CERT-UA

Archived: 2026-04-05 16:09:27 UTC

Загальна інформація

У понеділок, 26.01.2026, компанією Microsoft опубліковано інформацію про вразливість з ідентифікатором CVE-2026-21509 у продуктах Microsoft Office, з приміткою про активну експлуатацію останньої.

Вже 29.01.2026 в публічному доступі виявлено DOC-файл "Consultation_Topics_Ukraine(Final).doc", що містив експлойт для згаданої вразливості та був присвячений консультаціям Комітету постійних представників при ЄС (COREPER) по ситуації в Україні. При цьому метадані свідчать про те, що документ було створено 27.01.2026 о 07:43:00 (UTC), тобто, на наступний день після публікації згаданого сповіщення про вразливість від Microsoft.

Протягом того ж дня від учасників інформаційного обміну отримано повідомлення щодо розповсюдження, нібито від імені Укргідрометцентру, електронних листів із вкладенням у вигляді DOC-файлу "BULLETEN_H.doc". Згаданий лист було відправлено на більше ніж 60 електронних адрес переважно центральних органів виконавчої влади України.

Під час дослідження встановлено, що відкриття документу за допомогою програми Microsoft Office призводить до встановлення мережевого з'єднання із зовнішнім ресурсом з використанням протоколу WebDAV, подальшого завантаження файлу із заголовком файлу ярлика, який містить програмний код, призначений для завантаження та запуску виконуваного файлу.

Успішний запуск останнього призведе до створення на комп'ютері DLL-файлу "EhStoreShell.dll" (маскується під файл бібліотеки "Enhanced Storage Shell Extension"), файлу-зображення з шелкодом "SplashScreen.png", зміни значення шляху в реєстрі Windows для CLSID {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D} (реалізація COM hijacking) та створення запланованої задачі "OneDriveHealth".

Заплановане виконання задачі призведе до термінації та повторного запуску процесу explorer.exe, що, серед іншого, завдяки COM hijacking забезпечить завантаження DLL-файлу "EhStoreShell.dll", який здійснить виконання шелкоду з файлу-зображення, що, в свою чергу, забезпечить запуск на комп'ютері програмного засобу (фреймворку) COVENANT. Слід звернути увагу на той факт, що в якості інфраструктури для управління COVENANT використовує легітимне хмарне сховище Filen (filen.io).

В останні дні січня 2026 року виявлено ще три документи з аналогічним експлойтом, які, відповідно до їх вмісту, структури вбудованих URL та інших особливостей, були застосовані для кібератак у відношенні організацій країн ЄС. При цьому, в одному з випадків доменне ім'я, використане в атаці 30.01.2026, зареєстроване в цей же день.

Очевидно, що наближчим часом, в тому числі через інертність процесу (або неможливість) оновлення користувачами пакету програм Microsoft Office і/або застосування рекомендованих механізмів захисту, кількість кібератак із застосуванням описаної вразливості почне зростати.

У зв'язку із викладеним, з метою скорочення поверхні атаки рекомендуємо невідкладно вжити заходів, наведених в публікації Microsoft, зокрема, в частині налаштування реєстру Windows.

Беручи до уваги той факт, що програмний засіб COVENANT, який застосовується UAC-0001 (APT28) під час здійснення кібератак, використовує інфраструктуру сервісу Filen, рекомендуємо унеможливити і/або взяти під окремий моніторинг мережеву взаємодію з вузлами згаданого хмарного сховища (перелік доменних імен та IP-адрес наведено в розділі індикаторів).

Організації, які за допомогою граничних мережевих засобів власних інформаційно-комунікаційних систем і/або на рівні постачальників електронних комунікаційних послуг мають технологічну інтеграцію з системою реагування на кіберінциденти, кібератаки, кіберзагрози (забезпечення функціонування якої здійснюється Державним центром кіберзахисту Держспецзв'язку в рамках впровадження організаційно-технічної моделі кіберзахисту як складової національної системи кібербезпеки), автоматично отримують відповідний захист.

