МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ

ТЕХНОЛОГІЇ, ІНСТРУМЕНТИ ТА СТРАТЕГІЇ РЕАЛІЗАЦІЇ НАУКОВИХ ДОСЛІДЖЕНЬ

4 СЕРПНЯ 2023 РІК

М. ДНІПРО, УКРАЇНА

OPEN ACCESS

DOI 10.36074/mcnd-04.08.2023
ISBN 978-617-8126-39-1

УДК 001 (08)
Т 38

https://doi.org/10.36074/mcnd-04.08.2023

Організація, від імені якої випущено видання:
ГО «Міжнародний центр наукових досліджень»

Голова оргкомітету: Рабей Н.Р.

Верстка: Білоус Т.В.
Дизайн: Бондаренко І.В.

Конференцію зареєстровано Державною науковою установою «УкрІНТЕІ» в базі даних науково-технічних заходів України та бюлетені «План проведення наукових, науково-технічних заходів в Україні» (Посвідчення № 68 від 17.01.2023).

Т 38 **Технології, інструменти та стратегії реалізації наукових досліджень**: матеріали VI Міжнародної наукової конференції, м. Дніпро, 4 серпня, 2023 р. / Міжнародний центр наукових досліджень. — Вінниця: Європейська наукова платформа, 2023. — 200 с.

ISBN 978-617-8126-39-1
DOI 10.36074/mcnd-04.08.2023

Викладено матеріали учасників VI Міжнародної спеціалізованої наукової конференції «Технології, інструменти та стратегії реалізації наукових досліджень», яка відбулася 4 серпня 2023 року у місті Дніпро.

УДК 001 (08)

ISBN 978-617-8126-39-1

СЕКЦІЯ XVI.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

КРИПТОГАМАНЦІ ТА РІЗНОВИДИ АТАК НА НИХ

Демидов Захар Георгійович
ORCID ID: 0000-0003-2821-8047
Старший науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі
Харківський національний університет внутрішніх справ, Україна

Хлестков Олексій Володимирович
ORCID ID: 0000-0001-8777-8269
Старший науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі
Харківський національний університет внутрішніх справ, Україна

Зі зростанням популярності криптовалют у всьому світі, з'являється все більше способів їх зберігання. Однак разом з цим розширюється і арсенал зловмисників, які прагнуть опанувати цифрові гроші. Рівень захисту та сума, доступна для крадіжки, визначають складність використаних шахраями технологій та ступінь ретельності, з якою вони імітують легітимні ресурси.

Ми розглянемо два протилежні підходи до атак електронною поштою на два найпопулярніші способи зберігання криптовалюти: гарячі та холодні гаманці.

Гарячий гаманець (hot wallet) [1] є криптовалютним гаманцем, який постійно знаходиться в мережі Інтернет. Фактично це будь-який онлайн-сервіс, який надає послуги зберігання криптовалюти, від криптобірж до спеціалізованих додатків.

Гарячі гаманці є поширеним способом зберігання криптовалюти. Це пояснюється кількома чинниками: по-перше, створення такого гаманця досить просте, достатньо зареєструвати аккаунт на одному з сервісів, і по-друге, кошти з нього легко виводити та конвертувати в інші валюти. Через свою популярність та простоту використання, гарячі гаманці стають основною метою для зловмисників.

Проте є одна особливість: через те, що гарячі гаманці завжди підключені до інтернету, на них рідко зберігають великі суми. Тому зловмисникам варто не дуже вкладатись у складні фішингові кампанії. Натомість атаки на такі гаманці зазвичай використовують прості та неоригінальні методи, орієнтовані на недостатньо досвідчених користувачів.

Приклад типової фішингової атаки на власника гарячого криптогаманця виглядає так: зловмисники відправляють поштові повідомлення від імені відомої криптобіржі з проханням підтвердити транзакції або повторно верифікувати гаманець.

При переході на посилання користувач потрапляє на підроблену сторінку, де йому пропонується ввести сід-фразу. Сід-фраза (seed phrase або recovery phrase) [2] — це послідовність із 12 (або рідше 24) слів, яка потрібна для відновлення доступу до гаманця. По суті, це основний пароль від гаманця. Якщо зловмисники отримують доступ до сід-фрази, вони можуть отримати повний контроль над обліковим записом користувача та вивести всі кошти на свої адреси.

