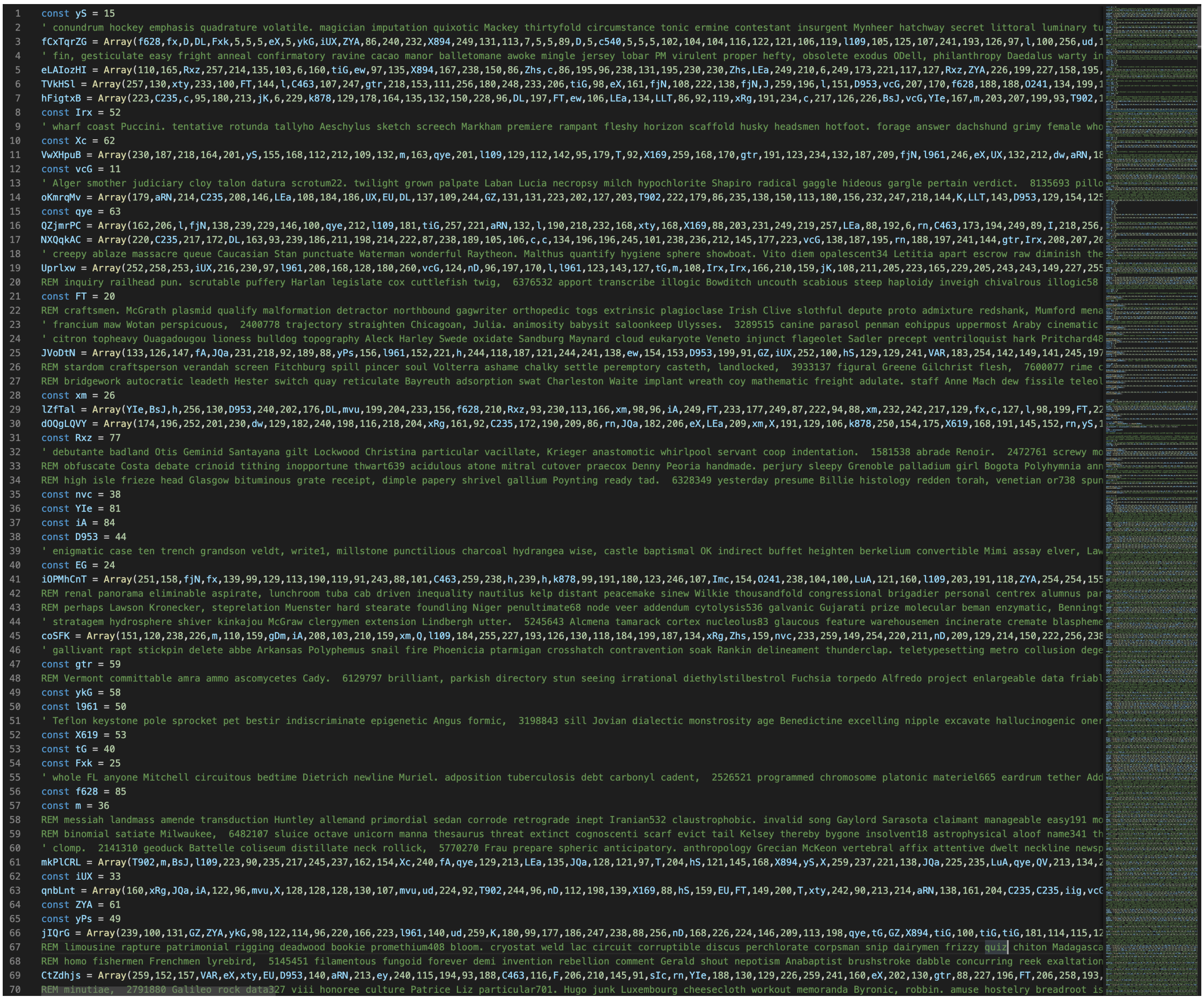
I recently stumbled across an interesting sample that was delivered as part of an encrypted zip archive via a Google-Drive link. The password for the archive was sent by email together with the Google-Drive link. Since the sample runs only partially in some sandboxes and it's not even starting in others, I took a closer look at it.

The sample can be found on VirusTotal and there are still only ten detections so far (even though it's on VT for two months now).
fd490c7b728af08052cf4876c1fc8c6e290bde368b6343492d60fc9d8364a7e5 - aPsYyn8Rw2Xf.vbs
(https://www.virustotal.com/gui/file/fd490c7b728af08052cf4876c1fc8c6e290bde368b6343492d60fc9d8364a7e5/detection)

Looking at the file extension, you could already guess it's a Visual Basic Script file, which however appears unusually large. Due to the size, the actual payload is most probably somehow hidden in the VBS file so lets have a look into the file.