Індикатори кіберзагроз

Файли:

```
7c396677848776f9824ebe408bbba943        c91183175ce77360006f964841eb4048cf37cb82103f2573e262927be4c7
d8e880975ab01c745386663409a9d3aa        b2e771cbfa0a74d0774db162d28c1eecd3a7cb384dfe97522e9baabd1c04
744bbe8d7c3d0421fa0deb582481f5ba        8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace9
4423b8f3456e54eb48dfbde0b4c7984b        52b6fb40e7efb09c2bebe8550178e7e30009600bdedd1acae085d753761b
418dc7365e78f79ef7dfcfbfe1bc8b0e        c4389cc34b672c4f885547f413bf38575e6ee2b23a0ddfdd306a69c1775d
331e055e6a519d443233bd740dbfe8ee        495cf3fd22d4fc2c6c86b689b68141ac7d0130b0bb5cbc834ef59275132e
6f528ad405bffa4a8c2f61b1fa2172fd        40c2e559992a7f595c593b419930a3f216516c3042ad86fb985348d53b6e
ee0b44346db028a621d1dec99f429823        9f4672c1374034ac4556264f0d4bf96ee242c0b5a9edaa4715b5e61fe8d5
4727582023cd8071a6f388ea3ba2feaa        5a17cfaea0cc3a82242fdd11b53140c0b56256d769b07c33757d61e0a0a6
95e59536455a089ced64f5af2539a449        b2ba51b4491da8604ff9410d6e004971e3cd9a321390d0258e294ac42010
d47261e52335b516a777da368208ee91        fd3f13db41cd5b442fa26ba8bc0e9703ed243b3516374e3ef89be71cbf07
b6a86f44d0a3fa5a5ac979d691189f2d        969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e956
```

Мережеві:

```
(smb)://freefoodaid[.]com/documents/template_2_2.doc
(smb)://wellnesscaremed[.]com/davwwwroot/buch/Downloads/blank.doc
(smb)://wellnesscaremed[.]com/davwwwroot/venezia/Favorites/blank.doc
(smb)://wellnessmedcare[.]org@ssl/cz/Downloads/blank.doc
(smb)://wellnessmedcare[.]org@ssl/pol/Downloads/blank.doc
hXXp://freefoodaid[.]com/davwwwroot/2_2.lNk?init=
hXXp://freefoodaid[.]com/documents/2_2.lNk?init=
hXXps://wellnesscaremed[.]com/buch/Downloads/document.doc.LnK?init=
hXXp://wellnesscaremed[.]com/buch/Downloads/document.doc.LnK?init=
hXXp://wellnesscaremed[.]com/venezia/Favorites/document.doc.LnK?init=
hXXp://wellnesscaremed[.]com/venezia/d/s.d
hXXps://wellnessmedcare[.]org/davwwwroot/cz/Downloads/document.LnK?init=
```

```
hXXp://wellnessmedcare[.]org/davwwwroot/cz/Downloads/document.LnK?init=
hXXps://wellnessmedcare[.]org/davwwwroot/pol/Downloads/document.LnK?init=
hXXp://wellnessmedcare[.]org/davwwwroot/pol/Downloads/document.LnK?init=
freefoodaid[.]com       2026-01-12
wellnesscaremed[.]com   2026-01-12
wellnessmedcare[.]org   2026-01-30
159[.]253.120.2
193[.]187.148.169
23[.]227.202.14

Інфраструктура хмарного сховища Filen
*.filen.net
*.filen-1.net
*.filen-2.net
*.filen-3.net
*.filen-4.net
*.filen-5.net
*.filen-6.net
*.filen.io
*.filen.dev
146.0.41.204
146.0.41.205
146.0.41.206
146.0.41.207
146.0.41.208
146.0.41.231
146.0.41.232
146.0.41.233
146.0.41.234
```

```
smb://freefoodaid.com/documents/template_2_2.doc
smb://wellnesscaremed.com/davwwwroot/buch/Downloads/blank.doc
smb://wellnesscaremed.com/davwwwroot/venezia/Favorites/blank.doc
smb://wellnessmedcare.org@ssl/cz/Downloads/blank.doc
smb://wellnessmedcare.org@ssl/pol/Downloads/blank.doc
http://freefoodaid.com/davwwwroot/2_2.lNk?init=
http://freefoodaid.com/documents/2_2.lNk?init=
https://wellnesscaremed.com/buch/Downloads/document.doc.LnK?init=
http://wellnesscaremed.com/buch/Downloads/document.doc.LnK?init=
http://wellnesscaremed.com/venezia/Favorites/document.doc.LnK?init=
http://wellnesscaremed.com/venezia/d/s.d
https://wellnessmedcare.org/davwwwroot/cz/Downloads/document.LnK?init=
http://wellnessmedcare.org/davwwwroot/cz/Downloads/document.LnK?init=
https://wellnessmedcare.org/davwwwroot/pol/Downloads/document.LnK?init=
http://wellnessmedcare.org/davwwwroot/pol/Downloads/document.LnK?init=
freefoodaid.com
```

```
wellnesscaremed.com
wellnessmedcare.org
159.253.120.2
193.187.148.169
23.227.202.14
```

