Аналіз методів компрометації облікових записів телеграму: технічний огляд, рекомендації та прогнози

В умовах повномасштабної війни та цифровізації українського суспільства захист персональних даних і комунікацій набуває критичного значення. Месенджери, зокрема телеграм, стали не лише простором для спілкування, а й важливим майданчиком для отримання чи поширення оперативної інформації, у тому числі для координації волонтерської і військової діяльності, а також для підтримки зв'язку з близькими в різних регіонах України та за кордоном

Аналітика звернень до гарячої лінії з цифрової безпеки Nadiyno.org у 2024 році виявляє тривожну тенденцію: щомісяця від 70% до 80% зафіксованих інцидентів кібербезпеки стосуються несанкціонованого доступу до телеграм-акаунтів. Це створює значні ризики не лише для окремих користувачів, а й для національної безпеки в цілому.

У цьому технічному звіті команда Nadiyno.org подає детальний аналіз методів, які зловмисники використовують для компрометації акаунтів у 2024 та на початку 2025 року. На основі зібраних даних та документованих випадків ми провели глибокий аналіз технічних аспектів атак, механізмів їх реалізації та векторів поширення.

Для чого цей звіт?

Ми, експерти Nadiyno.org, розробили цей звіт, щоб:

1. **Підкреслити значущість проблеми**: одне з ключових упереджень серед українців, із якими зіштовхується технічна команда Nadiyno – користувачі не вірять, що їхні телеграм-акаунти є цікавими для зловмисників, проте це хибне переконання.
2. **Зрозуміти методи і мислення зловмисників**: ми дослідили, як зловмисники захоплюють акаунти, і розібрали конкретні методи атак, які вони використовують.
3. **Сформувати рекомендації для захисту**: на основі проведеного аналізу ми надаємо практичні поради для захисту облікових записів, зменшення ризиків компрометації та підвищення рівня загальної цифрової обізнаності користувачів.

Цей звіт має на меті не лише проінформувати про небезпеки, але й змотивувати користувачів телеграм дотримуватися правил кібергігієни.

Методологія дослідження

Методологія дослідження базувалася на комплексному підході до збору та аналізу даних, з акцентом на практичний аналіз реальних кейсів. Зокрема, щоби дізнатися, як саме зловмисники отримують доступ до облікових записів телеграм, ми проаналізували сотні реальних випадків, які описували в зверненнях на гарячу лінію Nadiyno.org.

Етапи збору даних

Збір даних здійснювався за такими напрямками:

1. **Аналіз звернень клієнтів на гарячу лінію Nadiyno.org:**
    - Вибірка звернень, що стосувалися компрометації облікових записів телеграму.
    - Аналіз описаних користувачами обставин зламу та методів шахрайства.
    - Ідентифікація найпоширеніших схем отримання несанкціонованого доступу.
    - Виявлення сценаріїв подальшого використання зламаних акаунтів.
    - Систематизація та категоризація методів атак за типами та темою.
2. **Моніторинг відкритих джерел інформації:**
    - Пошук додаткових відомостей про шахрайські схеми та інші методи атак у відкритих джерелах, таких як форуми, соціальні мережі, тематичні блоги та спеціалізовані ресурси.
3. **Технічне дослідження виявлених фішингових вебресурсів:**
    - Аналіз фішингових сайтів, знайдених через гарячу лінію та пошукові системи.

Технічні методи дослідження

У межах технічного дослідження було застосовано такі методи:

1. **Контрольоване тестування фішингових ресурсів:**
    - Використовували тестові акаунти, захищені двофакторною автентифікацією (2FA), для аналізу механізму роботи фішингових сайтів.

- Фіксували поведінку сайтів після введення облікових даних.

2. **Аналіз структури, змісту та логіки роботи фішингових вебресурсів:**
    - **Перехоплення трафіку:**
        - використовували проксі-сервер (Burp Suite) для перехоплення та аналізу HTTP / HTTPS-трафіку.
        - виявляли механізми перенаправлень та структуру вебзапитів.
    - **Фазинг (fuzzing):**
        - застосовували інструменти фазингу для виявлення прихованого змісту та функціоналу вебсайтів.
    - **Деобфускація JavaScript-коду:**
        - щоби зрозуміти приховану логіку роботи фішингових ресурсів, аналізували обфускований код, використовуючи спеціалізовані інструменти, такі як deobfuscate.io.
3. **Виявлення регістраторів доменних імен та хостингових провайдерів фішингових вебсайтів:**
    - використовували WHOIS-запити для отримання інформації про реєстраторів доменних імен;
    - застосовували RDAP-запити для ідентифікації хостинг-провайдерів або провайдерів CDN (Content Delivery Network), що забезпечували інфраструктуру для фішингових сайтів;
    - аналізували отримані дані для виявлення відповідальних організацій та контактних осіб;
    - формували скарги про порушення умов надання послуг, адресовані реєстраторам та хостинг-провайдерам, з метою блокування фішингових ресурсів.

Під час аналізу ми приділили особливу увагу безпеці. Щоби не ризикувати реальними даними користувачів, усі тести проводилися у захищеному середовищі з використанням спеціально створених для дослідження облікових записів.

Навіщо шахраям телеграм-акаунти?

За даними досліджень, незважаючи на російське походження, телеграм є найпопулярнішою соціальною мережею в Україні. На кінець 2023 року 75% українців використовували телеграм для спілкування, а 72% отримували звідти новини. Більшість користувачів переконані, що їхні облікові записи не цікаві для

зловмисників. Втім, понад 70% звернень на гарячу лінію з цифрової безпеки Nadiyno.org стосується саме шахрайських дій, у яких телеграм-акаунт стає інструментом для маніпуляцій та обману.

Навіть якщо у ваших чатах не знайдеться чутливої інформації, ваш акаунт може бути використаний для атак на інших користувачів.

Ось основні цілі шахраїв:

Для фінансової вигоди

Основна мотивація шахраїв — гроші. Зловмисники, до прикладу, викрадають акаунт і звертаються до контактів жертви з проханням терміново перевести кошти. У випадках, коли серед листувань знаходять чутливу інформацію, злочинці можуть вдаватися до шантажу власника акаунту передати чи зробити ці дані публічними.

Для подальшої компрометації контактів

Шахраї можуть використовувати викрадений обліковий запис для розповсюдження фішингових повідомлень контактам жертви, змушуючи їх переходити за посиланнями або встановлювати шкідливі програми.

Для отримання доступу до конфіденційної інформації

Найнебезпечнішими є випадки, коли серед листувань або в нотатках жертви знаходять конфіденційну інформацію: паролі, банківські реквізити, документи, чутливі дані, комерційні таємниці тощо. Це може стати початком ланцюгової реакції: компрометації інших облікових записів, фінансових втрат або й витоку інформації, що має стратегічну цінність.

Основні вектори атак

Аналіз інцидентів показав, що основним способом компрометації акаунтів у телеграмі є **фішингові атаки**. Шахраї поєднують соціальну інженерію та технічні методи для обману користувачів.

Додатково до основного вектору атаки, кіберзлочинці часто використовують методи **OSINT** (Open Source Intelligence) — зокрема для збору допоміжної інформації про потенційні цілі. Хоча сам по собі OSINT не викликає компрометацію акаунтів, зібрані дані допомагають зловмисникам зробити фішингові атаки більш персоналізованими та переконливими.

Окремо варто відзначити метод викрадення облікових записів через **перехоплення SMS-повідомлень**. Хоча ця техніка потребує значних ресурсів та підготовки, вона залишається реальною загрозою — особливо для

журналістів, громадських активістів, політиків, інфлуенсерів та інших публічних осіб.

Також одним із методів компрометації облікових записів є їх викрадення через **шкідливе програмне забезпечення**. Є багато «альтернативних» застосунків клієнта телеграму, які обіцяють додаткові функції, як-от збереження видалених повідомлень або безкоштовний доступ до преміум-можливостей. Встановлення таких програм може відкрити доступ шахраям як до вашого акаунту, так і до вашого пристрою в цілому.

Соціальна інженерія та фішингові атаки

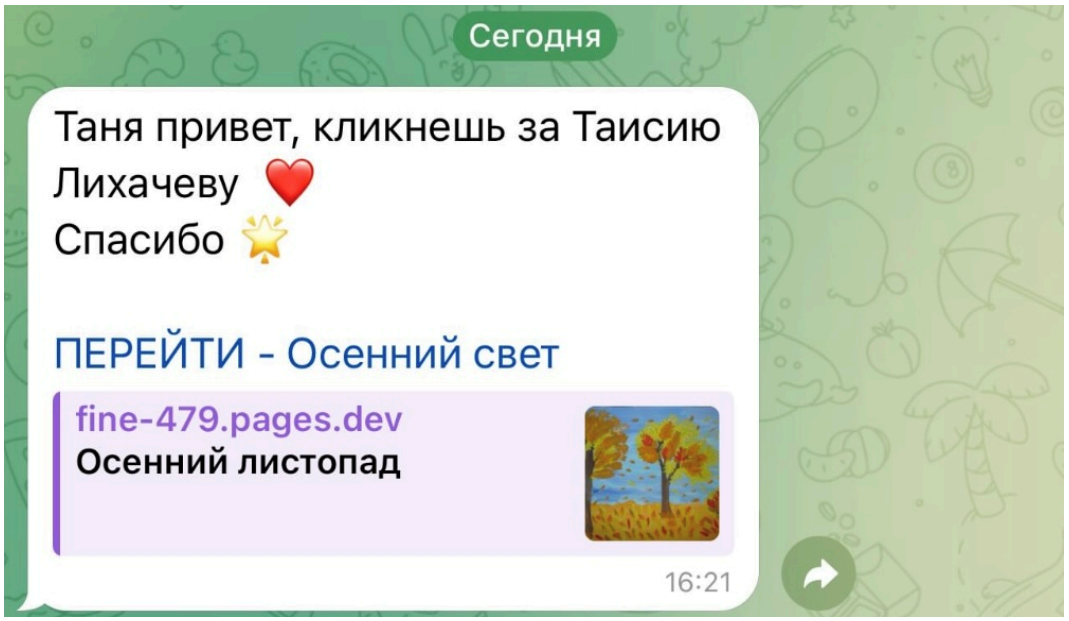
Соціальна інженерія та фішинг є одними із найефективніших векторів атак за останні роки. Люди часто не мають достатніх знань про цифрову безпеку – і шахраї це використовують. Зловмисники моделюють ситуації, щоби змусити людей добровільно віддати доступ до своїх акаунтів.

Особливо небезпечними такі атаки стають у воєнний час, коли люди перебувають під постійним психоемоційним напруженням.

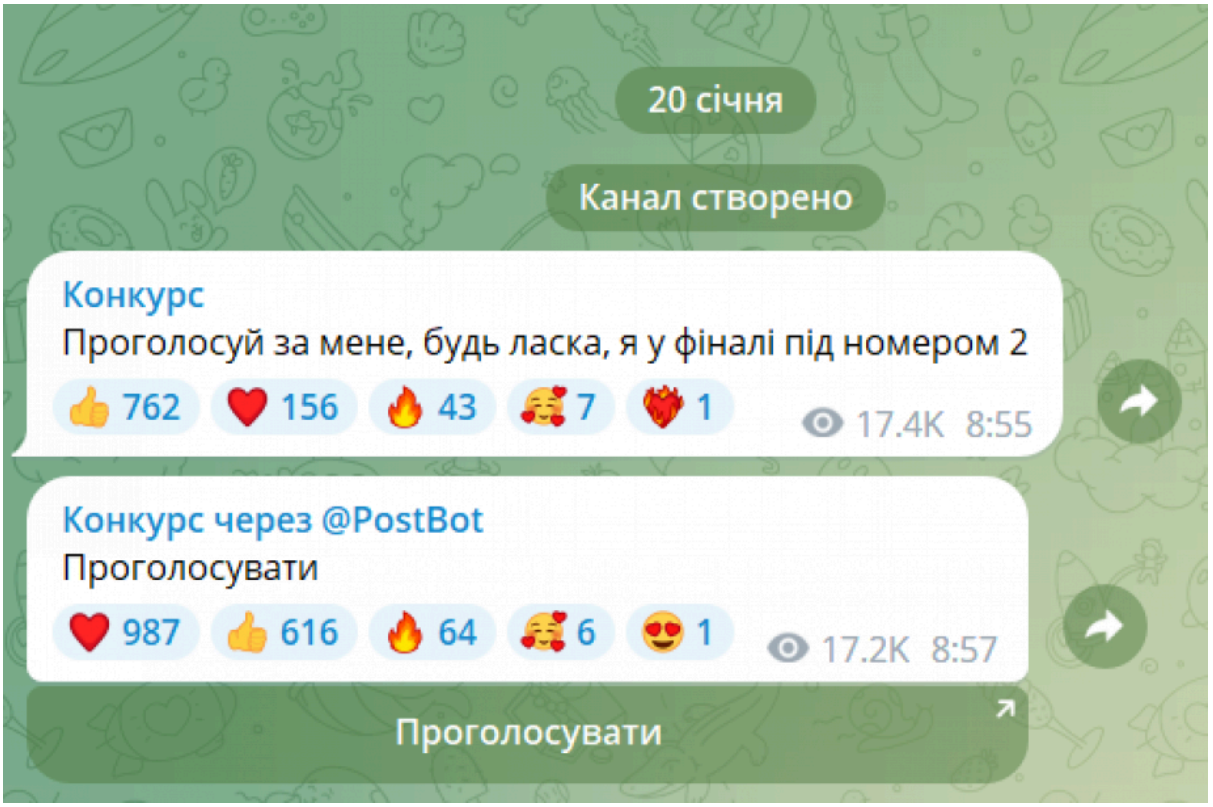
Важливо зазначити, що жертвами фішингу можуть стати не тільки пересічні користувачі, а й великі компанії з висококваліфікованими спеціалістами.

Приклад фішингової схеми 1. Голосування

Однією із найпоширеніших і найпростіших фішингових схем, пов'язаних зі зламом телеграм-акаунтів, є схема, за якою зловмисник спонукає користувача «взяти участь у голосуванні», змушуючи його перейти за шкідливим посиланням. Нижче приклади схожих повідомлень:

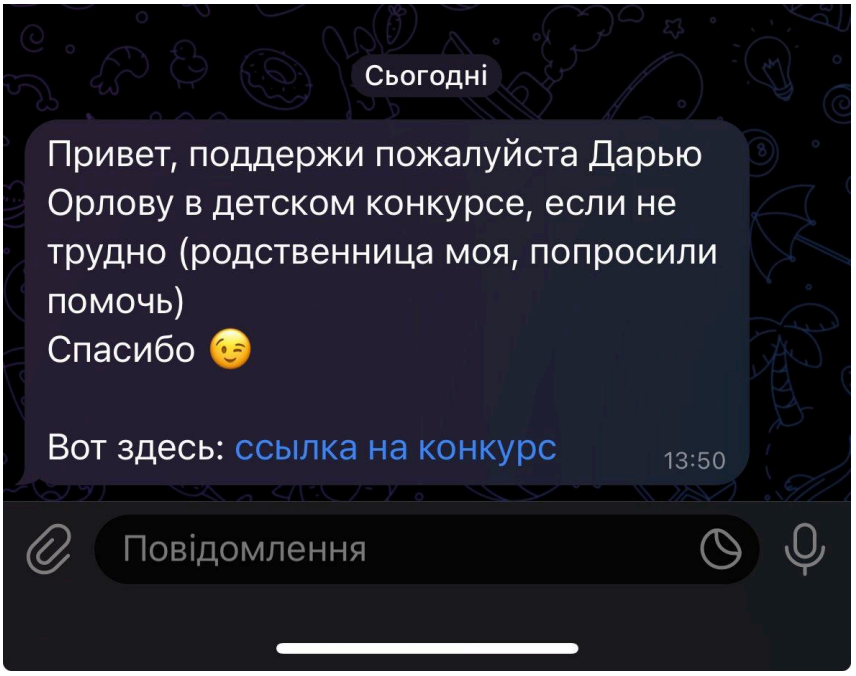


Джерело: Звернення на гарячу лінію Nadiyno.org

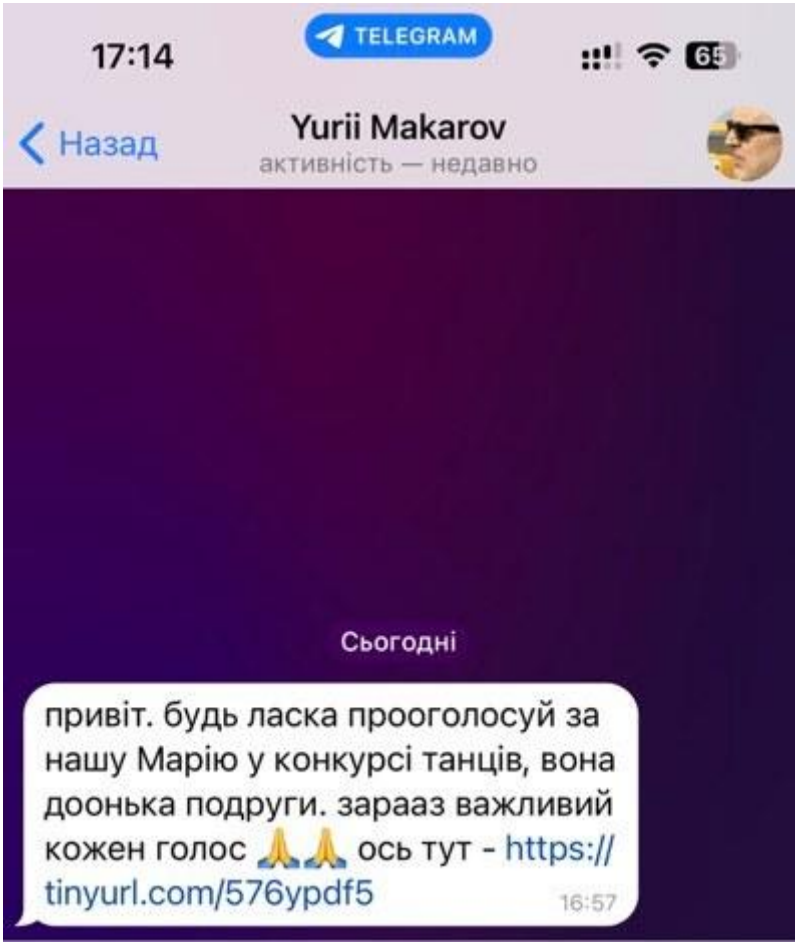


Джерело: Публікація у медіа Район.in.ua

Також зловмисники часто вбудовують посилання у текст або скорочують його за допомогою спеціалізованих сервісів. Це, в свою чергу, ускладнює процес візуальної ідентифікації підозрілих URL-адрес і збільшує ймовірність натискання на посилання.

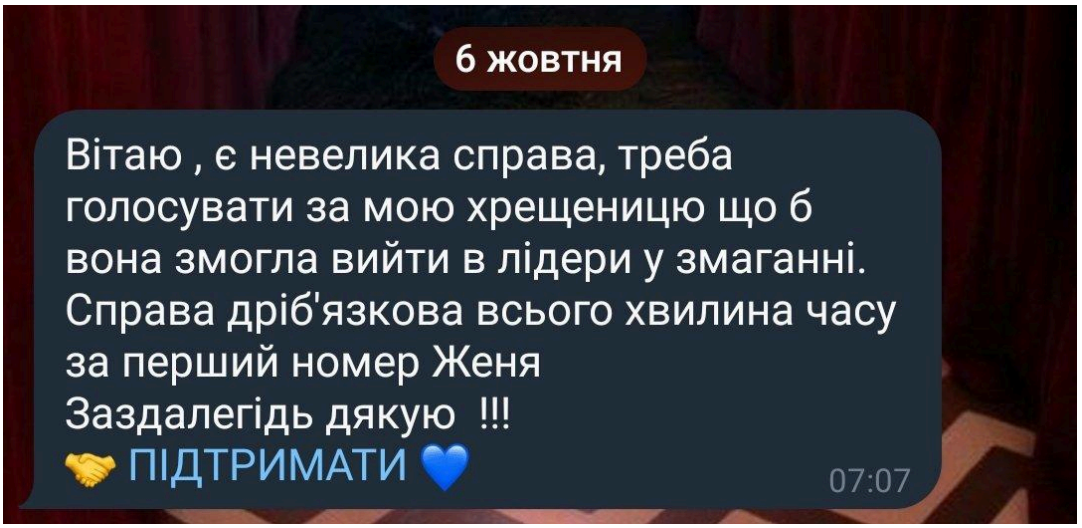


Джерело: Публікація на X



Джерело: Media Sapiens

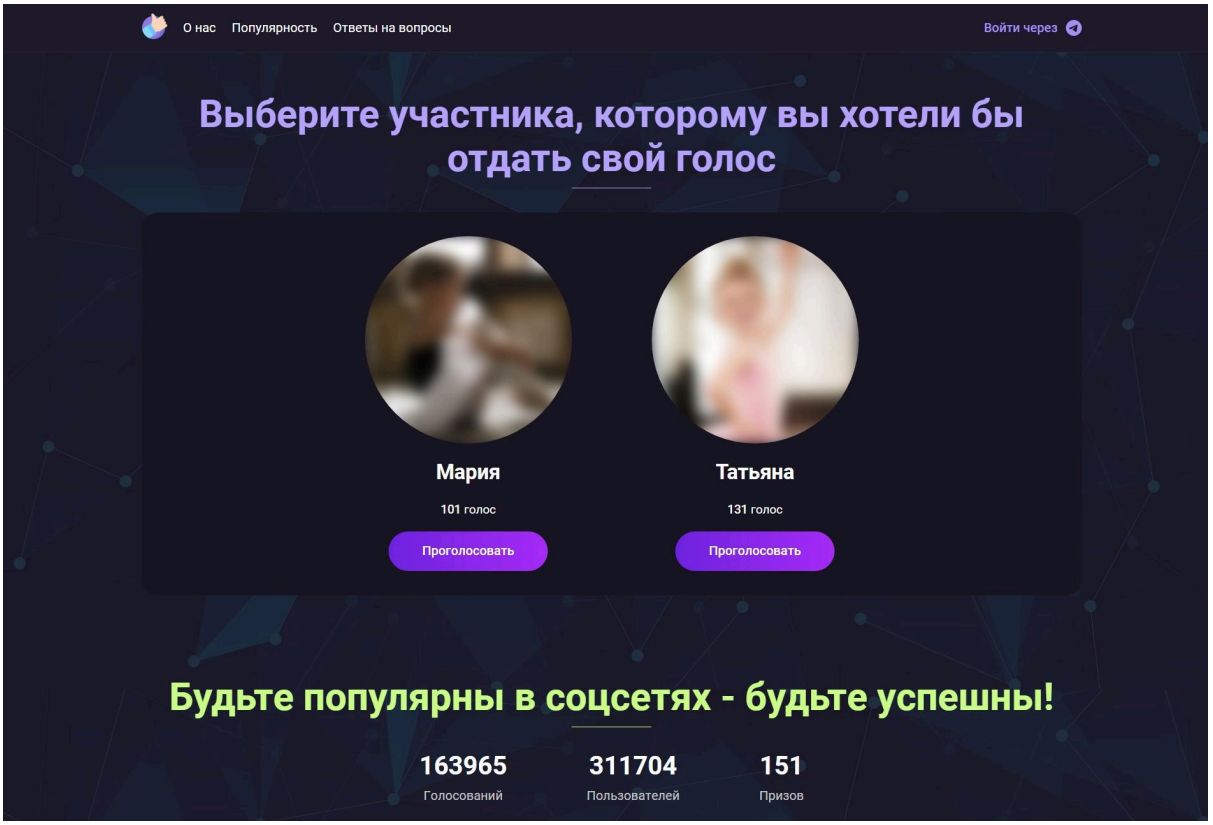
Іноді шахраї надсилають такі фішингові повідомлення з уже зламаних акаунтів знайомих.