Такі схеми атак зазвичай націлені на масових користувачів та досить прості, не вимагають складних технічних чи психологічних прийомів. Форма введення сід-фрази зазвичай мінімалістична і містить лише поле для введення та логотип біржі, жодних додаткових елементів.

Холодний гаманець (cold wallet або cold storage) [1] є криптовалютний гаманець, який не завжди підключений до інтернету. Це може бути окремий фізичний пристрій або навіть записаний на папері приватний ключ. Найпоширенішим видом холодних гаманців є апаратні гаманці.

Користувачі вважають за краще зберігати значні суми на холодних гаманцях, оскільки вони практично завжди залишаються офлайн, що унеможливлює віддалений доступ до них. Проте варто зазначити, що холодні гаманці також можуть бути скомпрометовані, хоча для цього зловмисникам необхідно отримати фізичний доступ до них або вкрасти їх.

Зловмисники застосовують соціальну інженерію, щоб отримати доступ до активів користувачів, навіть якщо вони зберігають свої кошти на апаратних холодних гаманцях. Вони можуть використовувати різні методи, наприклад, атаки фішинга. Нещодавно було помічено, що зловмисники проводять поштове розсилання, яке націлене саме на власників апаратних холодних гаманців.

Наприклад, такі атаки можуть починатися з масових розсилок на тему криптовалюти, де користувачеві пропонується брати участь у роздачі токенів XRP від відомої криптобіржі Ripple. При переході на посилання користувач потрапляє на підроблену сторінку блогу, на якій пропонується зареєструватися.

Зловмисники намагаються зробити сторінку максимально схожою на офіційний сайт, використовуючи punycode-атаку для підробки доменного імені. Після того, як користувач вводить адресу свого XRP-акаунта, сайт пропонує вибрати метод авторизації для отримання бонусних токенів.

Апаратні гаманці, такі як Trezor та Ledger, часто стоять першими у списку запропонованих методів. При виборі одного з них користувач переадресується на офіційний сайт виробника апаратного гаманця. Зловмисники хочуть, щоб користувач підключив свій пристрій до їхнього фішингового сайту і дав їм можливість здійснювати транзакції з його рахунку.

Далі зловмисники використовують API фішингового сайту та веб-сокет офіційної криптобіржі Ripple для взаємодії з XRP-акаунтом жертви. Вони генерують одноразові проміжні гаманці, щоб приховати кінцеву адресу виведення від виявлення. Ці проміжні рахунки використовуються лише для отримання коштів від жертви та подальшого виведення їх на адресу зловмисників, що робить операцію складнішою для відстеження.

Зловмисники, націлені на апаратні гаманці, дійсно застосовують складніші тактики, ніж при атаках на користувачів онлайн-сервісів. Хоча апаратні криптогаманці вважаються більш надійними та безпечними, власникам слід залишатися пильними та вживати заходів для захисту своїх активів.

Перед тим, як надати доступ до свого гаманця якомусь ресурсу, важливо ретельно перевірити всі дані та підходити з обережністю до подібних запитів. Якщо є

хоч найменші сумніви щодо справжності запиту чи посилання, краще відмовитися від підключення. Важливо пам'ятати, що ніякий сервіс чи організація не повинні вимагати вашу сід-фразу, приватний ключ або інші приватні дані. Ці дані повинні залишатися суворо конфіденційними та не передаватися третім особам.

Також, щоб зменшити ймовірність атакувати, рекомендується купувати апаратні гаманці тільки у офіційних та надійних виробників, а також оновлювати програмне забезпечення пристрою вчасно. При появі підозрілої активності або незвичайних запитів слід негайно звернутися до служби підтримки виробника апаратного гаманця для отримання допомоги та порад.

Пильність та усвідомлення потенційних загроз допоможуть власникам апаратних гаманців захистити свої криптовалютні активи та убезпечити себе від шахрайства.

Список використаних джерел:

1. Гарячі гаманці проти холодних гаманців: у чому різниця? Вилучено з: https://coinmarketcap.com/alexandria/uk/article/hot-wallets-vs-cold-wallets-whats-the-difference.
2. Що таке сід-фраза (seed phrase)? Вилучено з: https://tsecrypto.com/article/shho-take-sid-fraza-seed-phrase.