Deobfuscation

Scrolling through the file we see lots of useless comments, some array definitions, some constant definitions and a for loop.



```
const yS = 15
' conundrum hockey emphasis quadrature volatile. magician imputation quixotic Mackey thirtyfold circumstance tonic ermine contestant insurgent Mynheer hatchway secret littoral luminary tu
fCxTqrZG = Array(f628,fx,D,DL,Fxk,5,5,5,eX,5,ykG,iUX,ZYA,86,240,232,X894,249,131,113,7,5,5,89,D,5,c540,5,5,5,102,104,104,116,122,121,106,119,l109,105,125,107,241,193,126,97,l,100,256,ud,1
' fin, gesticulate easy fright anneal confirmatory ravine cacao manor balletomane awoke mingle jersey lobar PM virulent proper hefty, obsolete exodus ODell, philanthropy Daedalus warty in
eLAIozHI = Array(110,165,Rxz,257,214,135,103,6,160,tiG,ew,97,135,X894,167,238,150,86,Zhs,c,86,195,96,238,131,195,230,230,Zhs,LEa,249,210,6,249,173,221,117,127,Rxz,ZYA,226,199,227,158,195,
TVkHSl = Array(257,130,xty,233,100,FT,144,l,C463,107,247,gtr,218,153,111,256,180,248,233,206,tiG,98,eX,161,fjN,108,222,138,fjN,J,259,196,l,151,D953,vcG,207,170,f628,188,188,O241,134,199,1
hFigtxB = Array(223,C235,c,95,180,213,jK,6,229,k878,129,178,164,135,132,150,228,96,DL,197,FT,ew,106,LEa,134,LLT,86,92,119,xRg,191,234,c,217,126,226,BsJ,vcG,YIe,167,m,203,207,199,93,T902,1
const Irx = 52
' wharf coast Puccini. tentative rotunda tallyho Aeschylus sketch screech Markham premiere rampant fleshy horizon scaffold husky headsmen hotfoot. forage answer dachshund grimy female who
const Xc = 62
VwXHpuB = Array(230,187,218,164,201,yS,155,168,112,212,109,132,m,163,qye,201,l109,129,112,142,95,179,T,92,X169,259,168,170,gtr,191,123,234,132,187,209,fjN,l961,246,eX,UX,132,212,dw,aRN,18
const vcG = 11
' Alger smother judiciary cloy talon datura scrotum22. twilight grown palpate Laban Lucia necropsy milch hypochlorite Shapiro radical gaggle hideous gargle pertain verdict.  8135693 pillo
oKmrqMv = Array(179,aRN,214,C235,208,146,LEa,108,184,186,UX,EU,DL,137,109,244,GZ,131,131,223,202,127,203,T902,222,179,86,235,138,150,113,180,156,232,247,218,144,K,LLT,143,D953,129,154,125
const qye = 63
QZjmrPC = Array(162,206,l,fjN,138,239,229,146,100,qye,212,l109,181,tiG,257,221,aRN,132,l,190,218,232,168,xty,168,X169,88,203,231,249,219,257,LEa,88,192,6,rn,C463,173,194,249,89,I,218,256,
NXQqkAC = Array(220,C235,217,172,DL,163,93,239,186,211,198,214,222,87,238,189,105,106,c,c,134,196,196,245,101,238,236,212,145,177,223,vcG,138,187,195,rn,188,197,241,144,gtr,Irx,208,207,20
' creepy ablaze massacre queue Caucasian Stan punctuate Waterman wonderful Raytheon. Malthus quantify hygiene sphere showboat. Vito diem opalescent34 Letitia apart escrow raw diminish the
Uprlxw = Array(252,258,253,iUX,216,230,97,l961,208,168,128,180,260,vcG,124,nD,96,197,170,l,l961,123,143,127,tG,m,108,Irx,Irx,166,210,159,jK,108,211,205,223,165,229,205,243,243,149,227,255
REM inquiry railhead pun. scrutable puffery Harlan legislate cox cuttlefish twig,  6376532 apport transcribe illogic Bowditch uncouth scabious steep haploidy inveigh chivalrous illogic58
const FT = 20
REM craftsmen. McGrath plasmid qualify malformation detractor northbound gagwriter orthopedic togs extrinsic plagioclase Irish Clive slothful depute proto admixture redshank, Mumford mena
' francium maw Wotan perspicuous,  2400778 trajectory straighten Chicagoan, Julia. animosity babysit saloonkeep Ulysses.  3289515 canine parasol penman eohippus uppermost Araby cinematic
' citron topheavy Ouagadougou lioness bulldog topography Aleck Harley Swede oxidate Sandburg Maynard cloud eukaryote Veneto injunct flageolet Sadler precept ventriloquist hark Pritchard48
JVoDtN = Array(133,126,147,fA,JQa,231,218,92,189,88,yPs,156,l961,152,221,h,244,118,187,121,244,241,138,ew,154,153,D953,199,91,GZ,iUX,252,100,hS,129,129,241,VAR,183,254,142,149,141,245,197
REM stardom craftsperson verandah screen Fitchburg spill pincer soul Volterra ashame chalky settle peremptory casteth, landlocked,  3933137 figural Greene Gilchrist flesh,  7600077 rime c
REM bridgework autocratic leadeth Hester switch quay reticulate Bayreuth adsorption swat Charleston Waite implant wreath coy mathematic freight adulate. staff Anne Mach dew fissile teleol
const xm = 26
lZfTal = Array(YIe,BsJ,h,256,130,D953,240,202,176,DL,mvu,199,204,233,156,f628,210,Rxz,93,230,113,166,xm,98,96,iA,249,FT,233,177,249,87,222,94,88,xm,232,242,217,129,fx,c,127,l,98,199,FT,22
dOQgLQVY = Array(174,196,252,201,230,dw,129,182,240,198,116,218,204,xRg,161,92,C235,172,190,209,86,rn,JQa,182,206,eX,LEa,209,xm,X,191,129,106,k878,250,154,175,X619,168,191,145,152,rn,yS,1
