CERT-UA

Archived: 2026-04-05 12:55:13 UTC

Загальна інформація

У березні-квітні 2024 року під час проведення заходів з реагування на кіберінцидент в інформаційно-комунікаційній системі (ІКС) центрального органу виконавчої влади, національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA ідентифіковано технічний засіб під управлінням операційної системи Windows, що виконував роль серверу, на якому, серед іншого, було виявлено два програмні засоби реалізації кіберзагрози, а саме: BEARDSHELL та SLIMAGENT.

BEARDSHELL

Програма, розроблена з використанням мови програмування C++. Забезпечує завантаження, дешифрування (chacha20-poly1305) та виконання PowerShell-сценаріїв, а також вивантаження отриманого результату. Управління бекдором здійснюється через API сервісу Icedrive. Для кожної ураженої ЕОМ формується каталог, назва якого – це хеш hash64_fnv1a від назви ЕОМ та GUID профілю апаратного забезпечення ЕОМ (GetCurrentHwProfileW).

SLIMAGENT

Програма, розроблена з використанням мови програмування C++. Основне функціональне призначення - виготовлення знімків екрану (EnumDisplayMonitors -> CreateCompatibleDC/CreateCompatibleBitmap/BitBlt -> GdipSaveImageToStream), їх шифрування (AES+RSA) та збереження локально на ЕОМ у форматі: %TEMP%\Desktop_%d-%m-%Y_%H-%M-%S.svc.

На момент дослідження обставини первинної компрометації серверу, зокрема, спосіб доставки програм, встановлено не було. Інформацію щодо виявлених файлів передано для дослідження довіреному колу виробників засобів захисту та дослідників кіберзагроз.

Водночас, у травні 2025 року від компанії ESET отримано оперативну інформацію щодо виявлення ознак несанкціонованого доступу до електронної поштової скриньки в доменній зоні gov.ua.

З метою запобігання реалізації кіберзагрози, CERT-UA у взаємодії з Центром кібернетичної безпеки інформаційно-телекомунікаційних систем військової частини А0334 вжито заходів з реагування на кіберінцидент.

В результаті проведення комп'ютерно-технічного дослідження виявлено програмні засоби - компонент фреймоворку COVENANT та бекдор BEARDSHELL, а також з'ясовано спосіб первинного ураження. На цей раз невстановленою особою за допомогою Signal надіслано документ з назвою "Акт.doc", що містив макрос. При цьому, що очевидно з переписки, зловмисник мав достатньо інформації щодо об'єкту атаки та володів деталями стану справ в частині, що стосується.

У випадку активації вмісту документу код макросу забезпечить створення на ЕОМ двох файлів: %APPDATA%\microsoft\protect\ctec.dll (буде скопійовано з %TEMP%\cache_d3qf5gw56jikh5tb6) та %LOCALAPPDATA%\windows.png, а також, створення ключа в реєстрі операційної системи: "HKCU\Software\Classes\CLSID\{2227A280-3AEA-1069-A2DE-08002B30309D}\InProcServer32" (COM-hijacking), що, у свою чергу, забезпечить завантаження створеної DLL при наступному запуску процесу explorer.exe (процес також завершується та запускається кодом макросу).

Основним призначенням файлу "ctec.dll" є дешифрування і запуск шеллкоду з файлу "windows.png", що, у свою чергу, призведе до запуску в пам'яті ЕОМ компоненту фреймворку COVENANT ("ksmqsyck.dx4.exe"), який, в якості каналу управління, використовує API сервісу Koofr.

Виходячи з деталей комп'ютерно-технічного дослідження припускаємо, що COVENANT використано для завантаження на ЕОМ виконуваного файлу "%LOCALAPPDATA%\Packages\PlaySndSrv.dll" та файлу "%USERPROFILE%\Music\Samples\sample-03.wav". Насамкінець, "PlaySndSrv.dll" забезпечить зчитування з файлу "sample-03.wav" та запуск шелкоду, що в результаті призведе до запуску на ЕОМ бекдору BEARDSHELL. Зауважимо, що персистентність "PlaySndSrv.dll" забезпечується створенням ключа в реєстрі "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InProcServer32" (COM-hijacking), що призведе до запуску останньої штатним запланованим завданням "Microsoft\Windows\Multimedia\SystemSoundsService".

Успішність реалізації кіберзагрози пояснюється можливістю запуску макросів, неконтрольованістю хостовими засобами захисту Signal'у, як засобу доставки інформації на ЕОМ, а також використанням API легітимних сервісів як каналу управління. Рекомендуємо звернути увагу на мережеву взаємодію з "app.koofr.net" та "api.icedrive.net".

Описану активність асоційовано з діяльністю угруповання UAC-0001 (APT28).