Джерело: Публікація на X

Джерело: [Голос Громад]

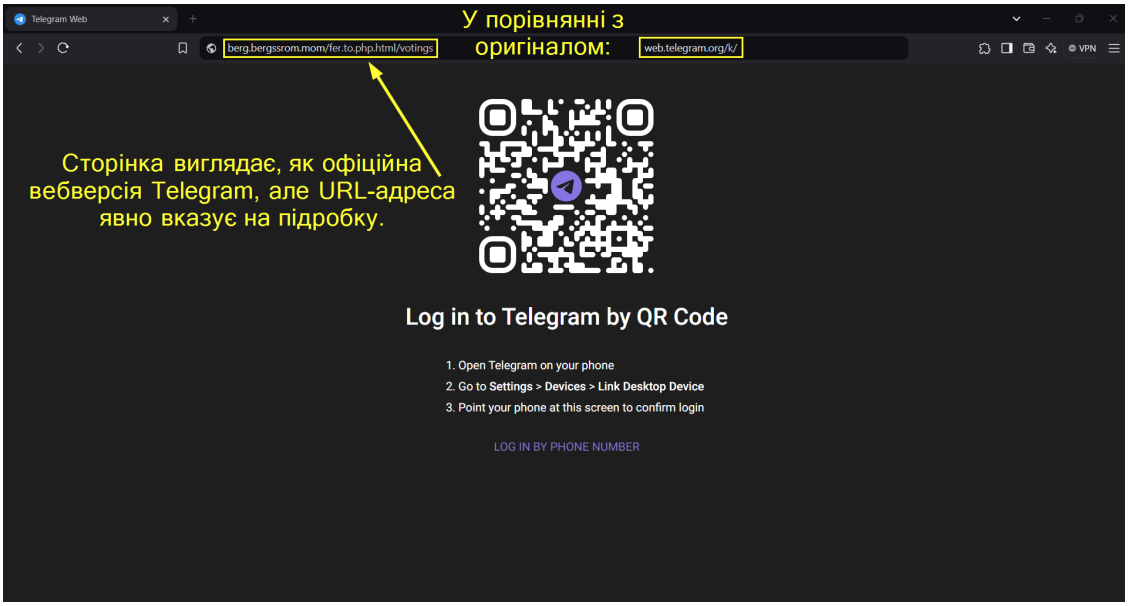
Нижче – приклади того, як виглядають вебсторінки, на які ведуть фейкові прохання взяти участь у голосуваннях:



Джерело: Фішинговий вебсайт

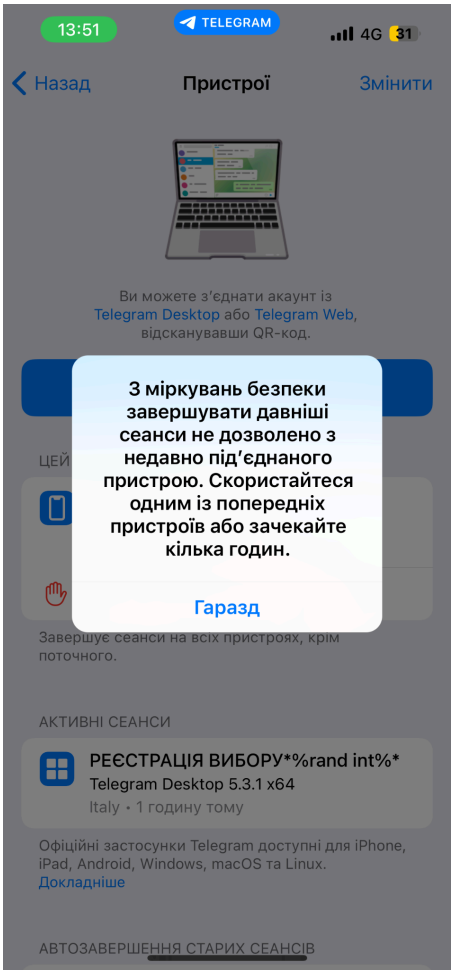
Джерело: Фішинговий вебсайт

Наступний етап цієї фішингової схеми найчастіше виглядає таким чином: коли користувач намагається проголосувати, сайт просить увійти через телеграм. Наприклад, може з'явитися QR-код для прив'язки нового пристрою.



Джерело: Фішинговий вебсайт

Коли користувач відсканує цей код, шахрай отримає доступ до акаунту. Якщо жертва не помітить факт зламу, через 24 години зловмисник зможе зробити свій пристрій «довіреним» і навіть викинути з акаунту справжнього власника.

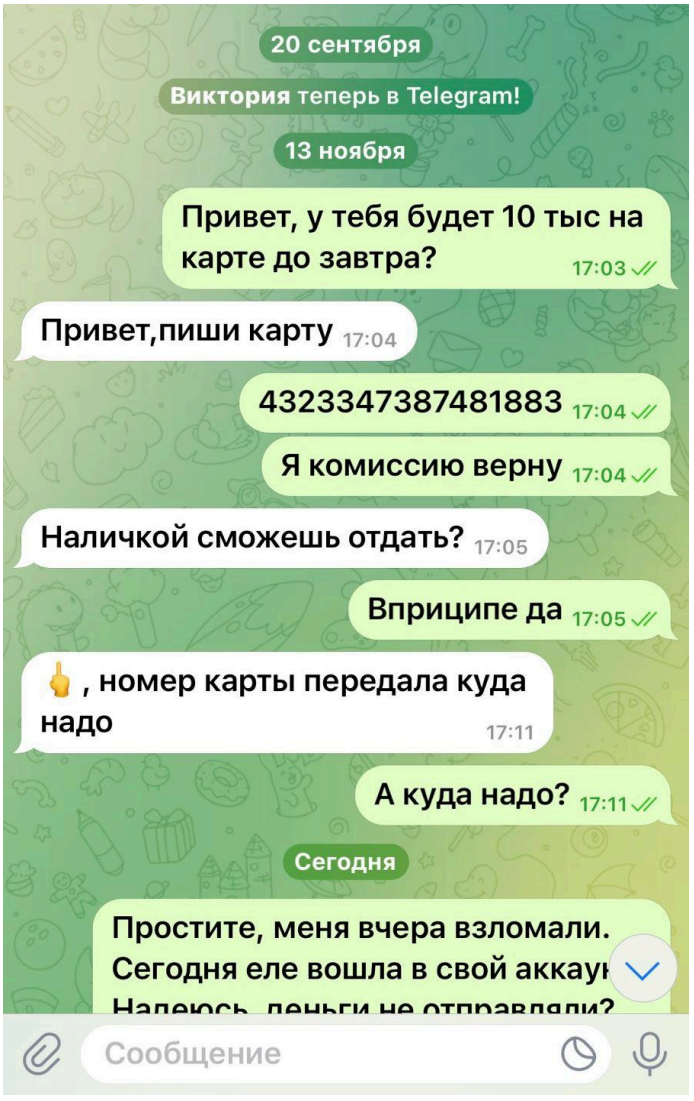


Джерело: Звернення на гарячу лінію Nadiyno.org

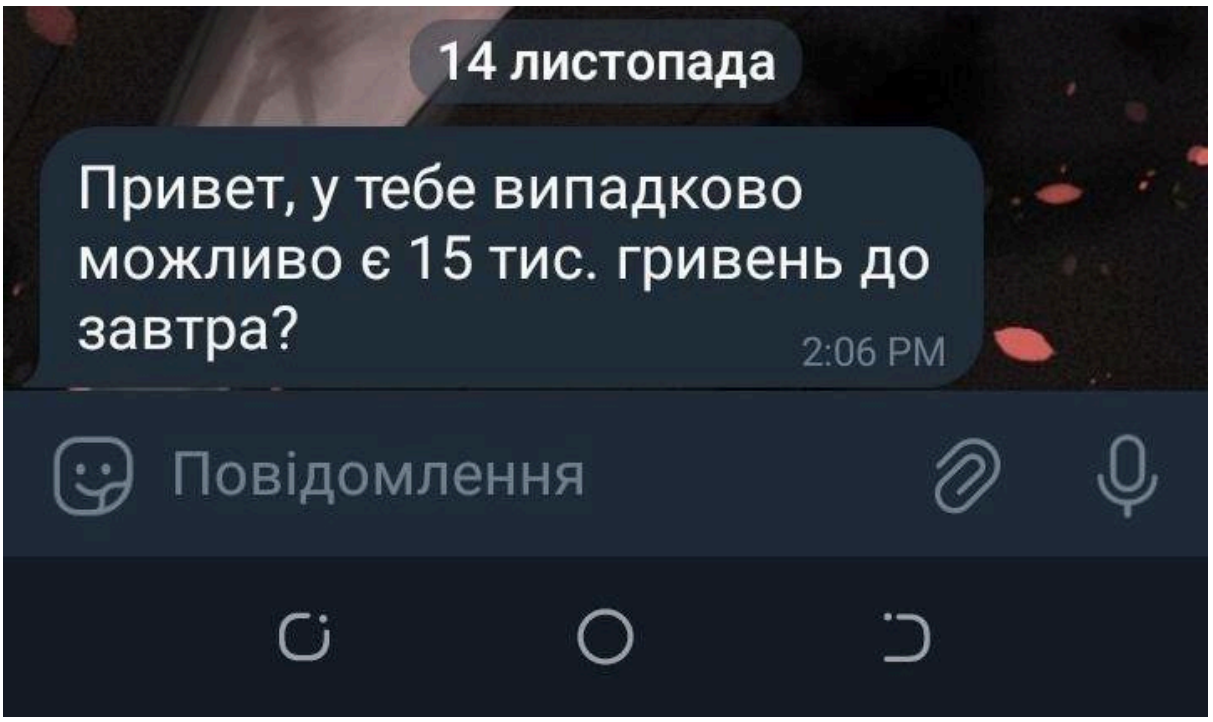
Таким чином, зловмисник може отримати майже постійний доступ до акаунту та обмежити вхід власнику. Більшість користувачів, які зверталися до гарячої лінії Nadiyno.org, скаржилися, що їх одразу викидає з телеграму після входу — ймовірно, цей процес автоматизований.

Ще одна небезпека — швидке поширення атаки. Шахраї, захопивши акаунт, розсилають фішингові повідомлення його контактам, просячи гроші або участь у голосуваннях. Відтак, захоплюються нові облікові записи.

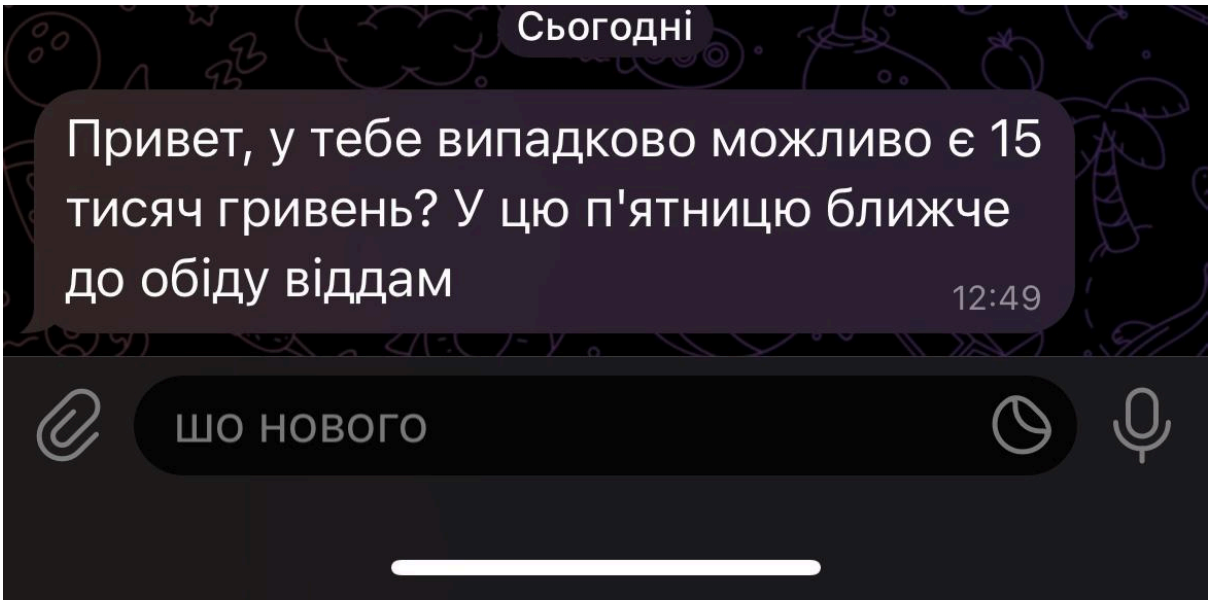
Джерело: [Media Sapiens]



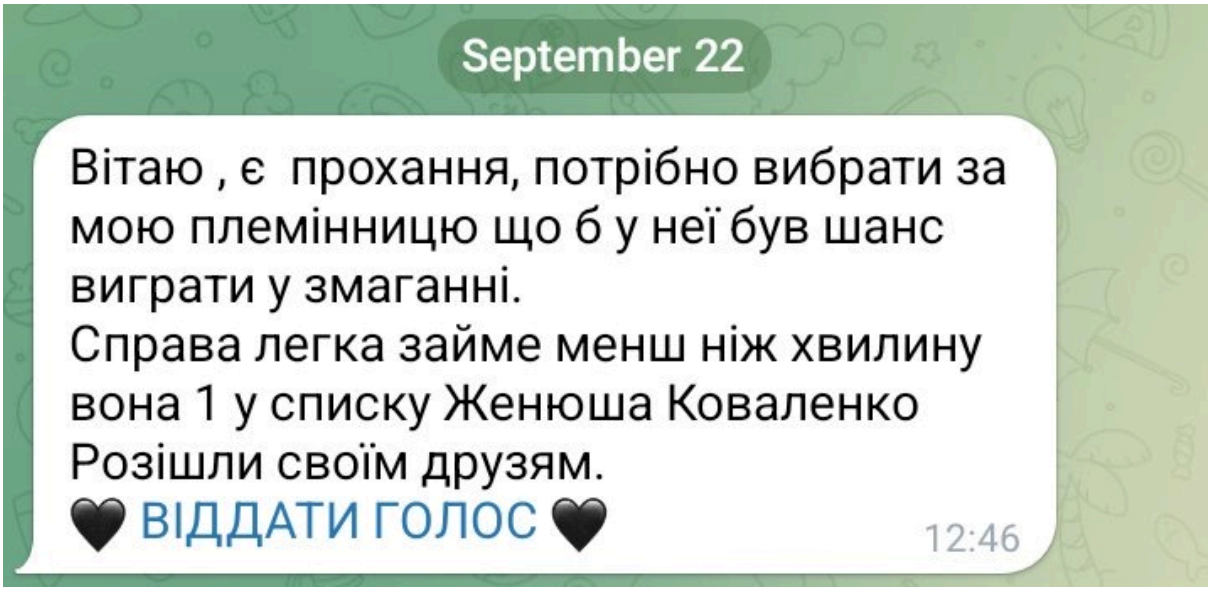
Джерело: Звернення на гарячу лінію Nadiyno.org



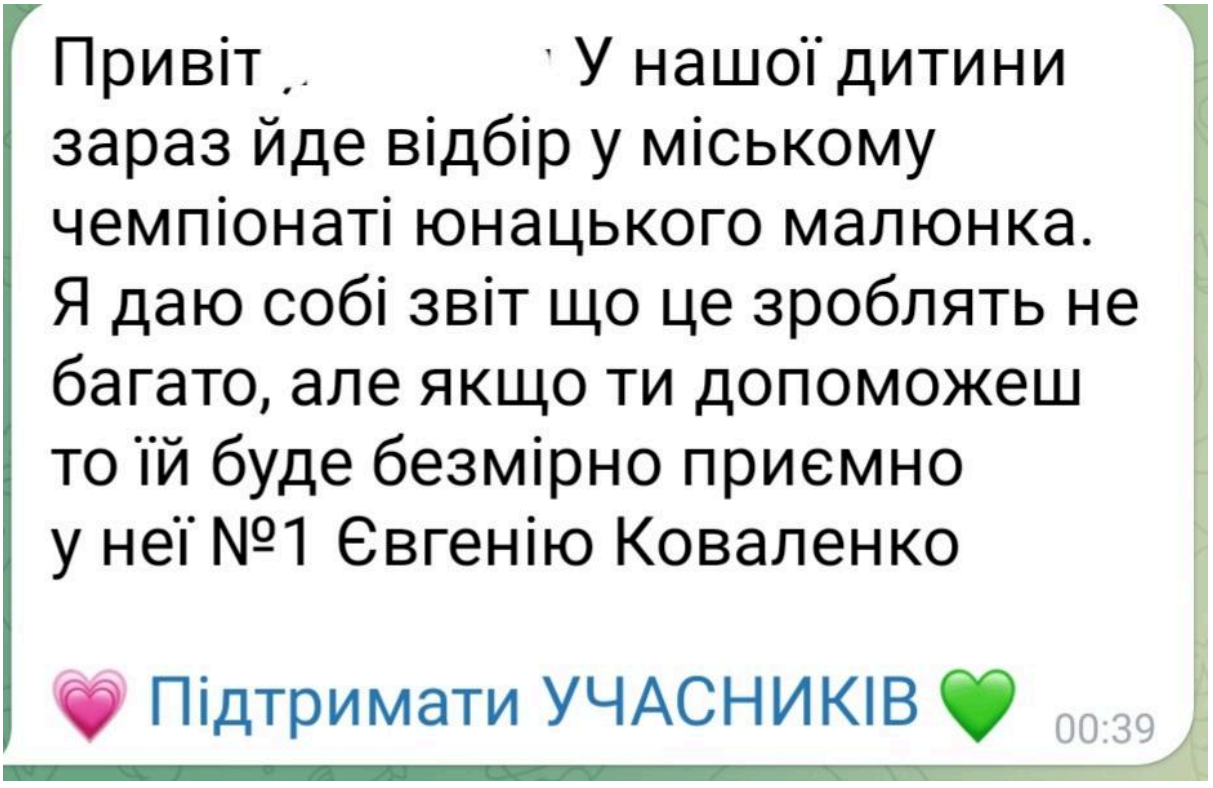
Джерело: Звернення на гарячу лінію Nadiyno.org



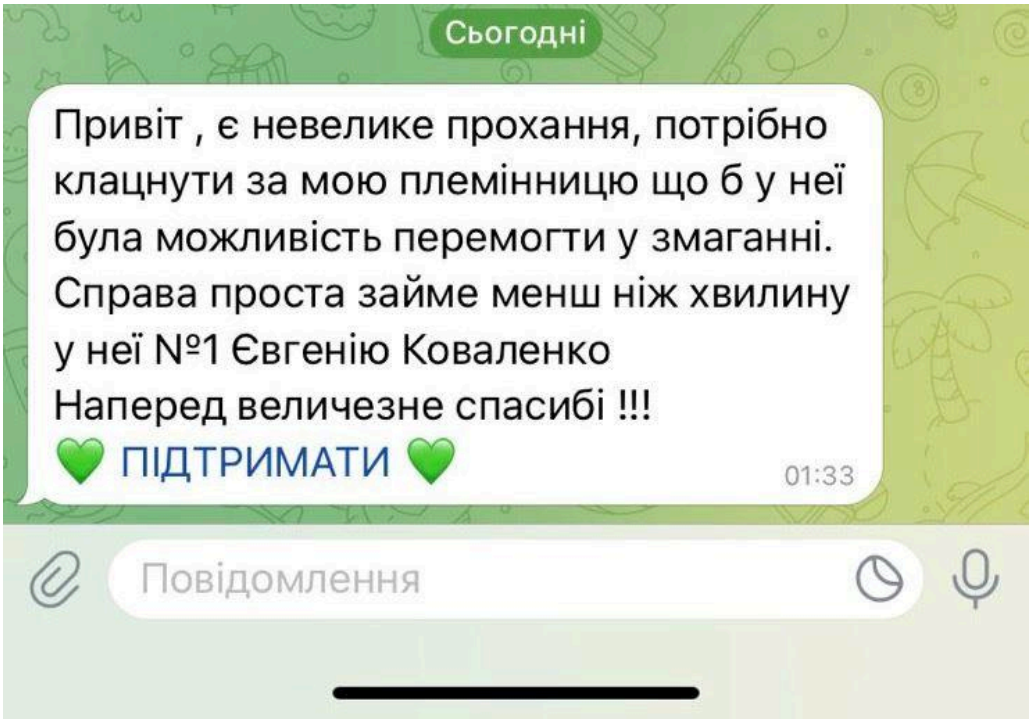
Джерело: Звернення на гарячу лінію Nadiyno.org



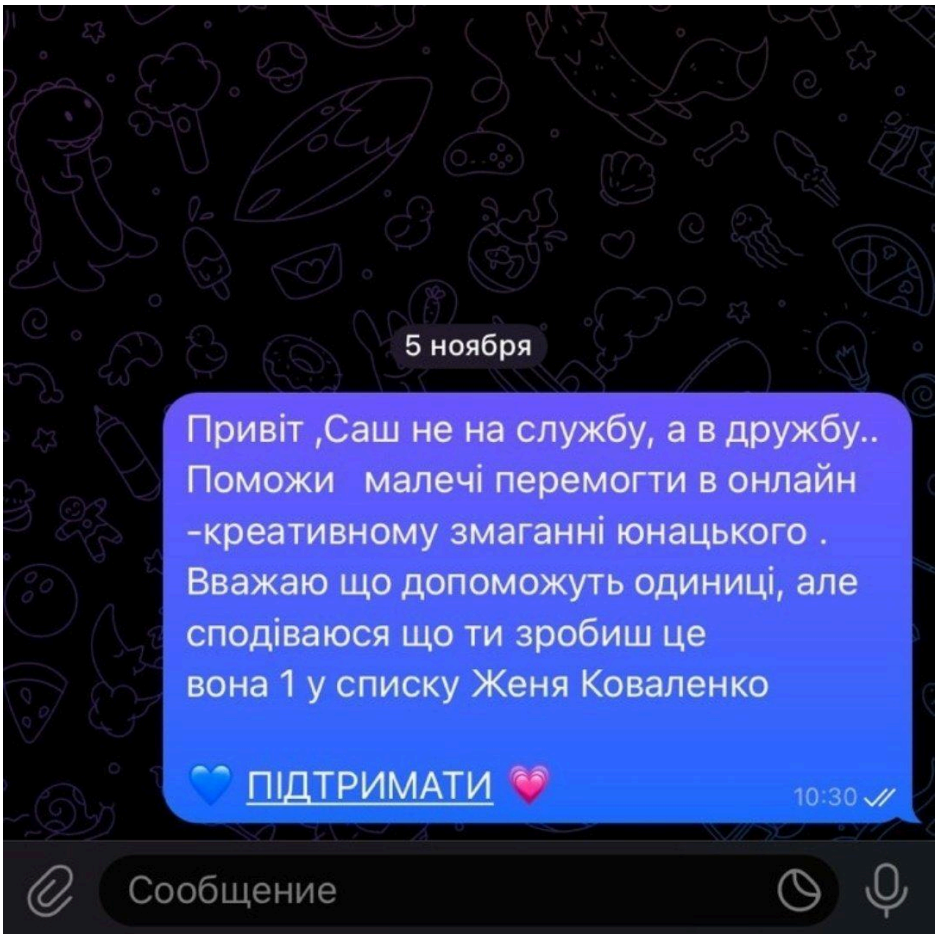
Джерело: Звернення на гарячу лінію Nadiyno.org



Джерело: Публікація на X

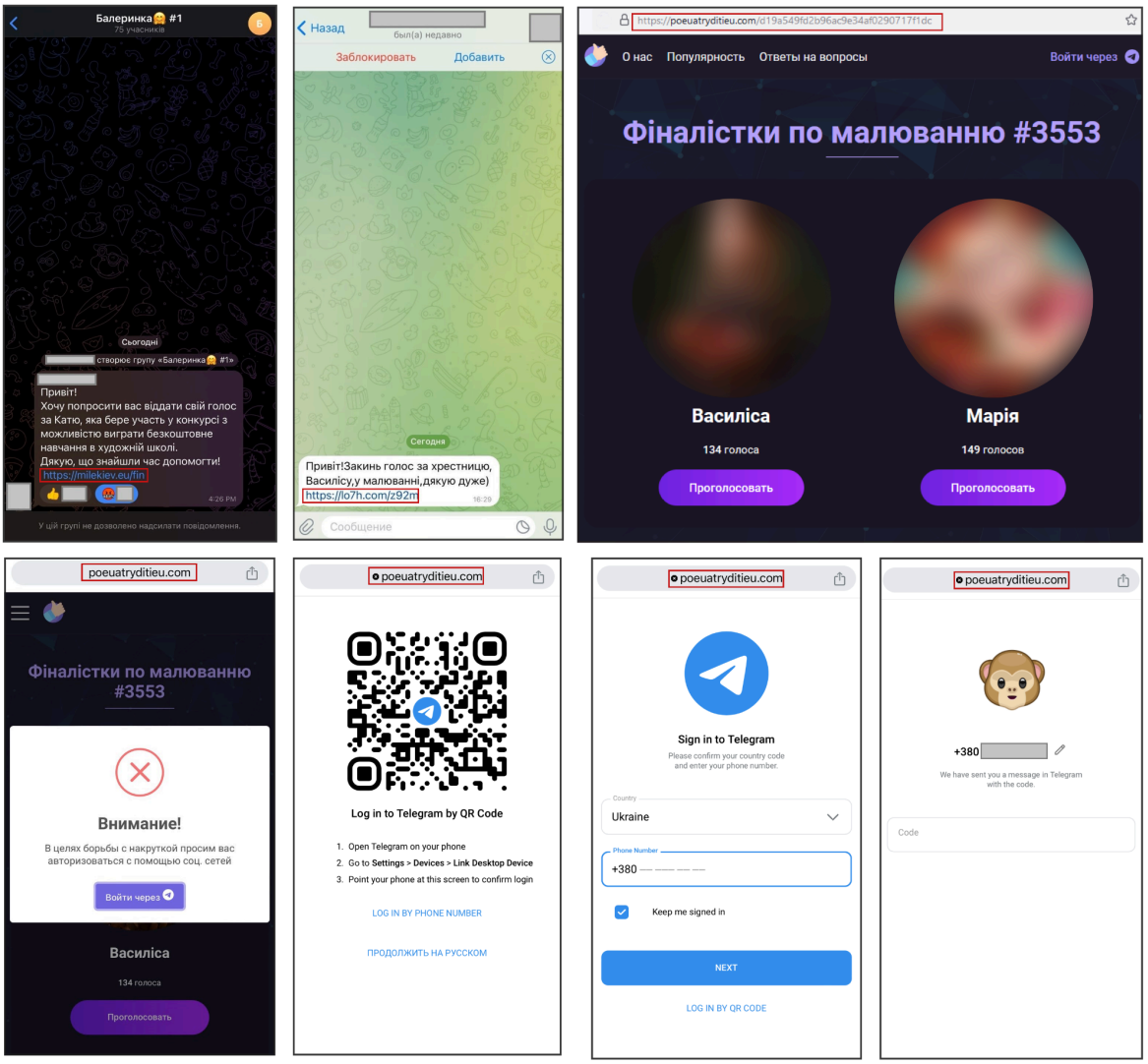


Джерело: Звернення на гарячу лінію Nadiyno.org



Джерело: Публікація на X

Цей метод працює завдяки тому, що люди переважно довіряють повідомленням від знайомих, друзів і родичів. Шахраєві достатньо зламати один акаунт, щоби запустити ланцюгову реакцію подальших зламів. Отже, поєднання такого ефективного методу маніпуляції із низькою обізнаністю в кібербезпеці створює ідеальні умови для швидкого поширення шахрайської схеми.