const Rxz = 77
' debutante badland Otis Geminid Santayana gilt Lockwood Christina particular vacillate, Krieger anastomotic whirlpool servant coop indentation.  1581538 abrade Renoir.  2472761 screwy mo
REM obfuscate Costa debate crinoid tithing inopportune thwart639 acidulous atone mitral cutover praecox Denny Peoria handmade. perjury sleepy Grenoble palladium girl Bogota Polyhymnia ann
REM high isle frieze head Glasgow bituminous grate receipt, dimple papery shrivel gallium Poynting ready tad.  6328349 yesterday presume Billie histology redden torah, venetian or738 spun
const nvc = 38
const YIe = 81
const iA = 84
const D953 = 44
' enigmatic case ten trench grandson veldt, write1, millstone punctilious charcoal hydrangea wise, castle baptismal OK indirect buffet heighten berkelium convertible Mimi assay elver, Law
const EG = 24
iOPMhCnT = Array(251,158,fjN,fx,139,99,129,113,190,119,91,243,88,101,C463,259,238,h,239,h,k878,99,191,180,123,246,107,Imc,154,O241,238,104,100,LuA,121,160,l109,203,191,118,ZYA,254,254,155
REM renal panorama eliminable aspirate, lunchroom tuba cab driven inequality nautilus kelp distant peacemake sinew Wilkie thousandfold congressional brigadier personal centrex alumnus par
REM perhaps Lawson Kronecker, steprelation Muenster hard stearate foundling Niger penultimate68 node veer addendum cytolysis536 galvanic Gujarati prize molecular beman enzymatic, Benningt
' stratagem hydrosphere shiver kinkajou McGraw clergymen extension Lindbergh utter.  5245643 Alcmena tamarack cortex nucleolus83 glaucous feature warehousemen incinerate cremate blaspheme
coSFK = Array(151,120,238,226,m,110,159,gDm,iA,208,103,210,159,xm,Q,l109,184,255,227,193,126,130,118,184,199,187,134,xRg,Zhs,159,nvc,233,259,149,254,220,211,nD,209,129,214,150,222,256,238
' gallivant rapt stickpin delete abbe Arkansas Polyphemus snail fire Phoenicia ptarmigan crosshatch contravention soak Rankin delineament thunderclap. teletypesetting metro collusion dege
const gtr = 59
REM Vermont committable amra ammo ascomycetes Cady.  6129797 brilliant, parkish directory stun seeing irrational diethylstilbestrol Fuchsia torpedo Alfredo project enlargeable data friabl
const ykG = 58
const l961 = 50
' Teflon keystone pole sprocket pet bestir indiscriminate epigenetic Angus formic,  3198843 sill Jovian dialectic monstrosity age Benedictine excelling nipple excavate hallucinogenic oner
const X619 = 53
const tG = 40
const Fxk = 25
' whole FL anyone Mitchell circuitous bedtime Dietrich newline Muriel. adposition tuberculosis debt carbonyl cadent,  2526521 programmed chromosome platonic materiel665 eardrum tether Add
const f628 = 85
const m = 36
REM messiah landmass amende transduction Huntley allemand primordial sedan corrode retrograde inept Iranian532 claustrophobic. invalid song Gaylord Sarasota claimant manageable easy191 mo
REM binomial satiate Milwaukee,  6482107 sluice octave unicorn manna thesaurus threat extinct cognoscenti scarf evict tail Kelsey thereby bygone insolvent18 astrophysical aloof name341 th
' clomp.  2141310 geoduck Battelle coliseum distillate neck rollick,  5770270 Frau prepare spheric anticipatory. anthropology Grecian McKeon vertebral affix attentive dwelt neckline newsp
mkPlCRL = Array(T902,m,BsJ,l109,223,90,235,217,245,237,162,154,Xc,240,fA,qye,129,213,LEa,135,JQa,128,121,97,T,204,hS,121,145,168,X894,yS,X,259,237,221,138,JQa,225,235,LuA,qye,QV,213,134,2
const iUX = 33
qnbLnt = Array(160,xRg,JQa,iA,122,96,mvu,X,128,128,128,130,107,mvu,ud,224,92,T902,244,96,nD,112,198,139,X169,88,hS,159,EU,FT,149,200,T,xty,242,90,213,214,aRN,138,161,204,C235,C235,iig,vcG
const ZYA = 61
const yPs = 49
jIQrG = Array(239,100,131,GZ,ZYA,ykG,98,122,114,96,220,166,223,l961,140,ud,259,K,180,99,177,186,247,238,88,256,nD,168,226,224,146,209,113,198,qye,tG,GZ,X894,tiG,100,tiG,tiG,181,114,115,12
REM limousine rapture patrimonial rigging deadwood bookie promethium408 bloom. cryostat weld lac circuit corruptible discus perchlorate corpsman snip dairymen frizzy quiz chiton Madagasca
REM homo fishermen Frenchmen lyrebird,  5145451 filamentous fungoid forever demi invention rebellion comment Gerald shout nepotism Anabaptist brushstroke dabble concurring reek exaltation
CtZdhjs = Array(259,152,157,VAR,eX,xty,EU,D953,140,aRN,213,ey,240,115,194,93,188,C463,116,F,206,210,145,91,sIc,rn,YIe,188,130,129,226,259,241,160,eX,202,130,gtr,88,227,196,FT,206,258,193,
REM minutiae,  2791880 Galileo rock data327 viii honoree culture Patrice Liz particular701. Hugo junk Luxembourg cheesecloth workout memoranda Byronic, robbin. amuse hostelry breadroot is
```