Індикатори кіберзагроз

Файли:

```
915179579ab7dc358c41ea99e4fcab52    c49d4acad68955692c32d5fa924eb5bb3f95a192d2c70ff6b0b2ce63c6afe985
2cae8dc37baf5216a3e7342aac755894    be588c14f7ed3252e36c7db623c09cde8e01fa850c5431d9d621ac942695804d
b52c71318815836126f1257a180a74e7    0a0fefb509a85c069539003c03c4f9c292d415fb27d18aef750446b63533b432
5171e84d59fd2bbef9235dfa6459ad8a    84e9eb9615f16316adac6c261fe427905bf1a3d36161e2e4f7658cd177a2c460
99f2fd309b88b8ec3a9c9c50dddb08b5    296b294a5fed830c2ff1fac9cb361a2d665b70f2f37188b593b5d1401cd6ca28
bd76f54d26bf00686da42f3664e3f2ae    225b7abe861375141f6cfebde4981f615cb2aa4d913faf85172666fa4b4b320b
b859f38bfa8bba05d7c0eb4207b95037    d1deeaf0f1807720b11d0f235e3c134a1384054e4c3700eabab26b3a39d2c19a
b6e3894c17fb05db754a61ac9a0e5925    20987f7163c8fe466930ece075cd051273530dfcbe8893600fd21fcfb58b5b08
d802290cb9e5c3fed1ba1a8daf827882    88e28107fbf171fdbcf4abbc0c731295549923e82ce19d5b6f6fefa3c9f497c9
8e0143a6fd791c859d79445768af44d1    39c1f38d0bdc70e50588964ccf3e63dabb871dca83392305a0c64144c7860155

(2024 рік)
5d938b4316421a2caf7e2e0121b36459    2eabe990f91bfc480c09db02a4de43116b40da2d6eaad00a034adf4214dac4d1
889b83d375a0fb00670af5276816080e    9faeb1c8a4b9827f025a63c086d87c409a369825428634b2b01314460a332c6c
```

Хостові:

```
%APPDATA%\microsoft\protect\ctec.dll
%LOCALAPPDATA%\Packages\PlaySndSrv.dll
%LOCALAPPDATA%\windows.png
%TEMP%\cache_d3qf5gw56jikh5tb6
%TEMP%\io1snrb41da2gn5.tmp
%USERPROFILE%\Music\Samples\sample-03.wav
%TEMP%\cache_ertf5gw56jikh5dwe
%PUBLIC%\Pictures\WordIllustration.png
HKEY_CURRENT_USER\Software\Classes\CLSID\{2227A280-3AEA-1069-A2DE-08002B30309D}\InProcServer32
HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InProcServer32
Microsoft\Windows\Multimedia\SystemSoundsService

(2024 рік)
C:\Windows\System32\tcpiphlpsvc.dll
C:\Windows\System32\wbem\eapphost.dll
reg.exe ADD HKLM\SYSTEM\CurrentControlSet\Services\tcpiphlpsvc\Parameters /v ServiceDll /t REG_EXPANI
sc.exe create tcpiphlpsvc binPath= "C:\Windows\System32\svchost.exe -k TCPIPHLPSVC start= auto Displ
```

Мережеві:

```
(легітимні сервіси)
api.icedrive[.]net
app.koofr[.]net
hXXps://api.icedrive[.]net
hXXps://app.koofr[.]net
icedrive[.]net
koofr[.]net
```

