CERT-UA

Archived: 2026-04-05 13:04:50 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено файл "Доповідь_050722_4.ppt", що містить зображення-мініатюру, на якій згадєуться оперативне командування "Південь".

У випадку відкриття документу та активації макросу останній забезпечить створення файлів "gksg023ig.lnk" та "sgegkseg23mjl.exe", а також виконання LNK-файлу за допомогою rundll32.exe, що, в свою чергу, призведе до запуску згаданого EXE-файлу.

Виконуваний файл є .NET-програмою, обфускованою за допомогою ConfuserEx, що здійснює завантаження JPEG-файлу "thumb_d_F3D14F4982A256B5CDAE9BD579429AE7.jpg", пошук відповідного офсету, дешифрування та декомпресію даних і запуск отриманої в результаті .NET-програми MCMDiction.exe (дата компіляції: 2022-07-08).

Надалі, після ряду перетворень (Gzip, AES, base64, XOR), в тому числі, із застосуваннями стеганографії, на комп'ютері буде виконано шкідливу програму-стілер AgentTesla (дата компіляції: 2022-07-06).

Зважаючи на ім'я та контент-приманку PPT-документу, припускаємо, що атаку було спрямовано на державні організації України.

Індикатори компрометації

Файли:

```
5675473bb46fad83c92865c9c6afbd5e    00fdb03518c238dc649a39e94f0bcc95dacf3b832979d14d0ed5194b9b482b87
c71f41f71e0beea474049af497eae7b7    cffc6a854632d979e3c12d4c29835490229db79909b18010d3dbaabbb89ad2cc
88c2f95bb1e008e2952799a427ab8492    bc92a5b1c4205ea1fbfec9144b8aab485e095142c7105c9d616b089ec668f198
24a95b0c3d0bab9451e49ebd2a95efb4    c40e6b176ad3fd7332cd217191e557352ef4b82bf91f29939121267598737990
050a2254623b88bdd5d171715542bee1    8a9262fecbb58364982f38bdefd44336005632079e254e6f82693050fa29c403
3249773213e0a41ed4d49174ad651f28    664723f55237e2d14b39938878fd0a3744cc808d4d3e67e22f1bcbd410960557
```

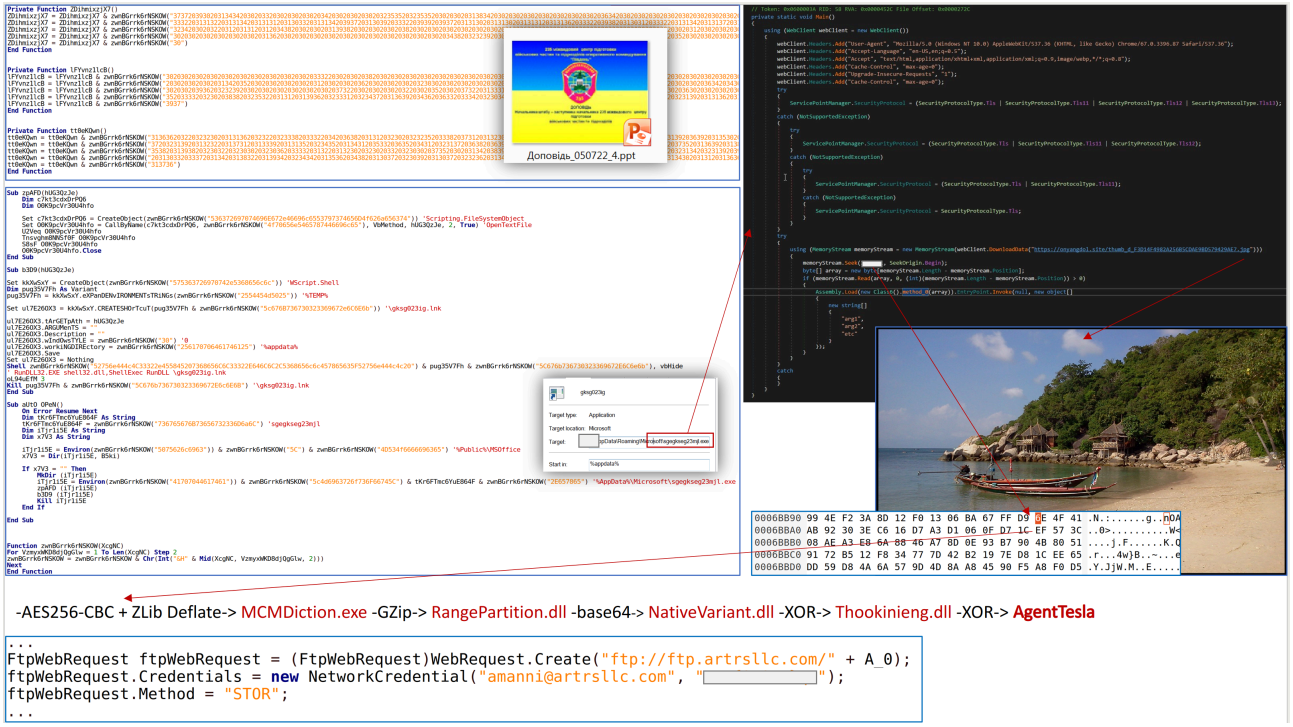
Мережеві:

```
onyangdol[.]site
ftp.artrsllc[.]com
hXXps://onyangdol[.]site/thumb_d_F3D14F4982A256B5CDAE9BD579429AE7.jpg
fXp://ftp.artrsllc[.]com/
```

Хостові:

```
RunDLL32.EXE shell32.dll,ShellExec_RunDLL %TMP%\gksg023ig.lnk
%APPDATA%\Microsoft\sgegkseg23mjl.exe
%TMP%\gksg023ig.lnk
```

Графічні зображення



Source: https://cert.gov.ua/article/861292