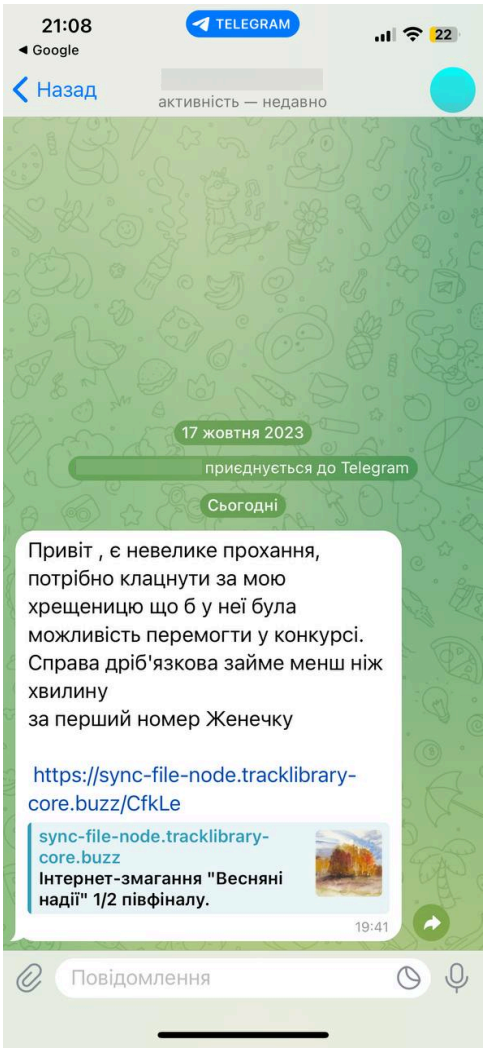
Джерело: [CERT-UA]

Аналіз фішингових вебсайтів

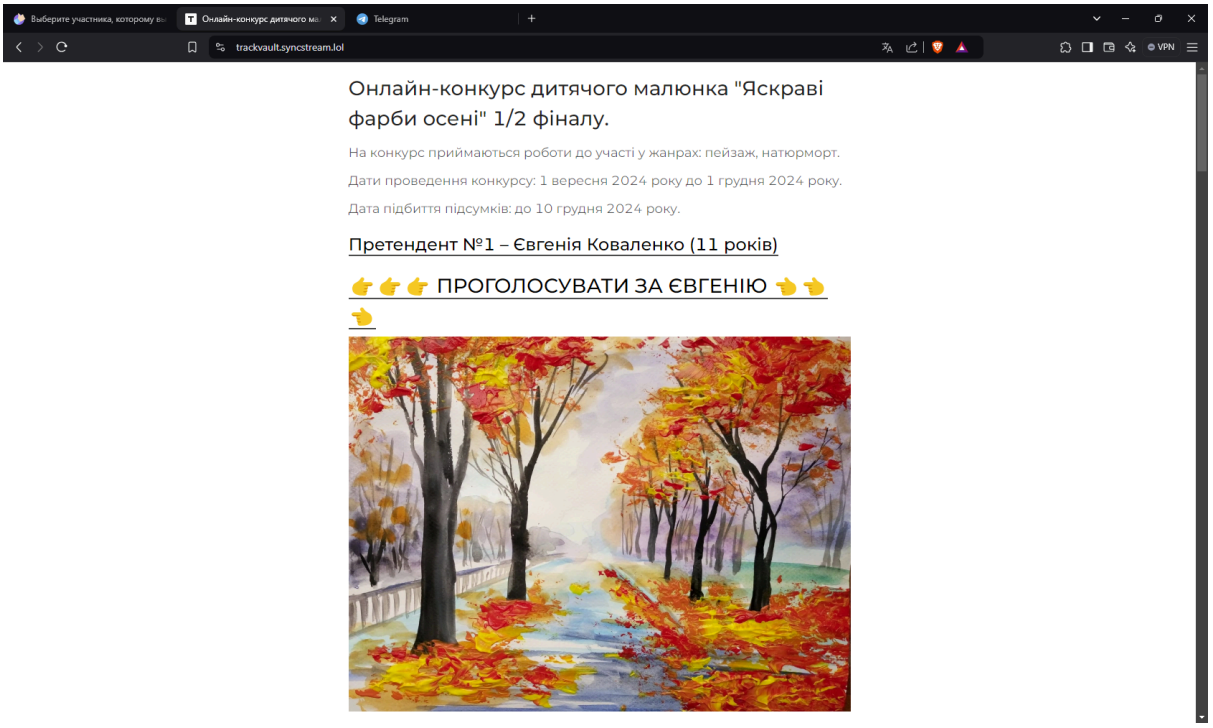
Розберемося, як працюють фішингові сайти, що крадуть телеграм-акаунти, і крок за кроком пройдемо через увесь процес соціальної інженерії.

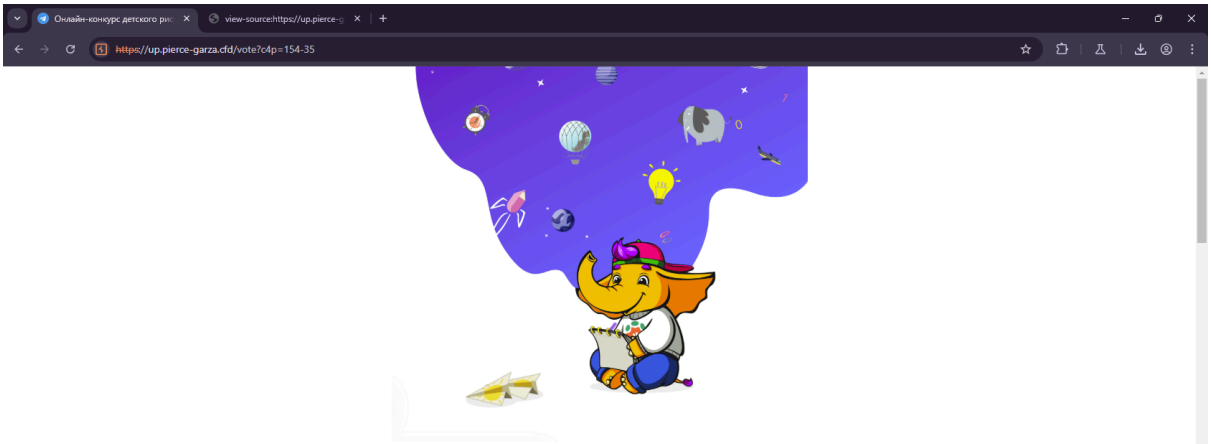
Повідомлення з посиланням. Конкурс малюнків

Спершу користувач отримує повідомлення від знайомого зі списку контактів з емоційним проханням проголосувати за малюнок хрещениці:



Посилання перенаправляє на вебсайт з нібито онлайн-конкурсом дитячих малюнків:





Онлайн-конкурс детского рисунка

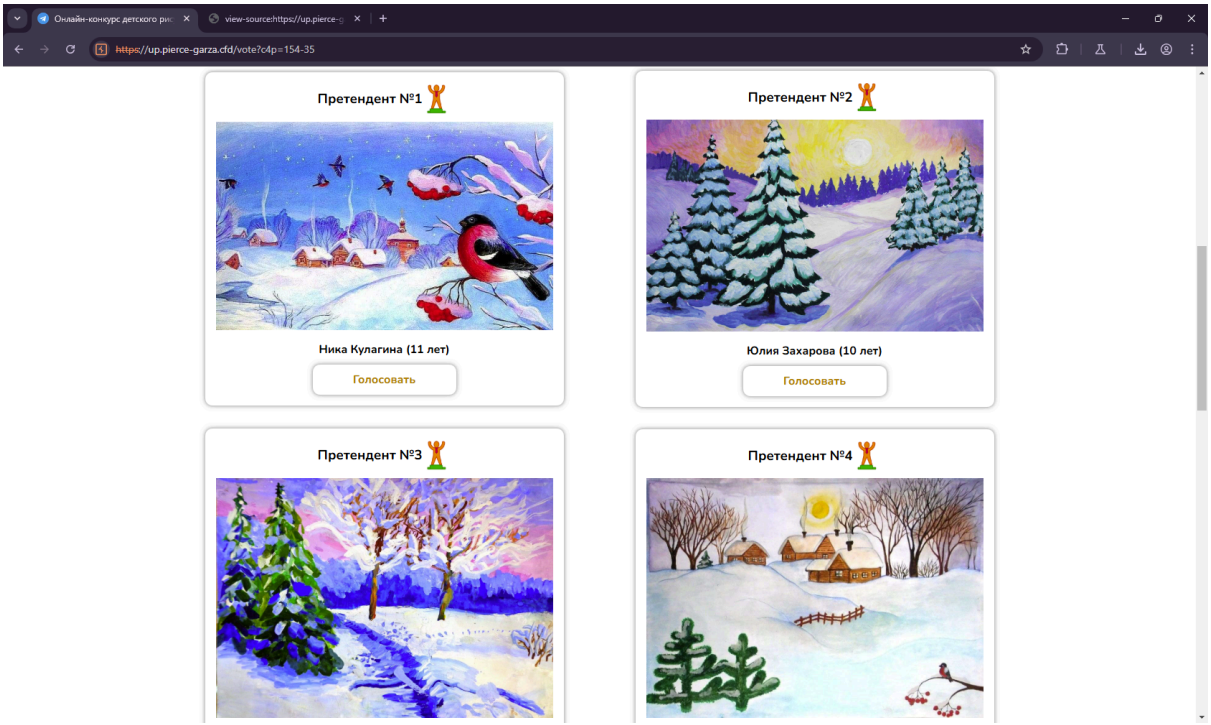
"Морозная сказка"

1/4 финала

На конкурс принимаются к участию работы в жанрах: пейзаж, натюрморт.

ПОДСЧЁТ ГОЛОСОВ ЗАВЕРШИТСЯ ЧЕРЕЗ:

11	13	07
ДНЕЙ	ЧАСОВ	МИНУТ



Претендент №1

Ника Кулагина (11 лет)

Голосовать

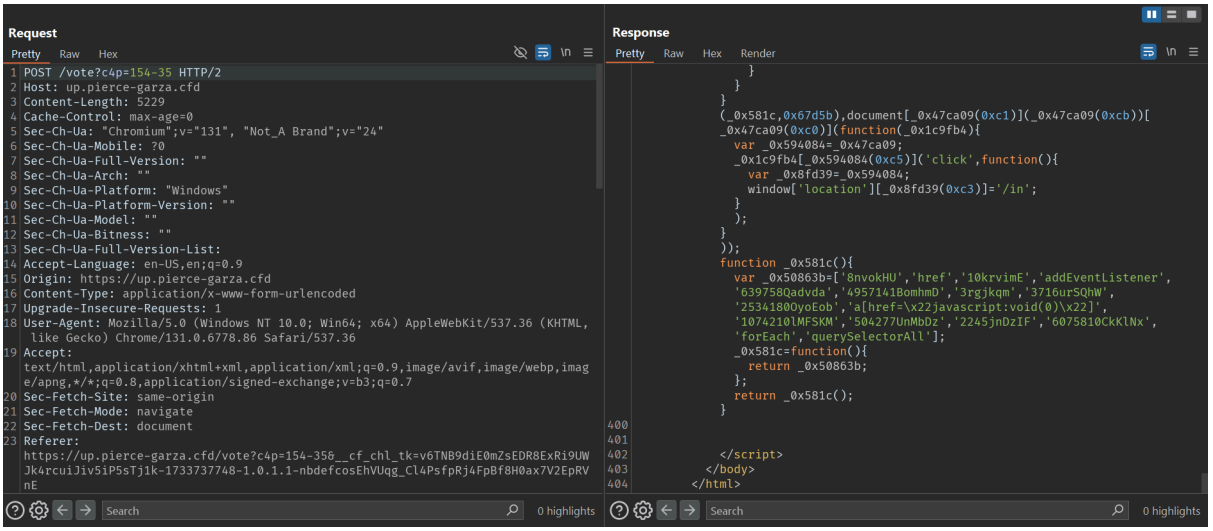
Претендент №2

Юлия Захарова (10 лет)

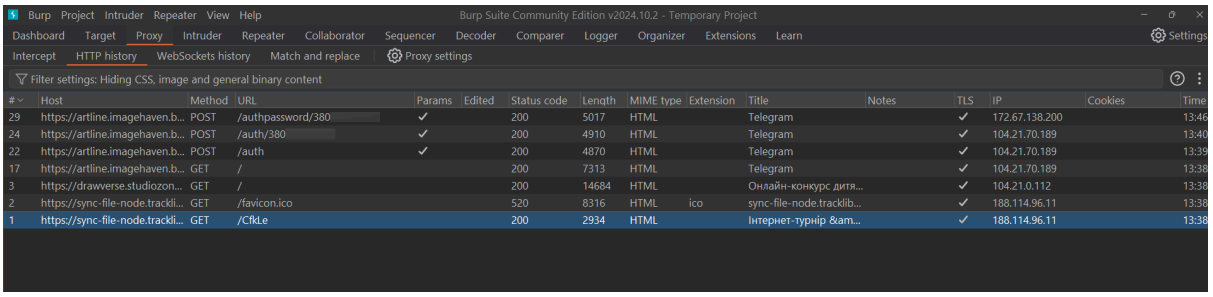
Голосовать

Претендент №3

Претендент №4

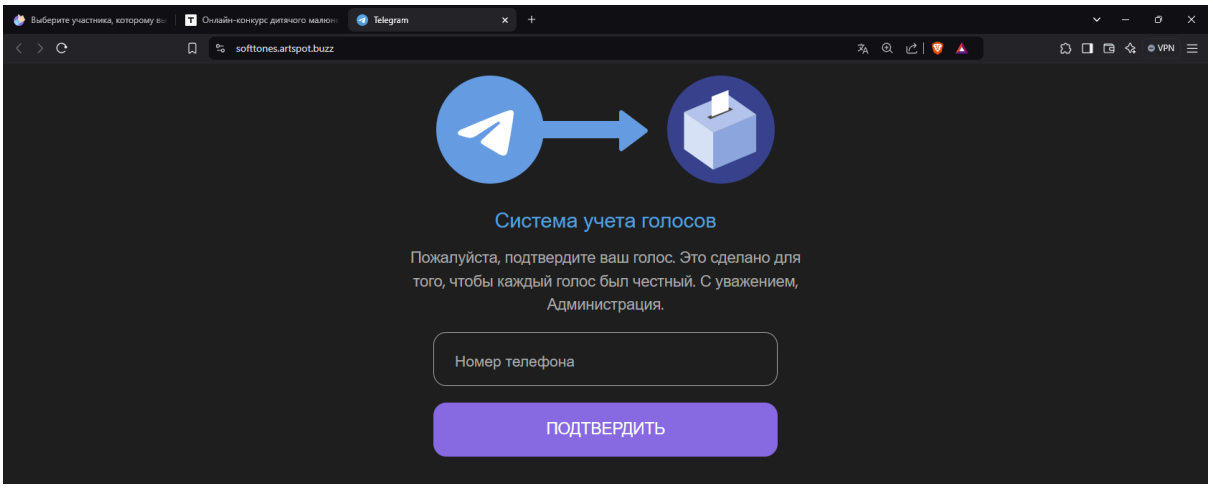


Зазвичай схожі сайти швидко блокують, але тут перше посилання перенаправляло користувачів на працюючі копії сайтів навіть після блокування окремих сторінок.



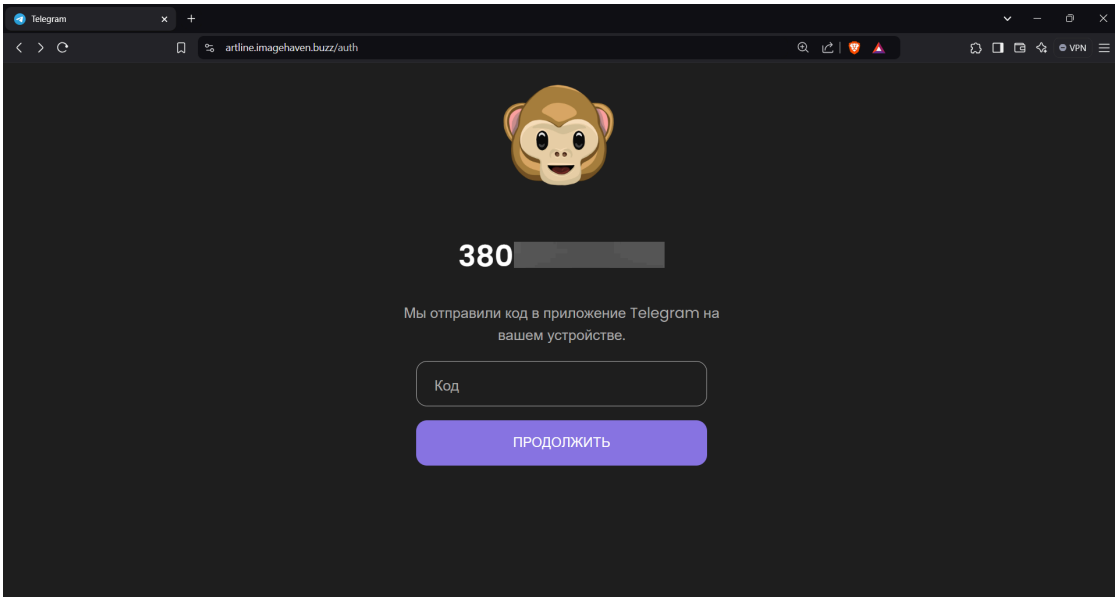
Запит номера телефону

Користувач пробує проголосувати, сайт перенаправляє на інший домен і під приводом «для забезпечення чесності голосування» вимагає номер телефону:

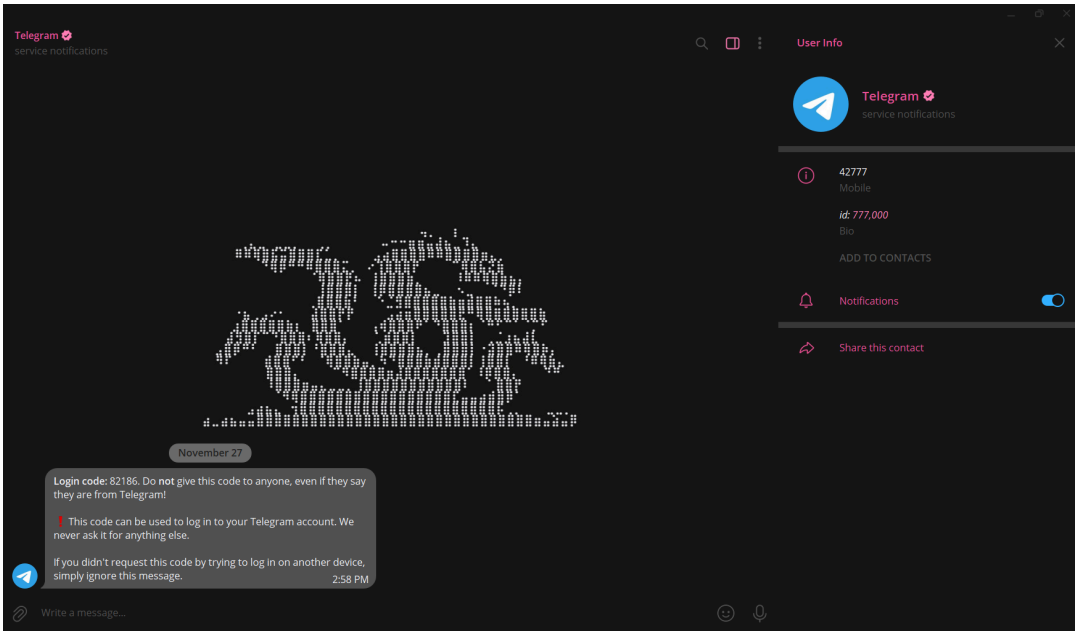


Запит даних авторизації

У користувача жодних підозр. Однак на наступному кроці, повідомляють про надсилання коду в застосунок телеграм.



Це було би прийнятним, якби адміністрація сама зв’язалася з користувачем і надіслала код у приватні повідомлення. Але насправді код приходить у чат службових сповіщень телеграму, тому що зловмисники просто ініціювали вхід у телеграм за номером, який ввів користувач.