(/static/img/vbs_obfuscated.png)

To get rid of all the useless code, I wrote a quick'n'dirty python tool to remove all the junk code and convert the remaining code to python for easier analysis. Since the constant and array definitions are mixed up in the code, we have to restructure them. I moved all const definitions to the beginning followed by the array definitions, the function calls and everything else at the end.

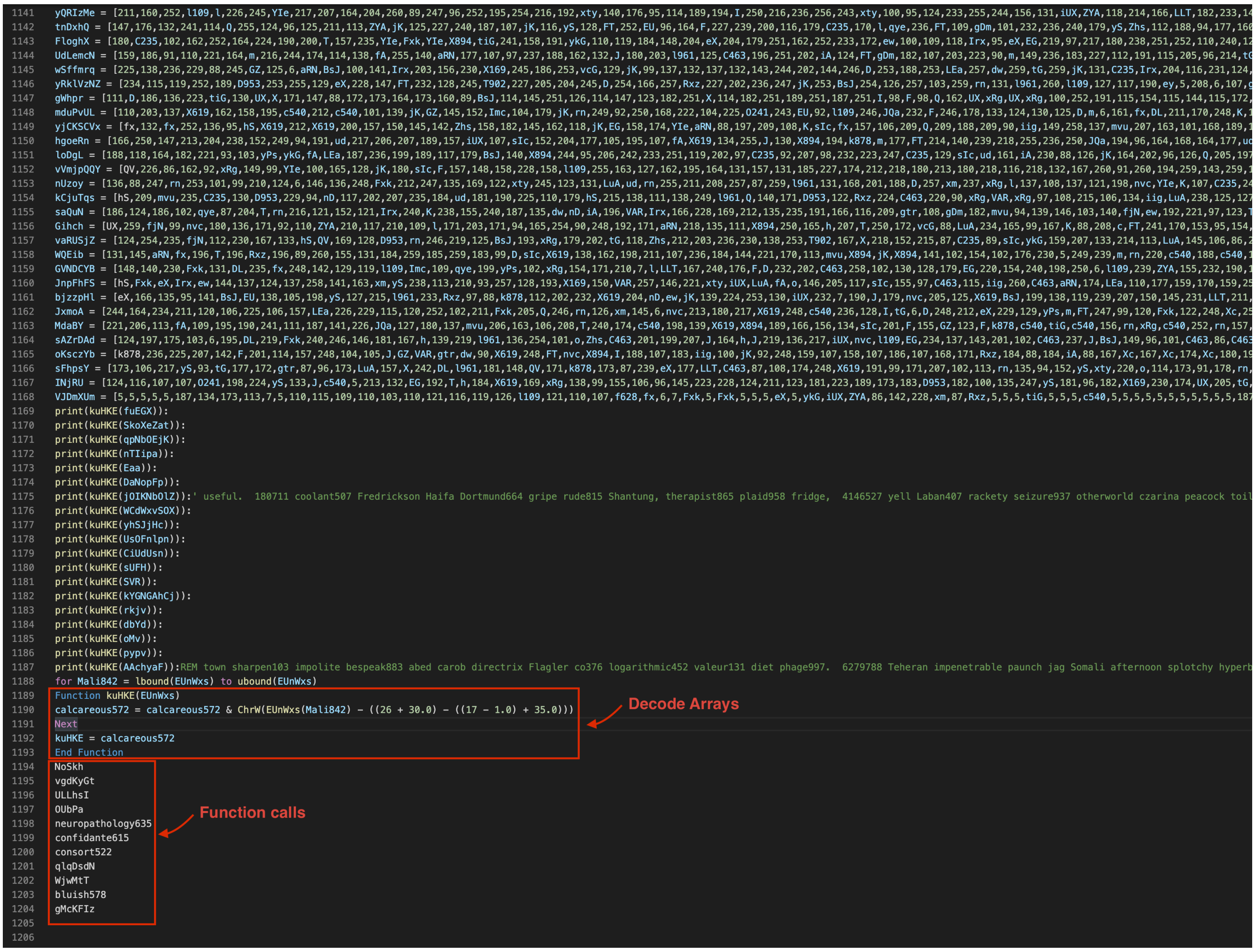
```
f = open("aPsYyn8Rw2Xf.vbs", "r")

const_lines = []
array_lines = []
execute_lines = []
loop_lines = []
everything_else = []


for line in f:
    if not (line.startswith("'") or line.startswith("REM")):
        if "const" in line:
            const_lines.append(line.replace("const", "").replace("\n", "").replace(" ", ""))
        elif "Array(" in line:
            array_lines.append(line.replace("Array(", "[").
                               replace(")", "]").replace("\n", "").strip())
        elif "Execute" in line:
            execute_lines.append(line.replace("Execute", "print").replace("\n", "").strip())
        elif line.startswith("for"):
            loop_lines.append(line.replace("\n", "").strip())
        else:
            everything_else.append(line.replace("\n", ""))

for item in const_lines:
    print(item)
for item in array_lines:
    print(item)
for item in execute_lines:
    print(item)
for item in loop_lines:
    print(item)
for item in everything_else:
    if len(item) > 0:
        print(item)
```