Графічні зображення

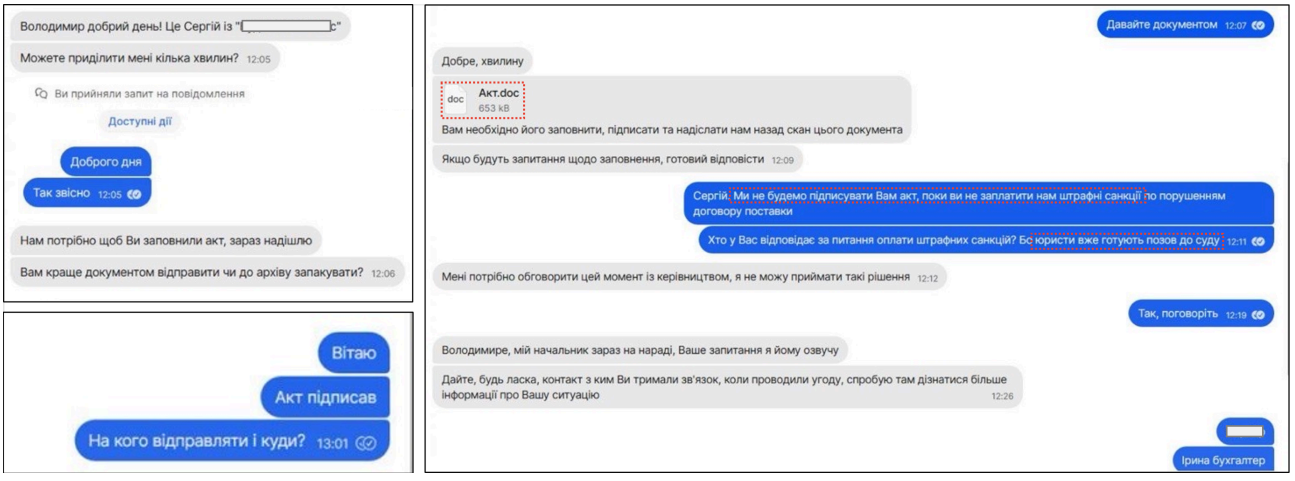

Рис. 1 Приклад комунікації зі зловмисником у Signal

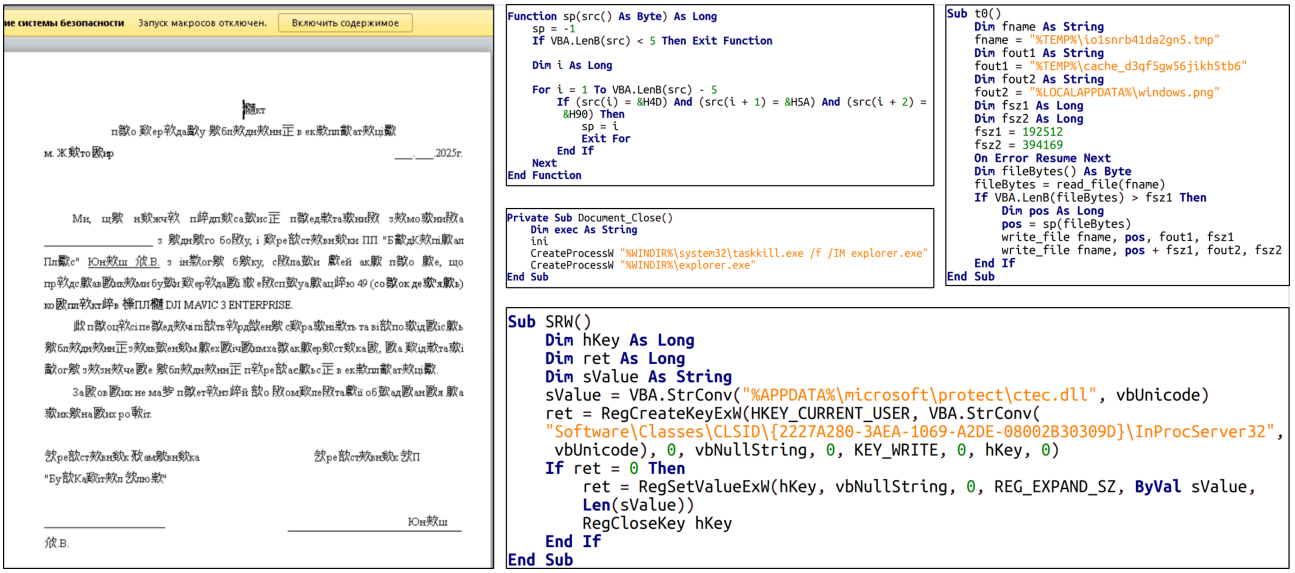

Рис. 2 Приклад документу да частин коду деобфускованого макросу

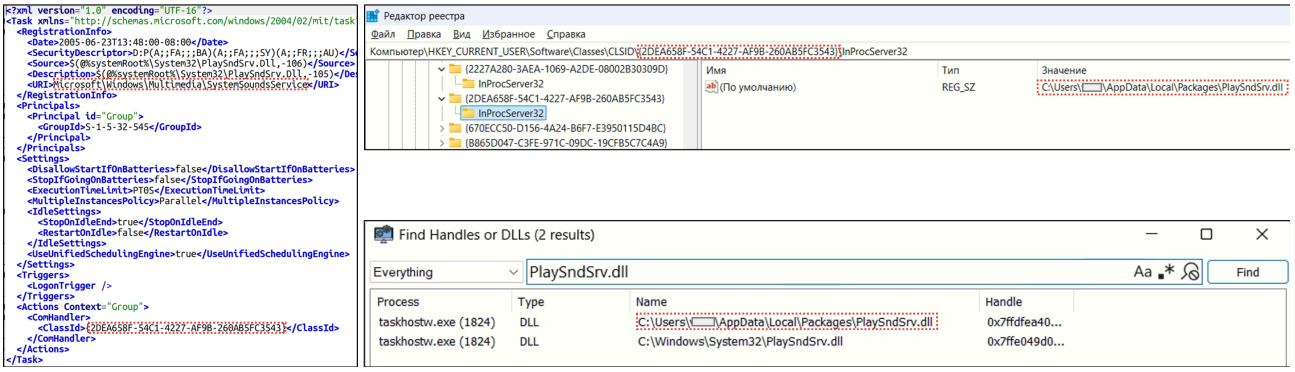

Рис. 3 Приклад способу забезпечення персистентності лоадеру для бекдору BEARDSHELL

Source: https://cert.gov.ua/article/6284080