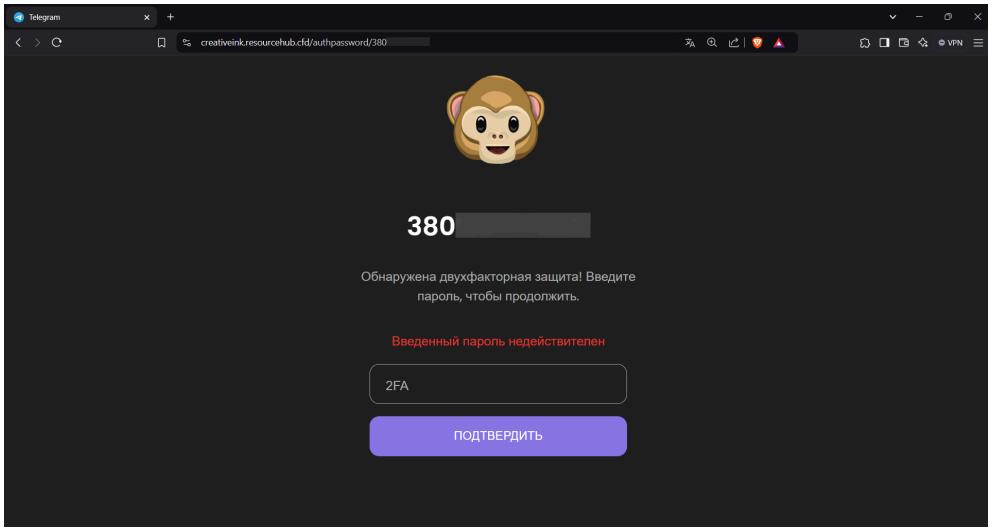


У повідомленні від телеграму навіть є попередження такого змісту: «**За допомогою цього коду можна ввійти до вашого телеграм-акаунту. Ми більше ні для чого його не просимо. Якщо ви не намагаєтесь увійти з**

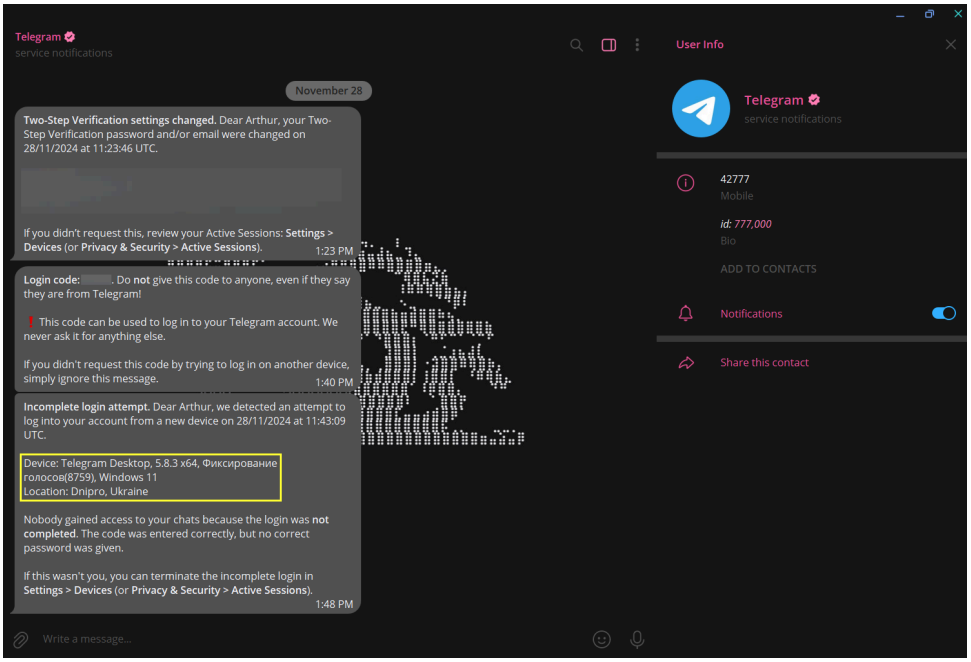
іншого пристрою, проігноруйте це повідомлення». Проте часто користувачі не звертають на це уваги.

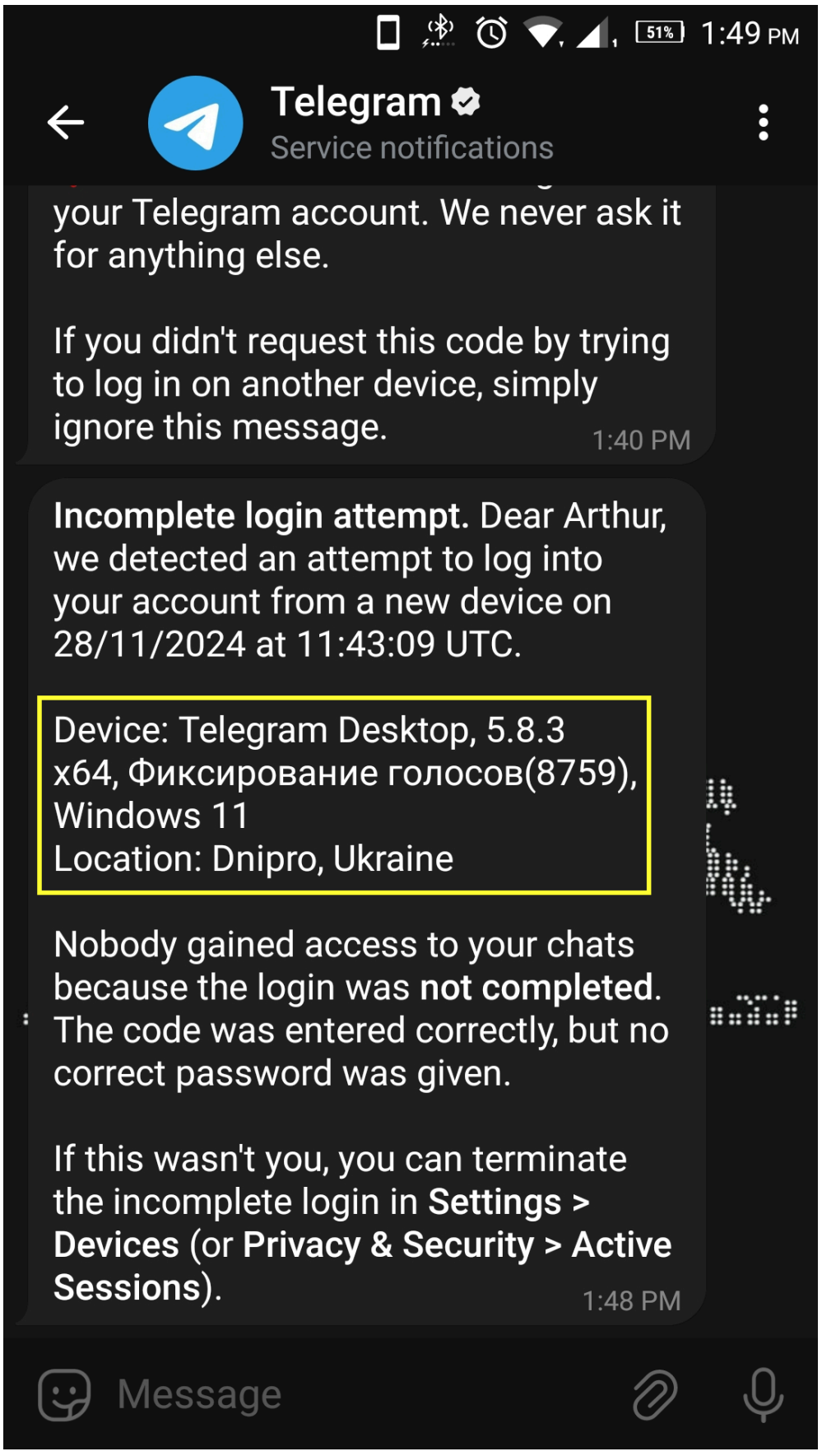
Якщо у користувача не налаштована двоетапна перевірка, і він при цьому введе код на фішинговому сайті — зловмисники отримають доступ до його акаунту. Телеграм надішле повідомлення про вхід з нового пристрою, але шахраї, ймовірно, одразу його видалять.

Якщо ж двоетапна перевірка налаштована, вебсайт вимагатиме ввести додатковий пароль до облікового запису:



Якщо все це здасться підозрілим і користувач відмовиться, через деякий час телеграм надішле повідомлення про невдалу спробу входу. У ньому повідомлять час, пристрій, локацію та інструкцію, як завершити сесію зловмисника:




1:49 PM
Telegram
Service notifications
your Telegram account. We never ask it for anything else.
If you didn't request this code by trying to log in on another device, simply ignore this message.
1:40 PM
Incomplete login attempt. Dear Arthur, we detected an attempt to log into your account from a new device on 28/11/2024 at 11:43:09 UTC.
Device: Telegram Desktop, 5.8.3 x64, Фиксирование голосов(8759), Windows 11
Location: Dnipro, Ukraine
Nobody gained access to your chats because the login was not completed. The code was entered correctly, but no correct password was given.
If this wasn't you, you can terminate the incomplete login in Settings > Devices (or Privacy & Security > Active Sessions).
1:48 PM
Message

2:09

Пристрої

Ви можете з’єднати акаунт із
Telegram Desktop або Telegram Web,
відсканувавши QR-код.

З’єднати з комп’ютером

Цей пристрій

[redacted]

Завершити всі інші сеанси

Вийти з акаунта на всіх пристроях, крім цього.

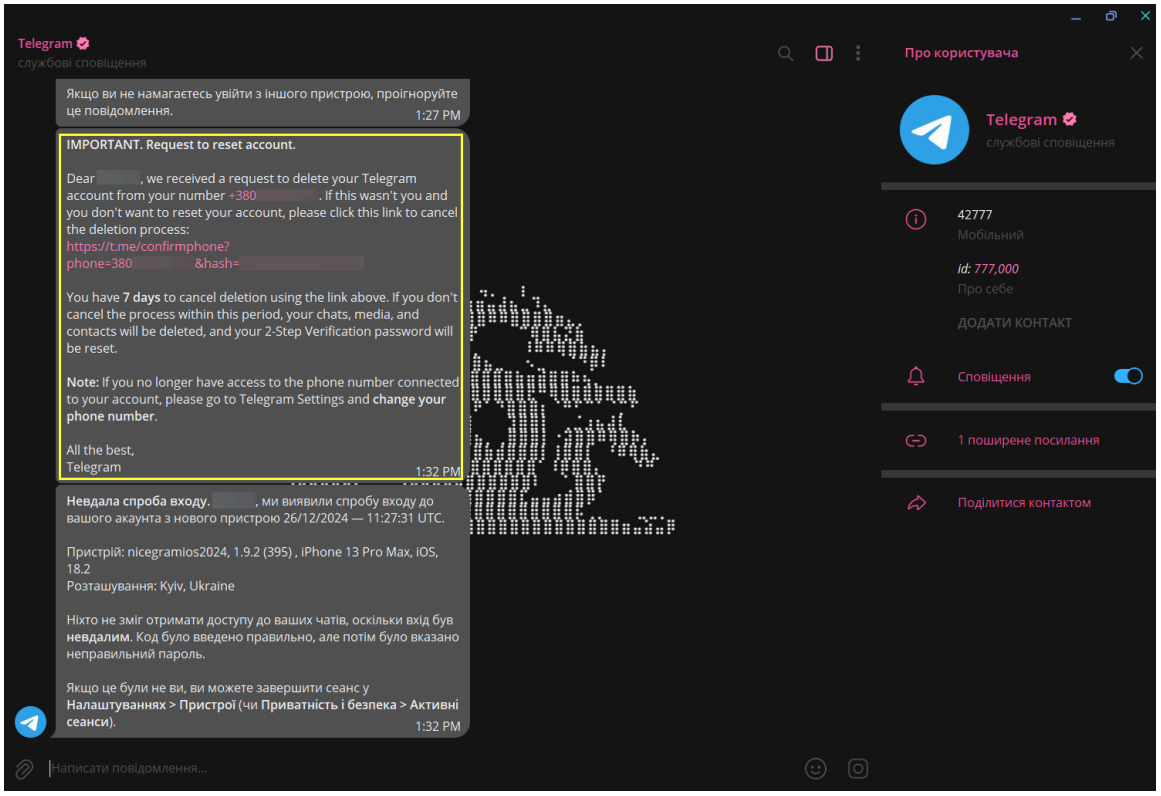
Незавершені спроби входу

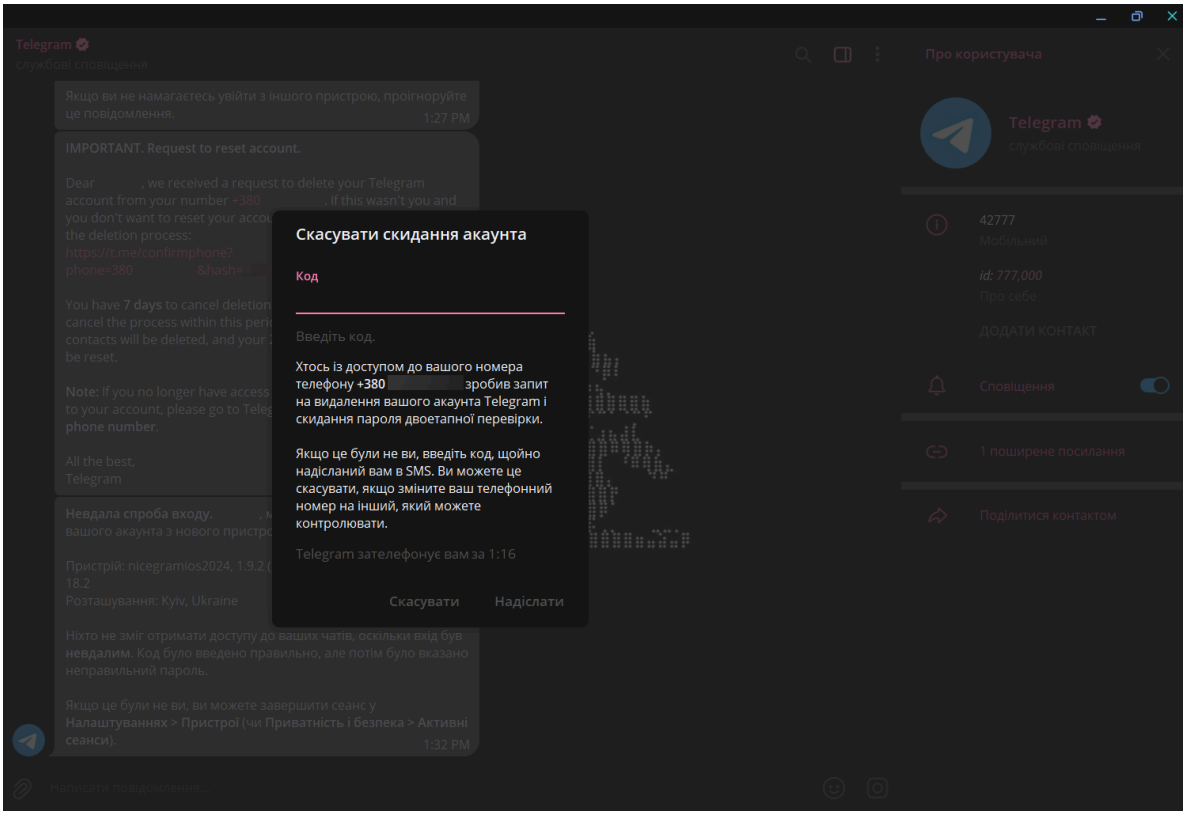
ГОЛОС-4817 ПІДТВЕРДЖЕННЯ
Telegram Desktop 5.9 x64
Boryspil, Ukraine • 2:08 PM

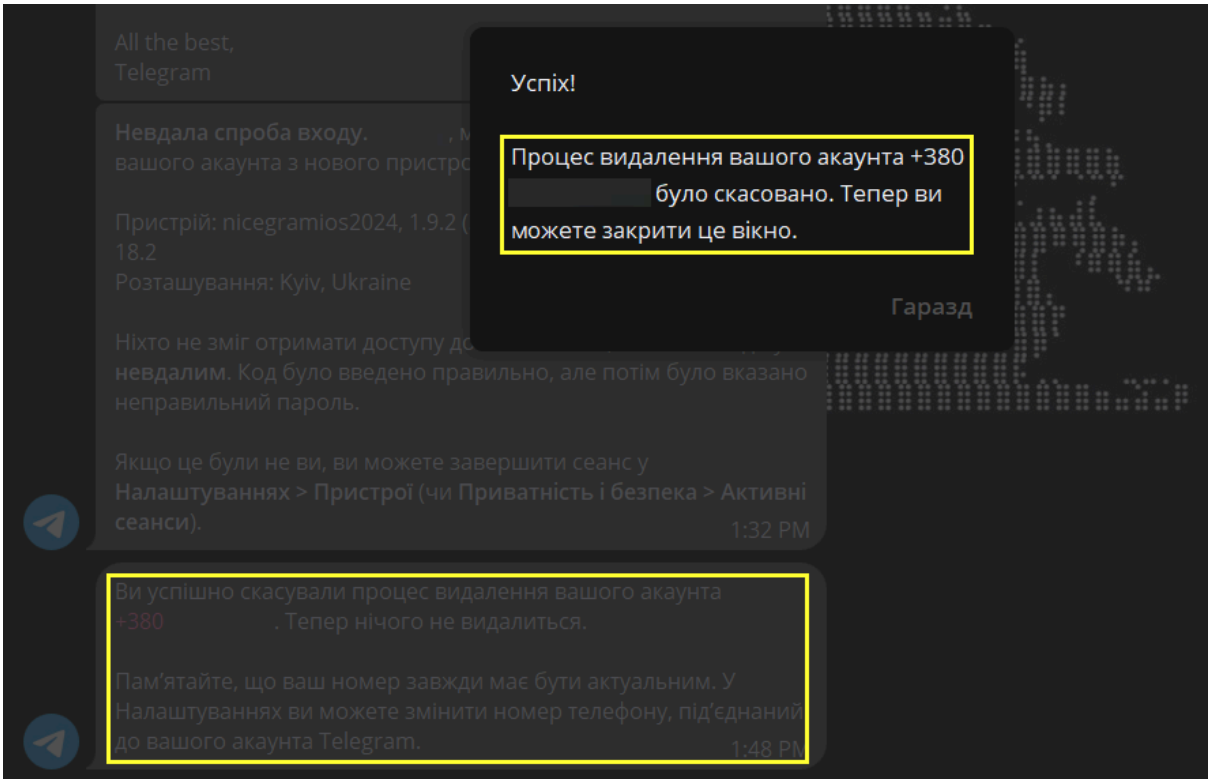
ПЕРЕВІРКА ГОЛОСУ-9736
Telegram Desktop 5.9 x64
Uzhhorod, Ukraine • 1:51 PM

На цих пристроях доступу до ваших повідомлень немає. При вході з них код був уведений правильно, але правильний пароль був не вказаний.

На цьому етапі зловмисники також можуть ініціювати процес видалення акаунту, щоби завдати ще більше шкоди користувачеві. Якщо користувач не помітить сповіщення та не скасує процес видалення, через тиждень обліковий запис буде остаточно знищений — разом із усіма чатами та контактами.

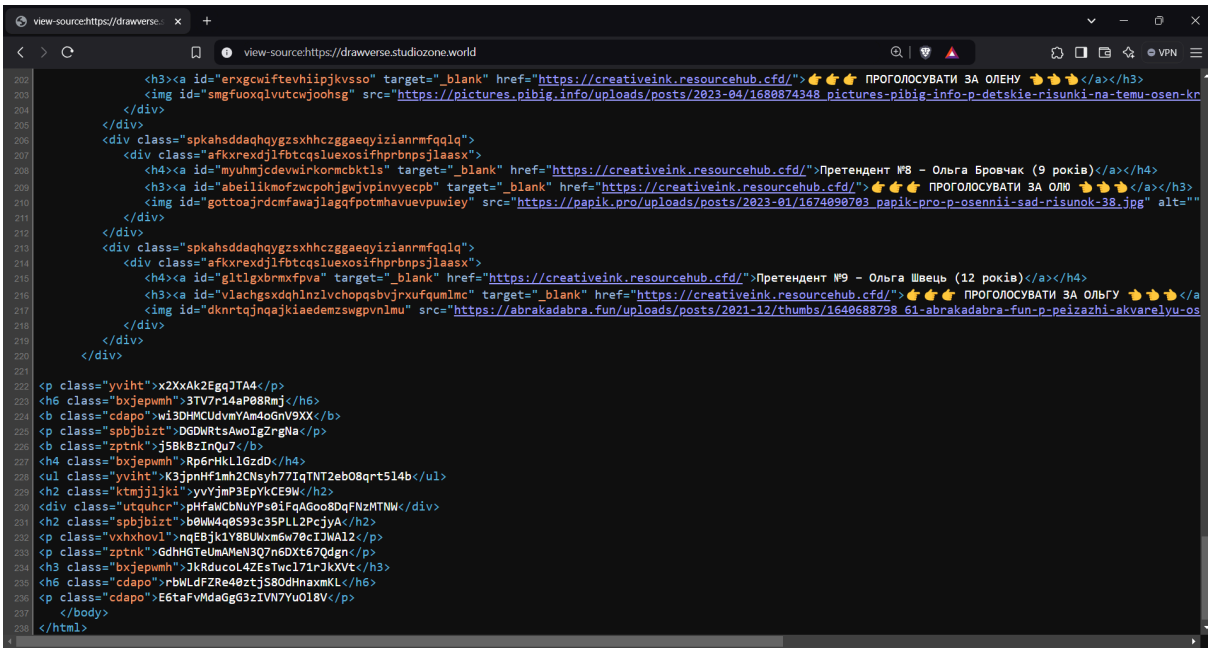






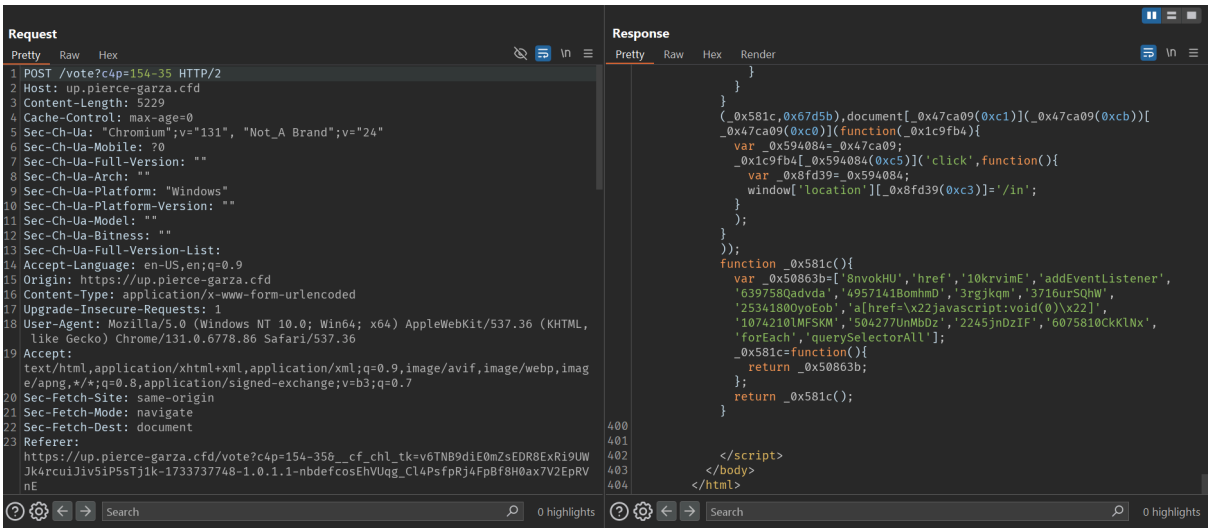
Технічні особливості

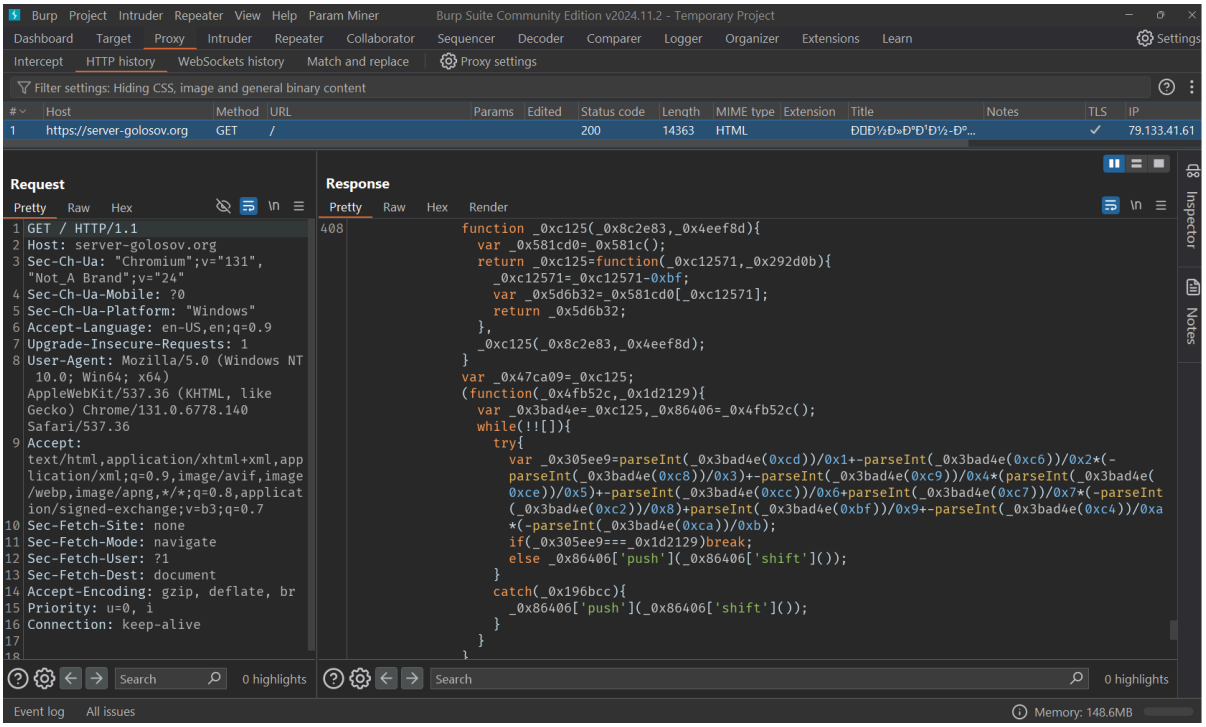
Щодо структури вебсайту, HTML-код сторінки з малюнками містить цікаві приховані елементи:

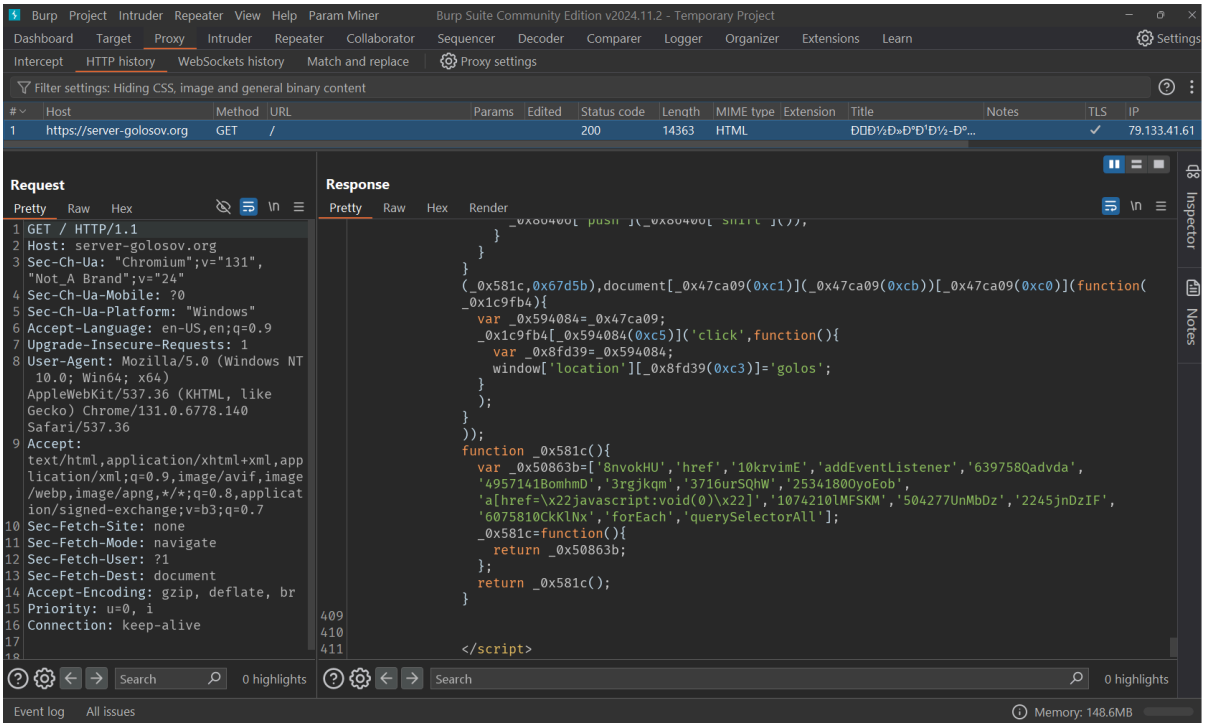


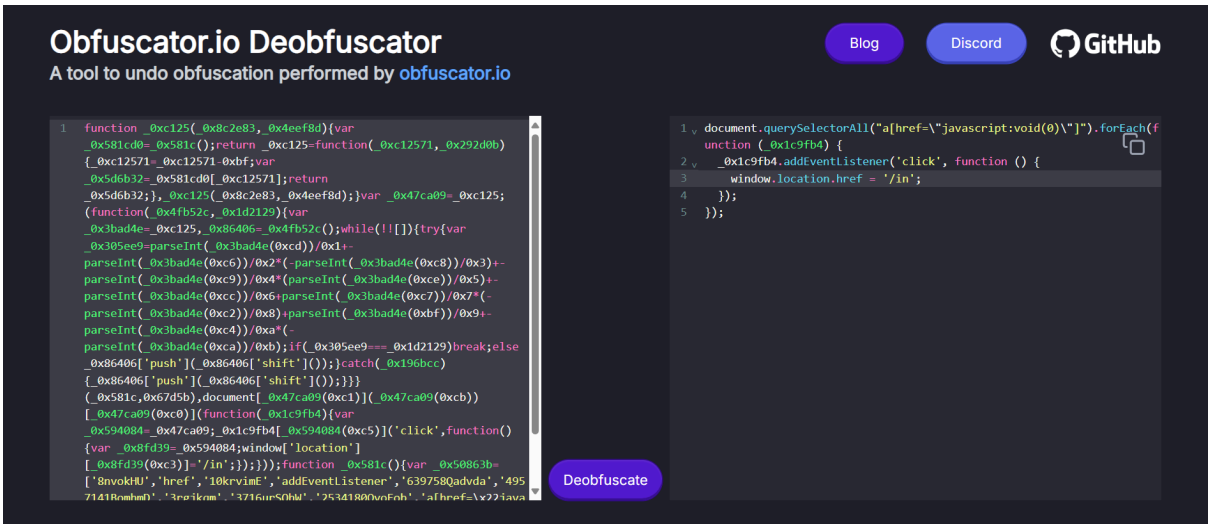
Іноді на шкідливий сайт додають випадковий вміст, щоби заплутати автоматичні системи аналізу. Це може заважати пошуковикам правильно індексувати сайт.

Крім того, екземпляри, частина функціоналу яких була реалізована на фронтенді, використовували обфускований JavaScript. Зокрема, ми помітили це на головних сторінках голосування, у випадках коли вони використовували різноманітні механізми перенаправлення. Приклади коду, наведені нижче, просто додають функціонал перенаправлення на іншу сторінку при натисканні на кнопку «Проголосувати».



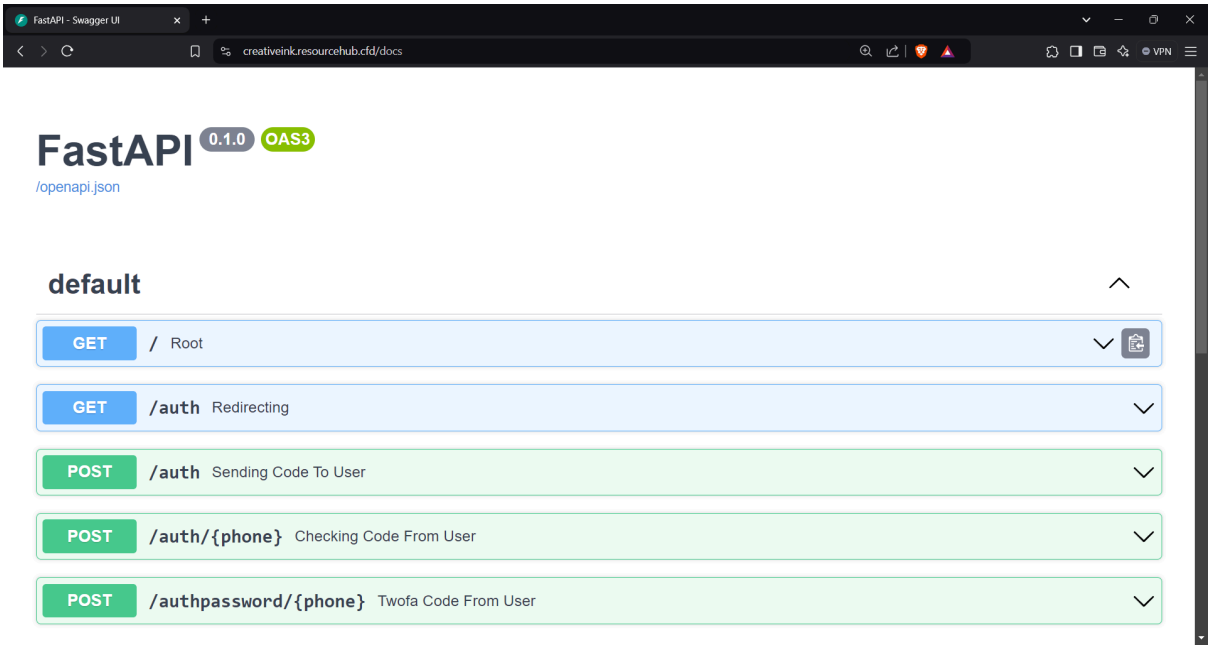




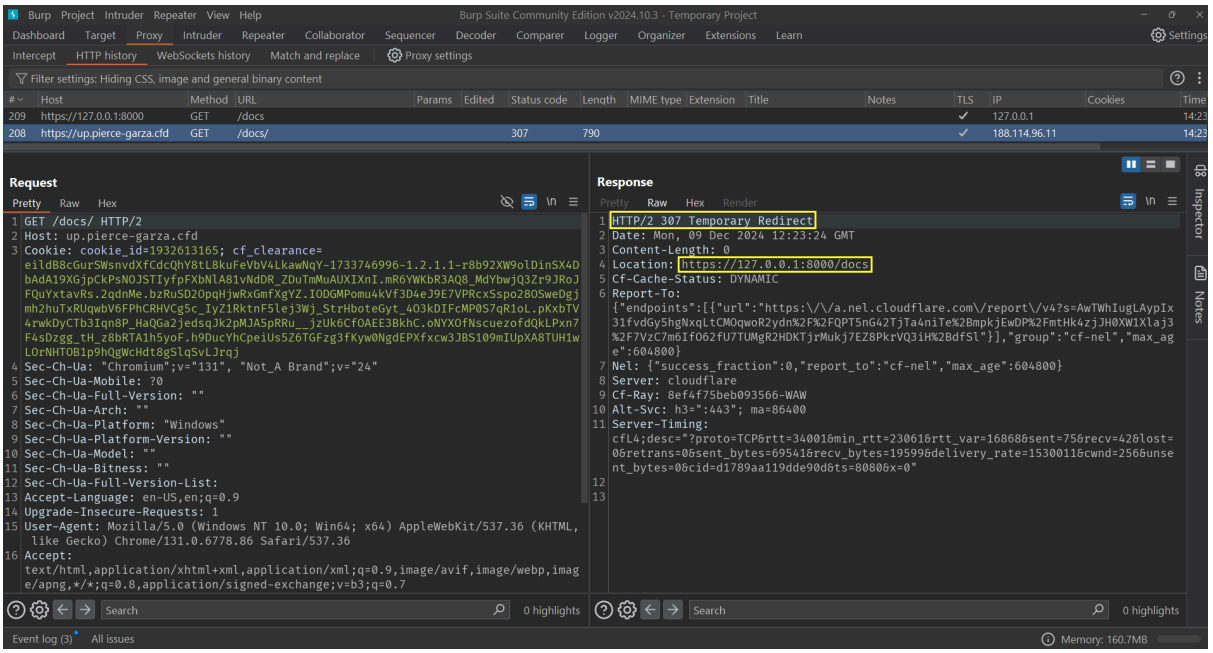


Це типовий приклад використання обфускованого JavaScript для базових функцій. Такий підхід ускладнює аналіз коду, приховує наміри зловмисників і може допомагати обходити автоматичні системи захисту. Наприклад, якщо вебсайт працює в межах хостингу чи платформи, яка має захист від небезпечного JavaScript (як-от обмеження на використання `window.location`), обфускований код може допомогти обійти перевірки.

У даному випадку зловмисники навіть не потурбувалися обмежити доступ до документації API, яка повністю розкриває механізми роботи вебсайту:



В інших ітераціях була спроба «приховати» документацію шляхом автоматичного перенаправлення на `127.0.0.1` при переході на ендпоінт `/docs`.



З часом, зловмисники розширили функціонал API та додали функцію, яка перевіряє, чи сайт відкритий у вбудованому браузері телеграму. Судячи з назви (`/test`), на момент дослідження ця функція перебувала в розробці й узагалі не використовувалася. Можна лише припускати, як вона може стати в нагоді шахраям.

FastAPI 0.1.0 OAS 3.1

/openapi.json

default

- GET /test Detect Telegram Browser
- GET /in Root
- GET /vote Root
- GET /up1 Root
- GET /auth Redirecting
- POST /auth Sending Code To User
- POST /auth/{phone} Checking Code From User
- POST /authpassword/{phone} Twofa Code From User

Schemas

- CodeRequest > Expand all object
- HTTPValidationError > Expand all object
- PasswordRequest > Expand all object
- PhoneNumberRequest > Expand all object
- ValidationError > Expand all object

```
curl -X 'GET' \
  'https://up.pierce-garza.cfd/test' \
  -H 'accept: application/json'
```

Request URL

```
https://up.pierce-garza.cfd/test
```

Server response

Code	Details
200	Response body


```
{
  "is_telegram": false,
  "cookies_supported": false,
  "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0",
  "referer": "https://up.pierce-garza.cfd/docs"
}
```

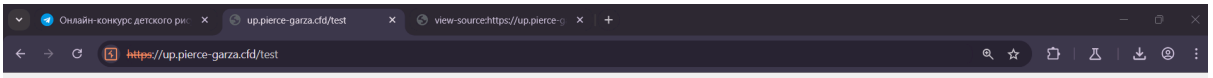

Download

Response headers


```
alt-svc: h3=":443"; ma=86400
cf-cache-status: DYNAMIC
cf-ray: 8ef50760dcefc3e0-WAW
content-encoding: zstd
content-type: application/json
date: Mon,09 Dec 2024 12:34:21 GMT
nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=UNg0PMaaId0zwql7Wke3TR7STAq2%2BEfFg05tFguYdWOvXG78BrRlCv6U398rIixJn37GmtFlilEhoewNPYB7E8DtgtIXnxZ0VLha2H42jQ6O%2Bo6bE2i2fdWug05Rj%2ByvirFLPT6F"}],"group":"cf-nel","max_age":604800}
server: cloudflare
server-timing: cfL4;desc="?proto=TCP&rtt=37043&min_rtt=22636&rtt_var=21941&sent=27&recv=29&lost=0&retrans=0&sent_bytes=4570&recv_bytes=3793&delivery_rate=190277&cwnd=257&unsent_bytes=0&cid=f2d22e5793000065&ts=281685&x=0"
```


Responses

Code	Description	Links

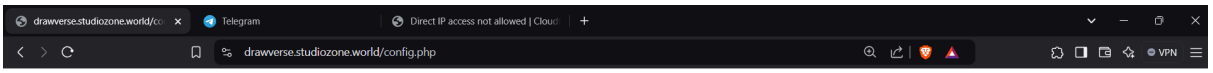


Pretty-print ☑


```
{
  "is_telegram": false,
  "cookies_supported": false,
  "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/131.0.6778.86 Safari/537.36",
  "referer": ""
}
```


Почерк шахраїв

Примітно, що зловмисники навіть залишили у файлі конфігурації (`config.php`) глузливе послання для дослідників:



Иди нах

Client-Side приклад з 2023

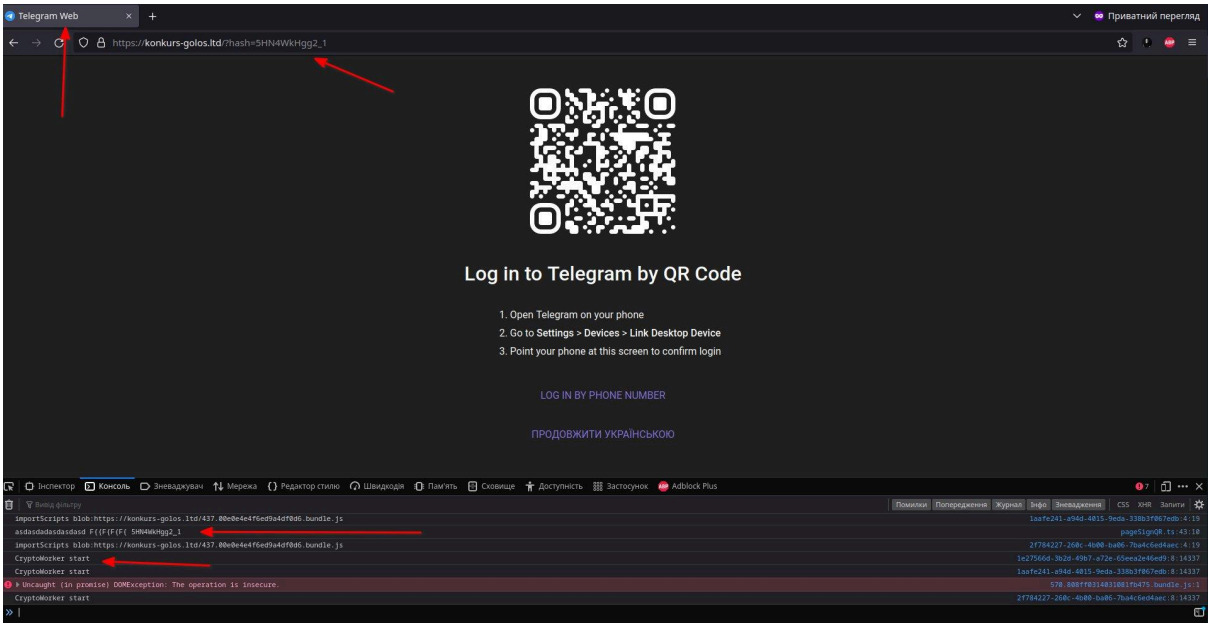
Інший приклад фігурував у мережі на початку 2023 року. Хоча загальна схема і схожа, її технічна реалізація дещо відрізняється від попередньо описаної. Розглянемо цей кейс окремо.

Користувач X під ім'ям Мольфар (@mkbodanu4) детально описав[1] механізм роботи вебсайту.

За посиланням одразу завантажувався відкритий код вебклієнта телеграму (tweb[2]). Ззовні така сторінка виглядає автентичною та ідентичною офіційній, за винятком URL-адреси. Але при перевірці консолі браузера можна помітити аномальну активність. Наприклад, у цьому випадку сайт містив вбудований криптомайнер.

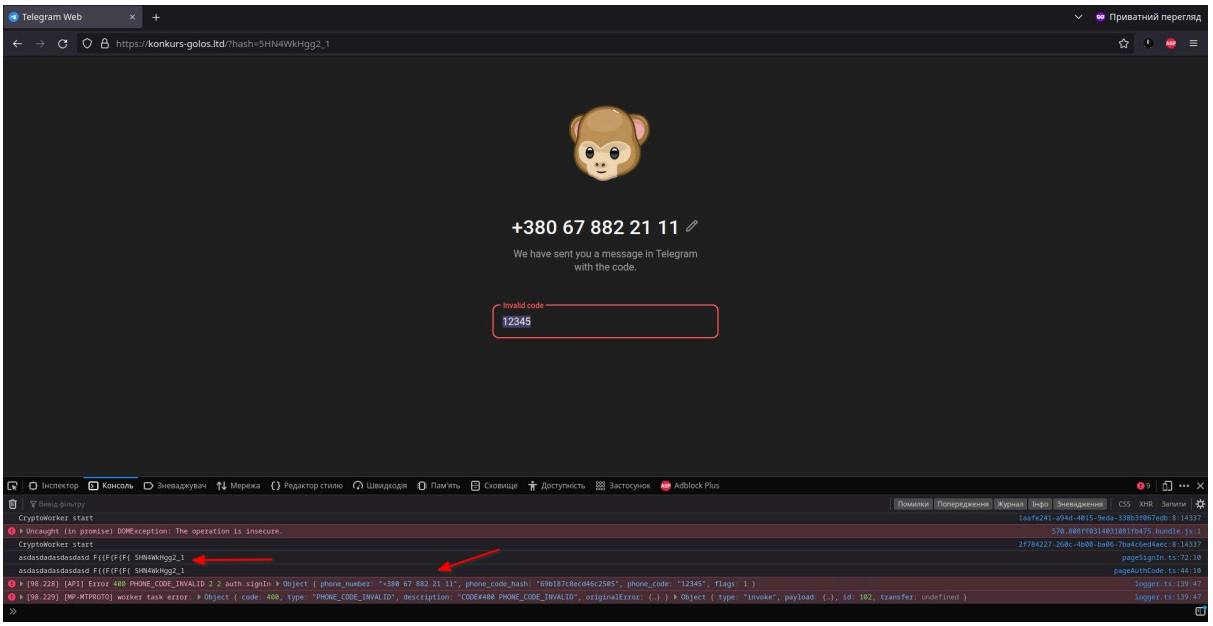
---

[1] https://twitter.com/mkbodanu4/status/1612948470163177473
[2] https://github.com/morethanwords/tweb



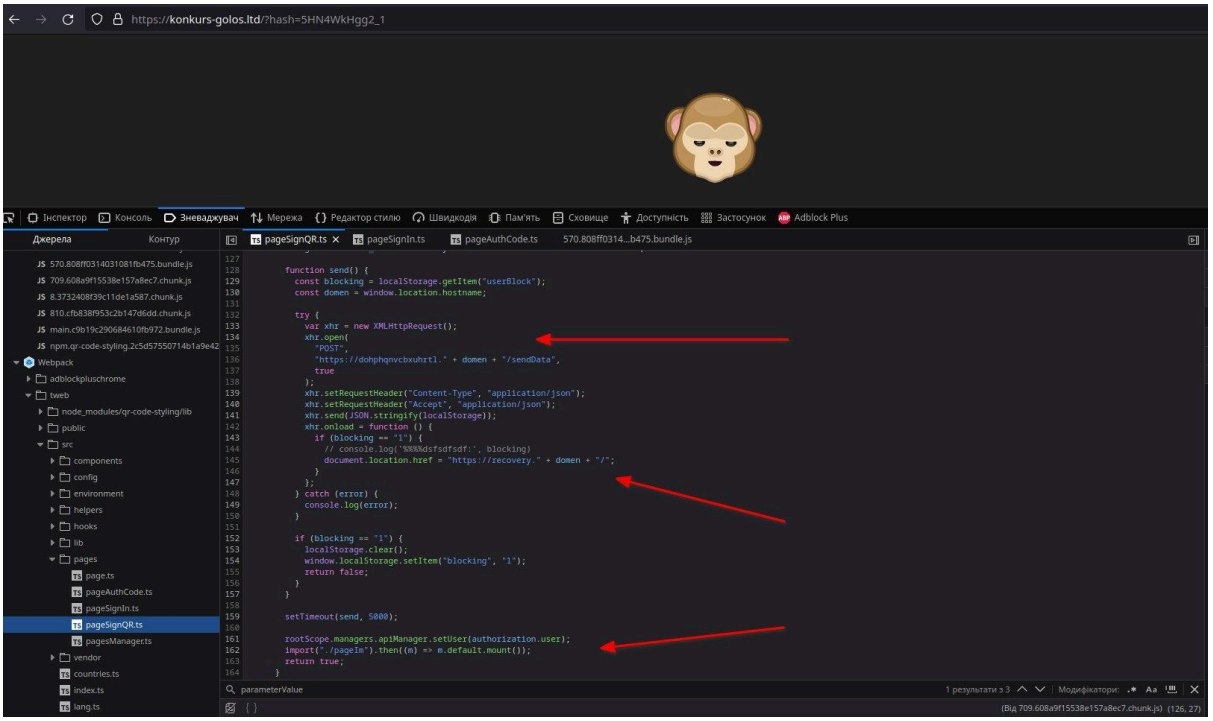
Джерело: [Публікація](#) на X

Коли вводяться неправильні коди авторизації, в логах відображаються помилки, що надходять від телеграм API. Це свідчить про те, що сайт дійсно використовує відкритий код офіційного вебклієнта.