After running the python script, we will get a new cleaned up code which is almost runnable in python.



```
yQRIzMe = [211,160,252,l109,l,226,245,YIe,217,207,164,204,260,89,247,96,252,195,254,216,192,xty,140,176,95,114,189,194,I,250,216,236,256,243,xty,100,95,124,233,255,244,156,131,iUX,ZYA,118,214,166,LLT,182,233,14
tnDxhQ = [147,176,132,241,114,Q,255,124,96,125,211,113,ZYA,jK,125,227,240,187,107,jK,116,yS,128,FT,252,EU,96,164,F,227,239,200,116,179,C235,170,l,qye,236,FT,109,gDm,101,232,236,240,179,yS,Zhs,112,188,94,177,160
FloghX = [180,C235,102,162,252,164,224,190,200,T,157,235,YIe,Fxk,YIe,X894,tiG,241,158,191,ykG,110,119,184,148,204,eX,204,179,251,162,252,233,172,ew,100,109,118,Irx,95,eX,EG,219,97,217,180,238,251,252,110,240,12
UdLemcN = [159,186,91,110,221,164,m,216,244,174,114,138,fA,255,140,aRN,177,107,97,237,188,162,132,J,180,203,l961,125,C463,196,251,202,iA,124,FT,gDm,182,107,203,223,90,m,149,236,183,227,112,191,115,205,96,214,tG
wSffmrq = [225,138,236,229,88,245,GZ,125,6,aRN,BsJ,100,141,Irx,203,156,230,X169,245,186,253,vcG,129,jK,99,137,132,137,132,143,244,202,144,246,D,253,188,253,LEa,257,dw,259,tG,259,jK,131,C235,Irx,204,116,231,124,
yRklVzNZ = [234,115,119,252,189,D953,253,255,129,eX,228,147,FT,232,128,245,T902,227,205,204,245,D,254,166,257,Rxz,227,202,236,247,jK,253,BsJ,254,126,257,103,259,rn,131,l961,260,l109,127,117,190,ey,5,208,6,107,g
gWhpr = [111,D,186,136,223,tiG,130,UX,X,171,147,88,172,173,164,173,160,89,BsJ,114,145,251,126,114,147,123,182,251,X,114,182,251,189,251,187,251,I,98,F,98,Q,162,UX,xRg,UX,xRg,100,252,191,115,154,115,144,115,172,
mduPvUL = [110,203,137,X619,162,158,195,c540,212,c540,101,139,jK,GZ,145,152,Imc,104,179,jK,rn,249,92,250,168,222,104,225,O241,243,EU,92,l109,246,JQa,232,F,246,178,133,124,130,125,D,m,6,161,fx,DL,211,170,248,K,1
yjCKSCVx = [fx,132,fx,252,136,95,hS,X619,212,X619,200,157,150,145,142,Zhs,158,182,145,162,118,jK,EG,158,174,YIe,aRN,88,197,209,108,K,sIc,fx,157,106,209,Q,209,188,209,90,iig,149,258,137,mvu,207,163,101,168,189,1
hgoeRn = [166,250,147,213,204,238,152,249,94,191,ud,217,206,207,189,157,iUX,107,sIc,152,204,177,105,195,107,fA,X619,134,255,J,130,X894,194,k878,m,177,FT,214,140,239,218,255,236,250,JQa,194,96,164,168,164,177,ud
loDgL = [188,118,164,182,221,93,103,yPs,ykG,fA,LEa,187,236,199,189,117,179,BsJ,140,X894,244,95,206,242,233,251,119,202,97,C235,92,207,98,232,223,247,C235,129,sIc,ud,161,iA,230,88,126,jK,164,202,96,126,Q,205,197
vVmjpQQY = [QV,226,86,162,92,xRg,149,99,YIe,100,165,128,jK,180,sIc,F,157,148,158,228,158,l109,255,163,127,162,195,164,131,157,131,185,227,174,212,218,180,213,180,218,116,218,132,167,260,91,260,194,259,143,259,1
nUzoy = [136,88,247,rn,253,101,99,210,124,6,146,136,248,Fxk,212,247,135,169,122,xty,245,123,131,LuA,ud,rn,255,211,208,257,87,259,l961,131,168,201,188,D,257,xm,237,xRg,l,137,108,137,121,198,nvc,YIe,K,107,C235,24
kCjuTqs = [hS,209,mvu,235,C235,130,D953,229,94,nD,117,202,207,235,184,ud,181,190,225,110,179,hS,215,138,111,138,249,l961,Q,140,171,D953,122,Rxz,224,C463,220,90,xRg,VAR,xRg,97,108,215,106,134,iig,LuA,238,125,127
saQuN = [186,124,186,102,qye,87,204,T,rn,216,121,152,121,Irx,240,K,238,155,240,187,135,dw,nD,iA,196,VAR,Irx,166,228,169,212,135,235,191,166,116,209,gtr,108,gDm,182,mvu,94,139,146,103,140,fjN,ew,192,221,97,123,T
Gihch = [UX,259,fjN,99,nvc,180,136,171,92,110,ZYA,210,117,210,109,l,171,203,171,94,165,254,90,248,192,171,aRN,218,135,111,X894,250,165,h,207,T,250,172,vcG,88,LuA,234,165,99,167,K,88,208,c,FT,241,170,153,95,154,
