



Загальна інформація

Починаючи з січня 2026 року CERT-UA фіксує непоодинокі випадки розповсюдження електронних листів, нібито від імені центральних органів виконавчої влади та обласних адміністрацій із закликом оновити мобільні застосунки широко використовуваних цивільних і військових систем.

Електронний лист може містити вкладення у вигляді архіву, у якому знаходиться EXE-файл, або ж посилання на легітимний, проте вразливий до XSS (Cross-site scripting) вебсайт, відвідування якого призведе до виконання JavaScript-коду та подальшого завантаження на комп'ютер виконуваного файлу. При цьому згадані EXE-файли та скрипти розміщуються на ресурсах легітимного сервісу GitHub.

Протягом січня-лютого 2026 року підтверджено використання таких програмних засобів реалізації кіберзагроз:

- SHADOWSNIFF (стілер з GitHub)
- SALATSTEALER (MaaS стілер)
- DEFTICK (примітивний бекдор на Go)

Під час дослідження в одному з репозиторіїв GitHub виявлено програму з ознаками «шифрувальника-вимагача» (внутрішня назва «AVANGARD ULTIMATE v6.0»), а також архів із експлойтом для уразливості WinRAR (CVE-2025-8088).

Детальне вивчення обставин та засобів реалізації кіберзагрози, включаючи експерименти з публічно доступним інструментарієм, дозволяє пов'язати описану активність з діяльністю осіб, яку висвітлюють у Telegram-каналі «PalachPro».

Активність відстежується за ідентифікатором UAC-0252.

Індикатори кіберзагроз

Файли:

510690f2a21e677f05094e4fcfea9a9a	
df31cd6305169271c026723a6d638bf8afbcbcb429972e7339ac89b53c48a35a8	popup.js
e457cb42ca5a6ecd8b99d89ed2958b29	
b5e685e57c625032ec067be94a2854cce1b7c5a51e8d6bd833841a893d5d88b7	
Diia_Update_4.7.1_Official.exe (DEAFTICK)	
6ba7f82518e76a436d5eeb50f626d218	
84bd898154543075e9b2f3566b710f7a8ef3028c8f07c73113a8f4f45332e3d6	update.rar
2591d145ff510f7fc4d6290d3bfcbb130	
3abf295b79992532b03261a81643124d134fa7e86fb901b3bfc74ad0f192dc7f	updateV3.23.exe
(SHADOWSNIFF)	
b6480aa6c364715a21ba28c4d26a5b6e	
c2a4212573d7566acf5b610b4ce3598237acd37459670daa1b6950f107d50e03	updateV3.23.exe
(SHADOWSNIFF)	
f3dc1e16cde2995f701c8db509f351c9	
e5941df780ae251bcfad3b833f45ee44bd1599ab45b7adf1f1c79510930642d	EdgeUpdate.exe
(DEAFTICK)	
cdc1919fc612772b34daecbcf2e38a05	
ba1498476b0613d0b25224deb44130c642467653ec475a47c3fa3024bcb4d7f4	1.rar (CVE-2025-8088)
dcc2c9a08044e8b3e445f17461d054f1	
7b35b332a999d56d65241a4f35bbce2e9ad2644a84c09f7dbae42e39cd559bcf	build.exe (DEAFTICK)
a3e8f8dc8702474452b1b0889a9d77d1	
278f178676289f074251609d940132d162cf252666bed7c3056f01424d6abf07	popup.js
974cc318d509301be0966cc1b397076b	
c149a236ddf07fb96de1a893b8d09cdfdd2c28abfc4c3c17bb3ebd8c3c7b5cef	main.exe (SALATSTEALER)
9a9a98117b483439cf54c9f7ffa4e417	
a4f1a6f8f5a407ea0113253b557a6dc75c35398edf21bbc5322c47ac1fd0b689	main.deupx.exe
(SALATSTEALER)	
c2b70e79a3c7e9d392b02da9d7265d1f	
b7a89f32f5e64003cfcd1de630bdf36b2254866083e01ea6493186549772c082	MikolaevApp.exe
(AVANGARD)	

Мережеві:

```

hXXp://150[.]241.64.21:8888/client/addclient
hXXp://95[.]85.224.14:8000/client/addclient
hXXps://nfkavn[.]bond/client/addclient
hXXps://salat[.]cn/sa1at/
hXXps://salator[.]es/sa1at/
hXXps://salator[.]ru/sa1at/
hXXps://websalat[.]top/sa1at/
hXXps://wrat[.]in:992/sa1at/
hXXps://mk-gov-
ua.github[.]io/jgfdhkmmbvn.github[.]io/raw/refs/heads/main/Diia_Update_4.7.1_Official.exe
hXXps://mk-gov-ua.github[.]io/jgfdhkmmbvn.github[.]io/popup.js
hXXp://security.digital-ua[.]digital/soft/security/updateV3.23.exe
hXXp://ua-gov[.]info/soft/security/updateV3.23.exe
hXXps://governmentnerc.github[.]io/nerc.gov.ua/popup.js
hXXps://91[.]92.34.130/main.exe
mk-gov-ua.github[.]io
governmentnerc.github[.]io
digital-ua[.]digital
nfkavn[.]bond
ua-gov[.]info
ukremai[.]com
sa1at[.]ru
salat[.]cn
salator[.]es
salator[.]ru
websalat[.]top
wrat[.]in
150[.]241.64.21
95[.]85.224.14
95[.]85.231.199
64[.]188.83.228
64[.]188.79.226
95[.]85.252.196
64[.]188.83.192
91[.]92.34.130
85[.]198.98.75

```

Хочови:

```

attrib +h +s %TMP%\svchost.exe
powershell -Command "Add-MpPreference -ExclusionPath '%TMP%\svchost.exe'"
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v WindowsUpdateService /t
REG_SZ /d %TMP%\svchost.exe /f
%TMP%\svchost.exe
%APPDATA%\Microsoft\Edge\Cache\EdgeUpdate.exe
%APPDATA%\Microsoft\Edge\Cache\edge_updater.exe
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\'WindowsUpdateService'

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\'MicrosoftEdgeUpdateTask'

```

Графічні зображення:

Рис.1 Приклад ланцюга ураження

Рис.2 Приклад ланцюга ураження

Рис.3 Приклад ланцюга ураження

Рис.4 Приклад фішинового листа

[Попередня](#)

["Бюлетень небезпеки": УАС-0001 \(APT28\) здійснює кібератаки у відношенні України та країн ЄС з використанням експлойту CVE-2026-21509 \(CERT-UA#19542\).](#)