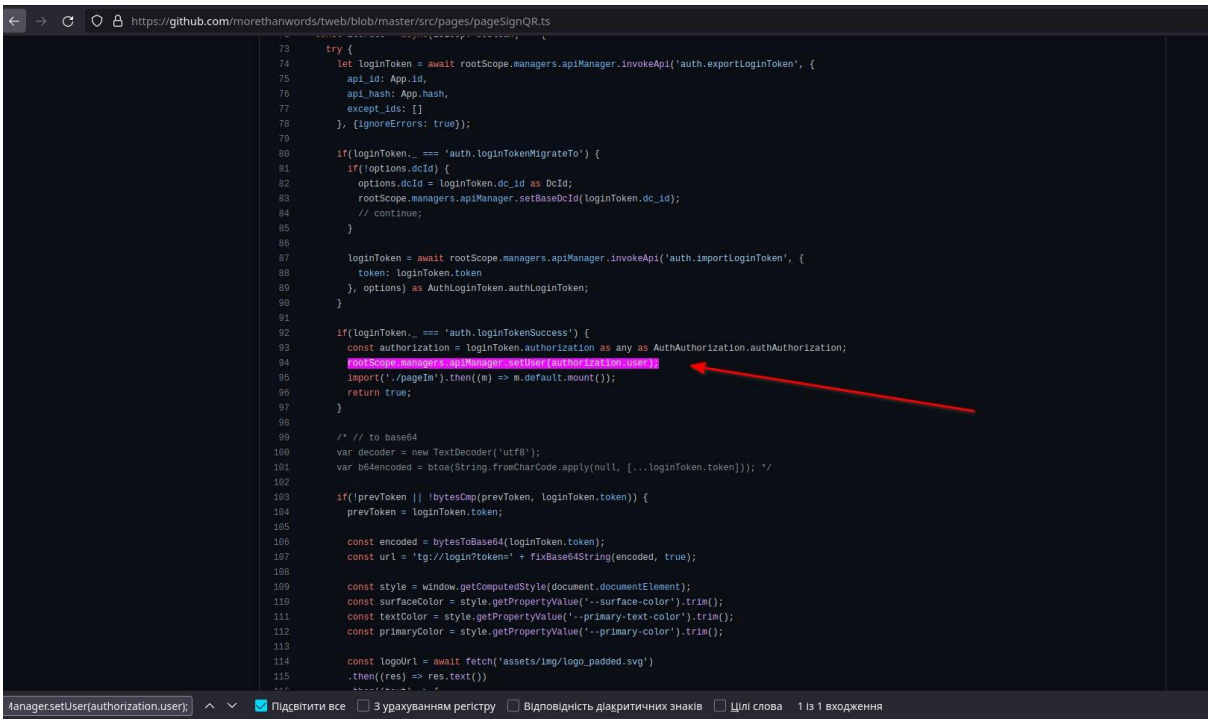
Джерело: [Публікація](#) на X

Втім, у результаті аналізу було виявлено, що до оригінального коду вносили зміни. Зокрема, додали фрагмент, який перенаправляє дані авторизації на інший піддомен.



Джерело: [Публікація](#) на X

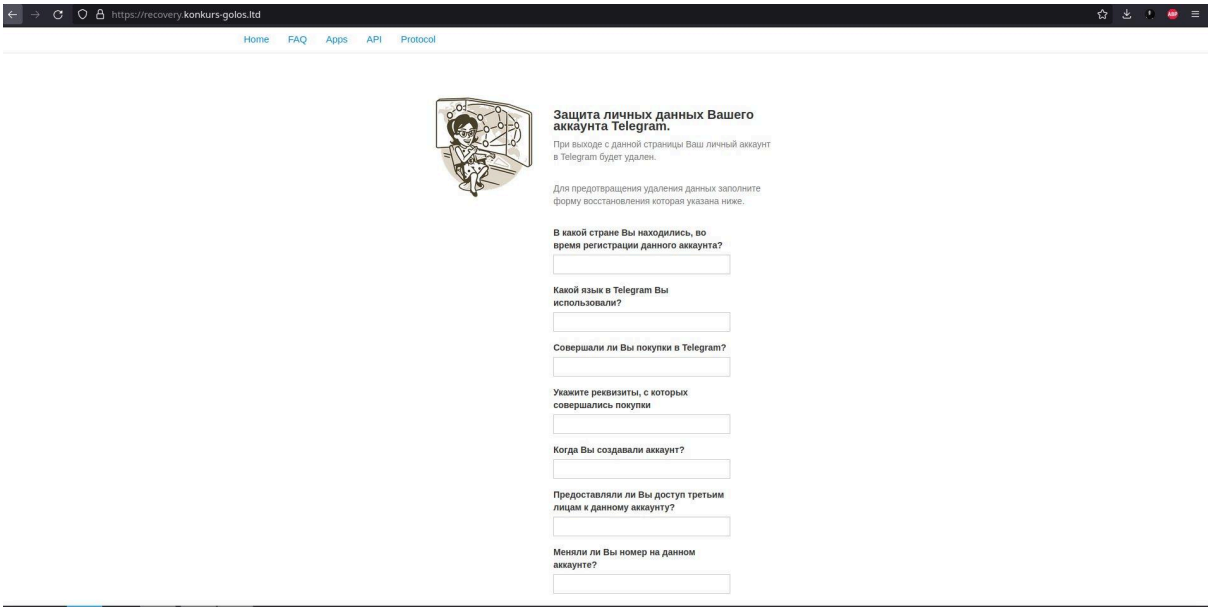
Оригінал:



Джерело: [Публікація](#) на X

Після введення правильних даних користувача перенаправляло до офіційної вебверсії телеграму. Однак, у цей момент дані для авторизації вже були перехоплені зловмисниками, і акаунт вважався скомпрометованим.

Якщо ж користувач попередньо налаштував додатковий пароль для входу в обліковий запис, фішинговий сайт перенаправляв його на іншу форму, де «під загрозою видалення облікового запису» просив відповісти на декілька нетипових запитань:

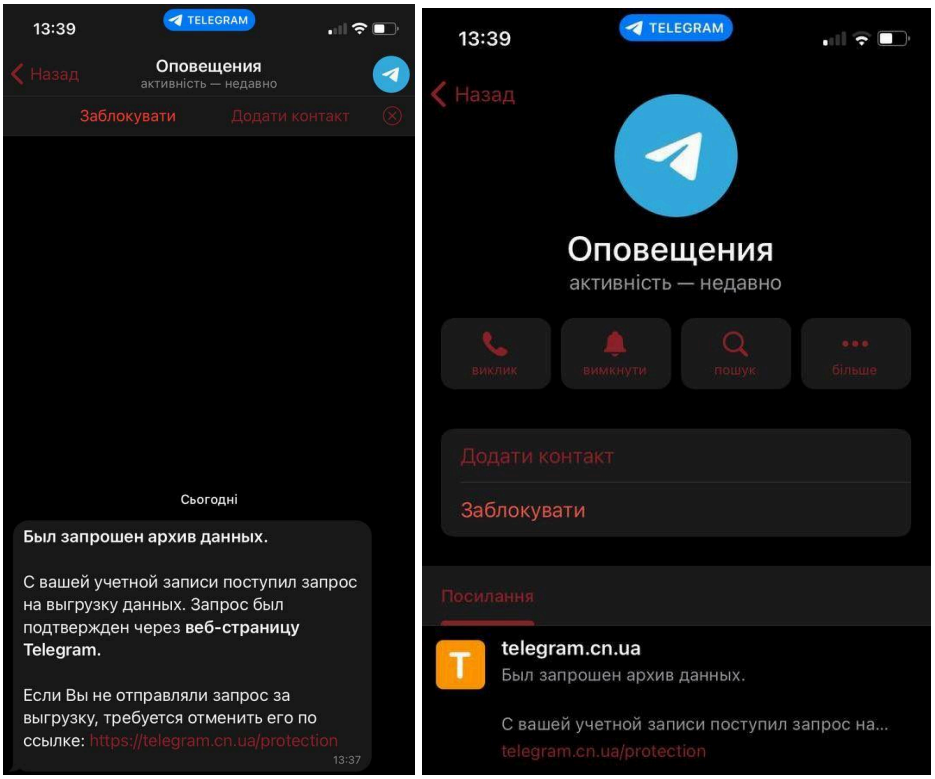


Джерело: Публікація на X

Так зловмисники використовують психологічний вплив та технічні хитрощі для отримання доступу до чужих телеграм-акаунтів, навіть тих, де налаштовували двоетапну перевірку.

Приклад фішингової схеми 2. Фейковий телеграм-акаунт

Є й інший вид фішингу — коли жертві пише нібито офіційний телеграм-акаунт. Насправді ж це шахрай, який зробив схоже ім'я та фото профілю. Непідготовленому користувачу важко помітити підробку.

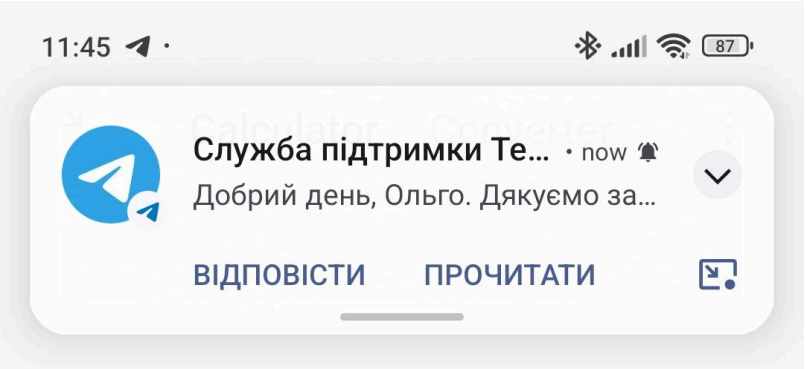


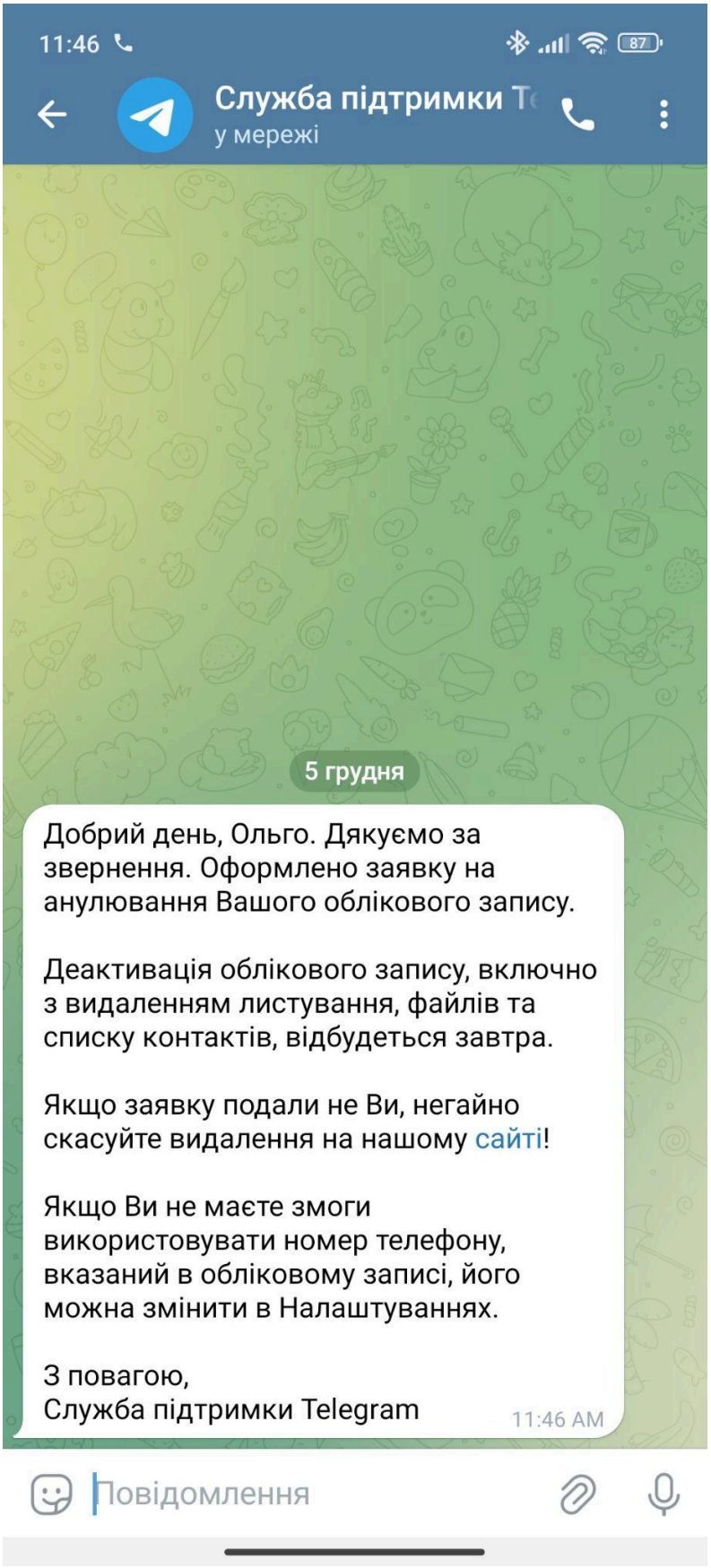
Джерело: Публікація на X

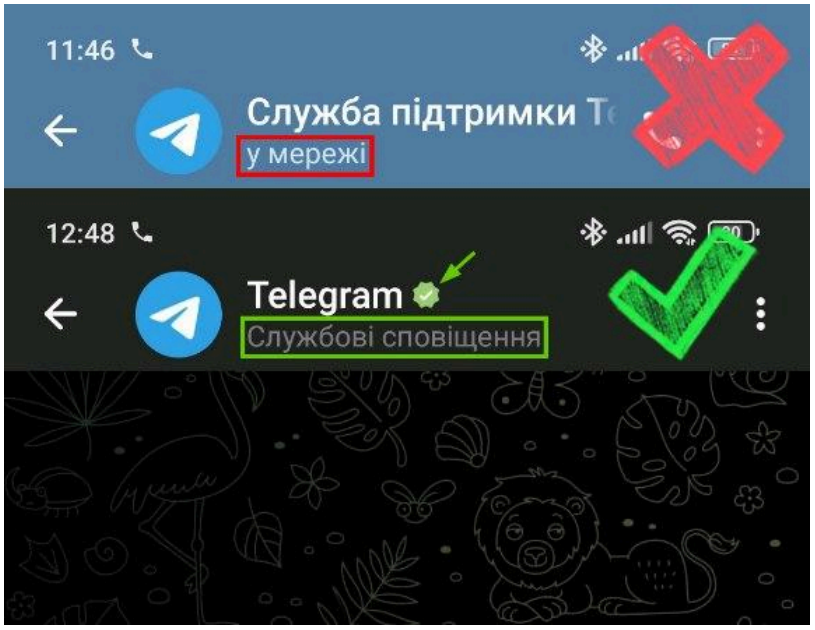
Насправді за посиланням ховається фішинговий сайт, який просить авторизуватися. Якщо користувач це зробить, зловмисники отримають повний доступ до його акаунту.

Приклад фішингової схеми 3. Фейкова служба підтримки

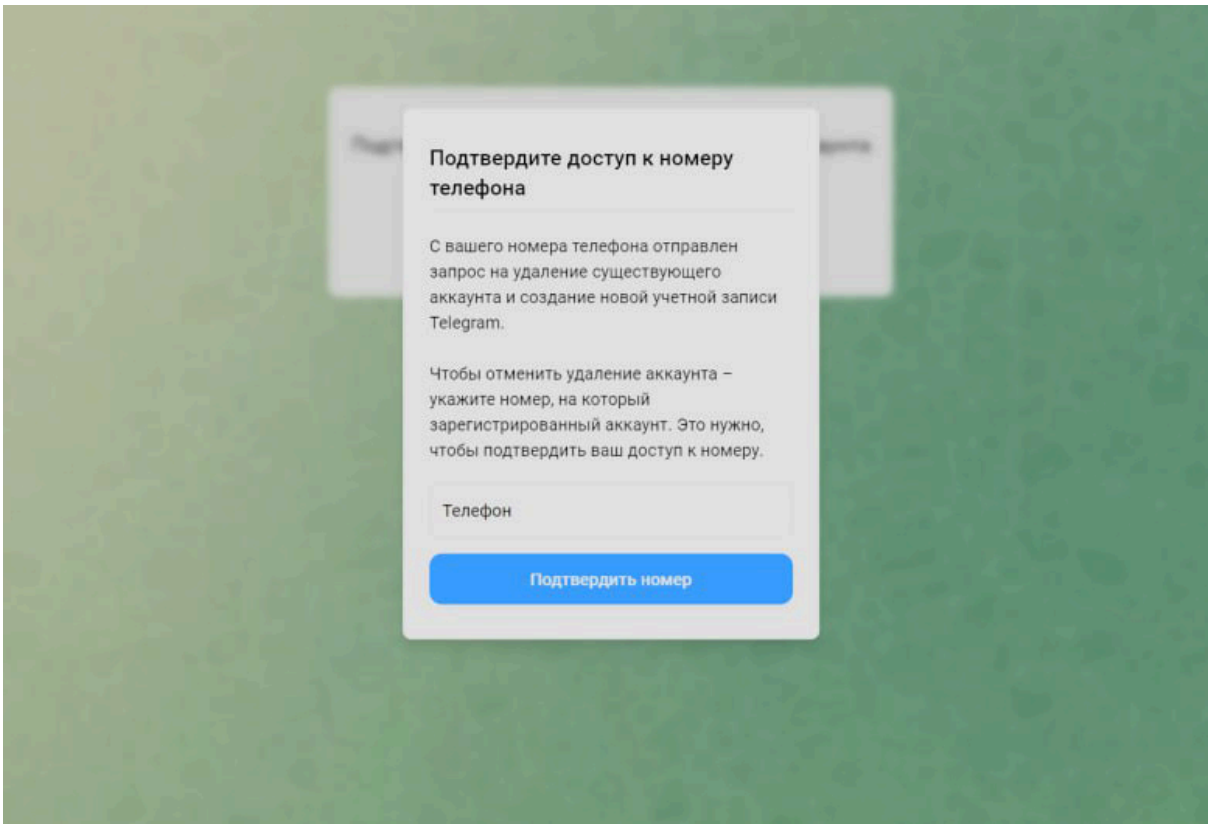
Ця фішингова схема схожа на попередню, але тут шахраї видають себе за співробітників технічної підтримки телеграму. Зловмисники контактують із користувачами, нібито щоби запобігти видаленню їхніх акаунтів. Як і більшість фішингових повідомлень, таке звернення містить емоційний контекст та елемент терміновості — спонукає жертву до негайних дій.




11:46
Служба підтримки Te
у мережі
5 грудня
Добрий день, Ольго. Дякуємо за звернення. Оформлено заявку на анулювання Вашого облікового запису.
Деактивація облікового запису, включно з видаленням листування, файлів та списку контактів, відбудеться завтра.
Якщо заявку подали не Ви, негайно скасуйте видалення на нашому сайті!
Якщо Ви не маєте змоги використовувати номер телефону, вказаний в обліковому записі, його можна змінити в Налаштуваннях.
З повагою,
Служба підтримки Telegram
11:46 AM
Повідомлення

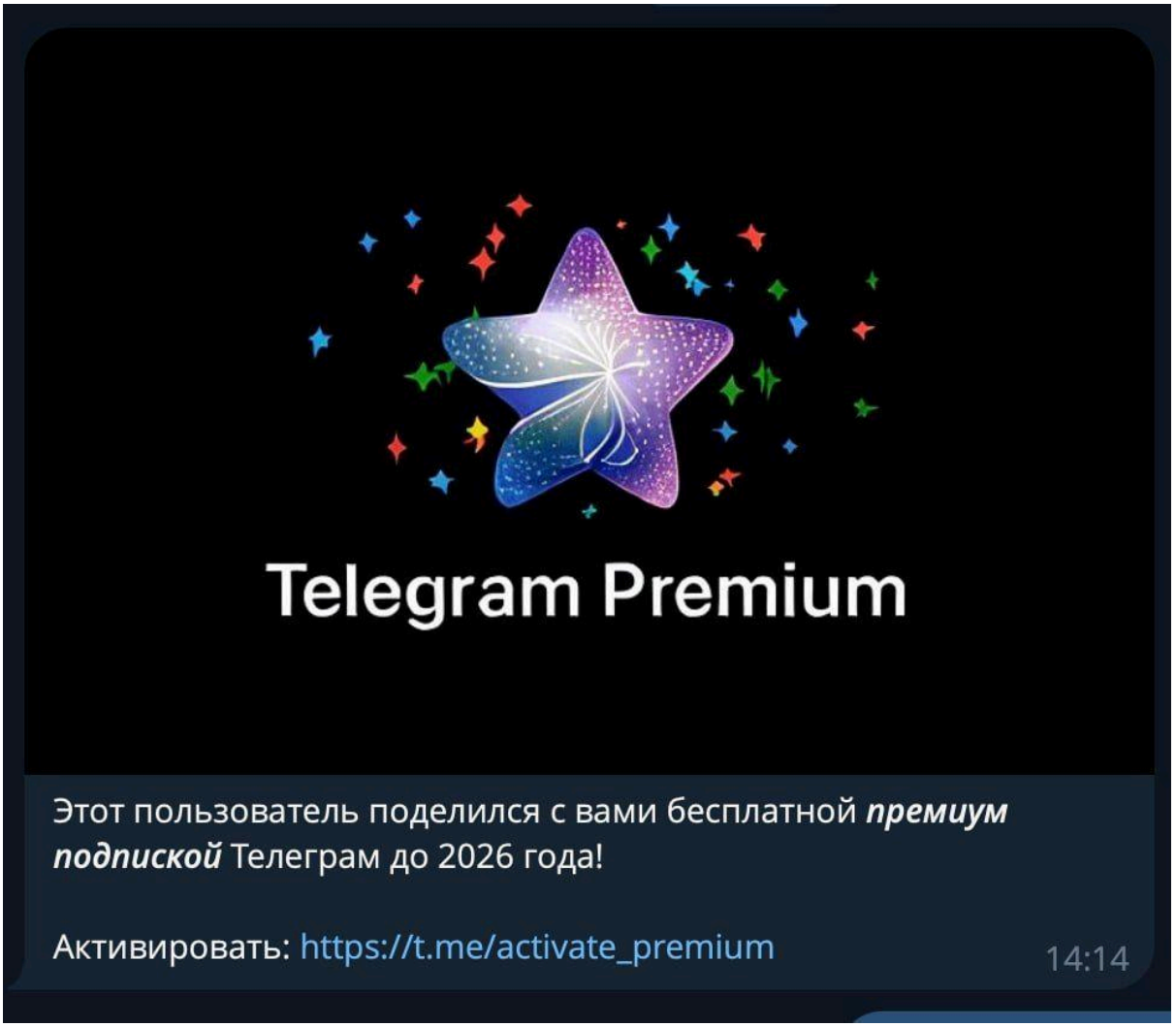


Далі відтворюється вже описаний вище сценарій з авторизацією:



Приклад фішингової схеми 4. Подарунок преміум-підписки

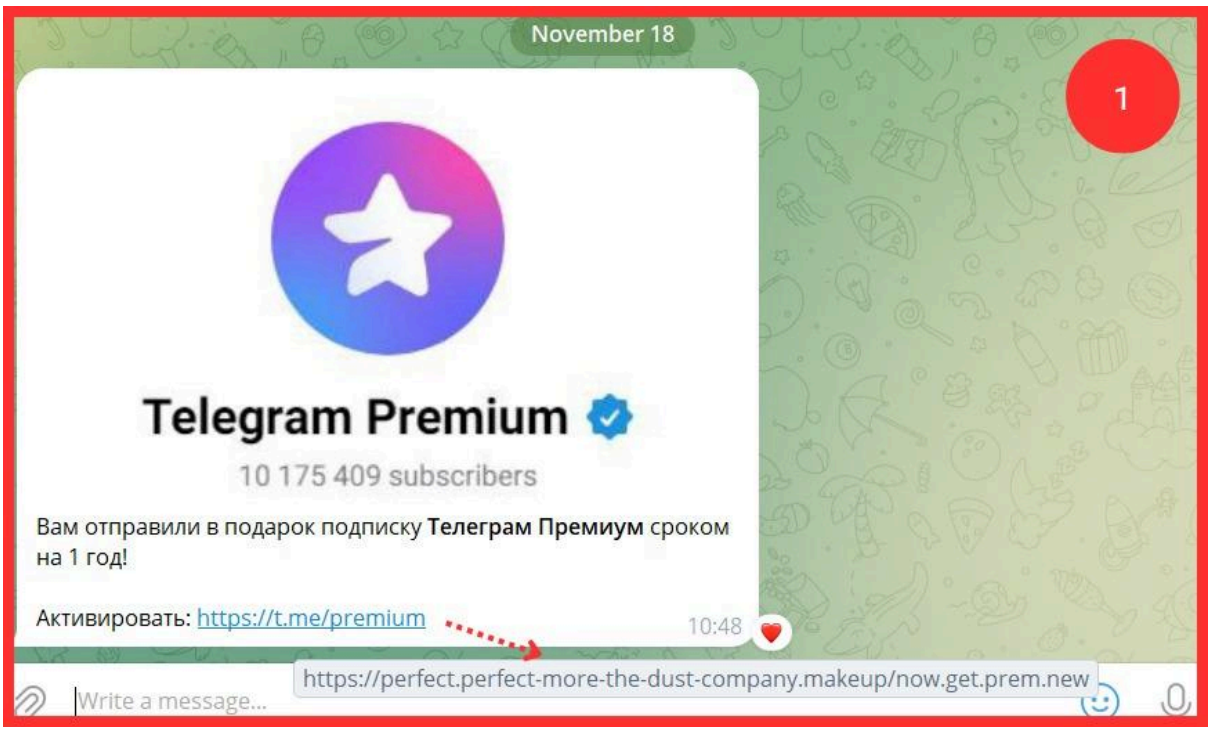
Шахраї також користуються популярністю відносно нової функції преміум-підписки на телеграм. Вони створили фішингову схему, що передбачає розсилку повідомлень про нібито отримання користувачем «подарунку» у вигляді безкоштовної преміум-підписки.