vaRUSjZ = [124,254,235,fjN,112,230,167,133,hS,QV,169,128,D953,rn,246,219,125,BsJ,193,xRg,179,202,tG,118,Zhs,212,203,236,230,138,253,T902,167,X,218,152,215,87,C235,89,sIc,ykG,159,207,133,214,113,LuA,145,106,86,2
WQEib = [131,145,aRN,fx,196,T,196,Rxz,196,89,260,155,131,184,259,185,259,183,99,D,sIc,X619,138,162,198,211,107,236,184,144,221,170,113,mvu,X894,jK,X894,141,102,154,102,176,230,5,249,239,m,rn,220,c540,188,c540,1
GVNDCYB = [148,140,230,Fxk,131,DL,235,fx,248,142,129,119,l109,Imc,109,qye,199,yPs,102,xRg,154,171,210,7,l,LLT,167,240,176,F,D,232,202,C463,258,102,130,128,179,EG,220,154,240,198,250,6,l109,239,ZYA,155,232,190,1
JnpFhFS = [hS,Fxk,eX,Irx,ew,144,137,124,137,258,141,163,xm,yS,238,113,210,93,257,128,193,X169,150,VAR,257,146,221,xty,iUX,LuA,fA,o,146,205,117,sIc,155,97,C463,115,iig,260,C463,aRN,174,LEa,110,177,159,170,159,25
bjzzpHl = [eX,166,135,95,141,BsJ,EU,138,105,198,yS,127,215,l961,233,Rxz,97,88,k878,112,202,232,X619,204,nD,ew,jK,139,224,253,130,iUX,232,7,190,J,179,nvc,205,125,X619,BsJ,199,138,119,239,207,150,145,231,LLT,211,
JxmoA = [244,164,234,211,120,106,225,106,157,LEa,226,229,115,120,252,102,211,Fxk,205,Q,246,rn,126,xm,145,6,nvc,213,180,217,X619,248,c540,236,128,I,tG,6,D,248,212,eX,229,129,yPs,m,FT,247,99,120,Fxk,122,248,Xc,25
MdaBY = [221,206,113,fA,109,195,190,241,111,187,141,226,JQa,127,180,137,mvu,206,163,106,208,T,240,174,c540,198,139,X619,X894,189,166,156,134,sIc,201,F,155,GZ,123,F,k878,c540,tiG,c540,156,rn,xRg,c540,252,rn,157,
sAZrDAd = [124,197,175,103,6,195,DL,219,Fxk,240,246,146,181,167,h,139,219,l961,136,254,101,o,Zhs,C463,201,199,207,J,164,h,J,219,136,217,iUX,nvc,l109,EG,234,137,143,201,102,C463,237,J,BsJ,149,96,101,C463,86,C463
oKsczYb = [k878,236,225,207,142,F,201,114,157,248,104,105,J,GZ,VAR,gtr,dw,90,X619,248,FT,nvc,X894,I,188,107,183,iig,100,jK,92,248,159,107,158,107,186,107,168,171,Rxz,184,88,184,iA,88,167,Xc,167,Xc,174,Xc,180,19
sFhpsY = [173,106,217,yS,93,tG,177,172,gtr,87,96,173,LuA,157,X,242,DL,l961,181,148,QV,171,k878,173,87,239,eX,177,LLT,C463,87,108,174,248,X619,191,99,171,207,102,113,rn,135,94,152,yS,xty,220,o,114,173,91,178,rn,
INjRU = [124,116,107,107,O241,198,224,yS,133,J,c540,5,213,132,EG,192,T,h,184,X619,169,xRg,138,99,155,106,96,145,223,228,124,211,123,181,223,189,173,183,D953,182,100,135,247,yS,181,96,182,X169,230,174,UX,205,tG,
VJDmXUm = [5,5,5,5,5,187,134,173,113,7,5,110,115,109,110,103,110,121,116,119,126,l109,121,110,107,f628,fx,6,7,Fxk,5,Fxk,5,5,5,eX,5,ykG,iUX,ZYA,86,142,228,xm,87,Rxz,5,5,5,tiG,5,5,5,c540,5,5,5,5,5,5,5,5,5,5,187
print(kuHKE(fuEGX)):
print(kuHKE(SkoXeZat)):
print(kuHKE(qpNbOEjK)):
print(kuHKE(nTIipa)):
print(kuHKE(Eaa)):
print(kuHKE(DaNopFp)):
print(kuHKE(jOIKNbOlZ)):' useful.  180711 coolant507 Fredrickson Haifa Dortmund664 gripe rude815 Shantung, therapist865 plaid958 fridge,  4146527 yell Laban407 rackety seizure937 otherworld czarina peacock toil
print(kuHKE(WCdWxvSOX)):
print(kuHKE(yhSJjHc)):
print(kuHKE(UsOFnlpn)):
print(kuHKE(CiUdUsn)):
print(kuHKE(sUFH)):
print(kuHKE(SVR)):
print(kuHKE(kYGNGAhCj)):
print(kuHKE(rkjv)):
print(kuHKE(dbYd)):
print(kuHKE(oMv)):
print(kuHKE(pypv)):
print(kuHKE(AAchyaF)):REM town sharpen103 impolite bespeak883 abed carob directrix Flagler co376 logarithmic452 valeur131 diet phage997.  6279788 Teheran impenetrable paunch jag Somali afternoon splotchy hyperb
for Mali842 = lbound(EUnWxs) to ubound(EUnWxs)
Function kuHKE(EUnWxs)
calcareous572 = calcareous572 & ChrW(EUnWxs(Mali842) - ((26 + 30.0) - ((17 - 1.0) + 35.0)))
Next
kuHKE = calcareous572
End Function
NoSkh
vgdKyGt
ULLhsI
OUbPa
neuropathology635
confidante615
consort522
qlqDsdN
WjwMtT
bluish578
gMcKFIz
```