Хостові:

```
%PROGRAMDATA%\Microsoft OneDrive\setup\Cache\SplashScreen.png
%PROGRAMDATA%\USOPublic\Data\User\EhStoreShell.dll
%TMP%\Diagnostics\office.xml
HKCU\Software\Classes\CLSID\{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}\InProcServer32\'(Default)'
HKCU\Software\Classes\CLSID\{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}\InProcServer32\'ThreadingModel'
schtasks /delete /f /tn OneDriveHealth
schtasks.exe /Create /tn "OneDriveHealth" /XML "%TMP%\Diagnostics\office.xml"
start explorer >nul 2>&1
taskkill /f /IM explorer.exe >nul 2>&1
OneDriveHealth
```

Графічні зображення:

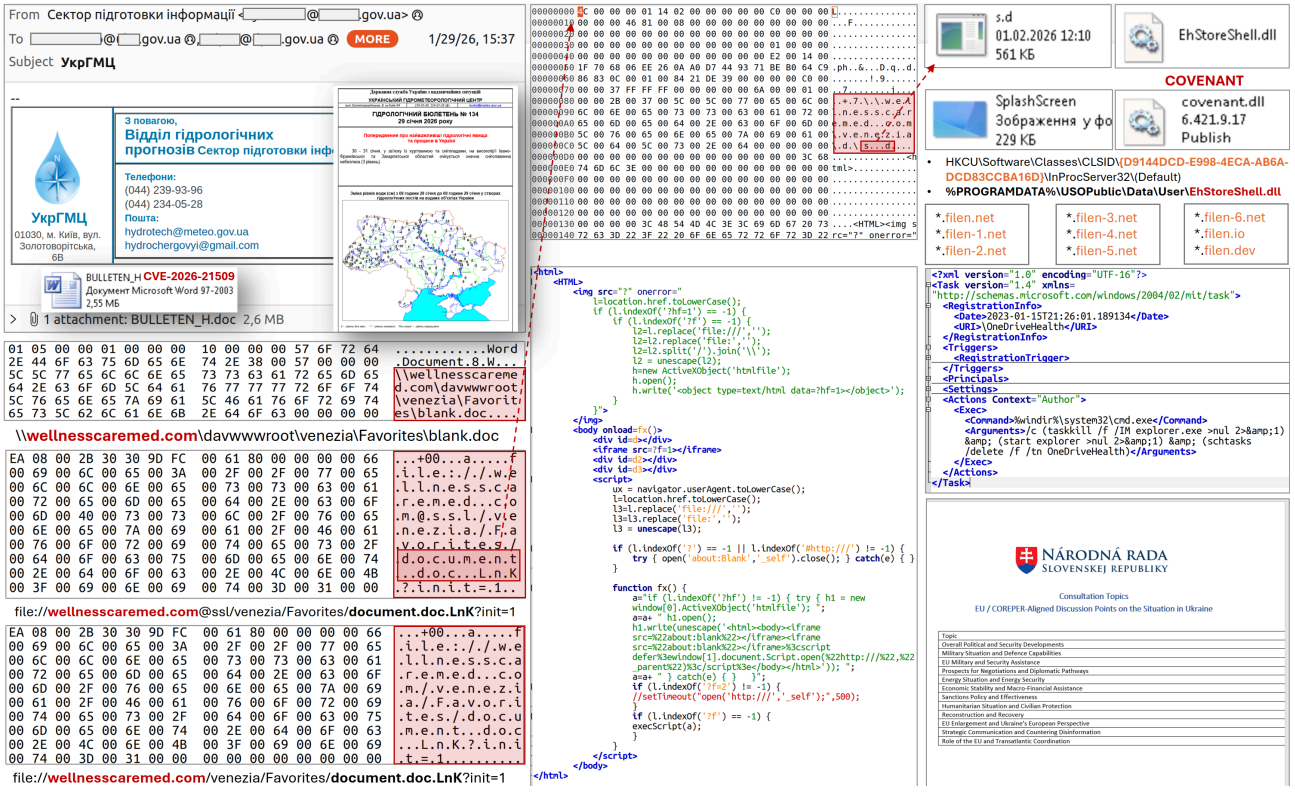
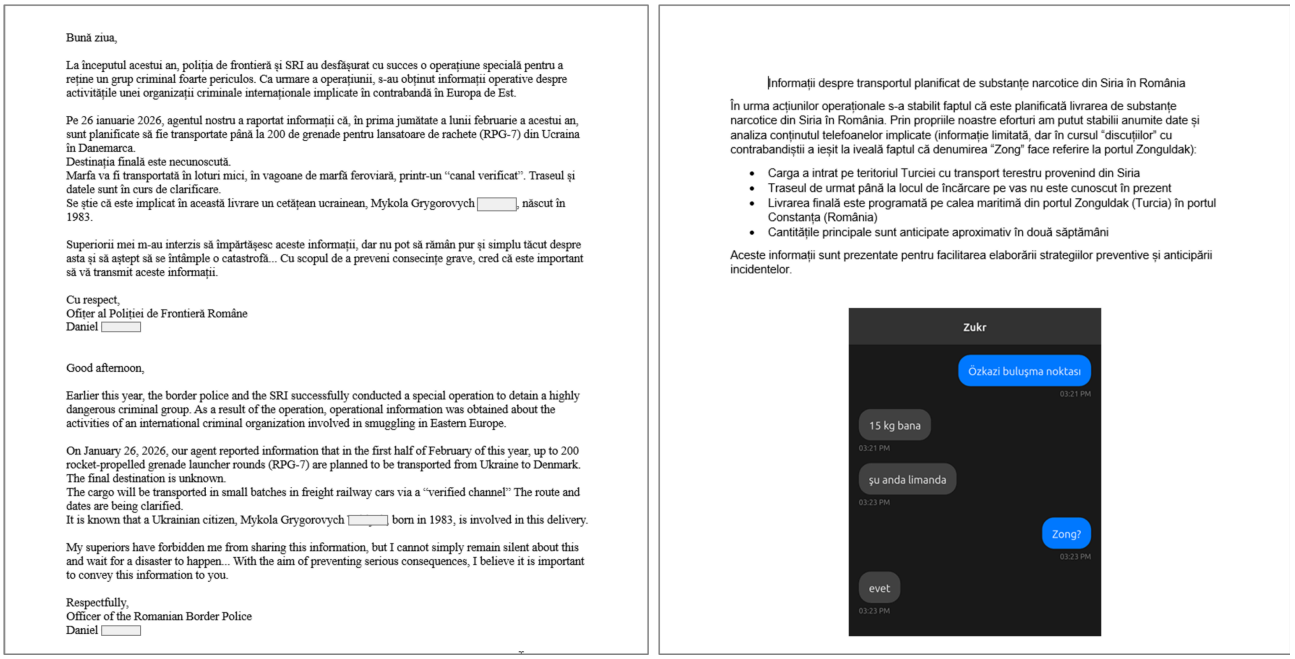