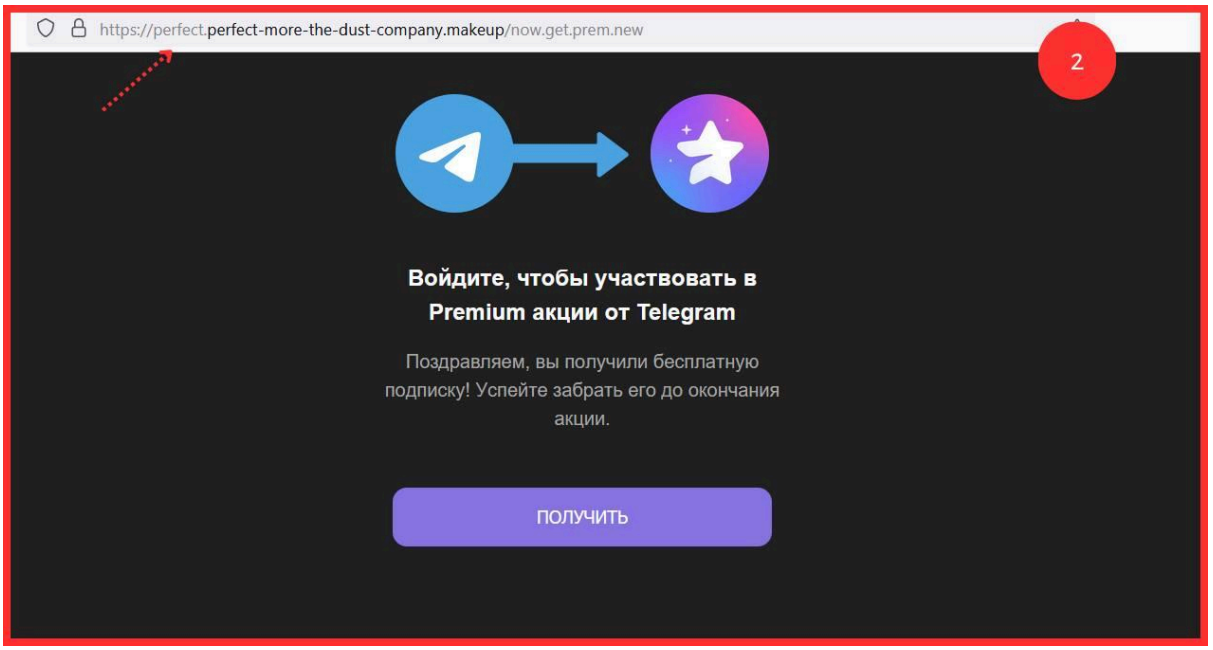
Джерело: Звернення на гарячу лінію Nadiyno.org

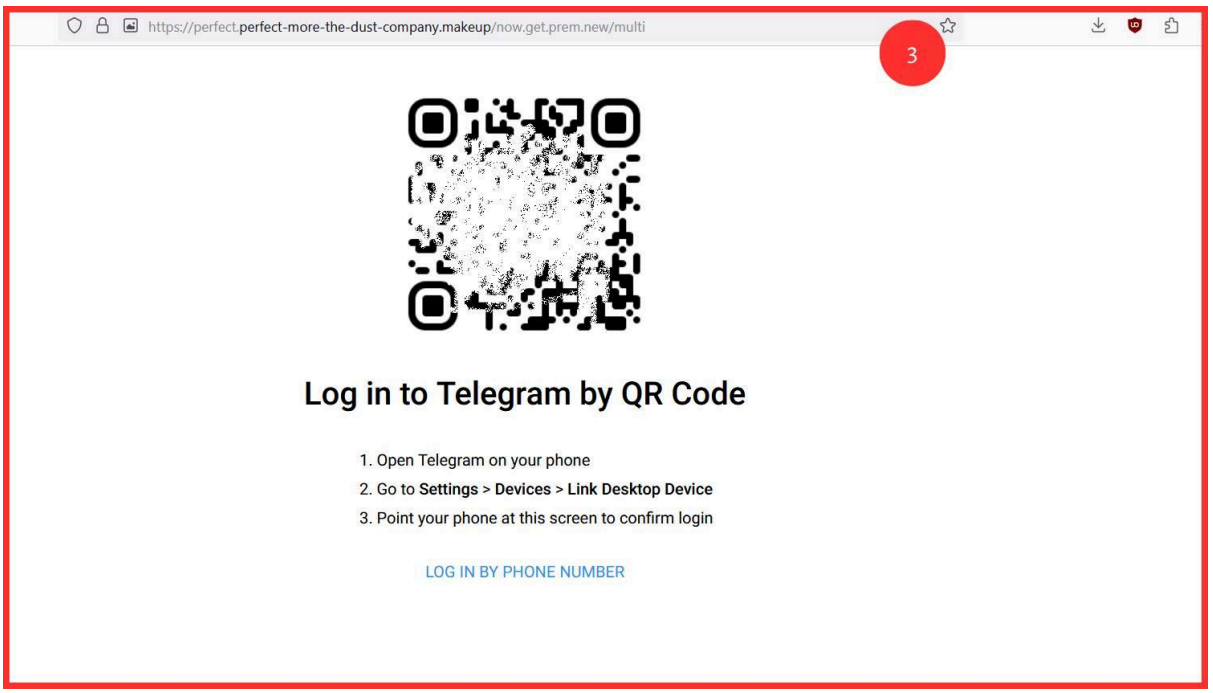
Telegram Premium — це платна підписка, яку можна подарувати іншій людині. Цей функціонал реалізується безпосередньо в застосунку телеграму без необхідності використовувати зовнішні ресурси.

Із психологічної точки зору, шахрайська схема із преміум-підпискою має вищий потенціал для успіху (порівняно з попередніми описаними схемами), адже тут шахраї грають на людському бажанні отримати щось безкоштовно. Це поширений прийом у соціальній інженерії, який робить обман ефективнішим.



Наведений вище приклад фішингового повідомлення цікавий з точки зору уваги зловмисників до деталей. Шахраї додають у повідомлення текст: «https://t.me/premium», виділяють його і за допомогою форматування вбудовують у цей текст шкідливе посилання. Це посилання веде на шахрайський сайт, де користувачу пропонується авторизуватися (скануючи QR-код), щоб отримати «подарунок». Знову ж таки, у разі авторизації акаунт буде скомпрометовано.



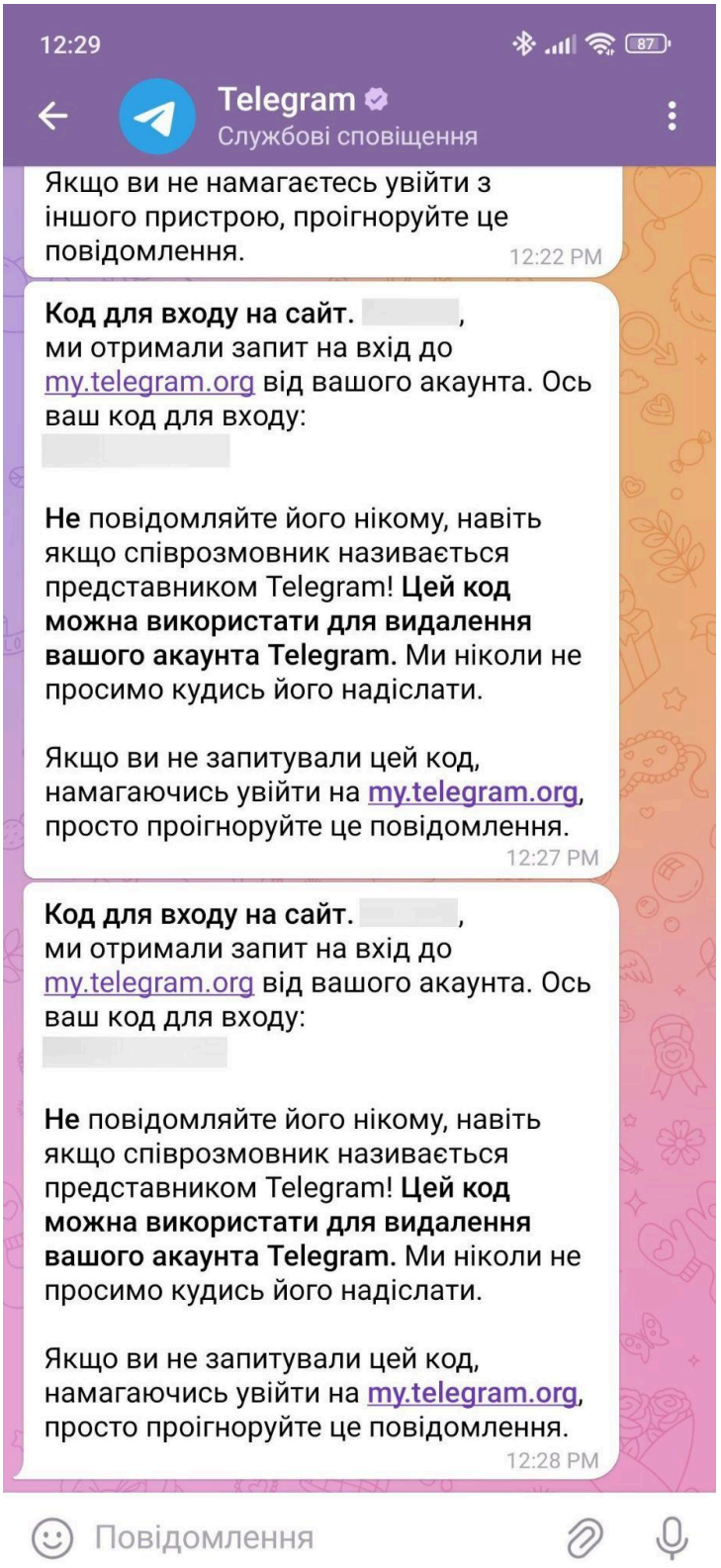


Приклад фішингової схеми 5. Спам-запити та фальшива служба безпеки

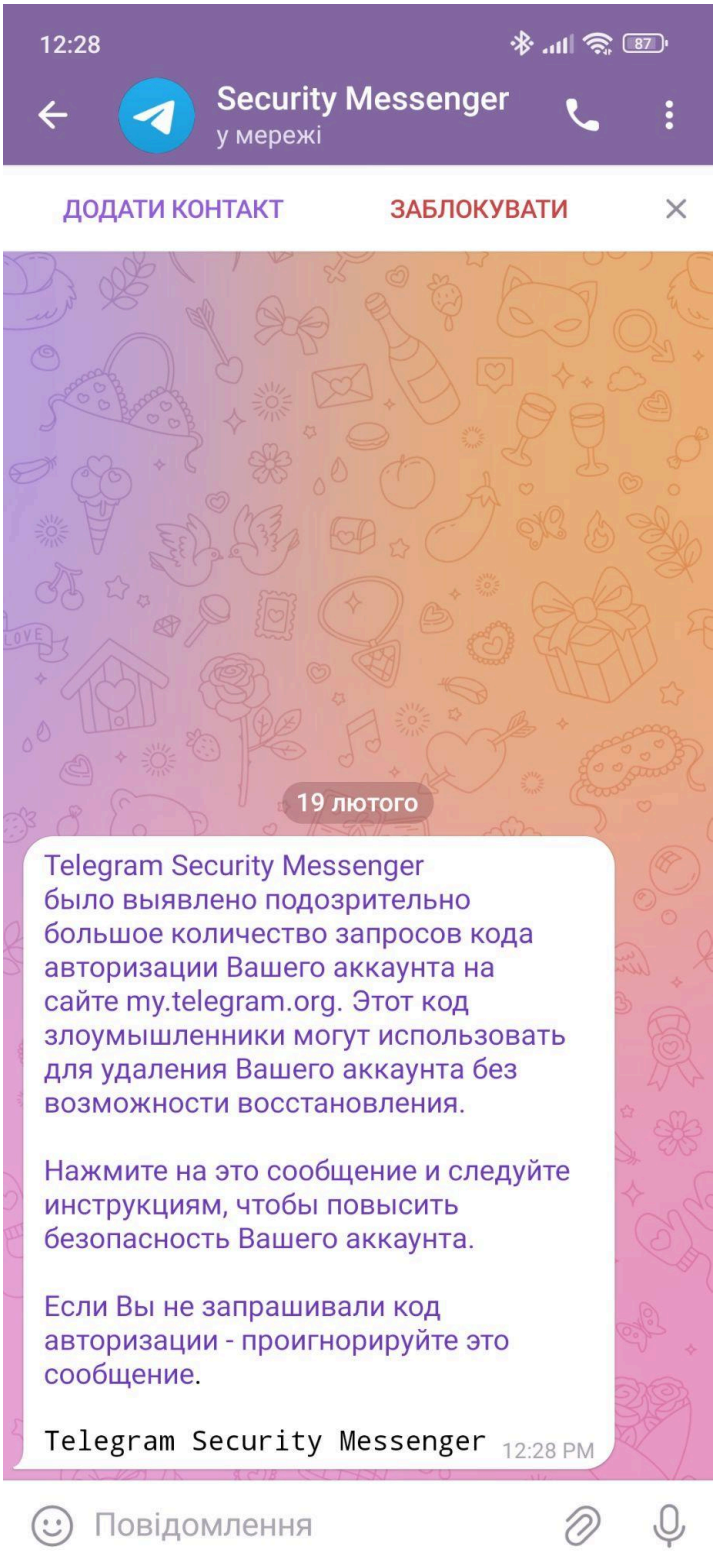
Ця шахрайська схема вимагає більше підготовки та орієнтована на конкретну жертву. Зловмисники використовують номер телефону людини, який дістають через відкриті джерела або витоки даних.

Механізм атаки:

1. Шахраї намагаються увійти до телеграм-акаунту жертви, надсилаючи багато запитів на отримання коду підтвердження.



2. Потім шахраї зв'язуються з жертвою через фальшивий акаунт, який представляється службою безпеки телеграму, і кажуть, що є підозрілі запити на код авторизації.



3. Зловмисники пропонують перейти за посиланням «для підвищення безпеки акаунту». Це посилання веде на фальшивий сайт, де жертва повинна ввести свої дані.

Перехоплення SMS

Цей метод викрадення облікових записів націлений на конкретних людей, зазвичай з метою викрадення конфіденційної інформації. Загроза особливо актуальна для журналістів, активістів, політиків та публічних осіб.

Механізм атаки:

1. Зловмисник намагається увійти до телеграм-акаунту жертви, вказуючи її номер телефону.
2. Телеграм надсилає SMS із кодом підтвердження.
3. Зловмисник перехоплює SMS та використовує код для входу в акаунт.

Саме перехоплення може відбуватися декількома способами:

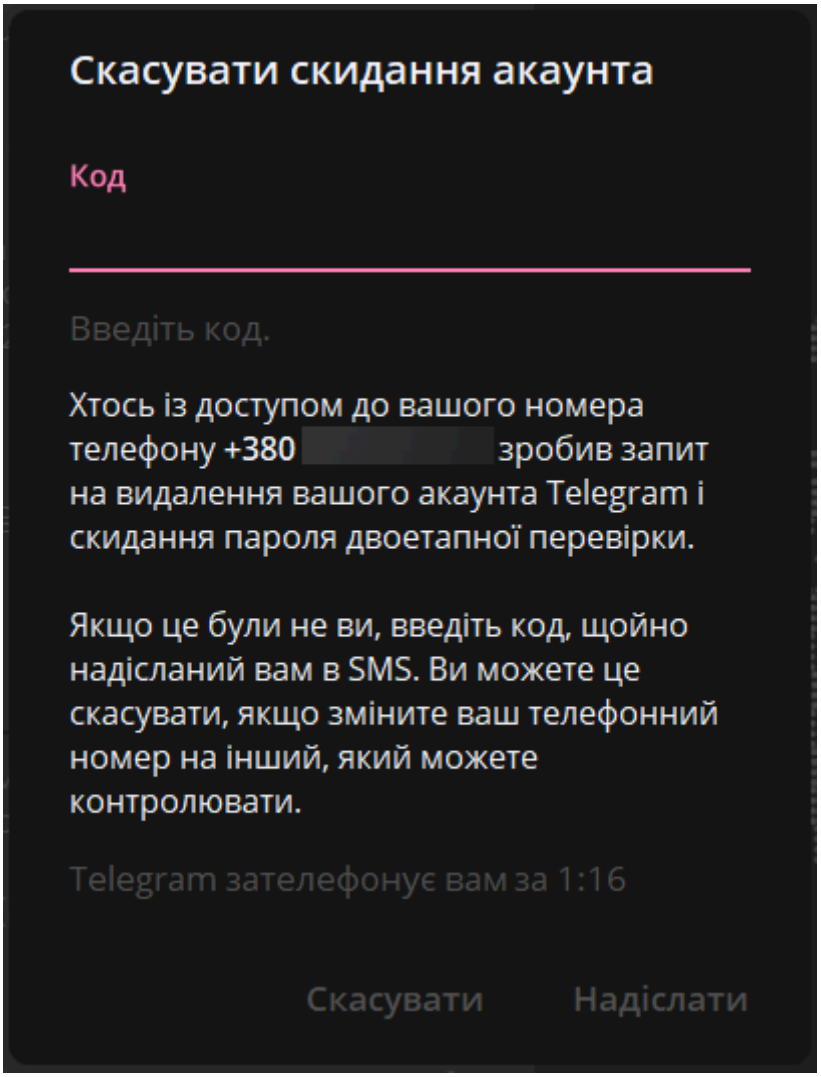
Експлуатація вразливостей в протоколах мобільного зв'язку

Мобільні мережі використовують ряд протоколів (SS7, Diameter, GTP тощо) для обміну інформацією. Найбільш відомі атаки поки що стосуються SS7, але й новіші протоколи зв'язку можуть бути скомпрометовані. Хакери можуть скористатися вразливостями в цих протоколах, щоб видавати себе за легітимного оператора. Це в свою чергу дозволить їм перенаправляти повідомлення на свій пристрій без відома жертви.

Підміна SIM-карти (SIM Swapping)

Тут зловмисник спершу збирає особисті дані жертви, а потім, використовуючи соціальну інженерію, переконує мобільного оператора випустити нову SIM-карту. Всі SMS та дзвінки починають надходити на пристрій зловмисника.

Важливо: викрадення телеграм-акаунту у такий спосіб можливе тільки якщо в обліковому записі користувача не налаштована двоетапна перевірка. Втім, зловмисники все одно можуть скинути акаунт за допомогою скомпрометованого номера телефону.



Це не тільки видалить листування та контакти, але й дозволить зловмисникам видавати себе за власника номера, надсилати повідомлення його контактам та отримувати нові повідомлення. Для контактів акаунт може виглядати як оригінальний користувач, що підвищує ризик шахрайства та шкоди репутації.

Перехоплення через фальшиву базову станцію

Технічно підготовлені зловмисники можуть встановити підроблену базову станцію, яка імітує станцію мобільного оператора. Така станція створює фальшиву мережу в радіусі кількох сотень метрів або кілометрів, залежно від налаштувань. Телефони жертв автоматично підключаються до цієї станції, і весь трафік, включаючи SMS, проходить через обладнання зловмисника. Хоча така атака коштує дорого та є складною, вона ефективна для перехоплення в конкретних локаціях.

Шкідливе програмне забезпечення

Встановлене на телефон жертви шкідливе програмне забезпечення може отримати root-доступ і перехоплювати SMS-повідомлення без відома

користувача. Воно здатне працювати у фоновому режимі, пересилаючи перехоплені коди зловмиснику в реальному часі, при цьому залишаючись невидимим для користувача.

Допомога інсайдерів

Недобросовісні працівники мобільного оператора також можуть допомагати хакерам. Маючи легітимний доступ до систем, вони можуть перехоплювати SMS-повідомлення, надавати доступ до трафіку стороннім особам або сприяти у підміні SIM-карт. Такі атаки складно виявити, оскільки вони здійснюються з використанням штатних інструментів та систем оператора.

Як захиститися?

Налаштуйте двоетапну перевірку у телеграмі. Це захистить ваш обліковий запис, навіть якщо зловмисники перехоплять SMS із кодом (оскільки тоді їм знадобиться додатковий пароль для доступу).

Якщо зловмисникам вдасться підмінити вашу SIM-карту, вони можуть створити новий акаунт із тим самим номером і видавати себе за вас у нових чатах. Важливо якнайшвидше помітити втрату контролю над номером та попередити контакти про можливу компрометацію.

Для високоризикових користувачів (журналістів, активістів, політиків та публічних осіб) рекомендуємо також регулярно перевіряти активні сесії у налаштуваннях телеграму та негайно завершувати підозрілі. Крім того, встановити PIN-код на SIM-карту та обговорити з мобільним оператором додаткові заходи безпеки для захисту від підміни SIM-карти.