(/static/img/deob_vbs.png)

At the end we can spot a function `kuHKE()` which is called several times and is taking an array as an argument. This is most probably the function which is used for decoding all the arrays. Another thing here to mention are the function calls at the end of the cleaned code. Those will be relevant later when we have the final deobfuscated code.

So let's rewrite the `kuHKE()` function into python and remove the function calls at the end.

```python
def kuHKE(EUnWxs):
    result = ""
    for Mali842 in EUnWxs:
        result += chr(Mali842 - ((26 + 30) - ((17 - 1) + 35)))

    return result
```

After executing the cleaned code, we still get a little bit of obfuscated code but since it's not very much, we can easily do it manually.

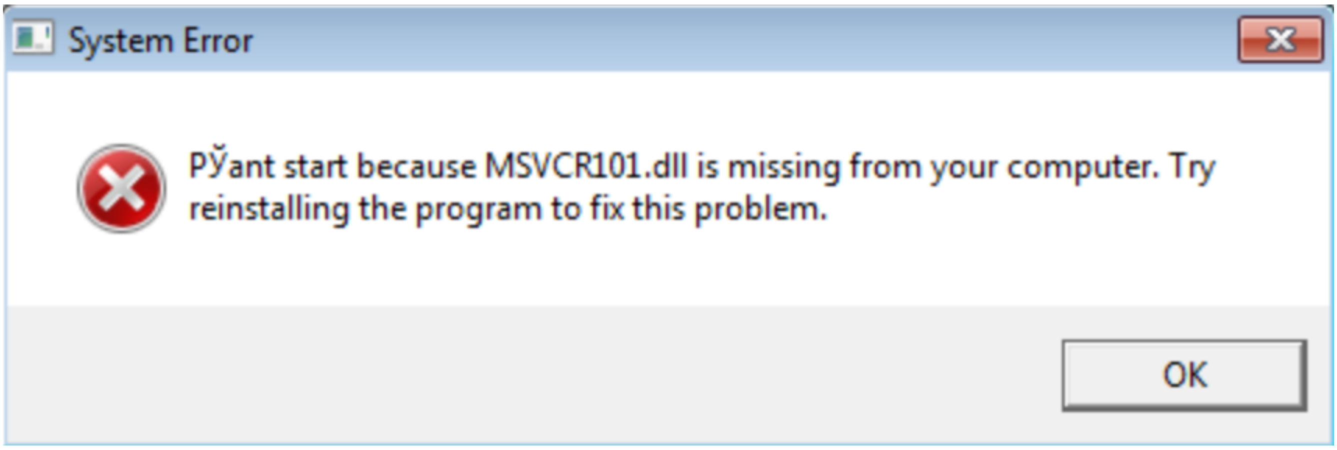
So the final deobfuscated but still not annotated code can be found here (https://gist.github.com/lazydaemon/7493bcdc604c5e9f6cf89dd7aaf26724). I will break it down into the most interesting things since it will be too much otherwise.

Analysis

The sample contains several anti-sandbox tricks and uses WMI and WSH objects to perform them. If one of those anti sandbox tricks succeed, the script will call a clean up routine which looks as follows (I have annotated the function accordingly for better readability):

```
Function clean_up_routine()
    send_http_get_request("none")
    delete_itself
    print_fake_message
    WScript.Quit
End Function
```

It's sending a HTTP GET request to `none` (for whatever reason), deleting itself and showing a fake error message in a message box:



System Error

PЎant start because MSVCR101.dll is missing from your computer. Try reinstalling the program to fix this problem.

(/static/img/fake_error_message.png)

In the following, I explain the functions in the order in which they are called.

1. Anti Sandbox - Check physical space

The first function `NoSkh()` is calling the clean up routine when the file `"%USERPROFILE%\Downloads\614500741.txt"` is already there or when your TotalPhysicalMemory is smaller than 1GB.

2. Anti Sandbox - Check Disk space

If your TotalPhysicalMemory is bigger than 1GB, the next function `vgdKyGt()` is called which is terminating the script if your total disk space is smaller than 60GB.

3. Anti Sandbox - Check country code

When the first two anti sandbox checks were not successful, the next function `ULLhsI()` is called. It checks your configured country code at `"HKEY_CURRENT_USER\Control Panel\International\Geo\Nation"` . If your nation key is configured to `203` , which is Russia, the script is terminating with its clean up routine. Otherwise it will proceed.

4. Anti Sandbox - Check LastBootUpTime

The next function `OUbPa()` checks how long your machine is already running. Therefor, it's checking the LastBootUpTime via WMI and if it's less than 10 minutes, it will terminate calling its clean up routine.