Рис.1 Приклад ланцюга ураження



Bună ziua,

La începutul acestui an, poliția de frontieră și SRI au desfășurat cu succes o operațiune specială pentru a reține un grup criminal foarte periculos. Ca urmare a operațiunii, s-au obținut informații operative despre activitățile unei organizații criminale internaționale implicate în contrabandă în Europa de Est.

Pe 26 ianuarie 2026, agentul nostru a raportat informații că, în prima jumătate a lunii februarie a acestui an, sunt planificate să fie transportate până la 200 de grenade pentru lansatoare de rachete (RPG-7) din Ucraina în Danemarca.
Destinația finală este necunoscută.
Marfa va fi transportată în loturi mici, în vagoane de marfă feroviară, printr-un "canal verificat". Traseul și datele sunt în curs de clarificare.
Se știe că este implicat în această livrare un cetățean ucrainean, Mykola Grygorovych [redacted], născut în 1983.

Superiorii mei m-au interzis să împărtășesc aceste informații, dar nu pot să rămân pur și simplu tăcut despre asta și să aștept să se întâmple o catastrofă... Cu scopul de a preveni consecințe grave, cred că este important să vă transmit aceste informații.

Cu respect,
Ofițer al Poliției de Frontieră Române
Daniel [redacted]

Good afternoon,

Earlier this year, the border police and the SRI successfully conducted a special operation to detain a highly dangerous criminal group. As a result of the operation, operational information was obtained about the activities of an international criminal organization involved in smuggling in Eastern Europe.

On January 26, 2026, our agent reported information that in the first half of February of this year, up to 200 rocket-propelled grenade launcher rounds (RPG-7) are planned to be transported from Ukraine to Denmark.
The final destination is unknown.
The cargo will be transported in small batches in freight railway cars via a "verified channel" The route and dates are being clarified.
It is known that a Ukrainian citizen, Mykola Grygorovych [redacted] born in 1983, is involved in this delivery.

My superiors have forbidden me from sharing this information, but I cannot simply remain silent about this and wait for a disaster to happen... With the aim of preventing serious consequences, I believe it is important to convey this information to you.

Respectfully,
Officer of the Romanian Border Police
Daniel [redacted]

Informații despre transportul planificat de substanțe narcotice din Siria în România

În urma acțiunilor operaționale s-a stabilit faptul că este planificată livrarea de substanțe narcotice din Siria în România. Prin propriile noastre eforturi am putut stabilii anumite date și analiza conținutul telefoanelor implicate (informație limitată, dar în cursul "discuțiilor" cu contrabandiștii a ieșit la iveală faptul că denumirea "Zong" face referire la portul Zonguldak):

- Carga a intrat pe teritoriul Turciei cu transport terestru provenind din Siria
- Traseul de urmat până la locul de încărcare pe vas nu este cunoscut în prezent
- Livrarea finală este programată pe calea maritimă din portul Zonguldak (Turcia) în portul Constanța (România)
- Cantitățile principale sunt anticipate aproximativ în două săptămâni

Aceste informații sunt prezentate pentru facilitarea elaborării strategiilor preventive și anticipării incidentelor.

Рис.2 Приклад вмісту документів з експлойтом

Source: https://cert.gov.ua/article/6287250