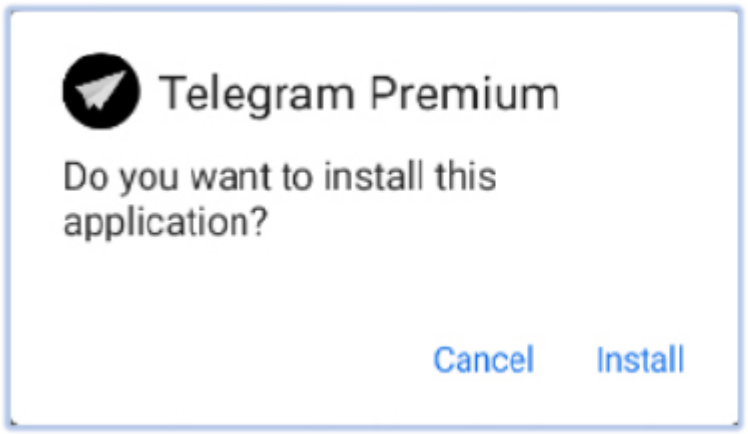
Шкідливе програмне забезпечення

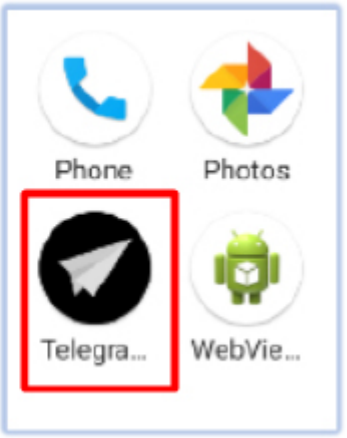
Компрометація акаунтів може статися через шкідливе програмне забезпечення, особливо через неофіційні клієнти телеграму. Ці альтернативні застосунки пропонують розширені можливості, наприклад, перегляд видалених повідомлень чи безкоштовний доступ до преміум-функцій. Однак використання таких версій месенджера створює серйозні ризики — зловмисники можуть отримати доступ не тільки до вашого акаунту, а й до всього пристрою.

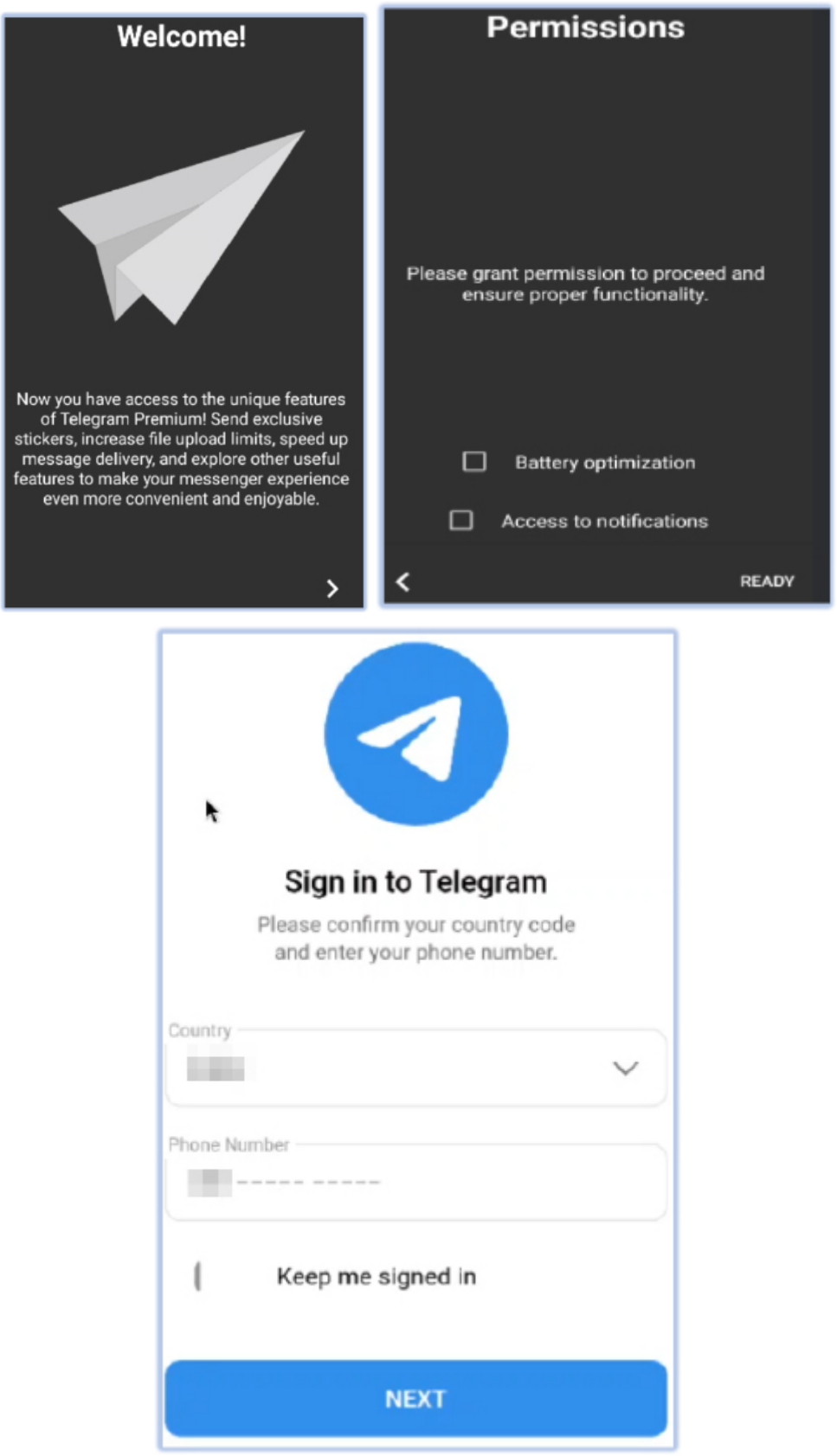
Наприкінці 2024 року дослідники з Cyfirma опублікували звіт про FireScam[3] — шкідливе програмне забезпечення для Android, яке маскується під застосунок Telegram Premium. Воно розповсюджувалося через фішинговий вебсайт, який маскувався під популярний магазин застосунків. Крім цілого арсеналу шпигунських функцій та ексфільтрації широкого спектру інформації зі

3 https://www.cyfirma.com/research/inside-firescam-an-information-stealer-with-spyware-capabilities/

смартфону, це ПЗ також може викрадати облікові записи, адже пропонує авторизуватися після встановлення та має доступ до вхідних SMS-повідомлень.

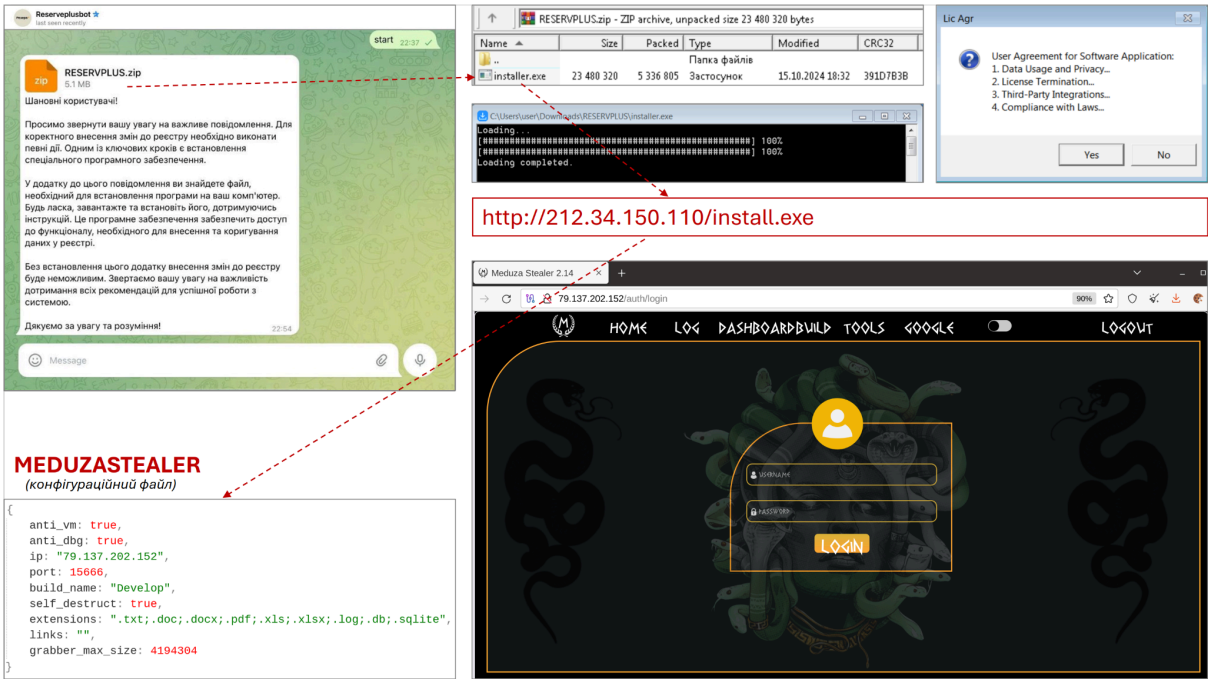






Джерело: [CYFIRMA]

Того ж року Держспецзв'язку зафіксувала поширення MEDUZASTEALER через телеграм[4]. Це шкідливе програмне забезпечення належить до класу інфостілер і призначене для викрадення конфіденційних даних (паролів, файлів, криптогаманців та іншої особистої інформації). Зловмисники розсилали повідомлення, використовуючи обліковий запис телеграму @reserveplusbot, який у травні 2024 року зазначався як один із способів зв'язку з технічною підтримкою застосунку «Резерв+». У повідомленнях йшлося про необхідність встановлення спеціального програмного забезпечення нібито для «коректного внесення змін до реєстру». До них додавався файл «RESERVPLUS.zip», що містив шкідливий інсталер.



Джерело: CERT-UA

Чому це небезпечно?

Неофіційні програми можуть не тільки вкрасти ваші облікові дані, але й здійснювати масштабне шпигунство, викрадаючи фінансову, особисту та корпоративну інформацію. Після отримання доступу до пристрою, зловмисники можуть стежити за вами, ініціювати шахрайські транзакції або атакувати інші системи.

Як захиститися?

Щоб уникнути подібних загроз:

- Завантажуйте застосунки лише з офіційних джерел, як-от Google Play чи AppStore.

4 https://cip.gov.ua/ua/news/zafiksovano-poshirennya-shkidlivikh-program-cherez-telegram-nibito-vid-tekhnichnoyi-pidtrimki-rezerv

- З обережністю ставтеся до застосунків, які обіцяють підозріло вигідні функції.
- Перевіряйте дозволи, які запитує застосунок, і відмовляйте у доступі, якщо вони здаються невиправданими.
- Використовуйте антивірусне програмне забезпечення для перевірки файлів та застосунків перед встановленням.
- Залишайтеся уважними та поінформованими про нові загрози в цифровій сфері.

Рекомендації

Для захисту свого телеграм-акаунту від викрадення важливо вжити низку заходів безпеки. Ці рекомендації допоможуть мінімізувати ризики та забезпечити надійний захист від потенційних атак:

1. **Увімкніть двофакторну аутентифікацію (2FA).** У налаштуваннях телеграму активуйте двоетапну перевірку, встановивши надійний додатковий пароль для входу. Переконайтеся, що email, вказаний для відновлення, теж захищений двофакторною аутентифікацією і має складний пароль.
    - Що таке двофакторна аутентифікація
    - Як увімкнути двофакторну аутентифікацію в Telegram
    - Чому двофакторна аутентифікація надійніша за використання пароля
2. **Перевіряйте джерела.** Будьте обережні з посиланнями, навіть якщо вони надійшли від знайомих. Для додаткової безпеки використовуйте спеціальні онлайн-інструменти перевірки посилань. Завжди перевіряйте достовірність повідомлення, зв'язавшись із відправником через інші канали комунікації. Якщо хтось просить гроші чи надсилає підозрілі посилання, додатково з'ясуйте деталі особисто.
    - Як перевірити, що приховується за посиланням
    - Як зрозуміти, що ховається під скороченим посиланням
3. **Ніколи не вводьте дані аутентифікації та особисту інформацію через сторонні ресурси.** Не використовуйте телеграм для авторизації через інші ресурси, краще обирайте інші способи.
    - Які основні ознаки фішингових сайтів
    - Які ознаки можуть свідчити про те, що я натрапив на підробну веб-сторінку

4. **Регулярно перевіряйте активні сесії.** Перевіряйте, які пристрої підключені до вашого облікового запису, та завершуйте давні, незнайомі чи ті сесії, в яких сумніваєтеся.
    - Як перевірити, які пристрої підключені до мого Telegram
5. **Використовуйте секретні чати.** Для чутливої інформації використовуйте функцію «секретних чатів», які забезпечують додатковий рівень шифрування і не зберігаються на сервері телеграму.
    - Що таке «секретний чат» в Telegram та навіщо він потрібен
    - Як увімкнути секретний чат у Telegram
6. **Захистіть SIM-карту.** Прив'яжіть до паспортних даних, або перейдіть на контрактну форму обслуговування; налаштуйте PIN-код для SIM-карти та активуйте захист від заміни SIM через мобільного оператора.
    - Як встановити пароль на SIM-карту
    - Викрадають номер телефону: як захиститися від нової хвилі шахрайства
7. **Використовуйте лише офіційні застосунки.** Завантажуйте телеграм виключно з офіційних джерел — App Store, Google Play або telegram.org. Не встановлюйте неофіційні чи піратські версії месенджера, навіть якщо вони пропонують привабливі додаткові функції.
    - Які ризики існують при встановленні мобільних застосунків
    - Як вберегти себе при встановленні мобільних застосунків
8. **Дотримуйтесь основних принципів кібергігієни.** Регулярно дізнавайтеся більше про цифрову безпеку, щоб уникнути ризиків і вчасно реагувати на загрози. Вивчайте основи кібергігієни, дотримуйтесь перевірених правил захисту в інтернеті та діліться знаннями з іншими.
    - Що таке цифрова безпека
    - 10 базових правил цифрової безпеки
    - Як не стати жертвою інтернет-шахрайства: 10 правил
    - 6 ознак, за якими ви розпізнаєте шахраїв у телеграмі
9. **Звертайтеся за консультацією до Nadiyno**. Якщо маєте питання стосовно безпеки в інтернеті або стали жертвою онлайн-шахрайства, звертайтеся на безоплатну гарячу лінію з цифрової безпеки Nadiyno.org.

Прогнози

Популярність платформи

Популярність телеграму зростає і, ймовірно, тенденція зберігатиметься. Наразі месенджером користуються близько 950 мільйонів людей у всьому світі, і їхня кількість стабільно збільшується. Завдяки зручності та широкому функціоналу він приваблює нових користувачів, але водночас стає зручною ціллю для зловмисників.

Загрози безпеці

Основні загрози для телеграм-акаунтів — соціальна інженерія та фішинг, і вони залишатимуться актуальними. З ростом цифрової активності атаки стануть складнішими, а розпізнати їх буде важче навіть досвідченим користувачам. Оскільки ці методи ефективні та прості у виконанні, зловмисники продовжать вдосконалювати свої техніки, створюючи ще більш переконливі фішингові схеми.

Штучний інтелект та фішинг

Штучний інтелект стає потужним інструментом для фішингу. AI вже може імітувати стиль спілкування конкретних осіб, що підвищує успішність атак. У майбутньому ШІ зможе ще краще:

- створювати персоналізовані фішингові повідомлення з урахуванням психології жертви,
- генерувати реалістичні голосові та відеоповідомлення (deepfake phishing),
- визначати оптимальний час для атаки на основі поведінкових даних.

Також ШІ може використовуватися зловмисниками для автоматичної генерації фішингових вебсайтів з використанням обфускованого коду, який складніше аналізувати та виявляти системами безпеки. Зокрема, це дозволить:

- масово генерувати шкідливий код, який важко виявити,
- маскувати загрози у звичайних функціях вебсторінок,
- динамічно створювати різні версії фішингових сайтів для обходу списків блокувань.

Нещодавно, до прикладу, експерти Palo Alto Networks розробили алгоритм машинного навчання, який використовує великі мовні моделі (LLM) для створення обфускованого JavaScript-коду[5]. У 88% випадків ця технологія успішно обходила системи виявлення загроз.

[5] https://unit42.paloaltonetworks.com/using-llms-obfuscate-malicious-javascript/

Вдосконалення безпеки телеграму

Телеграм розвиває свої механізми безпеки, зокрема впровадивши інноваційну систему верифікації від третіх сторін[6]. Це децентралізоване рішення дозволяє авторизованим сервісам надавати додаткові значки верифікації для акаунтів та чатів, що значно полегшує ідентифікацію офіційних джерел інформації та допомагає у боротьбі з шахрайством і дезінформацією. Ми очікуємо, що телеграм продовжить удосконалювати механізми безпеки та розширювати функціонал для захисту користувачів.

Подальша діяльність Nadiyno

Команда Nadiyno продовжить дослідження у сфері кібербезпеки та роботу над вдосконаленням інструкцій і рекомендацій щодо відновлення доступу до викрадених облікових записів.

Ми плануємо:

- розширювати інформаційні матеріали про захист облікових записів,
- покращувати процедури допомоги користувачам, які стали жертвами атак,
- впроваджувати нові методики виявлення та попередження шахрайств.

Наша мета — підвищити рівень цифрової безпеки українських громадян та сприяти формуванню культури свідомого користування технологіями. Ми прагнемо забезпечити доступ до актуальної інформації про кіберзагрози, розробляти ефективні стратегії захисту та сприяти розвитку інструментів для запобігання шахрайству та зловживанням у цифровому просторі.

Висновки

Результати дослідження демонструють, що найчастіше користувачі самі надають доступ до своїх облікових записів зловмисникам — через неуважність або недостатню обізнаність. Наразі неможливо повністю завадити шахраям створювати і розміщувати фішингові вебсайти. Тож найкращий спосіб боротьби — швидке виявлення, подання скарг, блокування таких ресурсів та підвищення рівня цифрової гігієни на загальнонаціональному рівні.

Хоча телеграм і має вбудовану антиспам систему, вона не може забезпечити стовідсотковий захист від фішингових атак з кількох причин. По-перше, платформа обслуговує сотні мільйонів користувачів, які щодня обмінюються величезною кількістю повідомлень. По-друге, шахраї постійно створюють нові фішингові сайти, які ще не внесені до бази підозрілих ресурсів, тож автоматичні системи не завжди встигають їх виявити.

---

[6] https://telegram.org/blog/collectible-gifts-and-more/uk?ln=a#verifkatsya-vd-treth-storn

Якщо ж говорити про боротьбу з причинами, а не лише наслідками, то найдієвішим способом захисту є підвищення обізнаності користувачів щодо кібербезпеки. Освіта в питаннях кібергігієни та розуміння ризиків можуть значно знизити кількість успішних атак шахраїв.

База знань Nadiyno містить широкий спектр відповідей на запитання щодо безпеки у кіберпросторі. Якщо потрібної відповіді немає, ви завжди можете звернутися на безоплатну гарячу лінію з цифрової безпеки. Наші експерти допоможуть із питаннями особистої та корпоративної безпеки в інтернеті.

Використані ресурси

- **Генрі Дем'янович**. «Як ламають Telegram: що робити та куди звертатись?», *Лойер*, 18 жовтня 2024. Доступно: https://loyer.com.ua/uk/yak-lamayut-telegram-shho-robyty-ta-kudy-zvertatys/
- **Юлія Поліковська**. «Шахраї зламують телеграм-акаунти за допомогою посилання на голосування за дівчину на конкурсі бальних танців»,
- *MEDIASAPIENS*, 27 травня 2024. Доступно: https://ms.detector.media/sotsmerezhi/post/35033/2024-05-27-shakhrai-zlamuyut-telegram-akaunty-za-dopomogoyu-posylannya-na-golosuvannya-za-divchynu-na-konkursi-balnykh-tantsiv/
- **Світлана Кирилова**. «Волинянам масово розсилають у Telegram фішингове посилання», *Інформаційне агентство «Район ін юа»*, 20 січня 2023. Доступно: https://rayon.in.ua/news/568060-volinyanam-masovo-rozsilayut-u-telegram-fishingove-posilannya
- **Голос Громад**. «У Телеграмі шириться новий вид фішингу», *Голос Громад*, 15 лютого 2024. Доступно: https://kntp.com.ua/2024-02-15/u-telehrami-shyrytsya-novyy-vyd-fishynhu/
- **CERT-UA**. «Тематика голосування в месенджерах — новий спосіб викрадення акаунтів набирає обертів (CERT-UA#9688)», *CERT-UA*, 30 травня 2024. Доступно: https://cert.gov.ua/article/6279491
- **Лужна Софія**. «Telegram під атакою в Україні: як убезпечити свій акаунт від злому», *Український технологічний портал iTechua*, 27 серпня 2024. Доступно: https://itechua.com/news/265392
- **CYFIRMA**, «Inside FireScam : An Information Stealer with Spyware Capabilities», *CYFIRMA*, 30 грудня 2024. Доступно:

https://www.cyfirma.com/research/inside-firescam-an-information-stealer-with-spyware-capabilities/

- **Державна служба спеціального зв'язку та захисту інформації України**. «Зафіксовано поширення шкідливих програм через Telegram нібито від технічної підтримки „Резерв+“», *Державна служба спеціального зв'язку та захисту інформації України*, 16 жовтня 2024. Доступно: https://cip.gov.ua/ua/news/zafiksovano-poshirennya-shkidlivikh-program-cherez-telegram-nibito-vid-tekhnichnoyi-pidtrimki-rezerv

- **CERT-UA**. «Розповсюдження MEDUZASTEALER засобами Telegram, начебто, від імені технічної підтримки Резерв+ (CERT-UA#11603)», *CERT-UA*, 16 жовтня 2024. Доступно: https://cert.gov.ua/article/6281018

- **Yurii Prokopyshyn**. «Як зламують Telegram, що робити якщо зламали?», *Блог HyperHost*, 11 листопада 2024. Доступно: https://hyperhost.ua/info/uk/iak-zlamuiut-telegram-shho-robiti-iakshho-zlamali

- **CyberLab**. «Вразливості Telegram та відновлення доступу до акаунту», *CyberLab*, 1 жовтня 2024. Доступно: https://cyberlab.ua/archives/5922

- **Мар'яна Капранова**. «Найпоширеніші цифрові атаки на журналістів у 2020-му», *Інститут масової інформації*, 23 грудня 2020. Доступно: https://imi.org.ua/monitorings/najposhyrenishi-tsyfrovi-ataky-na-zhurnalistiv-u-2020-i36844

- **Cybercalm**. «Telegram зламали за допомогою SMS-кодів: як вберегтися від кіберзлочинців?», *Кібертиша*, 5 грудня 2019. Доступно: https://cybercalm.org/novyny/telegram-zlamaly-za-dopomogoyu-sms-kodiv-yak-vberegtysya-vid-kiberzlochyntsiv/

- **Ярослав Герасименко**. «Журналіст-розслідувач „Схем“ заявив, що його акаунт у Telegram намагалися зламати. Перехопили SMS для входу», *Громадське Телебачення*, 19 лютого 2024. Доступно: https://hromadske.ua/posts/zhurnalist-rozsliduvach-shem-zayaviv-sho-jogo-akaunt-u-telegram-namagalisya-zlamati-perehopili-sms-dlya-vhodu

- **Ірина Земляна**, «Кібержесть. Як журналістів переслідують в інтернеті», *Інститут масової інформації*, 25 лютого 2021. Доступно: https://imi.org.ua/monitorings/kiberzhest-yak-zhurnalistiv-peresliduyut-v-interneti-i37803

- **Блог Binance**, «Залишайтеся в безпеці: як розпізнавати й уникати шахрайств у Telegram», *Блог Binance*, 28 червня 2024. Доступно: https://www.binance.com/uk-UA/blog/all/залишайтеся-в-безпеці-як-розпізнавати-й-уникати-шахрайств-у-telegram-5644955869257264091