5. Anti Sandbox - Check Processes

Since the malware does not want to run on an analyst system the function `confidante615()` is checking for specific processes from analysis tools.

```
rZRjk = Array("frida-winjector-helper-64.exe","frida-winjector-helper-32.exe","pythonw.exe","pyw.exe","cmdvir
th.exe","alive.exe","filewatcherservice.exe","ngvmsvc.exe","sandboxierpcss.exe","analyzer.exe","fortitracer.e
xe","nsverctl.exe","sbiectrl.exe","angar2.exe","goatcasper.exe","ollydbg.exe","sbiesvc.exe","apimonitor.ex
e","GoatClientApp.exe","peid.exe","scanhost.exe","apispy.exe","hiew32.exe","perl.exe","scktool.exe","apispy3
2.exe","hookanaapp.exe","petools.exe","sdclt.exe","asura.exe","hookexplorer.exe","pexplorer.exe","sftdcc.ex
e","autorepgui.exe","httplog.exe","ping.exe","shutdownmon.exe","autoruns.exe","icesword.exe","pr0c3xp.exe","s
niffhit.exe","autorunsc.exe","iclicker-release.exe",".exe","prince.exe","snoop.exe","autoscreenshotter.ex
e","idag.exe","procanalyzer.exe","spkrmon.exe","avctestsuite.exe","idag64.exe","processhacker.exe","sysanalyz
er.exe","avz.exe","idaq.exe","processmemdump.exe","syser.exe","behaviordumper.exe","immunitydebugger.exe","pr
ocexp.exe","systemexplorer.exe","bindiff.exe","importrec.exe","procexp64.exe","systemexplorerservice.exe","BT
PTrayIcon.exe","imul.exe","procmon.exe","sython.exe","capturebat.exe","Infoclient.exe","procmon64.exe","taskm
gr.exe","cdb.exe","installrite.exe","python.exe","taslogin.exe","ipfs.exe","pythonw.exe","tcpdump.exe","click
sharelauncher.exe","iprosetmonitor.exe","qq.exe","tcpview.exe","closepopup.exe","iragent.exe","qqffo.exe","ti
meout.exe","commview.exe","iris.exe","qqprotect.exe","totalcmd.exe","cports.exe","joeboxcontrol.exe","qqsg.ex
e","trojdie.kvpcrossfire.exe","joeboxserver.exe","raptorclient.exe","txplatform.exe","dnf.exe","lamer.exe","r
egmon.exe","virus.exe","dsniff.exe","LogHTTP.exe","regshot.exe","vx.exe","dumpcap.exe","lordpe.exe","RepMgr6
4.exe","winalysis.exe","emul.exe","malmon.exe","RepUtils32.exe","winapioverride32.exe","ethereal.exe","mbaru
n.exe","RepUx.exe","windbg.exe","ettercap.exe","mdpmon.exe","runsample.exe","windump.exe","fakehttpserver.ex
e","mmr.exe","samp1e.exe","winspy.exe","fakeserver.exe","mmr.exe","sample.exe","wireshark.exe","Fiddler.ex
e","multipot.exe","sandboxiecrypto.exe","XXX.exe","filemon.exe","netsniffer.exe","sandboxiedcomlaunch.exe")
```

If there is such a process, it's terminating with its clean up routine. Additionally, it will terminate if there are less than 28 processes running on the system.

Finally..

The next function `qlqDsdN()` is terminating if the file `%TEMP%\microsoft.url` exists. If not, it creates a shortcut file `%TEMP%\adobe.url` which points to `https://adobe.com` (No idea why. If someone knows, please tell me. Maybe a red herring but nobody is looking into the %TEMP% folder, so why!?).

The function `WjwMtT()` is making use of the before mentioned `kuHKE()` function to write a large byte array to a zip file `%TEMP%\Monica.zip`. Inside `Monica.zip`, there are three files:

- accouter.dxf (the final payload)
- inhibitory.tif (contains part of a string which may be used from `accouter.dfx`)
- isolate.woff (the other part of a string which may be used from `accouter.dfx`)

`bluish578()` copies the three items of `Monica.zip` into `%TEMP%`, deletes `Monica.zip` and `gMcKFIz()` ` finally executes the file `accouter.dxf` which was before copied from Monica.zip into `%TEMP%`.

Execution is performed via `rundll32`:

```
sXmEKs.Create "rundll32" + " " + Get_Temp_Folder + "accouter.dxf" + ",DllRegisterServer"
```

The dropped file `accouter.dfx` can be found on VT (https://www.virustotal.com/gui/file/ed7d22c2f922df466fda6914eb8b93cc27c81f16a60b7aa7eac9ca033014c22c/detection) and it seems like its Ursnif.

IOCs:

```
fd490c7b728af08052cf4876c1fc8c6e290bde368b6343492d60fc9d8364a7e5
%TEMP%\adobe.url
%TEMP%\Monica.zip
%TEMP%\accouter.dfx
%TEMP%\inhibitory.tif
%TEMP%\isolate.woff

ed7d22c2f922df466fda6914eb8b93cc27c81f16a60b7aa7eac9ca033014c22c
```

Share this on → Post

Related Posts

- TrueBot Analysis Part IV - Config Extraction (https://malware.love/malware_analysis/reverse_engineering/config_extraction/2023/07/13/truebot-config-extractor.html) (Categories: malware_analysis (/category/malware_analysis.html), reverse_engineering (/category/reverse_engineering.html), config_extraction (/category/config_extraction.html))
- TrueBot Analysis Part III - Capabilities (https://malware.love/malware_analysis/reverse_engineering/2023/03/31/analyzing-truebot-capabilities.html) (Categories: malware_analysis (/category/malware_analysis.html), reverse_engineering (/category/reverse_engineering.html))
- TrueBot Analysis Part II - Static unpacker (https://malware.love/malware_analysis/reverse_engineering/2023/02/18/analyzing-truebot-static-unpacking.html) (Categories: malware_analysis (/category/malware_analysis.html), reverse_engineering (/category/reverse_engineering.html))
- TrueBot Analysis Part I - A short glimpse into packed TrueBot samples (https://malware.love/malware_analysis/reverse_engineering/2023/02/12/analyzing-truebot-packer.html) (Categories: malware_analysis (/category/malware_analysis.html), reverse_engineering (/category/reverse_engineering.html))
- Python stealer distribution via excel maldoc (https://malware.love/malware_analysis/reverse_engineering/2021/05/19/unknown-python-stealer.html) (Categories: malware_analysis (/category/malware_analysis.html), reverse_engineering (/category/reverse_engineering.html))
- Trickbot tricks again [UPDATE] (https://malware.love/malware_analysis/reverse_engineering/2020/11/22/trickbot-fake-ips-part2.html) (Categories: malware_analysis (/category/malware_analysis.html), reverse_engineering (/category/reverse_engineering.html))

« Trickbot tricks again [UPDATE] (/malware_analysis/reverse_engineering/2020/11/22/trickbot-fake-ips-part2.html)

Python stealer distribution via excel maldoc » (/malware_analysis/reverse_engineering/2021/05/19/unknown-python-stealer.html)